MASTER THESIS

DEPLOYING SECURITY FORCES TO INTERCEPT THREATS

T.L.C. van der MIJDEN

ELECTRICAL ENGINEERING, MATHEMATICS AND COMPUTER SCIENCE
APPLIED MATHEMATICS
INDUSTRIAL ENGINEERING AND OPERATIONS RESEARCH
STOCHASTIC OPERATIONS RESEARCH

EXAMINATION COMMITTEE
prof. dr. R.J. Boucherie
dr. J.B. Timmer
dr. G.J. Still
dr. H. Monsuur

DOCUMENT NUMBER
TW - M2012 – 15595

UNIVERSITY OF TWENTE.

25 JUNI 2012

Abstract

To protect valuable objects and critical infrastructures, security forces are often deployed to surveil and patrol assigned areas, aiming to intercept incoming threats. This study's purpose is to help deploy these security forces most effectively, while taking into account that these forces operate in an uncertain environment and are often faced with multiple threats. To do this, an interdiction game on a queueing network is developed and analyzed. We prove the existence of optimal strategies and locate these strategies for special networks. In application of this research, counter-piracy efforts are considered. We analyze the deployment of naval ships to patrol areas to intercept pirates attempting to reach shipping lines. We provide a method to determine where available naval ships should patrol to reduce pirate attacks maximally.

Management summary

Motivation
To protect valuable objects and critical infrastructure, security forces are often deployed to surveil and patrol assigned areas. The purpose of these forces is the interception of incoming threats before actual damage can be done. The question that arises in deploying security forces is how to deploy these forces optimally, i.e. where are these forces deployed most effectively?

Goals
This study's purpose is to help answering this question. We assume that threats, e.g. terrorists, move through a network attempting to reach a certain destination. Security forces are deployed in this network to surveil network sections and intercept encountered threats. We take into account that security forces operate in a stochastic environment, one never knows when and where the next threat will emerge. We also allow for multiple active threats at the same time. The question we will answer is:

How to deploy security forces in the network in order to minimize the number of threats reaching their destination?

Furthermore, in direct application of our research, we consider counter-piracy operations in the Somali Basin. Pirates operating from Somalia, move to shipping routes to hijack passing merchant ships. To counter this piracy threat, naval ships are deployed in patrol areas to surveil maritime traffic and to intercept pirates. We investigate the optimal deployment of these naval ships.

Approach
To answer these questions, we study an interdiction game on a queueing network. An interdiction game describes how two adversaries compete over a value of a system. In our application, the two adversaries are the naval forces and the pirates and the value over which they compete is the number of successful pirate attacks. A queueing network allows us to incorporate the stochastic time environment and multiple threats.

Results
We prove that in an interdiction game on a queueing network optimal mixed strategies exist for both players. Moreover, we prove that there exists an optimal pure strategy for the deployment of security forces. The location of these optimal strategies is found in case of networks of parallel queues or tandem queues. For simple networks, the developed interdiction game can be applied to determine the optimal deployment of security forces in a network. This is done in the context of counter-piracy. We provide insight in the effects of deploying naval ships in the Somali Basin to counter the threat of piracy. Moreover the method presented, can be used to determine where available naval ships should patrol to reduce successful pirate attacks maximally. Also we show that equipping naval ships with Unmanned Aerial Vehicles may descrease the number of naval ships needed for counter-piracy significantly.

Preface

Around June 2010, I had my first appointment with the chair holder of the Stochastic Operations Research (SOR) group, Prof. Dr. R.J. Boucherie, to discuss my graduation program at the University Twente. During this meeting we talked about my preference to apply operations research within the military domain. Months before this first meeting, I had followed an academic minor in military sciences which rekindled my youth interest in military subjects. It was then, that I decided to explore the possibility to apply my math skills to problems arising from the military domain.

After being brought into contact with Dr. H. Monsuur of the Netherlands Defense Academy (NLDA), the research direction was established. It was no surprise that it would include both queueing theory, an expertise of the SOR group, and game theory, an expertise of the Operations Research group at the NLDA.

The research started quite theoretical, which was fine for the beginning, but over time it brought down my motivation. New motivation came along with the opportunity to apply my research to counter-piracy operations in the Somali Basin. Commander P.J. van Maurik of the Royal Netherlands Navy was doing research on (counter-) piracy activity and could use my research to obtain some insight in optimal deployment of naval forces and its effect on piracy activity. Talking about naval ships, patrol areas and pirates instead of queues and customers was a welcome change.

I would like to thank everyone who has supported me during my graduation. In particular my thanks to my supervisors Richard Boucherie and Herman Monsuur, with the help of their knowledge, supervising skills and enthusiasm, I was able to bring forth this research. Also I would like to thank Peter van Maurik for giving me insight in the piracy problem in the Somali Basin and for all the interesting conversations we had. Thanks to all colleagues, fellow student, friends and family for all their support to me and my research.

Tom van der Mijden

Table of contents

1 Introduction

1.1 Background

Over the last decade, *critical infrastructure protection* has received considerable attention. Economy and society are more and more dependent on infrastructures such as energy, transport and telecommunications. This increases the need to identify and protect those infrastructure elements that, if lost, would cause significant disruption of the (inter)national economy and society. The loss of infrastructure can be caused by random events (e.g. earthquakes) or intentional attacks (e.g. terrorist attacks). These causes constitute probabilistic respectively strategic risks to infrastructure. Protecting critical infrastructure against strategic risks is of great concern to homeland security, especially after the terrorist attacks of September 2001. Homeland security and protection is often a task of intercepting threats before any harm is done and is always faced with uncertainty, one will never know when the next threat will emerge. Here, threats may be interpreted as nuclear weapons being smuggled from country to country or pirates attempting to hijack merchant vessels. Another very topical interpretation is the threat of cyber-attacks, although much more interpretations are possible.

To intercept threats security forces may rely on intelligence and respond whenever a new threat emerges. However security forces may also be deployed, actively surveilling areas and searching for threats. The latter case is often applied when threats occur regularly, e.g. pirate attacks in the Somali Basin. Although threats may arrive regularly, the time of appearance is always uncertain. This is inconvenient, because in order to intercept a threat one has to be at the same place at the same time. On the other hand, security forces themselves cannot be predictable in their search patterns and schedules, since that would surely be exploited by those imposing the threats.

In the context of piracy, the Somali Basin is a current stage for such a problem. In 2011 there were 160 pirate attacks reported in de Somali Basin and even more attacks were attributed to pirates operating from Somalia. Over the last years, this number of pirate attacks has increased vastly. Therefore, several coalitions and countries have sent naval ships to the area to surveil maritime activity and intercept pirates. Due to the expanse of the area, a single naval ship has to cover a great area and cannot surveil the whole assigned patrol area at any time and timing is crucial in the interception of pirates.

When deploying security forces with the task of surveilling and patrolling certain areas, the purpose is to minimize the number of threats that become actual attacks. The question that arises is; how to deploy the available security forces in the most effective manner, i.e. to minimize the number of threats not being intercepted. This question is the main focus of this research.

Homeland security is faced with intelligent adversaries. Those imposing threats like pirates or terrorists think rationally and aim to maximize the effect of their actions. This implies

that most homeland security issues are strategic in nature. To help decision-making in strategic environments, game theory provides a way. Much research has been done in the area of *game-theoretic risk analysis* applied to homeland security and defense (see e.g. Bier and Azaiez (2009)). An important class of game-theoretic models in the field of homeland security and defense are interdiction models. Brown et al. (2006) apply such an interdiction (or *attacker-defender*) model to assess infrastructure vulnerability to intentional attacks. These interdiction models may also be applicable to issues concerning deployment of security forces to intercept threats.

1.2 Interdiction models

1.2.1 Overview of interdiction models

An interdiction model describes an infrastructure system and its value, including how the actions of two adversaries influence this value. The two adversaries, often called the interdictor and the operator, have opposite goals; while the operator's goal is to maximize the value of the system, the interdictor attempts to minimize this value. Interpretation of the value may be very different depending on the actual system being modeled. For example the value may mean financial profit, production capacity or probability of non-detection. Interdiction models have a wide range of applications including hospital infection control (Assimakopoulus (1987)), electric power grid protection (Salmeron (2004)), ballistic missile defense (Brown et al. (2005)) and interdiction of a nuclear-weapons project (Brown et al. (2009)). Most interdiction models are *Stackelberg games*; the interdictor and operator perform their actions sequentially. Furthermore, since the interdictor and operator have opposite goals, these games are *zero-sum games*. To solve these Stackelberg games, the models are regularly formulated as bi-level (integer) programs, see for example Brown et al. (2006). An important class of interdiction models focuses on systems that can be described by a network consisting of arcs and nodes. This leads to the concept of network interdiction models.

Network interdiction models are optimization models, in which the interdictor performs interdiction actions on a network in order to minimize the maximum value the operator can obtain from the network. The network consists of nodes connected by arcs. In literature two models have received considerable attention. The first is the *maximum flow network interdiction* model. In this model the value to the operator is determined by the amount of flow he can put through the network. The second model, the *shortest path network interdiction* model, considers the case where the network value to the operator is determined by the length of the shortest path between two specified points. To impede the operator, the interdictor can perform interdiction actions on the network components. Interdiction actions change the components' capacity or length, often effectively removing the interdicted components from the network. Interdiction comes with a cost and the interdictor is limited in his actions by a budget. Two types of interdiction are considered; *discrete* and *continuous* interdiction. In case of discrete interdiction, interdiction actions have fixed cost and result in a fixed change of capacity or length. A special case of discrete interdiction is when actions have unitary costs and reduce the capacity to zero (or increase the length to infinity); in this case the interdictor can remove a number of network components limited by a cardinality constraint. In case of continuous interdiction, the change in a component's capacity or length is often a linear function of interdiction resources allocated to this component. In some studies the success of an interdiction action is considered to be stochastic. Although in most cases information is symmetric, meaning that the interdictor and the operator have the same network information and agree on the network parameters, some studies have been done in which both actors have different perceptions of the network parameters. Also the use of deception is considered in some studies.

1.2.2 Literature on interdiction

Since in literature considerable attention is given to the maximum flow and shortest path interdiction models, we give an overview of the literature following this subdivision. In the *maximum flow network interdiction* model the operator maximizes the flow of some commodity from a source node through the network to an end node, while the interdictor attempts to minimize this flow by interdicting (e.g. removing) network components. One of the first to explore this field was Wollmer (1964), who was concerned with removing a fixed number of arcs in a network in order to minimize the maximum flow through the network. Corley and Chang (1974) also considered this model, but their interdiction actions consisted of removing a fixed number of nodes from the network. The maximum flow network interdiction model was generalized by Wood (1993), who considered interdiction costs for removing arcs. The interdictor in this case is constrained by an interdiction budget. Wood also showed the NP-hardness of the problem and developed an integer programming model. Phillips (1993) considered the case in which the decrease in arc capacity is linear in the interdiction efforts put in that arc. Other research was done by Lim and Smith (2007) and Royset and Wood (2007), who considered respectively models with multiple commodity flows and models in which the interdictor minimizes both the maximum flow and the interdiction costs. Stochastic variants of the maximum flow network interdiction model were studied by Cormican et al. (1998) and Janjarassuk and Linderoth (2008). In those models arc capacities and interdiction successes can be stochastic. Recent studies of Altner et al. (2010) and Zenklusen (2010) deal with the development of the methods of finding an optimal solution for the maximum flow network interdiction problem.

The *shortest path network interdiction* model considers an operator whose objective is to minimize the length of the shortest path between two specified points, while an interdictor attempts to maximize this length. The interdictor can remove or lengthen arcs subject to a resource constraint. Early work was done by Fulkerson and Harding (1977). In their model an interdiction action increases the length of an arc and the cost of this action is linear in the length increase. Corley and Sha (1982) and Malik et al. (1989) identify a fixed number of arcs in a shortest path network, whose removal would result in the greatest increase in the length of the shortest path between two specified points. Ball et al. (1989) generalize this problem by introducing removal costs for each arc and restrict the interdictor's actions by a budget constraint. They also show that their problem is NP-hard. Israeli and Wood (2002) formulate the shortest path network interdiction problem as a bi-level integer program. They consider binary interdiction variables, increasing the length of an arc by a fixed parameter if that arc is interdicted. Stochastic problems were investigated by Pan et al. (2003) and Morton et al. (2007). In their models the source-sink pair of the shortest path is only known through a probability distribution. Morton et al. (2007) also model the case in which the network user and the interdictor have different perceptions of the network parameters. In a deterministic setting Bayrak and Bailey (2008) also consider the concept of asymmetric information. Salmeron (2011) introduces deception to the (shortest path) network interdiction problem. In these models the interdictor may use de-

ception, effectively creating asymmetric information. Cappanera and Scaparra (2011) develop a multi-level optimization model to solve the shortest path network interdiction problem in which network components can be hardened, making them invulnerable to interdiction.

In the models described above, the interdictor and the network user move sequentially. First the interdictor changes the network, after which the operator optimizes his value using the altered network. However, there are some studies in which the interdictor and the operator choose their actions simultaneously. Washburn and Wood (1995) consider a shortest path network interdiction model, in which arc lengths are interpreted as detection probabilities. In their model an evader attempts to travel across a network undetected, while an interdictor sets up an inspection point. The evader chooses a path to travel and the interdictor chooses an arc to inspect, both making their decision without knowing the decision of their adversary. If the inspected arc is part of the chosen path, then the evader is detected with a certain probability. This problem establishes a normal zero-sum game, where the players choose a randomized strategy. Another study, done by Washburn and Ewing (2011), models a traffic network under threat by Improved Explosive Devices (IEDs). In this model a number of traffic units move over road segments per unit time. An interdictor places IEDs with a certain rate on these road segments, aiming to inflict maximum damage to the traffic. Simultaneously, the network user deploys IED clearance units, resulting in the removal of IEDs without damaging any traffic. The problem constitutes a game which is played indefinitely in time. Alpern et al. (2011) present a patrolling game. In this game, an attacker chooses to perform an attack on a certain node in a network. This attack will take some time periods, in which the attacker may be detected by a patroller. This patroller chooses a patrol schedule through the network, this schedule describes where the patroller is located in each time period. If the location of the patroller at some time period coincides with the location of the attacker, the attacker is intercepted and the patroller wins. This study provides insight to help schedule patrols through museums and other vulnerable facilities.

Another area of research is the study of *flow intercepting facilities*. These studies are concerned with locating facilities on a network, so as to intercept the maximum fraction of pre-existing network flows. Such models arise when one has to locate police radar units or advertising vehicles on traffic networks. Hodgson (1990) and Berman et al. (1992) introduce the problem by investigating the optimal locations for a fixed number of facilities in order to maximize the number of intercepted flow units. Berman et al. (1995) investigate the models in which either flow units can be intercepted only once or multiple times. For an extensive description of models and problems concerning flow intercepting facilities see Boccia et al. (2009). Although in these models there is no interaction between adversaries, i.e. there is only one actor, the research done in this area has some links to the network interdiction models. Especially in the single counting model of Berman et al. (1995), one can interpret locating a flow intercepting facility as an interdiction action on the network. The interdictor in this case aims to intercept as many flow units as possible.

1.3 Goals

Although the literature on network interdiction models is quite extensive and useful in the area of homeland security, there are some aspects that have not received much attention and yet may be relevant factors.

