Target-Oriented Utility for Interdiction of Transportation Networks

by

Fuat Kosanoglu

A dissertation submitted in partial fulfillment of

the requirements for the degree of

Doctor of Philosophy

(Industrial and Systems Engineering)

at the

UNIVERSITY OF WISCONSIN-MADISON

2014

Date of final oral examination: 12/12/2014

The dissertation is approved by the following members of the Final Oral Committee:

Vicki M. Bier, Professor, Industrial and Systems Engineering
James Luedtke, Associate Professor, Industrial and Systems Engineering
Oguzhan Alagoz, Associate Professor, Industrial and Systems Engineering
Laura McLay, Associate Professor, Industrial and Systems Engineering
Teresa Adams, Professor, Civil and Environmental Engineering

Acknowledgments

I am very grateful and indebted to my advisor, Professor Vicki Bier, for her guidance, understanding, and patience during my graduate study. I am also thankful to her for giving me the opportunity to benefit her vast knowledge and experience. I feel privileged for having the pleasure of working with her.

I am grateful to Professor James Luedtke, for his great help and guidance in the modeling and solving my problem. I sincerely thank to Professor Laura McLay, Professor Oguzhan Alagoz and Professor Teresa Adams for their valuable suggestions and insights which helped me strengthen various aspects of this dissertation.

I would like to thank my lab mates Mehmet Ertem, Jonathan Welburn, Sinan Tas, Wen-Chieh Hu, Taher Jamshidi, Shuji Liu and Chen Wang. Last but not least I also would like to thank my other friends at the University of Wisconsin-Madison: Mucahit Cevik, Mehmet Ali Ergun, Sait Tunc, Mehmet Ayvaci, Safa Erenay, Mustafa Rasim Kilinc, Turgay Ayer, Onur Asan, Merve Bodur, Oguz Akkas, and James Codella for their support during my study. My special thanks to my friends Fikrullah Kisa, Berk Yavuzoglu, Kerim Karaoglu, Gultekin Gollu, Sinan Kesriklioglu, and other wonderful friends that I have had in Madison.

I am deeply and forever indebted to my beloved family for their love, support and encouragement throughout my entire life.

Table of Contents

List of Tables

List of Figures

Abstract

Optimal resource allocation in security has been a significant challenge for critical infrastructure protection. Numerous studies use game theory as the method of choice, because of the fact that an attacker can often observe the defender's investment in security and adapt his choice of strategies accordingly. However, most of these models do not explicitly consider deterrence, with the result that they may lead to wasted resources if less investment would be sufficient to deter an attack. In this research, we assume that the defender is uncertain about the level of defensive investment that would deter an attack, and use target-oriented utility theory to optimize the level of defensive investment, taking into account the probability of deterrence.

We first apply our models to simple systems (in particular, only parallel and series systems, and with only two components). In that case, we are able to show that the use of target-oriented utility to model attack deterrence can result in significantly more cost-effective protection. We then extend this study to optimal resource allocation for more cost-effective protection of transportation networks. We apply target-oriented, utility theory and use mixed-integer programming to determine the optimal level of investment to interdict an attacker on a transportation network. In our model, we consider optimal placement of detectors on a transportation network in order to reduce the success probability of an attack, and consequently deter attacks.

1 Introduction

Optimal resource allocation for protection of transportation networks is a major challenge for homeland security, due to the complex structure of such networks. The US ground transportation network is highly complex and interconnected with thousands of miles of highways and paved roadways [1]. This highly developed network enables traveling within cities and between cities and states for people and commercial suppliers, but also for attackers, who can utilize the road network in a covert manner. For example, an attacker can travel on highways or city roads with a vehicle loaded with explosives or radiological material mimicking a commercial supplier, reaching a crowded area or some critical infrastructure (e.g., an airport, hospital, or state capitol), and launching an attack that may result in hundreds of fatalities and billions of dollars of economic damage. Therefore, although monitoring all road networks is not possible, some critical roads likely need to be protected.

The Department of Homeland Security is spending millions of dollars on surveillance systems for fighting terrorism [2]. Some municipal security authorities are also investing in protection of critical infrastructures and strategic locations; for example, the New York Police Department has installed explosives sensors, radiation detectors, and security cameras on strategic roads and bridges. Development and efficient deployment of sensors and detector technologies is important for monitoring and protecting transportation networks. Wireless sensor networks and sophisticated detectors are commonly used for detection and early warning systems [3]. However, funds are limited, so resources need to be spent cost-effectively.

Game theory and optimization (in particular, network interdiction models) have been used to analyze the optimal protection of transportation networks. Protection against intentional attacks (such as terrorist attacks) is often modeled as a two player game in which an attacker aims to

maximize his payoff (e.g., maximize expected damage), and a defender invests in protection to reduce the attacker's payoff [4] with a limited budget. Although, current models can determine optimal allocation of a limited defensive budget, most models do not attempt to determine the optimal budget level. Also, few models explicitly consider deterrence of an attack, which can result in wasted resources if less investment would be sufficient to deter an attack.

Therefore, this research proposes to apply target-oriented utility theory [5] to achieve more cost-effective sensor placement on transportation networks. Target-oriented utility theory assumes that the decision maker wishes to maximize the probability of achieving an uncertain target (in our case deterrence threshold). In our research, we aim to develop a model that determines the optimal level of investment in security, taking into account the possibility of deterrence. Although we do not include attack cost in our models, deterrence is more plausible when the attack cost is high. For example, low-cost attacks (such as some computer network attacks) may be difficult to deter, if the attacker can simply launch multiple attacks without regard to cost [6], but high-cost attacks (e.g., involving acquisition of a nuclear weapon) may be deterred even if the success probability of the attack is not extremely low [7].

Of course, the threshold at which attackers will be deterred is generally not known by the defender. However, in the literature, there are limited empirical studies that provide some ideas of deterrence behavior. In the light of these studies, we capture the defender's uncertainty about the deterrence threshold with a probability distribution that enables us to consider the deterrence behavior of different types of attackers.

Moreover, the structure of the transportation network itself may have an important role in our research. For example, more complex and connected networks may be more difficult to protect than less connected networks.

This research aims to develop a method that can determine the most cost-effective resource allocation policies for different types of networks and against different types of attackers. In this work, we utilize game theory, optimization techniques, and target-oriented utility theory.

2 Literature Review

Transportation networks have always been attractive targets for terrorist attacks. Security of transportation networks has become more important for governments after September 11, 2001 [8]. Transportation networks include aviation, roads, maritime, mass transit, pipeline, and rail.

Although most efforts to secure transportation systems in the last few years have focused on aviation, there has been more consideration of highway/road networks (especially transportation of hazardous materials) in recent years [9]. In the past decade, there has also been growing research on sensor and detector technologies. Wireless sensor networks and sophisticated detectors are commonly used for detection and early warning systems [3]. However, most prior work has focused on detector development, with less consideration given to optimum deployment of these detectors over a network [10].

Optimal resource allocation for protection of transportation networks is a major challenge for homeland security, due to the complex structure of such networks and the potentially high cost of protecting a large network. The Department of Homeland Security is spending millions of dollars on surveillance systems (such as detectors and surveillance cameras) for fighting terrorism [2]. However, funds are limited, so resources need to be spent cost-effectively.

Conventional game theoretic models assume that the defender wishes to minimize or maximize some quantity, such as minimizing expected damage from an attack or maximizing the cost of an attack to the attacker. However, these models can result in wasted resources if less

investment would be sufficient to deter an attack. Few game-theoretic models explicitly consider attacker deterrence.

We discuss game-theoretic models (including models of deterrence) in section 2.1. In section 2.2, we review models for optimal protection of transportation networks, and discuss approaches for solving such models. Finally, in section 2.3, we review target oriented utility models, which provide one way of accounting for attack deterrence.

2.1 Game-theoretic Approaches to Resource Allocation in Security

Resource allocation in security has been extensively studied by many authors after the terrorist attacks on September 11, 2001. Numerous studies use game theory as the method of choice, because of the fact that an attacker can often observe the defender's investment in security and adapt his choice of strategies accordingly. Thus, the optimal defensive allocation should take into account the attacker's strategy and capabilities.

Investment in defense aims to reduce threat (by deterring a possible attack), vulnerability (by hardening a system), and/or consequences. Bier and Abhichandani [11] suggest a model for optimal resource allocation in series and parallel systems, assuming that the attacker wishes to maximize the success probability of an attack on the system, and the defender tries to minimize the probability of system failure. The extension of this work by Bier et al. [4] assumes that the attacker wishes to maximize the expected damage from an attack, while the defender's objective is to minimize the expected loss, taking into account not only system functionality, but also the inherent values of the components. In this model, the attacker may still launch an attack even if he cannot disable the entire system, due to the inherent values of the components (so, for example, disabling a single component in a parallel system can be worthwhile even though it won't lead to system failure).

Levitin has extensively studied security models. Most of his work assumes a static threat, and uses reliability theory rather than game theory. However, the following works illustrate his use of game theory to model optimum resource allocation in security. Levitin and Hausken [12] compare the effectiveness of redundancy versus component hardening. In this study, the authors analyze a two-stage min-max reliability game where the defender moves first by investing in protection (either redundancy or hardening); the attacker can then observe the system protections, and choose the best attack strategy. In a later study, Hausken and Levitin [13] present a game-theoretic optimization model in which two fully strategic agents (an attacker and a defender) both have perfect knowledge about the system and the available actions. The system consists of series and parallel components, and each component consists of elements in parallel. The defender can physically separate the system components, in order to apply different protection strategies to them; conversely, the attacker can attack different combinations of components using different attack strategies. The defender objective is to minimize expected damage, while the attacker maximizes expected damage, both subject to a budget constraint. In more recent work, Hausken and Levitin [14] [15] [16] assume that the defender can deploy false targets that the attacker cannot easly distinguish from the true targets. Both the defender and the attacker are assumed to be fully strategic, and both are assumed to have complete knowledge about the system structure and the available actions, but only the defender is assumed to know which targets are false.

In some situations (such as computer networks, aviation security, etc.), the level and effectiveness of defensive investment may depend on the actions of other defenders. Kunreuther and Heal [17] examine an interdependent-security (IDS) model in which any agent in the group suffers a loss in case of a successful attack. A loss can occur either if an agent doesn't invest in protection of its own asset, or due to contamination by other agents that didn't invest in security;

for example, even an airline that screens all incoming baggage could be affected by a bomb transferred from another airline that didn't screen baggage. In this model, each agent has perfect information about the risks and costs of security investment, and decides whether to invest in security. Heal and Kunreuther [18] propose a general model that encompasses three different types of IDS problems. In the first type, an agent may suffer a loss due to contamination by other agents even if he invests in security (partial protection with negative externalities). In the second type of IDS problem, if an agent invests in security, he will not be vulnerable to contamination by other agents (complete protection with negative externalities). For the third type, agents that invest in security may create positive externalities for other agents. In this paper, each agent makes its own decision regarding investment in security, but its outcome can be affected by the decisions of other agents. If an agent invests in security, he may avoid direct loss with certainty, yet may still be harmed by contamination from other agents that don't invest in security.

Note that most of these models do not explicitly consider deterrence, with the result that they may lead to wasted resources if less investment would be sufficient to deter an attack. However, deterrence is an important aspect of cost-effective counterterrorism security systems for homeland security [19]. In particularly one objective of investment in defense is often to deter a possible attack. McGill [20] discusses possible methods to deter an attack, including decreasing the success probability of an attack by investing in defense, reducing the perceived level of loss resulting from a successful attack, and increasing the perceived likelihood of retaliation after an attempted attack.

Keohane and Zeckhauser [21] discuss four types of security externalities. They note that investment in protection of a target may reduce the probability of attack on other targets in the same region, creating a positive local externality (discouragement), if protection of the original

target makes the entire region less attractive to the attacker (e.g., by total reducing expected damage). However, protecting a target in a given region may also divert the attack to other targets in the same region (diversion), creating a negative externality. If the attack is diverted to other regions, this is referred to as displacement. Finally, the fourth type of security externality is containment, in which protection of one target provides partial protection to other targets by reducing the risk of contamination (as discussed by Heal and Kunreuther [18]), without reducing the probability of direct attacks on those other targets. In this work, we define deterrence to involve diversion, displacement, and discouragement. Although containment is not directly included in our definition of deterrence, it could still contribute to deterrence (e.g., if the reduced consequences due to containment, making attacking a less attractive strategy).

Sandler and Arce [22] present a model of deterrence in which a terrorist group can attack either a business site or a tourist site. In this model, both types of sites wish to minimize the cost of deterring an attack plus the expected loss from an attack, while the attacker tries to maximize his payoff from launching an attack. Deterrence in this case involves diverting the attack to another site or target.

Arce et al. [23] study a model in which an attacker can use either a conventional attack or suicide tactics, while a defender invests in protection of multiple targets. When the attacker's effort exceeds the defender's effort, the attacker wins, and vice versa. Arce et al. find that, at equilibrium, the attacker may be deterred with positive probability, and if not will choose to attack at most one target.

Bier et al. [24] study a strategic model in which a defender allocates his resources to defense, and an attacker chooses a location to attack. The defender is assumed to be uncertain about the attacker's preferences, while the attacker can perfectly observe the defender's investment

in security. The attacker seeks to maximize his payoff from launching an attack, and the defender seeks to minimize the damage of an attack. In this model, like that of Sandler and Arce [22], defensive investment in one component may increase the probability of an attack on another component (diversion or displacement). Thus, the defender may optimally leave some components undefended, sometimes preferring higher vulnerability at a particular component (even if lower vulnerability could be achieved at no cost) in order to avoid diverting the attack to more valuable components. When the attacker has an "outside option" other than attacking, it is possible for defensive investment to deter any type of attack in this model, by reducing the overall success probability of an attack (a form of discouragement). In an application of this model, Bier et al. [25] quantify the attractiveness of various targets, and explore how the optimal budget allocation depends on the cost effectiveness of defensive investment.

Hausken and Zhuang [26] develop a model in which the defender moves first and the attacker moves second in each of multiple time periods. The attacker and the defender are myopic, in the sense of considering payoffs in only one time period when choosing their strategies for that period. Since parameter values may change over time (e.g., due to technological change), the attacker and the defender will in general use different strategies in each time period. Hausken and Zhuang indicate that when the attacker's valuation of the target is not sufficiently large relative to his attack effort, the attacker will not attack at all even if there is no investment in defense, and will instead carry over the unused attack resources to the next period. Moreover, even if the attacker's valuation of the target would have been large enough to justify an attack on an undefended target, the attacker may still be deterred by additional investment in defense, if the defender's valuation of the target is sufficiently large to justify a suitable level of investment. Deterrence in this case involves a form of discouragement, by reducing the attack success

probability (or increasing the level of attack effort that would be required to achieve a given success probability).

Azaiez and Bier [27] assume that the defender wishes to deter an attack by maximizing the cost of an attack to the attacker (again a form of discouragement, although not quite the same as that discussed by Keohane and Zeckhauser). The authors assume that the defender's investment in security increases the level of effort required for the attacker to attain a given probability of success. However, Azaiez and Bier do not explicitly consider the level of attack cost at which an attacker would be deterred, leading to possible overinvestment in security.

Zhuang and Bier [28] study a game theoretic model that finds equilibrium strategies for both attacker and defender in a resource allocation model for protecting against both terrorist attacks and natural disasters. In this study, the defender tries to maximize her expected utility (reducing probability of damage from both causes by investing). Their results indicate that attacker effort can be initially increasing in the level of defender effort in protecting against intentional attacks (reflecting a lack of deterrence), then decreasing, and eventually goes to zero for sufficiently large defensive effort (which means that the attacker has been deterred by discouragement).

Bier and Haphuriwat propose a model to determine how many containers would need to be inspected in order to deter smuggling attempts [29]. The model assumes that a sufficiently high probability of being caught may deter an attacker from smuggling weapons of mass destruction into US ports (through a form of discouragement). The defender moves first by choosing an inspection level to minimize the inspection cost plus the expected loss from a weapon being successfully smuggled into the US (both the expected damage plus the cost of any resulting retaliation), while the attacker wishes to find the best response to the defender's policy in order to

maximize his expected reward. In an extension of this work, Haphuriwat et al. [7] suggest a model to identify the required percentage of containers to inspect in order to deter one or more nuclear weapons from being smuggled into the US in shipping containers.

2.2 Network Interdiction

2.2.1 Models of Network Interdiction

Network interdiction models have been a subject of interest in both transportation security and military applications. In the literature, there are both deterministic models, in which all parameters (e.g., arc capacities and/or arc lengths) are known, and stochastic models, in which some parameters are specified only by probability distributions. We discuss first deterministic models, and then stochastic models.

An early study of interdiction of transportation networks is by Wollmer [30], who proposes an algorithm for sensitivity analysis on transportation network flows. In particular, the algorithm chooses which arcs to remove from a network in order to minimize the maximum network capacity between an origin and a destination node. In this study, the decision maker can remove only a fixed number of arcs (subject to a cardinality constraint). McMasters and Mustin [31] introduce a network interdiction algorithm for reducing the supply capability of the opposing force in a war. Like Wolmer, McMasters and Mustin also consider minimizing the maximum flow capacity between an origin and destination node, but allow incremental interdiction (rather than only complete elimination of an arc), in which the interdictor incurs a cost for reducing the capacity of an arc. In this study, the budget constraint is the number of aircraft available for use in reducing the capacity of the enemy's supply lines. In a similar study, Ghare et al. [32] provide an algorithm that minimizes the amount of an enemy's war materiel flowing from depots to battlefield areas. The interdictor chooses a set of arcs to remove from the system in order to minimize the maximum

flow with a limited budget. Wood [33] studies a variation of this problem, and proposes an integer programming formulation. Ratliff et al. [34] also aim to minimize the maximum flow capacity of a network by finding the *n* most vital arcs whose simultaneous removal from a connected network would result in the maximum decrease in the capacity of the remaining network.

Fulkerson and Harding [35] consider the problem of maximizing the length of the shortest path between a source node and a sink node given a limited budget, with a cost per unit for increasing the length of an arc. They investigate the optimal budget allocation among arcs, and show that this problem is computationally equivalent to the minimum cost flow problem. In a similar study, Golden [36] also considers maximizing an adversary's shortest path. Golden's model ensures an increase in the length of the adversary's shortest path via a least-cost investment strategy. A different version of the shortest path problem considers removing (or interdicting) a fixed number of arcs to cause the maximum increase in the length of the shortest path [37] [38] [39]. Israeli and Wood [40] formulate a generalization of this problem such that instead of removing a fixed number of arcs, the defender has a limited interdiction budget.

Bayrak and Bailey [41] study a similar network interdiction model with asymmetric information. In this model, the evader aims to travel through the network without being detected, so his objective is to find the path that minimizes the detection probability; the interdictor installs sensors throughout the network to maximize this probability. However, the interdictor and evader have different information on the detection probabilities. The interdictor has full knowledge of both the detection probabilities and the evader's estimates of the detection probabilities, while the evader has only his own estimates.

The models discussed above are all deterministic. Specifically, arc capacities and/or arc lengths are all assumed to be known, as is the effectiveness of interdiction efforts. Cormican et al.

[42] present a stochastic variant of a network interdiction model. They propose a stochastic network-interdiction problem (SNIP) in which the defender minimizes the expected maximum flow that can be achievable by an attacker, with probabilistic interdiction success or failure (i.e.,the arc will be interdicted with probability *p,* but the defender will fail to interdict the arc with probability *1-p*), formulated as a two-stage stochastic program. In the first stage, the defender chooses which arcs to attempt to destroy or interdict in order to minimize the expected maximum flow that can be achieved by the attacker, such that if an arc is successfully destroyed, that arc capacity becomes zero. In the second stage, an attacker with full knowledge of the resulting network chooses the path that actually maximizes the flow through the remainig network.

Hemmecke et al. [43] study a SNIP model that maximizes the expected shortest path length between source and target nodes. However, they note that for some cases (such as drug transport networks), maximizing the expected shortest path length may not be an appropriate objective function. Thus, they also maximize the probability that the shortest path exceeds a certain length. Held et al. [44] study a similar problem, maximizing the probability that the length of the shortest path between source and target nodes exceeds a certain threshold.

Morton et al. [45] provide two SNIP models for nuclear smuggling interdiction. In the first model, the smuggler aims to travel through a network on a path that maximizes the probability of non-detection, while the interdictor tries to minimize the smuggler's non-detection probability by installing sensors on the network (at most one sensor can be installed on each arc). In this model, the smuggler can observe the sensor locations. Both the smuggler and the interdictor have accurate knowledge of the detection probabilities, but the interdictor has only a probability distribution for the smuggler's origin-destination pair. In the second model, the smuggler and the interdictor have different perceptions of the network (since the smuggler knows only some of the sensor locations).

Morton et al. also give solutions for a special case of these two models in which sensor placement is restricted to be only at border crossings, and once the smuggler is detected he cannot make another attempt to cross the border (which means that the smuggler can encounter only a single sensor). These types of networks are called bipartite networks, since the nodes can be partitioned into two subsets (i.e., on the two sides of the border), with no links between nodes in the same subset. Morton et al. develop valid inequalities to reduce computation time, and present computational results for bipartite networks. An extension of this work by Pan and Morton [46] solves this problem more generally (instead of just for bipartite networks). They develop valid inequalities for the more general model in which the defender can install multiple sensors along any given path between the source and target nodes, and a smuggler therefore can encounter multiple sensors.

2.2.2 Solution Approaches for Network Interdiction Models

A typical network interdiction problem is in general a nested "min-max" model, in which the attacker and the defender have different objective functions. For example, in the inner problem, the attacker may maximize his objective function, while in the outer problem, the defender minimizes the attacker's objective function. Commercial software is generally not able to solve such problems directly.

Network interdiction problems can sometimes be solved indirectly with commercial software by taking the dual of the inner linear program and reformulating the entire problem as a nonnested mixed integer program (MIP). For example, Morton [47] analyzes both deterministic and stochastic network interdiction of shortest-path and maximum-reliability-path problems, and reformulates the original nested "max-min" optimization model to a non-nested mixed integer model using duality, yielding a model that is easier to solve. However, this method may fail when

taking the dual of the inner linear program is difficult or impossible, or the size of the problem is too large. For those cases, we may need more advanced solution methods. Solving stochastic network interdiction problems may require especially advanced methods, since stochastic network interdiction problems are generally more difficult to solve than deterministic network interdiction problems.

In moderately complex cases, decomposition algorithms can be employed. Decomposition algorithms decompose the master problem into sub-problems, and iteratively improve the bounds of the objective function value by solving the attacker and the defender problems for every sub-problem [48]. These methods can be employed for solving both deterministic and stochastic network interdiction models. However, as mentioned above, stochastic network interdiction problems may require more advanced methods when the number of sub-problems becomes too large.

In such cases, a more advanced method, sequential approximation, can be combined with decomposition algorithms to solve difficult stochastic network interdiction problems [42]. Sequential approximation generates lower and upper bounds on the objective function value based on Jensen's inequality, by replacing each random element (e.g., an arc capacity) by its mean. This method generates two different network interdiction formulations, one with a concave objective function, and the other with a convex objective function but the same optimal value of the objective function. In this approach, an approximate solution of the true problem is found by solving the problem for subsets from the state space of all possible scenarios of the original stochastic problem. At each iteration, decomposition algorithms are applied to each subset to find bounds on the objective function's optimal value; the upper bound (resulting from the concave objective function) and the lower bound (resulting from the convex objective function) are then refined by

considering additional subsets sequentially until the gap between the upper and lower bounds is sufficiently small. For example, Cormican et. al [42] uses sequential approximation to solve a stochastic network interdiction problem. However, when the number of scenarios is large, sequential approximation may confront the same limitations as decomposition without sequential approximation.

Another method for solving large scale stochastic network interdiction problems is sample average approximation. In this approach, instead of solving the original problem, sampling-based approximations of the problem are solved [49]. Monte Carlo random samples are generated from the original state space of all possible scenarios, and the solutions to these sample-average problems are used to find upper and lower bounds on the optimal value of the original objective function. As the size of the random sample gets large, the sample-average approximation solution will converge to the actual solution (provided that the sample average problem does not itself become too large to solve to optimality).

2.3 Target- Oriented Utility Theory

Conventional utility theory suggests maximizing utility (or expected utility, when uncertainty is involved). However, in many problems, a decision maker may want to achieve a target. Thus, use of targets is natural for many real-life problems. For example, a car company may simply want to achieve better reliability than its competitors, instead of aiming to maximize reliability; likewise, a defender may wish to achieve sufficient protection to deter attacks.

Target-oriented utility theory assumes that the decision maker wishes to maximize the probability of achieving an uncertain target. Of course, performance targets can be used for both single-attribute and multiattribute decision making. We start our discussion with single-attribute decision problems, and then continue with the multiattribute case.

Borch [50] is one of the earliest studies of target-oriented utility. He states that maximizing expected utility is equivalent to minimizing the probability of ruin (when ruin is defined in terms of a single attribute), if the utility function is increasing and its possible values are bounded both above and below. Berhold [51] shows that monotonically increasing and bounded single-attribute utility functions can be represented by probability distribution functions using linear transformation. He discusses the advantages of using probability distribution functions instead of utility functions due to the known properties of probability distribution.

Castagnoli and LiCalzi [52] study a single-attribute target-oriented utility model, and introduce a new interpretation of von Neumann-Morgenstern (VNM) utility. They interpret the normalized VNM utility function as the cumulative distribution of an uncertain target *T*, and show that maximizing the probability of meeting the uncertain target is equivalent to maximizing VNM expected utility. Bordley and LiCalzi [53] further show that single-attribute target-oriented utility satisfies Savage's axioms, and discuss the advantages of a target-oriented model.

Abbas and Matheson [54] study a normative target-based model, which introduces a new quantity, the "aspiration equivalent", as a deterministic performance target. In particular, they replace the usual utility function by a step utility function, where the step occurs at the "aspiration equivalent" (a point such that the expected utility of the original utility function equals the expected utility of the new step function). A step utility function defines an aspiration level that divides the range of outcomes into satisfactory (where the utility function is one) and unsatisfactory (where the utility function is zero). In this formulation, each alternative has its own aspiration equivalent. Abbas and Matheson give a comparison of different target setting methods (i.e., certainty equivalent, simulated random targets, aspiration equivalents), and note aspiration equivalents are deterministic targets that take into account both the utility function and the probability distribution

for the outcome of interest. In their study, they also show that maximizing expected utility is equivalent to choosing the alternative that maximizes the probability of meeting the aspiration equivalent. Unlike the targets of Castagnoli and LiCalzi, aspiration equivalents are deterministic targets that are known before the choice of an alternative.

In many decision making problems, the decision maker must consider multiple attributes. Bordley and Kirkwood [55] propose a new target-oriented utility approach that can be applied to multiattribute decision making. In this study, the decision maker seeks to maximize the probability of achieving uncertain targets for all attributes, assuming that targets and outcomes are independent. They also show that there is always a multilinear utility function that is strategically equivalent to the target-oriented formulation when targets are independent. However, Tsetlin and Winkler [56] show that multiattribute utility functions do not necessarily have an equivalent target-oriented formulation if the targets for different attributes are not independent. Furthermore, they describe the necessary conditions for expressing a multiattribute utility function in a target-oriented form, and identify a class of multiattribute utility functions that can be expressed in target-oriented form. However, they note that it is difficult to define sufficient conditions for a utility function to be expressed in target-oriented form. They also note that the commonly used additive utility function is consistent with the target-oriented formulation if the achievement of the various targets is independent. Tsetlin and Winkler [57] extend their work to allow dependence among attributes and target levels, and show the effects of dependence. For example, for the two-attribute case, increased positive dependence increases the chance that either both targets are met, or neither target is met, and reduces the chance that only one target is met. Likewise, in a multiattribute extension of Abbas and Matheson [54], Abbas and Matheson [58] present a model for setting deterministic targets for multiattribute decision making in a manner consistent with utility

maximization that takes into account trade-offs among attributes.

Bordley and Pollock [59] propose a utility-based utility maximization model for reliability-based design optimization. In general, uncertainty is often involved in design projects (e.g., regarding customer needs). Instead of maximizing utility under uncertain constraints, they instead maximize the probability that the design achieves its target (e.g., the probability that the designed product meets customer needs, when customer needs are uncertain).

In a similar study, Bordley and Pollock [60] propose a model to set targets for organizational activities. This study considers the case of a manager who needs to set performance targets appropriately. Setting targets too high may lead to risky and unreasonable decisions on the part of project leaders attempting to achieve these targets. On the other hand, setting easily achievable targets may result in underutilization for the organization. Therefore, the decision maker chooses a set of targets in order to maximize the probability of the overall value function for the organization exceeding its uncertain target and all the various individual targets being achievable (in the face of uncertainty about the maximum achievable performance).

In this study, we use target oriented utility to analyze the optimal protection of transportation networks, to reflect the fact that one goal of securing transportation systems is deterring a terrorist attack before it occurs. Target oriented utility allows us to model the defender's uncertainty about the threshold at which the attacker's success probability will be small enough to deter attacks. Therefore, we propose to apply target-oriented utility theory [55] to achieve more cost-effective protection of transportation networks, assuming that the defender aims to minimize the expected loss from an attack (taking into account uncertainty about the attacker's deterrence threshold), plus the investment in protection, and the attacker aims to maximize the probability of a successful attack.

3 Target-Oriented Utility Models for Simple Series and Parallel Systems

3.1 Basic Model Formulation

3.1.1 Single-Component System

We begin our work by constructing a basic model for a single-component system. This simple system gives us insights about how the value of the defender's objective function depends on the values of the parameters in the model. In this model, the defender aims to minimize the expected loss from an attack (i.e., the probability of failing to deter the attacker, times the loss from an attack), plus the level of defensive investment. The initial problem formulation for a single component is thus as follows:

$$min\ L\ (1 - P_d(c)) + x \tag{3.1}$$

where

L = Loss from a successful attack (which will be treated as a constant, even though it may of course be the expected value of a probability distribution for uncertain attack consequences)

c_0 = Initial investment in the component (prior to the start of our analysis)

x = Additional resources invested in the component

$c = x + c_0$ = Total investment

$P_d(c)$= Probability that an attack on a given component will be deterred at investment level c

We consider only two possible outcomes; either the defender successfully deters an attack, or the defender fails to deter an attack and suffers a loss L. In order to explore the effects of different probability distributions for the deterrence threshold, we assume that the level of investment x needed to deter an attack follows an exponential, Rayleigh, or Weibull distribution. In other words, our objective function can be:

$$min\ L\left(e^{-\lambda(x+c_0)}\right) + x \quad when\ P_d(c)\ is\ exponential \tag{3.2}$$

$$min\ L\left(e^{\frac{-\lambda^2(x+c_0)^2}{2}}\right)+x\ \ when\ P_d(c)\ is\ Rayleigh \tag{3.3}$$

$$min\ L\left(e^{-\left(\frac{x+c_0}{b}\right)^a}\right)+x\ \ \ when\ P_d(c)\ \ is\ Weibull \tag{3.4}$$

From now on, we will ignore c_0, and treat the initial investment as zero. This implies that the probability of deterring an attack is zero when the additional investment x is zero. In the real world, however, a system or component may of course have some inherent level of security even if no investment is made in protection.

As expected, the optimum defensive investment x^* is increasing in the loss L (see Fig's. 3.1-3.3). The defender is willing to pay more (and achieves a higher probability of deterrence) when the expected loss L from a successful attack is large. When $P_d(c)$ is exponential, the optimum level of defensive investment x^* is initially increasing in the cost effectiveness λ, and then decreasing (see Fig. 3.4). To understand this behavior, consider the fact that when cost effectiveness is zero, it is obviously optimum not to invest in defense, since investment would not affect the probability of deterrence. Then, for moderately small values of λ, the defender would need to invest quite a bit to achieve deterrence; as λ gets larger, lower levels of investment would still be enough to deter an attacker. When $P_d(c)$ is Rayleigh or Weibull, the optimum level of investment is initially zero; then, when the cost effectiveness of defensive investment is big enough to justify investing, the optimum level of investment x^* becomes positive and decreasing in the cost effectiveness of defensive investment (see Fig's 3.5-3.6).

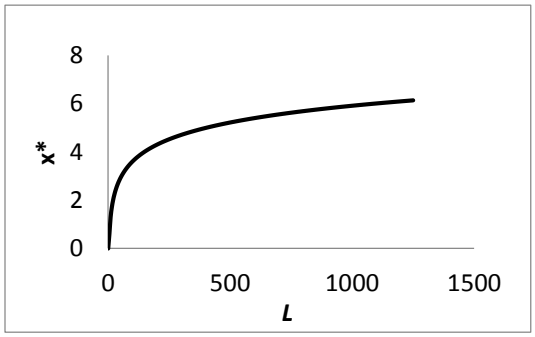

Figure 3. 1 Optimal defensive investment in a single component as a function of loss from a successful attack for exponential distribution (where $\lambda=1$)

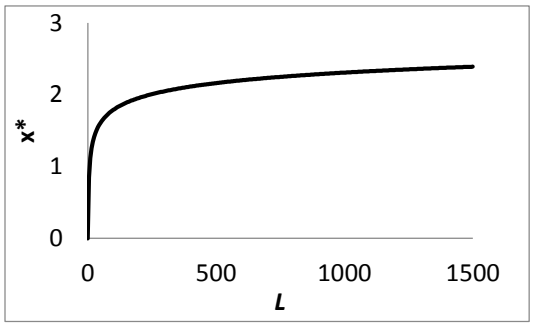

Figure 3. 2 Optimal defensive investment in a single component as a function of loss from a successful attack for Rayleigh distribution (where $\lambda=1$)

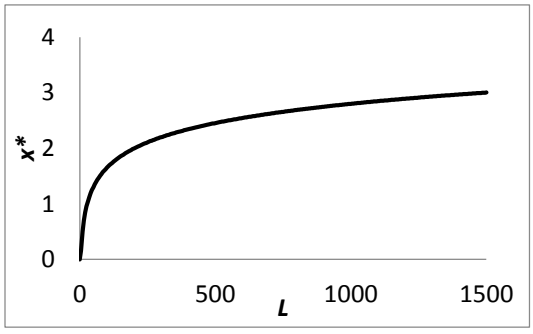

Figure 3. 3 Optimal defensive investment in a single component as a function of loss from a successful attack for Weibull distribution (where $\beta=1,\alpha=2$)

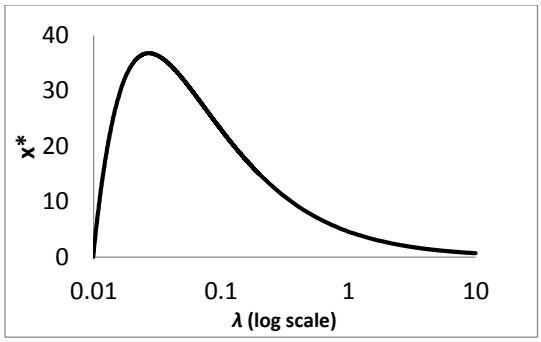

Figure 3. 4 Optimal defensive investment in a single component as a function of cost effectiveness of defense for exponential distribution in single systems (where L=100)

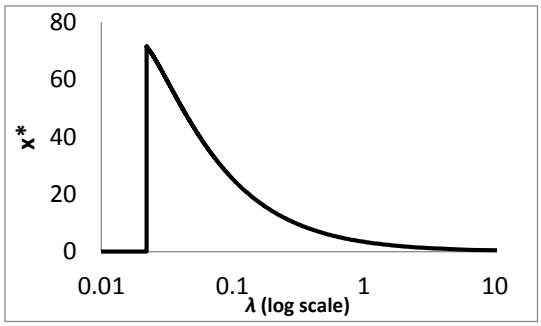

Figure 3. 5 Optimal defensive investment in a single component as a function of cost effectiveness of defense for Rayleigh distribution (where L=100)

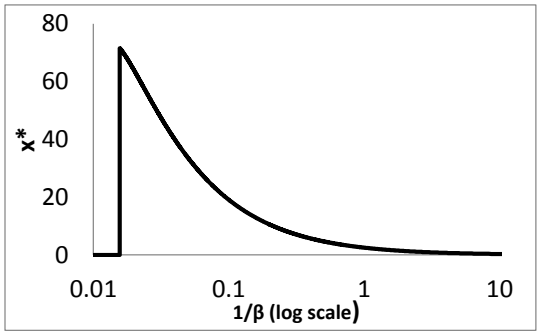

Figure 3. 6 Optimal defensive investment in a single component as a function of cost effectiveness of defense for Weibull distribution (where L=100, $\alpha=2$)

3.1.2 Two Components in Series

In series systems, a successful attack on even a single component would be enough to cause system failure. In some cases, this could be because the components are physically in series (such as electricity lines or pipelines); in other systems, components may be physically in parallel, but if both components are necessary for the system to function, they are still conceptually in series [11]. Since the components are in series, the attacker can succeed by disabling only one of them. However, the attacker may of course choose to attack both components; in this model, he is assumed to make independent decisions about whether to attack each component, based on whether the investment in defense of that component is sufficient to deter an attack.

The defender must protect both components to ensure the functionality of the system. Thus, the defender's objective function is to maximize the expected value of deterring attacks on both components, minus the defensive cost. The resulting model formulation for two components in series is as follows:

$$min\ \ L\,[\,1 - P_d(c_1)P_d(c_2)\,] + \ R \tag{3.5}$$

$$R = c_1 + c_2 = Total\ investment \tag{3.6}$$

where we have

$$min\ L\left[1 - \left(1 - e^{-\lambda_1 x}\right)\left(1 - e^{-\lambda_2 (R-x)}\right)\right] + R \qquad when\ F(c)\ is\ exponential \tag{3.7}$$

$$min\ L\left[1 - \left(1 - e^{\frac{-(a_1 x)^2}{2}}\right)\left(1 - e^{\frac{-a_2^2 (R-x)^2}{2}}\right)\right] + R \qquad when\ F(c)\ is\ Rayleigh \tag{3.8}$$

$$min\ L\left[1 - \left(1 - e^{-\left(\frac{x}{\beta_1}\right)^{\alpha_1}}\right)\left(1 - e^{-\left(\frac{(R-x)}{\beta_2}\right)^{\alpha_2}}\right)\right] + R \qquad when\ F(c)\ \ is\ Weibull \tag{3.9}$$

Results will be given in section 3.1.4.

3.1.3 Two Components in Parallel

In parallel systems, the attacker must disable both components to ensure failure of the entire system, since only one component is sufficient to ensure system functionality. The attacker is still assumed to make independent decisions about whether to attack each component (perhaps unrealistically, since attacks on any one component would not be sufficient to cause failure of the system). We relax this assumption later by taking into account the probability of successfully disabling entire system. The defender's objective is to minimize the expected loss from possible attacks on both components, plus the defensive cost. The resulting problem formulation for two components in parallel is as follows:

$$min\ \ L\ [\ (1 - P_d(c_1))(1 - P_d(c_2))\ ] +\ R \tag{3.10}$$

where we have

$$min\ L\left[\ \left(e^{-\lambda_1 x}\right)\left(e^{-\lambda_2 (R-x)}\right)\right] + R \qquad when\ F(c)\ is\ exponential \tag{3.11}$$

$$min\ L\left[\left(e^{\frac{-a_1^2(x)^2}{2}}\right)\left(e^{\frac{-a_2^2(R-x)^2}{2}}\right)\right] + R \qquad when\ F(c)\ is\ Rayleigh \tag{3.12}$$

$$min\ L\left[\left(e^{-\left(\frac{x}{\beta_1}\right)^{\alpha_1}}\right)\left(e^{-\left(\frac{(R-x)}{\beta_2}\right)^{\alpha_2}}\right)\right] + R \qquad when\ F(c)\ \ is\ Weibull \tag{3.13}$$

3.1.4 Results for Two-Component Systems

For convenience, we first consider a system of two identical components.

Proposition 1: *In a series system with two identical components, if the distribution $P_d(c)$of the deterrence threshold is exponential, the optimum is to invest equally in both components.*

Proof: When we differentiate the objective function and equate the result to zero, we get the following:

$$\frac{d(L\left[\left(1-e^{-\lambda x}\right)\left(1-e^{-\lambda(R-x)}\right)\right]-R}{dx}=L\left[\left(\lambda e^{-\lambda x}\right)-\left(\lambda e^{-\lambda(R-x)}\right)\right]=0$$

$$\left(\lambda e^{-\lambda x}\right)=\left(\lambda e^{-\lambda(R-x}\right)$$

$$-\lambda x=-\lambda(R-x)$$

$$x^{*}=\frac{R}{2}$$

We have not been able to show this analytically for other choices of F(c), but numerical sensitivity analysis suggests that the result holds (at least to a good approximation) for other distributions as well.

Proposition 2*: In a parallel system with two identical components, if $P_d(c)$ is exponentially distributed, the value of the objective function does not depend on the investment in either component individually.*

Proof:

$Z= min\ L\left[\left(e^{-\lambda x}\right)\left(e^{-\lambda(R-x)}\right)\right]+R = minLe^{-\lambda R}+R$, which does not depend on x.

However, this result is not valid for other distributions, as shown below.

Proposition 3: *In a parallel system with two identical components, if $P_d(c)$ is Rayleigh or Weibull distributed, the optimum is to invest the entire budget R in a single component.*

Proof: We provide a proof here for the Rayleigh distribution. The proof for the Weibull distribution is similar.

When we differentiate the objective function with respect to x and set the result equal to zero, we obtain

$$\frac{d\left(L\left[\left(e^{\frac{-a^2(x)^2}{2}}\right)\left(e^{\frac{-a^2(R-x)^2}{2}}\right)\right]+R\right)}{dx}=\frac{d\left(L\left[\left(e^{\frac{-a^2(x)^2-a^2(R-x)^2}{2}}\right)\right]+R\right)}{dx}$$

$$=L\left(e^{\frac{-a^2(x)^2-a^2(R-x)^2}{2}}\right)(-2x+2(R-x))=0$$

Note that $L\left(e^{\frac{-a^2(x)^2-a^2(R-x)^2}{2}}\right)$ will always be positive, so the above will be satisfied only when $2R-4x=0$, or in other words$x=\frac{R}{2}$. However, we still need to determine whether $x=\frac{R}{2}$is a minimum or a maximum. To do this, we compare the objective values at $x=\frac{R}{2}$ with the values at $x=0$ and $x=R$.

$$Z(0)=L\left[\left(e^{\frac{-a^2(R)^2}{2}}\right)\right]+R$$

$$Z(R)=L\left[\left(e^{\frac{-a^2(R)^2}{2}}\right)\right]+R$$

$$Z\left(\frac{R}{2}\right)=L\left[\left(e^{\frac{-a^2(R)^2}{4}}\right)\right]+R$$

Due to the factor of 4 in the denominator of the expression for $Z\left(\frac{R}{2}\right)$, we can see that

$$Z(0)=Z(R)<\ Z\left(\frac{R}{2}\right)$$

Thus, the objective function is minimized at either $x=0$ or $x=R$, meaning that all investment should be allocated to a single component.

Let R_p^* be the optimum level of investment in a parallel system with two identical components, and R_s^* be the optimum level of investment in series system with the same parameters (R_s^*). Then we have the following results.

Proposition 4: *When $P_d(c)$ is exponential,*

$$(i)\ If\ L\lambda < 1, R_s^* = R_p^* = 0 \tag{3.14}$$

$$(ii)\ If\ 1 < L\lambda < 5, 0 = R_s^* < R_p^* \tag{3.15}$$

$$(iii)\ If\ 5 \leq L\lambda, R_p^* < R_s^* \tag{3.16}$$

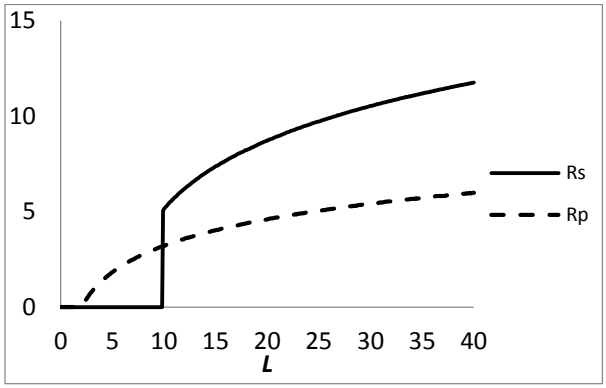

Figure 3. 7 Optimal total investment as a function of L in series and parallel systems where $P_d(c)$ is exponential distributed (λ=*1/2*)

The proof of this proposition is in the appendix.

We also used the BARON global-optimization software to explore whether results similar to those presented in proposition 4 hold for other distributions. Figure's. 3.8-3.9 below suggest that similar results do hold for other distributions. In particular, since series systems are more difficult and costly to defend than parallel systems, for moderate values of $L\lambda$, they are not worth defending at all. When $L\lambda$ is big enough for a series system to be worth defending, its defense requires greater investment at optimality, since it is inherently less secure.

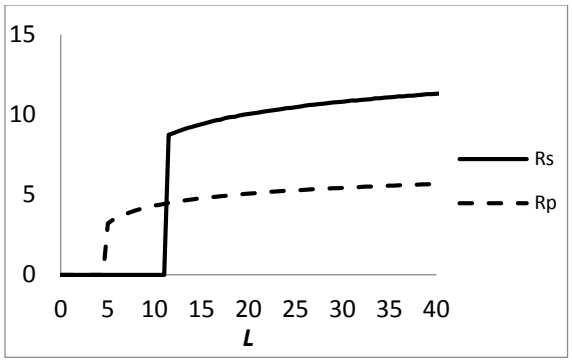

Figure 3. 8 Optimal total investment as a function of L in series and parallel systems where $P_d(c)$ is Rayleigh distributed (λ=1/2)

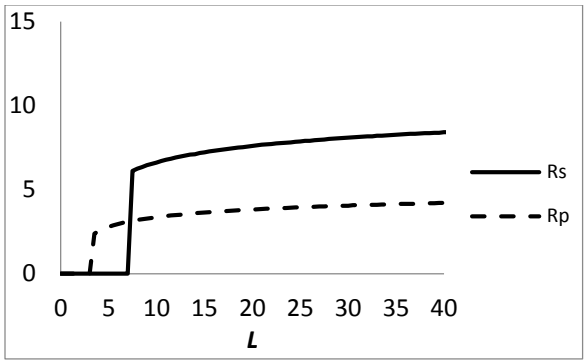

Figure 3. 9 Optimal total investment as a function of L in series and parallel systems where $P_d(c)$ is Weibull distributed (α=2,β=2)

We now consider components with different cost effectiveness of defensive investment. In particular, we hold the cost effectiveness of defensive investment in component 1 constant, and change the cost effectiveness of investment in component 2, such that $\frac{\lambda_2}{\lambda_1}$ =k ranges from 0 to 10.

In a series system, the optimal level of investment in component 1 is constant in k, while the optimal investment in component 2 is initially increasing in k, and then rapidly decreasing (see Fig. 3.10 for the exponential distribution and Fig. 3.11 for the Rayleigh distribution). For a parallel system, by contrast, when $P_d(c)$ is exponential, the defender does not invest in protection of component 2 at all unless it is more cost effective than component 1; conversely, there is no investment in component 1 when $\lambda_2 > \lambda_1$ (see Fig. 3.12). (Results for the Weibull distribution are similar to the results shown in Fig's. 3.11 and 3.13 for the Rayleigh distribution, so are omitted for reasons of space.)

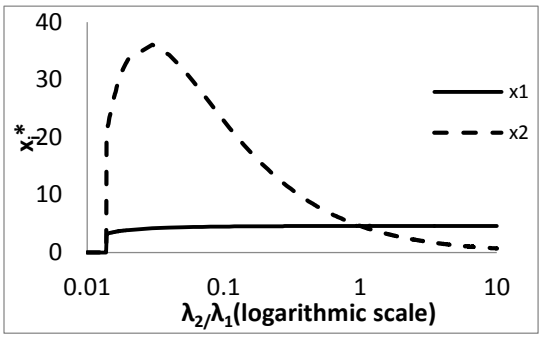

Figure 3. 10 Optimum investment level as a function of λ2 /λ1 in a parallel system ($P_d(c)$ is exponentially distributed, L=100, λ1=1)

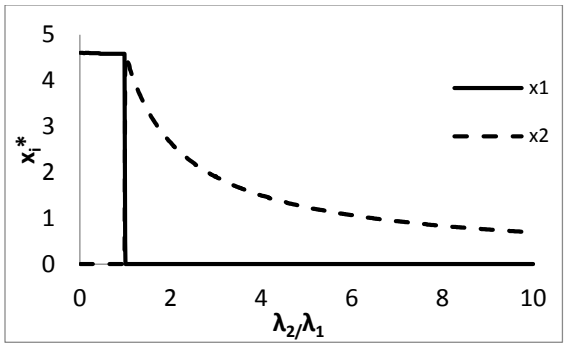

Figure 3.12 Optimum investment level as a function λ2 /λ1 in a series system ($P_d(c)$ is Rayleigh distributed, L=100, λ1=1)

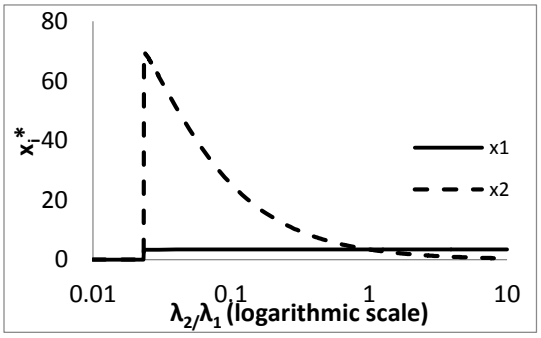

Figure 3. 11 Optimum investment level as a function of λ_2/λ_1 in a parallel system ($P_d(c)$ is exponentially distributed, L=100, λ_1=1)

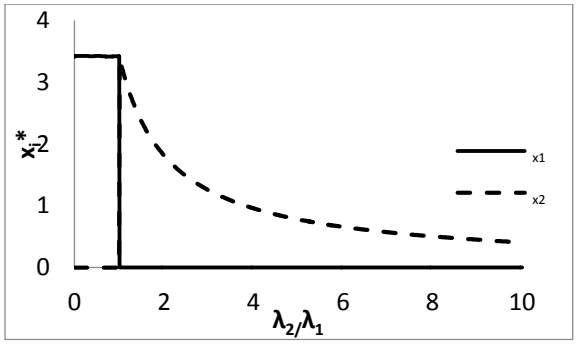

Figure 3. 13 Optimum investment level as a function of λ_2/λ_1 in a parallel system ($P_d(c)$ is Rayleigh distributed, L=100, λ1=1)

3.2 Probability of Deterrence as a Function of the Success Probability of an Attack

In this section, we define the probability of deterrence to be a function of the attacker's probability of successfully disabling the entire system. Here, we assume that an attacker would give up attacking when the success probability is sufficiently small. Thus, the defender may invest in protection both to reduce the success probability of an attack (if one occurs), and to deter the attacker (if the success probability becomes sufficiently small). The model formulation for a single component is as follows:

$$Z = min\ L\big[1 - P_d\big(P_s(x)\big)\big]P_s(x) + x \tag{3.17}$$

where

x= Resources invested

Z= The defender's optimum objective value

$P_s(x)$= *The success probability of an attack when investment level is* x

$P_d\big(P_s(x)\big)$= *The attack deterrence probability when the success probability of an attack is* $P_s(x)$

Since data directly relevant to deterrence of terrorist attacks is not available, it is difficult to determine the functional form of the deterrence probability. Fortunately, however, there are related empirical studies that can give some insight into the functional form of the probability of deterrence. In particular, based on data from interviews with imprisoned drug dealers, Anthony [61] suggests that a drug dealer would not be deterred at all if the perceived probability of interdiction is not sufficiently high, and then finds that the marginal rate of deterrence is increasing in the probability of success. In another empirical study based on interview data from serious adolescent offenders, Loughran et al. [62] suggest that increases in the detection probability reduce the rate of offending more when the detection probability is close to 0 or 1, resulting in a reverse S-shaped function. To reflect this behavior, we assume that the probability of deterrence follows a Kumaraswamy distribution [63]. It is defined over a domain of [0, 1], like the Beta distribution, but has the advantages of a simple closed-form cumulative distribution function. Moreover, since the Kumaraswamy distribution has two shape parameters (α,β), it is reasonably flexible; for example, in cases where attacks will be almost completely deterred for even a moderately large success probability, higher values of α will fit better. As shown in Fig. 3.14, the Kumaraswamy distribution with parameter values higher than 2 is S-shaped, and for parameter values lower than 1 is reverse S-shaped.

As stated above, Loughran et al. [62] suggest a reversed S-shaped function for deterrence, based on interview data from serious adolescent offenders. By contrast, in Anthony's work on imprisoned drug dealers [61], the deterrence probability is zero when the dealer has a success

probability close to 1; even if a drug dealer has a zero chance of success, he still cannot be deterred for sure. Moreover, decrements in success probability have less effect on deterrence when the success probability is low than it is high. Unlike both Anthony and Loughran, we believe that for terrorism, the probability of deterrence should be close to 1 when the probability of success is sufficiently low, since launching a terrorist attack is costly, so may not be undertaken at all when the probability of success is below some threshold. Thus, in the rest of this study, we will use an S-shaped deterrence function with parameter values α=2, β=2.

$$F(x) = 1 - (1 - x^{\alpha})^{\beta}, \quad 0 < x < 1 \qquad Kumaraswamy\ distribution \qquad 3.18$$

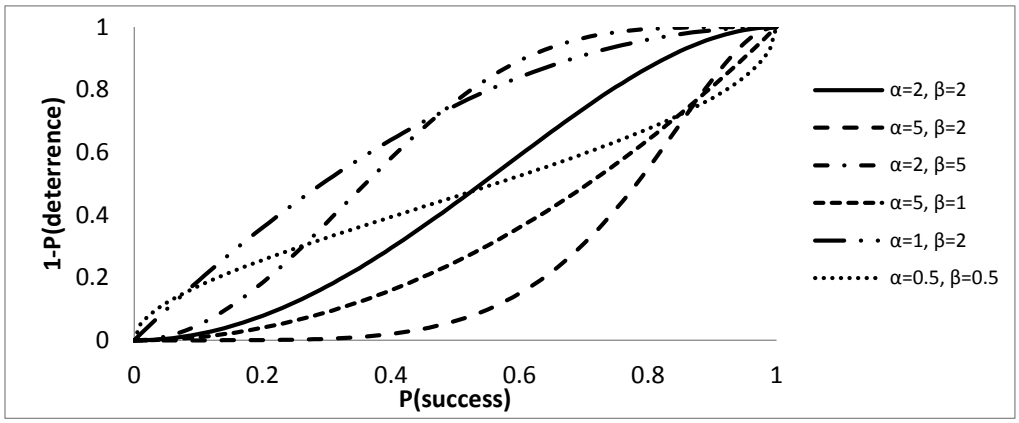

Figure 3. 14 The Kumaraswamy distribution with different shape parameters

We treat the probability of attack success as either an exponential or a Rayleigh function of the level of defensive investment. When the initial investment is expected to be more cost-effective than subsequent investments (e.g., representing decreasing marginal return), then the success probability function is assumed to be exponential.

By contrast, using the Rayleigh distribution, investment is initially relatively ineffective, than becomes highly effective near the mode of the distribution, and then reflects diminishing marginal returns after that. This might be a useful model for situations in which some minimal level of investment is required in order for investment to be highly cost effective (e.g., if the most cost-effective defensive options are also quite costly).

$$P(deter) = (1 - P(success)^{\alpha})^{\beta} \qquad (Kumaraswamy) \tag{3.19}$$

$$\begin{cases} P_s(x) = e^{-\lambda x} & (exponential) \\ or\ P_s(x) = e^{-\left(\frac{(\lambda x)^2}{2}\right)} & (Rayleigh) \end{cases} \tag{3.20}$$

The results for a single component are shown below. Increasing α results in a higher deterrence probability for a given success probability (see Fig. 3.14). This means that large values of α encourage non-zero spending even for low values of cost effectiveness (i.e., even when a given investment does not have much effect on the success probability of an attack), as shown in Fig.'s 15-16. At high cost effectiveness, high values of α permit deterrence to be achieved even with modest investment. As a result, larger values of α also lead to higher deterrence probabilities at optimality for a given level of cost effectiveness (see Fig.'s 3.17-18). By contrast, increasing β results in a lower deterrence probability for a given success probability. Thus, as β increases, the defender demands a higher level of cost effectiveness before beginning to invest at all (see Fig.'s 3.15-3.16). Moreover, for sufficiently high levels of cost effectiveness, high values of β also require higher levels of investment at optimality (see Fig.'s 3.15-3.16), to compensate for the smaller effect of attack success probabilities on deterrence (see Fig.'s 3.17-3.18).