First of all, literature lacks *time-dependent interdiction* models. In the studies on interdiction, the focus is on static, time-independent models. The maximum flow interdiction models consider static flows and in the shortest path interdiction models, the operator is not actually moving along the path in time. In addition literature describes, with some exceptions, interdiction models in which timing of interdiction actions is not relevant. However, one can imagine situations in which units are actually moving through the network in time and where interdiction actions can only be executed in certain time windows. For example, the interception of a terrorist can only take place after its detection and before it reaches its destination and causes some harm (e.g. see Wein and Atkinson (2007)). Also, one can only interdict a task of a weapons manufacturing project when it is not yet finished. Besides, like in the case of a terrorist interception, one often cannot use the same interdiction resource (e.g. a police car) for multiple interdiction efforts at the same time. Although timing is crucial in intercepting threats before they become actual attacks, few studies incorporated a time element in their research.

The second aspect arises from the evader-detection models like in Washburn and Wood (1995). In these models only single evaders are considered. *Multiple evaders* or threats are not considered. Yet it is not unlikely that multiple threats are active at the same time and while intercepting a first threat, a second threat may pass unchecked. So the notion of multiple threats is one of quite importance in interdiction models.

The application of the theory that will be developed in this study deals with the deployment of security forces to intercept threats. Deployed forces surveil and patrol assigned areas and intercept encountered threats. We will take into account that these forces operate in a stochastic time environment; threats emerge at random points in time and search patterns and schedules have some degree of unpredictability. Moreover since patrolling forces are often deployed to counter threats which appear frequently, we allow for multiple active threats at the same time. Our concern will be to deploy the available security forces in the most effective manner.

In direct application of the theory we discuss counter-piracy operations. To counter piracy in the Somali Basin, maritime patrol areas are established and naval ships are allocated to these areas to intercept pirates moving to shipping routes. Our objective will be to allocate the available naval ships in order to minimize the number of successful pirate attacks by intercepting them during their transit to their areas of operation.

In order to address these issues, a time-dependent interdiction model with multiple operator units is developed, where security forces relate to the interdictor and threats relate to units

the operator sends through the network. We will consider *dynamic network flows*, i.e. flows of which units are actually moving through the network in time. Moreover we assume that each single flow unit is vulnerable to interception while moving through the network. The model relates to both the maximum flow and shortest path network interdiction. Each single flow unit can be seen as a single threat attempting to reach its destination undetected, yet together the threats constitutes a flow, which is to be maximized by the operator.

An interdictor and an operator compete over these network flows. The interdictor aims to minimize the value the operator can obtain from the dynamic flow network, while the operator tries to maximize this value. We will mainly be concerned with models in which the value will be determined by the number of flow units reaching their destination, i.e. the throughput. However, also other values may be considered, such as the expected travel time from source to destination for a single flow unit (provided the flow unit reaches its destination), or the probability that at least a certain fraction of the flow reaches its destination. Furthermore the operator may route different types of flow units through the network, each type with its own value.

The interdiction strategy will consist of the allocation of security agents to the network. Agents will intercept flow units (threats) if they are at the same location at the same time. Several allocation strategies may be considered. Each agent may be allocated to a specified location or may patrol several locations. Also agents can be stationed at a base location and move from this base to other network locations. Furthermore, detection and interception can be separated by introducing detection sensors to the network, like in Yates et al. (2011). Other cases may consider agents that act dependent on available information.

The main research question in the context of the counter-piracy application is:

- *How to allocate available naval ships to patrol areas in order to minimize the number of successful pirate attacks?*

In the development of the theory we generalize this to:

- *How to deploy available interception resources in a dynamic flow network in order to minimize the total throughput of the network?*

1.4 Approach

To model dynamic flow networks and the actors on these networks, we will combine two separate areas of research; game theory and queueing theory. Where game theory provides a way to model the interaction between the interdictor and the operator, queueing theory can be used to model the dynamic flows and time-dependent interdictions in a stochatic environment. In queueing models, the movement of a flow unit, usually called a customer, is actually modelled in time; the unit arrives at a certain time at the queue, there it has to wait and/or receives service for some time and then moves on, possibly to another queue. Since a queueing model describes precisely where a flow unit is located in the system at a given time, it is also possible to intercept this unit at a certain time and location. Moreover queueing theory gives us tools to model interaction between customers and/or agents.

Although there are some studies that incorporate queueing theory in their analysis, the use of queueing theory in the area of interdiction models remains virtually unexplored. Atkinson and Wein (2008) and Yates et al. (2011) use respectively a spatial queueing model and a hypercube queueing model to analyze the performance of interception units chasing vehicles that pose a potential threat. Further, in the research of Washburn and Ewing (2011) an infinite-server queue is used to model the number of IEDs located on a road segment. But apart from these studies, queueing models and interdiction models are rarely combined.

In our research we use queueing theory to model and analyze the time-dependent behavior in our interdiction models. We replace the usual network of nodes and arcs in network interdiction models by a network of interconnected queues. In these networks of queues, customers (flow units) move through the network via several queues. At the queues the customers have to stay for some time, possibly depending on the presence of other customers. These customers are called positive or regular, because upon arrival at a queue they increase the number of customers at this queue. We use the notion of negative customers, introduced by Gelenbe (1991), to model the agents who intercept the flow units. Upon arrival at a queue, negative customers remove a regular customer, if present, from that queue. Removed customers are interpreted as intercepted customers and do not add to the throughput of the network. Now the problem is described as follows. The operator has to route the regular customers through the network in order to maximize the throughput. The interdictor on the other hand decides on the arrival rates and routing of the negative customers, while aiming to minimize the throughput.

The main research question can be reformulated as

- *What are optimal strategies for the interdictor and operator in a queueing network in order to maximize, respectively minimize the throughput of the network?*

To answer this question, first the following subquestion are answered:

- *Do there exist optimal strategies for the interdictor and the operator?*
- If optimal strategies exist, *are these optimal strategies mixed or pure strategies?*

- If optimal strategies exist, *are we able to find them in general and/or specific cases?*

Several distinctions in the models can be made with regard to the type of the queue and the characteristics of the negative customers.

Type of the queues
Our main focus is on the single server queues, but one may also consider infinite server queues. In networks of single server queues, the time a customer spends at a queue is dependent on the number of other customers present at that queue, this in contrast to a network of infinite server queues. In these networks the time spend at a queue by a customer is independent of other (regular) customers.

Customer removal policies
Upon arrival of a negative customer at a queue, several removal policies can be considered. The negative customers may remove only one customer (e.g the one being served), a subset of the present customers or it may remove all customers it finds present at that queue. Furthermore, in case only one customer is removed, the removed customer may have been any of the present customers or a specific one, e.g. the customer that arrived first at that queue.

Negative customer allocation
There are two methods to allocate negative customers. Negative customers may be allocated to specific queues, arrive from outside the network and leave the network upon leaving a queue. However, a negative customer may also be allocated to a number of queues. Upon leaving a queue such negative customer is routed to another queue, possibly with some delay. This second method models agents that are patrolling several locations. In this study negative customers are allocated to specific queues.

1.5 Report structure

This report is structured as follows. Section 2 describes the proposed model, both the queueing and the game theory aspects are discussed. This section also gives a relation to existing literature. Section 3 is concerned with the existence of optimal strategies and, if they exist, whether they are mixed or pure strategies. In section 4 some special cases are analyzed and also some model extensions are discussed. Section 5 applies the developed model to a current defense issue, the hijacks attempts of pirates operating from Somalia. Results of this application are found in section 6. The report closes with section 7 giving some final conclusions and topics for further research.

2 Basic model

2.1 Introduction

To address the allocation problem of security forces in a network to intercept threats effectively, a model needs to be developed. This section descibes the formation of an interdiction game on a queueing network. The part concerning the interdiction game incorporates the aspect of an intelligent opponent, while the part involving queueing theory incorporates the stochastic time environment and the notion of multiple threats. In the first section the network is described, where each node of the network represents a queue. Thereafter some basic analysis is given concerning the stationary distribution of the network and the probability of intercepting a threat. In section 2.4 the game is descibed, with action sets and payoff function. The last section relates the described model to a model already studied in literature.

2.2 Network description

Let G be a network with source node 0, sink node $J+1$ and a set of intermediate nodes $I = \{1, \ldots, J\}$, see figure 1. The whole set of nodes is denoted by V, $V = \{0, 1, \ldots, J, J+1\}$. The set of links in the network is denoted by E, node j is connected to node k if $(j,k) \in E$. The forward star $FS(j)$ of node j is the set of all nodes k for which $(j,k) \in E$, i.e. $FS(j) = \{k|(j,k) \in E\}$. Likewise, the backward star $BS(j)$ of node j is the set of all nodes k for which $(k,j) \in E$, i.e. $BS(j) = \{k|(k,j) \in E\}$. A path l is a finite sequence of nodes $(l_1, \ldots, l_{m(l)})$ such that $l_i \in V$ for $i = 1, \ldots, m(l)$ and $(l_i, l_{i+1}) \in E$ for $i = 1, \ldots, m(l)-1$, where $m(l)$ denotes the length of path l. We denote by L the set of all possible paths from node 0 to node $J+1$. A simple path is a path in which no node is visited twice, i.e. a path without cycles. The set of all simple paths is denoted by $\bar{L}$.

We assume that in G there are no links entering node 0, i.e. $BS(0) = \emptyset$, and there are no links leaving node $J+1$, i.e. $FS(J+1) = \emptyset$. Furthermore we assume that there is at least one path from node 0 to node $J+1$, but there is no link between node 0 and node $J+1$, i.e. $(0, J+1) \notin E$.

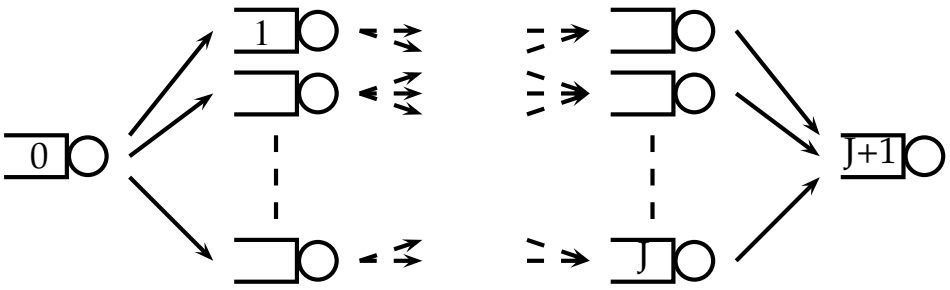

Figure 1: The network G

Each node in the network G represents a queue where regular (or positive) customers arrive and are served by a single server according to a FIFO service discipline. These customers arrive from the outside of the network at node 0 according to a Poisson process with rate γ. The total arrival rate of regular customers at queue j is denoted by λ_j^+. The service time at node j is exponentially distributed with mean $1/\mu_j$. After service completion at node j, a regular customer is routed to node k with probability $r(j,k)$. Regular customers leave the network after finishing service at node $J+1$. We refer to R as the transition matrix with elements $r(j,k)$. Since customers can only leave the network at node $J+1$ we have

$$\sum_{k=0}^{J+1} r(j,k) = 1, \quad \text{for } j = 0, \ldots, J. \tag{1}$$

Furthermore, customers cannot be routed over links that do not exists, so

$$r(j,k) = 0, \quad \forall (j,k) \notin E.$$

In addition to regular customers also negative customers arrive at queues $j \in I$. The concept of negative customers was first introduced by Gelenbe et al. (1991). Upon arrival of a negative customer a regular customer, if present, is removed from the network. If a negative customer arrives at an empty queue, the negative customer simply disappears. Negative customers do not receive service and are not routed through the network. Negative customers arrive at queue $j \in I$, according to a Poisson process with rate λ_j^-. For convenience we define $\lambda_0^- = \lambda_{J+1}^- = 0$ and denote by λ^- the vector of length $J+2$ with elements λ_j^-.

2.3 Stationary distribution

2.3.1 A single isolated node

The state of the network process can be described by the number of regular customers present at each node. Let n_j be the number of regular customers present at node j, the state is given by $n = (n_0, n_1, \ldots, n_{J+1})$. Our aim is to find the stationary distribution of the process, i.e. to find the probability that in equilibrium the network is in state n. This probability is denoted by $\pi(n)$. In order to determine the stationary distribution, we first consider a single node in isolation.

Consider node j in isolation and let $\pi_j(n_j)$ denote the stationary probability that there are n_j customers present at node j in equilibrium. The process satisfies the following balance equations.

$$\lambda_j^+ \pi_j(0) = (\mu_j + \lambda_j^-)\pi_j(1), \tag{2}$$

$$(\lambda_j^+ + \mu_j + \lambda_j^-)\pi_j(n_j) = \lambda_j^+ \pi_j(n_j - 1) + (\mu_j + \lambda_j^-)\pi_j(n_j + 1), \quad n_j \geq 1. \tag{3}$$

Equation (2) and (3) arise from balancing the probability flows in equilibrium. The solution to these equations is given by

$$\pi_j(n_j) = (1 - \rho_j)\rho_j^{n_j}, \quad n_j \geq 0, \tag{4}$$

where

$$\rho_j = \frac{\lambda_j^+}{\mu_j + \lambda_j^-} \tag{5}$$

and provided that $\rho_j < 1$. Note that this node with negative customers has the same dynamics as an ordinary M/M/1 queue with arrival rate λ_j^+ and service rate $\mu_j + \lambda_j^-$. The arrival of negative customers with Poisson rate λ_j^- has the same effect on the stationary distribution as increasing the service rate of the node with λ_j^-.

Let q_j be the probability that a regular customer leaves node j due to a service completion. This probability equals the departure rate due to service completion at node j divided by the total departure rate at node j. In equilibrium the total departure rate equals the total arrival rate. So we have,

$$q_j = \frac{\rho_j \mu_j}{\lambda_j^+}, \tag{6}$$

$$= \frac{\mu_j}{\mu_j + \lambda_j^-}. \tag{7}$$

Likewise, we have the probability that a customer is removed by a negative customers at node j,

$$1 - q_j = \frac{\lambda_j^-}{\mu_j + \lambda_j^-}. \tag{8}$$

One can obtain these probabilities also via some other reasoning. First assume that a negative customer will remove the regular customer in service. (This assumption may be dropped, but it helps to get some idea about the dynamics of the queue.) Both the interarrival time of a negative customer and the service time of a regular customer are exponentially distributed. The probability that a customer completes its service equals the probability when entering the service, the service time is smaller than the time until the next arrival of a negative customer. This probability equals the probability that an exponentially distributed variable with mean $1/\mu_j$ is smaller than an exponentially distributed variable with mean $1/\lambda_j^-$, this is precisely given by equation (7).

2.3.2 The network

In the network the arrival rates of regular customers are given by the traffic equations,

$$\lambda_j^+ = \sum_{k=0}^{J} \rho_k \mu_k r(k,j), \quad j = 1, \ldots, J+1, \tag{9}$$

$$\lambda_0^+ = \gamma. \tag{10}$$

Here, ρ_k is given by equation (4). Let e_j be a vector of length $J+2$ with the $(j+1)^{\text{th}}$ element equal to 1 and zeros elsewhere. Like in the case of a single node we can establish the balance equations which are satisfied by $\pi(n)$.

$$\pi(n) \sum_{j=0}^{J+1} \lambda_j^+ + (\mu_j + \lambda_j^-)\mathbf{1}[n_j > 0] = \sum_{j=0}^{J+1} \pi(n - e_j)\lambda_j^+ \mathbf{1}[n_j > 0] + \pi(n + e_j)(\mu_j + \lambda_j^-), \quad \forall n, \tag{11}$$

where $\mathbf{1}[x] = 1$ if x is true and 0 otherwise. Now, by quasi-reversiblity of M/M/1 queues, the stationary distribution of a network of M/M/1 queues is given by the product of the stationary distribution of each node in isolation. Since the dynamics of the nodes in our network are the same as an ordinary M/M/1 queue, we derive that the stationary distribution of the network is given by

$$\pi(n) = \prod_{j=0}^{J+1} \pi_j(n_j), \quad \forall n \geq 0. \tag{12}$$

with $\pi_j(n_j)$ given by equation (4).

Remark. For a more extensive discussion of queues with negative customers and networks of these queues see Gelenbe et al. (1991) and Gelenbe (1991).

2.4 Game description

In the described network, an operator and an interdictor compete over the throughput of the network; the departure rate of regular customers at node $J+1$. The operator aims to maximize this throughput by choosing an appropriate routing matrix R. The interdictor attempts to minimize the throughput by deciding on the arrival rates of the negative customers at the nodes. The resulting game is a zero-sum game, i.e. what the operator gains on throughput is lost by the interdictor.

The action set from which the operator can choose its action is given by

$$A_{operator} = \left\{ R \left| \sum_{k=0}^{J+1} r(j,k) = 1 \text{ for } j = 0, \ldots, J,\ r(j,k) \geq 0,\ \forall (j,k) \in E,\ r(j,k) = 0\ \forall (j,k) \notin E \right. \right\}. \tag{13}$$

The action set from which the interdictor can choose is given by

$$A_{interdictor} = \left\{ \lambda^- \left| \sum_{j=0}^{J+1} \lambda_j^- \leq \Lambda^-,\ \lambda_j^- \geq 0,\ \forall j,\ \lambda_0^- = \lambda_{J+1}^- = 0 \right. \right\}. \tag{14}$$

The interdictor is constrainted in its action by a total arrival rate Λ^- of negative customers to the network. The payoff of this game is given by the departure rate of regular customers at node $J+1$. Since there are no arrivals of negative customers at node $J+1$, the departure rate of this node equals its arrival rate. We have, given R and λ^-, a payoff of

$$v(R, \lambda^-) = \lambda_{J+1}^+. \tag{15}$$

As λ_{J+1}^+ is determined by R and λ^- via equation (5), (9) and (10), this payoff is defined implicitly.

A strategy for a player is a probability distribution over the set of actions of that player. A strategy for the operator is a measure F defined on the set $A_{operator}$ such that $F(A_{operator}) = 1$. Similary, a strategy for the interdictor is a measure G defined on the set $A_{interdictor}$ such that $G(A_{interdictor}) = 1$. A pure strategy for either player is a measure that gives measure 1 to a single element of the action set of that player. So, a pure strategy for the operator will be a measure F such that $F(R) = 1$, this means that with probability 1 the operator chooses action R. A strategy which is not pure, is called a mixed strategy. The expected payoff is defined as

$$\begin{aligned} E(F,G) &= \int_{A_{operator} \times A_{interdictor}} v(R, \lambda^-) d(F \times G), \\ &= \int_{A_{operator}} \int_{A_{interdictor}} v(R, \lambda^-) dG(\lambda^-) dF(R), \\ &= \int_{A_{interdictor}} \int_{A_{operator}} v(R, \lambda^-) dF(R) dG(\lambda^-). \end{aligned} \tag{16}$$

Define the following two numbers

$$v_I = \sup_F \inf_G E(F,G), \tag{17}$$

$$v_{II} = \inf_G \sup_F E(F,G). \tag{18}$$

The first question is whether or not $v_I = v_{II}$. If $v_I = v_{II}$ then the game is said to have a value. If furthermore also sup inf and inf sup can be replaced by max min and min max respectively, then there exist optimal strategies.

Section 3 will answer these questions, but first recall the payoff function. This payoff function, given by equation (15), equals the rate at which regular customers arrive at node $J+1$. Hence, these customers have left every node they had visited due to service completion, otherwise they would have been removed from the network by a negative customer. Let l be a path from node 0 to node $J+1$, then the probability that a customer, moving along this path, arrives at node $J+1$ and leaves the network due to service completion equals

$$\prod_{i=1}^{m(l)-1} q_{l_i}, \tag{19}$$

where q_j is given by equation (7). From the transition probabilities we can derive the probability that a path l will be travelled by a customers, this probability equals

$$\prod_{i=1}^{m(l)-1} r(l_i, l_{i+1}). \tag{20}$$

By conditioning on the path travelled by a customers, the probability that an arbitrary customer arrives at node $J+1$ equals

$$\sum_{l \in L} \prod_{i=1}^{m(l)-1} r(l_i, l_{i+1}) q_{l_i}. \tag{21}$$

Multiplying by the total arrival rate at node 0, we obtain the rate at which customers arrive at node $J+1$, and thus

$$v(R, \lambda^-) = \gamma \sum_{l \in L} \prod_{i=1}^{m(l)-1} r(l_i, l_{i+1}) q_{l_i}. \tag{22}$$

Note that the set L of all possible paths from node 0 to node $J+1$ has an infinite number of elements; a path may include an arbitrary number of cycles. In section 3.2 we prove that we can restrict the summation in (22) to all simple path from node 0 to node $J+1$, i.e. replace L by $\bar{L}$.

2.5 Link to a previous study

As special case of the game descibed in the previous section may be interpreted as a generalization of the game described in Washburn and Wood (1995). Suppose that instead of deciding on the arrival rates of the negative customers, the interdictor can only decide on which nodes negative customers will arrive. The action of the interdictor is descibed by the vector $x = (x_j)$, where $x_j = 1$ if the interdictor chooses node j and 0 otherwise. The action set of the interdictor is given by

$$\bar{A}_{interdictor} = \left\{ x \left| \sum_{j \in I} x_j \leq M,\ x_j \in \{0,1\},\ \forall j \in I \right. \right\}. \tag{23}$$

Here M denotes the capacity constraint of the interdictor. Suppose furthermore that if $x_j = 1$ that negative customers will arrive at node j according to a Poisson process with given rate λ_j^-. Then the payoff function is given by

$$\begin{aligned} \bar{v}(R,x) &= \gamma \sum_{l \in L} \prod_{i=1}^{m(l)-1} r(l_i, l_{i+1}) \frac{\mu_{l_i}}{\mu_{l_i} + x_{l_i} \lambda_{l_i}^-}, & (24) \\ &= \gamma \sum_{l \in L} \prod_{i=1}^{m(l)-1} r(l_i, l_{i+1}) \left(1 - \frac{\lambda_{l_i}^-}{\mu_{l_i} + \lambda_{l_i}^-} x_{l_i} \right). & (25) \end{aligned}$$

If $x_j = 1$ a customer is removed at node j by a negative customer with probability $\frac{\lambda_j^-}{\mu_j + \lambda_j^-}$. Each regular customer is routed independently of each other regular customer, furthermore also the removal probabilities of a regular customer at the nodes are independent of other regular customers. As a consequence this game is equivalent to the game, played repeatedly, in which only one regular customer is routed from node 0 to node $J+1$. This is exactly a game descibed by Washburn and Wood (1995) where a single evader moves through a network and where multiple interdictors try to intercept the evader.

3 Game analysis

3.1 Introduction

In the previous section, a new interdiction game is described. In this section we are concerned with the existence of optimal strategies in this game. First we will look for optimal mixed strategies. In doing so, we deal with routing strategies of the operator which result in positive customers being routed in cycles. After establishing a result concerning optimal mixed strategies, we consider optimal pure strategies. To prove existence of an optimal pure strategy for the interdictor, convexity of the payoff function has to be analysed.

3.2 Optimal mixed strategies

3.2.1 No cycles

A routing strategy R^* is optimal for a given λ^- if

$$R^* = \arg\max_R v(R, \lambda^-). \tag{26}$$

Furthermore we say that R contains a cycle if there exists a node for which the probability that it will be visited more than once by the same customer is strict positive.

Theorem 1. There exists an optimal R for every λ^- such that R does not contain any cycle.

Before we prove the theorem, we first prove a slightly easier lemma.

Lemma 1. If $\lambda_j^- > 0$ then node j cannot be contained in a cycle in an optimal routing matrix R^*.

Proof of Lemma 1. Define η_j as the marginal benefit to the operator in the throughput of routing an additional customer through node j. Under the optimal routing matrix R^*, η_j satisfies the following relations

$$\eta_0 = \max_{k \in FS(0)} \eta_k, \tag{27}$$

$$\eta_j = \frac{\mu_j}{\mu_j + \lambda_j^-} \max_{k \in FS(j)} \eta_k, \quad \forall j \in I, \tag{28}$$

$$\eta_{J+1} = 1. \tag{29}$$

If a customer is routed through node j, then with probability $\frac{\lambda_j^-}{\mu_j + \lambda_j^-}$ this customer is removed by a negative customer and the operator gains nothing. With probability $\frac{\mu_j}{\mu_j + \lambda_j^-}$ the customer is routed to a next node k^* and the benefit equals η_{k^*}. Since under R^* the operator maximizes the benefit per unit time, node k^* will be a node for which the marginal benefit is maximal.

Moreover, the marginal benefit of an additional customer is only strictly positive if the customer eventually reaches node $J+1$. Since $\lambda_j^- \geq 0$, it follows that

$$0 < \frac{\mu_j}{\mu_j + \lambda_j^-} \leq 1, \quad \forall j \in I \tag{30}$$

and thus we deduce from (28) that whenever a customer is routed under R^* from node j to node k the following must hold

$$\eta_j \leq \eta_k. \tag{31}$$

Let $c = (c_1, \ldots, c_m, c_1)$ be a cycle contained in R^*. From (31) follows

$$\eta_{c_1} \leq \eta_{c_2} \leq \ldots \leq \eta_{c_m} \leq \eta_{c_1}, \tag{32}$$

which yields,

$$\eta_{c_1} = \eta_{c_2} = \ldots = \eta_{c_m} = \eta_{c_1}. \tag{33}$$

In order for equation (33) to hold, we must have that $\lambda_{c_i}^- = 0$ for every c_i. Equivalently, if $\lambda_j^- > 0$ node j cannot be contained in a cycle. Hence, we have proven the lemma.

Proof of Theorem 1. Let λ^- be given and suppose that the optimal routing matrix R^* contains a cycle. Define $\lambda_{j,k}^+$ as the flow of regular customers moving along link (j,k), we have

$$\lambda_{j,k}^+ = \lambda_j^+ \frac{\mu_j}{\mu_j + \lambda_j^-} r(j,k). \tag{34}$$

As before let $c = (c_1, \ldots, c_m, c_1)$ be a cycle contained in R^*. From Lemma 1 follows that for every node c_i contained in a cycle we have $\lambda_{c_i}^- = 0$ and thus

$$\lambda_{c_i,c_{i+1}}^+ = \lambda_{c_i}^+ r^*(c_i, c_{i+1}), \qquad i = 1, \ldots, m(c)-1, \tag{35}$$

$$\lambda_{c_m,c_1}^+ = \lambda_{c_m}^+ r^*(c_m, c_1). \tag{36}$$

We will now construct a new routing matrix R^{**} from R^* which does not contain the cycle c and is also optimal. Let $\widetilde{\lambda}_j^+$ and $\widetilde{\lambda}_{j,k}^+$ denote respectively the total flow through node j and the flow along link (j,k) under the new routing matrix R^{**}. We construct R^{**} as follows. First define the flow of regular customers along the whole cycle c by

$$\zeta_c = \min_i \lambda_{c_i,c_{i+1}}^+. \tag{37}$$

Next, substract a flow of ζ_c from every link (j,k) contained in the cycle c and maintain the same flow for every other link.

$$\widetilde{\lambda}_{c_i,c_{i+1}}^+ = \lambda_{c_i,c_{i+1}}^+ - \zeta_c, \quad i = 1, \ldots, m(c)-1, \tag{38}$$

$$\widetilde{\lambda}_{c_m,c_1}^+ = \lambda_{c_m,c_1}^+ - \zeta_c. \tag{39}$$

Consequently the total flow through every node c_i in c is reduced by ζ_c. The total flow of all other nodes remains equal.

$$\widetilde{\lambda}^+_{c_i} = \lambda^+_{c_i} - \zeta_c, \quad i = 1, \ldots, m. \tag{40}$$

Note that all flows into a node and all flows out of a node are still balanced. Now, define R^{**} by the following equation

$$r^{**}(j,k) = \begin{cases} \frac{\widetilde{\lambda}^+_{j,k}}{\widetilde{\lambda}^+_j} & \text{if } \widetilde{\lambda}^+_j \neq 0, \\ r^*(j,k) & \text{if } \widetilde{\lambda}^+_j = 0. \end{cases} \tag{41}$$

It is easy to see that $R^{**} \in A_{operator}$: If node j is not contained in the cycle c or satisfies $\widetilde{\lambda}^+_j = 0$, there is no change in the transition probabilities from these nodes, i.e. $r^{**}(j,k) = r^*(j,k)$. Furthermore for each node c_i in the cycle c for which $\widetilde{\lambda}^+_{c_i} > 0$, we have

$$\begin{aligned} \sum_k r^{**}(c_i,k) &= \sum_k \frac{\widetilde{\lambda}^+_{c_i,k}}{\widetilde{\lambda}^+_{c_i}}, & (42) \\ &= \frac{\sum_k \lambda^+_{c_i,k} - \zeta_c}{\lambda^+_{c_i} - \zeta_c}, & (43) \\ &= 1. & (44) \end{aligned}$$

Moreover R^{**} still satisfies the conditions $r^{**}(j,k) \geq 0 \; \forall (j,k) \in E$ and $r^{**}(j,k) = 0 \; \forall (j,k) \notin E$. So, R^{**} is a feasible action for the operator. Also the cycle c is not contained in R^{**}, since for i^* being the argument of the minimization in (37) we have,

$$\widetilde{\lambda}^+_{c_{i^*},c_{i+1}} = \lambda^+_{c_{i^*},c_{i+1}} - \zeta_c = 0 \tag{45}$$

and hence

$$r^{**}(c_{i^*}, c_{i^*+1}) = 0. \tag{46}$$

Besides, by changing the routing matrix we did not change the flow into node $J+1$, since under our network assumptions node $J+1$ could not be part of any cycle. Therefore the payoff value under R^{**} is the same as under R^* and we conclude that R^{**} is also optimal. We can repeat the same procedure to remove all cycles in R^* resulting in an optimal routing matrix that does not contain any cycles.

3.2.2 Optimal mixed strategies

Theorem 1 shows that for every action of the interdictor, the operator has an optimal action which does not result in customers moving along cycles. As a consequence, there exists a optimal strategy for the operator in which the probability that a customers moves along a cycle is zero. Hence, we can limit summation in the payoff function, as given in equation (22), to the finite set of all simple paths. The payoff function becomes

$$v(R, \lambda^-) = \sum_{l \in \bar{L}} \prod_{i=1}^{m(l)-1} r(l_i, l_{i+1}) q_{l_i}. \tag{47}$$

This payoff function is continuous, because the set $\bar{L}$ is finite. The following theorem is due to Glicksberg (1952).