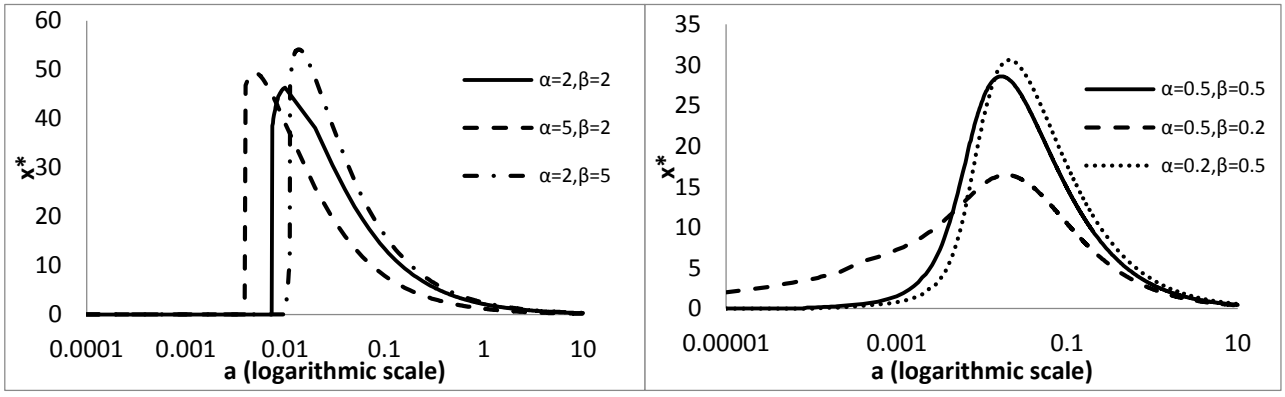

Figure 3. 15 Optimum investment level as a function of *a* in single-component systems where P_s is exponential (*L*=100)

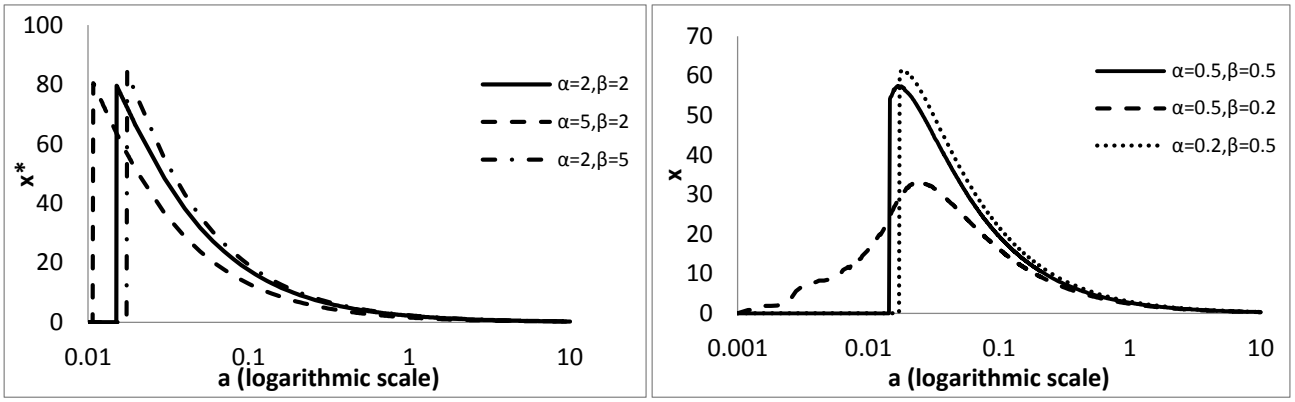

Figure 3. 16 Optimum investment level as a function of *a* in single-component systems where P_s is Rayleigh (*L*=100)

At moderately low cost effectiveness, high values of α also result in a reduced probability of success (see Fig's. 3.19-3.20), because they encourage investment. However, at higher cost effectiveness, high values of α are associated with increased values of the probability of success, because deterrence can be achieved even with moderately high probabilities of success. Conversely, for relatively low cost effectiveness, high values of β result in an increased probability of attack success, since no investment is made in protection. However, for higher cost effectiveness, higher values of β result in a reduced probability of attack success, to compensate for the reduced effect of the success probability on attack deterrence.

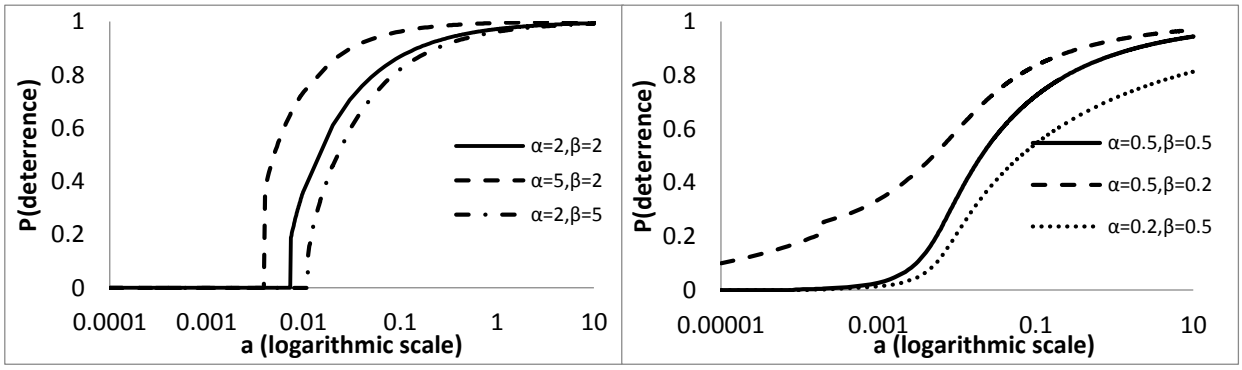

Figure 3. 17 Probability of deterrence as functions of *a* in single-component systems where P_s is exponential (*L*=100)

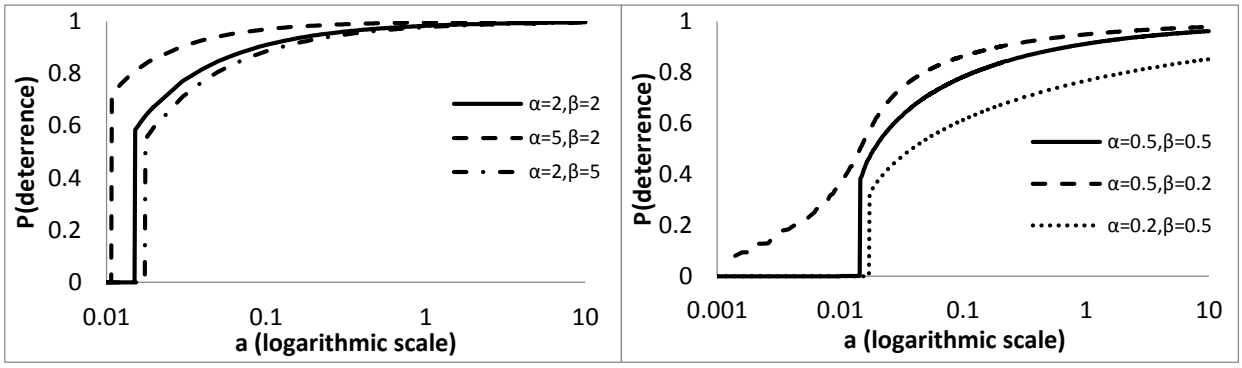

Figure 3. 18 Probability of deterrence as functions *a* in single-component systems where P_s is Rayleigh (*L*=100)

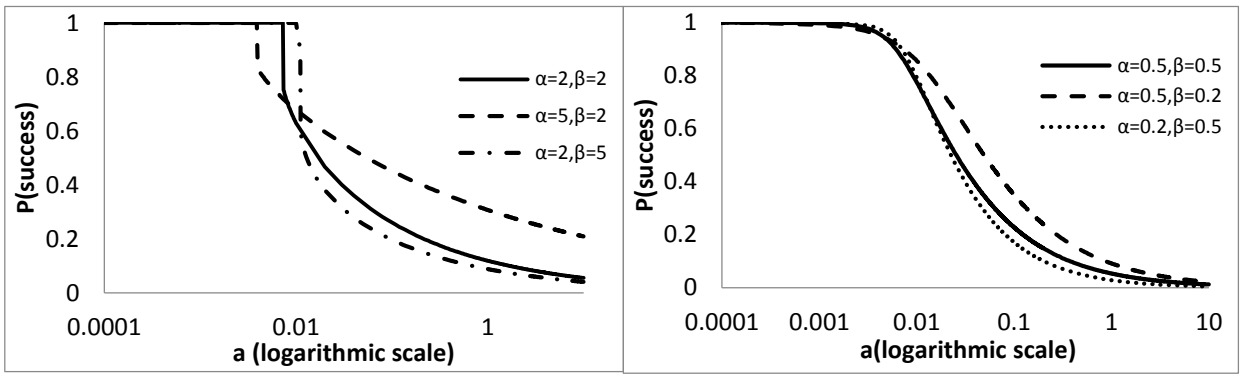

Figure 3. 19 Probability of success as functions of *a* in single-component systems where P_s is exponential (*L*=100)

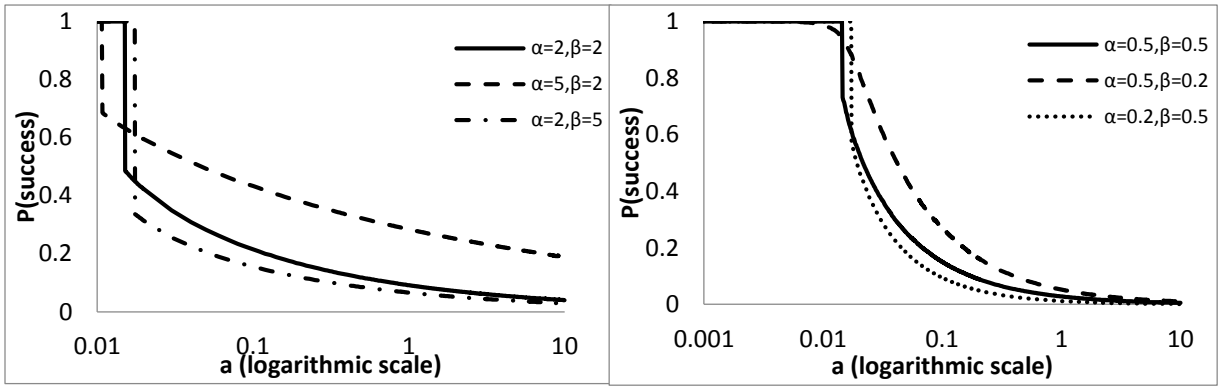

Figure 3. 20 Probability of success as functions *a* in single-component systems where P_s is Rayleigh (*L*=100)

3.2.1 Two Components in Parallel

In parallel systems, the attacker must disable both components to ensure failure of the entire system, since only one component is sufficient to ensure system functionality. An intelligent attacker hoping to fail the entire system would presumably not bother attacking only a single component. Therefore, for multi-component parallel systems, we assume that the attacker makes his decision about whether to attack based on the probability of successfully disabling the entire system, and define the probability of deterrence to be a function of that success probability. The resulting problem formulation for two components in parallel is as follows:

$$Z = min\ L\left[1 - P_d\left(P_s(x)\right)\right]P_s(x) + R \tag{3.21}$$

$$P_d\left(P_s(x)\right) = (1 - (P_s(x))^{\alpha})^{\beta} \qquad (Kumaraswamy) \tag{3.22}$$

$$P_s(x) = \prod_i P_s(x_i) \tag{3.23}$$

$$\begin{cases} P_s(x_i) = e^{-\lambda_i x_i} & (exponential) \\ or\ P_s(x_i) = e^{-\left(\frac{(\lambda_i x_i)^2}{2}\right)} & (Rayleigh) \end{cases} \tag{3.24}$$

where

$P_s(x) =$ *Probability of successfully disabling the entire system*
$P_s(x_i) =$ *Probability of successfully disabling component i*

We note that in a parallel system with two identical components, the success probability of an attack on the entire system does not depend on the investment in individual components when the success probability is exponential; it depends only on the total investment in the entire system. Fig. 3.21 below shows the optimal total investment level in the entire system. For the non-identical case, the defender chooses to invest only in the component that is more cost effective to defend (see Fig. 3.22).

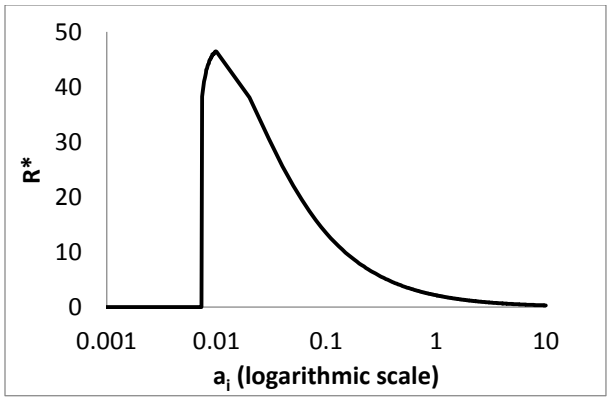

Figure 3. 21 Optimum investment level as a function of a in parallel systems where P_S is exponential (L=100 and α=2,β=2))

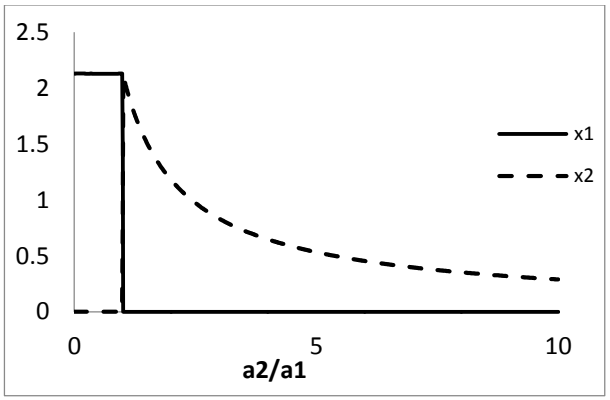

Figure 3. 22 Optimum investment level as a function of a_2/a_1 in parallel system where P_S is exponential (L=100 and α=2,β=2)

When the success probability of an attack is given by the Rayleigh distribution in a parallel system with two identical components, the defender chooses to invest in at most a single component. Total investment is initially zero, then positive and decreasing in the cost effectiveness a_i (see Fig. 3.23). We also note that the probability of success P_s is decreasing in a_i, and the probability of deterrence P_d is increasing in a_i, as for a single-component system (see Fig. 3.24). As shown in Fig. 3.25, for the non-identical case, the defender always chooses to invest in only the component with the higher cost effectiveness a_i.

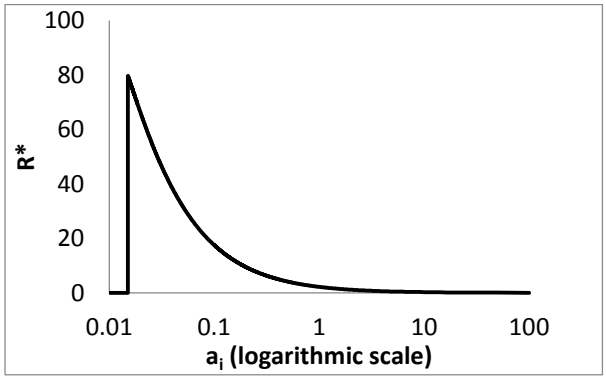

Figure 3. 23 Optimum investment level as a function of a in parallel systems where P_S is Rayleigh (L=100 and α=2,β=2)

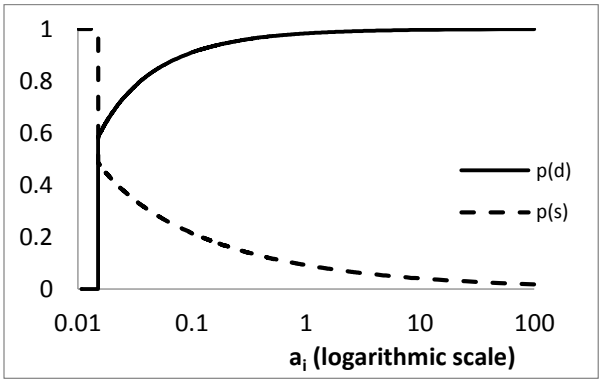

Figure 3. 24 Probability of success and probability of deterrence as functions a in parallel systems where P_S is Rayleigh (L=100 and α=2,β=2)

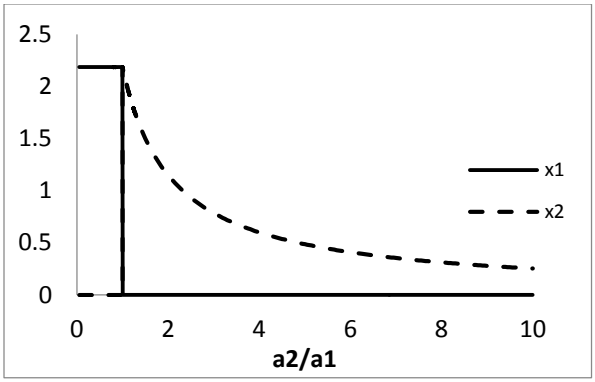

Figure 3. 25 Optimum investment level as a function of a_2/a_1 in parallel systems where $P_s$is Rayleigh (L=100 and α=2,β=2)

3.2.2 Two Components in Series

In series systems, a successful attack on even a single component would be enough to cause system failure. In some cases, this could be because the components are physically in series (such as electricity lines or pipelines); in other systems, components may be physically in parallel, but if both components are necessary for the system to function, they are still conceptually in series [11]. In attacking a series system, the attacker can choose to attack only one component or both. An attacker may prefer to attack only a single component if his only goal is disabling the entire system, or an attack on that component has an adequate chance of succeeding. Under other circumstances, an attacker might prefer to attack both components depending on the attack cost, the probability of success, and the attacker's budget. Since our model does not explicitly consider attack cost and attacker budget, here we consider two types of attackers: the first one attacks either both components or none; the second type attacks only the component with the higher success probability of attack (if attacking is worthwhile at all). In both cases, we model the probability of deterrence as a function of the attacker's probability of disabling the entire system, not the probability of disabling an individual component.

3.2.2.1 Attacker Attacks Both Components

In this case, the attacker attacks either both components or none. For example, the attacker may attack both components even when a single component failure would be sufficient to disable the system in order to increase the success probability of the attack, or maximize the damage, if attacks are sufficiently low in cost. The resulting problem formulation is as follows:

$$Z = min\ L\left[1 - P_d\left(P_s(x)\right)\right]P_s(x) + R \tag{3.25}$$

$$P_s(x) = 1 - \prod_i [1 - P_s(x_i)\,] \tag{3.26}$$

$$P_d\left(P_s(x)\right) = (1 - (P_s(x))^{\alpha})^{\beta} \qquad (Kumaraswamy) \tag{3.27}$$

$$\begin{cases} P_s(x_i) = e^{-a_i x_i} & (exponential) \\ or\ P_s(x_i) = e^{-\left(\frac{(a_i x_i)^2}{2}\right)} & (Rayleigh) \end{cases} \tag{3.28}$$

We first present results for two identical components. In this case, the levels of investment in defense of the two components will be equal. For low values of the cost effectiveness a_i, no investment in security is optimal, since investment would not have enough effect on the probability of success to be justified. When a is sufficiently large, the defender starts to invest; as the cost-effectiveness a_i gets larger, lower levels of investment would still be enough to deter the attacker (see Fig's. 3.26-3.27). Fig's. 3.28-3.29 show the probability of success (dashed line) and the probability of deterrence (solid line) as functions of the cost effectiveness a_i.

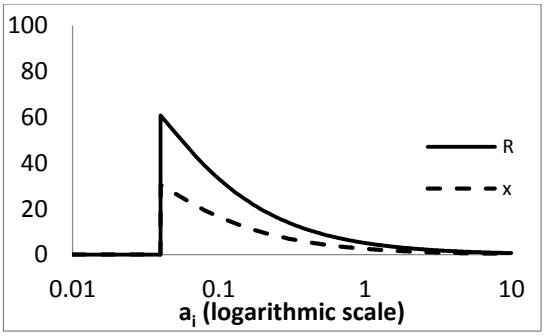

Figure 3. 26 Optimum investment level as a function of a in series systems where P_s is exponential and the attacker attacks both components (L=100 and α=2, β=2)

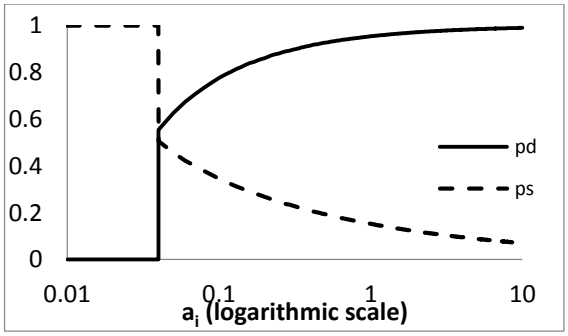

Figure 3. 27 Probability of success and probability of deterrence as a function of a in series systems where P_s is exponential and the attacker attacks both components (L=100 and α=2, β=2)

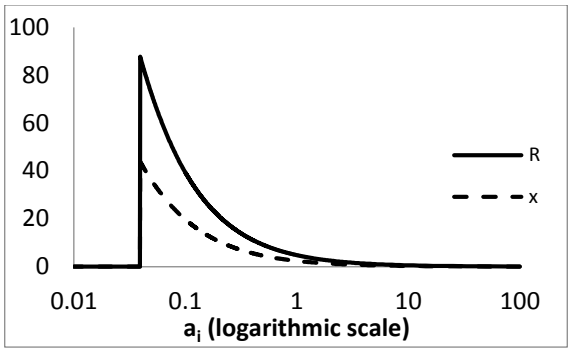

Figure 3. 28 Optimum investment level as a function of a in series systems where P_s is Rayleigh and the attacker attacks both components (L=100 and α=2, β=2)

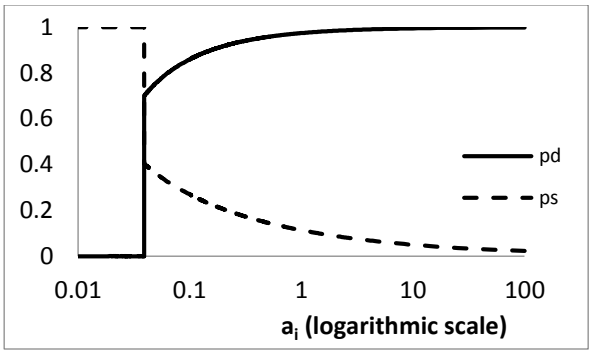

Figure 3. 29 The probability of success and the probability of deterrence as a function of a in a series system where P_S is Rayleigh and the attacker attacks both components (L=100 and α=2, β=2)

For a system with non-identical components, the defender invests more in the component with the lower cost-effectivness of defensive investment, as shown in Fig's. 3.30-3.31. Here, since both components are equally important to system functionaltiy, the defender attemps to make them equally vulnerable (or equally well protected).

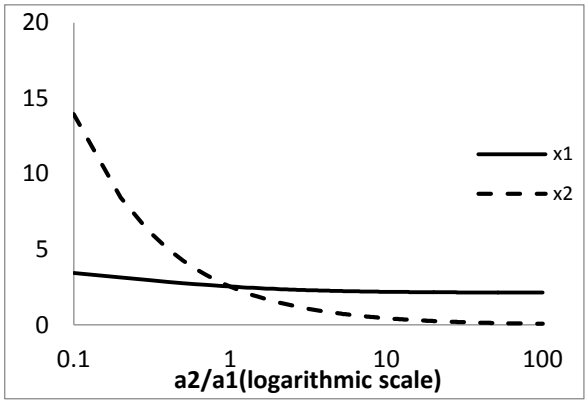

Figure 3. 30 Optimum investment level as a function of a_2/a_1 in series systems where P_s is exponential and the attacker attacks both components

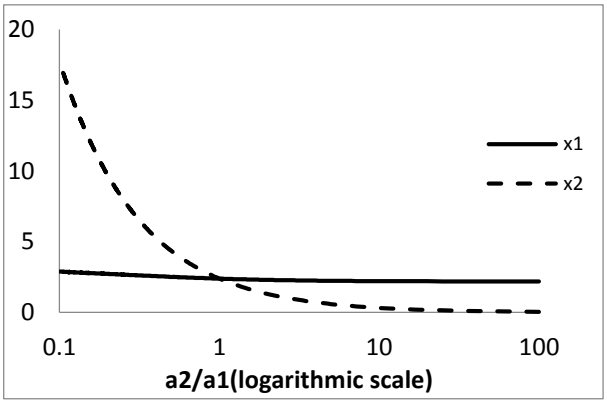

Figure 3. 31 Optimum investment level as a function of a_2/a_1 in series systems where P_s is Rayleigh and the attacker attacks both components

ble

In this case, the attacker chooses to attack the component with the higher probability of successful attack. This may be more realistic when the attacker has a limited budget or limited attack capabilities. The model formulation for this case is as follows:

$$Z = min\ L\left[1 - P_d\left(P_s(x)\right)\right]P_s(x) + R \tag{3.29}$$

$$P_s(x) = \max_i P_s(x_i) \tag{3.30}$$

$$P_d\big(P_s(x)\big) = (1 - (P_s(x))^{\alpha})^{\beta} \qquad (Kumaraswamy) \tag{3.31}$$

$$\begin{cases} P_s(x_i) = e^{-a_i x_i} & (exponential) \\ or\ P_s(x_i) = e^{-\left(\frac{(a_i x_i)^2}{2}\right)} & (Rayleigh) \end{cases} \tag{3.32}$$

As in the previous subsection, we first present results for a system with two identical components. As expected, the defender invests in both components equally, as shown in Fig's. 3.32-3.33. For low values of the cost effectiveness a, it is not worth investing at all, and the success probability of attack equals 1 (see Fig's. 3.34-3.35). When the cost effectiveness *a* is big enough to justify investing, then the success probability of attack is decreasing in a, and the probability of deterrence is increasing.

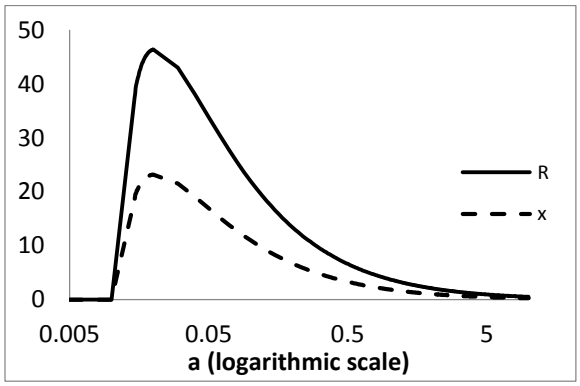

Figure 3. 32 Optimum investment level as a function of a in series systems where P_s is exponential and the attacker attacks the most vulnerable component (L=100 and α=2, β=2)

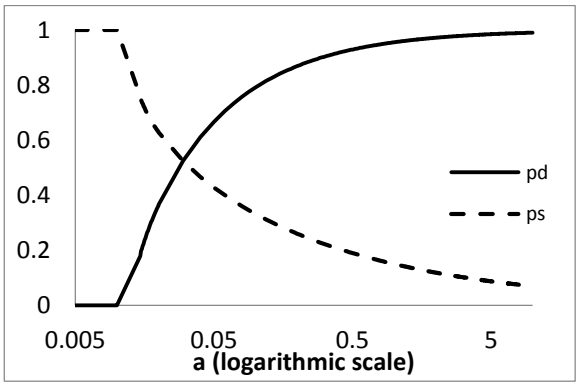

Figure 3.34 The probability of success and the probability of deterrence as a function of a in a series system where P_s is exponential and the attacker attacks the most vulnerable component (L=100 and α=2, β=2

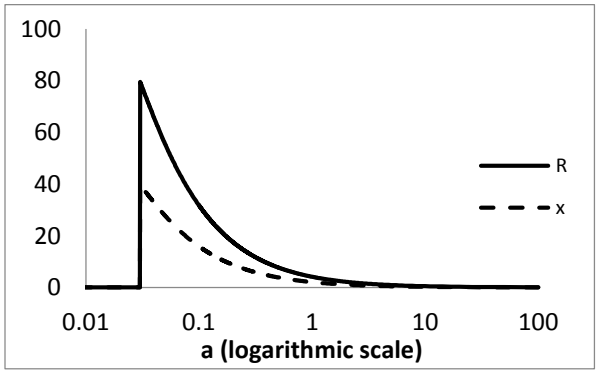

Figure 3. 33 Optimum investment level as a function of a in series systems where $P_s$is Rayleigh and the attacker attacks the most vulnerable component (L=100 and α=2, β=2)

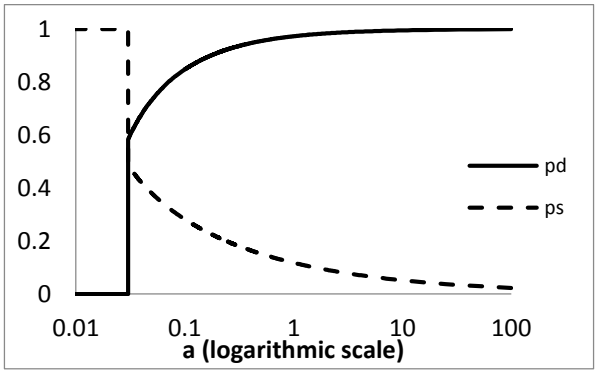

Figure 3. 35 The probability of success and the probability of deterrence as a function of a in a series system where $P_s$is Rayleigh and the attacker attacks the most vulnerable component (L=100 and α=2, β=2)

We also present results for series systems where each component has a different cost-effectiveness. As before, Fig's. 3.36-3.37 show that the defender invests more in the component that is less cost effective to defend. This is because the defender aims to have equal success probabilities of attack on both components, so must invest more in the component with smaller cost effectiveness.

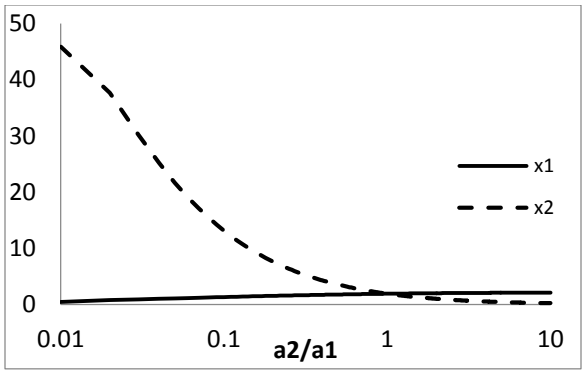

Figure 3. 36Optimum investment level as a function of a_2/a_1 in series systems where P_s is exponential and the attacker attacks the most vulnerable component (L=100 and α=2, β=2)

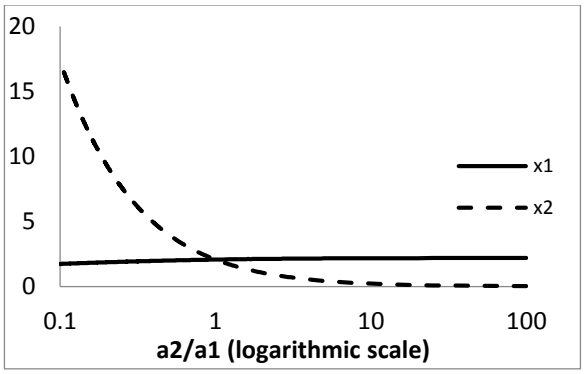

Figure 3.37 Optimum investment level as a function of a_2/a_1 in series systems where P_s is Rayleigh and the attacker attacks the most vulnerable component (L=100 and α=2, β=2)

3.3 Comparison of Target-Oriented Utility Model to a Conventional Game-Theoretic Model

As mentioned before, conventional game-theoretic models of homeland security can result in wasted resources when a lower level of investment would be sufficient for deterrence. Therefore, we now compare the target-oriented utility model to a conventional game-theoretic model that does not take into account the probability of deterrence. In the conventional model, the defender's objective is simply to minimize the expected loss (the actual loss L, times the success probability of an attack), plus the defense cost, assuming that an attack will take place regardless of the level of investment.

In the previous section, the success probability of an attack was assumed to be either an exponential or a Rayleigh function of defensive investment. Here, we will show only the

exponential case and omit the Rayleigh, since the results for the Rayleigh distribution are similar. The formulation of the non-deterrence model is as follows:

$$Z_N = \min_{x_N} LP_s(x_N) + x_N \tag{3.33}$$

where

$$P_s(x_N) = e^{-\lambda(x_N)}(exponential) \tag{3.34}$$

Let $x_N{}^*$ be the optimal investment level in the non-deterrence model.

By contrast, the formulation of the target-oriented utility model for a single component is;

$$Z_D = \min_{x_D} L\left[1 - P_d\left(P_s(x_D)\right)\right]P_s(x_D) + x_D \tag{3.35}$$

where

$$\begin{cases} P_s(x_D) = e^{-a(x_D)} & (exponential) \\ or\ P_s(x_D) = e^{-\left(\frac{(ax_D)^2}{2}\right)} & (Rayleigh) \end{cases} \tag{3.36}$$

$$P_d\left(P_s(x)\right) = (1 - (P_s(x))^{\alpha})^{\beta} \qquad (Kumaraswamy) \tag{3.37}$$

Let $x_D{}^*$ the optimal investment level in the deterrence model.

First, we explore the impact of the cost-effectiveness *a* in the exponential case. When the cost-effectiveness *a* is zero, the optimum investment levels x_D^* and x_N^* are both zero. As *a* gets larger, x_D^* is initially greater than x_N^* for small values of *a*, and then becomes less than x_N^* (see Fig. 3.38). Fig. 3.39 shows that the objective-function value for the model with deterrence (Z_D) is always better than for the model without deterrence (Z_N), as we would expect. However, that is for two different reasons; the ability to spend less when cost effectiveness is high, and the greater effectiveness of defense (due to the possibility of deterrence) when cost effectiveness is low.

We now explore what results would be achieved in the model with deterrence, if the optimum investment level from the model without deterrence (x_N^*) were chosen (e.g., if the

defender was not aware of the possibility of deterrence). Naturally, of course, x^*_D gives better results than x^*_N, as illustrated in Fig. 3.41, but for different reasons in different regions. At first, x^*_D is greater than x^*_N, but the defender benefits from a smaller expected loss, EL(x^*_D) < EL(x^*_N) (see Fig. 3.40). When *a* gets larger, and investment becomes more cost effective, x^*_N becomes greater than x^*_D, and therefore gives a worse value of the objective function, even though the expected loss when choosing x^*_N is less.

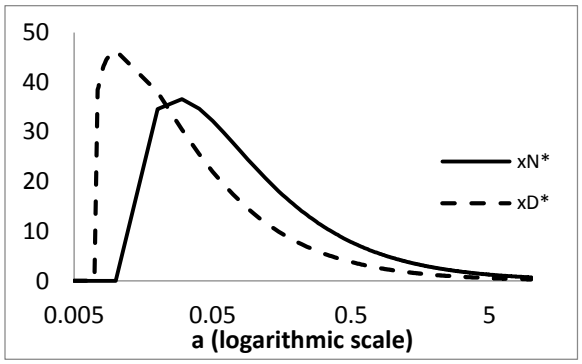

Figure 3. 38 Optimum investment levels as a function of cost effectiveness a for non-deterrence and deterrence models where P_s is exponential (L=100 and α=2, β=2)

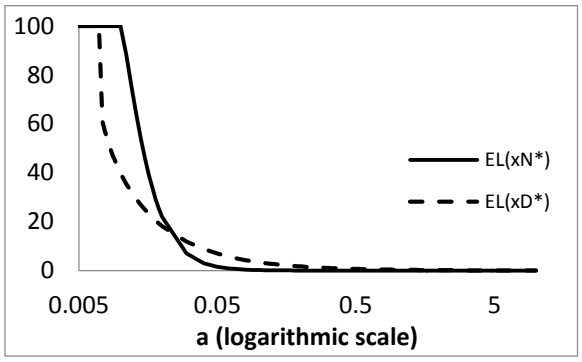

Figure 3. 40 Expected loss as a function of a for non-deterrence and deterrence models where $P_s$is exponential (L=100 and α=2, β=2)

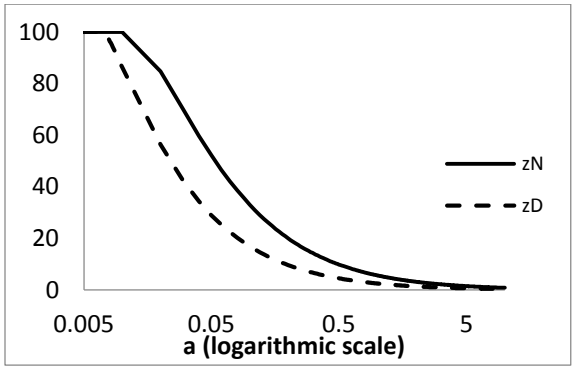

Figure 3. 39 Value of objective function as a function of cost effectiveness a for non-deterrence and deterrence models where P_s is exponential (L=100 and α=2, β=2)

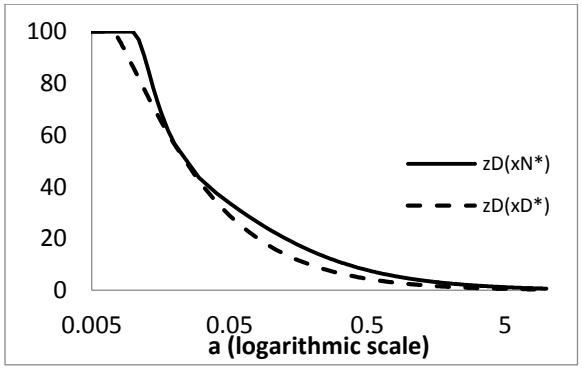

Figure 3. 41 Optimum objective values as a function of a for non-deterrence and deterrence models where $P_s$is exponential (L=100 and α=2, β=2)

We now compare how the models with and without deterrence perform with regard to the loss *L*. For small values of *L*, both models choose zero investment in security, so that $x^*_N = x^*_D = 0$. As *L* becomes larger, the model without deterrence eventually begins spending too much, as

shown in Fig. 3.42. Therefore, as shown in Fig. 3.43, the target-oriented utility model always results in a better objective-function value.

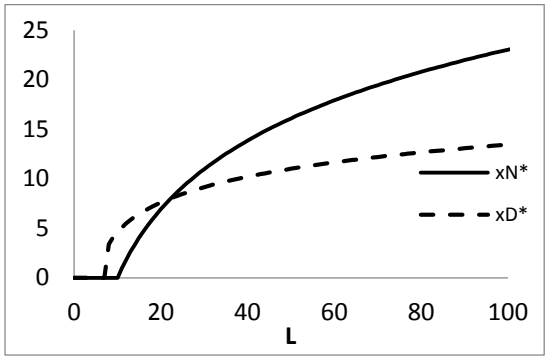

Figure 3. 42 Optimum investment as a function of the loss L from a successful attack for non-deterrence and deterrence models (a=0.1 and α=2,β=2)

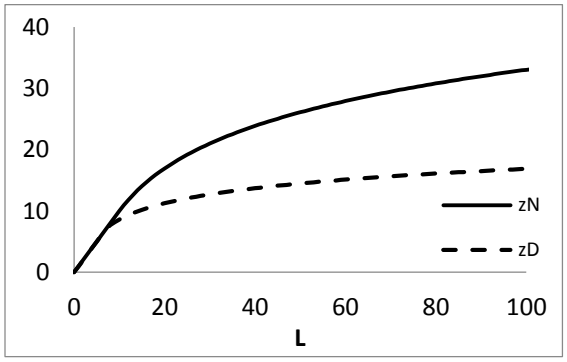

Figure 3. 43 Value of objective function as a function of the loss L from a successful attack for non-deterrence and deterrence models (a=0.1 and α=2,β=2)

3.5 Probability of Deterrence as a Function of Both Loss and Attack Success Probability

In our initial model, we assumed that the probability of deterrence was a function only of the investment level. Then, we modified our model to allow the probability of deterrence to be a function of the success probability of an attack. However, these are not the only factors that may influence the probability of deterrence. In particular, an attacker may be more easily deterred from an attack on a low-valued target. Therefore, we now modify the previous model to allow the probability of deterrence to be a function of both the loss *L* and the success probability of an attack. This is realistic, since the attacker may be much more motivated to launch an attack when the consequences of a successful attack would be severe, and hence, it may be more difficult to deter an attack when the loss *L* from a successful attack is high.

In this section, we assume that the deterrence function follows a Rayleigh distribution (instead of Kumaraswamy distribution), since the Kumaraswamy distribution is defined over a [0, 1] range, but the loss may take on arbitrarily large values. The new model formulation is as follows:

$$Z = min\ L\left[1 - P_d\left(P_s(x)\right)\right]P_s(x) + x \tag{3.38}$$

where

$$P_d\left(P_s(x)\right) = e^{-\left(\frac{L(P_S(x))^2}{2s^2}\right)} \qquad (Rayleigh) \tag{3.39}$$

$$P_s(x) = e^{-\lambda x} \qquad (exponential) \tag{3.40}$$

$$EL = L[1 - P_d\left(P_s(x)\right)]P_s(x) \tag{3.41}$$

Fig. 3.44 below shows how the optimum level of investment (x^*), the optimal objective value (Z^*), and the expected loss (EL) change as the loss L changes.

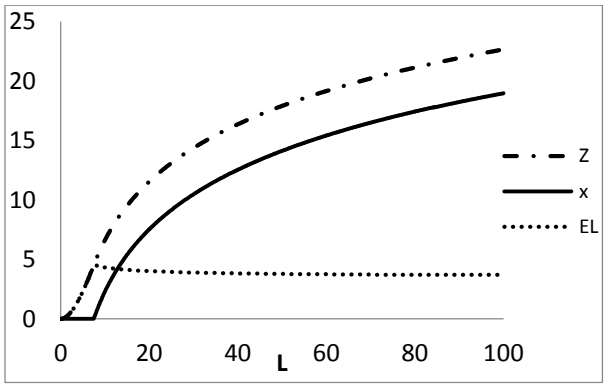

Figure 3. 44 Value of the objective function, optimum investment level, and expected loss *EL* as functions of the loss from an attempted attack (a=0.1, s=2)

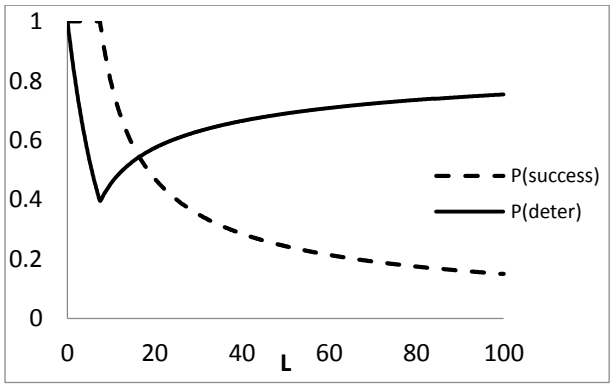

Figure 3. 45 Probability of success and probability of deterrence as a function of the loss from an attempted attack (a=0.1, s=2)

At low levels of the loss L, it is not cost-effective to invest in defense, so the defender chooses zero investment in security. Once L is big enough to justify investing in security, the optimal investment level x^* is increasing in the loss L (see Fig. 3.44). The success probability of an attack is initially 1, and then is decreasing in L. The probability of deterrence is initially decreasing in L, because as L gets larger, the system becomes more attractive to the attacker; however, when the defender starts investing, the probability of deterrence becomes increasing in L (see Fig. 3.45). The objective-function value Z is also increasing in L, due to the increasing investment cost x^*. Note that once the optimal investment level becomes positive, the expected

loss *EL* stays approximately constant. In other words, the defender invests just enough to compensate for the expected loss.

These results indicate that as the target value increases, the defender invests more in protection to reduce the success probability of an attack, and consequently increase the probability of deterrence. Thus, higher-value targets can in general expect to get more protection, pushing attacks down to lower-valued targets. In other words, in a well-functioning system, there should be few attacks on large targets, and more attacks on small targets.

This is consistent with much real-world experience. For example, in Israel, there have been many attacks, but so far no successful attacks against truly critical targets (e.g., the Knesset building). Table 3.1 below shows that no bombing attack in Israel since 2000 has led to more than about 30 fatalities. In other words, Israel has successfully prevented or deterred catastrophic attacks, resulting in attacks with relatively modest (although still tragic) numbers of fatalities.

Year	Number of Bombing Attacks	Number of Deaths due to Bombing Attacks	Maximum Number of Deaths in Any One Bombing Attack
2000	100	10	2
2001	565	100	21
2002	767	269	30
2003	471	151	23
2004	653	69	32
2005	234	26	7
2006	271	16	11
2007	271	5	3
2008	178	5	1
2009	32	1	1
2010	0	0	0
2011	1	8	8
2012	1	6	6

Table 3.1 Attacks in Israel since 2000 (Source: Israel Ministry of Foreign Affairs)

4 Target-Oriented Utility Model for Interdiction of Transportation Networks

4.1 Problem Definition

In this chapter, we model the optimal placement of detectors (e.g., radiation detectors or chemical sensors) on a transportation network. Here, the usual approach is to minimize the probability of attack non-detection [10] [64]; we will reformulate to minimize the expected loss from an attack (taking into account uncertainty about the attacker's deterrence threshold), plus investment in protection, where the level of investment in sensors (or, equivalently, the magnitude of detection probability) needed to deter an attack is assumed to be uncertain. In order to capture this uncertainty, we assume that the probability of deterrence follows a Kumaraswamy distribution [65]. The defender is assumed to either be successfully deter an attack, or to fail to deter an attack and suffer some expected consequences.

In our problem, we have a directed graph $D\ (N, A)$ with nodes N and arcs A, one attacker, and one defender. The attacker attempts to maximize the probability of reaching the target node (t) starting from an origin node (s) without being detected. If he successfully reaches the target node, there will be a loss (L) for the defender. Thus, the defender allocates her resources to decrease the success probability of the attacker. However, the attacker may give up attacking for some sufficiently low probability of success. Investing in defense of arc (ij) can reduce the probability of the attacker successfully traversing that arc from p_{ij} to q_{ij} , where $p_{ij} > q_{ij}$. The defender decides which arcs to protect in order to minimize the total investment in defense plus the expected loss from attacks (where expected loss is given by the loss L, times the probability of the attacker successfully traversing the network if an attack is attempted, times the probability that the attacker attempts an attack). This problem is a min-max structured bi-level optimization model.

4.2 Problem Formulation

In this section we adapt a model developed by Morton et al. [45], where the attacker wishes to maximize the probability of successfully traversing the network, and the defender tries to minimize this probability by investing in the protection of one or more arcs, subject to a budget constraint. However, in our model we omit the budget constraint, and instead put the cost of defense into the defender's objective function, since our model aims to find optimal level of investment. The notation we use and the resulting model formulation are given below.

Notation:

D (N, A): Directed graph with nodes *N* and arcs *A*

FS (i): Set of arcs leaving node *i*

RS (i): set of arcs entering node *i*

AD: The set of arcs in which the defender can invest

L: Loss after a successful attack

d_{ij}: Cost of protecting arc (*i*,*j*)

p_{ij}: Probability that the attacker can traverse arc (*i*,*j*) if it is not protected

q_{ij}: Probability that the attacker can traverse arc (*i*,*j*) if it is protected

x_{ij}: Defender's decision variable, which is 1 if the defender protects arc (*i*,*j*), and 0 otherwise.

y_{ij}: Probability that the attacker reaches node *i* and the chosen path includes arc *(i,j)*

α, β: Shape parameters of the Kumaraswamy distribution

Model formulation:

$$\min \; L\big[1 - P_d\big(Q(x)\big)\big]Q(x) + \sum_{(i,j)\in AD} c_{ij}\, x_{ij} \tag{4.1}$$

$$P_d\big(Q(x)\big) = (1 - y_t^{\alpha})^{\beta} \tag{4.2}$$

$$Q(x) = \max y_t \tag{4.3}$$

$$\sum_{(s,j)\in FS(s)} (y_{sj}) = 1 \tag{4.4}$$

$$\sum_{(i,j)\in FS(i)} (y_{ij}) - \sum_{(k,i)\in RS(i)} [p_{ki} y_{ki}\,(1 - x_{ki}) + q_{ki} y_{ki} x_{ki}] = 0 \quad for\ i \in N\backslash\{s,t\} \tag{4.5}$$

$$y_t = \sum_{(i,j)\in RS(t)} [p_{jt} y_{jt}(1 - x_{ji}) + q_{jt} y_{ji} x_{jt}] \tag{4.6}$$

$$x_{ij} \in \{0,1\} \qquad y_{ij} \geq 0$$

The defender's objective function (4.1) is the expected loss from attacks, plus the total defensive investment. Equation (4.2) calculates the probability of deterrence, which is a function of the attack success probability (y_t). Constraint (4.4) forces the attacker to choose one arc out of the source node (*s*). Constraint (4.5) enforces conservation of flow. Here, the success probability of reaching node *k* times the probability of successfully traversing arc (*k,i*), summed over all *k*, must equal the probability of reaching node *i*, which can be written as the sum over *j* of the probability of reaching node *i* and choosing arc (*i,j*). Constraint (4.6) calculates the probability of reaching the target node (*t*).

In order to linearize constraint (4.5), we introduce the following variables and reformulate our model as in [45]:

$$y'_{ij} = y_{ij}(1 - x_{ji}) \tag{4.7}$$

$$z'_{ij} = y_{ij} x_{ji} \tag{4.8}$$

This ensures that y'_{ij} can be non-zero only if arc (*i,j*) is not protected, z'_{ij} will be non-zero only if arc (*i,j*) is protected. The new formulation is as follows:

$\max y_t$

$$\sum_{(s,j)\in FS(s)} (y'_{sj} + z'_{sj}) = 1 \quad (4.9)$$

$$\sum_{(i,j)\in FS(i)} (y'_{ij} + z'_{ij}) - \sum_{(k,i)\in RS(i)} (p_{ki}y'_{ki} + q_{ki}z'_{ki}) = 0 \quad for\ i \in N\backslash\{s,t\} \quad (4.10)$$

$$y_t = \sum_{(i,j)\in RS(t)} (p_{jt}y'_{jt} + q_{jt}z'_{jt}) \quad (4.11)$$

$$0 \le y'_{ij} \le 1 - x_{ij} \qquad for\ (i,j) \in A \quad (4.12)$$

$$0 \le z'_{ij} \qquad for\ (i,j) \in AD \quad (4.13)$$

$x_{ij} \in \{0,1\} \quad y'_{ij} \ge 0 \quad z'_{ij} \ge 0$

Note that no upper bound is needed on z'_{ij} in constraint (4.13): The fact that $p_{ij} > q_{ij}$ will ensure that z'_{ij} will equal 0 except when y'_{ij} is enforced to equal zero because $x_{ij} = 1$.

4.3 Solution Approach

In this section, we solve the optimization problem given in the previous section. Since this problem is a min-max structured bi-level optimization model, and cannot be solved with standard mixed-integer programming methods, we used the duality approach as in Morton [45] to solve the problem. We have taken the dual of inner problem to get a min-min problem. The resulting new formulation is as follows:

$$\min L\left[1 - (1 - \omega_s^{\alpha})^{\beta}\right]\omega_s + \sum_{(i,j)\in AD} c_{ij}\, x_{ij} \quad (4.14)$$

$$\min \omega_s + \sum_{(i,j)\in AD} \lambda_{ij}(1 - x_{ij}) \quad (4.15)$$

$$\omega_i - p_{ij}\omega_j \ge 0 \qquad for\ (i,j) \in A\backslash AD \quad (4.16)$$

$$\omega_i - p_{ij}\omega_j + \lambda_{ij} \ge 0 \qquad for\ (i,j) \in AD \quad (4.17)$$

$$\omega_i - q_{ij}\omega_j \ge 0 \qquad for\ (i,j) \in AD \quad (4.18)$$

$$\lambda_{ij} \ge 0 \qquad for\ (i,j) \in AD \quad (4.19)$$

$\omega_t = 1$

where ω_i and λ_{ij} are dual variables. Here, the dual variables ω_i is the probability of the attacker traveling from node i to node t without being detected, given that he has already reached node i. The attacker's model finds a maximum reliability-path.

However, both the defender's and the attacker's objective are nonlinear. In order to linearize the attacker's objective function, Morton [45] introduced a new variable σ and $\lambda_{ij}(1 - x_{ij})$ replaced by σ. Also, to make sure that $\lambda_{ij}(1 - x_{ij}) = \sigma$, the constraint $-\lambda_{ij} \geq -\sigma_{ij} - x_{ij}$ is added to the problem formulation. The new formulation of the inner problem is given below.

$$\min \omega_s + \sum_{(i,j)\in AD} \sigma_{ij} \tag{4.20}$$

$$\omega_i - p_{ij}\omega_j \geq 0 \qquad for\ (i,j) \in A \backslash AD \tag{4.21}$$

$$\omega_i - p_{ij}\omega_j \geq -\lambda_{ij} \qquad for\ (i,j) \in AD \tag{4.22}$$

$$-\lambda_{ij} \geq -\sigma_{ij} - x_{ij} \qquad for\ (i,j) \in AD \tag{4.23}$$

$$\omega_i - q_{ij}\omega_j \geq 0 \qquad for\ (i,j) \in AD \tag{4.24}$$

$$\lambda_{ij} \geq 0 \qquad for\ (i,j) \in AD \tag{4.25}$$

$$\omega_t = 1 \tag{4.26}$$

Claim1: Inequalities 4.22 and 4.23 can be written as one inequality $\omega_i - p_{ij}\omega_j \geq -x_{ij}$

Proof: Inequalities 4.22 and 4.23 implies that $\omega_i - p_{ij}\omega_j \geq -\lambda_{ij} \geq -\sigma_{ij} - x_{ij}$ is true. Also, we know that we don't have anywhere else λ_{ij} in the model. Thus, λ_{ij} can take any values in $\omega_i - p_{ij}\omega_j \geq -\lambda_{ij} \geq -\sigma_{ij} - x_{ij}$ and we can write inequality $\omega_i - p_{ij}\omega_j \geq -\sigma_{ij} - x_{ij}$.

Claim 2: We can optimally find that $\sigma_{ij}$is zero.

Proof: In our new inequality $\omega_i - p_{ij}\omega_j \geq -\sigma_{ij} - x_{ij}$, if we take $\sigma_{ij} = 0$ it will be

$\omega_i - p_{ij}\omega_j \geq -x_{ij}$. For $x_{ij} = 1$,this is always true because $0 < \omega_i, p_{ij}, \omega_j < 1$. For $x_{ij} = 0$, we can still find feasible solution, since $p_{ij} < 1$.

We use piecewise linear approximation method introduced by Sherali [66] to linearize defender's objective function. Sherali [66] uses disaggregated convex combination weights λ_n and μ_n for the left and right points of the *n* segment of the objective function. The resulting formulation of the defender's objective function is as follows:

$$\min L \sum_{n=0}^{r} [f(a_n)\lambda_n + f(a_{n+1})\mu_n] + \sum_{(i,j)\in AD} c_{ij}\, x_{ij} \tag{4.27}$$

$$\omega_s = \sum_{k=0}^{r} (a_n\lambda_n + a_{n+1}\mu_n) \tag{4.28}$$

$$\lambda_n + \mu_n = \alpha_n \qquad for\ n = 1 \dots r \tag{4.29}$$

$$\sum_{n=1}^{r} \alpha_n = 1 \tag{4.30}$$

$$\lambda_n, \mu_n \geq 0 \qquad for\ n = 1 \dots r \tag{4.31}$$

$$\alpha_n \in \{0,1\} \quad x_{ij} \in \{0,1\}$$

Finally, since the function $\left[1 - (1 - \omega_s^{\alpha})^{\beta}\right]\omega_s$ is monotone increasing for positive α and β values, we can reformulate our problem as a mixed-integer optimization model that can be solved by commercial solvers (we solved the resulting non-nested problem using CPLEX). The final model is as follows:

$$\min L \sum_{k=0}^{r} [f(a_k)\lambda_k + f(a_{k+1})\mu_k] + \sum_{(i,j)\in AD} c_{ij}\, x_{ij} \tag{4.32}$$

$$\omega_i - p_{ij}\omega_j \geq 0 \qquad for\ (i,j) \in A \backslash AD \tag{4.33}$$

$$\omega_i - p_{ij}\omega_j \geq -x_{ij} \qquad for\ (i,j) \in AD \tag{4.34}$$

$$\omega_i - q_{ij}\omega_j \geq 0 \qquad for\ (i,j) \in AD \tag{4.35}$$

$$\omega_t = 1 \tag{4.36}$$

$$\omega_s = \sum_{k=0}^{r} (a_k \lambda_k + a_{k+1} \mu_k) \tag{4.37}$$

$$\lambda_k + \mu_k = \alpha_k \qquad for\ k = 1 \dots r \tag{4.38}$$

$$\sum_{k=1}^{r} \alpha_k = 1 \tag{4.39}$$

$$\lambda_k, \mu_k \geq 0 \qquad for\ k = 1 \dots r \tag{4.40}$$

$\alpha_k \in \{0,1\}$ $x_{ij} \in \{0,1\}$ $\omega_i > 0$

4.4 Computational Results

In this section, we present our results for two real-world transportation networks of different sizes in California (Lancaster-Palmdale, with 214 arcs and 73 nodes; and Northridge, with 374 arcs and 121 nodes). For each network, we choose 10 entering nodes (allowing the attacker to choose the most favorable one) and a single target node. In our analysis, we explore the effect of the shape parameters of the deterrence function (α and β), the success probabilities of attacks on arcs that are not protected (p_{ij}), the effectiveness of defensive investment (as measured by the ratio $\frac{q_{ij}}{p_{ij}}$), the target value (L), and the cost of protecting an arc (c_{ij}).

The arc success probabilities are chosen randomly rather than deterministically. Therefore, we use Monte Carlo simulation to study the effect of different possible distributions for the arc success probabilities. We conduct enough simulations to estimate the expected value of the attacker's overall success probability with an absolute error of no more than 0.02 at a 95% confidence level. For most cases, 1000 runs were enough to obtain this level of accuracy, but when this was not true, we conducted additional runs. We also compute the standard error for the optimal number of arcs protected, the optimal value of the defender's objective function, and the deterrence probability.

We use three different uniform distributions for the success probability of traversing an arc when the defender makes no investment (p_{ij}). In particular, our base case is U(0.5, 0.8). We also consider U(0.7, 1) (to explore the effect of a higher mean arc success probability), and U(0.4, 0.9) (to show the effect of a higher variance).

The success probability of traversing an arc when the defender invests in protection of that arc (q_{ij}) depends on the effectiveness of defensive investment. We examine cases where the effectiveness of defensive investment is 90%, 70%, and 30% (i.e., the ratio $\frac{q_{ij}}{p_{ij}}$ takes on values of 0.1, 0.3, and 0.7, respectively).

Of course, different types of sensors with different levels of sensitivity will involve different costs [1] [67]. The cost of a sensor also varies depending on the type of threat they detect (chemical, explosive, radiation etc.). For example, California and New Jersey have radiation detection devices called Adaptable Radiation Area Monitors (ARAM) which costs about $200,000 [68]. Although we don't know the cost, another example is, in California, explosive detection devices are installed to truck weigh stations which can detect explosive and chemical threats [69].Yates and Sanjeevi [9] studied a model of critical infrastructure protection. In experimental results of their model, they assume that each sensor costs for $200. Wein and Atkinson [67] studied a model of detection-interdiction systems to protect cities from nuclear terrorist attacks. They claim that, a radiation sensor would cost $50,000/year (including operation and maintenance cost). For convenience, we begin our analysis using values of $10K and $50K for the cost c_{ij} of protecting arc (ij), which give reasonable results for the sizes of networks we have studied based on our initial runs. In this study, we also use a wide range of target values ($10 million, $100 million, and $1000 million) to show how the target value affects the defender's optimal solution.