Theorem 2. In a two person zero-sum game, if the action sets of both players are compact and the payoff function is continuous, then the game has a value and optimal mixed strategies exist.

Clearly the sets $A_{operator}$ and $A_{interdictor}$ are compact and since the payoff function is continuous, Theorem 2 ensures that optimal mixed strategies exist and $v_I = v_{II}$.

3.3 Optimal pure strategy

3.3.1 Convexity

Now we have established a result that guarantees the existence of optimal mixed strategies, we like to investigate the existence of optimal pure strategies. However, first we are concerned with the convexity of the payoff function, for convexity will be sufficient condition for pure strategies. Recall that the payoff function is given by

$$v(R, \lambda^-) = \sum_{l \in \bar{L}} \prod_{i=1}^{m(l)-1} r(l_i, l_{i+1}) \frac{\mu_{l_i}}{\mu_{l_i} + \lambda_{l_i}^-}. \tag{48}$$

Lemma 2. Let the parameters μ_i, $i = 1, \ldots, n$ be given and strictly positive. The function

$$f(x) = \prod_{i=1}^{n} \frac{\mu_i}{\mu_i + x_i} \tag{49}$$

is strictly convex on the set $\{x \,|x_i \geq 0,\ i = 1, \ldots, n\}$.

Proof of lemma 2. A function is strictly convex if and only if its Hessian matrix is positive definite. So we prove that the Hessian of $f(x)$ is positive definite to establish the result. The Hessian $\nabla^2 f(x)$ is given by

$$[\nabla^2 f(x)]_{i,j} = \frac{\partial^2 f(x)}{\partial x_i \partial x_j}, \quad i, j = 1, \ldots, n, \tag{50}$$

where

$$\frac{\partial^2 f(x)}{\partial x_i^2} = \frac{2}{(\mu_i + x_i)^2} f(x), \tag{51}$$

$$\frac{\partial^2 f(x)}{\partial x_i \partial x_j} = \frac{1}{(\mu_i + x_i)(\mu_j + x_j)} f(x), \quad i \neq j. \tag{52}$$

We know that $\nabla^2 f(x)$ is positive definite if all leading principal minors are positive. Denote by M_m the m^{th} leading principal minor, then

$$M_m = \sum_{\sigma \in S_m} \operatorname{sgn}(\sigma) \prod_{i=1}^{m} [\nabla^2 f(x)]_{i,\sigma_i}. \tag{53}$$

where the summation is taken over all permutations of the set $\{1, \ldots, m\}$. The key is to note that in each term a product is taken over m elements. Each of these m elements are taken from different rows and columns. Due to the structure of the second partial derivatives of $f(x)$, we have that each product of elements will be equal to

$$c_\sigma \frac{(f(x))^m}{(g_m(x))^2} \tag{54}$$

where c_σ is a constant depending on the permutation σ and

$$g_m(x) = \prod_{i=1}^{m} \mu_i + x_i. \tag{55}$$

As a consequence

$$M_m = \frac{(f(x))^m}{(g_m(x))^2} \sum_{\sigma \in S_m} \operatorname{sgn}(\sigma) c_\sigma. \tag{56}$$

It turns out that

$$\sum_{\sigma \in S_m} \operatorname{sgn}(\sigma) c_\sigma \tag{57}$$

equals the determinant of a $m \times m$ matrix with diagonal elements equal to 2 and 1 elsewhere. We denote this matrix by H, furthermore let v be a vector of lenght m with all elements equal to 1. With I the identity matrix, we have

$$H = I + vv^T. \tag{58}$$

Now it follows from the equality

$$\begin{pmatrix} I & 0 \\ v^T & 1 \end{pmatrix} \begin{pmatrix} I + vv^T & v \\ 0 & 1 \end{pmatrix} \begin{pmatrix} I & 0 \\ -v^T & 1 \end{pmatrix} = \begin{pmatrix} I & -v \\ 0 & 1 + v^T v \end{pmatrix} \tag{59}$$

that

$$\det(H) = 1 + v^T v = m + 1. \tag{60}$$

It follows that the leading principal minors are given by the following equation

$$M_m = \frac{(m+1)\,(f(x))^m}{(g_m(x))^2}, \quad m = 1, \ldots, n. \tag{61}$$

Since $\mu_i > 0$ and $x_i \geq 0$ for all i, each $M_m > 0$. We thus conclude that $\nabla^2 f(x)$ is positive definite and the lemma is proven.

3.3.2 Optimal pure interdictor strategy

With this preparatory result established, we can state the following theorem.

Theorem 3. The interdictor has an unique optimal pure strategy.

Proof of theorem 3. Rewrite the payoff function $v(R, \lambda^-)$ as

$$v(R, \lambda^-) = \sum_{l \in \bar{L}} \prod_{i=1}^{m(l)-1} r(l_i, l_{i+1}) \prod_{i=1}^{m(l)-1} \frac{\mu_{l_i}}{\mu_{l_i} + \lambda_{l_i}^-}. \tag{62}$$

We recognize that $v(R, \lambda^-)$ is a linear combination of functions $f_l(\lambda^-)$, with

$$f_l(\lambda^-) = \prod_{i=1}^{m(l)-1} \frac{\mu_{l_i}}{\mu_{l_i} + \lambda_{l_i}}, \quad l \in \bar{L}. \tag{63}$$

As a result of lemma 2, these functions are strictly convex and hence $v(R, \lambda^-)$ is strictly convex in λ^- for $\lambda^- \in \left\{ \lambda^- \,\middle|\, \lambda_i^- \geq 0 \right\}$. Therefore, since the action sets of both players are compact, we can conclude from the work of Bohnenblust et al. (1950) that there exists an unique optimal pure strategy for the interdictor.

4 Special cases

4.1 Introduction

The previous sections were concerned with a general game model on a queueing network. Section 2 gave a description of the queueing network and the game that is played upon the network. After which, section 3 gave results on the existence of optimal strategies. This section considers special cases of the described game. On a network of parallel queues and a network of tandem queues, we provide optimal strategies for the operator and the interdictor. Sections 4.2 and 4.3 give these results. Furthermore section 4.4 extends the game of the previous sections to a game in which negative customers may remove more than one positive customer from a queue.

4.2 Parallel queues

Consider the network in which the nodes $j \in I$ are in parallel with each other, i.e. $r(j, J+1) = 1$ $\forall j \in I$. In this network regular customers can move along paths of the form $l = (0, j, J+1)$ with $j \in I$. The payoff function in now defined by

$$v(R, \lambda^-) = \gamma \sum_{j \in I} r(0, j) \frac{\mu_j}{\mu_j + \lambda_j^-}. \tag{64}$$

This function is convex in λ^- and linear in R, and thus also concave in R. Furthermore $A_{operator}$ and $A_{interdictor}$ are compact and convex sets. It can be proven that in this case optimal pure strategies exists (Fan (1953)). In other words

$$v = \max_R \min_{\lambda^-} v(R, \lambda^-) = \min_{\lambda^-} \max_R v(R, \lambda^-). \tag{65}$$

The operator has only to decide on the values of $r(0, j)$ $\forall j \in I$, thus every action R is a linear combination of the actions R_j in which $r(0, j) = 1$, $j \in I$. Due to the linearity of $v(R, \lambda^-)$ in R and the fact that each R is a linear combination of the actions R_j, we can find the optimal λ^- by solving the following minimization problem.

$$\min_{\lambda^-} w \tag{66}$$

subject to

$$\gamma \frac{\mu_j}{\mu_j + \lambda_j^-} \leq w, \quad \forall j \in I. \tag{67}$$

The constant w is interpreted as the maximum payoff the operator can obtain, which is minimized by the interdictor. Furthermore, due to the linearity in R we only need to make sure that $v(R, \lambda^-) \leq w$ for $R = R_j$ $\forall j \in I$. Now since $v(R, \lambda^-)$ is continuous in λ^-, we have that for an optimal λ^{-*}

$$\gamma \frac{\mu_j}{\mu_j + \lambda_j^{-*}} = v, \quad \forall j \in I. \tag{68}$$

Rewriting yields

$$\lambda_j^{-*} = \frac{\gamma - v}{v}\mu_j, \quad \forall j \in I. \tag{69}$$

Using

$$\sum_{j\in I} \lambda_j^{-*} = \Lambda^- \tag{70}$$

gives us,

$$\Lambda^- = \sum_{j\in I} \frac{\gamma - v}{v}\mu_j \tag{71}$$

or

$$\frac{\gamma - v}{v} = \frac{\Lambda^-}{\sum_{j\in I}\mu_j}. \tag{72}$$

Finally we obtain the optimal λ^{-*} by combining equations (69) and (72),

$$\lambda_j^{-*} = \frac{\mu_j}{\sum_{k\in I}\mu_k}\Lambda^-, \quad \forall j \in I. \tag{73}$$

The value of the game is given by

$$v = \frac{\sum_{j\in I}\mu_j}{\sum_{j\in I}\mu_j + \Lambda^-}\gamma. \tag{74}$$

So, given the capacity constraint Λ^-, the network of parallel nodes with service rates μ_j is equivalent, in terms of the throughput, to a system of one node with service rate $\sum_{j\in I}\mu_j$. Furthermore, the value and the optimal λ^{-*} are independent of the action of the operator, i.e. given that the interdictor chooses action λ^{-*}, the operator's action choice R does not influence the payoff of the game. However, for every R there is a unique optimal λ^-, since $v(R, \lambda^-)$ is strictly convex in λ^-. Hence, there is a unique R^* which should be played by the operator in order to guarantee at least a payoff equal to the value of the game. For R^* must hold

$$\gamma \sum_{j\in I} r^*(0,j)\frac{\mu_j}{\mu_j + \lambda_j^-} \geq v = \frac{\sum_{j\in I}\mu_j}{\sum_{j\in I}\mu_j + \Lambda^-}\gamma. \tag{75}$$

Suppose we choose R such that

$$r(0,j) = \frac{\mu_j}{\sum_{k\in I}\mu_k}, \quad \forall j \in I. \tag{76}$$

For $\lambda^- \in A_{interdictor}$ the payoff is given by

$$v(R, \lambda^-) = \frac{\gamma}{\sum_{k\in I}\mu_k}\sum_{j\in I}\frac{\mu_j^2}{\mu_j + \lambda_j^-}. \tag{77}$$

Minimizing this payoff over all possible λ^- using Lagrange multipliers, shows that the minimum is attained when $\lambda^- = \lambda^{-*}$. We thus conclude that R as given by equation (76) is the optimal

strategy for the operator. When giving it some thougths, one can obtain a quite intuitive interpretation for the form of the optimal strategy. The payoff depends on the probability q_j that a customer is not removed by a negative customer. This probability, given in equation (7), depends on the time a customer spend in service; the smaller the service time, the greater the probability of service completion. In this network of parallel nodes, the operator can choose those nodes which yields the smallest service times. Since all service times are stochastic, the operator should choose a node with probability equal to the probability that this node has the smallest service time. All service times are exponentially distributed, hence the probability that a node j has the smallest service time is given by

$$\frac{\mu_j}{\sum_{k\in I}\mu_k}, \tag{78}$$

which is precisely the optimal probability of routing a customers through node j as is given in equation (76).

4.3 Tandem queues

Consider the network in which the nodes $j \in I$ are in tandem, i.e. $r(i, i+1) = 1$ for $i = 0, \ldots, J$. In this network regular customers can only move along one path from node 0 to node $J+1$, visiting each node in the network. The payoff function for this network is given by

$$v(\lambda^-) = \gamma \prod_{j \in I} \frac{\mu_j}{\mu_j + \lambda_j^-}. \tag{79}$$

Since the operator has no choice in how to route the regular customers through the network, the interdictor action is found by just minimizing $v(\lambda^-)$ subject to the constraint

$$\sum_{j \in I} \lambda_j^- = \Lambda^-. \tag{80}$$

The lagrangian of the problem is given by

$$\nu(\lambda^-, \psi) = \gamma \prod_{j \in I} \frac{\mu_j}{\mu_j + \lambda_j^-} + \psi \left(\sum_{j \in I} \lambda_j^- - \Lambda^- \right). \tag{81}$$

Taking partial derivatives yields

$$\frac{\partial \nu}{\partial \lambda_j^-} = \frac{-1}{\mu_j + \lambda_j^-} v(\lambda^-) + \psi \quad \forall j \in I, \tag{82}$$

$$\frac{\partial \nu}{\partial \psi} = \sum_{j \in I} \lambda_j^- - \Lambda^-. \tag{83}$$

Equating the partial derivatives to zero results in

$$\frac{1}{\mu_j + \lambda_j^-} = \frac{\psi}{v(\lambda^-)}, \quad \forall j \in I. \tag{84}$$

Rewriting gives

$$\lambda_j^- = \frac{v(\lambda^-) - \psi \mu_j}{\psi}, \quad \forall j \in I. \tag{85}$$

Summing equation (85) over j yields

$$\Lambda^- = \sum_{j \in I} \left(\frac{v(\lambda^-)}{\psi} - \mu_j \right), \tag{86}$$

$$= \frac{v(\lambda^-)}{\psi} J - \sum_{j \in I} \mu_j. \tag{87}$$

Rewriting gives

$$\frac{v(\lambda^-)}{\psi} = \frac{\Lambda^- + \sum_{j \in I} \mu_j}{J}. \tag{88}$$

Combining equation (85) and (88) gives

$$\lambda_j^- = \frac{\Lambda^- + \sum_{k\in I}\mu_k}{J} - \mu_j, \quad \forall j \in I. \tag{89}$$

These are the values which the interdictor has to choose to minimize $v(\lambda^-)$, provided that

$$0 \leq \lambda_j^- \quad \forall j \in I. \tag{90}$$

Suppose that we have for some k, $\lambda_k^- < 0$. We can find an optimal feasible solution by setting $\lambda_k^- = 0$, and minimize $v(\lambda^-)$ over all λ_j^-, $j \neq k$. We can repeat this procedure until conditions (90) are met.

Equation (89) can be rewritten as

$$\lambda_j^- - \frac{\sum_{k\in I}\lambda_k^-}{J} = -\left(\mu_j - \frac{\sum_{k\in I}\mu_k}{J}\right), \quad \forall j \in I. \tag{91}$$

This equation shows that the difference between the arrival rate of negative customers at a specific node and its mean over all nodes equals the difference between the service rate at that node and the mean service rate over all nodes, up to a minus sign.

If equation (89) is rewritten as

$$\lambda_j^- + \mu_j = \frac{\sum_{k\in I}\lambda_k^- + \mu_k}{J}, \quad \forall j \in I, \tag{92}$$

we see that the rates at which regular customers leave the queues, given that the queues are not empty, are equal. This implies that when a queue has a smaller service rate, the rate at which negative customers arrive in the optimal strategy will be higher. This is explained as follows. In queues with smaller service rates, regular customers stay longer in service and thus are vulnerable to interception during a longer time period. Since the operator has no choice in routing the regular customers, the interdictor can put his resources there where these customers are most vulnerable: queues with low service rates.

The value of this game played on a network of tandem queues is given by

$$v = \gamma \prod_{j\in I} \frac{J\mu_j}{\Lambda^- + \sum_{k\in I}\mu_k}. \tag{93}$$

4.4 Model extensions

4.4.1 Batch removals

Instead of considering special networks, also some extensions with regard to the queues can be made. The first extension is to assume that arriving negative customers may remove a batch of positive customers. The queueing network with batch removals is described and analyzed in Gelenbe (1993). Following the same method as Gelenbe (1993), we describe the interdiction game on a queueing network with batch removals.

A single queue
Before analyzing the whole network, consider a single server queue with exponentially distributed service time with mean $1/\mu$. Positive customers arrive at this queue according to a Poisson process with rate λ^+. In addition to these customers, also negative customers arrive at the queue according to a Poisson process with rate λ^-. Upon arrival of a negative customer, a batch of B positive customers are removed from the queue according to some probability distribution; $P(B = s) = p_s$, $p_s \geq 0\ \forall s$, $\sum_s p_s = 1$. Since all interarrival times and service times are exponentially distributed, we do not have to know which customers are removed to determine the stationary distribution of the number of present customers, but we assume that regular customers are removed based on a 'first in first out'-procedure. For this queue we have the following balance equations,

$$(\lambda^+ + \lambda^-)\pi(0) = \mu\pi(1) + \lambda^- \sum_{n=0}^{\infty} \pi(n) \sum_{s=n}^{\infty} p_s, \tag{94}$$

$$(\lambda^+ + \mu + \lambda^-)\pi(n) = \lambda^+\pi(n-1) + \mu\pi(n+1) + \sum_{s=0}^{\infty} \pi(n+s)p_s, \quad n > 0. \tag{95}$$

Suppose $\pi(n) = c\rho^n$, then from (94) and (95) we obtain

$$\lambda^+ + \lambda^- = \mu\rho + \lambda^- \sum_{n=0}^{\infty} \rho^n \sum_{s=n}^{\infty} p_s, \tag{96}$$

$$\lambda^+ + \mu + \lambda^- = \lambda^+ \frac{1}{\rho} + \mu\rho + \lambda^- \sum_{s=0}^{\infty} \rho^s p_s. \tag{97}$$

Define

$$f(x) = \frac{1 - \sum_{s=0}^{\infty} x^s p_s}{1 - x}. \tag{98}$$

Both (96) and (97) are equivalent to

$$\rho = \frac{\lambda^+}{\mu + \lambda^- f(\rho)}. \tag{99}$$

If (99) has a solution such that $\rho < 1$, then the stationary distribtion is given by

$$\pi(n) = (1 - \rho)\rho^n, \quad \forall n. \tag{100}$$

If $p_1 = 1$, $f(\rho) = 1$ and we have the queueing model described in section 2.2. If $p_\infty = 1$, we have a queue with disasters (see Chao (1995))), i.e. negative customers which empty the whole queue upon arrival. In this case we have $f(\rho) = 1/(1-\rho)$.

The function f can be rewritten as follows.

$$\begin{aligned} f(x) &= \frac{1 - \sum_{s=0}^{\infty} x^s p_s}{1-x}, && (101)\\ &= \frac{\sum_{s=0}^{\infty} p_s - \sum_{s=0}^{\infty} x^s p_s}{1-x}, && (102)\\ &= \frac{\sum_{s=0}^{\infty} (1-x^s)\, p_s}{1-x}, && (103)\\ &= \frac{\sum_{s=0}^{\infty} \sum_{t=0}^{s-1} (1-x) x^t p_s}{1-x}, && (104)\\ &= \frac{\sum_{t=0}^{\infty} \sum_{s=t+1}^{\infty} (1-x) x^t p_s}{1-x}, && (105)\\ &= \sum_{t=0}^{\infty} \sum_{s=t+1}^{\infty} x^t p_s. && (106) \end{aligned}$$

If we tag an arbitrary customer at a queue, the probability that there are t customers in front of this tagged customer equals ρ^t. From this we can see that $f(\rho)$ equals the probability that an arriving disaster removes an arbitrary tagged customer.

A network of queues

In a network of J single server queues with batch removals, let μ_j be the service rate of queue j and let λ_j^- denotes the arrival rate of negative customers at queue j. Upon arrival at queue j a negative customer removes s customers with probability $p_{j,s}$. Define

$$f_j(x) = \frac{1 - \sum_{s=0}^{\infty} x^s p_{j,s}}{1-x}. \qquad (107)$$

The traffic equations are given by

$$\begin{aligned} \lambda_j^+ &= \sum_k \rho_k \mu_k r(k,j), && (108)\\ \lambda_0^+ &= \gamma. && (109) \end{aligned}$$

where

$$\rho_j = \frac{\lambda_j^+}{\mu_j + \lambda_j^- f_j(\rho_j)}. \qquad (110)$$

If (108) has a non-negative solution $\{\lambda_j^+\}$ such that

$$\lambda_j^+ < \mu_j + \lambda_j^- f_j(\rho_j), \qquad (111)$$

then the stationary distribution of the network is given by

$$\pi(n) = \prod_j (1 - \rho_j)\rho_j^{n_j}. \tag{112}$$

The probability that a customer leaves queue j unintercepted equals

$$\frac{\rho_j \mu_j}{\lambda_j^+} = \frac{\mu_j}{\mu_j + \lambda_j^- f_j(\rho_j)}, \tag{113}$$

which depends on both λ_j^- and λ_j^+. This might become a problem in analyzing the game, as λ_j^+ depends on the routing matrix R.

Game description
The game on the network of queues with batch removals is only changed with respect to the payoff function. The action sets of both the operator and the interdiction remain the same and are given by (13) and (14). The payoff is also still given by the throughput of the system, however the explicite expression of the payoff function in (22) is changed, for the probability that a customer leaves the queue due to a service completion is changed. The payoff function is now given by

$$v(R, \lambda^-) = \gamma \sum_{l \in L} \prod_{i=1}^{m(l)-1} r(l_i, l_{i+1}) \frac{\mu_{l_i}}{\mu_{l_i} + \lambda_{l_i}^- f_{l_i}(\rho_{l_i})}. \tag{114}$$

Since ρ_j is a solution of equation (110) and we cannot write ρ_j explicitly in terms of λ^-, R and μ_j, we cannot give an explicite expression of the payoff function in terms of the chosen actions of both players. As yet, this is an obstacle in our path to analyze this game any further.

4.4.2 Other queueing models

Routing negative customers
Another extension would be to route not only the positive customers through the network, but also the negative customers. In literature the routing of negative customers is often taken into account in studying queues with negative customers, see e.g. Gelenbe (1991). However in these studies the routing of negative customers relies on the presence of positive customers at the queues. Negative customers disappear from the network if they arrive at an empty queue. The routing of negative customers is taken into account by a probability that a positive customer leaving a queue is routed as a negative customer to a next queue.

However, in our model we will require that the routing of negative customers occurs independently of the presence of positive customers, i.e. negative customers are also routed to a next queue when arriving at an empty queue. The reason for this requirement arises from the applications we have in mind. When certain security forces are deployed to patrol several areas in sequence, these patrols should be finished even if no threats are encountered. Networks of queues with negative customers, which are routed through the network also when arriving at

empty queues are not studied in literature. In particular we cannot give an expression of the stationary distribution of such a network and thus we cannot analyse an interdiction game played on such network.

Infinite server queues

In the game on a network with single server queues, positive customers may have to wait on other customers before receiving service. When viewing this queueing aspect from the application's point of view, this interdependence of positive customers may not be realistic. Smugglers may not wait upon each other before crossing checkpoints in a traffic network. On the other hand when threats occur not too often, the assumption of a single server may stand, for in such a case the probability of having more than one customer in a queue would be very small. However, in cases where the assumption of a single server is not reasonable, a infinite server may be implemented. In a network of infinite server queues, customers move independently of other customers through the network. Although we are able to find a stationary distribution of a infinite server queue subject to arrivals of negative customers, we are not able to give a solution for the stationary distribution of a network of such queues. Hence, as in the case of routing negative customers, we come to a halt in our analysis.

5 Application to anti-piracy operations

5.1 Introduction

In the previous chapters we developed an interdiction model which takes time-dependency into account as well as multiple interdictor and operator units. In this section we apply the model to an actual problem which has become more and more pressing over the last couple of years; piracy. First the problem is described, after which the developed model is slightly adjusted and applied to the problem. The last section presents the results.

5.2 Problem description

The threat to international shipping formed by pirates operating from Somalia has increased over the last couple of years, despite the military presence of various countries and coalitions. Piracy in the form of hijacking merchant ships began in 2003 in the Gulf of Aden and expanded in 2005 along the whole coast of Somalia. However, due to the increased military activity and the abandonment of the shipping routes near Somalia, pirates moved their operating areas increasingly farther away from the Somali coastline. Nowadays pirates operate as far as 1000 nautical miles (nm) from the Somali coastline.

Although the probability that a merchant ship is hijacked, is very small, the effects of piracy on the international trade and economy are large. The estimated cost of piracy is around eight billion dollars per year. Although this cost is relatively low compared to the turnover of shipping companies the influence is major, for the profit margins are small.

To counter the threat of piracy, maritime patrol areas are established. The purpose of these areas is to intercept pirates during their transit from base to operating areas, i.e. to catch pirates before they become an imminent threat. One or more naval ships are assigned to each patrol area. The main question we will answer, is; how to allocate the available naval ships over all the patrol areas in the most effective way. Effectiveness is measured in term of the pirate's probability of succesfull completing its operation. The lower this probability, the more effective the patrol areas.

5.3 Anti-piracy model

The problem is modelled as a zero-sum game as descibed in section 2.4. The pirates and naval forces compete over the number of succesfull pirate operations. The pirates may choose their operating area(s) in their attempt to increase the number of succesfull hijacks. Naval forces have established patrol areas and decide on the number of ships allocated to each area in order to minimize the number of succesfull hijacks.

Figure 2 gives an schematic representation of the Somali region. Pirates operating from Somalia have multiple operating areas (OA) in which they may attempt to hijack passing merchant vessels. With each operating area i, a parameter g_i is associated. The parameter g_i indicates the pirate's probability of a succesful operation, given that the pirate reaches operating area i. This parameter depends on the traffic density in the area, the distance from shore and also military presence in the operating area. (This military presence in the operating areas in not taken into account beyond the parameters g_i.)

To reach an operation area, pirates have to transit through a maritime patrol area (PA). During their transit through a patrol area, pirates are vulnerable to interception. The patrol

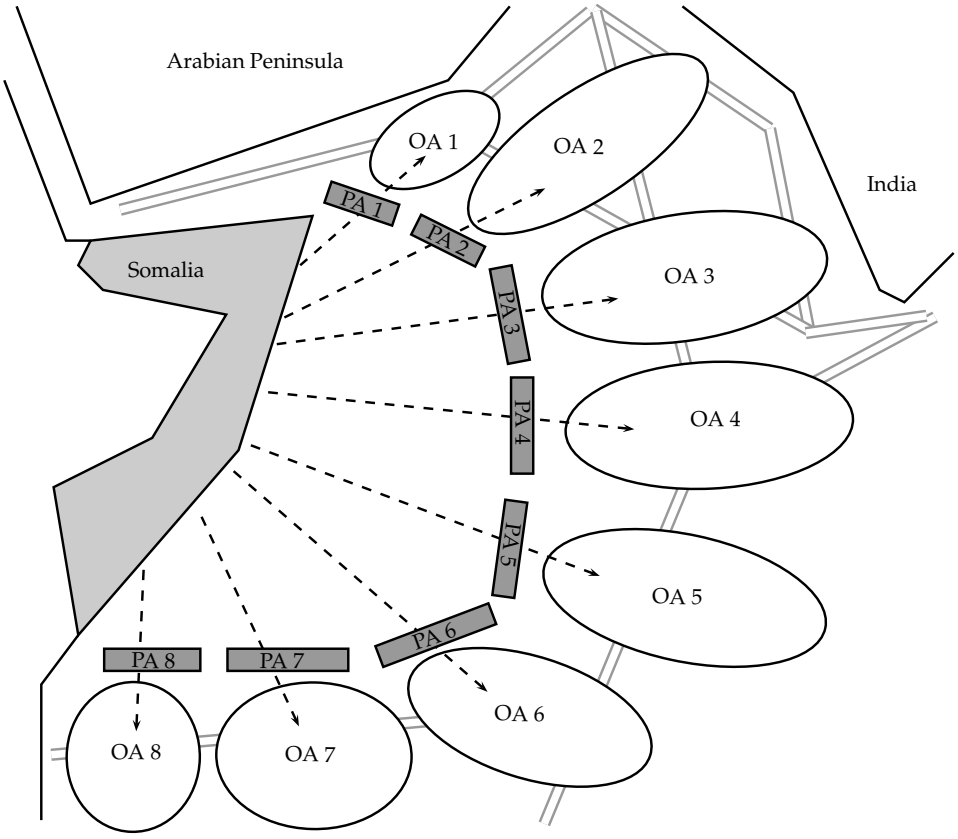

Figure 2: Schematic representation Somali region

areas are modelled as queues with arrivals of positive and negative customers, see section 2.2 and 2.3. The arrival of a pirate at a patrol area and its transit is represented by an arrival of a postive customer to a queue and its service at this queue. The removal of a positive customer due to an arrival of a negative customer represents the interception of a pirate by a naval ship.

The approach to determine optimal interdiction policies consists of two parts. First, by applying the model developed in section 2, we can find an optimal allocation of naval ships in terms of arrival rates at each patrol area. Since all patrol areas are in parallel the same solution method can be used as in section 4.2. From the optimal arrival rates of naval ships in the patrol areas, we can also derive the optimal interception probability in each area. The second part is to deduce the number of naval ships needed in a patrol area to achieve the optimal interception probability. This is done via a direct approximation. The next section will describe the determination of the optimal arrival rates and interception probability. Thereafter section 5.5 shows the direct approximation, which determines the interception probability given that a naval ship patrols an area of certian size.

5.4 Queueing model

The key in the first part of the model is to derive optimal interception probabilities for each patrol area, by determining the optimal arrival rates of naval ships. Let J denote the number of patrol areas. The interception probabilities of pirates, i.e. the removal probabilities of positive customers, depend solely on the arrival rate of naval ship and the transit time through the area and not on the arrival rate of the pirates themself (see section 2.3). Let $1/\mu_j$ be the deterministic service time of the pirates at queue j, then the interception probability at patrol area j is given by the probability that the interarrival time of the naval ship is less than $1/\mu_j$. Let λ_j^- denote the arrival rate of the negative customers at queue j, then the interception probability at patrol area j is given by

$$\mathcal{P}(\text{Interception at j}) = 1 - \mathsf{e}^{-\lambda_j^-/\mu_j}, \quad j = 1, \ldots, J. \tag{115}$$

The payoff is given by the number of pirates per unit time that succesfully complete their operation. These are pirates that are not intercepted by naval ships and when arrived in their operating area perform a succesfull hijack. Let $r(0, j)$ be the probability that a pirate will attempt to move through patrol area j. Then, given $R = (r(0, j))$ and $\lambda^- = \left(\lambda_j^-\right)$, the payoff function is given by

$$v(R, \lambda^-) = \gamma \sum_{j=1}^{J} r(0, j)\mathsf{e}^{-\lambda_j^-/\mu_j} g_j. \tag{116}$$

Since all patrol areas are in parallel, the optimal solution for this problem can be found in a similar way as in section 4.2. A strategy λ^- is optimal if for all j it holds that,

$$v = \gamma \mathsf{e}^{-\lambda_j^-/\mu_j} g_j. \tag{117}$$

Using the capacity contraint of the interdictor, i.e.

$$\sum_{j=1}^{J} \lambda_j^- = \Lambda^-, \tag{118}$$

we can solve equation (117) for λ^-. Rewrite equation (117) as

$$\lambda_j^- = \mu_j \log g_j + \mu_j \log \frac{\gamma}{v}. \tag{119}$$

Summing over j, using the capacity contraint and rearranging the terms yields

$$\log \frac{\gamma}{v} = \frac{\Lambda_j^- - \sum_k \mu_k \log g_k}{\sum_k \mu_k}. \tag{120}$$

From both equation (119) and (120) we deduce that the optimal strategy λ^{-*} is given by

$$\lambda_j^{-*} = \frac{\mu_j}{\sum_k \mu_k} \left(\Lambda^- + \sum_k \mu_k \log \frac{g_j}{g_k} \right). \tag{121}$$

The optimal strategy yields via equation (115) also optimal interception probabilities for each patrol area. In the next section we describe how we can translate the interception probabilities to number of naval ships per area.