We originally planned to examine five cases for the shape parameters of the deterrence function: ($\alpha=2$, $\beta=2$); ($\alpha=2$, $\beta=10$); ($\alpha=10$, $\beta=2$); ($\alpha=0.5$, $\beta=0.5$); and ($\alpha=0.2$, $\beta=0.8$). However, Table 4.1 shows that the case of ($\alpha=10$, $\beta=2$) is not interesting, since even with no investment in protection, the deterrence probability is almost 1.0. Therefore, we examine only the remaining four cases in our analysis. Note that cases with ($\alpha>1$, $\beta>1$) yield an S-shaped deterrence function, while cases with ($0<\alpha<1$, $0<\beta<1$) give a reverse S-shaped deterrence function.

Distribution	**U(0.5, 0.8)**	**U(0.7, 1)**	**U(0.4, 0.9)**
$P_{success}$ with no protection	0.271585	0.646207	0.2827
P_{deter} with no protection for $\alpha=10,\beta=2$	0.999986	0.965248	0.999942

Table 4.1Success probability of an attack and deterrence probability for the deterrence function with shape parameters $\alpha=10,\beta=2$ with no protection

In our analysis, we solve our MIP problem with the CPLEX solver. We were able to find optimal solutions for our models with piece-wise linear objective function (with 1000 linear segments). We ran the models on a computer with an Intel(R) Core(TM)2 CPU 2.13 GHz processor and 4 GB RAM. The results indicate that the computation time is sensitive to mean of arc success probabilities and defensive effectiveness. In particular, as the mean arc success probability increases, the required computation time also increases. Moreover, as effectiveness of defensive investment is decreases the computation time is increasing. The approximate average computation time for the cases with U(0.5, 0.8) arc success probability and 90% defensive effectiveness is ten hours, and for the cases with U(0.7, 1) arc success probability and 30% defensive effectiveness is 125 hours for 1000 replication.

We present the results for Lancaster-Palmdale network in four subsections. In section 4.4.1 below, we show how the various parameter values affect the number of arcs protected. In particular, we compare the results for different distributions, target values, effectiveness of defense, and protection costs for each set of shape parameters, and then discuss how the shape

parameters of the deterrence function affect the optimal solution. In section 4.4.2, we give a similar discussion for the defender's objective value. In section 4.4.3, we show the sensitivity of overall success probability of an attack to the various parameters. Finally, in section 4.4.4, we present results for the probability of deterrence function. In section 4.4.5, we give a general discussion about the results for Northridge network.

4.4.1 Sensitivity Analysis for Number of Arcs Protected

We begin our analysis by showing the effect of the distribution for the arc success probabilities p_{ij} on the number of arcs protected at optimality. Our results indicate that for a given variance of success probability, the distribution with the higher mean results in a higher number of protected arcs (comparing the dark and light bars in Figures 4.1-4.4), as expected. In each figure, the upper part of the figure reflects a sensor cost of \$10K, and the lower part of the figure reflects a sensor cost of \$50K. Although we have not proven that a higher mean arc success probability can never result in a lower expected number of arcs protected, we suspect that this may be true, and Figures 4.1-4.5 show that this conclusion is valid for each of the 72 comparisons we studied. Moreover, the difference is always larger than the standard error of the results.

We also observe that for a given mean success probability, the distribution with the higher variance usually results in a higher number of protected arcs (comparing the dark and light bars in Figures 4.5-4.8). However, we have one case with the opposite resulted (highlighted with " ↘ " in Figure 4.8). Moreover, in 20 cases (highlighted with dashed lines), the difference between the results for high and low variance is smaller than the standard errors of the results.

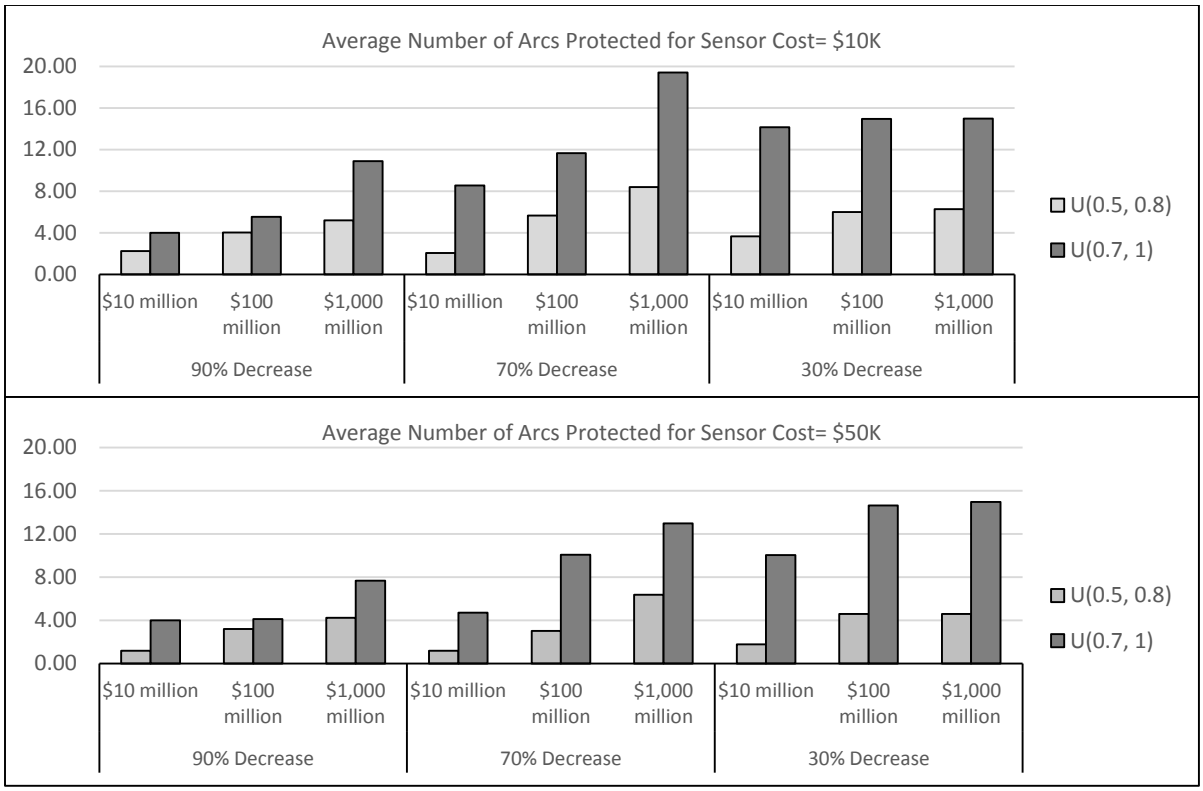

Figure 4.1 Average optimal number of arcs protected for attack success distributions with different means, when deterrence function's shape parameters are (α=2, β=2)

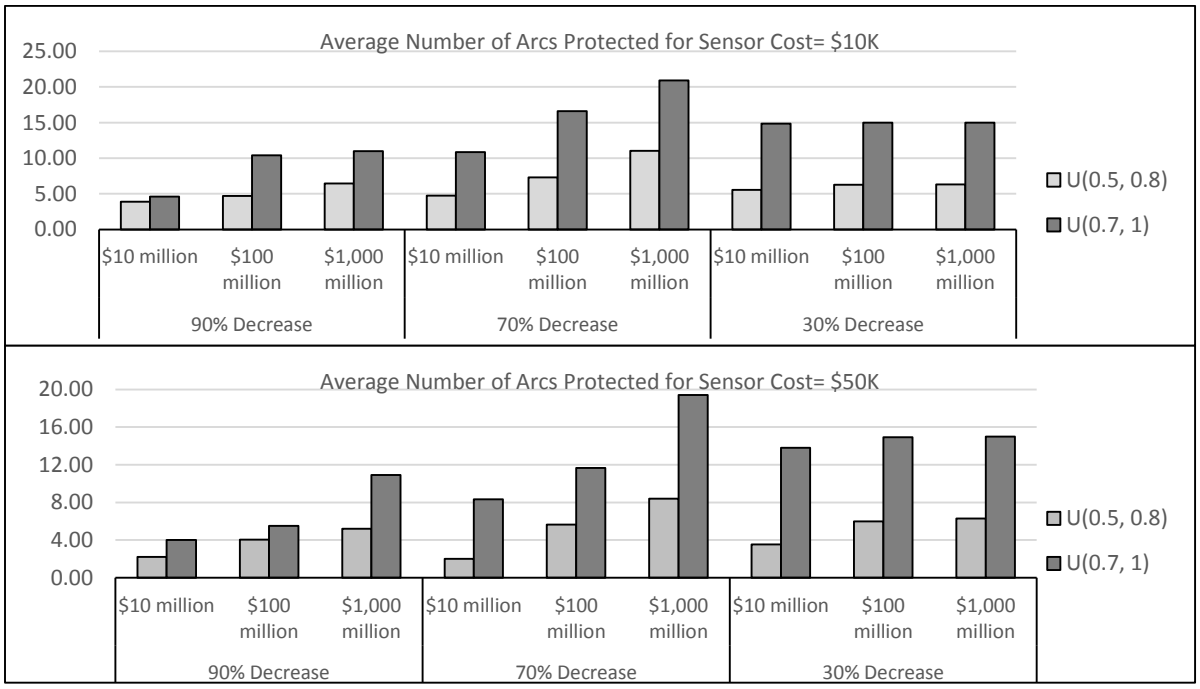

Figure 4.2 Average optimal number of arcs protected for attack success distributions with different means, when deterrence function's shape parameters are (α=2, β=10)

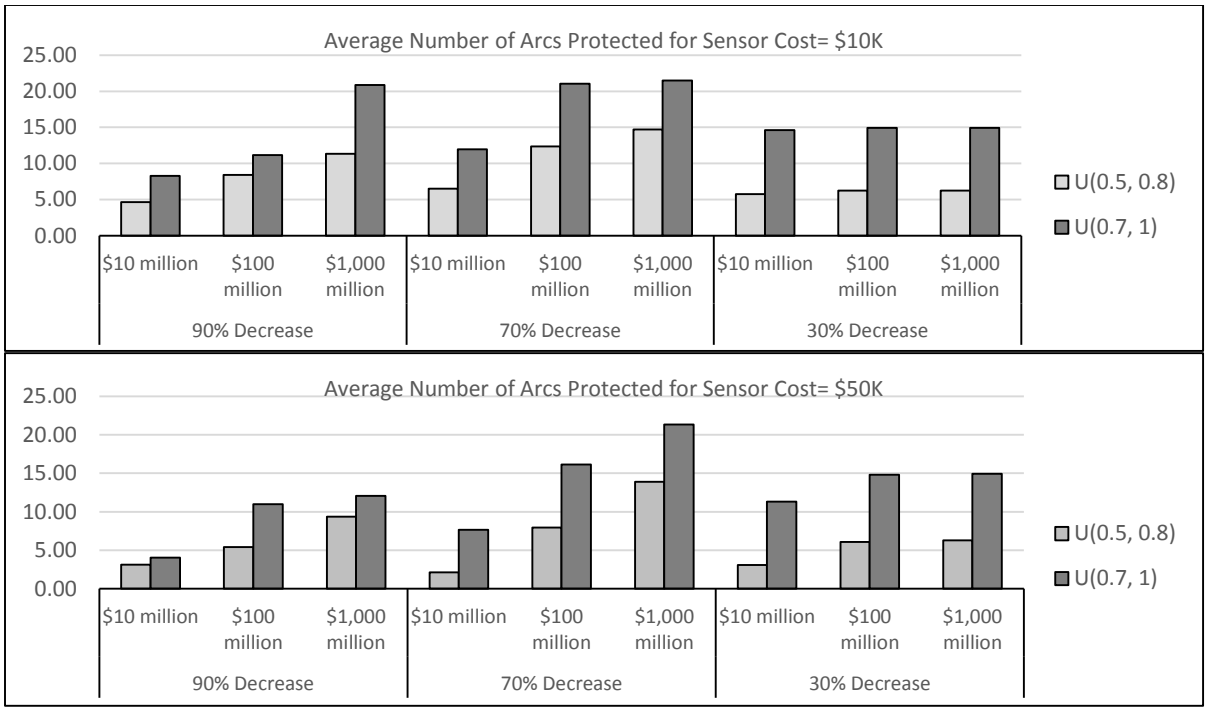

Figure 4.3 Average optimal number of arcs protected for attack success distributions with different means, when deterrence function's shape parameters are (α=0.5, β=0.5)

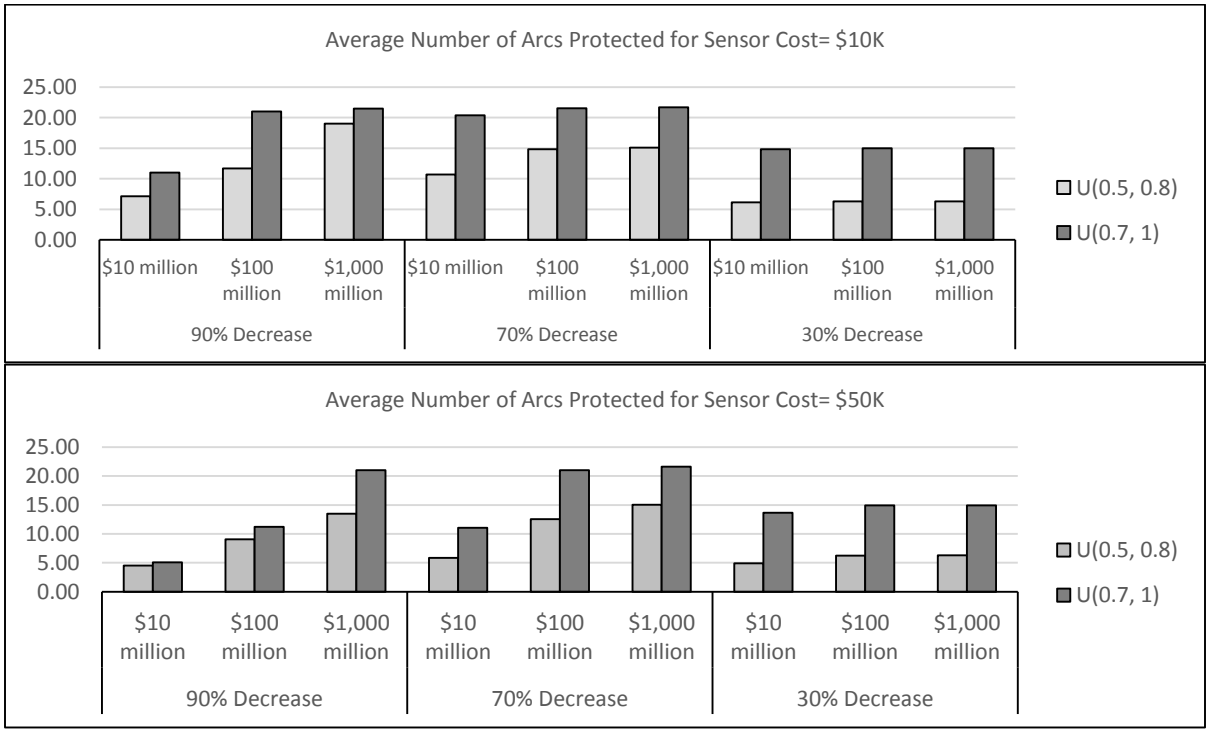

Figure 4.4 Average optimal number of arcs protected for attack success distributions with different means, when deterrence function's shape parameters are (α=0.2, β=0.8)

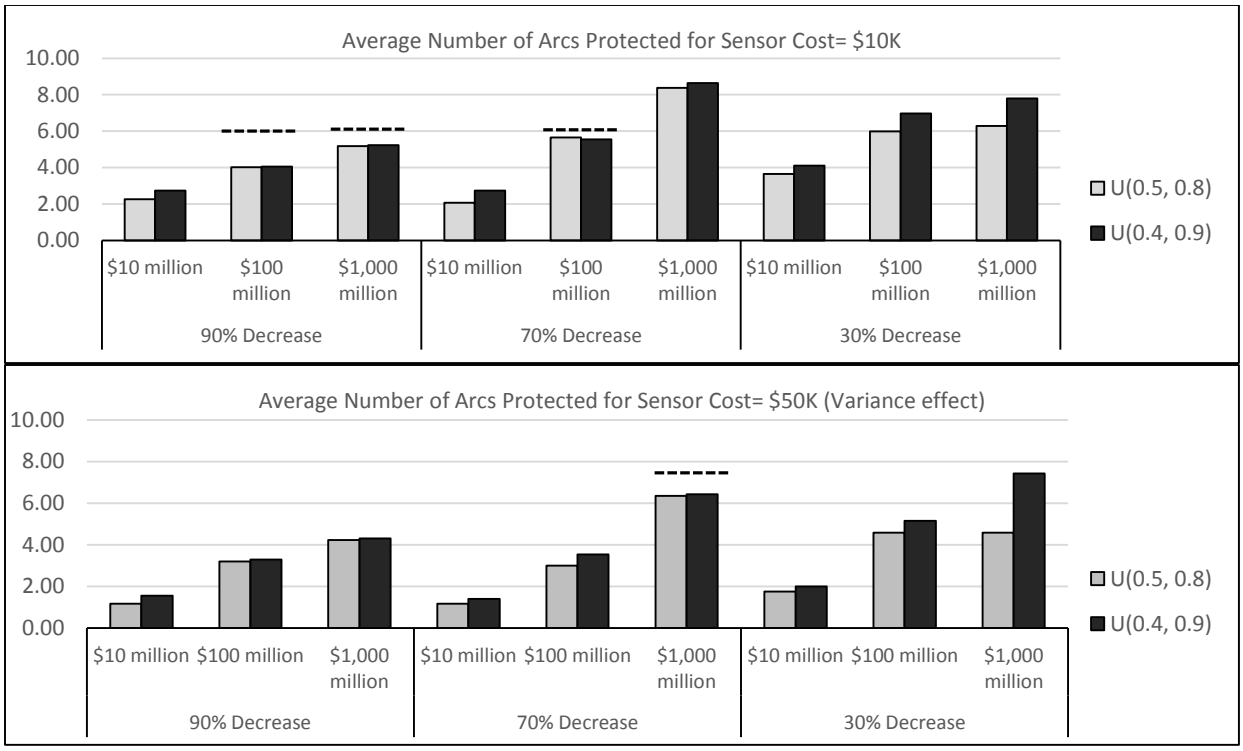

Figure 4.5 Average optimal number of arcs protected for attack success distributions with different variances, when deterrence function's shape parameters are (α=2, β=2)

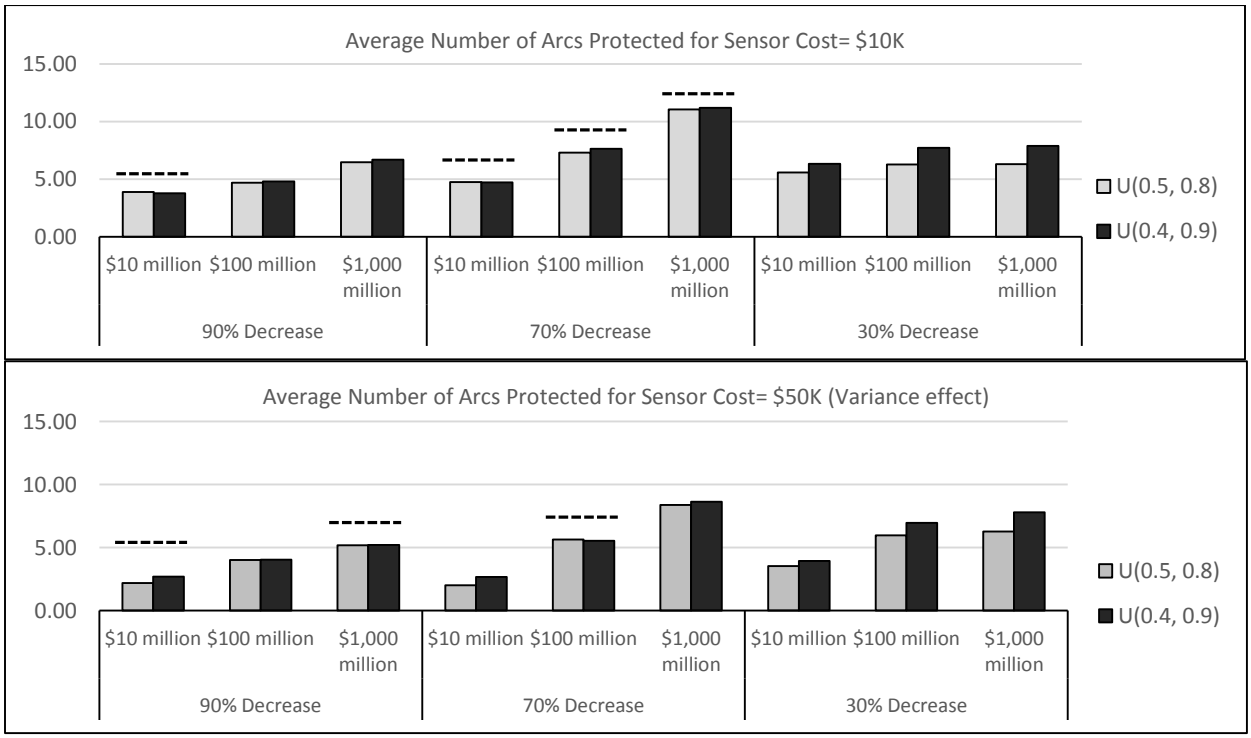

Figure 4.6 Average optimal number of arcs protected for attack success distributions with different variances, when deterrence function's shape parameters are (α=2, β=10)

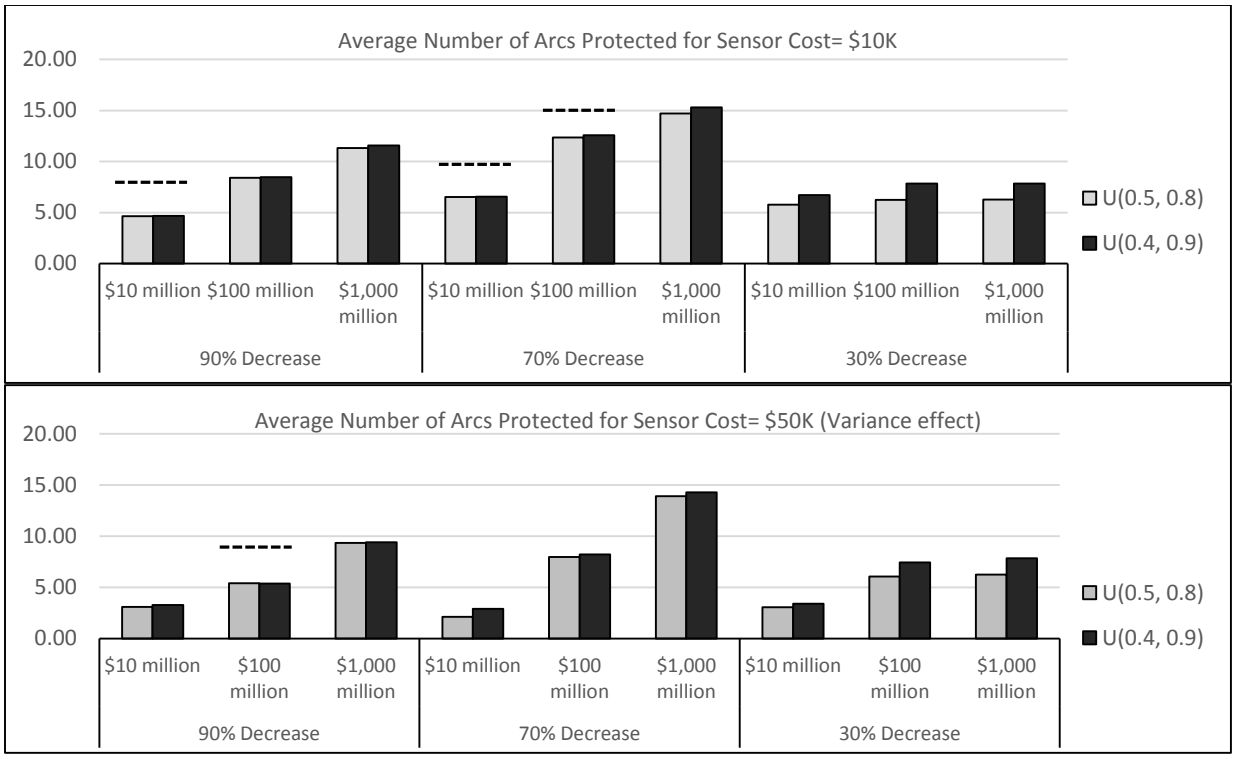

Figure 4.7 Average optimal number of arcs protected for attack success distributions with different variances, when deterrence function's shape parameters are (α=0.5, β=0.5)

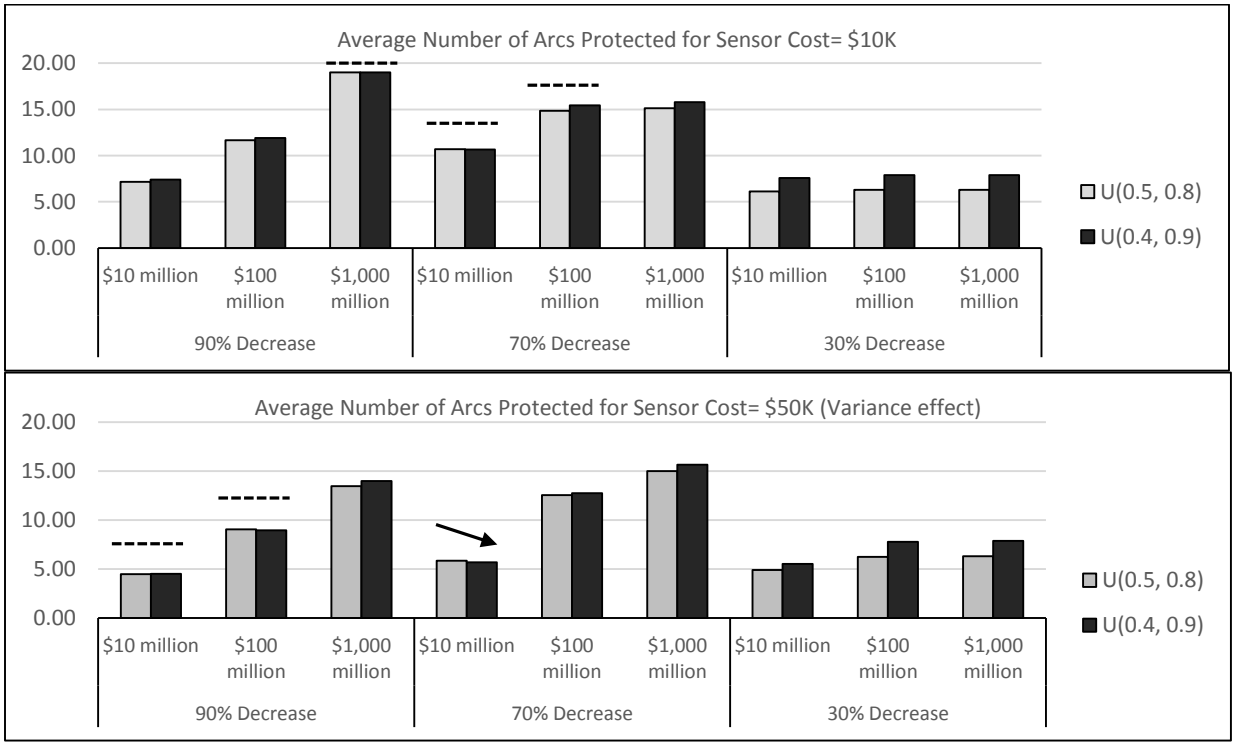

Figure 4.8 Average optimal number of arcs protected for attack success distributions with different variances, when deterrence function's shape parameters are (α=0.2, β=0.8)

The second parameter we examine is the target value L. Figures 4.9-4.11 below highlight the effect of the target value L. For all 72 cases, as the target value increases, the number of arcs that the defender optimally chooses to protect is either increasing or constant, but never decreasing. However, in four of the 72 cases (highlighted with dotted lines "....."), the difference between the high and low value targets is smaller than the standard errors of the results. Also, in 14 of the 72 cases (highlighted with dashed lines "----"), the difference between target values \$100 million and \$1000 million is smaller than the standard error of the results, but the difference between target values \$10 million and \$100 million is larger than the standard error of the results. The difference tends to be small particularly when the effectiveness of defensive investment is only 30%, perhaps because it is then not cost effective to spend more on defense of a higher-valued target. However, this is not always the case; in some cases, the increment in the number of arcs protected for high-valued targets is larger than the standard error of the results even when the effectiveness of defensive investment is small.

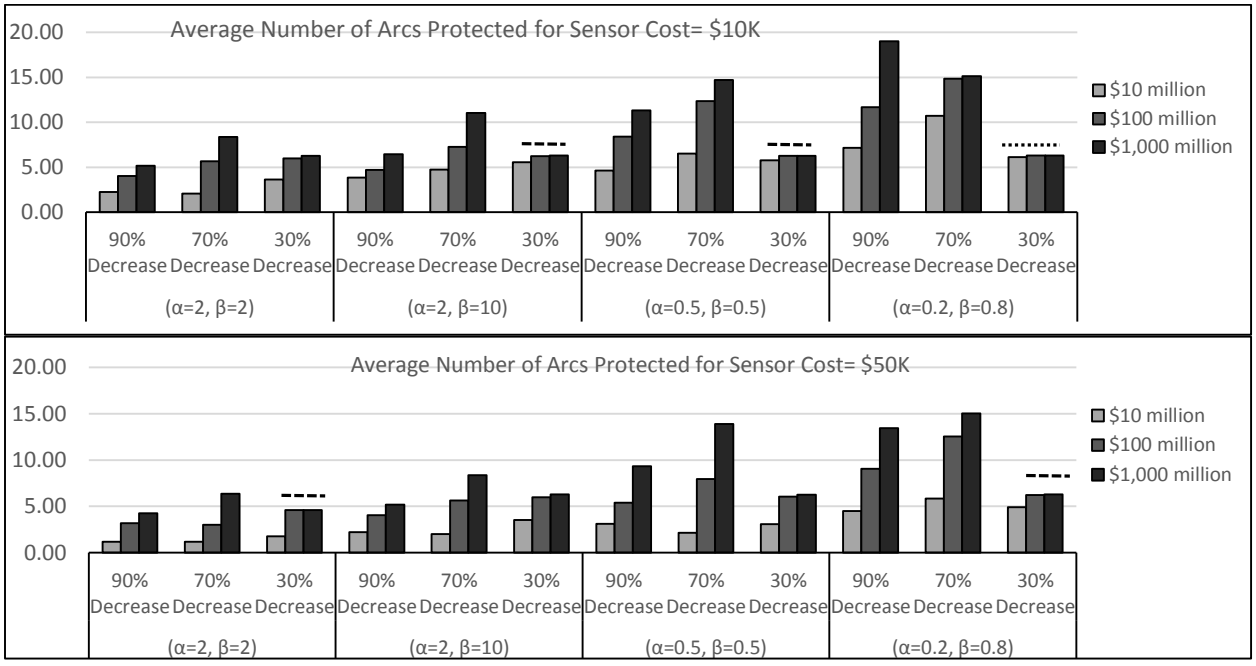

Figure 4.9 Optimal average number of arcs protected for different target values, when p_{ij} is generated from Uniform(0.5, 0.8)

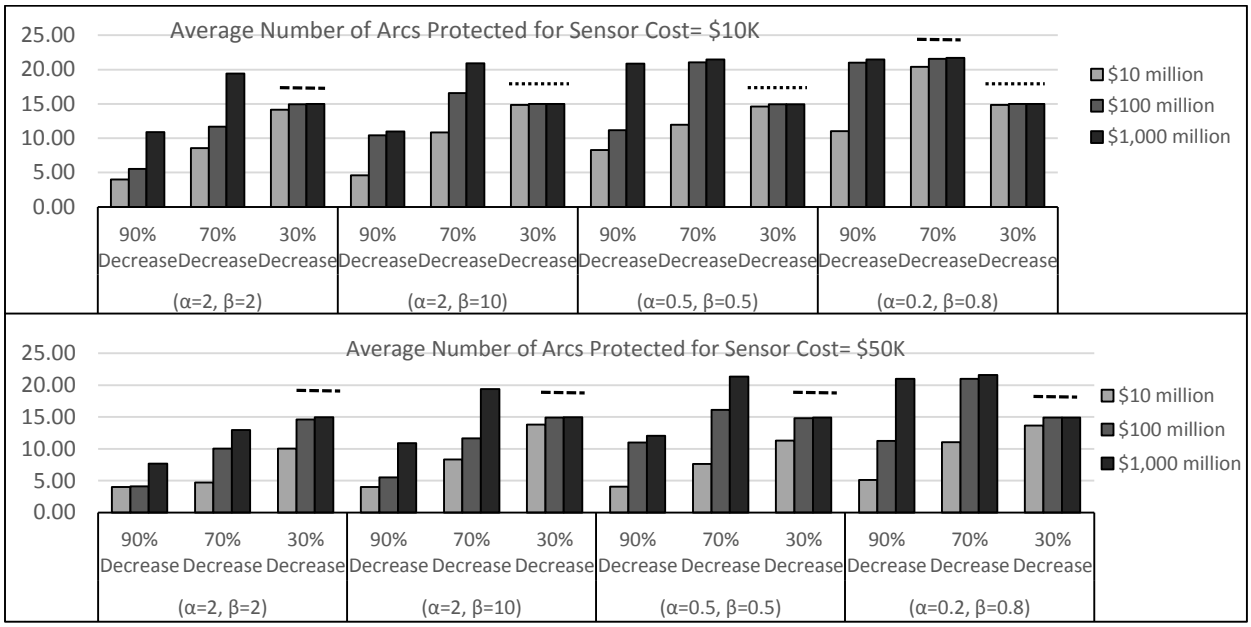

Figure 4.10 Optimal average number of arcs protected for different target values, when p_{ij} is generated from Uniform(0.7, 1)

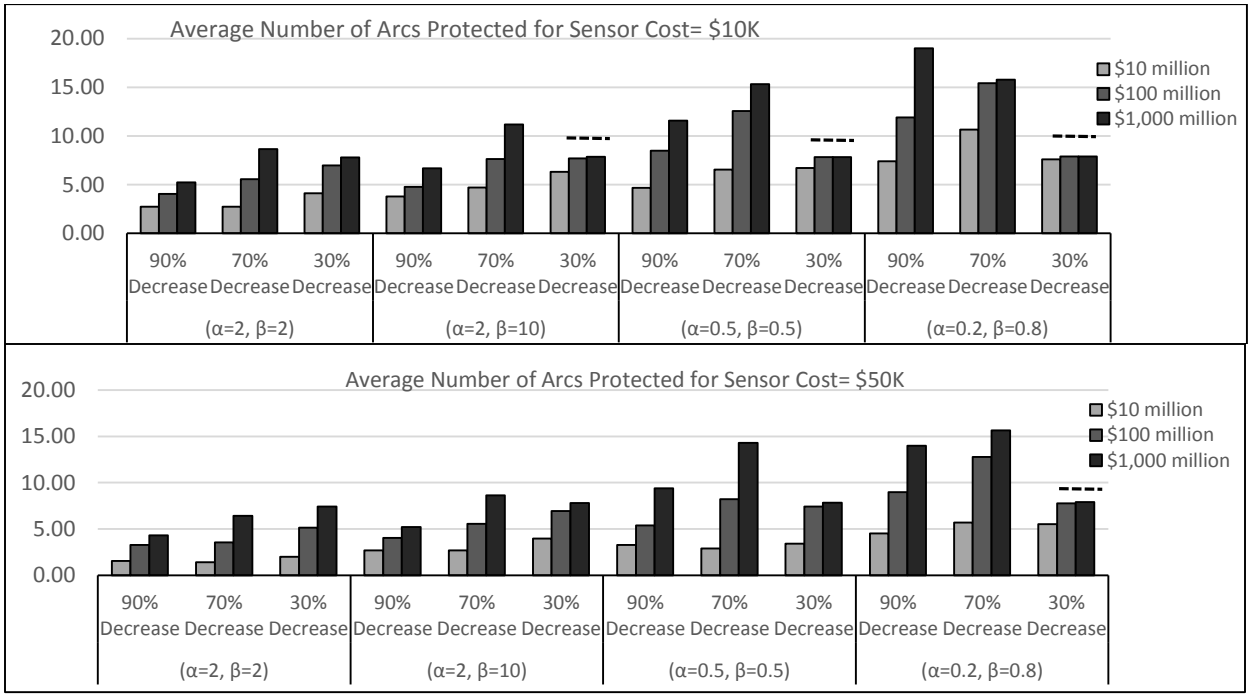

Figure 4.11 Optimal average number of arcs protected for different target values, when p_{ij} is generated from Uniform(0.4, 9)

Another important parameter is the cost of protecting an arc. We present results for this parameter in Figures 4.12-4.15. In each panel, the first two (crossed-hatched) bars show the effects of sensor cost when the success probability is U(0.5, 0.8); the middle two (solid) bars show the

effects of sensor cost when the success probability is U(0.4, 0.9); and the last two (crossed-hatched) bars show the effects of sensor cost when the success probability is U(07, 1). Unsurprisingly, the defender optimally always chooses to protect fewer arcs for higher protection cost (as shown by the dark bars in Figures 4.12-4.15) than for low protection cost (as shown by the light bars). However, in 21 of the 108 cases, the effect of sensor cost is less than the standard errors of the results (as shown by the dotted lines above the vertical bars). As before, most cases in which the difference is small (16 of the 21 cases) occur when the effectiveness of the defense is low (30%).

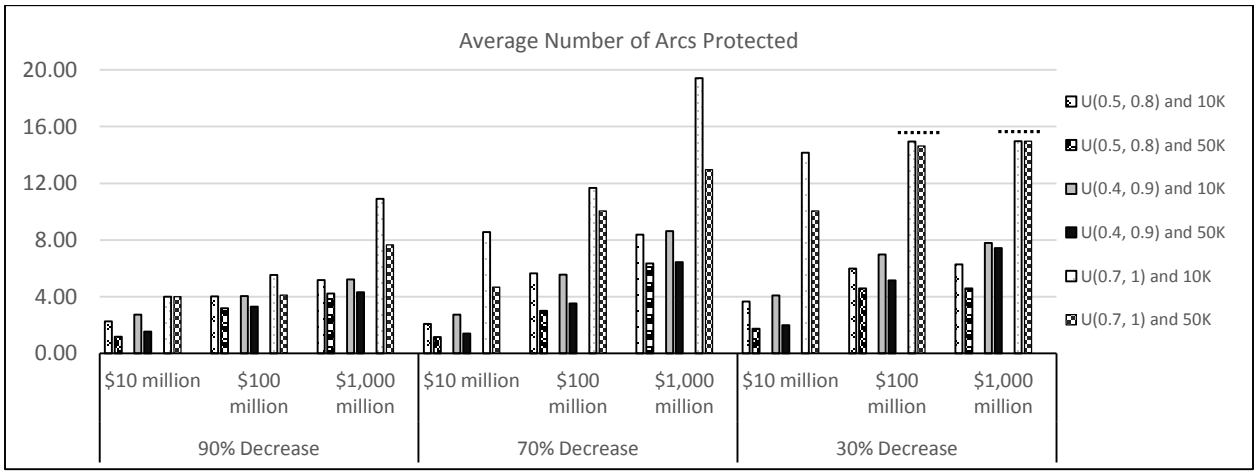

Figure 4.12 Comparison of average optimal number of arcs protected for different sensor costs, when deterrence function's shape parameters are (α=2, β=2)

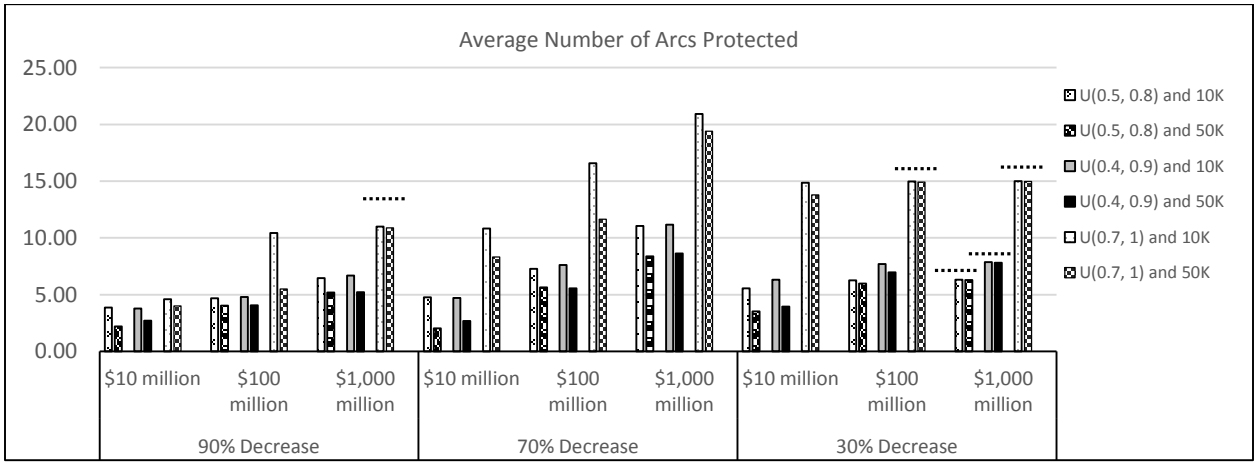

Figure 4.13 Comparison of average optimal number of arcs protected for different sensor costs, when deterrence function's shape parameters are (α=2, β=10)

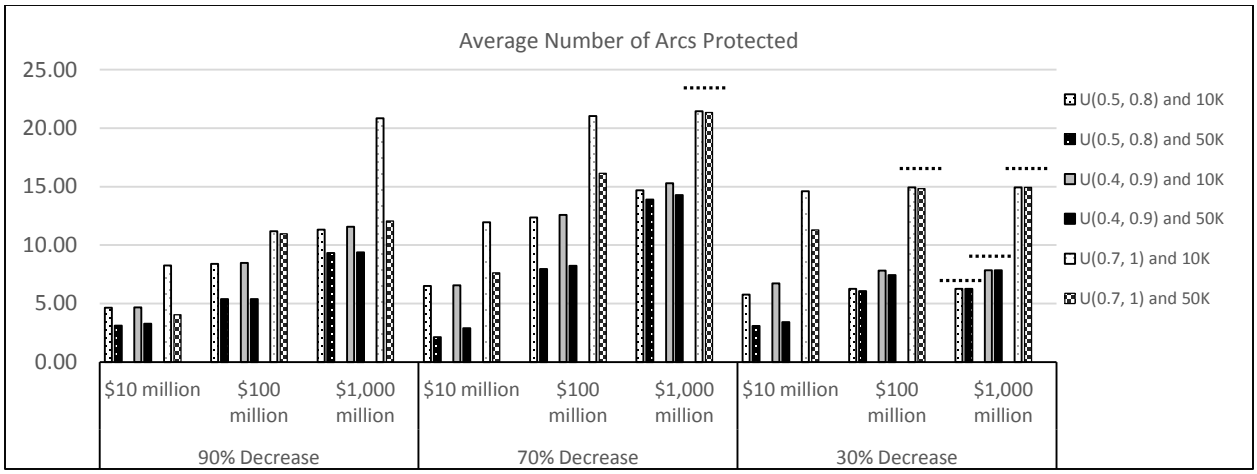

Figure 4.14 Comparison of average optimal number of arcs protected for different sensor costs, when deterrence function's shape parameters are (α=0.5, β=0.5)

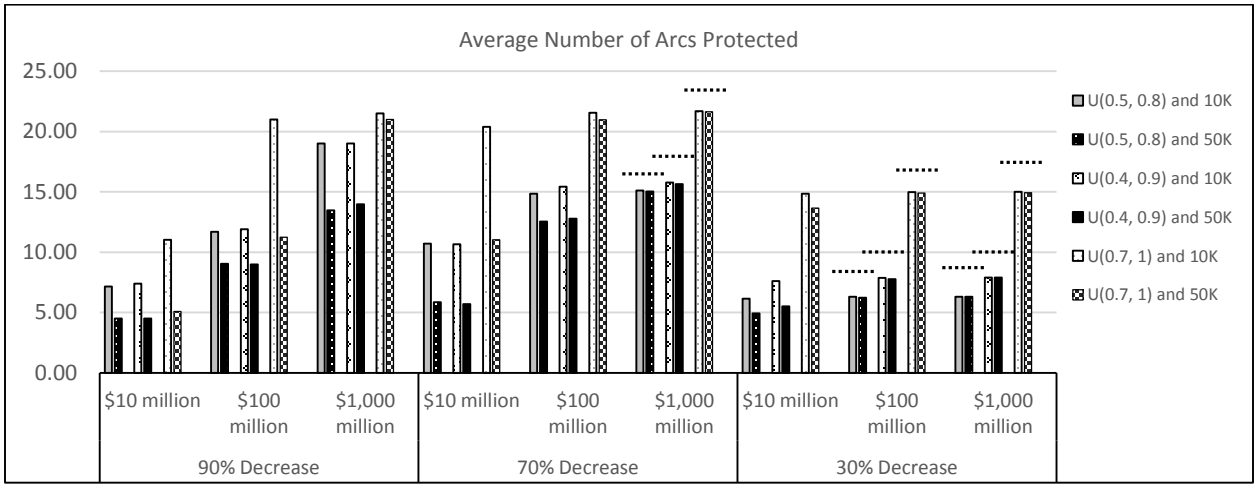

Figure 4.15 Comparison of average optimal number of arcs protected for different sensor costs, when deterrence function's shape parameters are (α=0.2, β=0.8)

The effectiveness of defensive investment clearly also has an important influence on the optimal number of arcs to protect. In Figures 4.16-4.18, we show how the effectiveness of defensive investment affects the number of arcs to protect. In most cases (40 of 72 cases), the optimal number of arcs protected is initially increasing in effectiveness of defensive investment (to compensate for reduced effectiveness of defense), and then decreasing when defense becomes less worthwhile; see the cases labeled with "⌒ " in Figures 4.16-4.18. This is consistent with what we would expect from the literature [28], and from chapter three of this thesis. For 21 of 72 cases (the cases labeled with "↗ " in Figures 4.16-4.18), the number of arcs protected is always

increasing; in two of 72 cases it is always decreasing (the cases labeled with " ↘ " in Figures 4.16-4.18); and in three cases (labeled with "---- "), the difference in the number of arcs protected is smaller than the standard error of results. All of these cases are potentially consistent with the expected pattern of initially increasing, then decreasing.

However, in six of the 72 cases (circled), the number of arcs protected is initially decreasing and then increasing, which contradicts what we expect. Although, the differences are larger than the standard errors of the results, these may be spurious results arising because of the large number of comparisons we performed.

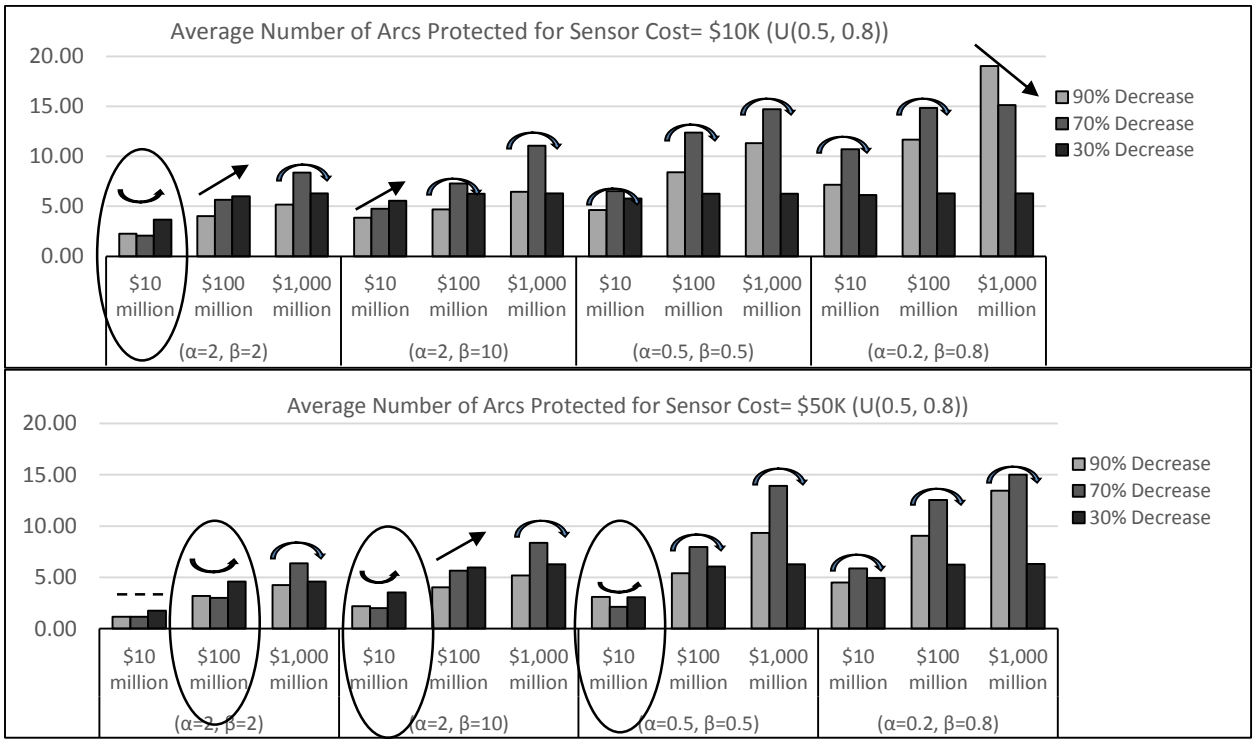

Figure 4.16Optimal average number of arcs protected for different defensive effectiveness values, when p_{ij} is generated from Uniform(0.5, 0.8)

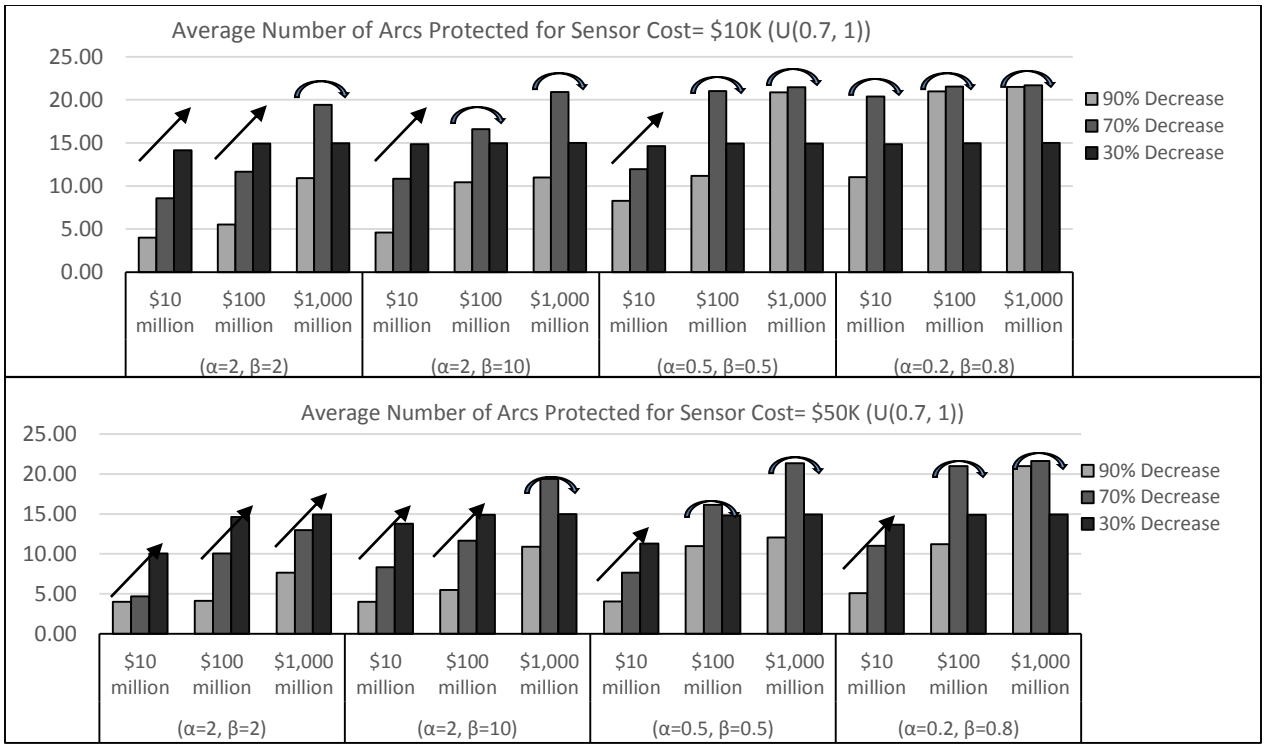

Figure 4.17 Optimal average number of arcs protected for different defensive effectiveness values, when p_{ij} is generated from Uniform(0.7, 1)

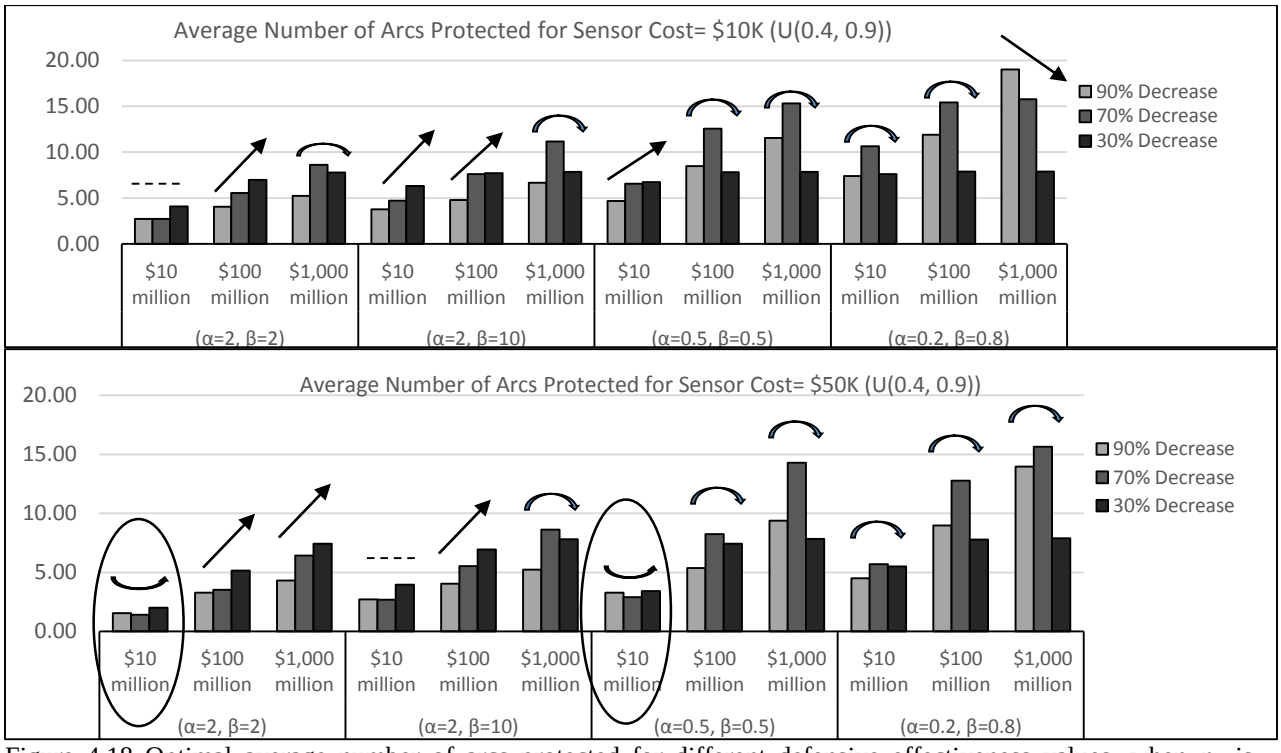

Figure 4.18 Optimal average number of arcs protected for different defensive effectiveness values, when p_{ij} is generated from Uniform(0.4, 0.9)

Finally, we show how the shape of the deterrence function affects the optimal number of protected arcs. For both S-shaped deterrence functions, with ($\alpha>1$, $\beta>1$) and reverse S-shaped deterrence functions, ($0<\alpha<1$, $0<\beta<1$), more arcs need to be protected in increasing β. For example, we can see the increase when moving from left to right within any given set of two solid bars in Figures 4.19-4.21 for S-shaped deterrence functions. The same trend can be also seen in the cross-hatched bars, for reverse S-shaped deterrence functions. In other words, when the attacker can be deterred for even moderately high success probabilities, the defender optimally chooses to protect fewer arcs. The trend never goes in the opposite direction, although in 17 cases, the differences are less than the standard error (as highlighted with dashed lines over the bars in Figures 4.19-4.21). However, this may not always be the case. For example, when the protection cost is large and the effectiveness of defensive investment is small, the defender may optimally choose to protect less when deterrence of an attack is more difficult. We did not find such a case in the above sensitivity analysis. However, we confirmed that this behavior can be observed when the cost of protection is higher ($200K, rather than $10K or $50K). For example, the defender protects more arcs when ($\alpha=2,\beta=2$) than when ($\alpha=2,\beta=10$) for the case where effectiveness of defensive investment is only 10% and the arc success probability is U(0., 1).

In particular, the defender protects more arcs when ($\alpha=2,\beta=2$) than when ($\alpha=2,\beta=10$), if the cost of protection is $200K, the effectiveness of defensive investment is only10%, and the arc success probabilities are distributed U(0.9, 1).