5.5 Interception probability

5.5.1 Approximation approach

In this section we derive a formula for approximating the interception probability of a pirate moving through a interception area, given that a naval ship patrols an patrol area with certain size.

Suppose a rectangular patrol area with width w and lenght l is given. An approximation of the interception probability in this area is made by considering a rectangular patrol area with with w and length $2r$, where r denotes the detection radius of the naval ship patrolling this area, see figure 3. The naval ship patrols the area with speed v_n along the horizontal center line. A pirate boat attempting to cross the patrol area moves perpendicular to this center line.

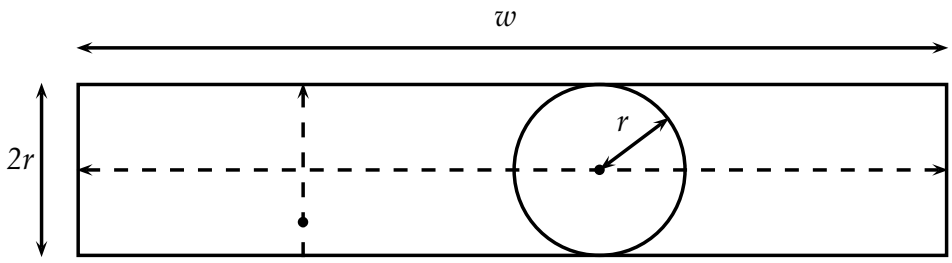

Figure 3:

The detection probability is approximated in two steps. First we determine the maximum horizontal distance between the naval ship and an arriving pirate boat, such that this pirate boat is intecepted during its transit. This distance depends on both the speeds of the ships, the detection radius of the naval ship and also the direction of travel of the navel ship. Given the maximum horizontal distance we can determine the detection probability by conditioning on the horizontal position of both the naval ship and the arriving pirate boat.

5.5.2 Maximum distance

Let v_n and v_p denote the speed of respectively the naval ship and pirate boat and denote the detection radius of the naval ship by r. First assume that the naval vessel is moving towards the pirate boat. Let x be the horizontal distance between the ships at the time of arrival of the pirate boat, see figure 4. Now the distance between both ship as function of the time t and the horizontal distance x is given by

$$D(t,x) = \sqrt{(x - v_n t)^2 + (-r + v_p t)^2}. \tag{122}$$

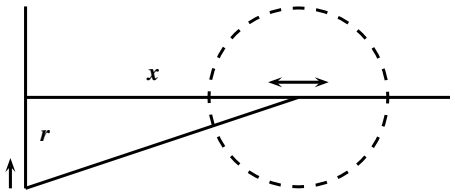

Figure 4:

To determine the maximum value of x given that the pirate will be intercepted, we first determine the time for which the distance $D(t, x)$ is minimal. This minimal distance needs to be smaller than r to intercept the pirate boat. So, equating the minimal distance to r will yield the maximum horizontal distance such that the pirate boat will still be intercepted during its transit. Taking the time derivative of $D(t, x)$ and equating is to 0 yields t^*, the time at which the distance is minimal,

$$t^* = \frac{xv_n + rv_p}{v_n^2 + v_p^2}. \tag{123}$$

The minimal distance as function of x is given by

$$\begin{aligned} D(t^*, x) &= \sqrt{\frac{(-v_p x + v_n r)^2}{v_n^2 + v_p^2}}, & (124) \\ &= \frac{-v_p x + v_n r}{\sqrt{v_n^2 + v_p^2}}. & (125) \end{aligned}$$

Equating this function to r and solving for x gives us the maximum horizontal distance x_1 if the naval ship is moving towards the pirate boat.

$$x_1 = \frac{v_n r}{v_p} + r\sqrt{1 + \frac{v_n^2}{v_p^2}}. \tag{126}$$

Using the same method we can determine the maximum horizontal distance x_2 if the naval ship is moving away from the pirate ship,

$$x_2 = -\frac{v_n r}{v_p} + r\sqrt{1 + \frac{v_n^2}{v_p^2}}. \tag{127}$$

5.5.3 Interception probability

The next step is to determine the interception probability by conditioning on the horizontal position and direction of the naval ship and the pirate boat. We assume that the horizontal position of the arriving pirate boat, x_p, is uniformly distributed on $[0, w]$, where w denotes the width of the patrol area. Furthermore, we assume that at the time the pirate boat enters the patrol area, the naval ship is at position x_n, which is also unifomly distributed on $[0, w]$.

$x_p \in \left[0, \frac{x_1+x_2}{2}\right]$	$\Rightarrow$	$x_n \in [0, x_p + x_1]$
$x_p \in \left[\frac{x_1+x_2}{2}, x_1\right]$	$\Rightarrow$	$x_n \in [0, x_1 - x_p] \cup [x_p - x_2, x_p + x_1]$
$x_p \in [x_1, w - x_1]$	$\Rightarrow$	$x_n \in [x_p - x_2, x_p + x_1]$
$x_p \in [w - x_1, w]$	$\Rightarrow$	$x_n \in [x_p - x_2, w]$

Table 1: Positions of both ships resulting in detection of the pirate boat.

The direction of the naval ship is either westward or eastward, both with probability $\frac{1}{2}$. We only consider the case in which the naval ship is moving westward and multiply the resulting probability by two to obtain the detection probability.

By conditioning on the position of both ships, multiple situation can be distinguished. For every position of the pirate boat, table 1 gives the positions of the naval ship which result in detection of the pirate boat. Given the ships their positions that result in detection, we can derive the probability of detection.

$$\begin{aligned}
\frac{1}{2}\mathcal{P}(\text{Detection}) &= \int_0^{\frac{x_1+x_2}{2}} \int_0^{x_p+x_1} \frac{1}{2w^2} \mathsf{d}x_n \mathsf{d}x_p && (128)\\
&\quad + \int_{\frac{x_1+x_2}{2}}^{x_1} \left(\int_0^{x_1-x_p} \frac{1}{2w^2} \mathsf{d}x_n + \int_{x_p-x_2}^{x_p+x_1} \frac{1}{2w^2} \mathsf{d}x_n \right) \mathsf{d}x_p && (129)\\
&\quad + \int_{x_1}^{w-x_1} \int_{x_p-x_2}^{x_p+x_1} \frac{1}{2w^2} \mathsf{d}x_n \mathsf{d}x_p && (130)\\
&\quad + \int_{w-x_1}^{w} \int_{x_p-x_2}^{w} \frac{1}{2w^2} \mathsf{d}x_n \mathsf{d}x_p && (131)\\
&= \frac{1}{8w^2} \left(-x_1^2 - 2x_1x_2 - x_2^2 + 4wx_1 + 4wx_2 \right), && (132)\\
&= \frac{x_1 + x_2}{2w} - \frac{(x_1 + x_2)^2}{8w^2}. && (133)
\end{aligned}$$

We obtain the result,

$$\begin{aligned}
\mathcal{P}(\text{Interception}) &= \frac{x_1 + x_2}{w} - \frac{(x_1 + x_2)^2}{4w^2}, && (134)\\
&= z - \frac{1}{4}z^2 && (135)
\end{aligned}$$

with

$$z = \frac{2r}{w}\sqrt{1 + \frac{v_n^2}{v_p^2}}. \quad (136)$$

The same result can be obtained using the relative area swept by the naval ship, see Wagner et al. (1999). We can inverse equation (135) to a equation from which we can determine the width

of a patrol area if a certain interception probability is to be achieved. Let p be the desired interception probability, then the width of the patrol are is given by

$$w = \frac{1 + \sqrt{1-p}}{p} r \sqrt{1 + \frac{v_n^2}{v_p^2}}. \tag{137}$$

This width indicates the width of an area patrolled by a single naval ship to achieve the desired interception probability in that area. If this desired interception probability is to be achieved in a patrol area with fixed width, we can divide this fixed width by the width resulting from equation (137) to obtain the number of naval ships needed in that patrol area.

5.6 The model

The previous sections developed two submodels that help to determine optimal deployment of naval ships to counter piracy threats. In the first part, described in section 5.4, optimal arrival rates of naval ships at patrol areas were determined which also result in optimal interception probabilities at these areas. Section 5.5 gave an approximation of the interception probability when a naval ships patrols an area of certain size and also allows for determination of the patrol area's width if a given interception probability is desired. This section combines both parts to one model which allows the user to determine the optimal deployment of naval forces in the Somali region.

We assume that the following parameters are given as input for our model. First of all the total number of naval ships available for allocation, and also the ship parameters, such as the speed of the naval ships, their detection radius and the speed of pirate boats. Furthermore we assume that patrol areas are given, so the number of patrol areas is known as well as the size of these areas, i.e. the length and width. Lastly also the success probability of pirates in their operating areas are assumed to be known.

In section 5.4 the optimal arrival rates of naval forces and sequentially the optimal interception probabilities are determined. This queueing model uses a fixed total arrival rate as a capacity constraint in finding the optimal arrival rates. This capacity constraint relates to the total number of available naval ships, yet in which way both parameters relate cannot be said. To overcome this obstacle, we will solve the model for a range of capacity constraint and determine the total number of ships needed from the model results.

For given input parameters, the optimal allocation of naval ships is determined as follows. First, for a range of capacity constraints Λ^- optimal arrival rates of naval ships at patrol areas, λ_j^{-*}, are determined by equation (121). Via equation (115) also optimal interception probabilities at the given patrol areas are determined. Given these optimal interception probabilities, equation (137) gives us the desired width of the patrol areas for given Λ^-. By dividing the actual width of the patrol areas by the desired width, we obtain the number of naval ships needed to be allocated to these patrol areas. By summing over all the naval ships needed in the patrol areas, we obtain the total number of naval ships and a relation between the capacity constraint Λ^- and the total number of available ships can be established. The number of successful pirate attacks is given by equation (117).

Section 6 will apply this model to the deployment problem in the Somali Basin, in that section input parameters are specified and results are given.

5.7 The use of queues

5.7.1 Motivation for queues

This section will verify the use of the queueing model of section 5.4. The choice of modelling the patrol areas as queues with negative customers is easiest to understand from the perspective of the pirates. A pirate arriving at a patrol area, has to travel through that area for some (fixed) time. During its transit through this area it may be intercepted by a patrolling naval ship. Section 2.2 discusses a queue with negative customers, in this model a positive customer in service may be removed by an arriving negative customers. In our model the pirate moving through a patrol area is represented by a positive customer receiving service. Service times are deterministic, since the pirates move at a given speed.

The negative customer removing a positive customer indicates a naval ship intercepting a pirate. Since the pirate in transit has no means to infer the search pattern, the patrolling speed and the location of the naval ship, the arrival of a naval ship within sight of the pirate occurs to him at a completely random point in time. This is modelled by the Poisson arrival process of negative customers at the queues. Also the arrivals of pirates to a patrol area is best modelled by a Poisson process due to the complete randomness of the process. Furthermore, since the interarrival times of pirates are much less than the transit time through a patrol area, the occupancy of the queue is very low and it suffices to use a single server queue to model the patrol area.

5.7.2 Verification

In absence of real data to compare the results of the queueing model to, a simulation model serves as reference point together with the direct approximation of section 5.5. In the simulation model the location of a naval ship patrolling a fixed area is simulated over time. The naval ship moves along a given patrol pattern through the area. In time also pirates move through the area, moving in a straight line from one border of the area to its opposite border. Whenever the distance between the naval ship and a pirate is less than the detection radius of the naval ship, the pirate is intercepted. From this simulation model we can derive results for the interception probability of a pirate.

The difficulty lies in comparing the results of the queueing model with the simulation results. The queueing model depends on the arrival rates of the negative customers, i.e. the naval ship, to determine the interception probability. The simulation model on the other hand, simulates only the movement and location of the naval ship and pirate boats in a given patrol area. If the patrol pattern of the naval ship and the size of the patrol area are to be translated to arrival rates of negative customers, we need to know the location of the queue in the patrol area, i.e. we need to know where the naval ships should arrive in order to determine its arrival rate. Since only the customer in service can be intercepted by negative customers, only the server of the queue is located within the patrol area. However, only if a pirate moves through the patrol area, the location of the server is known. In that case the pirate's location and the server's

location coincides. When the server is idle, the location is not known. Therefore we cannot observe the arrivals of a negative customer to a empty queue.

This problem is averted by assuming that the queue is never empty, i.e. there will always be a positive customer in service. Although this assumption is not realistic and therefore not usefull to determine the interception probability at the patrol area, it allows us to determine the arrival rate of the naval ship to the queue. For if the server is always busy, the time between two consecutive interceptions is equal to the time between two consecutive arrivals of the naval ship. In terms of the simulation model, the assumption means that whenever a pirate completes its transit through the area or is intercepted by the naval ship, immediately another pirate starts its transit through the area.

Via the determined arrival rates we can relate the queueing model to the given patrol area with a patrolling naval ship. Using the arrival rates of the naval ship the queueing model can determine the interception probability in this area. This result is compared with the interception probability resulting from the simulation model, without the assumption of an always busy server, and with the direct approximation of section 5.5.

Figure 5 shows the resulting interception probabilities determined by the different methods for various widths of patrol areas. The results are based on the default situation in which the patrol area has a length of 60 nautical miles (nm), the naval ship moves with 15 knots and has a detection radius of 6 nm, and in which pirates move with a speed of 6 knots.

All three methods yield with reasonable accuracy the same results. The small differences in the results are due to the different assumptions each method employs. Therefore we conclude that the choice of modelling patrol areas as queues is sound.