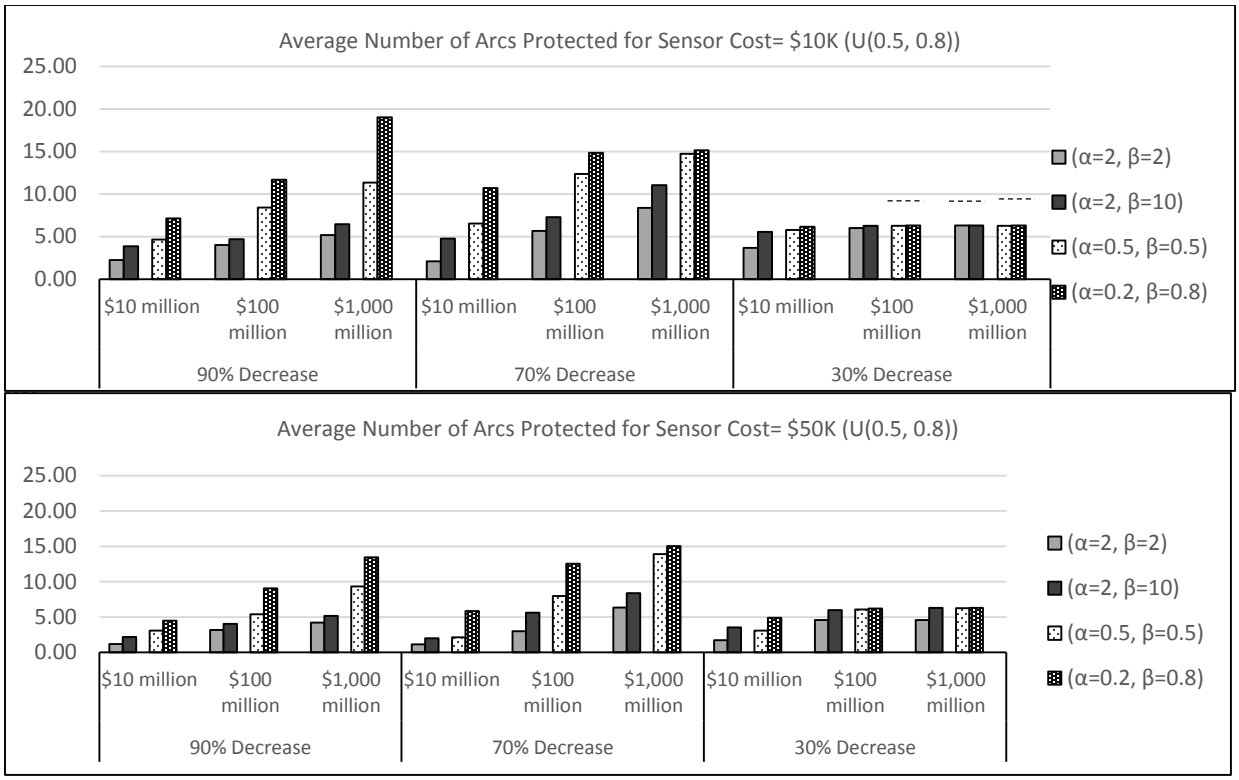

Figure 4.19 Optimal average number of arcs protected for different shape of deterrence function, when p_{ij} is generated from Uniform(0.5, 0.8)

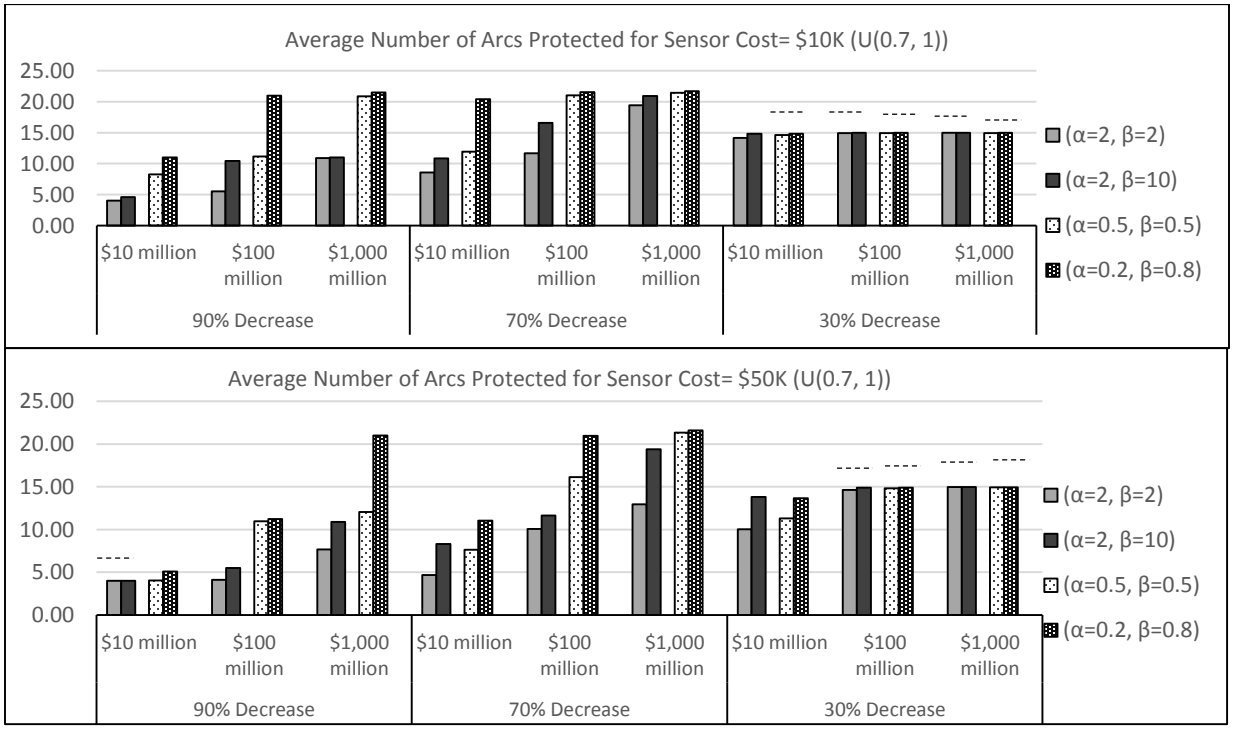

Figure 4.20 Optimal average number of arcs protected for different shape of deterrence function, when p_{ij} is generated from Uniform(0.7, 1)

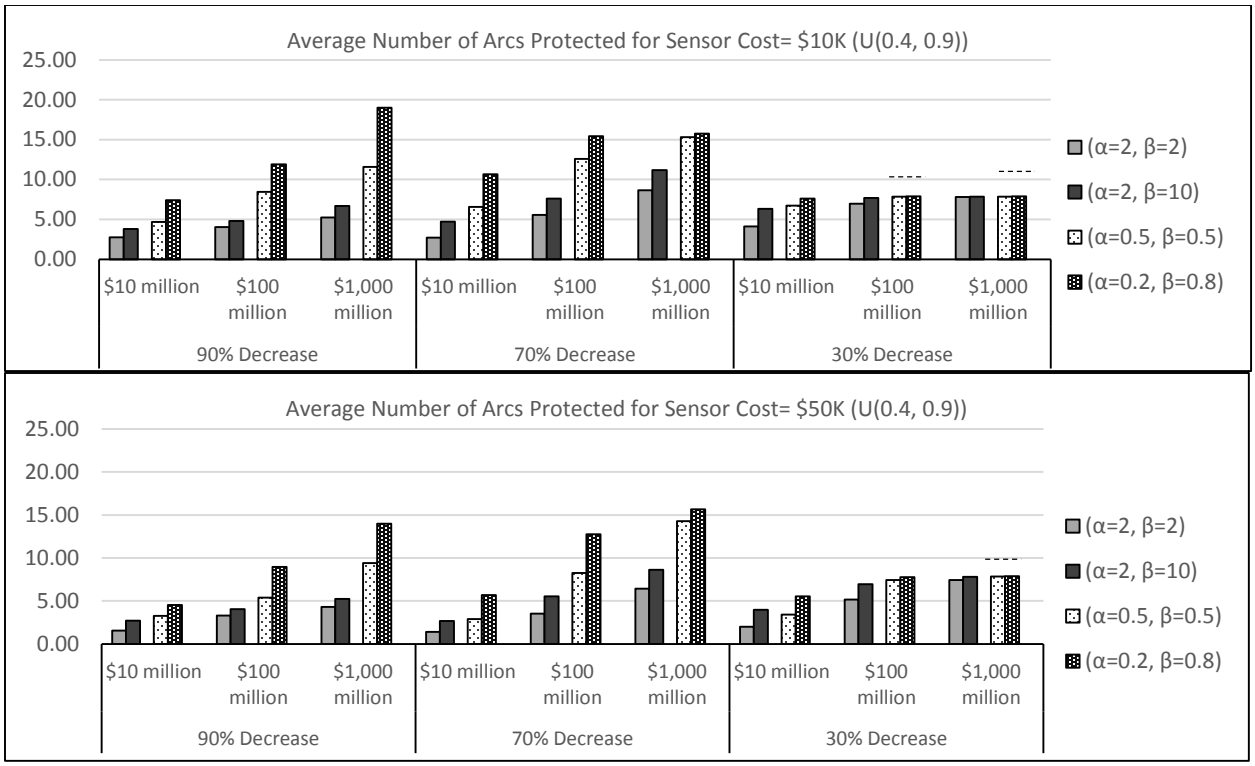

Figure 4.21 Optimal average number of arcs protected for different shape of deterrence function, when p_{ij} is generated from Uniform(0.4, 0.9)

4.4.2 Sensitivity Analysis for the Defender's Optimal Objective Function Value

In this section, we show how the various parameter values affect the optimal objective function value. For a given variance of success probability, the distribution with the higher mean of the arc success probabilities result in a larger (worse) defender objective value (comparing the dark and light bars in Figures 4.22-4.25). As in previous sections, in each figure, the upper part of the figure reflects a sensor cost of \$10K, and the lower part reflects a sensor cost of \$50K. Moreover, the difference is always larger than the standard error of the results. This seems reasonable, since when the mean success probability of an attack on an individual arc is large, the defender must either invest more to reduce the success probability (which increases protection expenditures), or tolerate larger attack success probabilities (and suffer a larger expected loss). In addition, for a given mean success probability, the distribution with higher variance usually results in a larger objective function value (Figures 4.26-4.29). However, in 25 of the 72 cases

(highlighted with dashed lines "- - - " over the bars), the difference between the results for high and low variance is smaller than the standard error of the results.

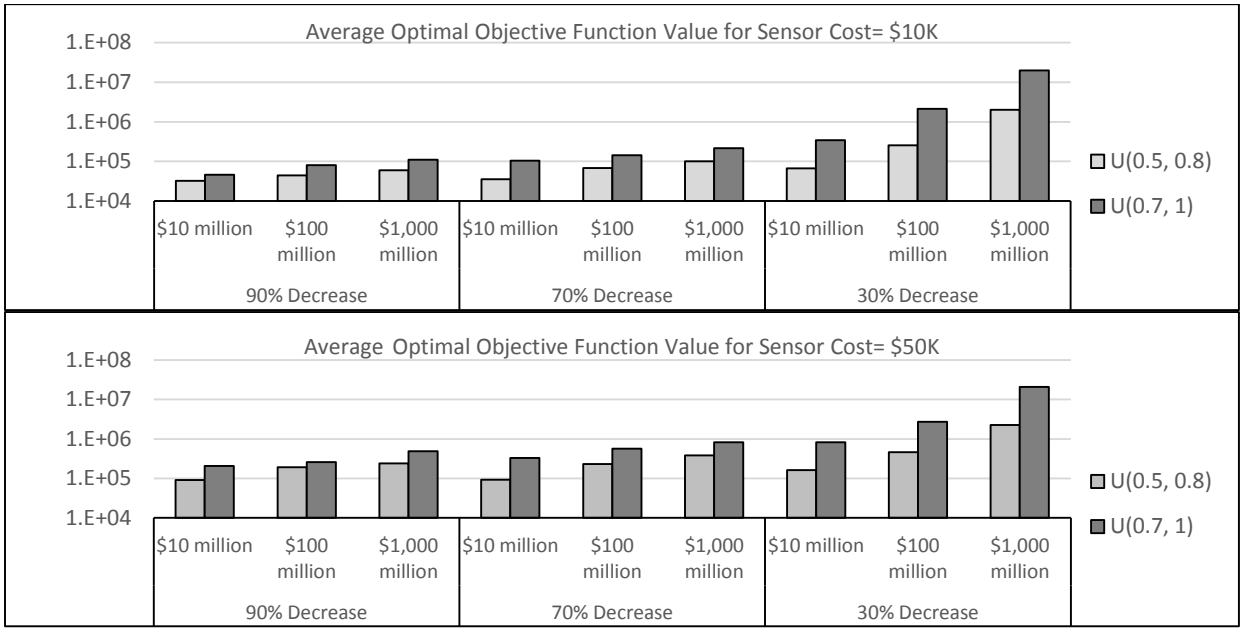

Figure 4.22 The defender's optimal objective function value (log-scale) for different types of distributions with different means, when deterrence function's shape parameters are (α=2, β=2)

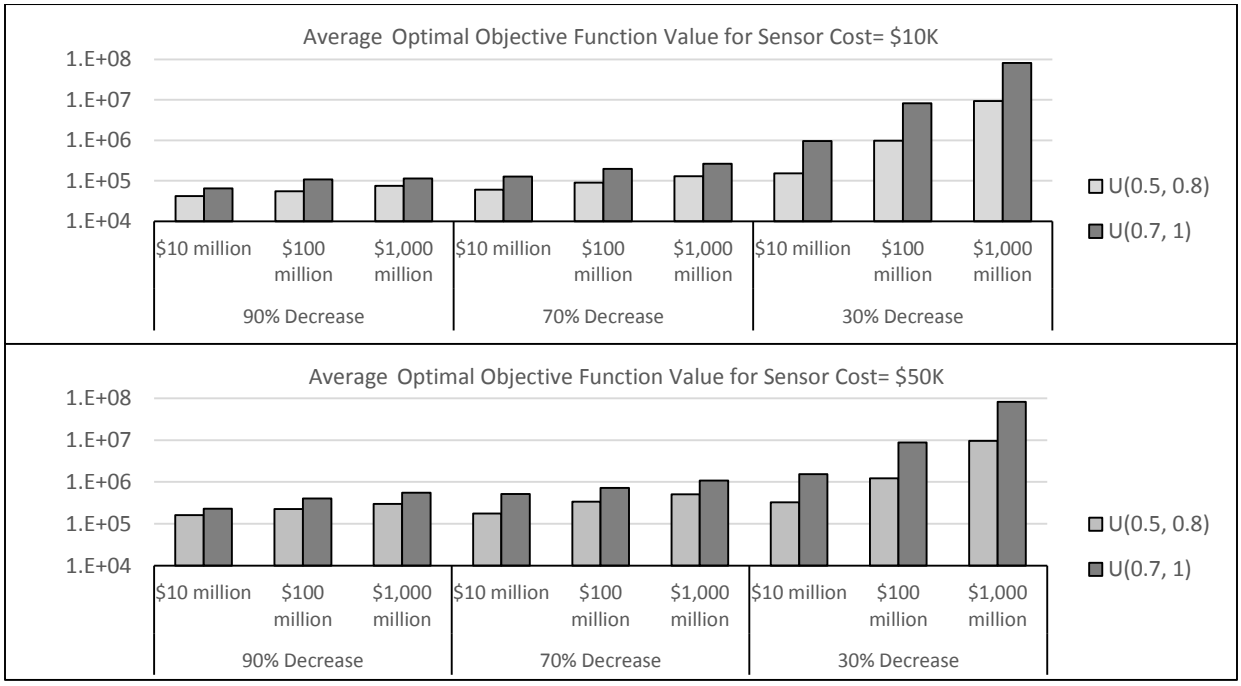

Figure 4.23 The defender's optimal objective function value (log-scale) for different types of distributions with different means, when deterrence function's shape parameters are (α=2, β=10)

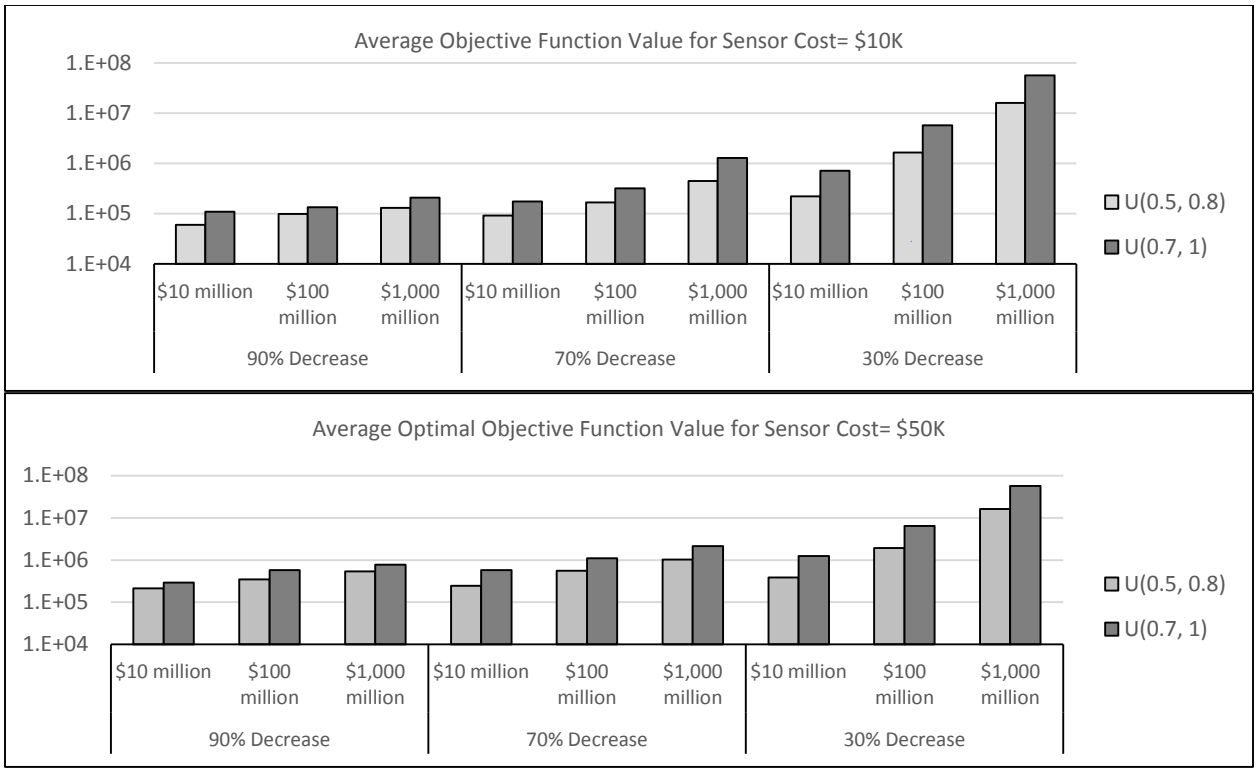

Figure 4.24 The defender's optimal objective function value (log-scale) for different types of distributions with different means, when deterrence function's shape parameters are (α=0.5, β=0.5)

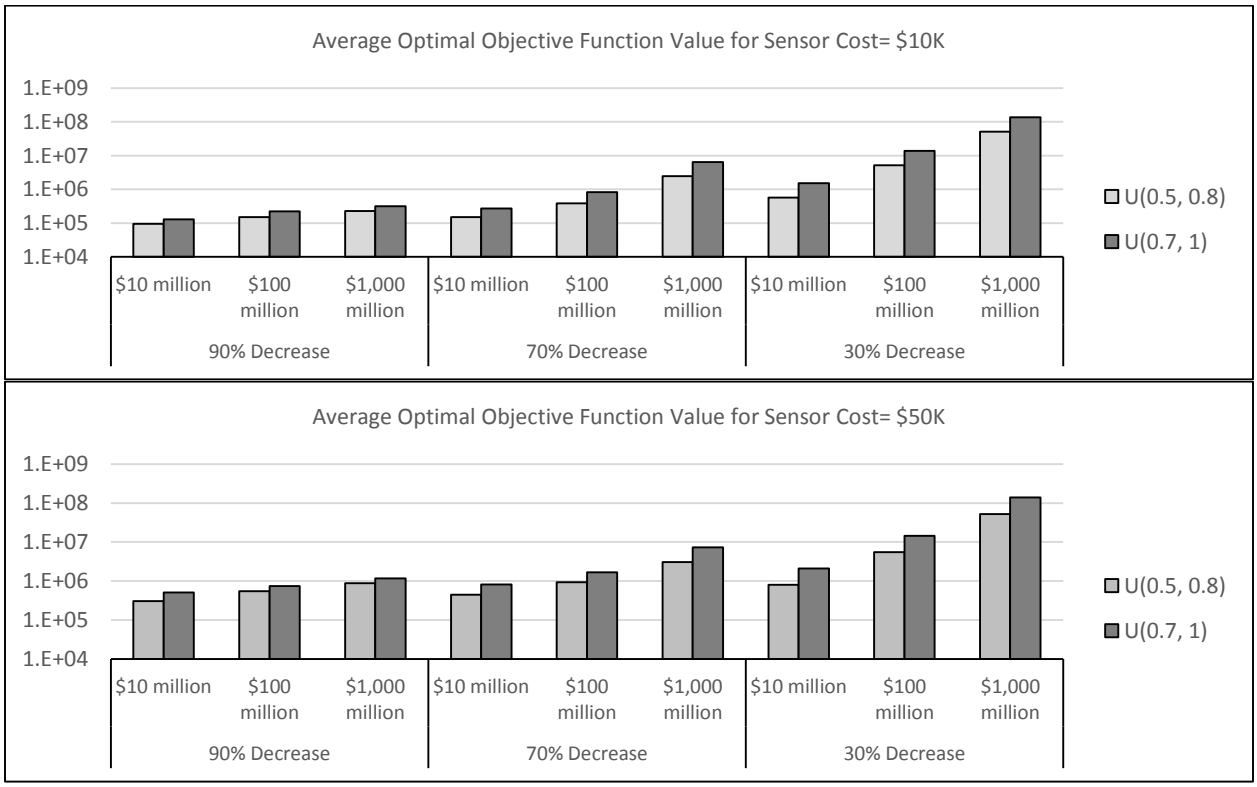

Figure 4.25 The defender's optimal objective function value (log-scale) for different types of distributions with different means, when deterrence function's shape parameters are (α=0.2, β=0.8)

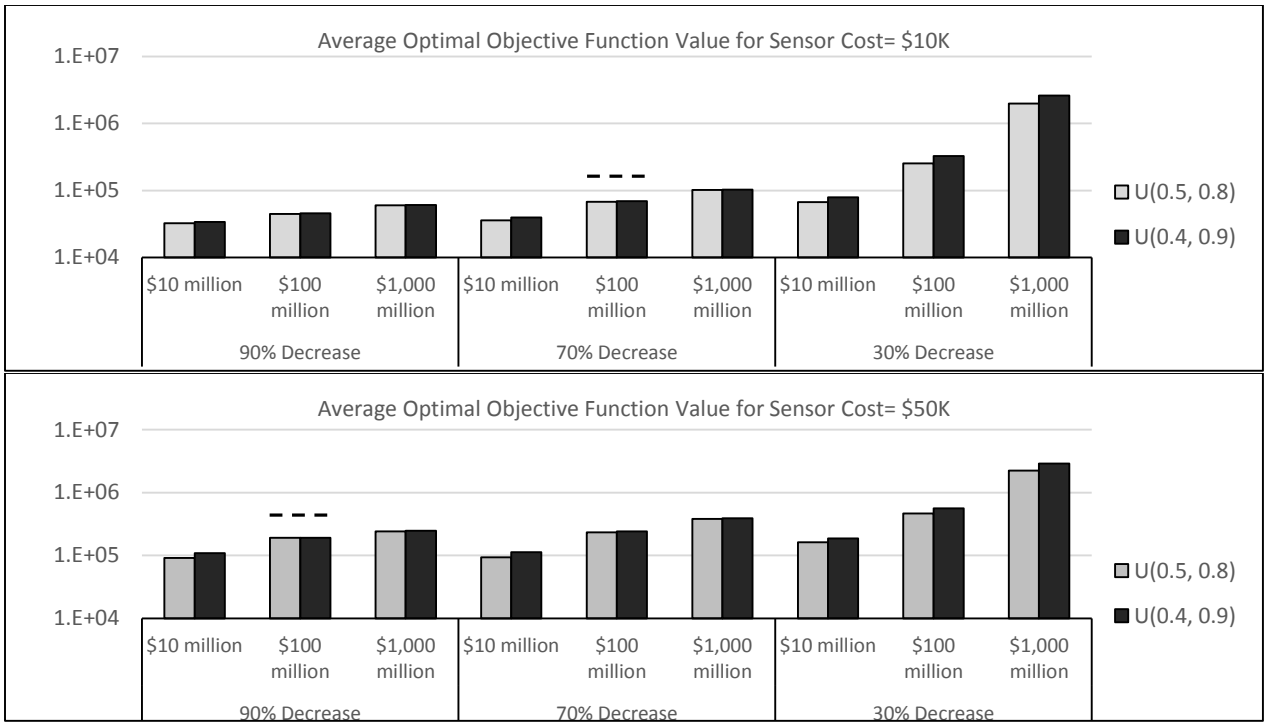

Figure 4.26 The defender's optimal objective function value (log-scale) for different types of distributions with different variances, when deterrence function's shape parameters are (α=2, β=2)

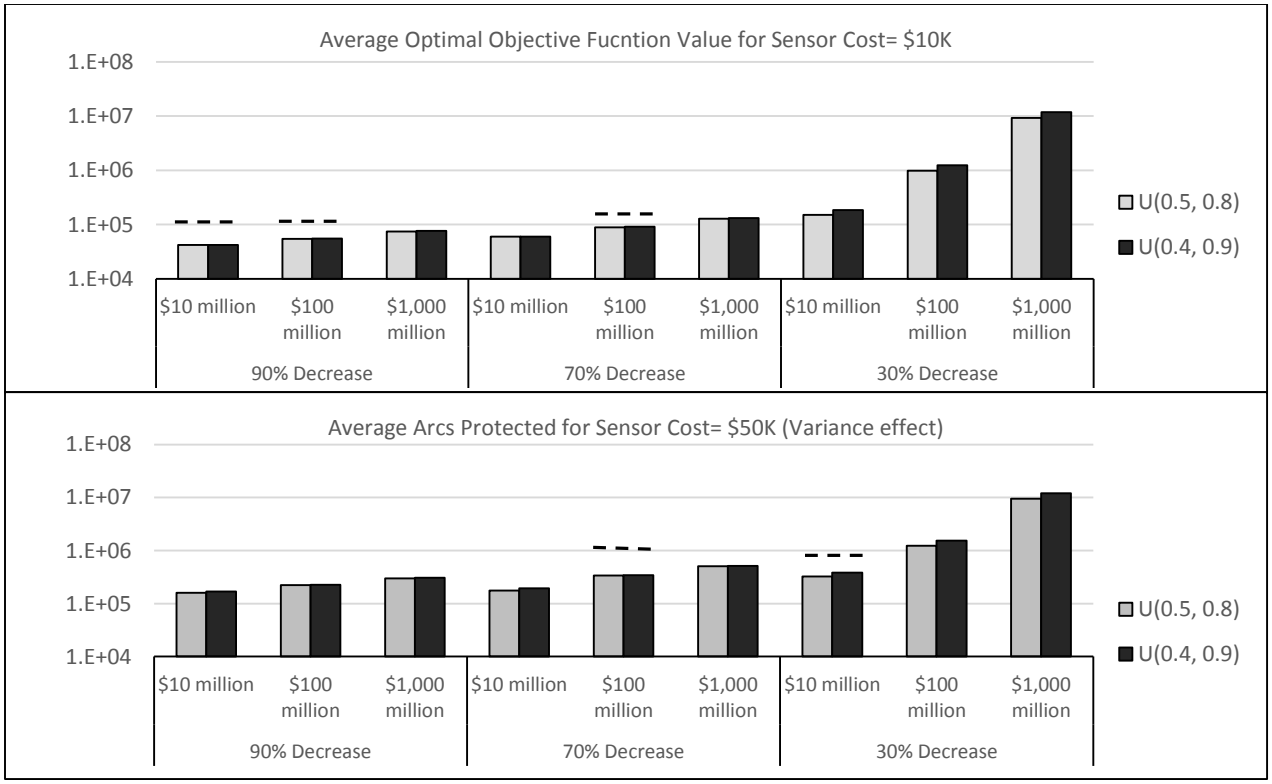

Figure 4.27 The defender's optimal objective function value (log-scale) for different types of distributions with different variances, when deterrence function's shape parameters are (α=2, β=10)

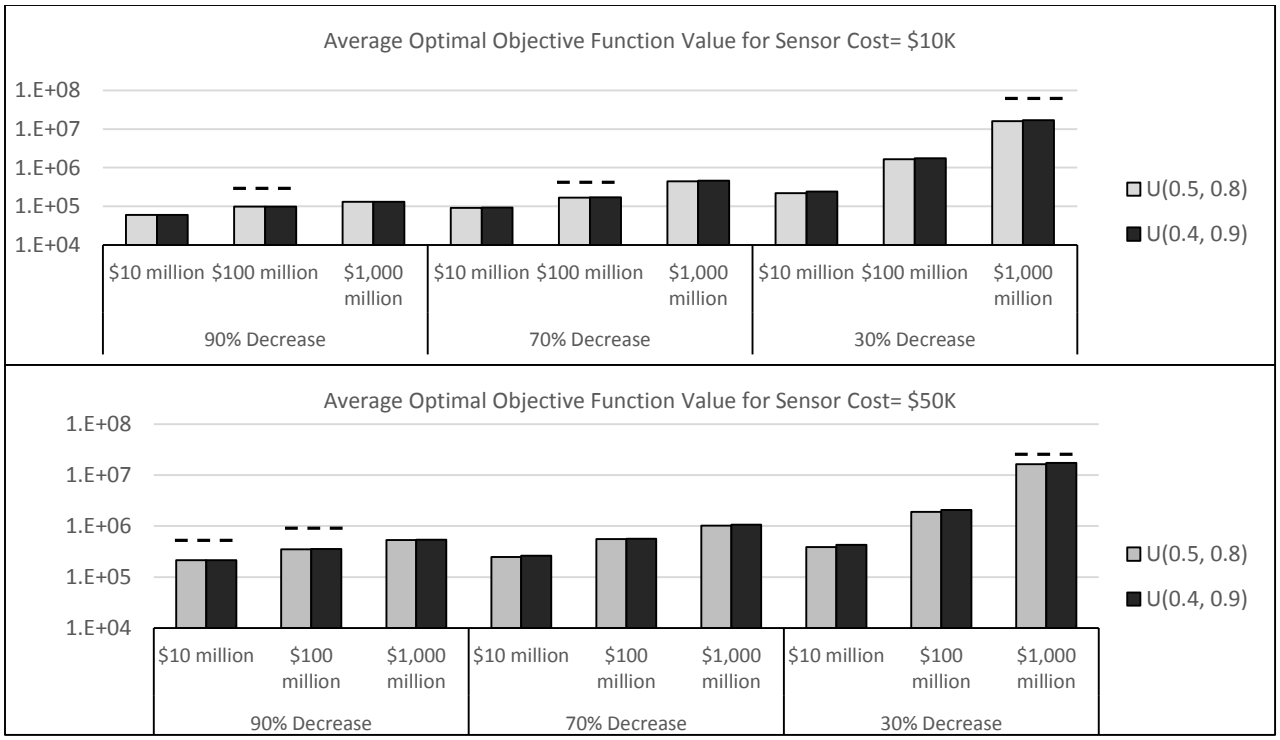

Figure 4.28 The defender's optimal objective function value (log-scale) for different types of distributions with different variances, when deterrence function's shape parameters are (α=0.5, β=0.5)

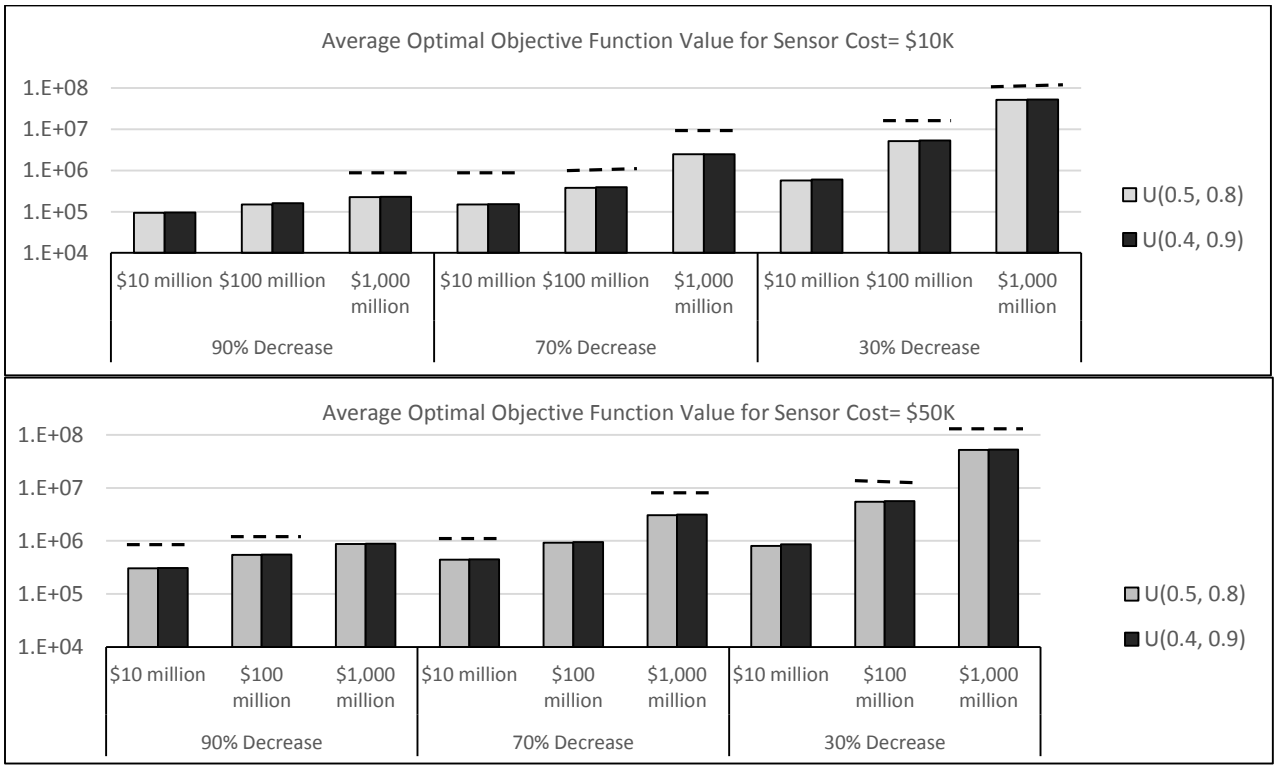

Figure 4.29 The defender's optimal objective function value (log-scale) for different types of distributions with different variances, when deterrence function's shape parameter are (α=0.2, β=0.8)

As in the previous section, the second parameter we examine is the target value *L*. Figures 4.30-4.33 below highlight the effect of *L* on the optimal objective function value. As expected, the average optimal objective function value is increasing as the target value increases. Moreover, in all cases, the difference between the objective function values for high and low valued targets is larger than the standard error of the results. Again, this is reasonable, since when the target value is large, either the expected loss will be large, or the defender will need to invest more to reduce the success probability of an attack.

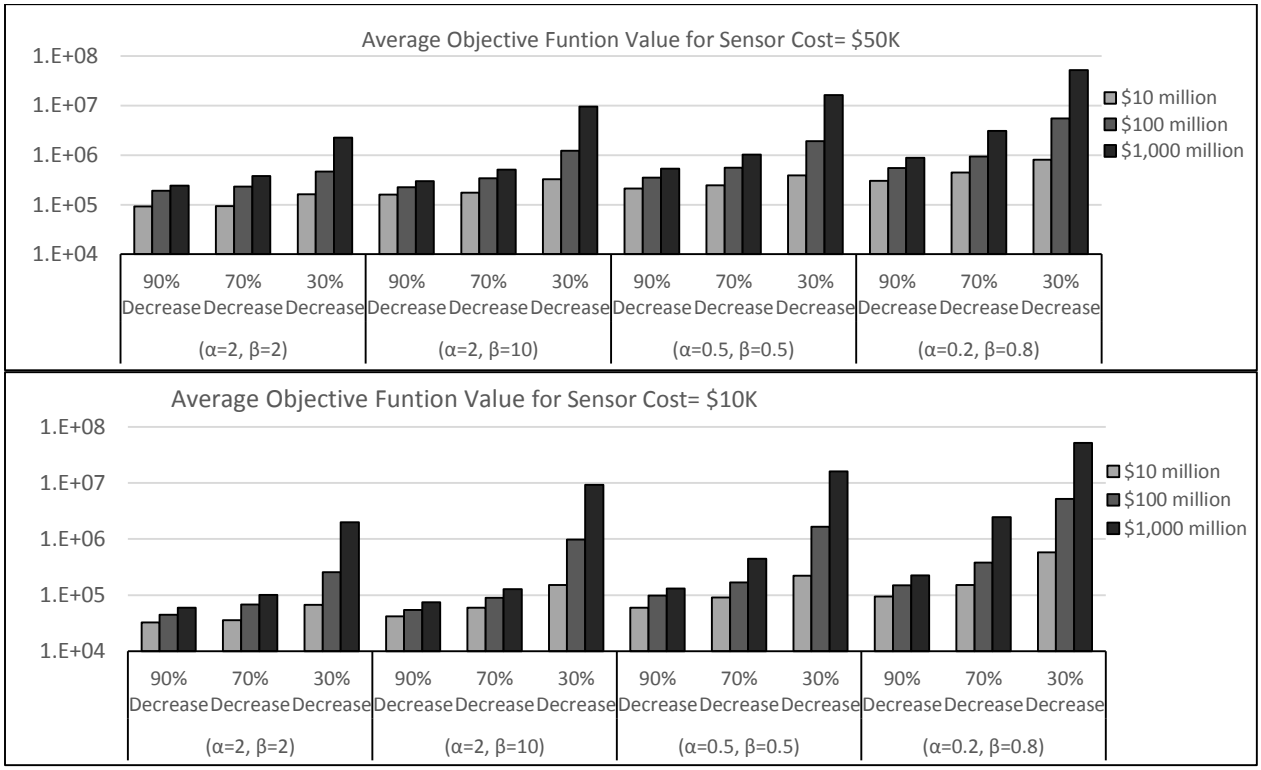

Figure 4.30 The defender's optimal objective function value (log-scale) for different target values, when p_{ij} is generated from Uniform(0.5,0.8)

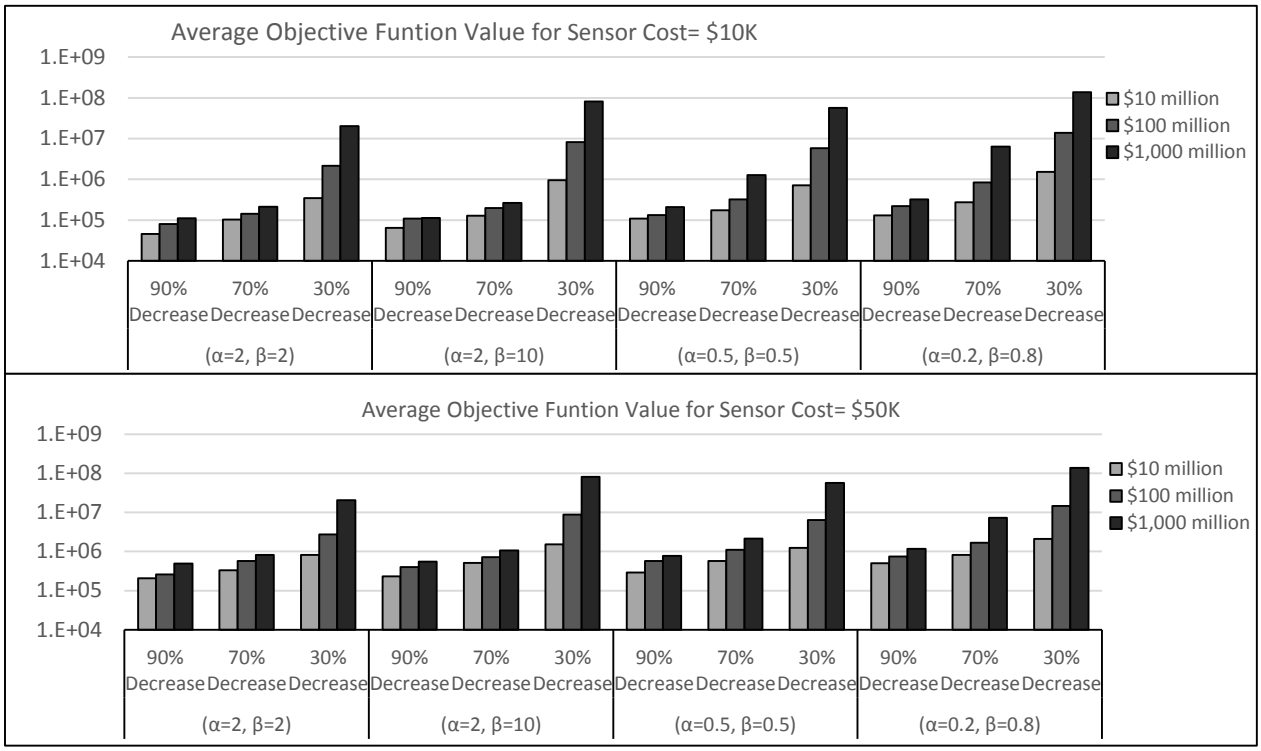

Figure 4.31The defender's optimal objective function value (log-scale) for different target values, when p_{ij} is generated from Uniform(0.7, 1)

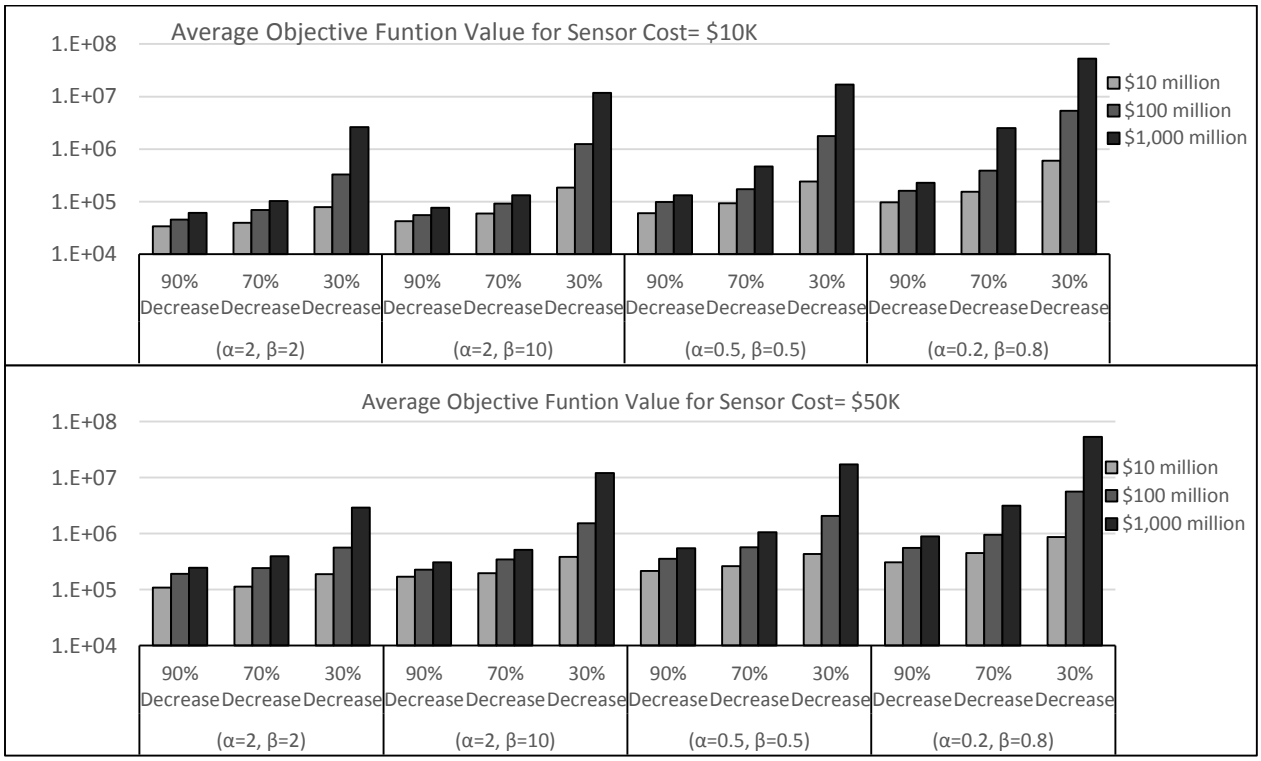

Figure 4.32 The defender's optimal objective function value (log-scale) for different target values, when p_{ij} is generated from Uniform(0.4, 0.9)

The cost of protecting an arc is another parameter affecting the optimal objective function value. Figures 4.33-4.36 below show the sensitivity of the defender's objective value to the cost of protection. As in the previous section, in each panel, the first two (crossed-hatched) bars evaluate the effects of sensor cost when the success probability of an attack on an arc is distributed U(0.5, 0.8); the middle two (solid) bars evaluate the effects of sensor cost when the success probability is U(0.4, 0.9); and the last two (cross-hatched) bars evaluate the effects of sensor cost when the success probability is U(07, 1). As expected, the average optimal objective function value for higher protection cost (as shown by the dark bars in Figures 4.33-4.36) is larger than for low protection cost (as shown by the light bars in Figures 4.33-4.36). However, in 10 of the 108 cases, the difference between the larger sensor cost and smaller sensor cost is less than the standard errors of the results (as shown by the dotted lines above the vertical bars).This occurs only when the effectiveness of defense is low (30%) and the target value is high ($1,000 million). In these cases, the objective function value is not highly sensitive to the cost of protection.

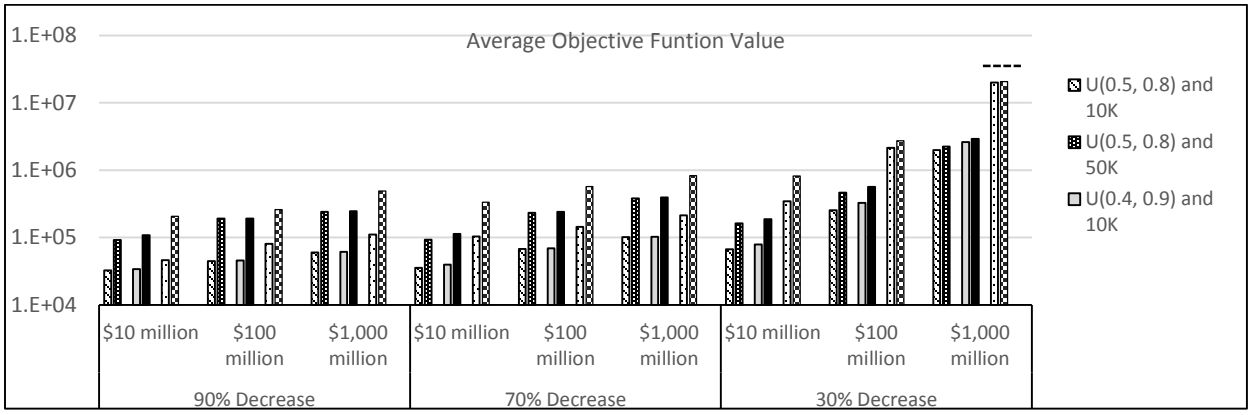

Figure 4.33 Comparison of average optimal defender's objective function value (log-scale) for different sensor costs, when deterrence function's shape parameters are (α=2, β=2)

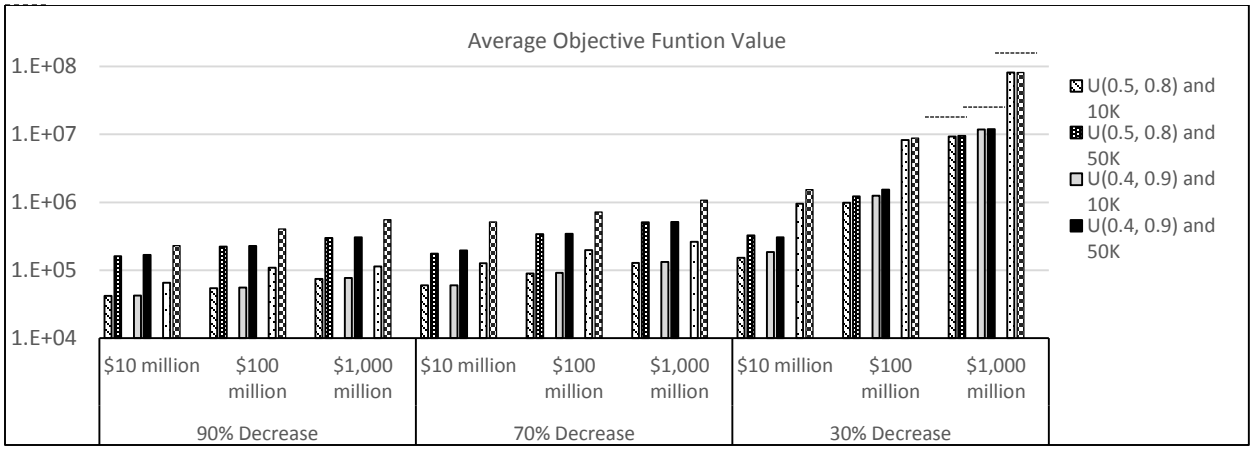

Figure 4.34 Comparison of average optimal defender's objective function value (log-scale) for different sensor costs, when deterrence function's shape parameters are (α=2, β=10)

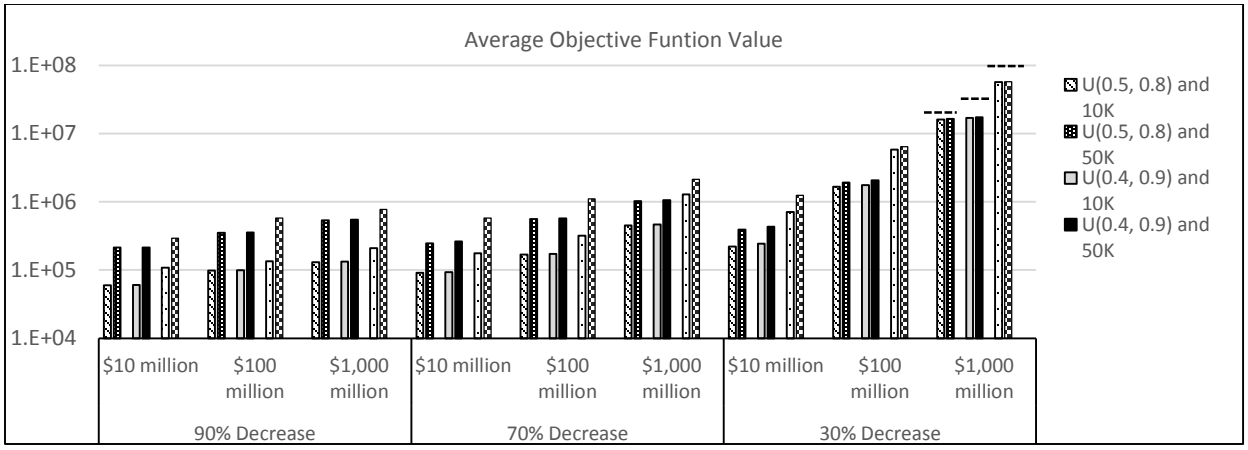

Figure 4.35 Comparison of average optimal defender's objective function value (log-scale) for different sensor costs, when deterrence function's shape parameters are (α=0.5, β=0.5)

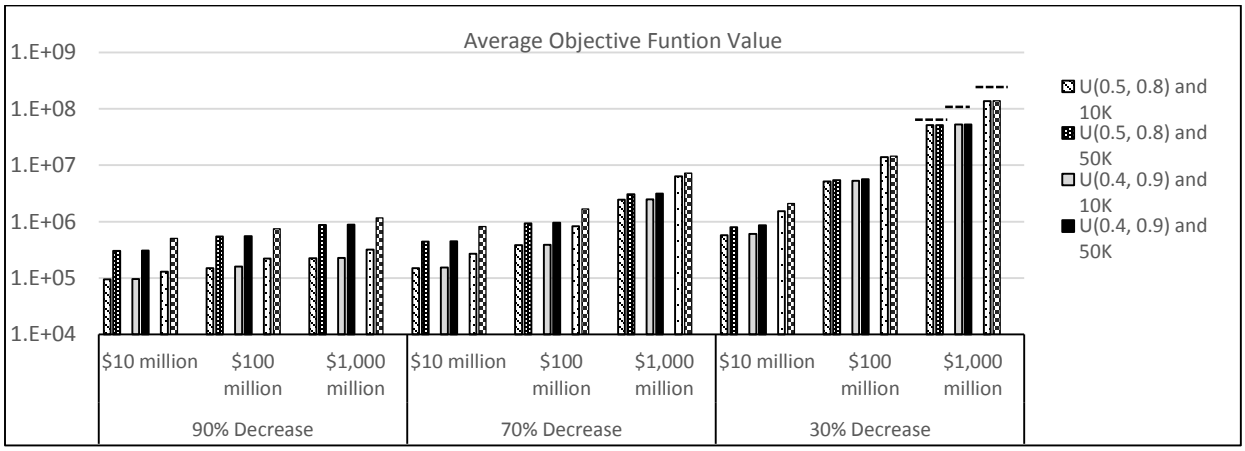

Figure 4.36 Comparison of average optimal defender's objective function value (log-scale) for different sensor costs, when deterrence function's shape parameters are (α=0.2, β=0.8)

We now explore the sensitivity of the defender's optimal objective function value to the effectiveness of defensive investment in Figures 4.37-4.39. Unsurprisingly, as the effectiveness of defense decreases, the optimal objective function value increases. The difference in the objective function values for different levels of defensive effectiveness are larger than the standard error of the results in all cases, except one case in Figure 4.37 (highlighted with "---") .

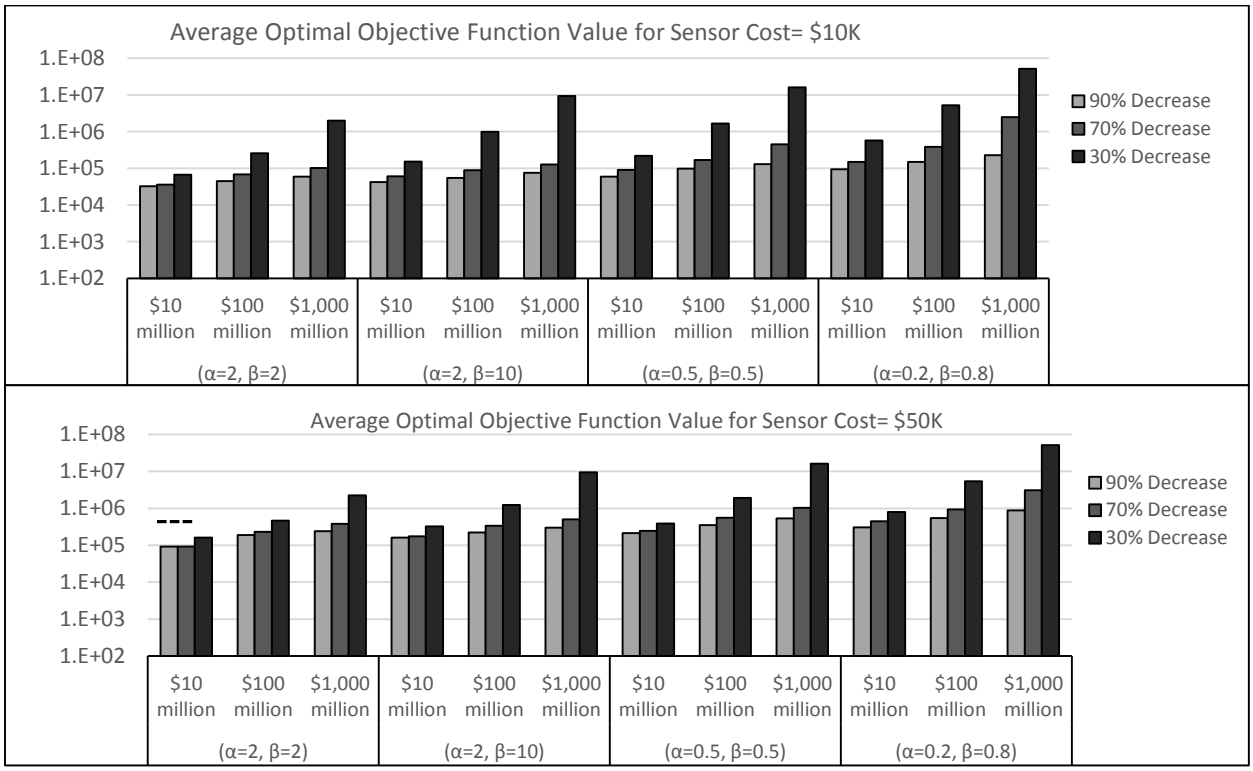

Figure 4.37 Optimal average defender's objective function value (log-scale) for different defensive effectiveness values, when p_{ij} is generated from U(0.5, 0.8)

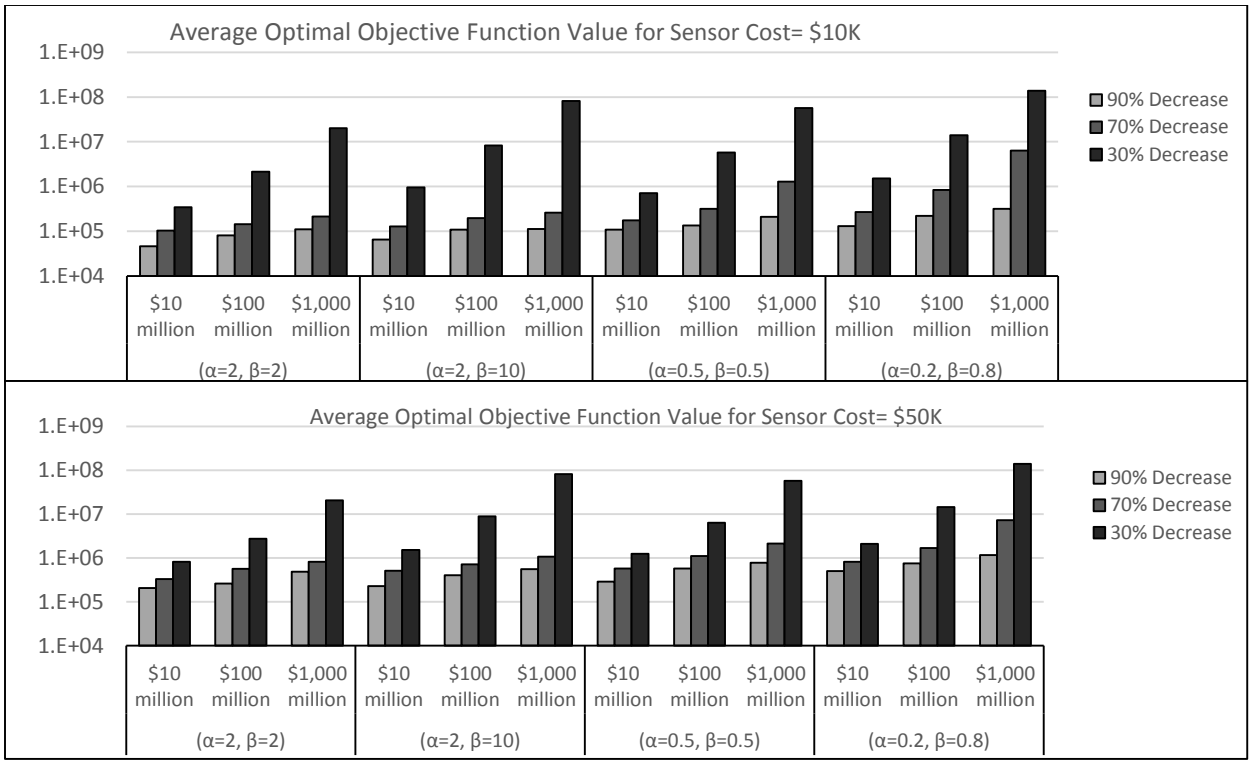

Figure 4.38 Optimal average defender's objective function value (log-scale) for different defensive effectiveness values, when p_{ij} is generated from U(0.7, 1)

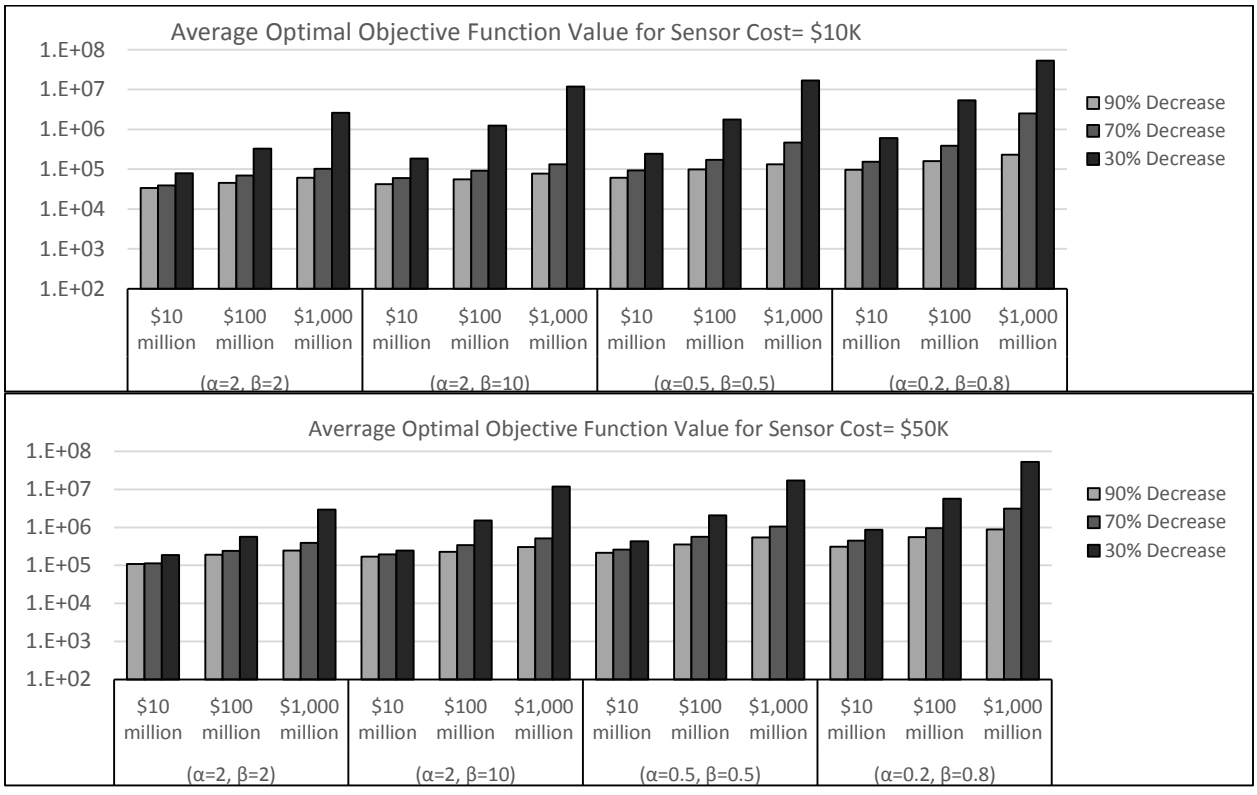

Figure 4.39 Optimal average defender's objective function value (log-scale) for different defensive effectiveness values, when p_{ij} is generated from U(0.4, 0.9)

The shape of the deterrence function also affects the optimal level of the defender's objective function. For S-shaped deterrence functions, the objective function values are larger for larger values of β (corresponding to cases in which the attacker is more difficult to deter); see the increase when moving from left to right within any given set of two solid bars in Figures 4.41-4.43. The same trend is observed for a reverse S-shaped deterrence function, as seen in the cross-hatched bars in Figures 4.40-4.42. The results also seem to be statistically reliable, since the differences are larger than the standard errors of the results.

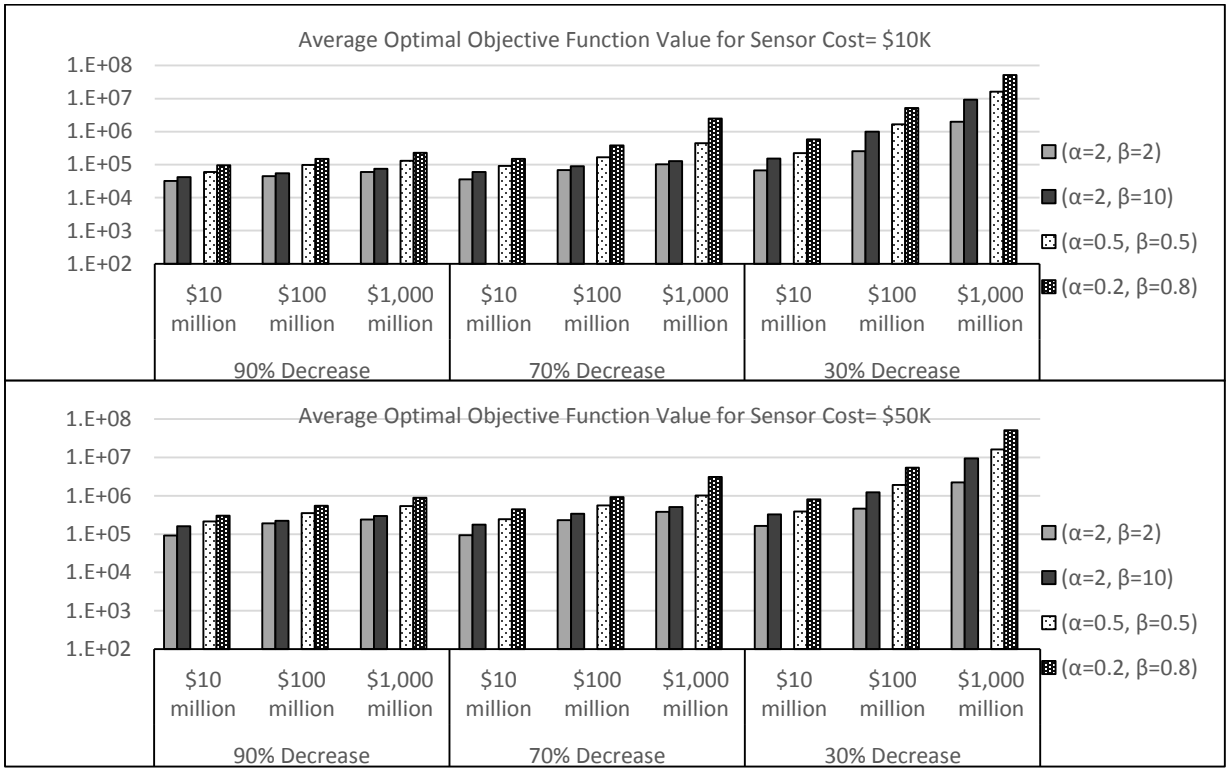

Figure 4.40 Optimal average defender's objective function value (log-scale) for different shape of deterrence function, when p_{ij} is generated from Uniform(0.5, 0.8)

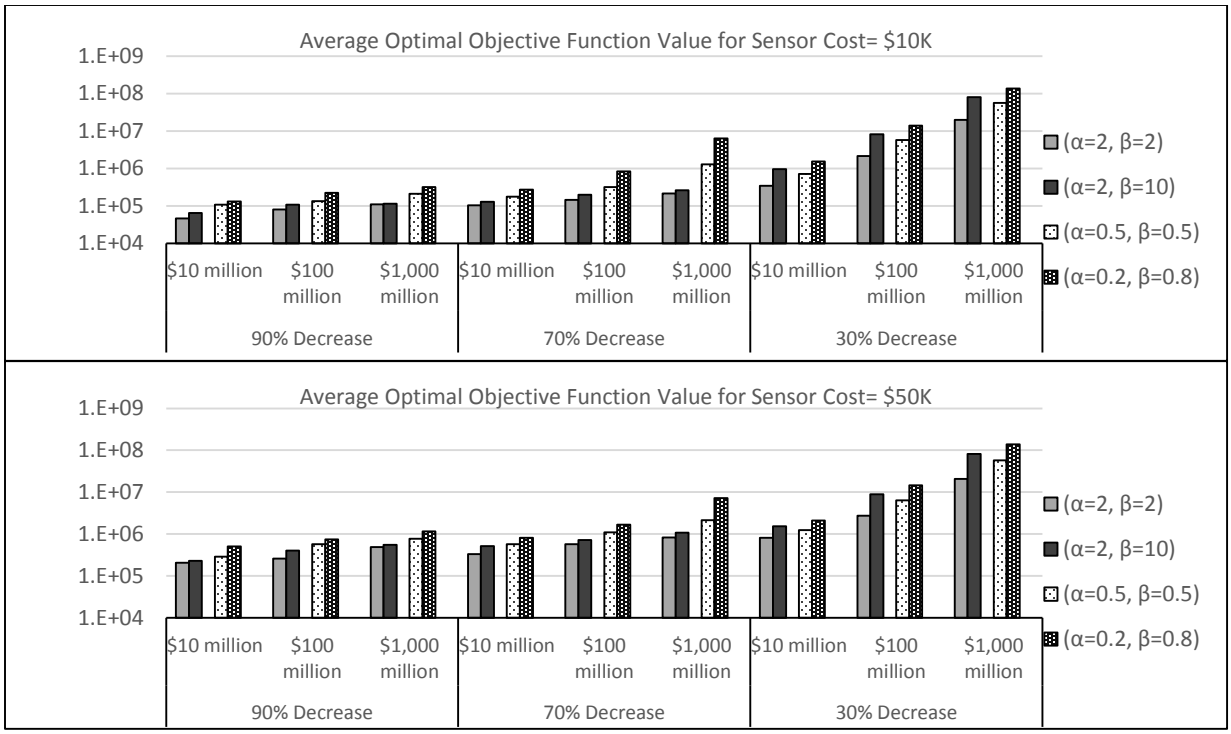

Figure 4.41 Optimal average defender's objective function value (log-scale) for different shape of deterrence function, when p_{ij} is generated from Uniform(0.7, 1)

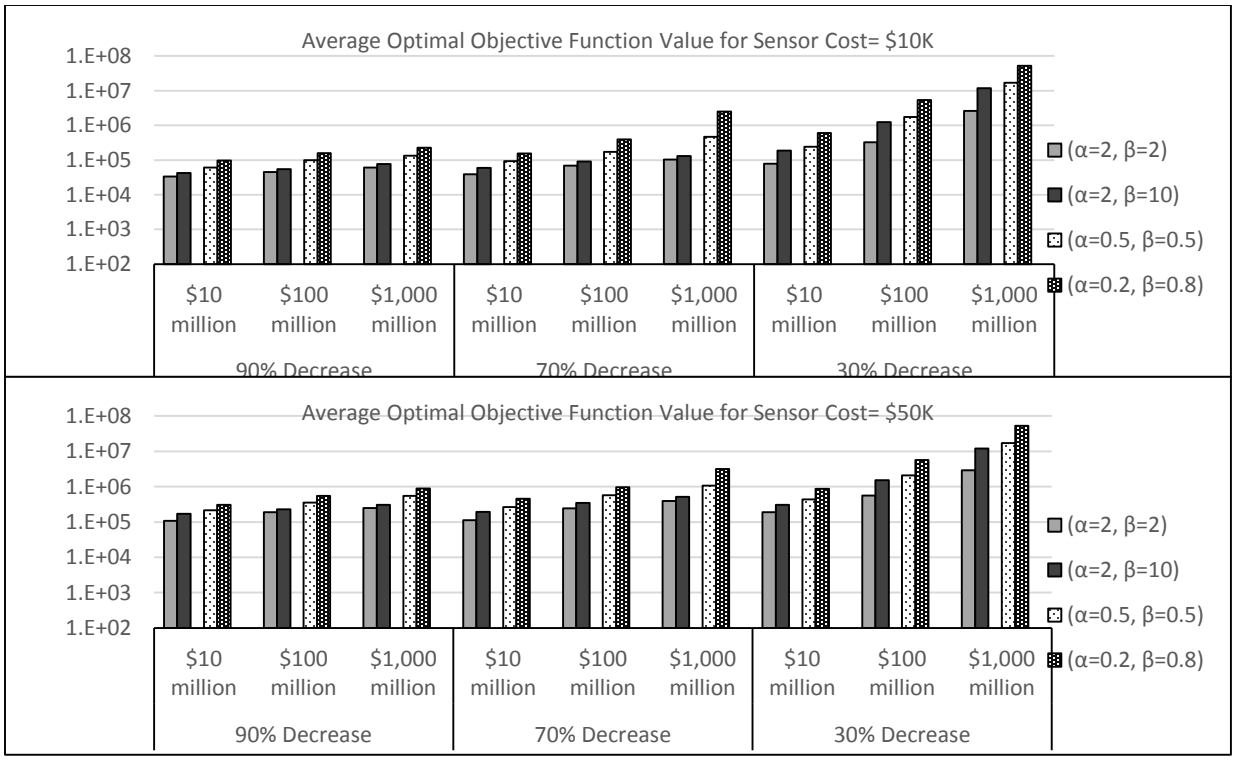

Figure 4.42 Optimal average defender's objective function value (log-scale) for different shape of deterrence function, when p_{ij} is generated from Uniform(0.4, 0.9)

In summary, the results presented above for sensitivity of the defender's objective function value to various parameters are all in the expected direction.

4.4.3 Sensitivity Analysis for the Overall Attack Success Probabilities

As in the previous sections, we begin our analysis by showing the effect of the distribution for the arc success probabilities p_{ij}. Since the overall attack success probability depends not only on the distribution of the p_{ij}, but also on the number of arcs protected (which must be integer in our model), we don't find a simple general result for how the mean of the distribution affects the overall attack success probability (comparing the dark and light bars in Figures 4.43-4.46). In particular, for a given variance of the arc success probability, the distribution with higher mean would clearly result in a higher overall attack success probability in an unprotected network. However, the defender may optimally choose to protect more arcs when the distribution has a higher mean, and may thereby achieve a lower overall attack success probability. Thus, in 13 of 72 cases (highlighted with "↘"), the overall attack success probability is decreasing as the mean arc success probability is increasing; for the remaining 59 cases (highlighted with "↗"), the overall attack success probability is increasing. The difference is always larger than the standard error of the results.

However, the distribution with the higher mean always results in a higher overall attack success probability when the effectiveness of defensive investment is low (30%), as shown in the rightmost three pairs of bars in Figures 4.42-4.46. This is because, although the defender optimally chooses to protect more arcs in the distribution with the higher mean (as shown in Figures 4.1-4.4), the overall success probability is still large due to the low effectiveness of defensive investment.

The variance of the distribution for the arc success probabilities also has inconsistent effects on the overall attack success probability, as shown in Figures 4.47-4.50. In 8 of 72 cases, the overall attack success probability is decreasing in the variance of the distribution for the arc success probabilities (highlighted with " ↘ "), for 11 out of 72 cases it is increasing (highlighted with " ↗ "), for remaining 53 cases there is no significant difference (highlighted with dashed line "- - - -").

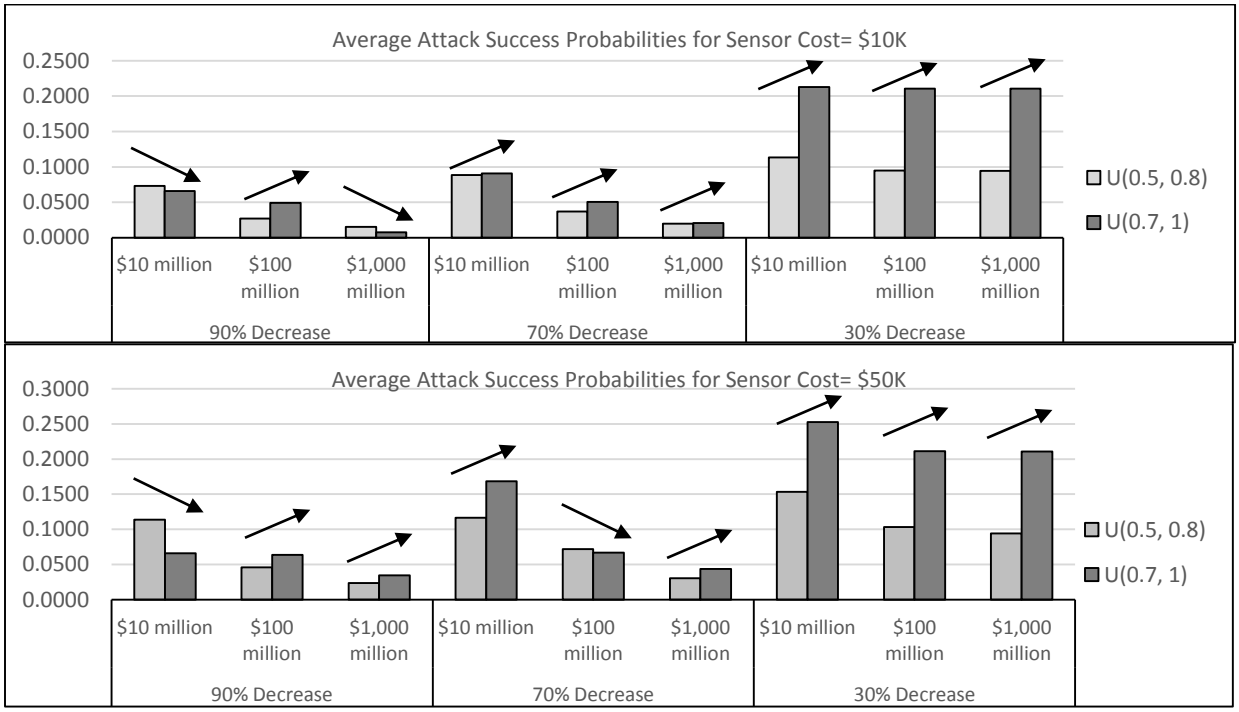

Figure 4.43 The average attack success probabilities for different types of distributions with different means, when deterrence function's shape parameters are (α=2, β=2)

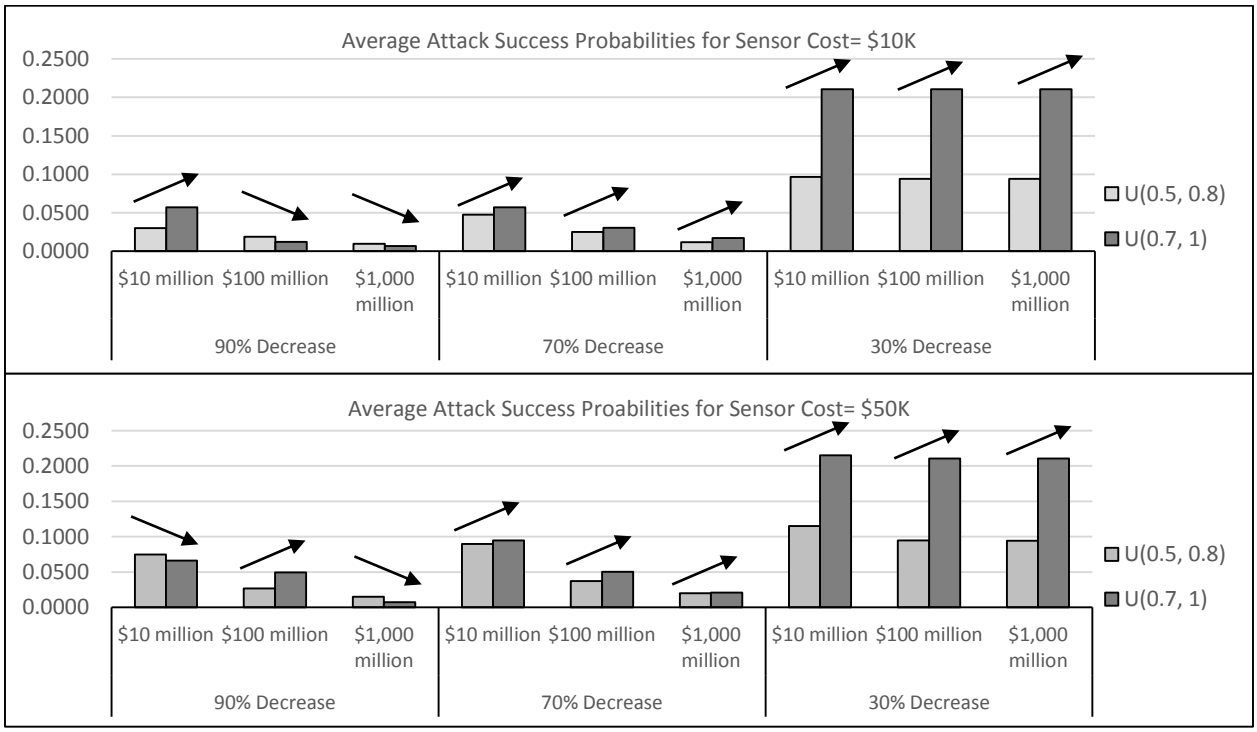

Figure 4.44 The average attack success probabilities for different types of distributions with different means, when deterrence function's shape parameters are (α=2, β=10)

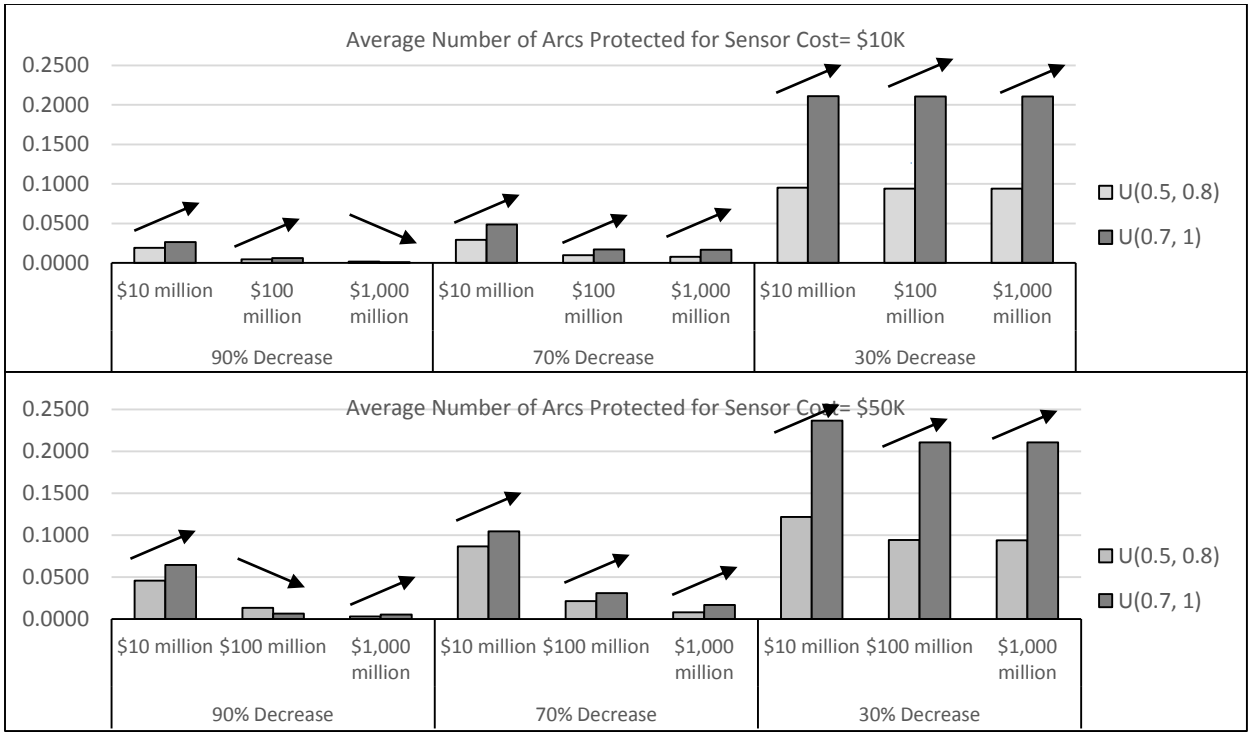

Figure 4.45 The average attack success probabilities for different types of distributions with different means, when deterrence function's shape parameters are (α=0.5, β=0.5)

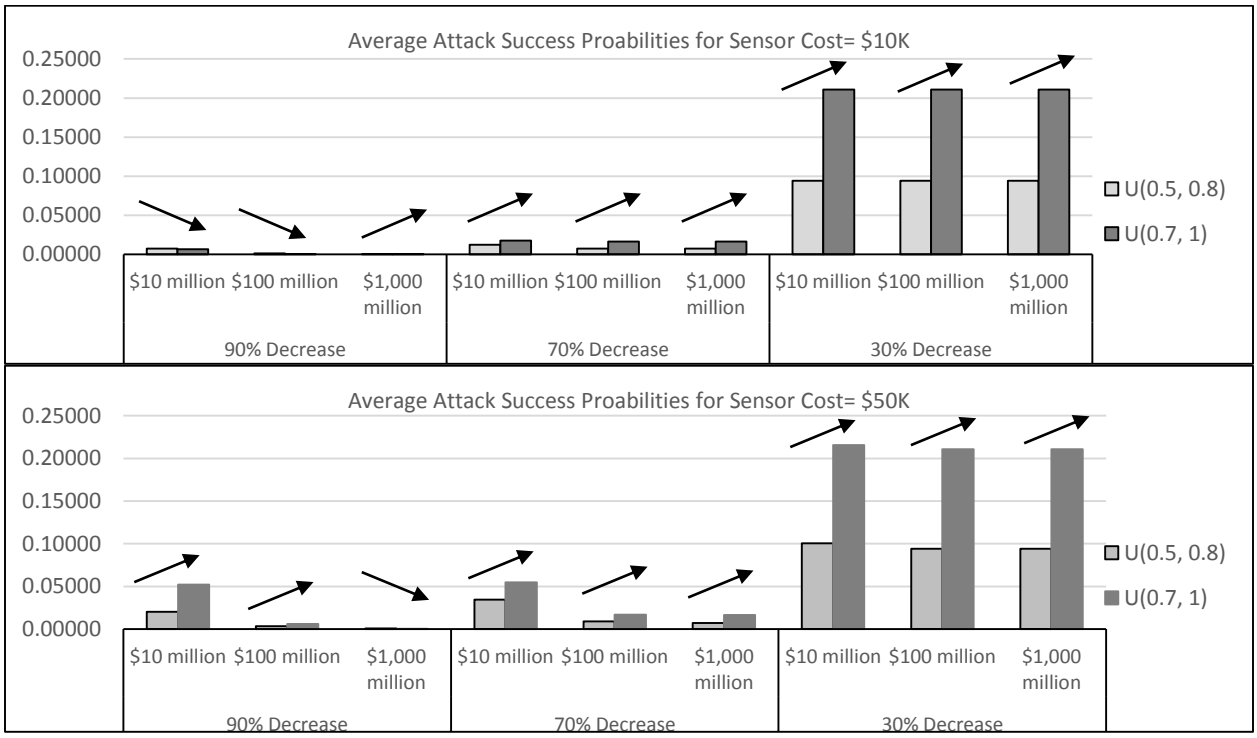

Figure 4.46 The average attack success probabilities for different types of distributions with different means, when deterrence function's shape parameters are (α=0.2, β=0.8)

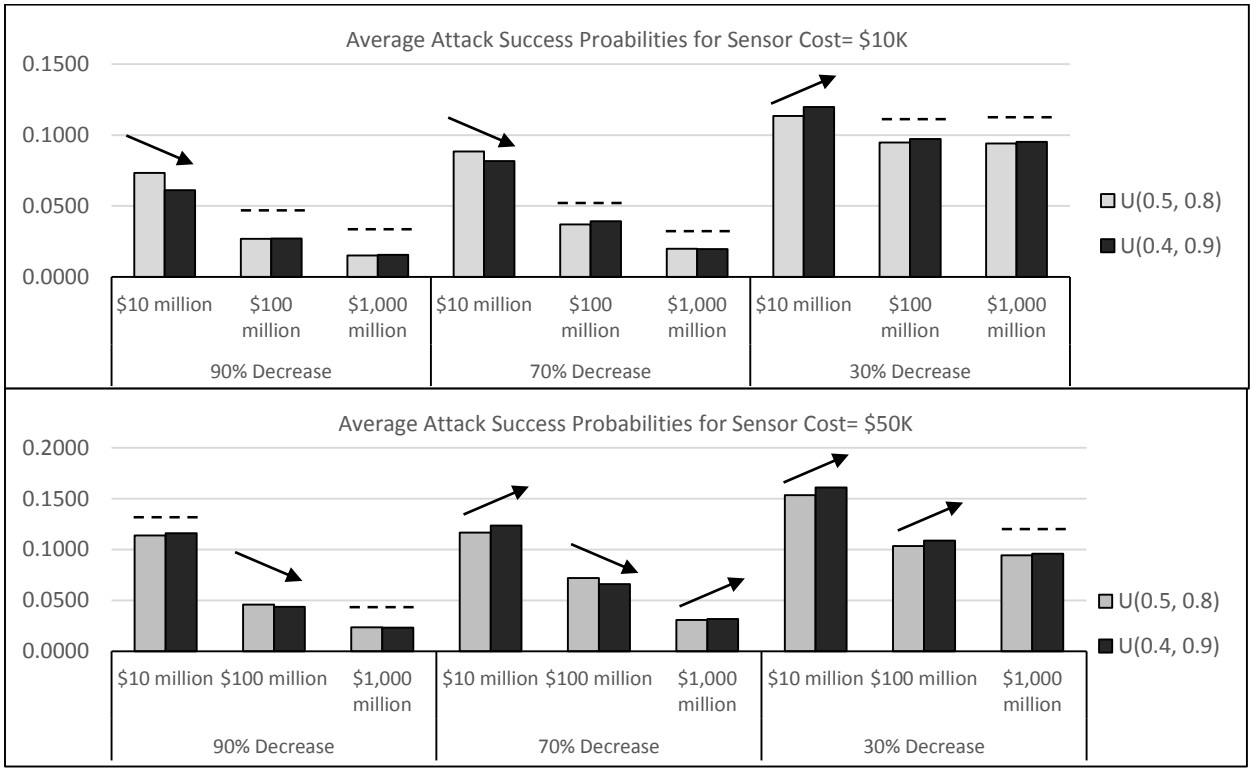

Figure 4.47 The average attack success probabilities for different types of distributions with different variances, when deterrence function's shape parameters are (α=2, β=2)

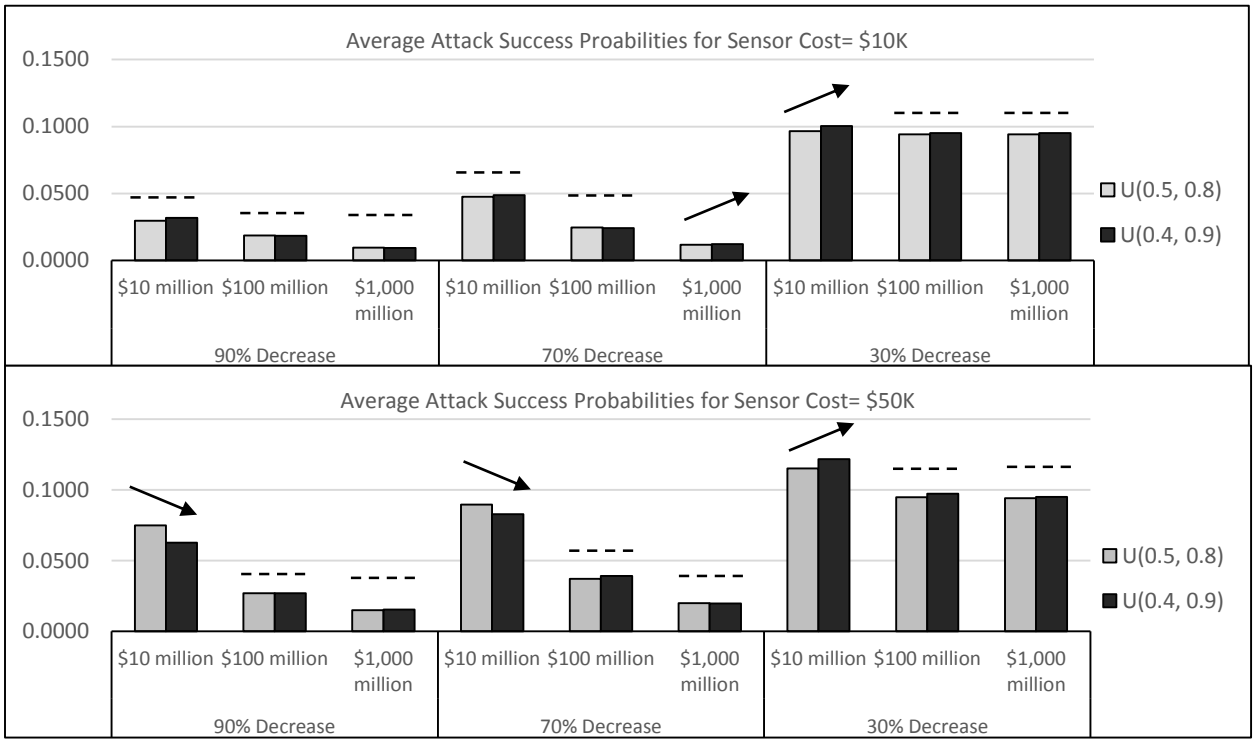

Figure 4.48 The average attack success probabilities for different types of distributions with different variances, when deterrence function's shape parameters are (α=2, β=10)

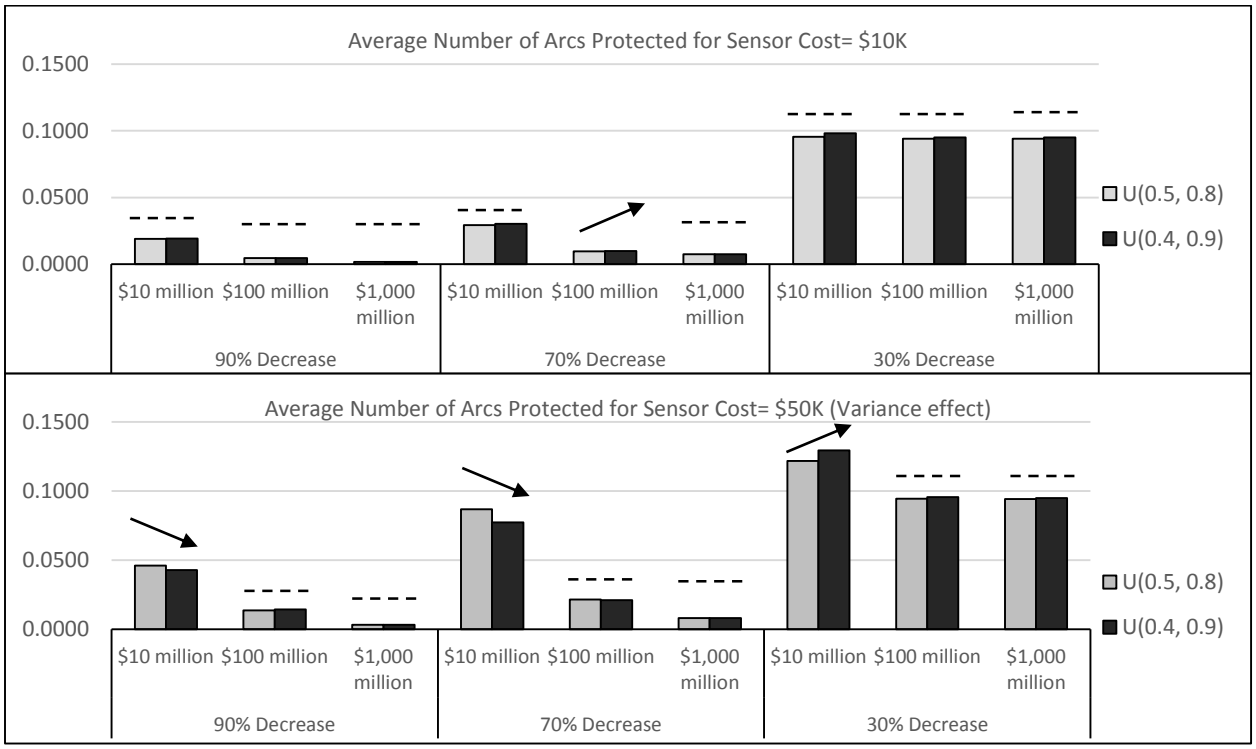

Figure 4.49 The average attack success probabilities for different types of distributions with different variances, when deterrence function's shape parameters are (α=0.5, β=0.5)

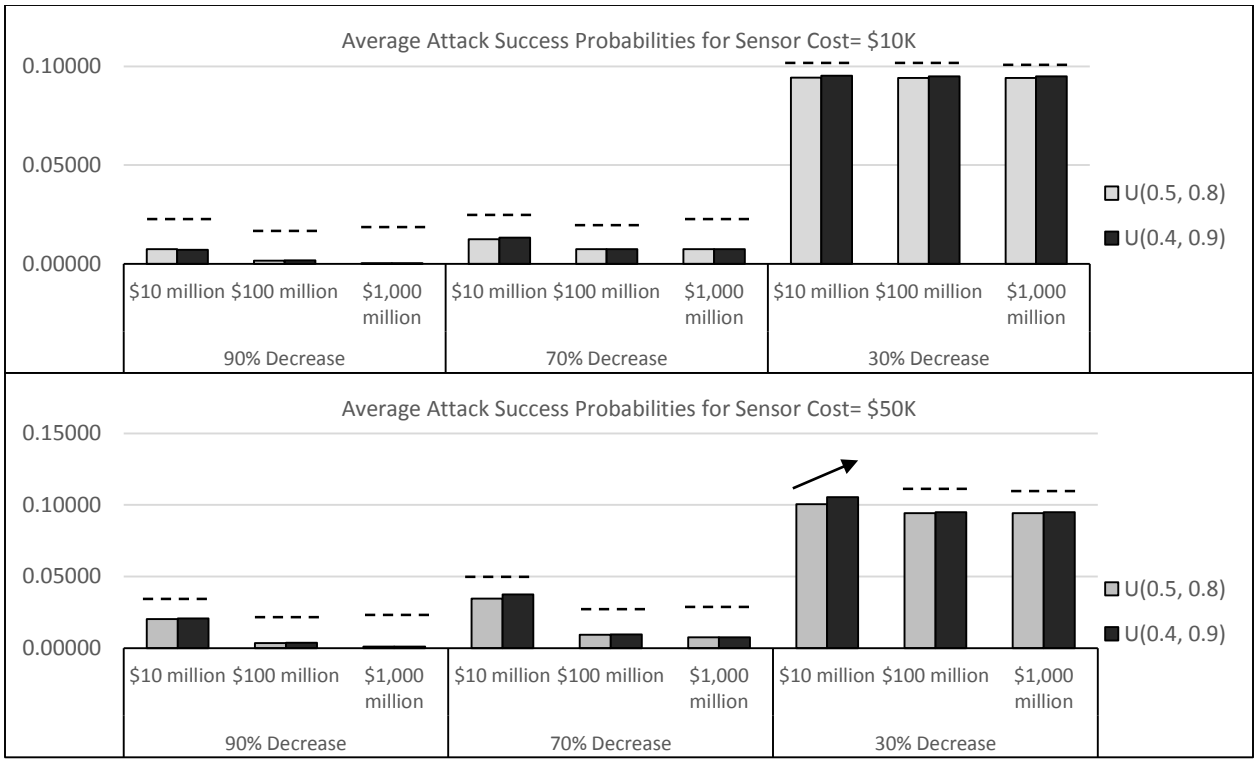

Figure 4.50 The average attack success probabilities for different types of distributions with different variances, when deterrence function's shape parameter are (α=0.2, β=0.8)

Next, in Figures 4.51-4.53, we explore how the overall attack success probability depends on the target valuation. For most cases (47 out of the 72 cases), the overall attack success probability is decreasing as the target value increases. This is reasonable, because when the target value is large, the defender optimally allocates more recourses to protection. However, in nine of the 72 cases (highlighted with dotted lines "------"), the difference between the higher and lower value targets is smaller than the standard errors of the results. Also, in 15 of the 72 cases (highlighted with dashed lines "- - "), the difference between target values of $100 million and $1000 million is smaller than the standard error of the results, but the difference between target values of $10 million and $100 million is larger than the standard error of the results. The effect of the target value tends to be small particularly when the effectiveness of defensive investment is small (e.g., in the rightmost set of three bars in each panel of Figures 4.51- 4.53), presumably because when defensive investment is not highly effective, it is not cost effective to spend more

on defense of a higher valued target. This is confirmed by reviewing the results in Figures 4.9-4.11, which show that the defender optimally chooses to protect similar numbers of arcs regardless of the target value, when the effectiveness of defensive investment is low.

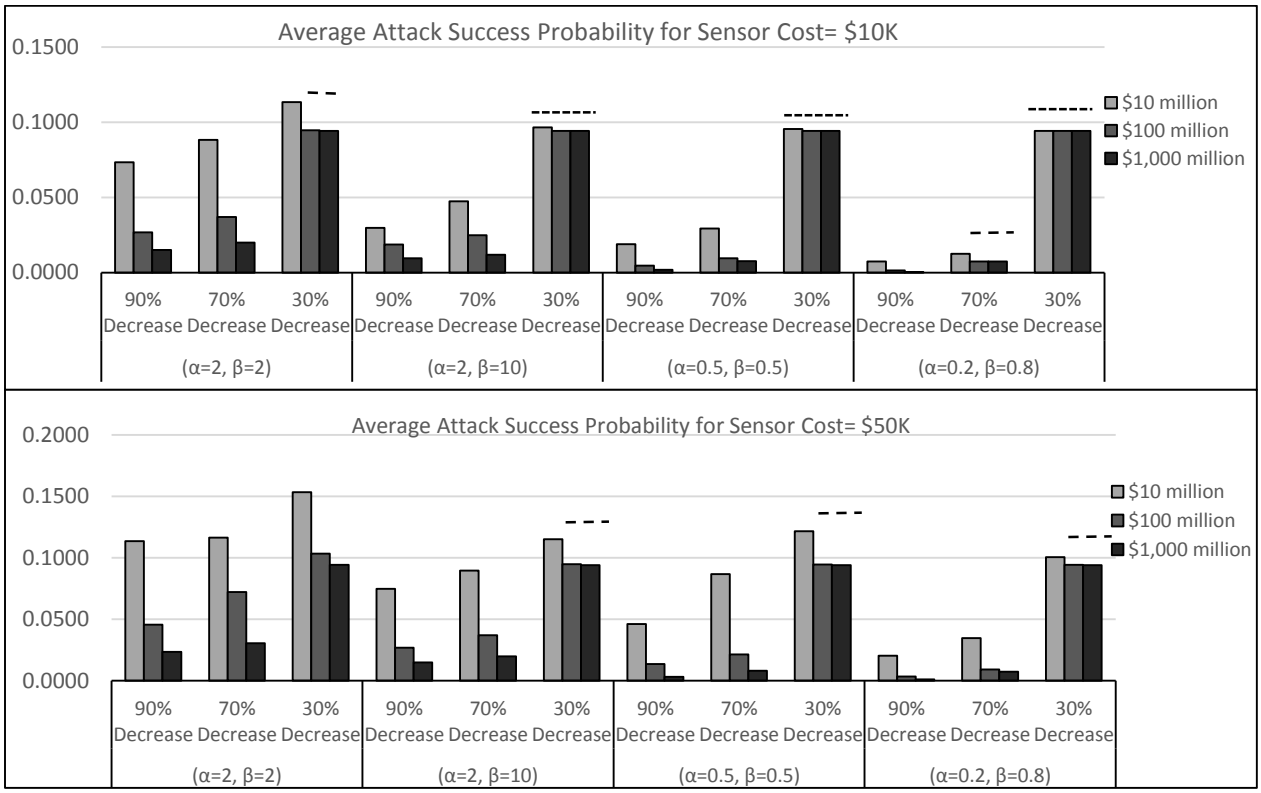

Figure 4.51 The average attack success probabilities for different target values, when p_{ij} is generated from Uniform(0.5,0.8)

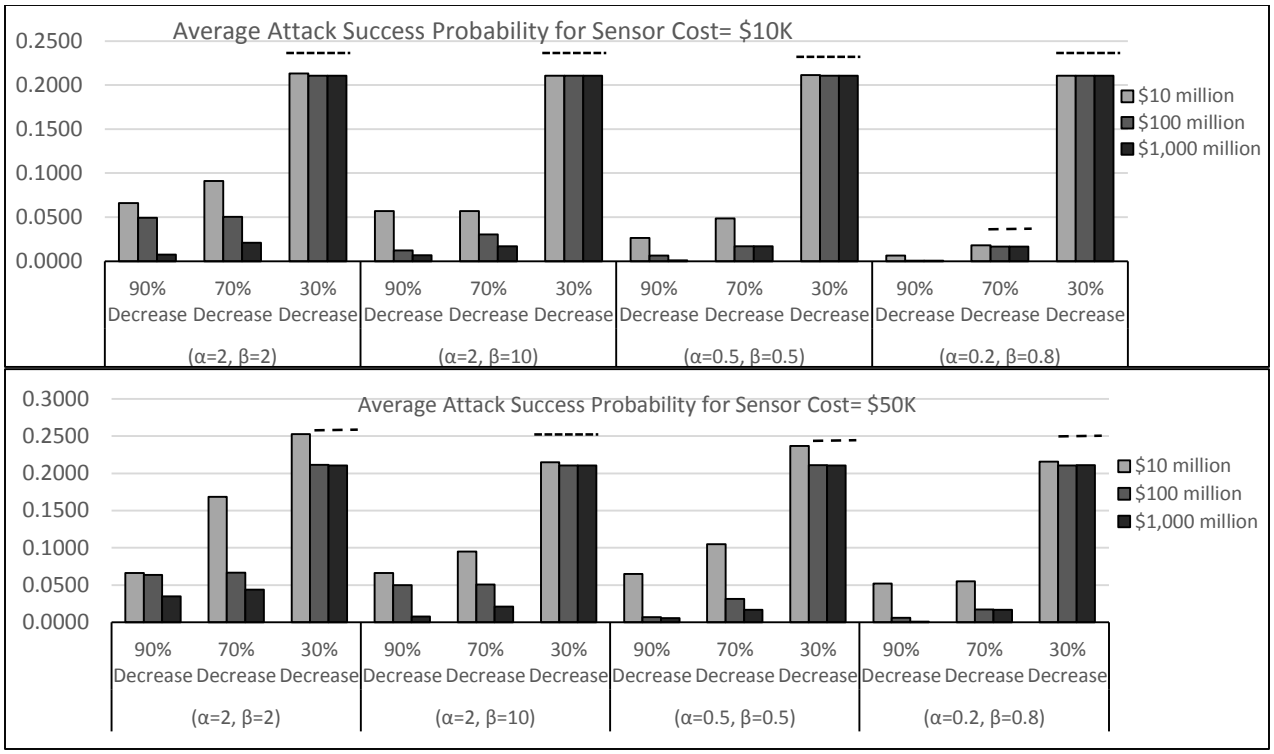

Figure 4.52 The average attack success probabilities for different target values, when pij is generated from Uniform(0.7, 1)

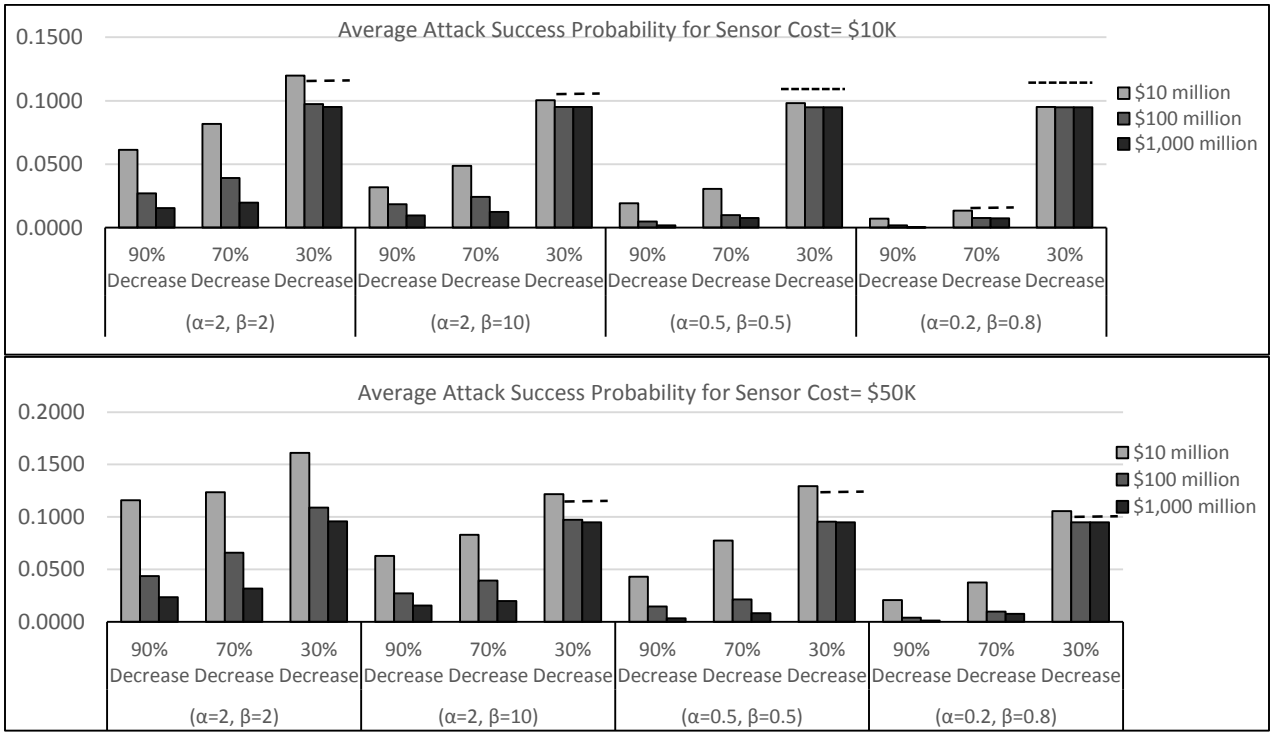

Figure 4.53 The average attack success probabilities for different target values, when p_{ij} is generated from Uniform(0.4, 0.9)

The effect of the cost of arc protection on the overall average attack success probability is presented in Figures 4.54-4.57 below. As in previous sections, in each panel, the first two (crossed-hatched) bars evaluate the effects of sensor cost when the success probability is U(0.5, 0.8), the middle two (solid) bars evaluate the effects of sensor cost when the success probability is distributed U(0.4, 0.9), and the last two (cross-hatched) bars evaluate the effects of sensor cost when the success probability is distributed U(07, 1). As expected, the average overall attack success probability is smaller when the protection cost is low (the light bars in each panel in Figures 4.54-4.57) than when it is high (the dark bars in each panel in Figures 4.54 -4.57.

However, in 28 of the 108 cases, the difference in attack success probability between cases with large and small protection costs is less than the standard errors of the results (as shown by the dotted lines above the vertical bars). Most of these cases occur when the effectiveness of defense is relatively low and the target values are large ($100 million or $1,000 million).

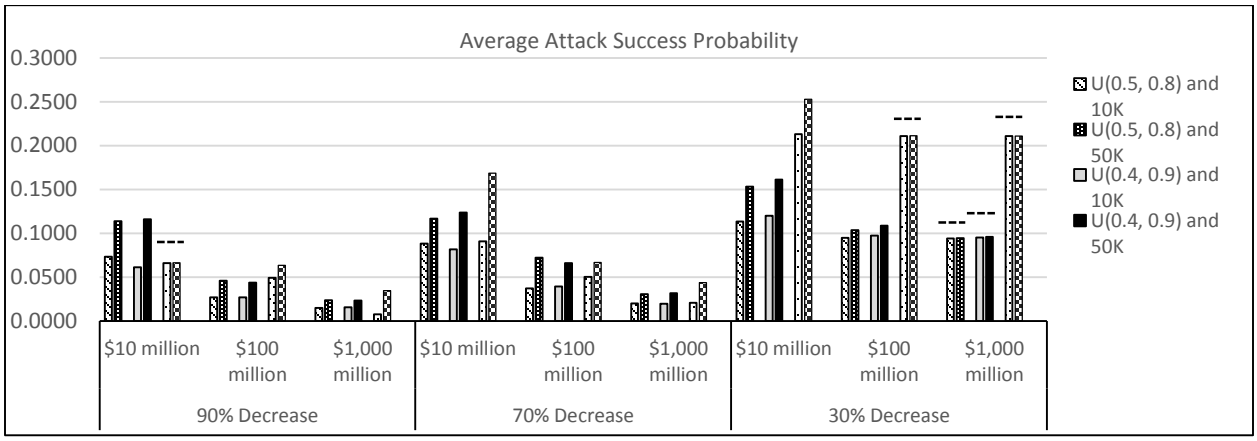

Figure 4.54 Comparison of the average attack success probabilities for different sensor costs, when deterrence function's shape parameters are (α=2, β=2)

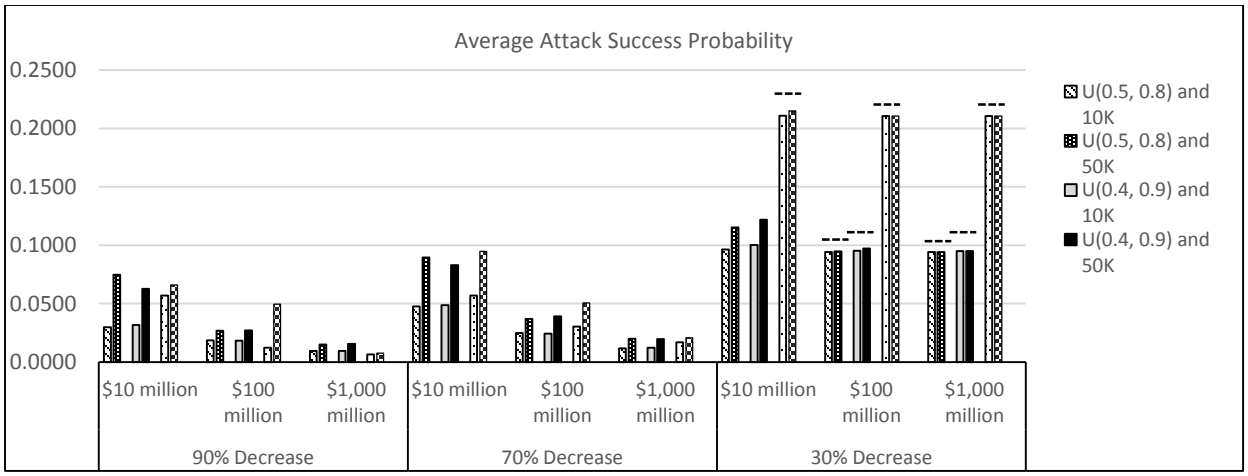

Figure 4.55 Comparison of the average attack success probabilities for different sensor costs, when deterrence function's shape parameters are (α=2, β=10)

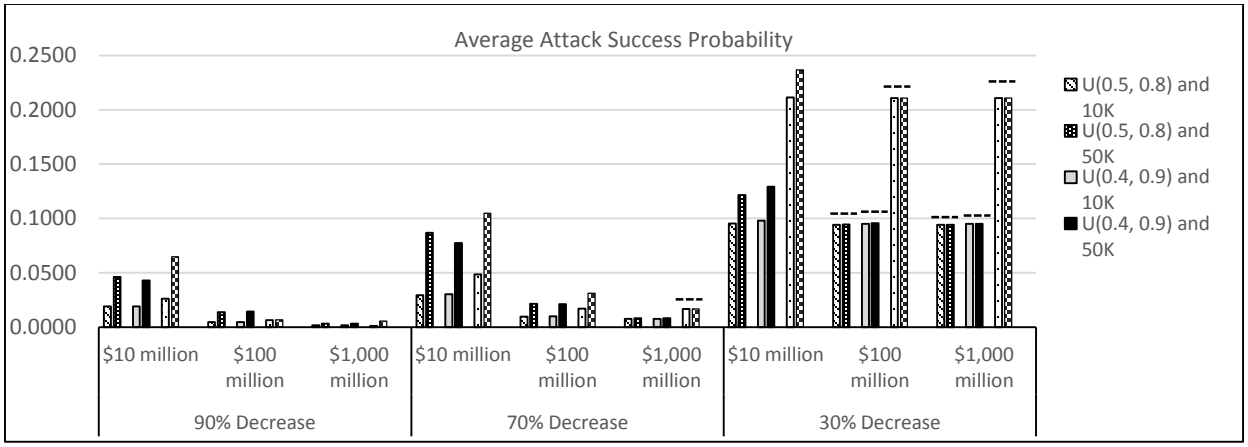

Figure 4.56 Comparison of the average attack success probabilities for different sensor costs, when deterrence function's shape parameters are (α=0.5, β=0.5)

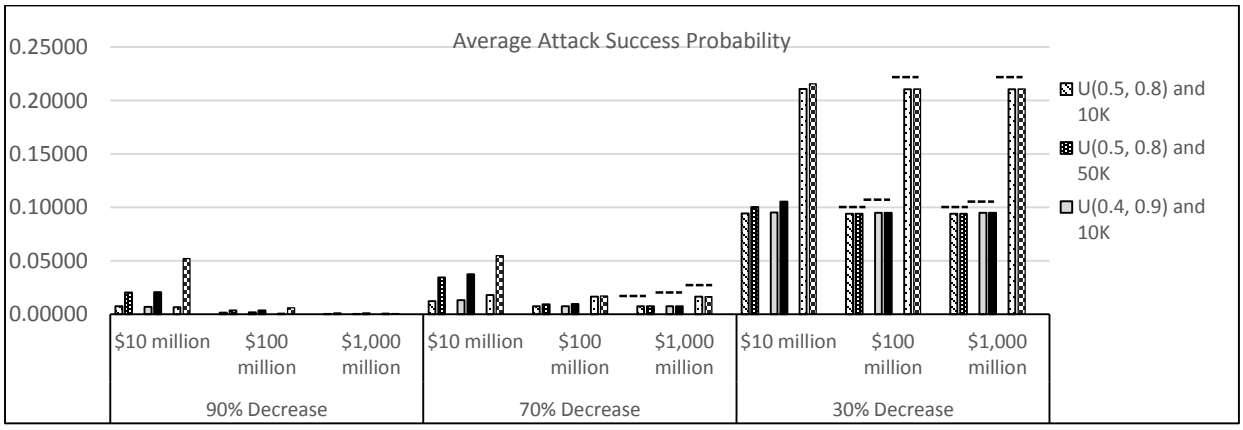

Figure 4.57 Comparison of the average attack success probabilities for different sensor costs, when deterrence function's shape parameters are (α=0.2, β=0.8)

Another important parameter affecting the overall average attack success probability is the effectiveness of defensive investment. We present the sensitivity of the attack success probability to the effectiveness of defensive investment in Figures 4.58-4.60. For 71 of the 72 cases, as the effectiveness of defense decreases, the average attack success probability increases; in the remaining case (highlighted with a dashed line "– – -"), the difference between the results for 90% and 70% effectiveness is smaller than the standard error of the results.