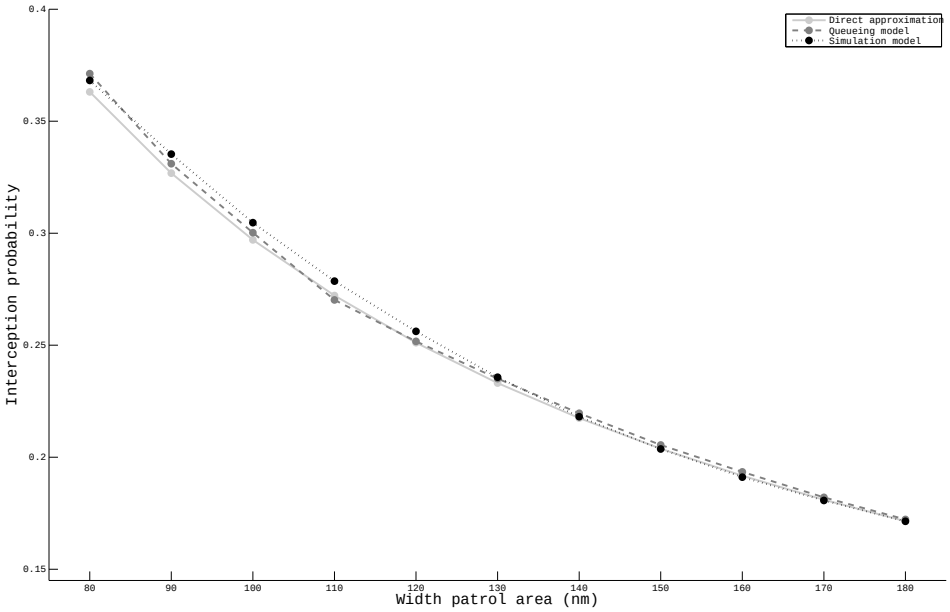
Direct approximation
Queueing model
Simulation model
Interception probability
Width patrol area (nm)
0.4
0.35
0.3
0.25
0.2
0.15
80
90
100
110
120
130
140
150
160
170
180

Figure 5:

6 Results on anti-piracy deployment

6.1 Introduction

The previous section developed a model to determine the optimal allocation of naval ships to patrol areas to counter pirate attacks in the Somali Basin. This section presents results for specified input parameters and also gives a comparison between two cases concerning the use of Unmanned Aerial Vehicles.

6.2 Pirate's success probability

The model developed in the previous sections allows us to analyse the number of naval ships and their allocation needed to achieve a certain level of effect. Again, effect is measured in term of the pirates' probability of successfully completing its operation, which is equivalent to the number of successful pirate attacks per time period. First results are given for a 'default' situation, in this situation the model parameters have values representing the current situation in the Somali Basin. Table 2 and 3 show the input parameters default values.

Pirate speed	6	knots
Navy speed	15	knots
Detection radius	6	nm

Table 2: Default values of ship parameters.

Area	1	2	3	4	5	6	7	8
Length PA (nm)	60	60	60	60	60	60	60	60
Width PA (nm)	90	90	120	120	120	150	150	150
Success probability OA	0.20	0.20	0.15	0.15	0.10	0.05	0.05	0.15

Table 3: Default values of area parameters.

Using the procedure described in section 5.6, we obtain the optimal allocation of naval ships for these input parameters. Figure 6 shows the first part of the model where for given capacity constraint Λ^-, optimal arrival rates λ_j^{-*} are determined and the pirate's success probability is calculated.

The second part of the model translates the optimal interception probabilities to the number of ships needed at each patrol area. The interception probabilities correspond to the success probability of the pirate, figure 7 shows the total number of naval ships needed to reduce the success probability of the pirates to a certain desired level. Since only an integer number of ships can be allocated to patrol areas, we need to round the number of ships allocated to each area. When rounding the number of naval ships, also the success probability of the pirates

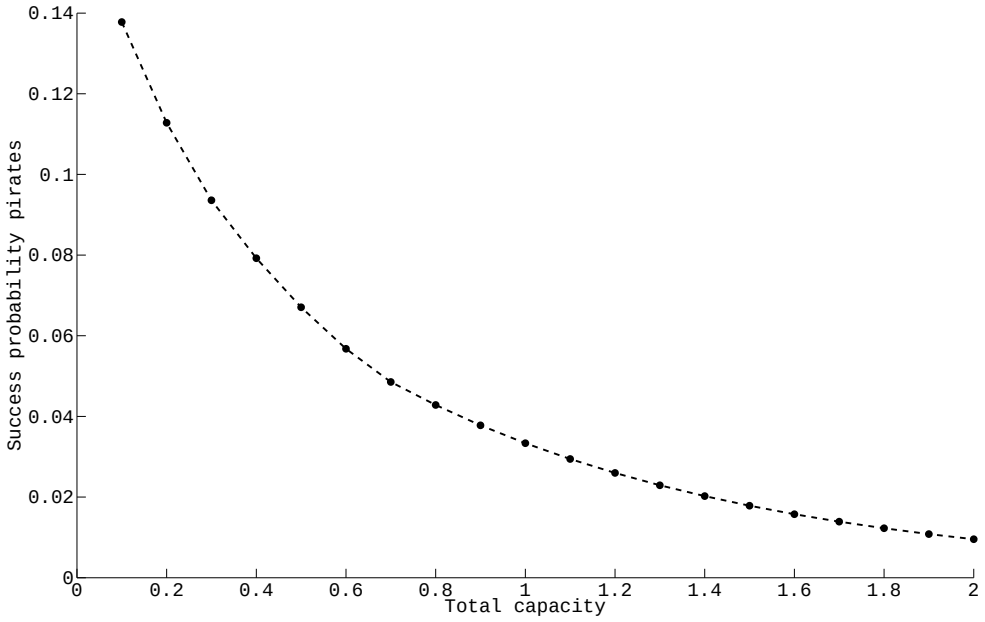

Figure 6: The success probability of the pirates, given the total arrival rate capacity Λ^-.

change. The success probability in case of a integer number of ships is determined by the maximum success probability over all patrol area. Figure 7 shows both the rounded and unrounded results.

Inverting figure 7 gives us the results we set out to obtain, the pirate's succes probability for given number of naval ships, these are displayed by figure 8. Without any naval ships patrolling the areas, the success probability of the pirate will be 0.20, the maximum success probability of all operating areas. To half this probability, there are 10 naval ships needed. These ships will not be allocated to patrol areas 6 and 7, because the success probabilities in their corresponding operating areas are less than 0.10. Table 4 shows where the naval ships are deployed

In table 4 the total number of naval ships increases with what seems an arbitrary amount, however there is a simple explanation. Several patrol areas have the same characteristics, i.e. the same length, width and succes probability in their corresponding operating area. It is clear that in an optimal strategy the number of ships allocated to two patrol areas with the same characteristics should be equal. If this was not the case, one of the patrol area would generate a higher success probability for the pirates, which would be exploited by the pirates. So, increasing the number of ships in only one of the equivalent patrol area would not have any effect on the success probability of the pirates. Therefore, if we are to increase the number of naval ships in an area, we also increase the number of naval ships in the areas with the same

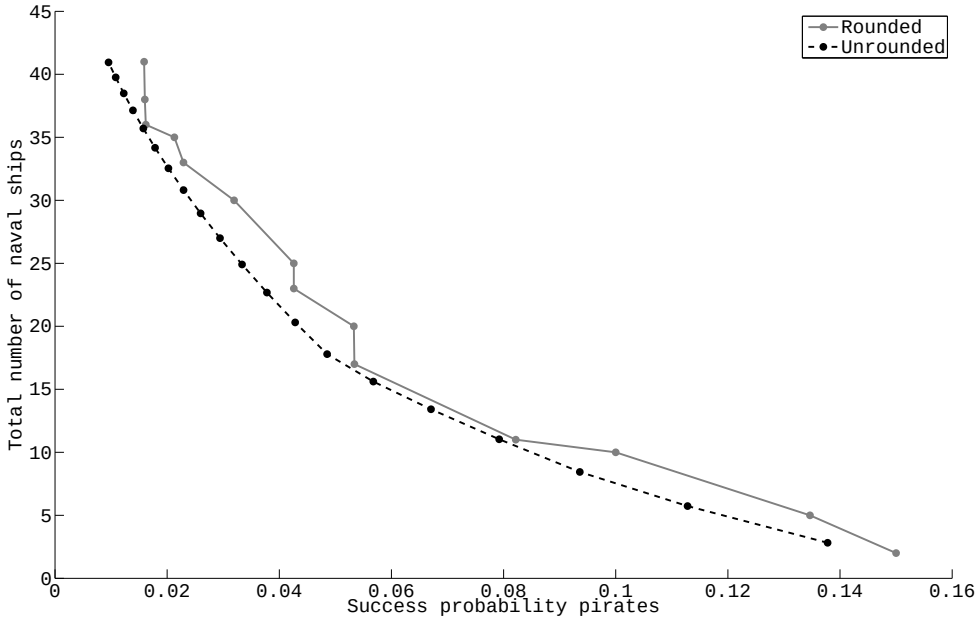

Figure 7: The number of naval ships needed for the reduction of the pirate's success probability.

characteristics, otherwise the extra naval ships would not generate any effect.

From figure 6 and 7 also the relation between the capacity constraint Λ^- and the total number of naval ships can be abstracted. Figure 9 displayes the relation between both capacity parameters. This relation is given via equations (121), (115) and (137).

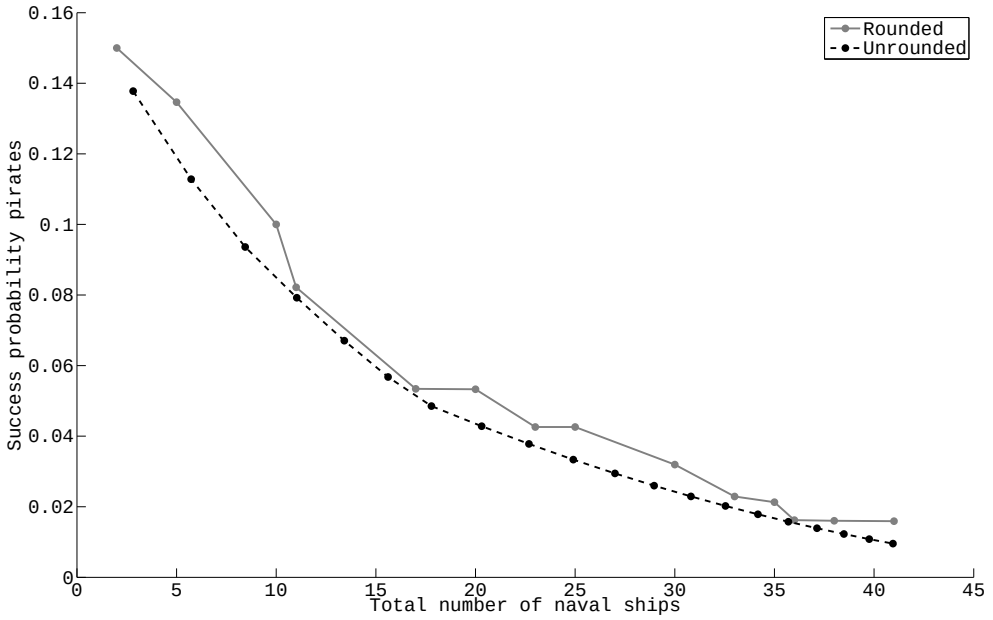

Figure 8: The pirate's success probability given the total number of naval ships being deployed.

Total number of naval ships	2	5	10	11	17	20	23	25	30	33	35	36	38	41
PA 1	1	1	2	2	3	3	3	3	4	4	4	4	4	4
PA 2	1	1	2	2	3	3	3	3	4	4	4	4	4	4
PA 3	0	1	2	2	3	3	4	4	4	5	5	5	5	6
PA 4	0	1	2	2	3	3	4	4	4	5	5	5	5	6
PA 5	0	0	0	1	2	3	3	3	4	4	4	5	5	5
PA 6	0	0	0	0	0	1	1	2	3	3	4	4	5	5
PA 7	0	0	0	0	0	1	1	2	3	3	4	4	5	5
PA 8	0	1	2	2	3	3	4	4	4	5	5	5	5	6

Table 4: Allocation of naval ships.

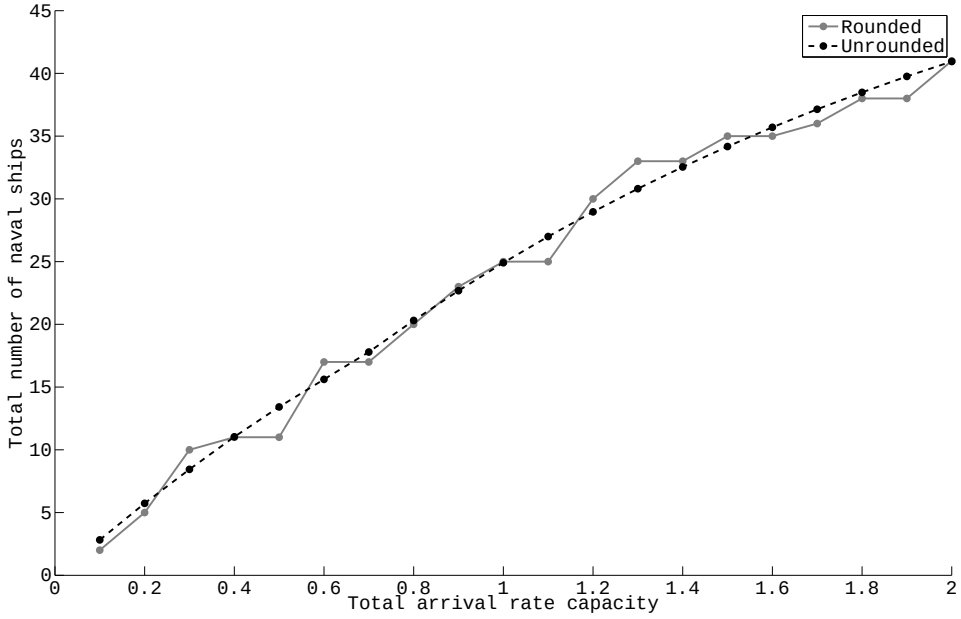

Figure 9: The relation between the total arrival rate and total number of naval ships.

6.3 Use of UAVs

To lower the success probability of the pirates, more naval ships are needed. However, the deployment of naval ships may be too expensive. An other way to increase the effect of the maritime patrol areas is to increase the naval ship's detection radius. If naval ships were equiped with Unmanned Aerial Verhicles (UAVs), the detection radius of the patrolling naval ships would increase greatly, while the costs of UAVs compared to the cost of entire naval ships are very small. Suppose that all naval ships are equiped with UAVs, what effect would that have on the total number of naval ships needed in the counter-piracy operation.

Naval ships equiped with UAVs have a larger detection radius, but move slower. Tabel 5 dispays the new ship parameters in this scenario.

Pirate speed	6	knots
Navy speed	12	knots
Detection radius	24	nm

Table 5: Ship parameters in case of UAV usage.

In table 6 the allocation of naval ships is shown in case the ships are equiped with UAVs together with the success probability of the pirates. We see that only 6 ships are needed to reduce the pirate's success probability to 0.05, without UAVs there were at least 20 ships needed to achieve such reduction.

Total number of naval ships	0	2	5	6	8	11	12	14
PA 1	0	1	1	1	1	1	1	1
PA 2	0	1	1	1	1	1	1	1
PA 3	0	0	1	1	1	2	2	2
PA 4	0	0	1	1	1	2	2	2
PA 5	0	0	0	1	1	1	2	2
PA 6	0	0	0	0	1	1	1	2
PA 7	0	0	0	0	1	1	1	2
PA 8	0	0	1	1	1	2	2	2
Success probability of pirates	0.2000	0.1500	0.1000	0.0500	0.0458	0.0326	0.0326	0.0326

Table 6: Allocation of naval ships with UAVs.