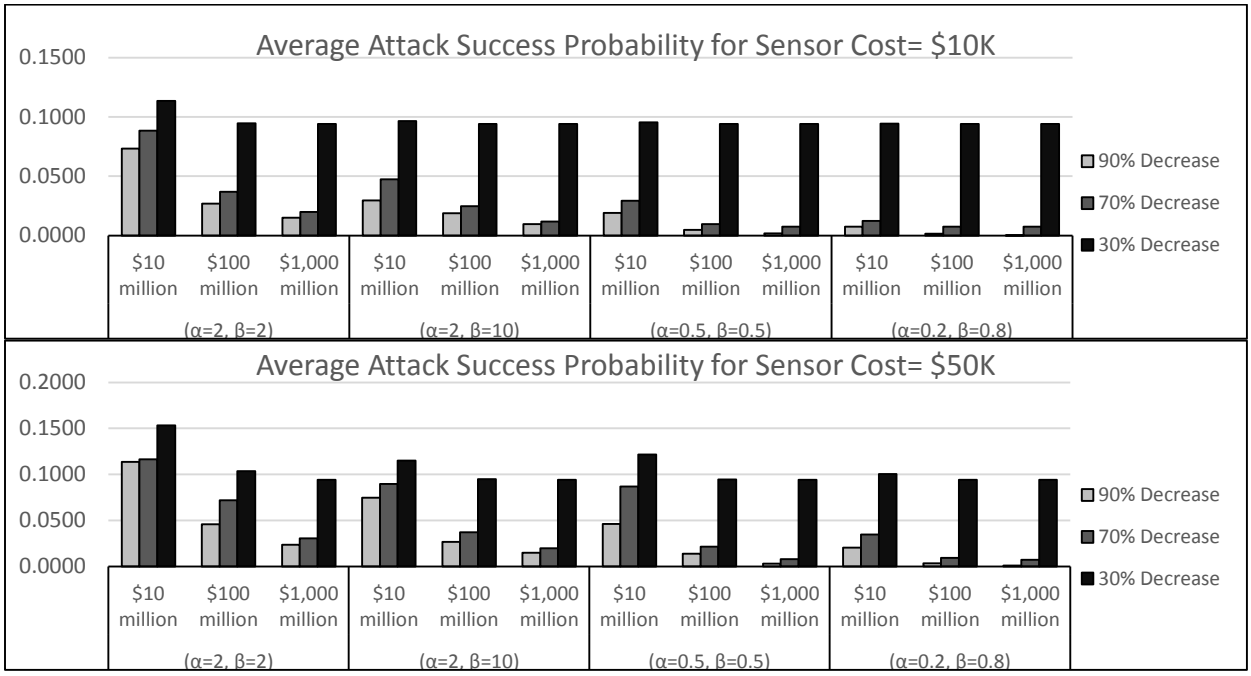

Figure 4.58 The average attack success probabilities for different defensive investment effectiveness, when p_{ij} is generated from Uniform(0.5, 0.8)

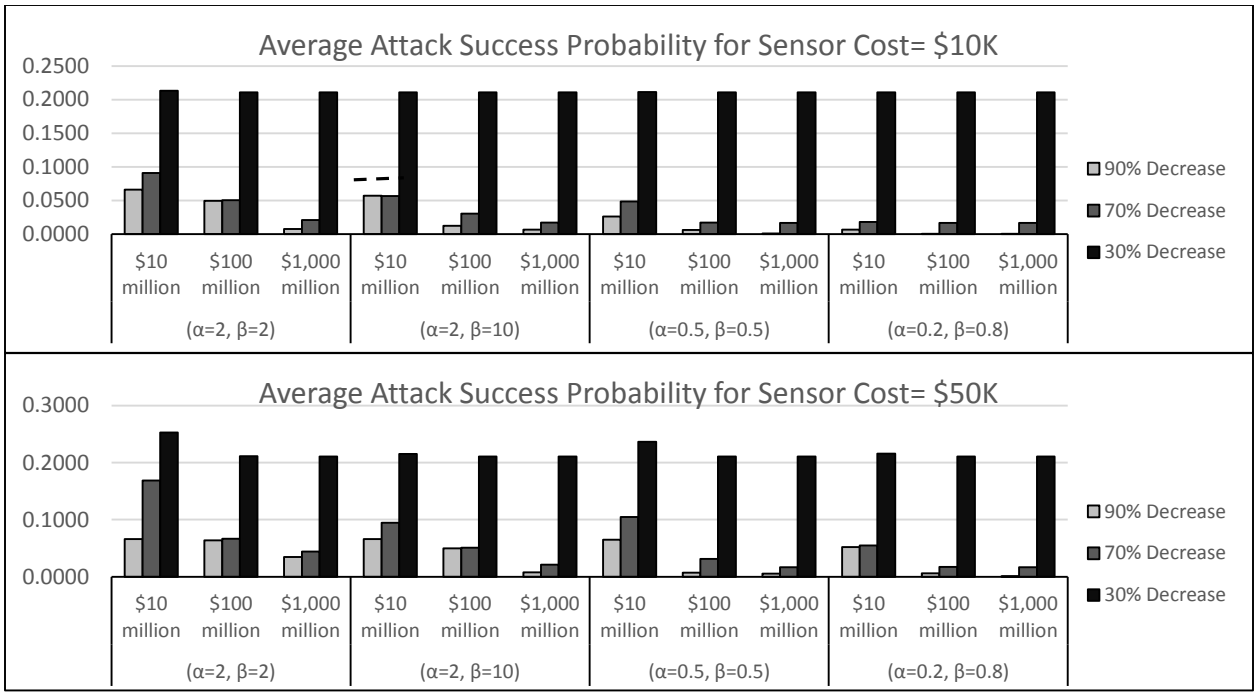

Figure 4.59 The average attack success probabilities for different defensive investment effectiveness, when p_{ij} is generated from U(0.7, 1)

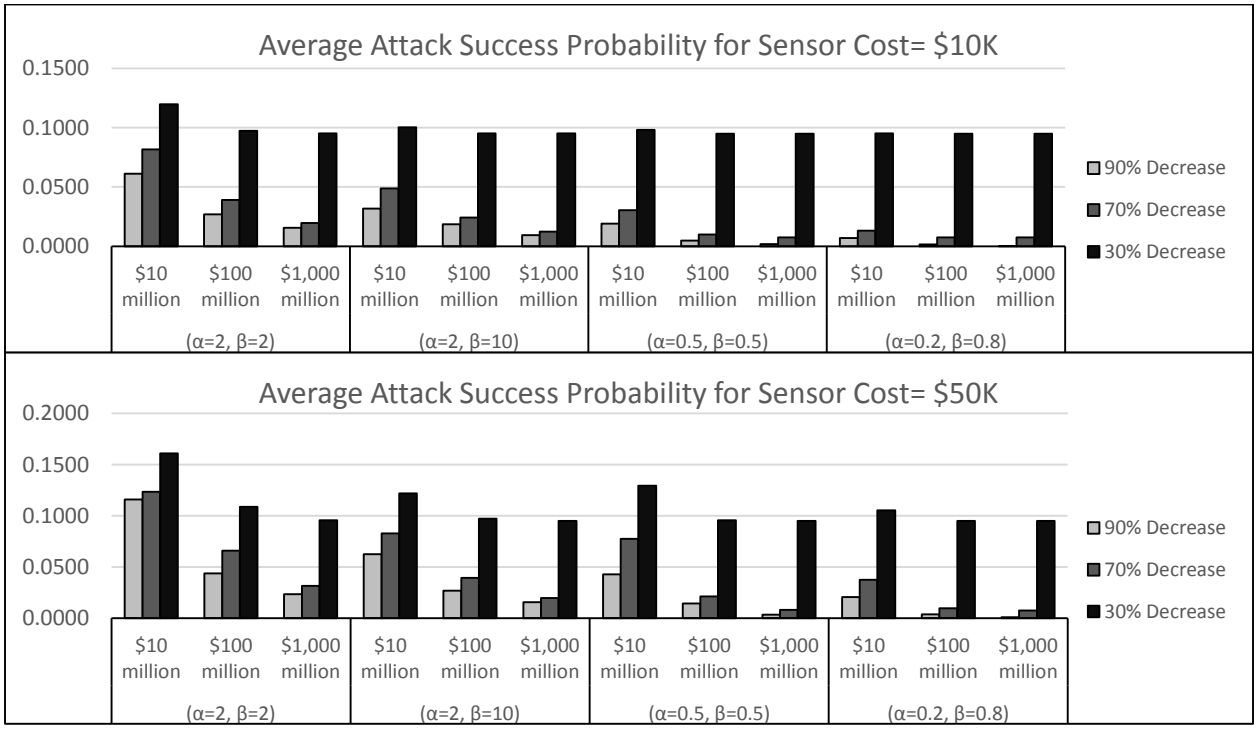

Figure 4.60 The average attack success probabilities for different defensive investment effectiveness, when p_{ij} is generated from U(0.4, 0.9)

Finally, we examine the impact of the shape of the deterrence function. As discussed previously, increasing β results in a lower deterrence probability for a given attack success probability. Therefore, in cases with larger β, deterring an attack is more difficult. For both S-shaped and reverse S-shaped deterrence functions, the average attack success probability is smaller when β is large (see the decrease when moving from left to right within any given pair of bars in Figures 4.61-4.63). However, for 30 out of the 108 cases, the difference is less than the standard error of the results (highlighted with a dotted line over the bars). This is consistent with the earlier results presented in Figures 4.19-4.21, showing that when β is large, the defender optimally chooses to protect more arcs to compensate for the greater difficulty of deterrence probability.

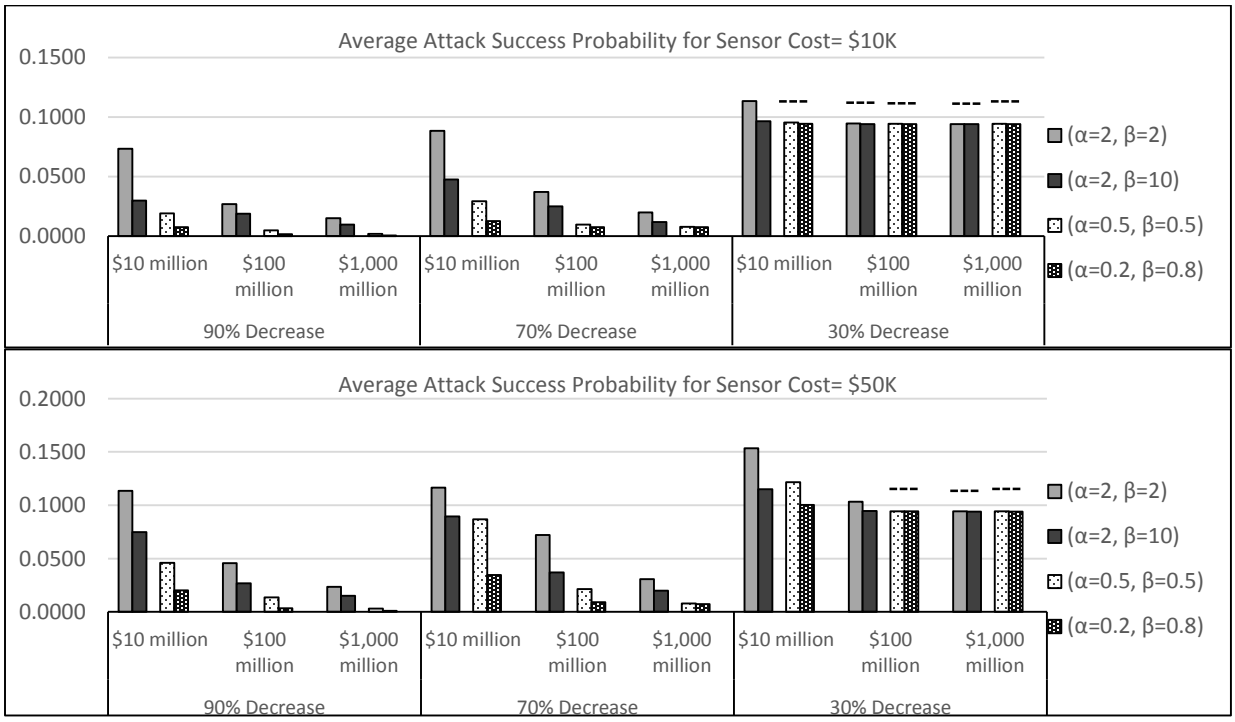

Figure 4.61 The average attack success probabilities for different shape of deterrence function, when p_{ij} is generated from Uniform(0.5, 0.8)

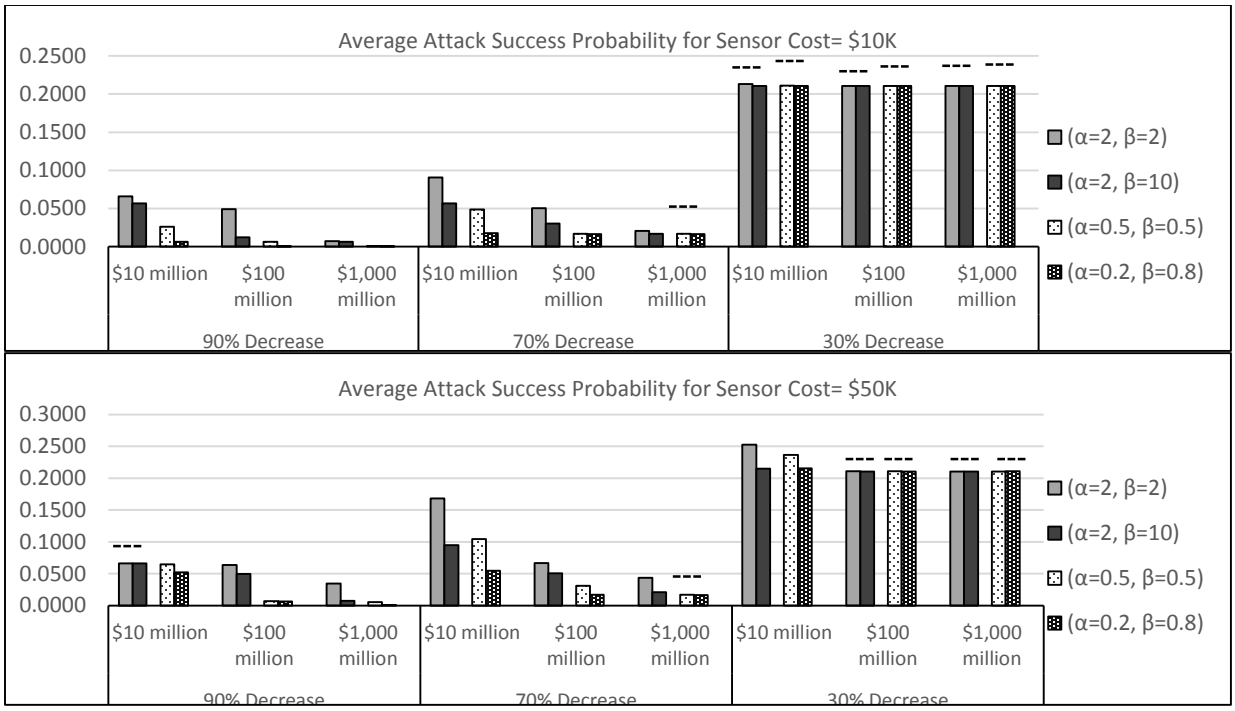

Figure 4.62 The average attack success probabilities for different shape of deterrence function, when p_{ij} is generated from Uniform(0.7, 1)

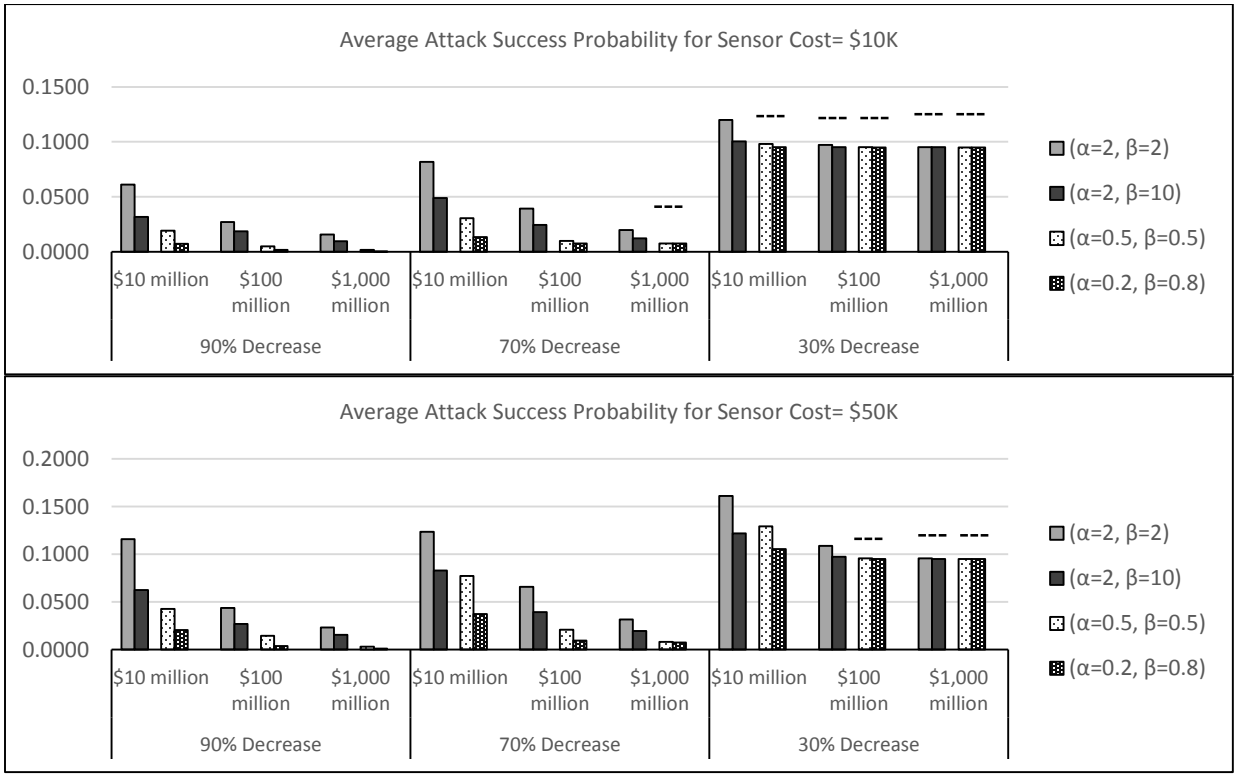

Figure 4.63 The average attack success probabilities for different shape of deterrence function, when p_{ij} is generated from Uniform(0.4, 0.9)

4.4.4 Sensitivity Analysis for the Average Deterrence Probability

The deterrence probability and the attack success probability are inversely related. Therefore, as expected, we found that for all parameters except the shape of the deterrence function and the variance of the distribution for the p_{ij}, if the success probability was observed to be increasing in a given parameter, then the deterrence probability was decreasing. Likewise, when a parameter had no significant effect on the success probability, we also observed no significant effect on the deterrence probability. Thus, those results are not shown here.

When considering the variance of the arc success probabilities, there are a few cases where a larger variance has no significant effect on the overall attack success probability, but leads to a significant decrease in the deterrence probability (due to the nonlinearity of the deterrence function). However, in most cases, the effect of the variance on the deterrence probability is again inversely related to its effect on the attack success probability, as expected. Therefore, in this section, we focus exclusively on how the deterrence probability depends on the shape of the deterrence function.

As discussed previously, increasing β makes deterrence more difficult to achieve for a given success probability. Thus, as expected, for both S-shaped and reverse S-shaped deterrence functions, the average deterrence probability was smaller for large values of β in 105 out of 108 cases. (The three cases where this is not true are highlighted by "↗".) This is shown by the decrease when moving from left to right for most pairs of bars in Figures 4.64-4.66. Moreover, this difference is larger than the standard error of the results. In fact, even though the defender optimally chooses to protect more arcs when β is large (as shown in Figures 4.19-4.21), this added investment is not enough to compensate for the greater difficulty of achieving deterrence for large values of β.

As noted above, in 3 out of 108 cases (all of them associated with S-shaped deterrence functions and highly effective defenses), we find the opposite effect. For those cases, the defender optimally chooses to protect many more arcs when β is large (as shown in Figures 4.19 and 4.20), and is therefore able to achieve a significantly larger deterrence probability, despite the large value of β.

We also observe that the decrease in deterrence probabilities for large values of β is much larger for reverse S-shaped deterrence functions (the dotted bars in Figures 4.64-4.66) than for S-shaped deterrence functions (the grey shaded bars). This makes sense, since with reverse S-shaped deterrence functions, the deterrence probability is a much steeper function of the success probability (for low values of the success probability, as we generally have at optimality) than with an S-shaped deterrence function when β is large (see Figure 3.14).

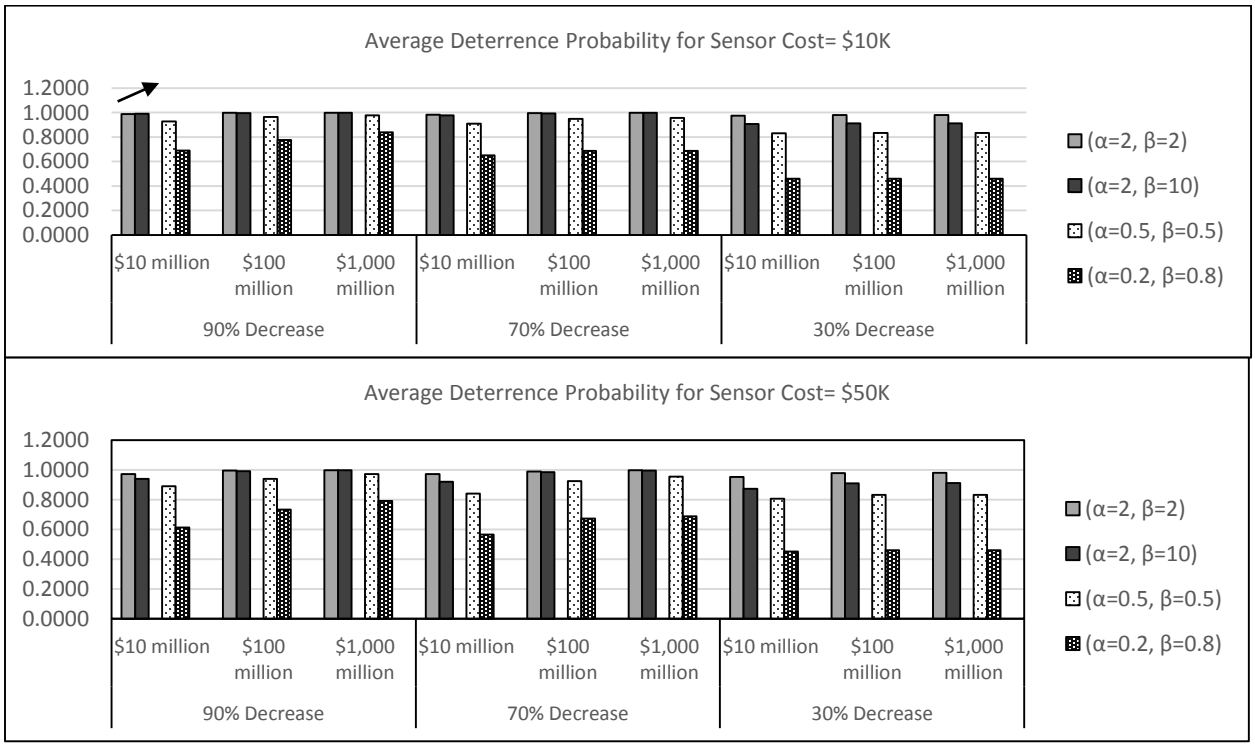

Figure 4.64 The average deterrence probabilities for different shape of deterrence function, when p_{ij} is generated from Uniform(0.5, 0.8)

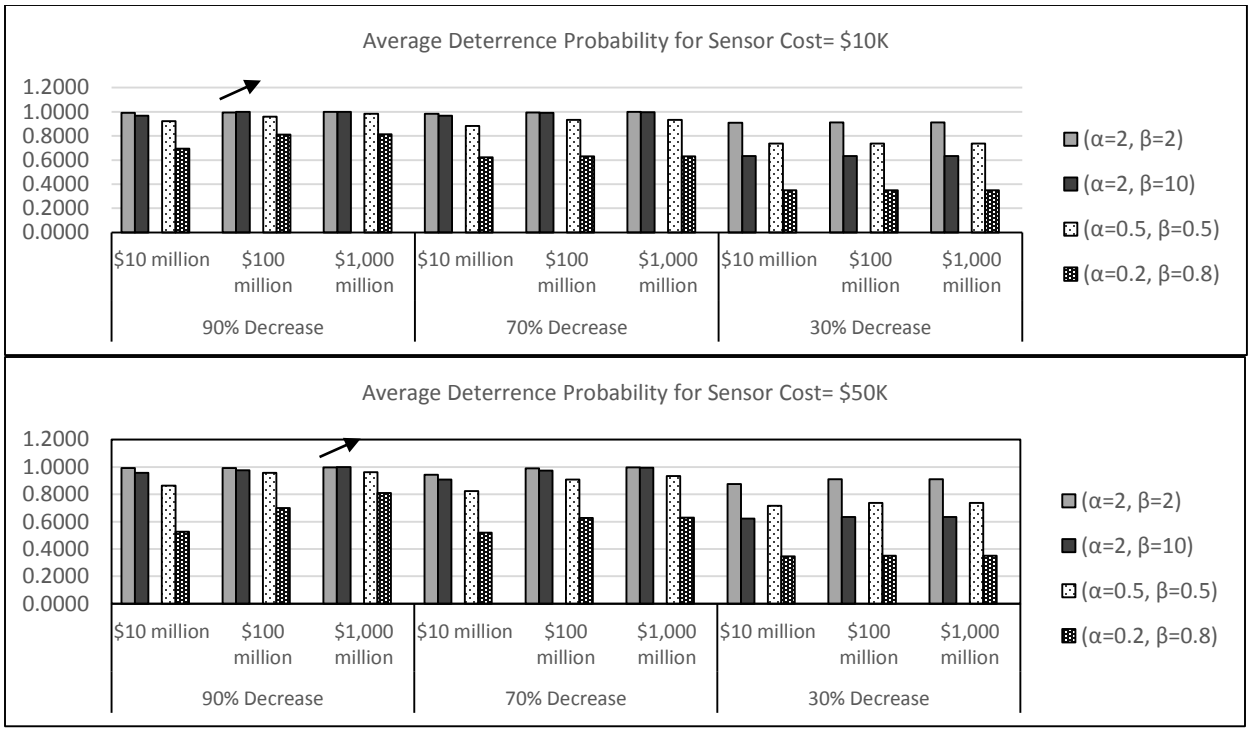

Figure 4.65 The average deterrence probabilities for different shape of deterrence function, when p_{ij} is generated from Uniform(0.7, 1)

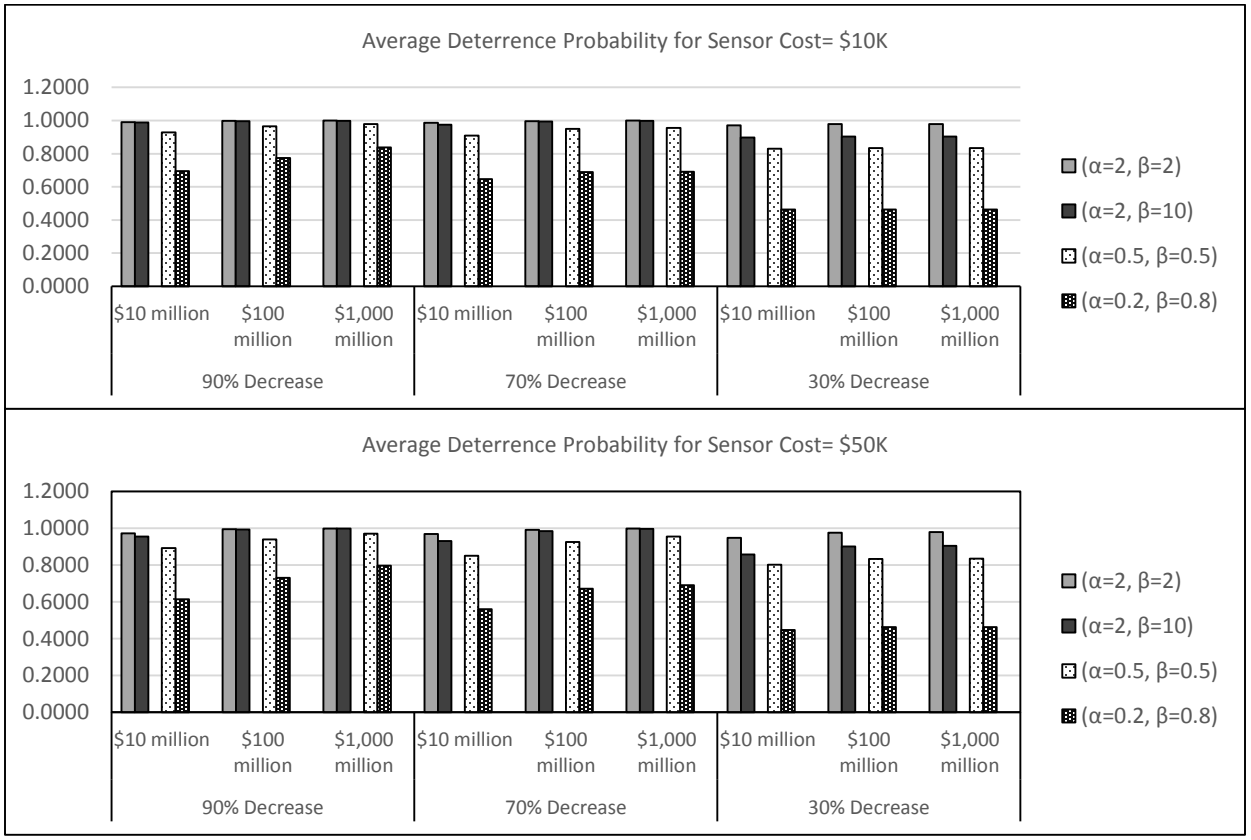

Figure 4.66 The average deterrence probabilities for different shape of deterrence function, when p_{ij} is generated from Uniform(0.4, 0.9)

4.4.5 General Discussion of Results for the Northridge Network

In previous sections, we presented the results of detailed sensitivity analysis for the Lancaster-Palmdale network. In this section, we discuss the similarities and differences between the results for the Northridge and Lancaster-Palmdale networks. Detailed results for the Northridge network are presented in Appendix B. We also summarize the comparison in Tables 4.2-4.6.

As in the Lancaster-Palmdale network, for a given variance of the arc success probabilities, the distribution with the higher mean results in a higher number of protected arcs (see Figures B1-B4 and Table 4.2). Also, for a given mean success probability, the distribution with the higher variance usually results in a higher number of protected arcs. However, in 5 of 72 cases, a higher variance is associated with a smaller number of protected arcs (as opposed to only one case for the Lancaster-Palmdale network), and in 19 of 72 cases the difference between the results for high and low variance is smaller than the standard errors of the results (see Figures B5-B8 and Table 4.2).

The numbers of arcs protected for the two networks depend in a similar manner on the target value L. In all cases, as the target value increases, the number of arcs that the defender optimally chooses to protect is either increasing or constant, but never decreasing (see Figures B9-B11 and Table 4.2).

Unsurprisingly, the defender optimally always chooses to protect fewer arcs for a high protection cost than for a low protection cost, as in the Lancaster-Palmdale network. However, in 16 of the 108 cases, the effect of sensor cost is less than the standard errors of the results (see Figures B12-B15 and Table 4.2).

Again, the number of arcs protected depends in a similar manner on the effectiveness of defensive investment for the two networks (see Figures B16-B18 and Table 4.3). However, for the Northridge network, we observe only 2 cases in which the number of arcs protected is initially

decreasing and then increasing (contrary to expectations), compared to 6 of 72 cases for the Lancaster-Palmdale network.

The shape of the deterrence function also has the same effect on the optimal number of protected arcs in both networks. For both S-shaped and reverse S-shaped deterrence functions, more arcs need to be protected for larger values of β (see Figures B19-B21 and Table 4.2).

The results for the defender's objective function are all either in the expected direction or insignificant for the Northridge network, except for 4 of 72 cases (highlighted in bold in Table 4.4), in which the objective value is larger (i.e., worse) when the variance of the distribution for the arc success probabilities is small. Therefore, we omit figures for the defender objective function from Appendix B, since the results are so similar to those for the Lancaster-Palmdale network, but we summarize the results.

As in section 4.3.3, we are not able to give a simple general result for how the mean and variance of the distribution of arc success probabilities affect the overall attack success probability (see Figures B22-B29 and Table 4.5). However, the distribution with the higher mean always results in a higher overall attack success probability when the effectiveness of defensive investment is low (30%), as in the Lancaster-Palmdale network (see the last three sets of bars in Figures B22-B25).

Again, the attack success probability depends in a similar manner on the target value L for the two networks. In most cases, the overall attack success probability is decreasing as the target value increases, but in 19 of the 72 cases, the effect of different target values is smaller than the standard error of the results (see Figures B30-B32 and Table 4.5).

As in the Lancaster-Palmdale network, the average overall attack success probability is usually smaller when the protection cost is low. However, in 17 of the 108 cases, the difference in

attack success probabilities between cases with large and small protection costs is less than the standard errors of the results (see Figures B33-B36 and Table 4.5).

The effectiveness of defensive investment also has a similar effect on the overall average attack success probability in both networks. For 68 of the 72 cases, as the effectiveness of defense decreases, the average attack success probability increases; in the remaining 4 cases, the difference between the results is smaller than the standard error of the results (see Figures B37-B39 and Table 4.5). Finally, the effects of the deterrence function on both the attack success probability and the deterrence probability are similar for the two networks (see Figures B40-B45 and Tables 4.5 -4.6).

Although in general the results are similar for the two networks, we can observe from figures in Appendix B that in the Northridge network, the defender is often able to achieve a small attack success probability with less investment (fewer arcs protected) than in the Lancaster-Palmdale network. This may be because the attacker needs to traverse more arcs to reach the desired target in the Northridge network, so the network is inherently better protected even in the absence of any defensive investment.

Increase in:	Network					
	Lancaster-Palmdale			Northridge		
	Increasing	No Significant Difference	Decreasing	Increasing	No Significant Difference	Decreasing
Mean of Arc Successes Probability	72 of 72	—	—	72 of 72	—	—
Variance of Arc Successes Probability	51 of 72	20 of 72	1 of 72	48 of 72	19 of 72	5 of 72
Target Value	122 of 144	22 of 144	—	130 of 144	14 of 144	—
Protection Cost	—	21 of 108	87 of 108	—	16 of 108	92 of 108
Shape Parameter of Deterrence Function β	91 of 108	17 of 108	—	93 of 108	15 of 108	—

Table 4.2 The effect of various parameters on the average optimal number of arcs protected

Network									
Lancaster-Palmdale					Northridge				
				- - - -					- - - -
40 of 72	21 of 72	2 of 72	6 of 72	3 of 72	17 of 72	51 of 72	—	2 of 72	2 of 72

Table 4.3 The effect of effectiveness of defensive investment on the average optimal number of arcs protected

Increase in:	Network					
	Lancaster-Palmdale			Northridge		
	Increasing	No Significant Difference	Decreasing	Increasing	No Significant Difference	Decreasing
Mean of Arc Successes Probability	72 of 72	—	—	72 of 72	—	—
Variance of Arc Successes Probability	47 of 72	25 of 72	—	55 of 72	13 of 72	**4 of 72**
Target Value	144 of 144	—	—	144 of 144	—	—
Protection Cost	98 of 108	10 of 108	—	102 of 108	6 of 108	—
Effectiveness of Defensive Investment	—	1 of 72	71 of 72	—	2 of 72	70 of 72
Shape Parameter of Deterrence Function β	108 of 108	—	—	108 of 108	—	—

Table 4.4 The effect of various parameters on the defender's optimal objective function value

Increase in:	Network					
	Lancaster-Palmdale			Northridge		
	Increasing	No Significant Difference	Decreasing	Increasing	No Significant Difference	Decreasing
Mean of Arc Successes Probability	59 of 72	—	13 of 72	57 of 72	5 of 72	10 of 72
Variance of Arc Successes Probability	11 of 72	53 of 72	8 of 72	28 of 72	23 of 72	11 of 72
Target Value	—	35 of 144	109 of 144	—	19 of 144	125 of 144
Protection Cost	—	28 of 108	80 of 108	—	17 of 108	91 of 108
Effectiveness of Defensive Investment	—	1 of 72	71 of 72	—	4 of 72	68 of 72
Shape Parameter of Deterrence Function β	—	30 of 108	78 of 108	—	17 of 108	91 of 108

Table 4.5 The effect of various parameters on the average attack success probability

Increase in:	Network					
	Lancaster-Palmdale			Northridge		
	Increasing	Decreasing	No Significant Difference	Increasing	Decreasing	No Significant Difference
Shape Parameter of Deterrence Function β	3 of 108	105 of 108	—	2 of 108	106 of 108	—

Table 4.6The effect of the shape of the deterrence function on the average deterrence probability

5 The Model with Multiple Possible Targets to Attack

In this chapter, we extend our previous model to consider situations in which the attacker can choose one among multiple possible targets, and will choose the best source node at which to enter the network for the chosen target. In many stochastic network interdiction models, the attacker's target choice is known by the defender only through a probability distribution [45]. This probability distribution is usually decided exogenously, ignoring factors such as the attractiveness of targets to the attacker and the attack success probabilities. However, in realistic cases, the attacker will presumably consider both the value of the target, and the likelihood of a successful attack. Thus, the attacker choice of target should ideally be decided endogenously.

In a fully endogenous model [24], the attacker may have his own valuation of each target, with the defender being uncertain about this valuation. In such a model, the attacker makes a deterministic choice of target, taking into account his target valuations and the success probabilities, but the defender is uncertain about the attacker choice (based on uncertainty about the target valuations). However, in or work, we assume that both the defender and the attacker have the same valuation for each target.

Major [70] proposes that the probability of selecting a given target could be proportional to the square root of the target value. Another common choice is a logit model [71] in which the choice probabilities A_k are related to the valuations λ_k by $A_k = \exp(\lambda_k) / \sum_i \exp(\lambda_i)$. Luce [72] proposes a simpler model in which the probability of choosing option k is given by $A_k = \lambda_k / \sum_i \lambda_i$.

In theory, one might consider adopting a model similar to Luce choice: e.g., letting the probability of a given target choice be proportional to the expected loss from an attack on that target:

$$A_k = \frac{L_k P_k}{\sum_i L_i P_i} \quad (5.1)$$

where L_k is the value of target k, and p_k is the probability of the attacker reaching that target given an optimal defender choice of sensors and an optimal attack choice of attack paths.

However, we chose to assume that the defender minimizes the worst case scenario. In particular, the defender calculates the expected damage for every individual target (given by the probability of successfully reaching that target, times the target value, times the probability of failing to deter an attack), and minimizes the highest expected loss plus the investment in protection. The new model is appropriately conservative, since the attacker is assumed to choose the best action with probability one, rather than choosing targets proportional to their attractiveness.

Ideally, it may have made more sense to assume that the attacker deterrence decision is a function of success probability times target value (rather than being a function of success probability alone). In particular, the current model (where the deterrence is a function of success probability alone) could in principle result in cases where the attacker chooses a target that does not have the highest product of success probability and target value, if the target with the highest product has a high target value but a low success probability (leading to a high probability of the attacker being deterred). However, making deterrence depend on target value would have necessitated a different choice for the deterrence function than Kumaraswamy distribution, since that function is defined only over [0, 1]. Therefore, for consistency with the previous sections, we kept the Kumaraswamy deterrence function and assumed that attacker deterrence is a function of only the attack success probability.

5.1 Problem Formulation for the Model with Multiple Possible Targets

In this section, we present our model, in which the attacker first chooses the best source node from which to enter the network for each choice of target, and then chooses the target that maximizes expected damage (as given the probability of reaching a target, times the target value, times the probability of the attack not being deterred). The defender then minimizes the expected loss plus the investment in protection, by choosing which arcs to protect to reduce the attacker's success probability (and hopefully deter the attack). The notation and the resulting model formulation are given below.

Notation:

D (N, A): Directed graph with nodes *N* and arcs *A*

FS (i): Set of arcs leaving node *i*

RS (i): set of arcs entering node *i*

AD: The set of arcs in which the defender can invest

c_{ij}: Cost of protecting arc (*i,j*)

p_{ij}: Probability that the attacker can traverse arc (*i,j*) if it is not protected

q_{ij}: Probability that the attacker can traverse arc (*i,j*) if it is protected

x_{ij}: Defender's decision variable, which is 1 if the defender protects arc (*i,j*), and 0 otherwise.

y_{ij}: Probability that the attacker reaches node *i* and the chosen path includes arc *(i,j)*

α, β: Shape parameters of the Kumaraswamy distribution

y_{t^k}: The probability of reaching the target given that the target is node k

L_k : The value of target *k*

Model formulation:

$$\min_{x} \max_{k} \left[1 - P_d^k(Q_k(x))\right] Q_k(x) L_k + \sum_{(i,j)\in AD} c_{ij}\, x_{ij} \tag{5.2}$$

$$P_d^k(Q_k(x)) = \left(1 - y_{t^k}^{\alpha}\right)^{\beta} \tag{5.3}$$

$$Q_k(x) = \max_{y,z} y_{t^k} \quad \text{for } \forall k \tag{5.4}$$

$$\sum_{(s,j)\in FS(s)} (y_{sj} + z_{sj}) = 1 \tag{5.5}$$

$$\sum_{(i,j)\in FS(i)} (y_{ij} + z_{ij}) - \sum_{(m,i)\in RS(i)} (p_{mi} y'_{mi} + q_{mi} z'_{mi}) = 0 \quad for\ i \in N\backslash\{s, t^k\} \tag{5.6}$$

$$y_{t^k} = \sum_{(i,t^k)\in RS(t^k)} (p_{jt^k} y_{jt^k} + q_{jt^k} z_{jt^k}) \tag{5.7}$$

$$0 \le y_{ij} \le 1 - x_{ij} \qquad for\ (i,j) \in A \tag{5.8}$$

$$0 \le z_{ij} \qquad for\ (i,j) \in AD \tag{5.9}$$

$$x_{ij} \in \{0,1\} \qquad y_{ij} \ge 0 \quad z_{ij} \ge 0$$

Here, in Equation 5.2 the defender minimizes the maximum expected damage (given by the probability of the attacker reaching a target, times the target value, times the probability of failing to deter an attack), plus the investment in protection. Equation 5.3 calculates the probability of deterrence, as in section 4.2. Equations 5.4-5.9 then represent the attacker decisions, in which the attacker solves a series of problems similar to those in section 4.2, one for each possible target *k*.

5.2 Solution Approach

The model presented in the previous section is a min-max bi-level optimization model, and cannot be solved with standard mixed-integer programming methods. Therefore, we reformulate the defender problem to facilitate solution. We first reformulate the defender's objective function

as given in equation 5.10, and add constraint 5.11 to let the variable Q represents the largest expected loss.

$$\min\ Q + \sum_{(i,j)\in AD} c_{ij}\, x_{ij} \tag{5.10}$$

$$Q \geq \left(1 - P_d^k(Q_k(x))\right)\, Q_k(x) L_k \qquad \text{for } \forall\, k \tag{5.11}$$

As noted earlier, the inner (attacker) problem presented in equations 5.4-5.9 above is a variation of the attacker problem studied in chapter 4. In fact, in this model, the attacker solves a series of similar problems, one for each possible target *k* (maximizing the success probability of reaching target *k*). Therefore, we used a similar approach as in section 4 (the duality approach of Morton [45]) to solve these problems. In particular, we take the dual of the attacker problems given in equations 5.4-5.9 to create a single non-nested minimization problem. The resulting new formulation is as follows:

$$\min\ Q + \sum_{(i,j)\in AD} c_{ij}\, x_{ij} \tag{5.12}$$

$$Q \geq (1 - P_d^k(Q_k)) Q_k L_k \qquad \text{for } \forall\, k \tag{5.13}$$

$$Q_k = \omega_{s^k} \qquad \text{for } \forall k \tag{5.14}$$

$$\omega_i - p_{ij}\omega_j \geq 0 \qquad for\ (i,j) \in A \backslash AD \tag{5.15}$$

$$\omega_i - p_{ij}\omega_j \geq -x_{ij} \qquad for\ (i,j) \in AD \tag{5.16}$$

$$\omega_i - q_{ij}\omega_j \geq 0 \qquad for\ (i,j) \in AD \tag{5.17}$$

$$\omega_{t^k} = 1 \tag{5.18}$$

where the ω_i are dual variables, ω_{s^k} is the success probability of reaching target *k*, and Q is the maximum expected damage. As above, Equation 5.12 is the defender's objective function, and Equation 5.13 ensures that Q is the maximum expected damage. Equations 5.14-5.18 then represent the attacker problem, as in section 4.3.

However, constraint 5.13 is non-convex, which makes this problem computationally difficult to solve for large instances. Therefore, we linearize this function by using the piecewise

linear approximation method introduced by Sherali [66]. Thus, as in section 4.3, we introduce variables a, λ, μ, and α where the $a_{n,k}$ represent the endpoints of the piecewise linear segments, and $\lambda_{n,k}$and $\mu_{n,k}$ ($\lambda_{n,k}+\mu_{n,k} = \alpha_{n,k}$) are weights on the left and right endpoints, respectively, chosen yield a chosen point on the nth line segment. We can then replace equation 5.13 with equation 5.20 and equations 5.24-5.27. We solve the resulting model using the GUROBI MIP solver. The final model formulation is as follows:

$$\min\ Q + \sum_{(i,j)\in AD} c_{ij}\, x_{ij} \tag{5.19}$$

$$Q \geq \sum_{n=0}^{r} \left[f\left(a_{n,k}\right)\lambda_{n,k} + f\left(a_{n+1,k}\right)\mu_{n,k} \right] \qquad \text{for } \forall k \tag{5.20}$$

$$\omega_i - p_{ij}\omega_j \geq 0 \qquad for\ (i,j) \in A\backslash AD \tag{5.21}$$

$$\omega_i - p_{ij}\omega_j \geq -x_{ij} \qquad for\ (i,j) \in AD \tag{5.22}$$

$$\omega_i - q_{ij}\omega_j \geq 0 \qquad for\ (i,j) \in AD \tag{5.23}$$

$$\omega_{t^k} = 1$$

$$\omega_{s^k} = \sum_{n=0}^{r} (a_{n,k}\lambda_{n,k} + a_{n+1,k}\mu_{n,k}) \qquad for\ \forall k \tag{5.24}$$

$$\lambda_{n,k}+\mu_{n,k} = \alpha_{n,k} \qquad for\ \forall k\ \ and\ n = 1 \ldots r \tag{5.25}$$

$$\sum_{n=1}^{r} \alpha_{n,k} \ = 1 \qquad for\ \forall k \tag{5.26}$$

$$\lambda_{n,k}, \mu_{n,k} \geq 0 \qquad for\ \forall k\ \ and\ n = 1 \ldots r \tag{5.27}$$

$\alpha_n \ \in \{0,1\} \quad x_{ij} \in \{0,1\}$

where $f\left(a_{n,k}\right) = \left(1 - \left(1 - a_{n,k}^{\alpha}\right)^{\beta}\right) a_{n,k} L_k$

5.3 Computational Results

In this section, we present our results for the Northridge network. For this network, we choose 10 possible entering nodes (allowing the attacker to choose the most favorable one) and 10 target nodes. In our analysis, we explore the effect of the availability of multiple targets to attack.

In particular, we investigate how the availability of multiple targets will influence the defender's protection decision. For example, we speculated that, under some circumstances (e.g., low defense cost), the defender could choose to protect more arcs in the presence of multiple targets, since there would be more possible targets that could be attacked. However, it is also possible that the defender may spend less in case of high defensive cost, since the need to defend multiple targets may make defense too costly. These hypotheses are explored below.

With regard to which target will be attacked, we explore cases with two and ten possible targets. We believe these cases are adequate to explore how the defender's optimal investment behavior depends on availability of multiple targets. Also, these numbers of targets are typical for other applications; for example, the Northridge network in our study has only one target (Airport) when the threat level is green, and a maximum of 23 targets when the threat level is red [64]. As before, the target values will span a wide range ($10 million, $100 million, and $1000 million). Of course, there can be higher target values (with values of billions of dollars) in larger networks, but we believe this range of values is appropriate for the network we are studying. We systematically change the target values within that range in the following manner. We make one target the most attractive (with a value of $1000 million), and let the rest of the targets have equal values (either $10 million or $100 million). We then let each target in the two-target case (for four target combinations), and two of the 10 targets in the 10 target case (for four target combinations), be the highest valued target, so that we can explore how target values and locations affect the optimal resource allocation.

We also vary the defense cost per arc to explore how the cost of defense affects the optimal defender behavior. In particular, we previously considered defense costs of $10K and $50K in

chapter 4. We now add a defense cost of $200K, to allow us to investigate whether the defender stops protecting when defending becomes too costly.

Another question we explore is the effect of multiple targets on the choice of which arcs to protect (rather than just the number of protected arcs). In particular, we compare the single target case to the multiple-target case. For example, prior to our analysis, we hypothesize that the arcs to be protected in the face of multiple targets would be spread out more broadly through the network than in the case of a single target. We do not have a specific measure to assess how broadly the protected arcs are spread out through the network, and simply assess this visually (for example, checking whether the protected arcs tend to be closer to each other when there is a single target than when there are multiple targets.

We do not explore the effect of all parameters considered in chapter 4 due to the greater computation time required to solve the multiple-target model. In particular, we use only the U(0.7, 1) distribution for arc success probabilities, since the other distributions used in chapter 4 yielded extremely low overall attack success probabilities even in the absence of protection. Similarly, for the effectiveness of defensive investments, we considered only a 70% decrease. We likewise use only (α=2, β=10) for the shape parameters of the deterrence function, since S-shaped deterrence function seems more reasonable for terrorism, but (α=2, β=2) gives unrealistically high deterrence probabilities. Finally, we use only the Northridge network in our analysis, since the targets in that network are spread widely through the network, enabling us to explore the effect of target location on the defender's optimal sensor placement.

Sensitivity Analysis	Shape Parameters (α=2, β=10)	Network (Northridge)	Effectiveness of Defense (70% decrease)	Target Value Combinations	Sensor Cost	Distributions for the Arc Success Probabilities	Total Runs
Number of Cases	1	1	1	2*2+2*2=8	3	1	24

Table 5.1 Total number of cases and total number of runs for the multiple target model

In our analysis, we use the GUROBI solver, which solves our problem in reasonably less computation time than the CPLEX solver. We were able to find an optimal solution for our linearized multiple target model (with 1000 linear segments). We ran the multiple target model on a computer with an Intel(R) Core(TM)2 CPU 2.13 GHz processor and 4 GB RAM. The results indicate that the computation time is sensitive to the location of the most valuable target and the number of targets. In particular, as the number of target increases, the required computation time also increases. Moreover, the computation time is larger when the most valuable target is located near center of the network. The approximate average computation time for the cases with a single target located at the edge of the network is seven hours, and for the cases with ten targets and the most valuable target is located near center of the network is 120 hours for 20 replications.

5.3.1 Comparison for cases with different numbers of possible targets

We now present results for cases with a single target, two targets, and ten targets, and explore how the number of possible targets affects the optimal number of arcs protected. We also explore the effect of the most valuable target's location. We then explore the effect of protection cost on the number of arcs protected in cases with multiple targets. Finally, we explore how the number of targets affects the locations of the protected arcs (rather than just their numbers). Since the computation time for the multiple-target case does not allow us to have the same precision as in chapter 4, we cannot rely on the averages of multiple replications. Instead of comparing the average of the replications, we therefore rely on nonparametric case-by-case comparison for 20 replications to see how the number of possible targets affects the optimal number of arcs protected.

Tables 5.2-5.4 present the optimal number of arcs protected for protection costs of \$10K, \$50K, and \$200K, respectively. In each table, the first two sets of columns present results when the most valuable target is at node 277 (located near the center of the network), and the last two

sets of columns present results when the most valuable target is at node 285 (located at the edge of the network).

Results in Tables 5.2-5.4 show that increasing the number of targets from one to two results in more arcs protected in 128 of 240 cases (highlighted with "*"), no effect in 109 cases, and a decrease in only three cases (highlighted in bold). Similarly, increasing the number of targets from two to ten leads to more arcs protected in 189 of 240 cases (highlighted with "*"), no effect in 47 cases and a decrease in only four cases (highlighted in bold). These results strongly suggest that the number of targets has an important effect on the number of arcs protected at optimality.

We used nonparametric statistics (sign test) to test whether these results could have occurred by chance. In particular, Table 5.2 shows the chance that this pattern would be observed, if in reality there was no significant effect of the number of targets. Note that the significance level is vanishingly small for most cases, especially when the most valuable target node is located at the periphery of the network.

	Node 277 =Most Valuable Other targets= 100M		Node 277= Most Valuable Other targets= 10M		Node 285= Most Valuable Other targets= 100M		Node 285= Most Valuable Other targets=10M	
Protection Cost	1 target to 2 target	2 target to 10 target	1 target to 2 target	2 target to 10 target	1 target to 2 target	2 target to 10 target	1 target to 2 target	2 target to 10 target
$10K	p=0.0898	p < 0.0001	-	p=0.75	p < 0.0001	p < 0.0001	p < 0.0001	p < 0.0001
$50K	-	p=0.0002	-	p=0.0005	p < 0.0001	p < 0.0001	p < 0.0001	p < 0.0001
$200K	p=0.75	p < 0.0001	-	p=0.5	p < 0.0001	p < 0.0001	p < 0.0001	p < 0.0001

Table 5.2 Probability of observing the pattern in our result without effect of the number of targets for different cases

The optimal number of arcs protected appears to be also sensitive to the location of the most valuable target. We consider two possible locations (circled nodes in Figure 5.1) for the most valuable target (node 277 and node 285). Node 277 is located near the center of the network, and has more connections with other nodes. On the other hand, node 285 is located at the edge of the network, and has few connections with other nodes. Figure 5.1 shows the protected arcs (dark lines) and the total number of protected arcs when the defensive cost is $10K, similar results also

hold for protection costs of $50K and $200K. This suggests that central locations, like node 277 is inherently more difficult to defend than peripheral locations, like node 285.

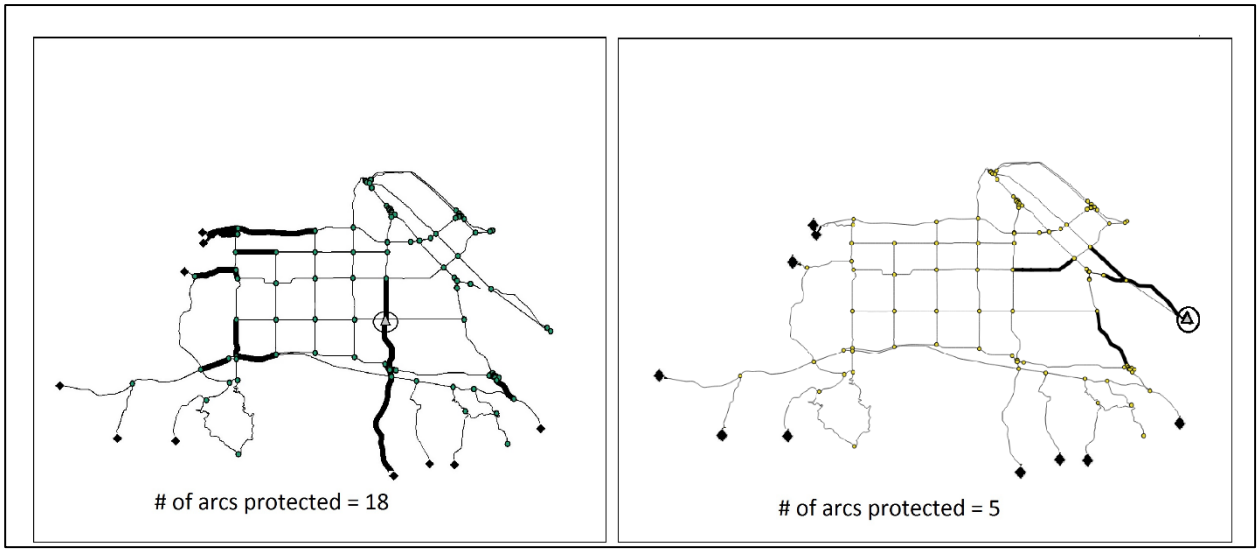

Figure 5.1 Protected arcs when target is node 277 (on the left) and when target is node 285 (on the right)

The defender rationally invests first in protecting the target with the largest expected loss, and then protects other targets as that target becomes less attractive. Since protecting node 285 is relatively easy, as the number of targets increases, the number of protected arcs also increases when the most valuable target is located at node 285 (see Tables 5.2-5.4). On the other hand, when the largest value target is located at node 277, the number of arcs protected is increasing in the number of targets only when the value of the other targets is $100M, as discussed in the previous nonparametric analysis. This is because, when the value of the other targets is only $10M, the defender will rarely be able to invest enough in defense of node 277 to make those other targets more attractive.

	Node 277 =Most Valuable Other targets= 100M			Node 277= Most Valuable Other targets= 10M			Node 285= Most Valuable Other targets= 100M			Node 285= Most Valuable Other targets=10M		
Rep. No	Single	Two	Ten	Single	Two	Ten	Single	Two	Ten	Single	Two	Ten
1	18	20*	24*	18	18	18	5	17*	23*	5	10*	16*
2	19	20*	27*	19	19	19	4	15*	25*	4	13*	17*
3	19	20*	26*	19	19	19	5	17*	26*	5	13*	17*
4	17	17	17	17	17	17	5	17*	17	5	12*	15*
5	18	18	25*	18	18	18	4	16*	24*	4	12*	16*
6	18	18	24*	18	18	19*	5	15*	21*	5	10*	17*
7	18	19*	25*	18	18	18	5	15*	25*	5	13*	16*
8	18	***17***	26*	18	18	18	4	17*	23*	4	12*	16*
9	20	20	27*	20	20	20	5	15*	24*	5	11*	16*
10	18	18	27*	18	18	18	5	16*	25*	5	12*	15*
11	19	20*	25*	19	19	***18***	5	13*	25*	5	13*	16*
12	20	20	21*	20	20	20	5	16*	25*	5	13*	16*
13	21	21	27*	21	21	21	4	15*	25*	4	12*	16*
14	18	18	25*	18	18	18	5	16*	20*	5	10*	17*
15	20	20	27*	20	20	20	5	15*	26*	5	14*	18*
16	20	***19***	25*	20	20	20	4	15*	22*	4	13*	17*
17	21	21	26*	21	21	21	5	16*	24*	5	11*	16*
18	19	19	25*	19	19	19	5	14*	23*	5	13*	17*
19	18	19*	26*	18	18	18	5	15*	25*	5	11*	16*
20	19	20*	26*	19	19	19	4	14*	25*	4	12*	17*

Table 5.3 The optimal number of protected arcs for different numbers of targets cases when protection cost is $10K (increase highlighted with "*", and decrease highlighted in bold)

	Node 277= Most Valuable Other targets= 100M			Node 277= Most Valuable Other targets= 10M			Node 285= Most Valuable Other targets= 100M			Node 285= Most Valuable Other targets= 10M		
Rep. No	Single	Two	Ten	Single	Two	Ten	Single	Two	Ten	Single	Two	Ten
1	16	16	18*	16	16	16	4	11*	18*	4	10*	14*
2	14	14	19*	14	14	14	4	13*	17*	4	8*	11*
3	15	15	19*	15	15	16*	5	12*	17*	5	7*	14*
4	17	17	17	17	17	17	4	12*	15*	4	7*	7
5	18	18	19*	18	18	18	2	11*	16*	2	9*	15*
6	14	14	17*	14	14	15*	3	9*	17*	3	7*	11*
7	16	16	18*	16	16	18*	3	11*	19*	3	10*	15*
8	17	17	19*	17	17	17	4	12*	17*	4	8*	14*
9	17	17	19*	17	17	18*	3	12*	16*	3	7*	15*
10	17	17	17	17	17	17	4	12*	15*	4	11*	15*
11	18	18	19*	18	18	18	4	12*	17*	4	7*	16*
12	14	14	20*	14	14	16*	5	13*	18*	5	8*	9*
13	14	14	19*	14	14	15*	2	11*	15*	2	8*	14*
14	15	15	19*	15	15	16*	4	11*	17*	4	8*	11*
15	19	19	20*	19	19	19	5	12*	17*	5	9*	16*
16	17	17	19*	17	17	18*	4	12*	16*	4	9*	14*
17	15	15	20*	15	15	17*	4	14*	18*	4	7*	15*
18	16	16	19*	16	16	17*	3	11*	16*	3	6*	11*
19	18	18	20*	18	18	18	3	11*	17*	3	11*	11*
20	16	16	20*	16	16	18*	4	12*	18*	4	8*	11*

Table 5.4 The optimal number of protected arcs for different numbers of targets cases when protection cost is \$50K (increase highlighted with "*", and decrease highlighted in bold)

	Node 277= Most Valuable Other Targets= 100M			Node 277= Most Valuable Other Targets = 10M			Node 285= Most Valuable Other Targets = 100M			Node 285= Most Valuable Other Targets = 10M		
Rep. No	Single	Two	Ten	Single	Two	Ten	Single	Two	Ten	Single	Two	Ten
1	12	12	18*	12	12	12	3	9*	13*	3	6*	8*
2	13	***11***	19*	13	13	13	4	9*	15*	4	6*	9*
3	10	11*	16*	10	10	10	4	10*	16*	4	6*	8*
4	11	11	17*	11	11	11	3	10*	13*	3	6*	7*
5	13	13	18*	13	13	15*	2	11*	15*	2	5*	9*
6	9	9	17*	9	9	10*	3	7*	16*	3	6*	8*
7	10	10	18*	10	10	10	3	11*	15*	3	6*	8*
8	13	13	16*	13	13	13	3	11*	13*	3	5*	9*
9	12	12	17*	12	12	***11***	3	9*	16*	3	5*	8*
10	14	14	17*	14	14	***10***	4	11*	15*	4	6*	7*
11	11	11	17*	11	11	11	3	11*	15*	3	6*	9*
12	12	12	18*	12	12	12	3	8*	15*	3	8*	9*
13	14	14	18*	14	14	***13***	2	7*	15*	2	7*	8*
14	10	10	15*	10	10	10	3	8*	15*	3	5*	9*
15	12	12	18*	12	12	12	3	11*	17*	3	7*	9*
16	12	12	17*	12	12	12	3	10*	15*	3	6*	9*
17	13	13	16*	13	13	13	3	8*	14*	3	6*	8*
18	10	10	16*	10	10	10	3	9*	16*	3	6*	8*
19	11	11	17*	11	11	11	3	11*	15*	3	6*	9*
20	12	12	17*	12	12	12	4	10*	15*	4	5*	10*

Table 5.5 The optimal number of protected arcs for different numbers of targets when protection cost is $200K (increase highlighted with "*", and decrease highlighted in bold)

Another parameter affecting the optimal number of arcs to protect is the cost of protecting an individual arc. As expected, the number of arcs protected usually decreases or stays constant (but never increases) as the protection cost increases (see Tables 5.5-5.6). (We omit the single-target case, since it was already presented in chapter 4.) In particular, in 284 of 320 cases, the number of arcs protected decreases as the protection cost increases; for the remaining 36 cases (highlighted with "#"), the number of arcs protected remains constant. Again, the chance that this pattern would be observed, without the effect of protection cost is smaller than 0.0001 for all cases. Thus, in general the defender optimally chooses to protect fewer arcs when defending an individual arc is more costly, consistent with the results in chapter 4.

	Node 277= Most Valuable Other Targets = 100M			Node 277= Most Valuable Other Targets = 10M			Node 285= Most Valuable Other Targets = 100M			Node 285= Most Valuable Other Targets = 10M		
Rep. No	$10K	$50K	$200K	$10K	$50K	$200K	$10K	$50K	$200K	$10K	$50K	$200K
1	20	16	12	18	16	12	17	11	9	10	10#	6
2	20	14	11	19	14	13	15	13	9	13	8	6
3	20	15	11	19	15	10	17	12	10	13	7	6
4	17	17#	11	17	17#	11	17	12	10	12	7	6
5	18	18#	13	18	18#	13	16	11	11#	12	9	5
6	18	14	9	18	14	9	15	9	7	10	7	6
7	19	16	10	18	16	10	15	11	11#	13	10	6
8	17	17#	13	18	17	13	17	12	11	12	8	5
9	20	17	12	20	17	12	15	12	9	11	7	5
10	18	17	14	18	17	14	16	12	11	12	11	6
11	20	18	11	19	18	11	13	12	11	13	7	6
12	20	14	12	20	14	12	16	13	8	13	8	8#
13	21	14	14#	21	14	14#	15	11	7	12	8	7
14	18	15	10	18	15	10	16	11	8	10	8	5
15	20	19	12	20	19	12	15	12	11	14	9	7
16	19	17	12	20	17	12	15	12	10	13	9	6
17	21	15	13	21	15	13	16	14	8	11	7	6
18	19	16	10	19	16	10	14	11	9	13	6	6#
19	19	18	11	18	18#	11	15	11	11#	11	11#	6
20	20	16	12	19	16	12	14	12	10	12	8	5

Table 5.6 The optimal number of protected arcs for different protection cost and two targets (no change highlighted with "#")

	Node 277= Most Valuable Other Targets = 100M			Node 277= Most Valuable Other Targets = 10M			Node 285= Most Valuable Other Targets = 100M			Node 285= Most Valuable Other Targets = 10M		
Rep. No	$10K	$50K	$200K	$10K	$50K	$200K	$10K	$50K	$200K	$10K	$50K	$200K
1	24	18	18#	18	16	12	23	18	13	16	14	8
2	27	19	19#	19	14	13	25	17	15	17	11	9
3	26	19	16	19	16	10	26	17	16	17	14	8
4	17	17#	17#	17	17#	11	17	15	13	15	7	7#
5	25	19	18	18	18#	15	24	16	15	16	15	9
6	24	17	17#	19	15	10	21	17	16	17	11	8
7	25	18	18#	18	18#	10	25	19	15	16	15	8
8	26	19	16	18	17	13	23	17	13	16	14	9
9	27	19	17	20	18	11	24	16	16#	16	15	8
10	27	17	17#	18	17	10	25	15	15#	15	15#	7
11	25	19	17	18	18#	11	25	17	15	16	16#	9
12	21	20	18	20	16	12	25	18	15	16	9	9#
13	27	19	18	21	15	13	25	15	15#	16	14	8
14	25	19	15	18	16	10	20	17	15	17	11	9
15	27	20	18	20	19	12	26	17	17#	18	16	9
16	25	19	17	20	18	12	22	16	15	17	14	9
17	26	20	16	21	17	13	24	18	14	16	15	8
18	25	19	16	19	17	10	23	16	16#	17	11	8
19	26	20	17	18	18#	11	25	17	15	16	11	9
20	26	20	17	19	18	12	25	18	15	17	11	10

Table 5.7 The optimal number of protected arcs for different protection cost and ten targets (no change highlighted with "#")

Finally, we explore how the number of targets affects the location of the protected targets. Figure 5.2 shows the protected arcs for cases with a single target (the upper figure), two targets (middle figure), and ten targets (the lower figure). As we suspected, when there are more targets, the defender appears to push the defense to peripheral arcs (see the lower figure in Figure 5.2). We also note that, while the number of arcs is increasing as the number of targets increases, the defender does not necessarily protect the same arcs as the number of targets changes.

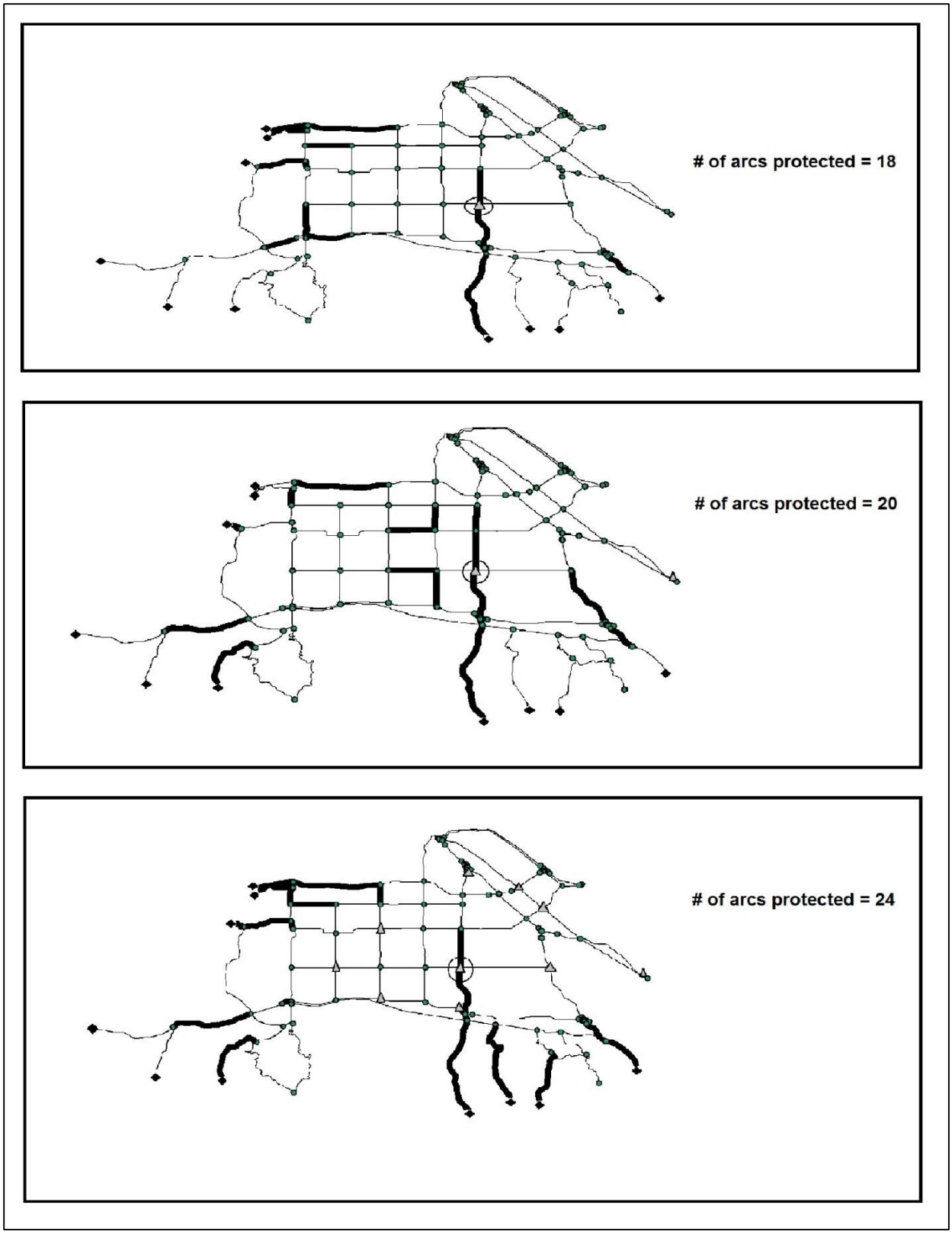

Figure 5.2 Protected arcs for the cases with single, two and ten targets (triangles are the target nodes, the circled node is the most valuable target)

6 Conclusions and Future Work

This research is an initial attempt to model attacker deterrence using target-oriented utility theory. The results provide the optimal levels of investment in security, taking into account the possibility of deterring an attacker. Although we do not include attack cost in our models, deterrence is more plausible when the attack cost is high. For example, low-cost attacks (such as some computer network attacks) may be difficult to deter, if the attacker can simply launch multiple attacks without regard to cost [6], but high-cost attacks (e.g., involving acquisition of a nuclear weapon) may be deterred even if the success probability of the attack is not practically low [7].

Our results for simple systems in chapter 3 indicate, not surprisingly, that the target-oriented model results in a better value of the defender's objective function than conventional game-theoretic models that do not consider deterrence. However, that improvement can arise for one of two different reasons; by spending less on defense when the cost effectiveness of defense is high, or by achieving improved security (due to the possibility of deterrence) when the cost effectiveness of defense is low. These results obviously depend on the assumption that an attacker might give up attacking for some feasible level of defensive investment.

Our results also support the idea that defending series systems is more difficult than defending parallel systems. In particular, when the cost-effectiveness of investment and the loss from a successful attack are large enough to justify investing in defense of a series system, series systems require higher levels of defensive investment than comparable parallel systems.

Finally, the results for simple systems indicate that target value is an important influence on defensive resource allocation. In particular, as the target value increases, the defender chooses to invest more in protection, to reduce the success probability of an attack and consequently

increase the probability of deterrence. Therefore, targets with higher values might in general be expected to get more protection, pushing attacks down to lower-valued targets. In other words, in a well-functioning system, there should be few if any successful attacks on large targets, and more attacks on small targets, which is exactly what we see in the Israeli experience, for example.

In chapters 4 and 5, we develop models for the optimal placement of detectors (e.g., radiation detectors or chemical sensors) on a more realistic and complex transportation network. We formulate the problem as a nested mixed integer programming problem in which the defender minimizes the expected loss from an attack (taking into account uncertainty about the attacker's deterrence threshold), plus the investment in protection. The level of investment in sensors (or, equivalently, the magnitude of the detection probability) needed to deter an attack is assumed to be uncertain. The defender is assumed to either successfully deter an attack, or fail to deter an attack and suffer some expected consequences. (By contrast, the usual approach is simply to maximize the probability of attack detection [10] [64], which ignores the possibility of deterrence.)

We are able to solve the problem for protection of either a single target or multiple targets. We solve both problems as mixed-integer linear programs, linearizing the nonlinear functions to reduce solution time.

In chapter 4, we explore how the parameter values affect the optimal resource allocation throughout the network in the single-target case. Our results indicate that higher attacker success probabilities prior to protection lead to higher levels of protection at optimality, as expected.

Target value is also an important influence on defensive resource allocation. As the target value increases, the defender chooses to invest more in protection, to reduce the success probability of an attack and consequently increase the probability of deterrence. Therefore, targets with higher

values can in general be expected to get more protection. This result is again consistent with the results of the simple model in chapter 3.

The effectiveness of defensive investment also affects the defender's optimal protection strategy. In particular, when effectiveness is low, the defender invests little in protection, since investment does not significantly affect either the deterrence probability or the attack success probability. For moderately large levels of effectiveness, the defender protects more arcs, since protection is now more worthwhile. Finally, for large values of effectiveness, even low levels of investment are still enough to protect the network.

We also explore the deterrence behavior of the attacker. We use S-shaped deterrence functions for cases in which the probability of deterrence is close to 1 even when the probability of success is only moderately low, and reverse S-shaped deterrence functions for cases when even small attack success probabilities can result in non-negligible probabilities of attack. For both cases, we found that the defender generally protects more arcs when deterrence of an attack is more difficult. However, we confirmed that this is not always the case; for example, when defense is extremely costly and not highly effective, then if deterrence is difficult to achieve, that is disincentive to invest.

Our model can be extended in numerous ways. For example, it might be worthwhile to extend our model to include retaliation for a successful attack, in addition to investment in security. When an attacker believes that the defender would retaliate after an attack, it may be possible for the defender to deter an attack with less investment, as long as retaliation is considered a "credible threat" by the attacker [29] [7]. Note also that retaliation may be more important for systems where an attacker can attack repeatedly at modest effort (e.g., attacks against computer networks). This

is because the attacker might be expected to attack in such cases even if the success probability of an attack is low, if not concerned about retaliation.

Additionally, models where the perceived value of a successful attack to the attacker differs from the loss to the defender might be another important extension. In our model, we treat the loss from a successful attack as a constant, which is assumed to be the same for both the defender and the attacker. However, target valuations may differ for the attacker and the defender; moreover, one could also treat the attacker's valuation as being uncertain to the defender [25].

Moreover, including travel time and arc length in consideration of arc attack success probabilities could be another extension. In particular, instead of generating arcs attack success probabilities randomly, they should be correlated with arc length and travel time. Also, different methods for interdiction could be considered other than installing sensors. For example, closing a critical arc, restricting travel direction, and restricting vehicle types on certain routes could be considered for interdiction.

Although we were able to solve our optimization problems for both single and multiple targets, it might be worthwhile to improve the solution approach to speed up the computation time beyond what we have been able to do. This may be necessary in order to apply the model to larger networks with more possible targets.

Moreover, we have only speculations about how the number of targets affects the location of the optimal protected arcs. In particular, we observe that as the number of targets increases, the defender seems to push the defense to peripheral arcs. We also observe that the location of the most valuable target seems to affect the number of protected arcs. However, we did not have a chance to do enough computation to confirm these speculations rigorously.

Our model with multiple possible targets could also be extended by assuming that the defender is uncertain about the attacker choice of target and optimizes resource allocation under uncertainty (instead of our conservative approach, in which the defender protects against the worst possible attack). This extension would most likely significantly increase the computational complexity of the problem.

Finally, the assessment of parameter values for deterrence models is of crucial importance. As long as data directly relevant to the deterrence of terrorism is sparse or unavailable, it will be difficult to estimate parameters of this model. However, interview methods could be used to estimate the deterrence behavior of attackers [61] [62]. Another method that could be used to estimate deterrence parameters, target values, etc. is expert opinion [73]. Numerous analytical methods for use of expert opinion have been developed. For example, probabilistic inversion has been used for parameter values that are difficult for the experts to estimate directly [74] [75]. Good methods of parameter estimation might be needed in order for models such as our to be useful in practice.

7 References

[1] J. Yates, R. Batta and M. Karwan, "Optimal placement of sensors and interception resource assessment for the protection of regional infrastructure from covert attack," *Journal of Transportation Security,* vol. 4, no. 2, pp. 145-169, 2011.

[2] C. Savage, "US Doles Out Millions for Street Cameras," 12 Agust 2007. [Online]. Available: http://www.boston.com/news/nation/washington/articles/2007/08/12/us_doles_out_millions_for_street_cameras/?page=1. [Accessed 6 July 2011].

[3] F. Southworth, "Multi-criteria Sensor Placement for Emergency Response," *Applied Spatial Analysis,* pp. 37-58, 2008.

[4] V. M. Bier, A. Nagaraj and V. Abhichandani, "Protection of simple series and parallel systems with components of different values," *Reliability Engineering and System Safety,* vol. 87, no. 3, pp. 315-323, 2005.

[5] R. F. Bordley and C. W. Kirkwood, "Multi Attribute Preference Analysis with Performance Targets," *Operations Research,* vol. 52, no. 6, pp. 823-835, 2004.

[6] M. Ertem, "A Stochastic Network-Interdiction Model For Cyber Security," Industrial and System Engineering Department, University of Wisconsin, Madison, 2014.

[7] N. Haphuriwat, V. M. Bier and H. H. Willis, "Deterring the smuggling of nuclear weapons in container freight through detection and retaliation," *Decision Analysis,* vol. 8, no. 2, pp. 88-102, 2011.

[8] C. N. Fink, "Antiterrorism Security and Surface Transportation Systems: Review of Case Studies and Current Tactics," *Transportation Research Record: Journal of the Transportation Research Board,* vol. 1822, no. 1, pp. 9-17, 2003.

[9] J. Yates and S. Sanjeevi, "Assessing the impact of vulnerability modeling in the protection of critical infrastructure," *Journal of Geographical Systems,* vol. 14, no. 4, pp. 415-435, 2012.

[10] N. Dimitrov, D. Michalopoulos, D. Morton, M. Nehme, F. Pan, E. Popova, E. Schneider and G. Thoreson, "Network deployment of radiation detectors with physics-based detection probability calculations," *Annals of Operations Research,* pp. 1-22, 2009.

[11] V. Bier and V. Abhichandani, "Optimal allocation of resources for defense of simple series and parallel systems from determined adversaries," in *Proceedings of the Engineering Foundation Conference on Risk-Based Decision Making in Water Resources X. American Society of Civil Engineers*, Santa Barbara, CA, 2002.

[12] G. Levitin and K. Hausken, "Protection vs. redundancy in homogeneous parallel systems," *Reliability Engineering & System Safety,* vol. 93, no. 10, p. 1444–1451, 2008.

[13] K. Hausken and G. Levitin, "Minmax defense strategy for complex multi-state systems," *Reliability Engineering & System Safety,* vol. 94, no. 2, pp. 577-587, 2009.

[14] G. Levitin and K. Hausken, "False targets efficiency in defense strategy," *European Journal of Operational Research,* vol. 194, no. 1, pp. 155-162, 2009.

[15] K. Hausken and G. Levitin, "Protection vs. false targets in series systems," *Reliability Engineering & System Safety,* vol. 94, no. 5, pp. 973-981, 2009.

[16] G. Levitin and K. Hausken, "False targets vs. redundancy in homogeneous parallel systems," *Reliability Engineering & System Safety,* vol. 94, no. 2, pp. 588-595, 2009.

[17] H. Kunreuther and G. Heal, "Interdependent security," *Journal of Risk and Uncertainty,* vol. 26, no. 2, pp. 231-249, 2003.

[18] G. Heal and H. Kunreuther, "Modeling interdependent risks," *Risk Analysis,* vol. 27, no. 3, pp. 621-634, 2007.

[19] A. R. Morral and B. A. Jackson, "Understanding the Role of Deterrence in Counterterrorism Security," RAND Corporation, Santa Monica, CA, 2009.

[20] W. L. McGill, "Defensive dissuasion in security risk management," in *Systems, Man and Cybernetics, 2009. SMC 2009. IEEE International Conference on*, San Antonio, 2009.

[21] N. O. Keohane and R. J. Zeckhauser, "The ecology of terror defense," *Journal of Risk and Uncertainty,* vol. 26, no. 2, pp. 201-229, 2003.

[22] T. Sandler and D. G. Arce, "Terrorism & game theory," *Simulation Gaming,* vol. 34, no. 3, pp. 319-337, 2003.

[23] D. G. Arce, D. Kovenock and B. Roberson, "Weakest-link attacker-defender games with multiple attack technologies," *Naval Research Logistics,* vol. 59, no. 6, pp. 457-469, 2012.

[24] V. Bier, S. Oliveros and L. Samuelson, "Choosing what to protect: Strategic defensive allocation against an unknown attacker," *Journal of Public Economic Theory,* vol. 9, no. 4, p. 563–587, 2007.

[25] V. M. Bier, N. Haphuriwat, J. Menoyo, R. Zimmerman and A. M. Culpen, "Optimal resource allocation for defense of targets based on differing measures of attractiveness," *Risk Analysis,* vol. 28, no. 3, pp. 763-770, 2008.

[26] K. Hausken and J. Zhuang, "The timing and deterrence of terrorist attacks due to exogenous dynamics," *Journal of the Operational Research Society,* vol. 63, no. 6, pp. 726-735, 2012.

[27] M. Azaiez and V. M. Bier, "Optimal resource allocation for security in reliability systems," *European Journal of Operational Research,* vol. 181, no. 2, pp. 773-786, 2007.

[28] J. Zhuang and V. M. Bier, "Balancing terrorism and natural disasters—defensive strategy with endogenous attacker effort," *Operations Research,* vol. 55, no. 5, pp. 976-991, 2007.

[29] V. Bier and N. Haphuriwat, "Analytical method to identify the number of containers to inspect at U.S. ports to deter terrorist attacks," *Annals of Operations Research,* vol. 187, no. 1, pp. 137-158, 2011.

[30] R. Wollmer, "Removing arcs from a network," *Operations Research,* vol. 12, no. 6, pp. 934-940, 1964.

[31] A. W. McMasters and T. M. Mustin, "Optimal interdiction of a supply network," *Naval Research Logistics Quarterly,* vol. 17, no. 3, pp. 261-268, 1970.

[32] P. M. Ghare, D. C. Montgomery and W. C. Turner, "Optimal interdiction policy for a flow network," *Naval Research Logistics Quarterly,* vol. 18, no. 1, pp. 37-45, 1971.

[33] R. Wood, "Deterministic network interdiction," *Mathematical and Computer Modelling,* vol. 17, no. 2, pp. 1-18, 1993.

[34] H. D. Ratliff, G. T. Sicilia and S. H. Lubore, " Finding the n most vital links in flow networks," *Management Science,* vol. 21, no. 5, pp. 531-539, 1975.

[35] D. Fulkerson and G. Harding, "Maximizing the minimum source-sink path subject to a budget constraint," *Mathematical Programming,* vol. 13, no. 1, pp. 116-118, 1977.

[36] B. Golden, "A problem in network interdiction," *Naval Research Logistics Quarterly,* vol. 25, no. 4, pp. 711-713, 1978.

[37] H. Corley and D. Y. Sha, "Most vital links and nodes in weighted networks," *Operations Research Letters,* vol. 1, no. 4, pp. 157-160, 1982.

[38] M. O. Ball, B. L. Golden and R. V. Vohra, "Finding the most vital arcs in a network," *Operations Research Letters,* vol. 8, no. 2, pp. 73-76, 1989.

[39] K. Malik, A. Mittal and S. Gupta, "The k most vital arcs in the shortest path problem," *Operations Research Letters,* vol. 8, no. 4, pp. 223-227, 1989.

[40] E. Israeli and R. K. Wood, "Shortest-path network interdiction," *Networks,* vol. 40, no. 2, pp. 97-111, 2002.

[41] H. Bayrak and M. D. Bailey, "Shortest path network interdiction with asymmetric information," *Networks,* vol. 52, no. 3, pp. 133-140, 2008.

[42] K. J. Cormican, D. P. Morton and R. K. Wood, "Stochastic network interdiction," *Operations Research,* vol. 46, no. 2, pp. 184-197, 1998.

[43] R. Hemmecke, R. Schultz and D. L. Woodruff, "Interdicting stochastic networks with binary interdiction effort," in *Network interdiction and stochastic integer programming*, D. L. Woodruff, Ed., Norwell, MA, Kluwer Academic Publishers, 2003, p. 69–84.

[44] H. Held, R. Hemmecke and D. L. Woodruff, "A decomposition algorithm applied to planning the interdiction of stochastic networks," *Naval Research Logistics,* vol. 52, no. 4, pp. 321-328, 2005.

[45] D. P. Morton, F. Pan and K. J. Seager, "Models for nuclear smuggling interdiction," *IIE Transactions,* pp. 3-14, 2007.

[46] F. Pan and D. P. Morton, "Minimizing a stochastic maximum-reliability path," *Networks,* vol. 52, no. 3, pp. 111-119, 2008.

[47] D. P. Morton, "Stochastic Network Interdiction," *Wiley Encyclopedia of Operations Research and Management Science,* 2011.

[48] K. J. Cormican, "Computational methods for deterministic and stochastic network interdiction problems," Monterey, California. Naval Postgraduate School, , 1995.

[49] U. Janjarassuk and J. Linderoth, "Reformulation and sampling to solve a stochastic network interdiction problem," *Networks,* vol. 52, no. 3, pp. 120-132, 2008.

[50] K. Borch, "Decision Rules Depending on the Probability of Ruin," *Oxford Economic Papers,* vol. 20, no. 1, pp. 1-10, 1968.

[51] M. H. Berhold, "The use of distribution functions to represent utility functions," *Management Science,* vol. 19, no. 7, pp. 825-829, 1973.

[52] E. Castagnoli and M. Calzi, "Expected utility without utility," *Theory and Decision,* vol. 41, no. 3, pp. 281-301, 1996.

[53] R. Bordley and M. LiCalzi, "Decision analysis using targets instead of utility functions," *Decisions in Economics and Finance,* vol. 23, no. 1, pp. 53-74, 2000.

[54] A. E. Abbas and J. E. Matheson, "Normative target-based decision making," *Managerial and Decision Economics,* vol. 26, no. 6, pp. 373-385, 2005.

[55] R. F. Bordley and C. W. Kirkwood, "Multiattribute preference analysis with performance targets," *Operations Research,* vol. 52, no. 6, pp. 823-835, 2004.

[56] I. Tsetlin and R. L. Winkler, "On equivalent target-oriented formulations for multiattribute utility," *Decision Analysis,* vol. 3, no. 2, pp. 94-99, 2006.

[57] I. Tsetlin and R. L. r. Winkle, " Decision Making with Multiattribute Performance Targets: The Impact of Changes in Performance and Target Distributions," *Operations Research,* vol. 55, no. 2, pp. 226-233, 2007.

[58] A. E. Abbas and J. E. Matheson, "Normative decision making with multiattribute performance targets," *Journal of Multi-Criteria Decision Analysis,* vol. 16, no. 3-4, pp. 67-78, 2009.

[59] R. F. Bordley and S. M. Pollock, "A Decision-Analytic Approach to Reliability-Based Design Optimization," *Operations Research* , vol. 57, no. 5, pp. 1262-1270 , 2009 .

[60] R. F. Bordley and S. M. Pollock, "Assigning resources and targets to an organization's activities," *European Journal of Operational Research,* vol. 220, no. 3, pp. 752-761, 2012.

[61] R. Anthony, "A calibrated model of the psychology of deterrence," *Bulletin on Narcotics,* vol. LVI , pp. 49-64, 2004.

[62] T. A. Loughran, G. Pogarsky, A. R. Piquero and R. Paternoster, "Re-examining the functional form of the certainty effect in deterrence theory," *Justice Quarterly,* vol. 10, pp. 1-30, 2011.

[63] M. Jones, "Kumaraswamy's distribution: A beta-type distribution with some tractability advantages," *Statistical Methodology,* vol. 6, no. 1, pp. 70-81, 2009.

[64] J. Yates and I. Casas, "Role of Spatial Data in the Protection of Critical Infrastructure and Homeland Defense," *Applied Spatial Analysis and Policy,* 2010.

[65] M. Jones, "Kumaraswamy's distribution: A beta-type distribution with some tractability advantages," vol. 6, no. 1, 2009.

[66] H. D. Sherali, "On mixed-integer zero-one representations for separable lower-semicontinuous piecewise-linear functions," *Operations Research Letters,* pp. 155-160, 2001.

[67] L. M. Wein and M. P. Atkinson, "The last line of defense: designing radiation detection-interdiction systems to protect cities from a nuclear terrorist attack," *Nuclear Science , IEEE Transactions,* vol. 54, no. 3, pp. 654-669, 2007.

[68] D. PAGE, "Officer.com," 1 05 2009. [Online]. Available: http://www.officer.com/article/10233631/the-radtruck-stops-here. [Accessed 26 7 2014].

[69] "Homeland Security News Wire," 7 7 2006. [Online]. Available: http://www.homelandsecuritynewswire.com/explosive-detection-systems-installed-truck-weighing-stations. [Accessed 26 7 2014].

[70] J. A. Major, "Advanced Techniques for Modeling Terrorism Risk," *Journal of Risk Finance,* vol. 4, no. 1, pp. 15-24, 2002.

[71] W. A. Kamakura and G. J. Russell, "A Probabilistic Choice Model for Market Segmentation and Elasticity Structure," *Journal of Marketing Research,* vol. 26, no. 4, pp. 379-390, 1989.

[72] L. R. Duncan, Individual Choice Behavior a Theoretical Analysis, New York : Wiley, 1959.

[73] R. Cooke, Experts in uncertainty: Opinion and subjective probability in science, New York & Oxford: Oxford University Press, 1991.

[74] C. Du, D. Kurowicka and R. Cooke, "Techniques for generic probabilistic inversion," *Computational Statistics & Data Analysis,* vol. 50, no. 5, p. 1164–1187, 2006.

[75] B. Kraan and T. Bedford, "Probabilistic inversion of expert judgments in the quantification of model uncertainty," *Management Science,* vol. 51, no. 6, pp. 995-1006, 2005.

[76] J.-P. Rodrigue, C. Comtois and B. Slack, The Geography of Transport Systems, New York: Routledge, 2009.

[77] J. Yates and I. Casas, "Role of Spatial Data in the Protection of Critical Infrastructure and Homeland Defense," *Applied Spatial Analysis and Policy,* vol. 5, no. 1, pp. 1-23, 2010.

[78] H. H. Willis, "Guiding Resource Allocations Based on Terrorism Risk," *Risk Analysis,* vol. 27, no. 3, pp. 597-606, 2007.

8 Appendix

8.1 Appendix A

Proof of Proposition 4: For both parallel and series systems we differentiate the objective functions with respect to the investment levels R and x, and then equate the result to zero, yielding the following results:

For two identical components in series, let

$g(x,R) = L\left[\left(1-e^{-\lambda_1 x}\right)\left(1-e^{-\lambda_2 (R-x)}\right)\right] - R$ be the objective function.

To find optimum points, we first check the first-order conditions

$$\nabla g(x,R) \equiv 0 \Leftrightarrow \begin{cases} g_x = 0 \\ g_R = 0 \end{cases}$$

Differentiating the objective function with respect to x and equating the result to zero gives

$$g_x = 0 \Leftrightarrow L\left[\left(\lambda e^{-\lambda x}\right) - \left(\lambda e^{-\lambda (R-x)}\right)\right] = 0$$

$$g_x = 0 \Leftrightarrow x = \frac{R}{2}$$

Similarly, differentiating the objective function with respect to R and equating the result to zero gives

$$g_R = 0 \Leftrightarrow L\left[\left(1-\lambda e^{-\lambda x}\right)\left(\lambda e^{-\lambda (R-x)}\right)\right] - 1 = 0$$

$$g_R = 0 \Leftrightarrow L\left[\left(1-\lambda e^{-\lambda x}\right)\left(\lambda e^{-\lambda (x)}\right)\right] - 1 = 0 \text{ (plug in } x = \tfrac{R}{2})$$

$$g_R = 0 \Leftrightarrow \begin{cases} R_1 = -\frac{2}{\lambda}\ln\left(\frac{\sqrt{L\lambda} + \sqrt{L\lambda - 4}}{2\sqrt{L\lambda}}\right. \\ R_2 = -\frac{2}{\lambda}\ln\left(\frac{\sqrt{L\lambda} - \sqrt{L\lambda - 4}}{2\sqrt{L\lambda}}\right. \end{cases}$$

Therefore, these two critical points are candidates to maximize the objective function.

$$\text{Critical points from } \nabla \equiv 0: \begin{cases} x_1 = -\frac{1}{\lambda}\ln(\frac{\sqrt{L\lambda}+\sqrt{L\lambda-4}}{2\sqrt{L\lambda}}, R_1 = -\frac{2}{\lambda}\ln(\frac{\sqrt{L\lambda}+\sqrt{L\lambda-4}}{2\sqrt{L\lambda}} \\ x_2 = -\frac{1}{\lambda}\ln(\frac{\sqrt{L\lambda}-\sqrt{L\lambda-4}}{2\sqrt{L\lambda}}, R_2 = -\frac{2}{\lambda}\ln(\frac{\sqrt{L\lambda}-\sqrt{L\lambda-4}}{2\sqrt{L\lambda}} \end{cases}$$

Other candidate optimal points can be found at *x=0* and *x= R*;

$g(0,R) = -R \ \ for\ R \in [0,\infty), which\ is$ is maximized at $R = 0$.Therefore, (0,0) is a candidate optimum.

$g(R,R) = -R$ is also maximized at $R = 0$, yielding that same candidate optimum.

Thus, we have three candidates to maximize objective function. The first two critical points, give real solutions on for $L\lambda \geq 4$; otherwise, the only solution is (0,0), and maximum value of objective funtion is zero. To determine which point maximizes the objective function, we compare the objective value at each point for values of $L\lambda \geq 4$ below.

For $5 > L\lambda \geq 4$, the objective function is maximized at (0,0), so the optimum objective value is still zero.

For $L\lambda \geq 5$, the objective function is maximized at $\left(-\frac{1}{\lambda}\ln(\frac{\sqrt{L\lambda}-\sqrt{L\lambda-4}}{2\sqrt{L\lambda}}, -\frac{2}{\lambda}\ln(\frac{\sqrt{L\lambda}-\sqrt{L\lambda-4}}{2\sqrt{L\lambda}}\right)$.

Thus, we have $R_s^* = -\frac{2}{\lambda}\ln\left(\frac{\sqrt{L\lambda}-\sqrt{L\lambda-4}}{2\sqrt{L\lambda}}\right) = \frac{1}{\lambda}\ln\left(\frac{4L\lambda}{\left(\sqrt{L\lambda}-\sqrt{L\lambda-4}\right)^2}\right)$ for $L\lambda \geq 5$.

For two identical components in parallel:

$$\frac{d(\,L\left[\left(e^{-\lambda x}\right)\left(e^{-\lambda(R-x)}\right)\right]+R}{dR} = \frac{d\left(\,Le^{-\lambda R}\right)+R}{dR} = 0$$

$$R_p^* = \frac{1}{\lambda}\ln(L\lambda) \quad \text{where } \lambda L \geq 1; \text{otherwise}, R = 0$$

Thus

$R_p^* = R_s^* = 0$ for $L\lambda < 1$

$0 = R_s^* < R_p^*$ for $1 \leq L\lambda < 5$

$R_p^* < R_s^*$ for $5 \leq L\lambda$

8.2 Appendix B

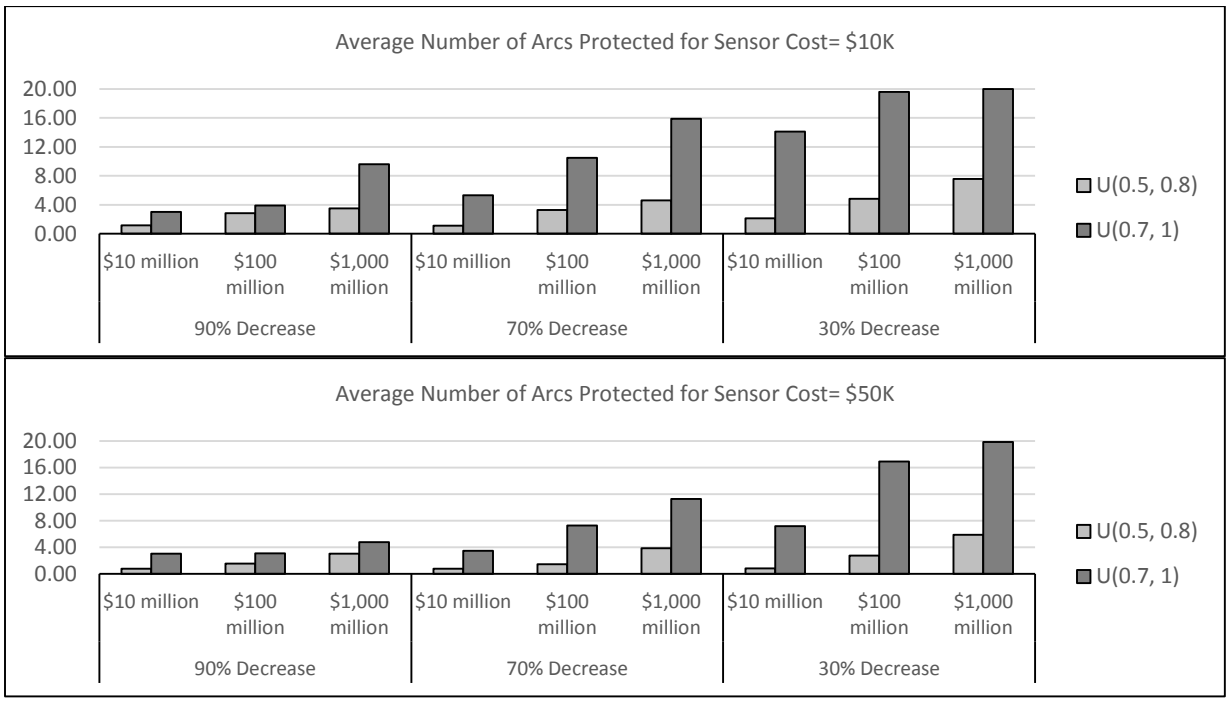

Figure B. 1 Average optimal number of arcs protected for attack success distributions with different means, when deterrence function's shape parameters are (α=2, β=2)

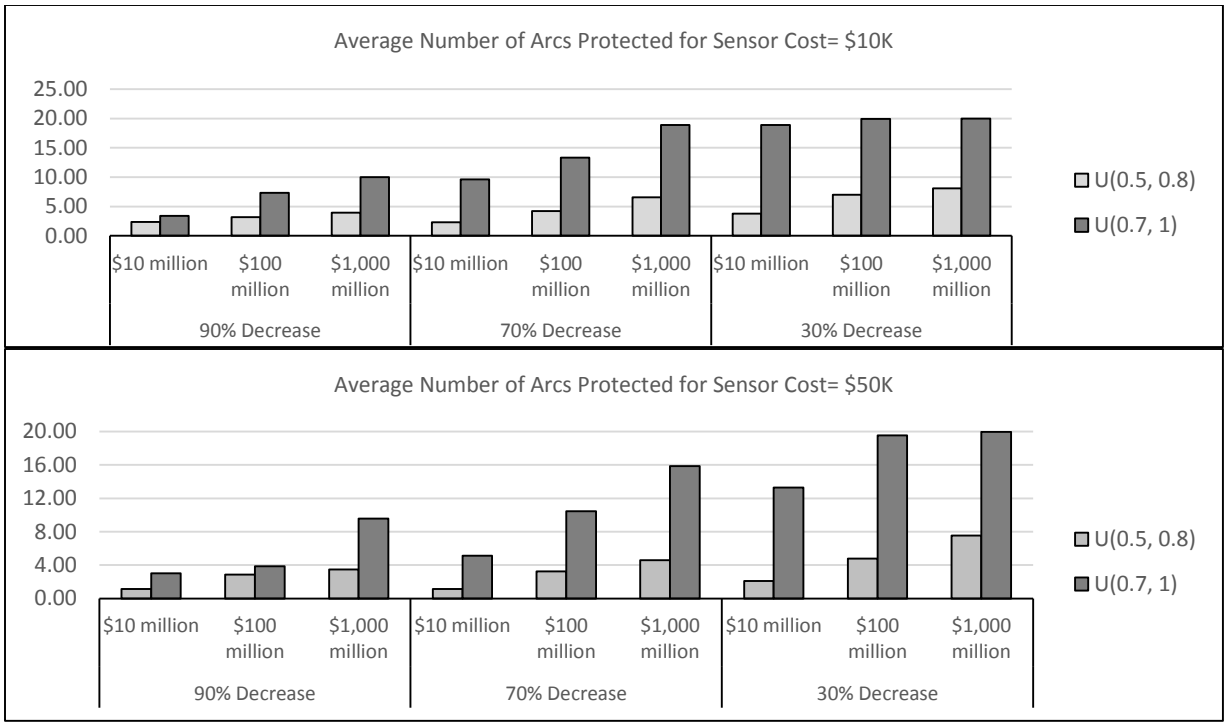

Figure B. 2 Average optimal number of arcs protected for attack success distributions with different means, when deterrence function's shape parameters are (α=2, β=10)

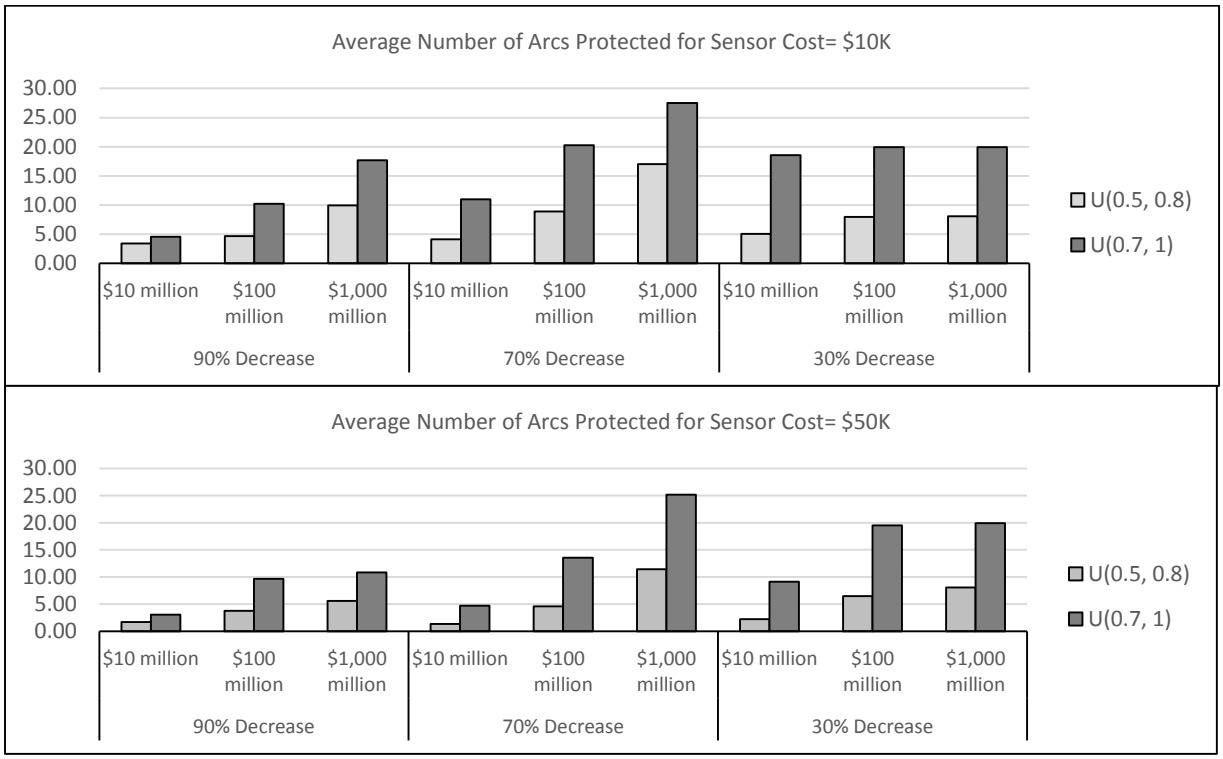

Figure B. 3 Average optimal number of arcs protected for attack success distributions with different means, when deterrence function's shape parameters are (α=0.5, β=0.5)

Figure B. 4 Average optimal number of arcs protected for attack success distributions with different means, when deterrence function's shape parameters are (α=0.2, β=0.8)

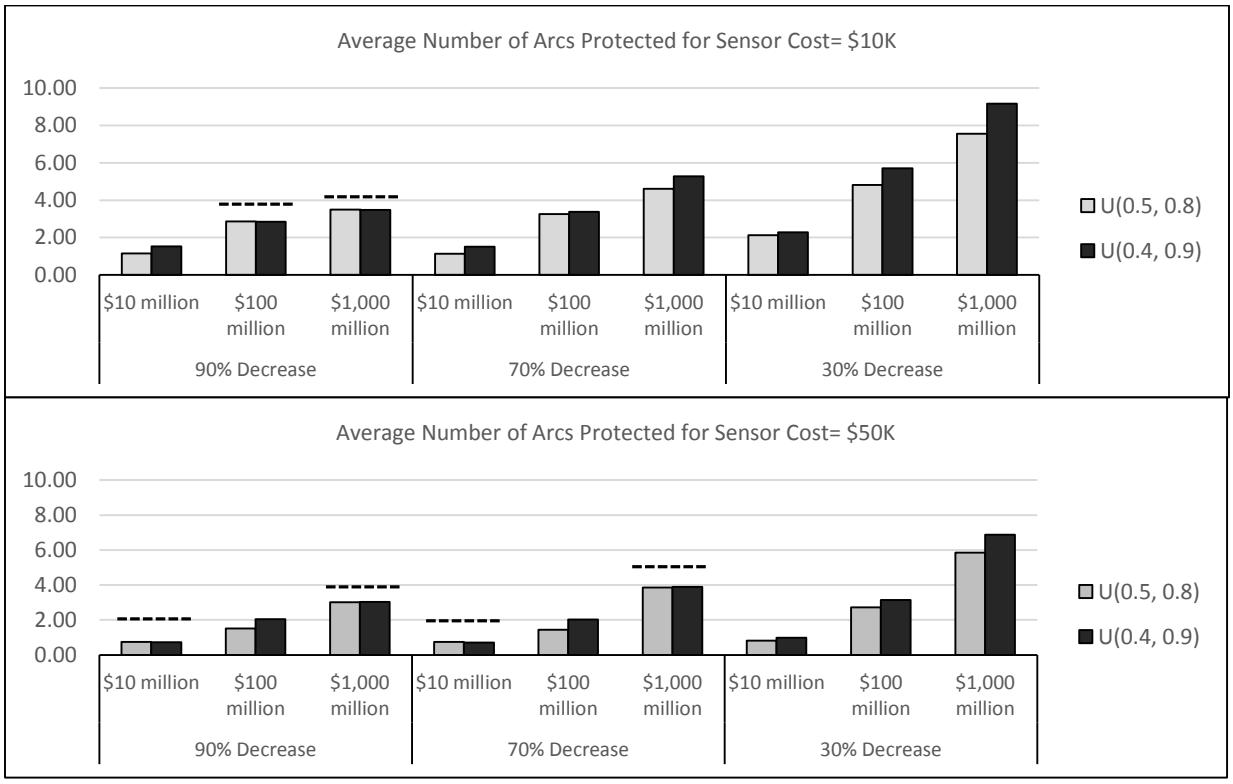

Figure B. 5 Average optimal number of arcs protected for attack success distributions with different variances, when deterrence function's shape parameters are (α=2, β=2)

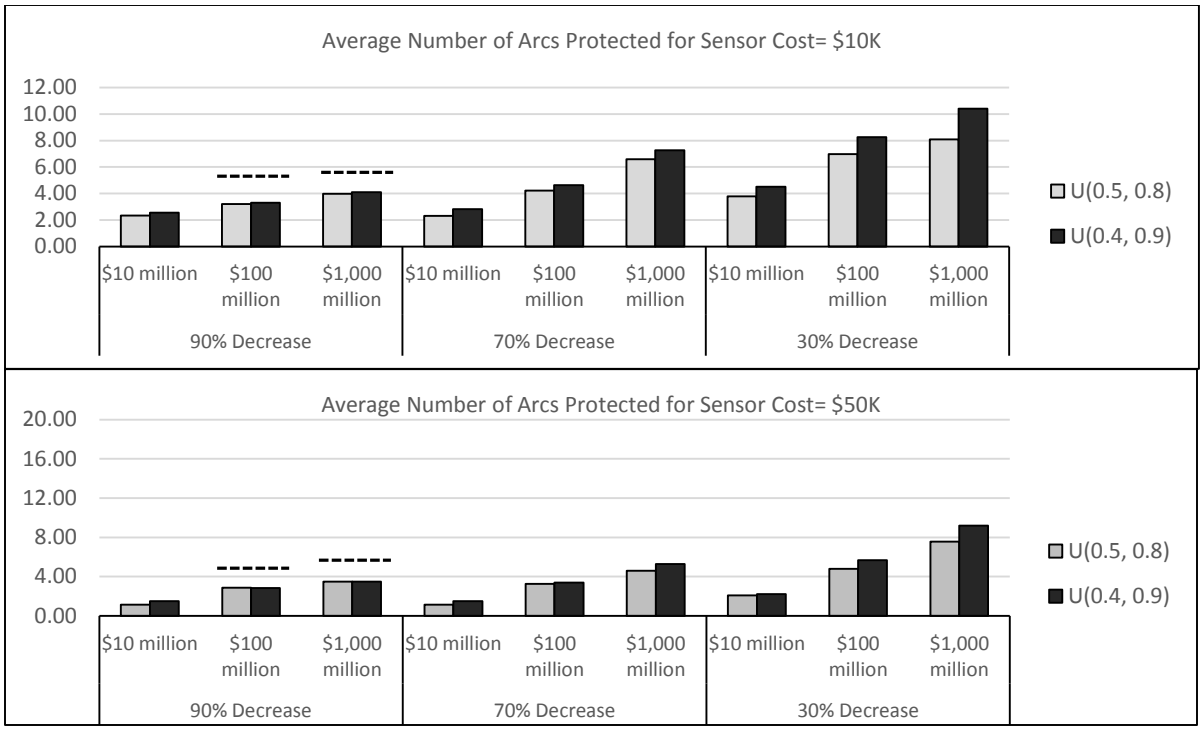

Figure B. 6 Average optimal number of arcs protected for attack success distributions with different variances, when deterrence function's shape parameters are (α=2, β=10)

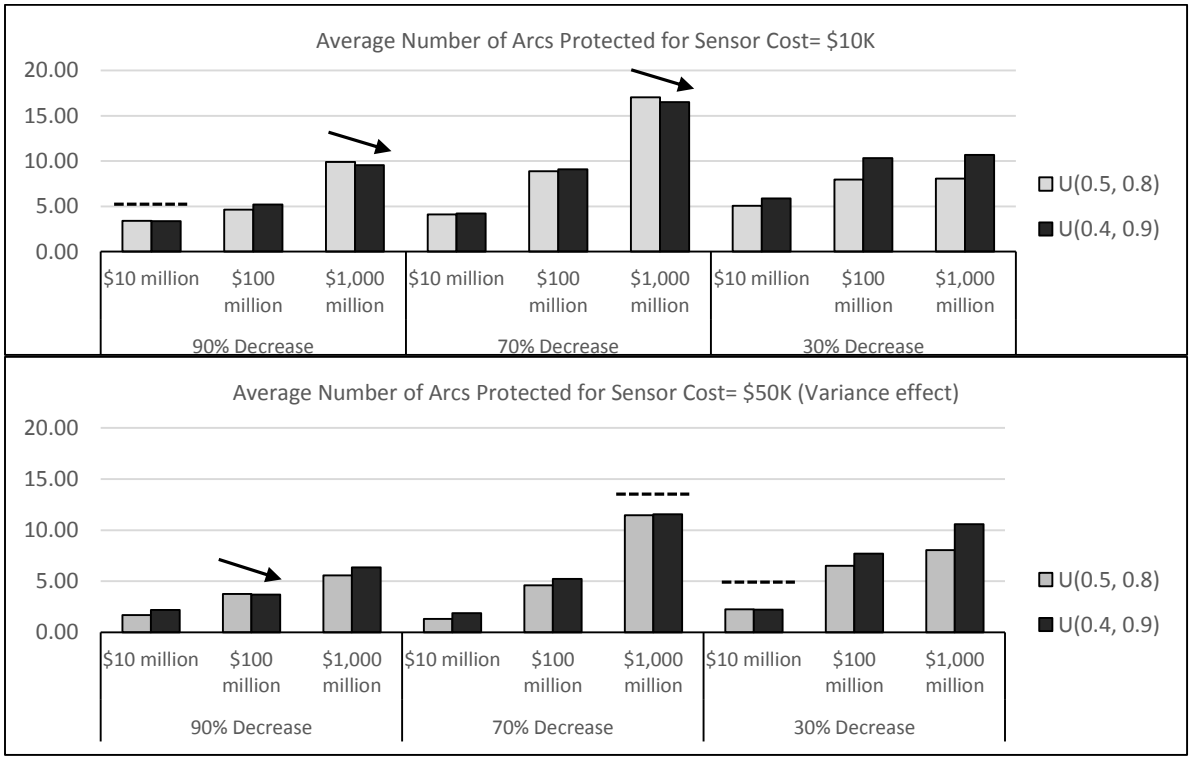

Figure B. 7 Average optimal number of arcs protected for attack success distributions with different variances, when deterrence function's shape parameters are (α=0.5, β=0.5)