Figure 10 shows resulting success probabilities for pirates for a given number of allocated naval ships, both with and without onboard UAVs. Clearly the increase in detection radius by the use of UAVs descreases the number of required naval ships significantly.

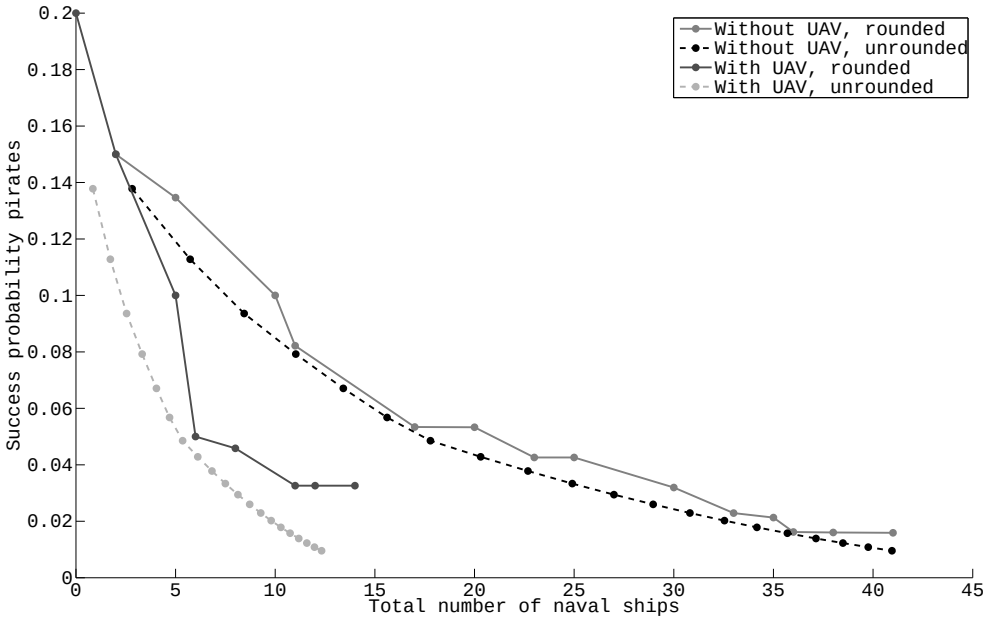

Figure 10: The success probability of the pirates, given the total number of naval ships with and without UAVs

7 Conclusions

7.1 Conclusions

This research developed a model to help decision making in area of homeland security and defense, in particular to help decision making concerning the deployment of security forces to intercept threats. The model is applied to the problem of allocating naval ships to maritime patrol areas in the Somali Basin to intercept pirates attempting to hijack passing merchant ships.

In deploying security forces to surveil areas and intercept threats, one has to keep in mind that threats emerge at unknown locations and unknown time. As a result deployed security forces operate in a stochastic environment. Furthermore, one has to take into account that multiple threats may be active at the same time at different locations. The model developed in this study takes both aspects into account in its approach to deploy security forces optimally. This in contrast to most models found in literature. Interdiction models as described in literature focus on static time-independent environment and model only single threats in a network. By taking the aspects of a stochastic time environment and multiple threats into account, the model presented in this study extends the interdiction models already studied.

Modeling the deployment of security forces in a network is done by an interdiction game on a queueing network. By using an interdiction game, we take into account that security forces are faced with intelligent opposers. The queueing network provides for the incorporation of multiple threats and a stochastic time environment. The notion of negative customers is used to model the interception of threats in the network by security forces. This interdiction game on a queueing network in analyzed and optimal strategies are obtained. In general networks optimal mixed strategies exists for both the interdictor, which deploys security forces, and the operator, which routes threats through the network. Moreover the interdictor has an optimal pure strategy in these games. For special networks, the network of parallel queues and the network of tandem queues, optimal strategies for both players are found.

In this study we also provided insight in the effects of deploying naval ships in the Somali Basin to counter the threat of piracy. We developed a method using the developed interdiction game, to consult on the allocation of naval ships to patrol areas. This method can be used to determine where available naval ships should patrol to reduce pirate attacks maximally. For given input parameters' values, we conclude that there are 10 naval ships needed to reduce the success probability of the pirates to 0.10. These naval ships need to be allocated to patrol areas corresponding to pirate operating areas with a higher success probability than 0.10. Furthermore a comparison is made between the deployment of naval ships equipped with Unmanned Aerial Vehicles (UAVs) and without. Analysis shows that equipping naval ships with UAVs significantly decrease the number of naval ships needed to achieve a certain effect. Without UAVs, 23 naval ships would be needed to reduce the probability of a successful pirate attack below 0.05. When equipping naval ships with UAVs, this number reduces to 6.

7.2 Discussion

While this research extends the interdiction models in literature, the applicability of this new model may be discussed. The results on the existence of optimal strategies hold for general networks. However these optimal strategies are only found in case of parallel queues and tandem queues. In networks with a general structure, the location of the optimal strategies is yet unknown. There may be many real life deployment problems which occur on networks with complicated structures, in these problems more analysis on our model should be done to help decision making.

In the application of the interdiction game on the deployment of naval forces in the Somali Basin, one may wonder if the applied method is the most simple and the most obvious method. Allocation problems are widely studied and other methods may be proposed to help decision making in this scenario. However, the value of the method developed in this study lies in the incorporation of the time-aspects of patrolling areas and the stochasticity involved in these time-aspects. Furthermore, the method proposed in this research is easy to implement and fast to solve.

7.3 Further research

As described, the presented interdiction game on queueing networks needs to be analyzed further to be applicable on problems occuring at general networks. This study only proves the existence of optimal strategies in the game on general networks, however the location of these optimal strategies is yet unknown except for specific network types.

Other research topics include new queueing models. This research focusses on single server queues with Poisson arrivals and exponential service times. Networks of these queues may not be well suited in all cases to model the interaction between security forces, threats and the environment. Other queueing models include the infinite server queues, where customers do not interact with and depend on other customers.

In application of the model of this research, one may consider cyber-security. Cyber-security is an important topic nowadays, which is concerned with the security of information in computer and communication networks. In these systems queueing models are often applied to model data-traffic between computer systems. So the use of queueing theory in these environments is natural and the use of interdiction games on queueing networks may help in decision making concerned with network security.

References

Assimakopoulos, N. 1987. A network interdiction model for hospital infection control. *Computers in Biology and Medicine*, 17(6): 413-422.

Alpern, S., A. Morton, K. Papadaki. 2011. Patrolling games. *Operations Research*, 59(5): 1246-1257.

Altner, D.S., . Ergun, N.A. Uhan. 2010. The Maximum Flow Network Interdiction Problem: Valid inequalities, integrality gaps, and approximability. *Operations Research Letters*, 38(1): 33-38.

Atkinson, M.P., L.M. Wein. 2008. Spatial queueing analysis of an interdiction system to protect cities from a nuclear terrorist attack. *Operations Research*, 56(1): 247-254.

Ball, M.O., B.L. Golden, R.V. Vohra. 1989. Finding the most vital arcs in a network. *Operations Research Letters*, 8(2): 73-76.

Bayrak, H., M.D. Bailey. 2008. Shortest path network interdiction with asymmetric information. *Networks*, 52(3): 133-140.

Berman, O., D. Krass, C.W. Xu. 1995. Locating flow-intercepting facilities: New approaches and results. *Annals of Operations Research*, 60(1): 121-143.

Berman, O., R.C. Larson, N. Fouska. 1992. Optimal location of discretionary service facilities. *Transportation Science*, 26(3): 201-211

Bier, V.M., M.N. Azaiez. 2009. Game Theoretic Risk Analysis of Security Threats. *Springer: The International Series of Operations Research and Management Science*, Vol. 128 (2009), ISBN 978-0-387-87766-2

Boccia, M., A. Sforza, C. Sterle. 2009. Flow Intercepting facility location: Problems, models and heuristics. *Journal of Mathematical Modelling and Algorithms*, 8(1): 35-79.

Bohnenblust, H., S. Karlin, L.S. Shapley. 1950. Games with continuous, convex pay-off. In: H.W. Kuhn, A.W. Tucker (Eds.), *Contributions to the Theory of Games, Annals of Mathematics Studies*, 24, Princeton University Press, Princeton (1950), pp. 181192

Brown, G., M. Carlyle, D. Diehl, J. Kline, K. Wood. 2005. A Two-Sided Optimization for Theater Ballistic Missile Defense. *Operations Research*, 53(5): 745-763.

Brown, G., M. Carlyle, R. Harney, E. Skroch, K. Wood. 2009. Interdicting a nuclear weapons project. *Operations Research*, 57(4): 866-877.

Brown, G., M. Carlyle, J. Salmern, K. Wood. 2006. Defending critical infrastructure. *Interfaces*, 36(6): 530-544.

Cappanera, P., M.P. Scaparra. 2011. Optimal Allocation of Protective Resources in Shortest-Path Networks. *Transportation Science*, 45(1): 64-80.

Chao, X. 1995. A queueing network model with catastrophes and product form solution. *Operations Research Letters*, 18(2): 75-79

Church, R.L., M.P. Scaparra, R.S. Middleton. 2004. Identifying Critical Infrastructure: The Median and Covering Facility Interdiction Problems. *Annals of the Association of American Geographers*, 94(3): 491-502.

Corley, H.W., H. Chang. 1974. Finding the n most vital nodes in a flow network. *Management Science*, 21(3): 362-364.

Corley, H.W., D.Y. Sha. 1982. Most vital links and nodes in weighted networks. *Operations Research Letters*, 1(4): 157-160.

Cormican, K.J., D.P. Morton, R.K. Wood. 1998. Stochastic Network Interdiction. *Operations Research*, 46(2): 184-197.

Fan, K. 1953. Minimax theorems. *Proceedings of the National Academy of Sciences USA*, 39:4247. 1953.

Fulkerson, D.R., G.C. Harding. 1977. Maximizing the minimum source-sink path subject to a budget constraint. *Mathematical Programming*, 13(1): 116-118.

Gelenbe, E., P. Glynn, K. Sigman. 1991. Queues with negative arrivals. *Journal of Applied Probability*, 28(1): 245-250.

Gelenbe, E. 1991. Product-form queueing networks with negative and positive customers. *Journal of Applied Probability*, 28(3): 656-663.

Gelenbe, E. 1993. G-networks with signals and batch removals. *Probability in the Engineering and Informational Sciences*, 7(3): 335-342.

Glicksberg, I.L. 1952. A further generalization of the kakutani fixed point theorem, with application to nash equilibrium points. *Proceedings of the American Mathematical Society*, 3(1): 170-174.

Golany, B., E.H. Kaplan, A. Marmur, U.G. Rothblum. 2009. Nature plays with dice - terrorists do not: Allocating resources to counter strategic versus probabilistic risks. *European Journal of Operational Research*, 192(1): 198-208.

Hodgson, M.J. 1990. A flow capturing location-allocation model. *Geographical Analysis*, 22(3): 270-279.

Israeli, E., K. Wood. 2002. Shortest-path network interdiction. *Networks*, 40(2): 97-111.

Janjarassuk, U., J. Linderoth. 2008. Reformulation and Sampling to Solve a Stochastic Network Interdiction Problem. *Networks*, 52(3): 120-132.

Lim, C., J.C. Smith. 2007. Algorithms for Discrete and Continuous Multicommodity Flow Network Interdiction Problems. *IIE Transactions*, 39(1): 15-26.

Malik, K., A.K. Mittal, S.K. Gupta. 1989. The k most vital arcs in the shortest path problem. *Operations Research Letters*, 8(4): 223-227.

Morton, D.P., F. Pan, K.J. Saeger. 2007. Models for nuclear smuggling interdiction. *IIE Transactions*, 39(1): 3-14.

Pan, F., W. Charlton, D. Morton. 2003. A stochastic program for interdicting smuggled nuclear material. D. L. Woodruff, ed. *Network Interdiction and Stochastic Integer Programming.* Kluwer Academic Publishers, Dordrecht, The Netherlands, 1-20.

Phillips, C. 1993. The network inhibition problem. *Proc. 25th Annual ACM Sympos. Theory Comput.* ACM Press, San Diego, CA, 776-785.

Royset J.O., R.K. Wood. 2007. Solving the Bi-Objective Maximum-Flow Network-Interdiction Problem. *INFORMS Journal on Computing*, 19(2): 175-184.

Salmeron, J., K. Wood, R. Baldick. 2004. Analysis of electric grid security under terrorist threat. *IEEE Transactions on Power Systems*, 19(2): 905-912.

Salmeron, J. 2011. Deception Tactics for Network Interdiction: A Multiobjective Approach. DOI: 10.1002/net.20458 Published 2011 *Wiley Periodicals, Inc.*

Wagner, D.H., W.C. Mylander, T.J. Sanders. 1999. Naval Operations Analysis. *Naval Institute Press*, 421p.

Washburn, A., P.L. Ewing. 2011. Allocation of clearance assets in IED warfare. *Naval Research Logistics*, 58(3): 180-187.

Washburn, A., K. Wood. 1995. Two person zero-sum games for network interdiction. *Operations Research*, 43(2): 243-251.

Wein, L.M., M.P. Atkinson. 2007. The Last Line of Defense: Designing Radiation Detection-Interdiction Systems to Protect Cities from a Nuclear Terrorist Attack. *IEEE Transactions on nuclear science*, 94(3): 654-669.

Wollmer, R.D. 1964. Removing arcs from a network. *Journal of the operation research society of America*, 12(6): 934-940.

Wood, R.K. 1993. Deterministic network interdiction. *Mathematical and Computer Modeling*, 17(2): 1-18.

Yates, J., R. Batta, M. Karwan. 2011. Optimal placement of sensors and interception resource assessment for the protection of regional infrastructure from covert attack. *Journal of Transportation Security*, 4(2): 145-169.

Zenklusen, R. 2010. Network flow interdiction on planar graphs. *Discrete Applied Mathematics*, 158(13): 1441-1455.

Samenvatting

Bescherming van kritieke infrastructuren en waardevolle objecten is vaak een taak van toezicht houden op en patrouilleren van bepaalde gebieden. Het doel van deze vorm van bescherming is het onderscheppen van bedreigingen nog voor dat er acuut gevaar optreedt. Om bedreigingen te onderscheppen worden veiligheidseenheden ingezet en toegewezen aan bepaalde gebieden. Deze studie richt zich op het inzetten van deze veiligheidseenheden op de meest effectieve manier. Hierbij houden we rekening met het feit dat deze eenheden opereren in een onzekere en onvoorspelbare omgeving en vaak worden geconfronteerd met meerdere bedreigingen tegelijkertijd. Om de meest effectieve inzet van eenheden te bepalen, wordt een interdictie spel op een netwerk van wachtrijen beschreven en geanalyseerd. Voor dit spel wordt het bestaan van optimale strategien bewezen en in speciale netwerken worden deze strategien ook daadwerkelijk gevonden. Het spel wordt toegepast op de antipiraterij-missies in de wateren rondom Somali. We analyseren de toewijzing van marineschepen aan patrouillegebieden, met als doel piraten te onderscheppen. Een methode wordt ontwikkeld die helpt bij het toewijzen van beschikbare marineschepen aan patrouillegebieden, zodanig dat het aantal succesvolle piratenaanvallen maximaal verminderd wordt.