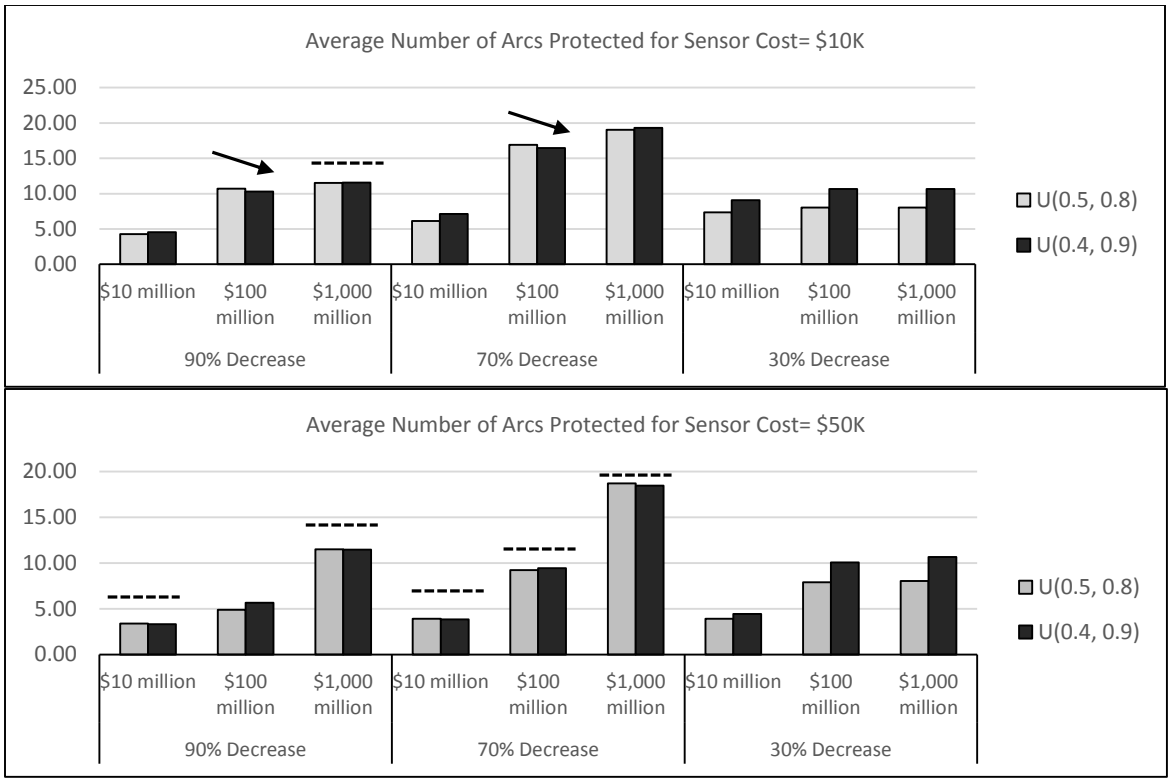

Figure B. 8 Average optimal number of arcs protected for attack success distributions with different variances, when deterrence function's shape parameters are (α=0.2, β=0.8)

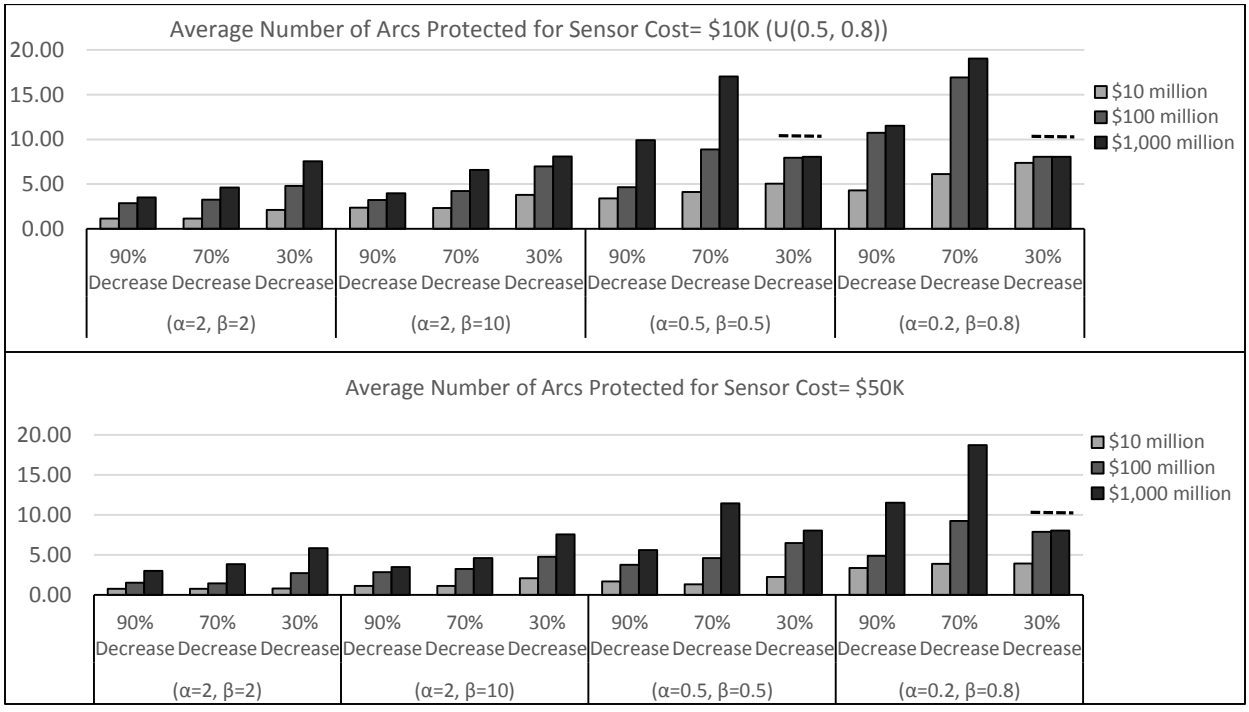

Figure B. 9 Optimal average number of arcs protected for different target values, when p_{ij} is generated from Uniform(0.5, 0.8)

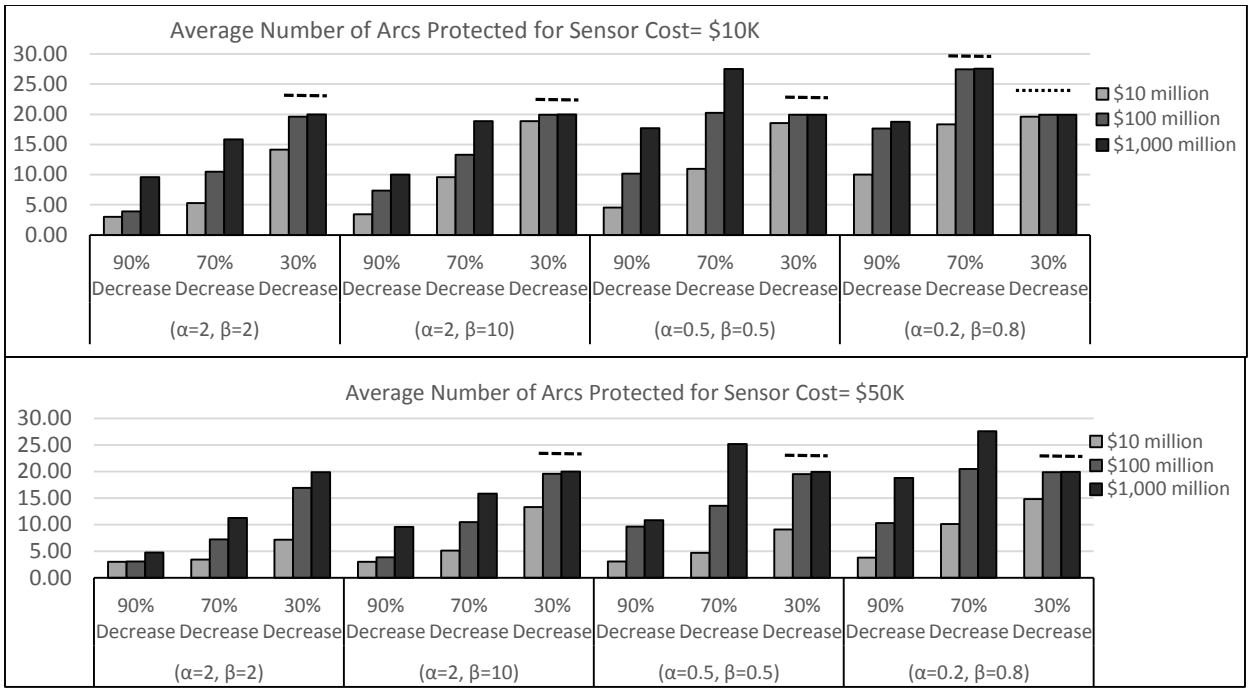

Figure B. 10 Optimal average number of arcs protected for different target values, when p_{ij} is generated from Uniform(0.7, 1)

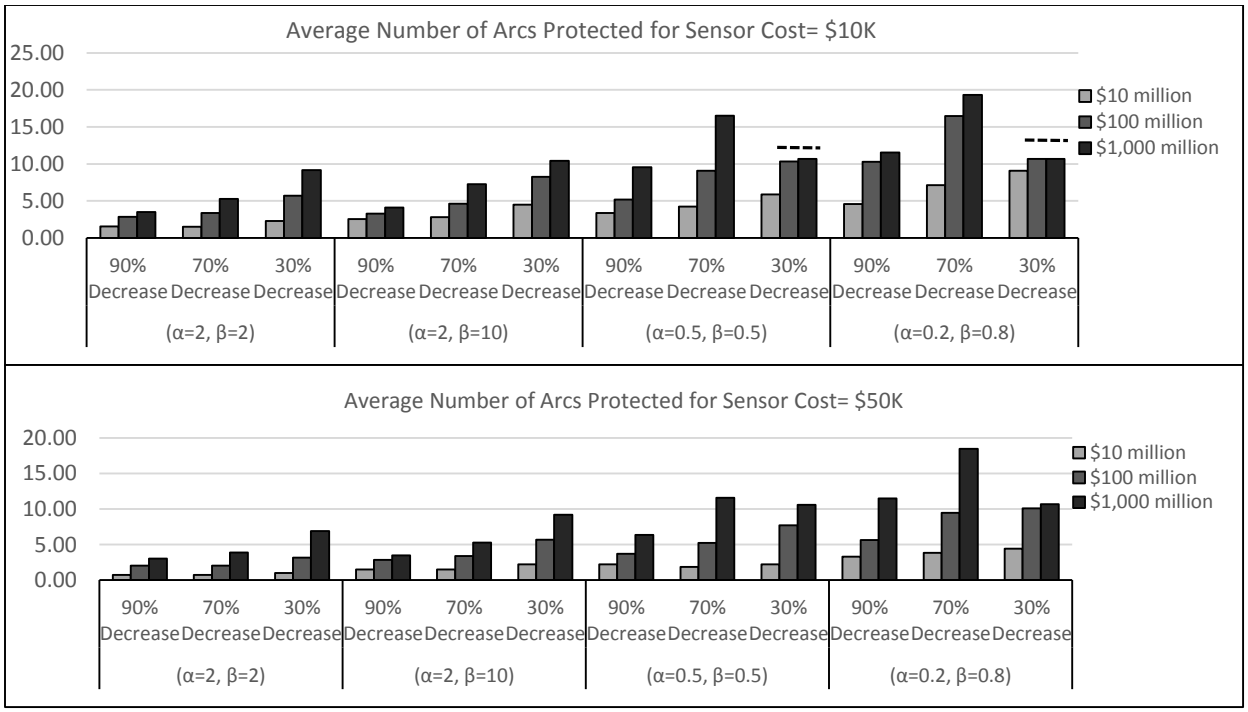

Figure B. 11 Optimal average number of arcs protected for different target values, when p_{ij} is generated from Uniform(0.4, 9)

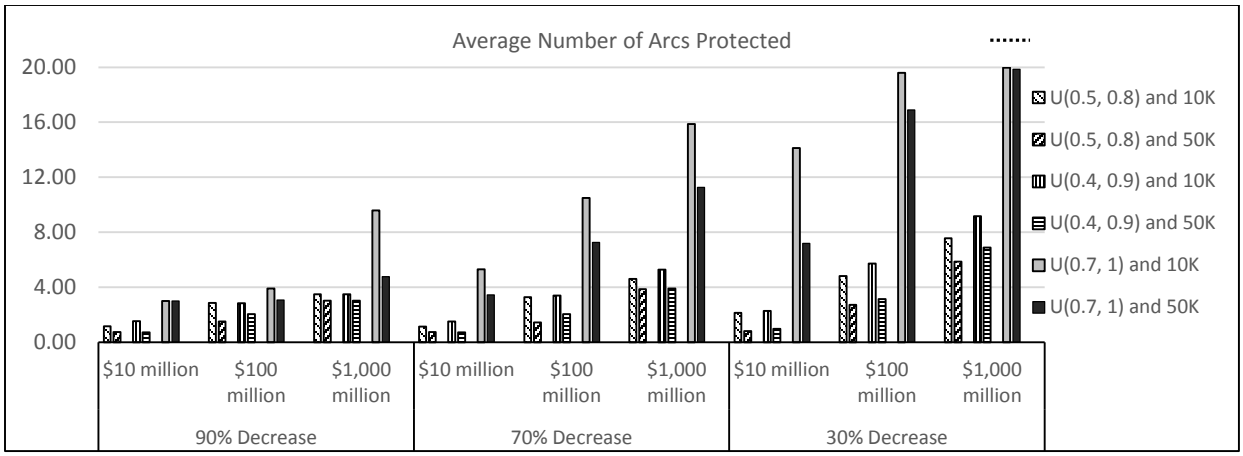

Figure B. 12 Comparison of average optimal number of arcs protected for different sensor costs, when deterrence function's shape parameters are (α=2, β=2)

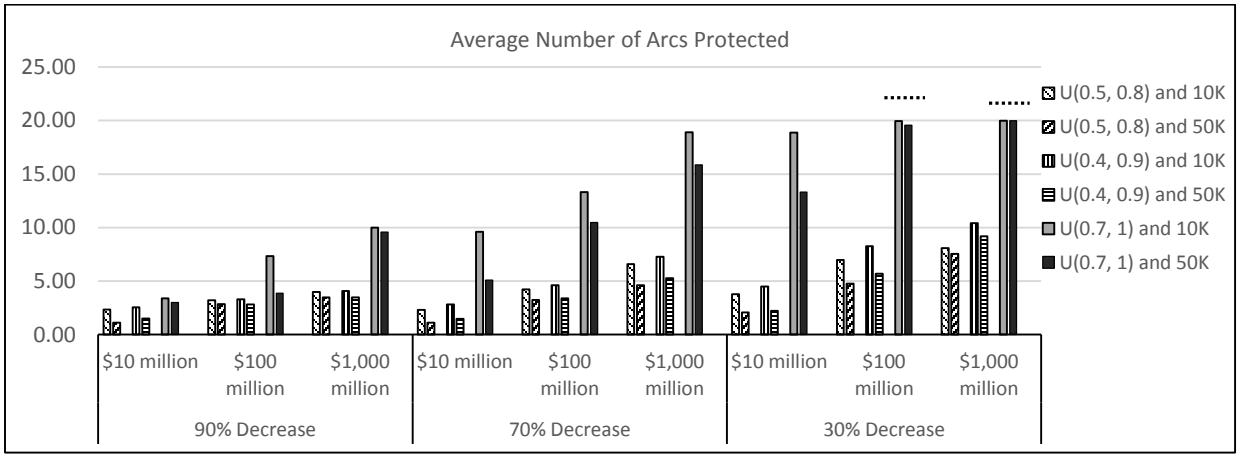

Figure B. 13 Comparison of average optimal number of arcs protected for different sensor costs, when deterrence function's shape parameters are (α=2, β=10)

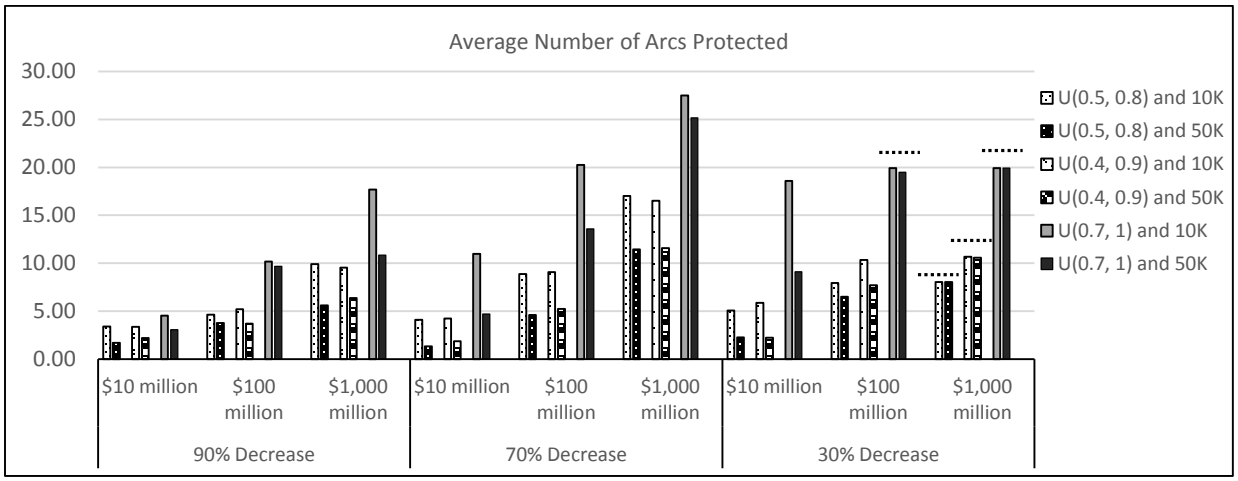

Figure B. 14 Comparison of average optimal number of arcs protected for different sensor costs, when deterrence function's shape parameters are (α=0.5, β=0.5)

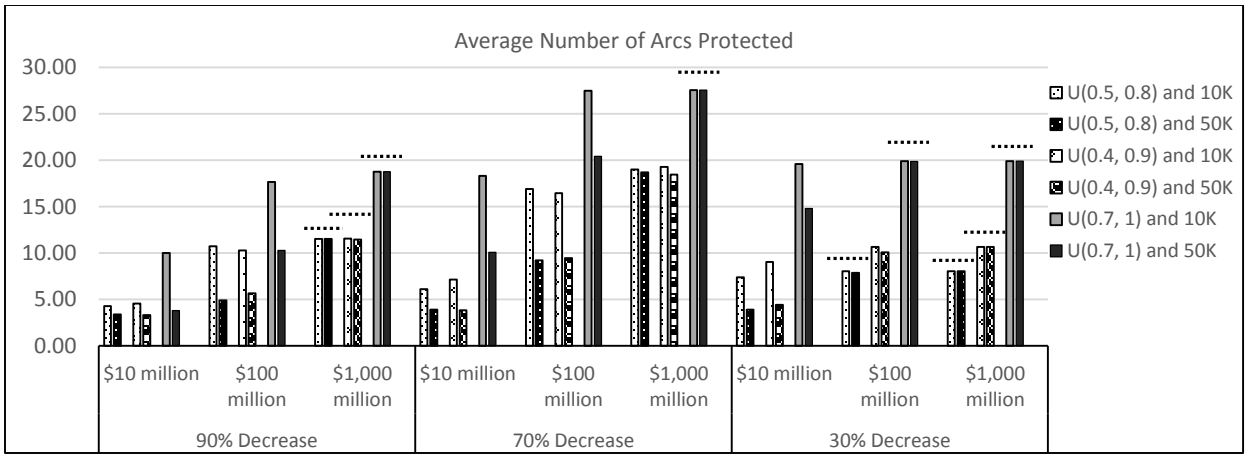

Figure B. 15 Comparison of average optimal number of arcs protected for different sensor costs, when deterrence function's shape parameters are (α=0.2, β=0.8)

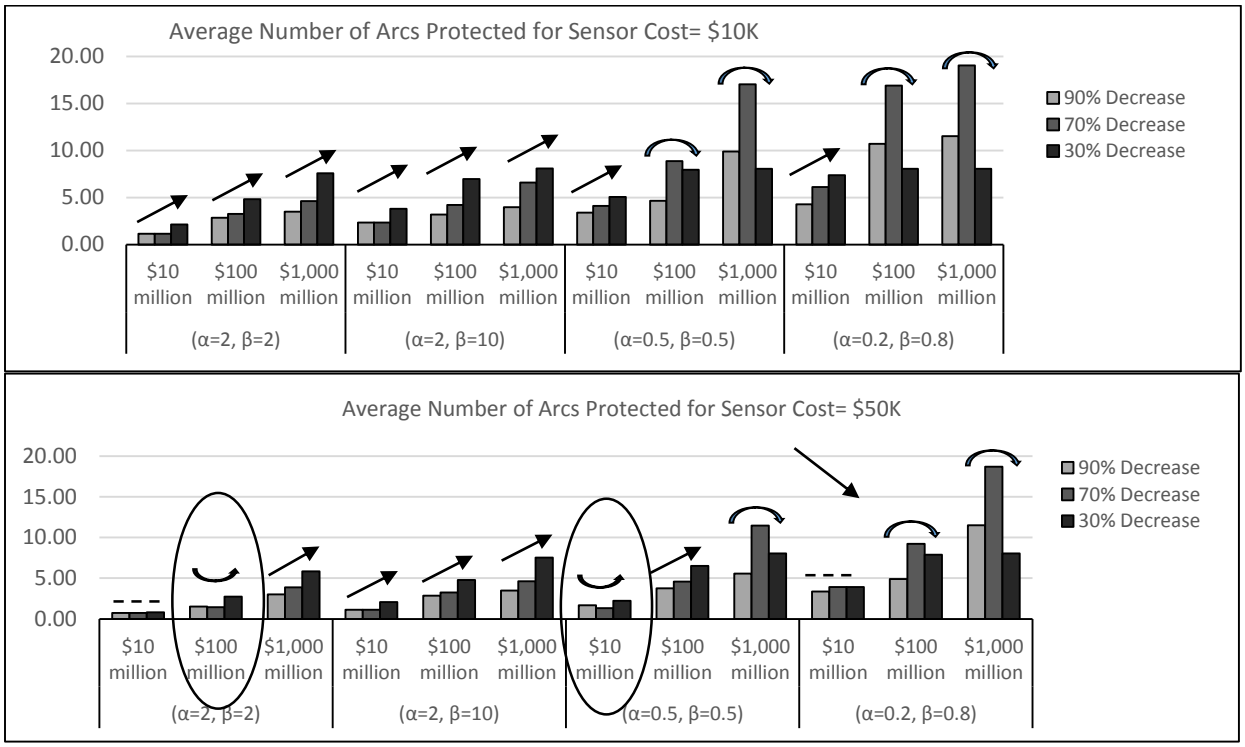

Figure B. 16 Optimal average number of arcs protected for different defensive effectiveness values, when p_{ij} is generated from Uniform(0.5, 0.8)

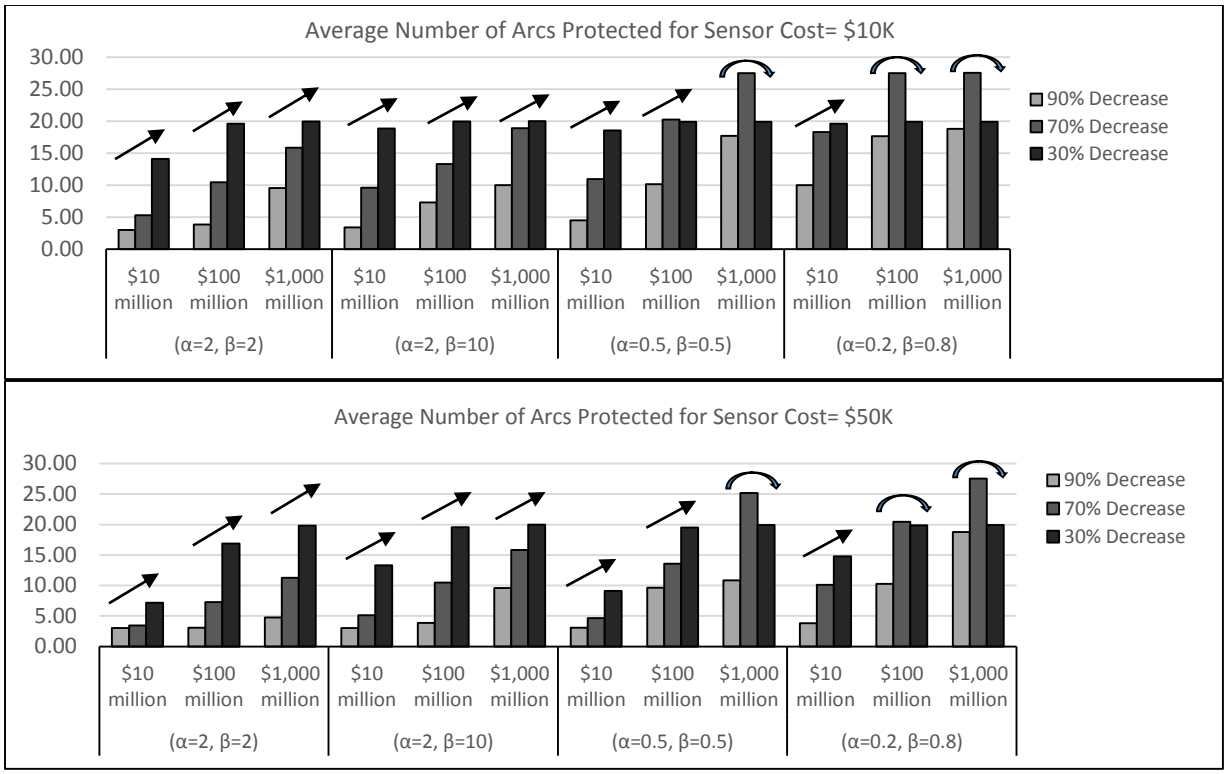

Figure B. 17 Optimal average number of arcs protected for different defensive effectiveness values, when p_{ij} is generated from Uniform(0.7, 1)

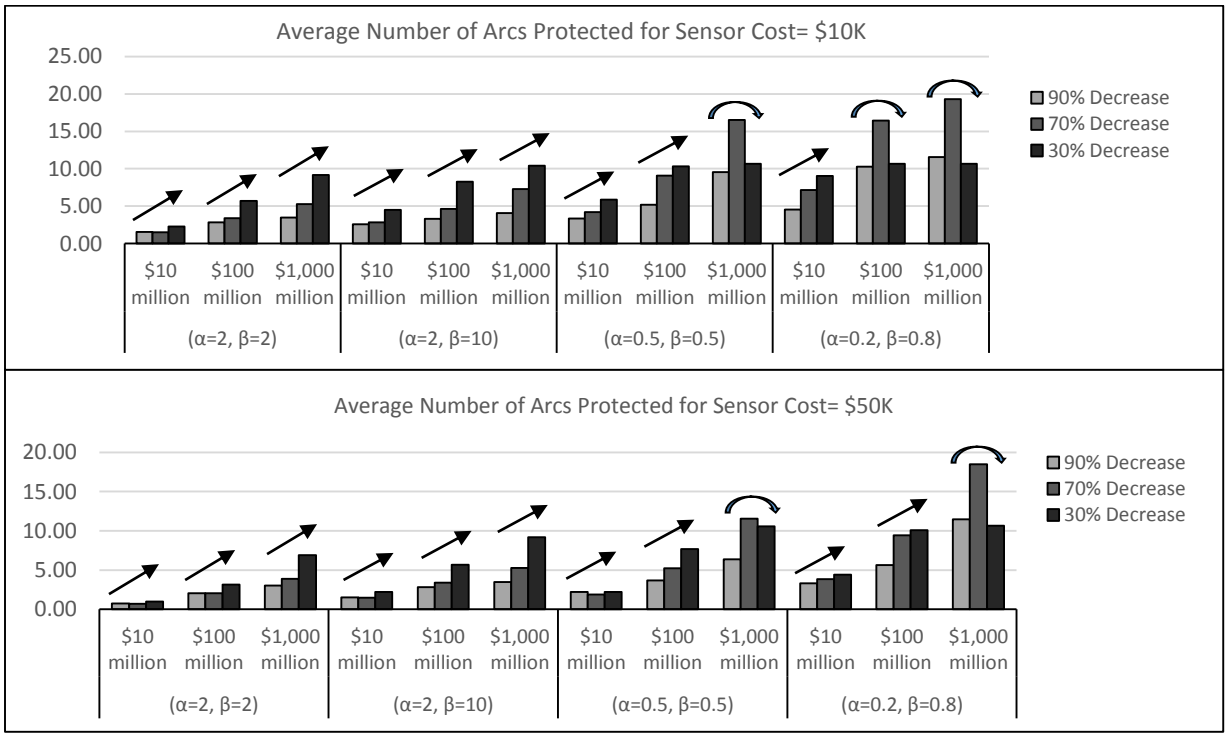

Figure B. 18 Optimal average number of arcs protected for different defensive effectiveness values, when p_{ij} is generated from Uniform(0.4, 0.9)

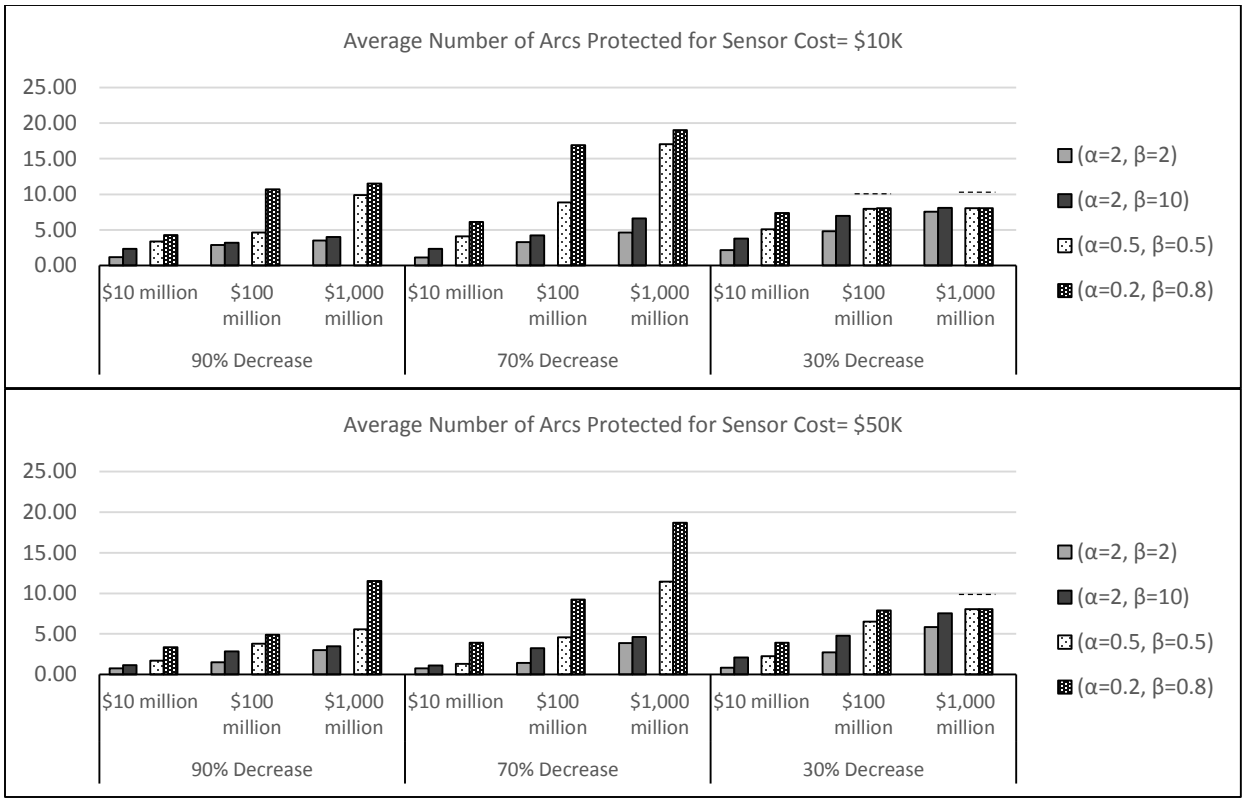

Figure B. 19 Optimal average number of arcs protected for different shape of deterrence function, when p_{ij} is generated from Uniform(0.5, 0.8)

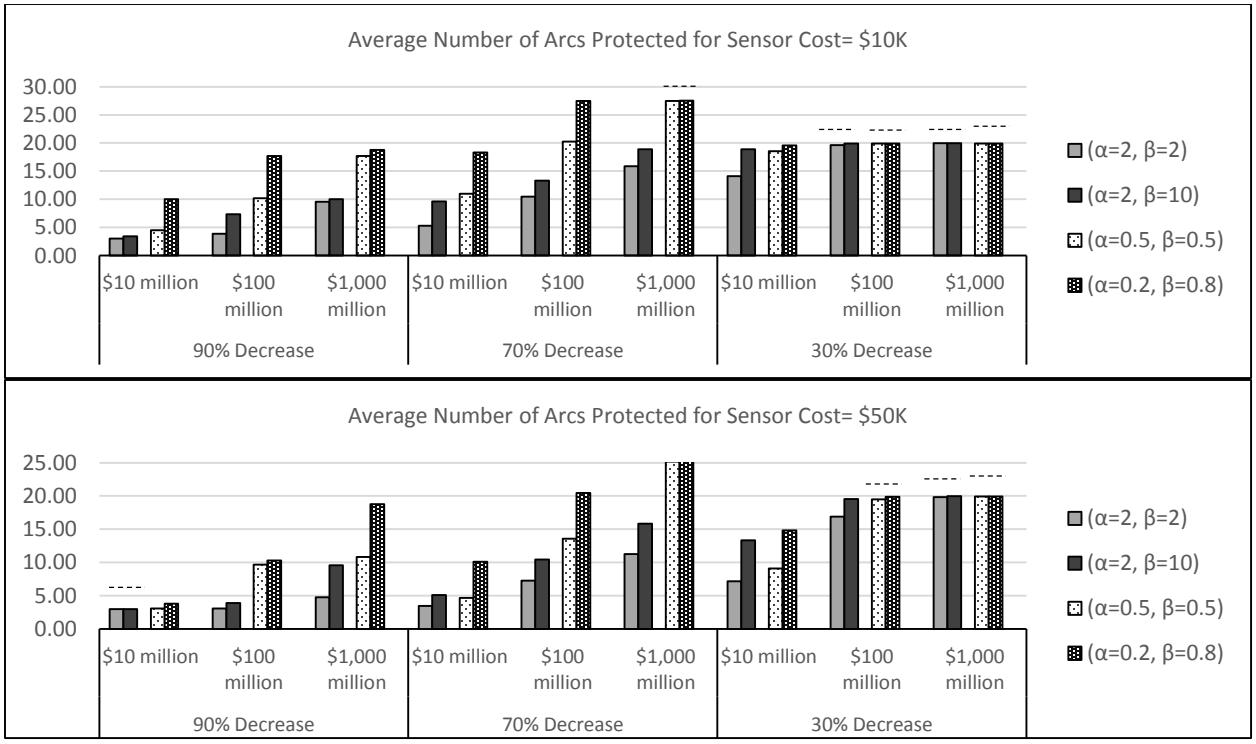

Figure B. 20 Optimal average number of arcs protected for different shape of deterrence function, when p_{ij} is generated from Uniform(0.7, 1)

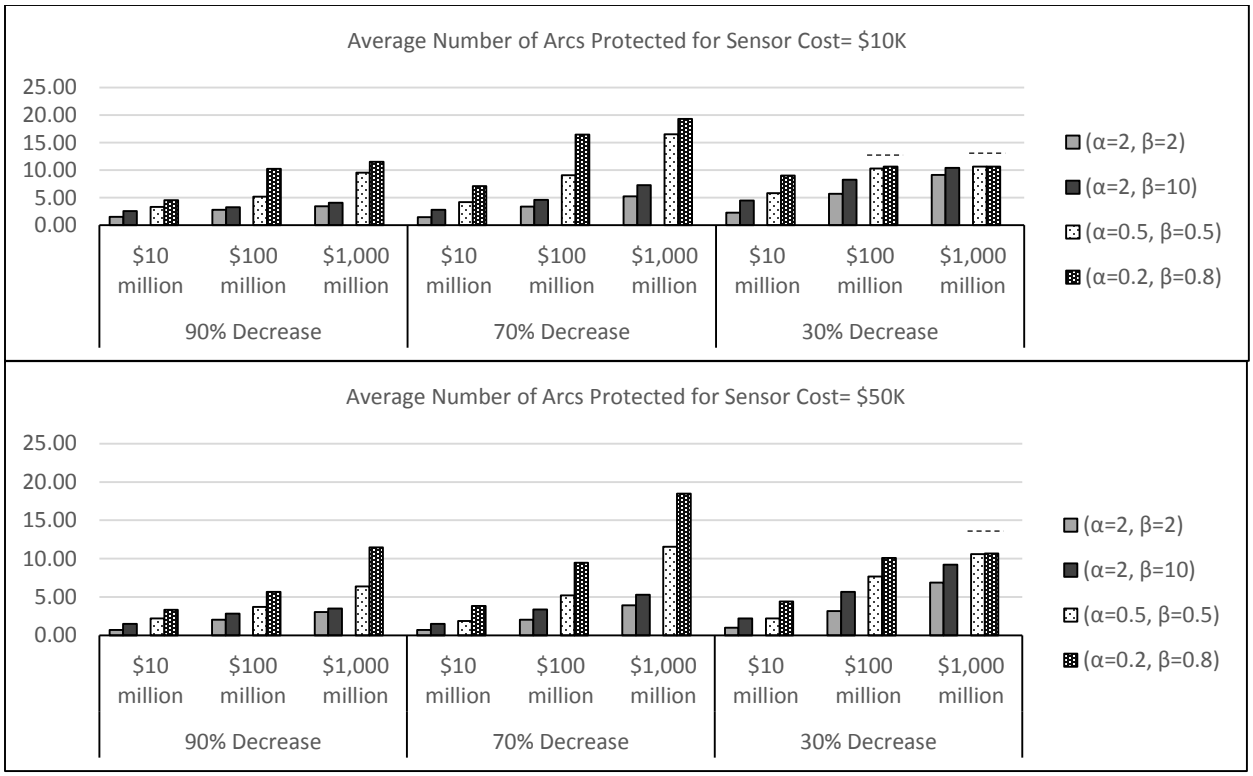

Figure B. 21 Optimal average number of arcs protected for different shape of deterrence function, when p_{ij} is generated from Uniform(0.4, 0.9)

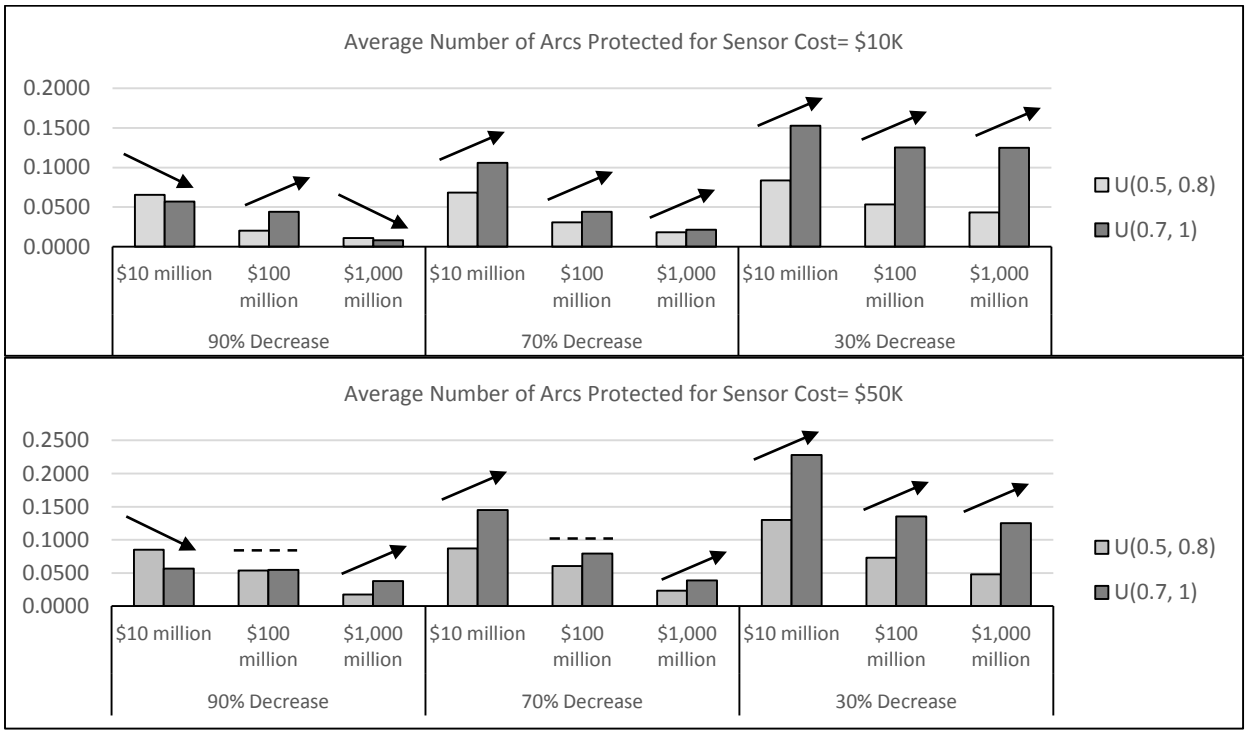

Figure B. 22 The average attack success probabilities for different types of distributions with different means, when deterrence function's shape parameters are (α=2, β=2)

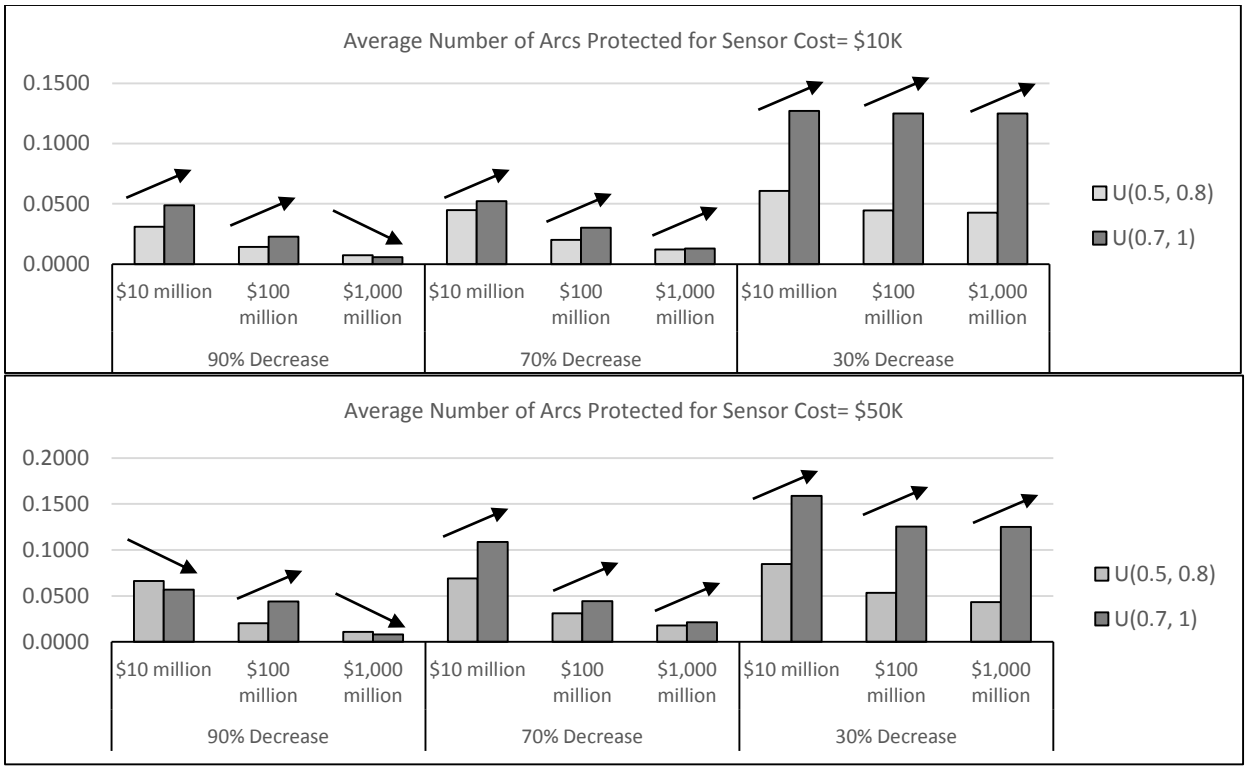

Figure B. 23 The average attack success probabilities for different types of distributions with different means, when deterrence function's shape parameters are (α=2, β=10)

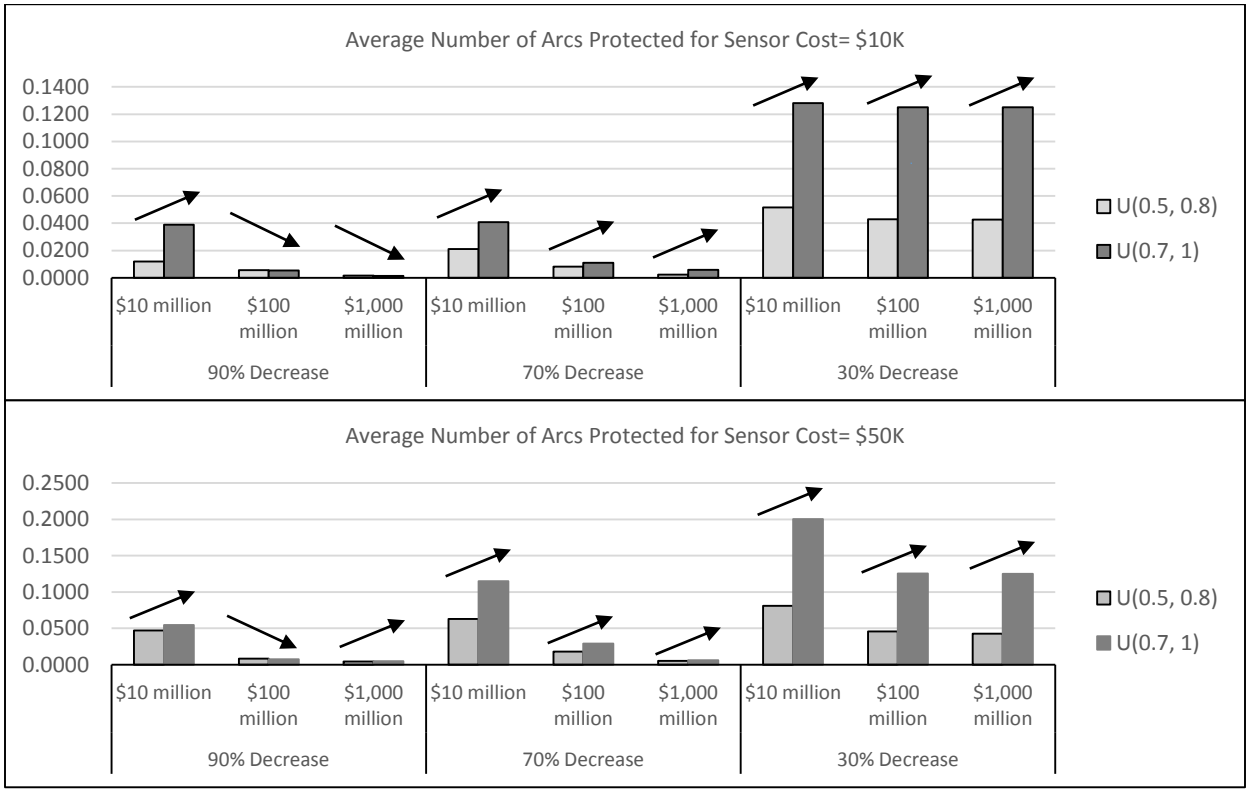

Figure B. 24 The average attack success probabilities for different types of distributions with different means, when deterrence function's shape parameters are (α=0.5, β=0.5)

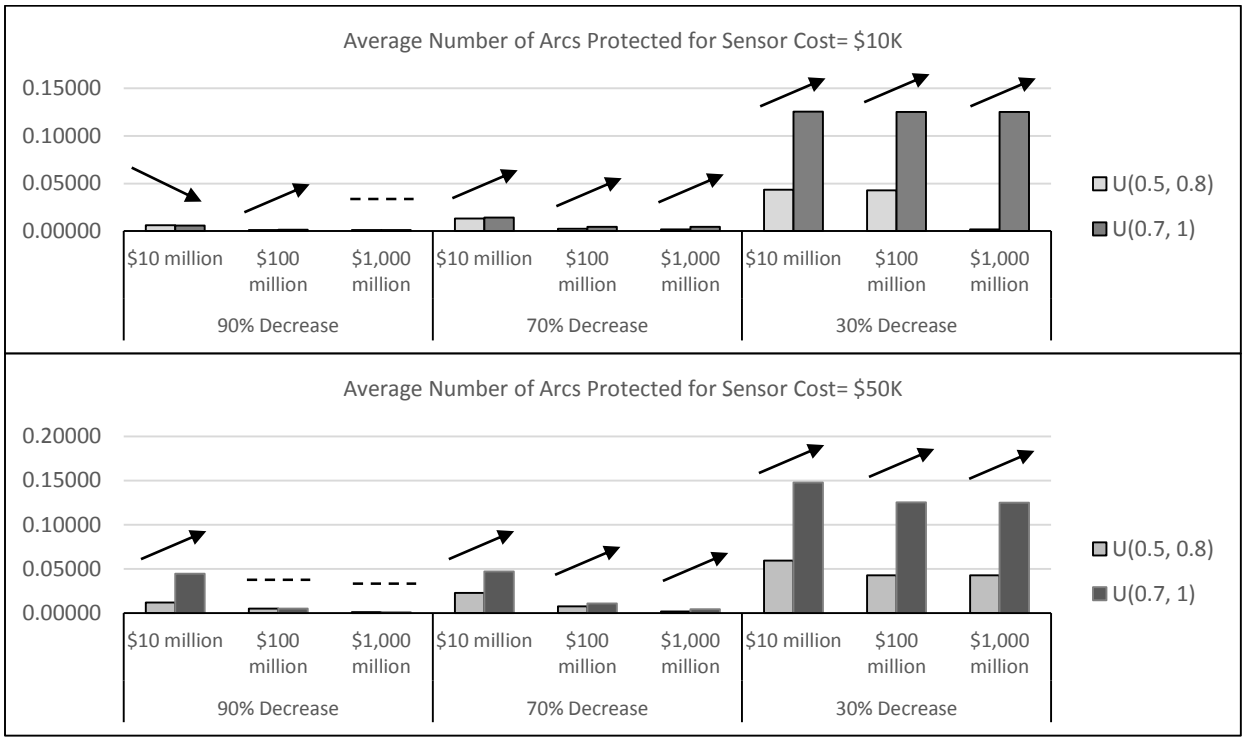

Figure B. 25 The average attack success probabilities for different types of distributions with different means, when deterrence function's shape parameters are (α=0.2, β=0.8)

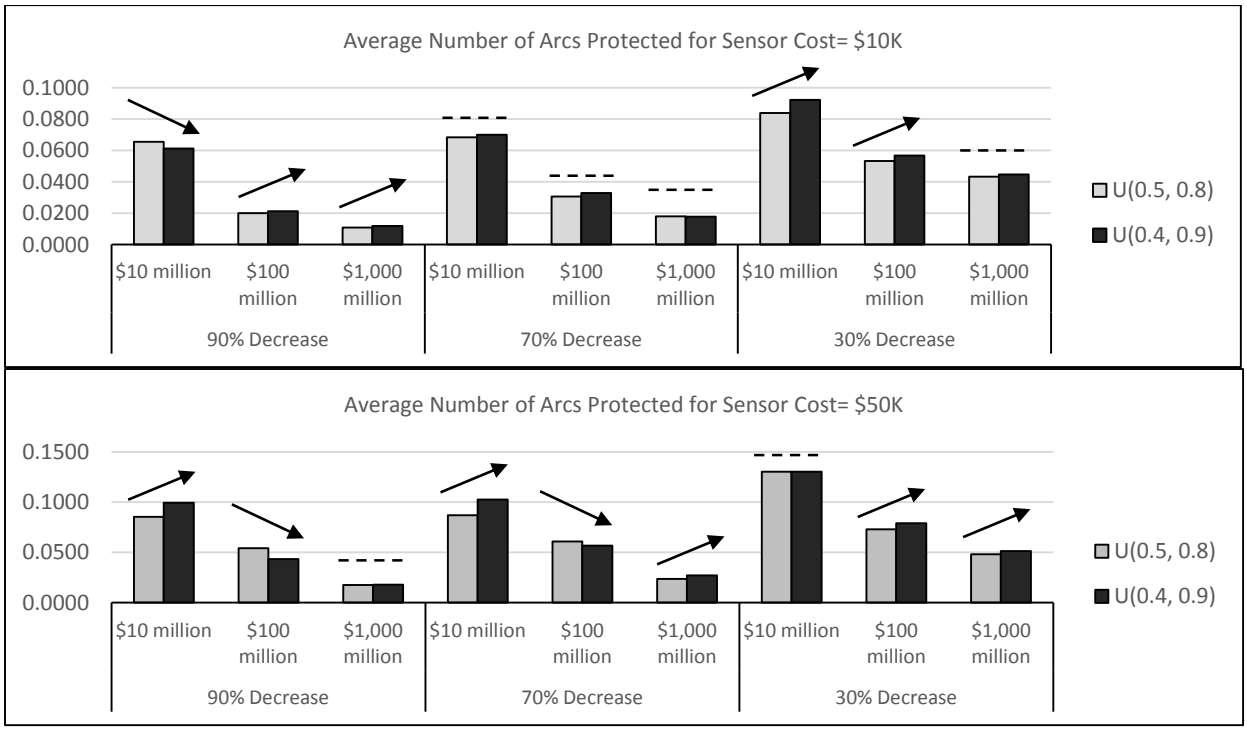

Figure B. 26 The average attack success probabilities for different types of distributions with different variances, when deterrence function's shape parameters are (α=2, β=2)

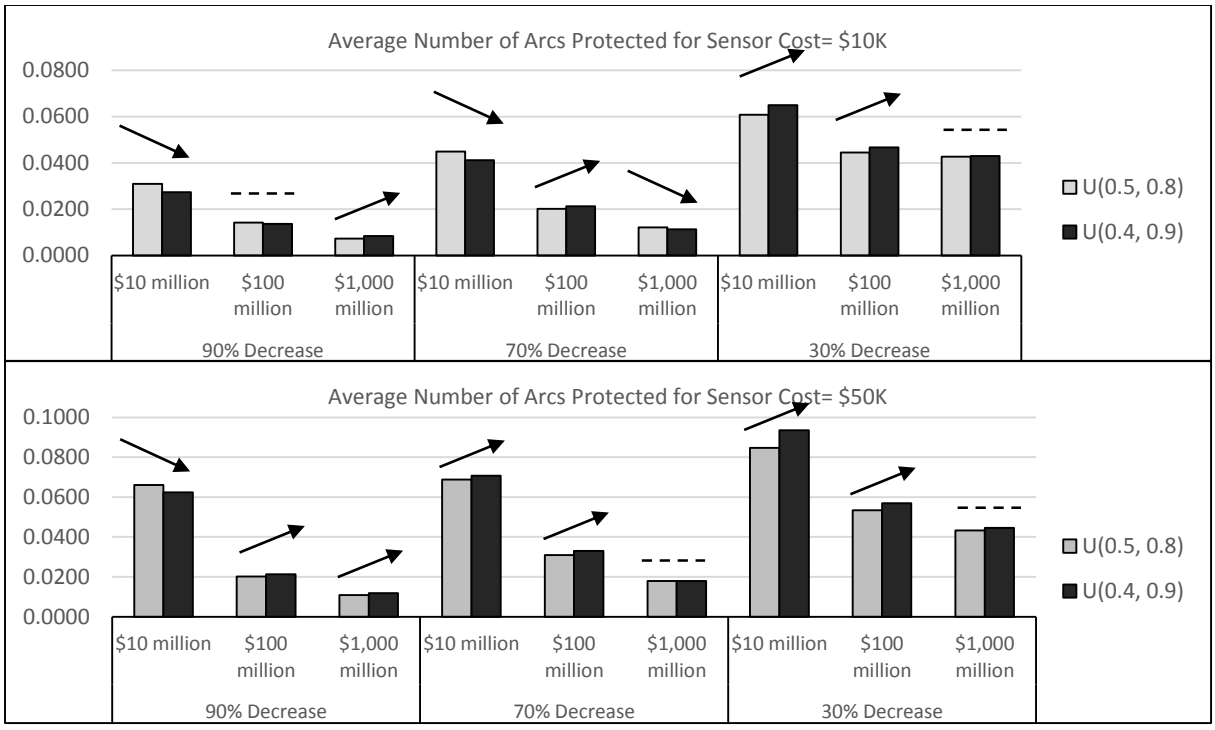

Figure B. 27 The average attack success probabilities for different types of distributions with different variances, when deterrence function's shape parameters are (α=2, β=10)

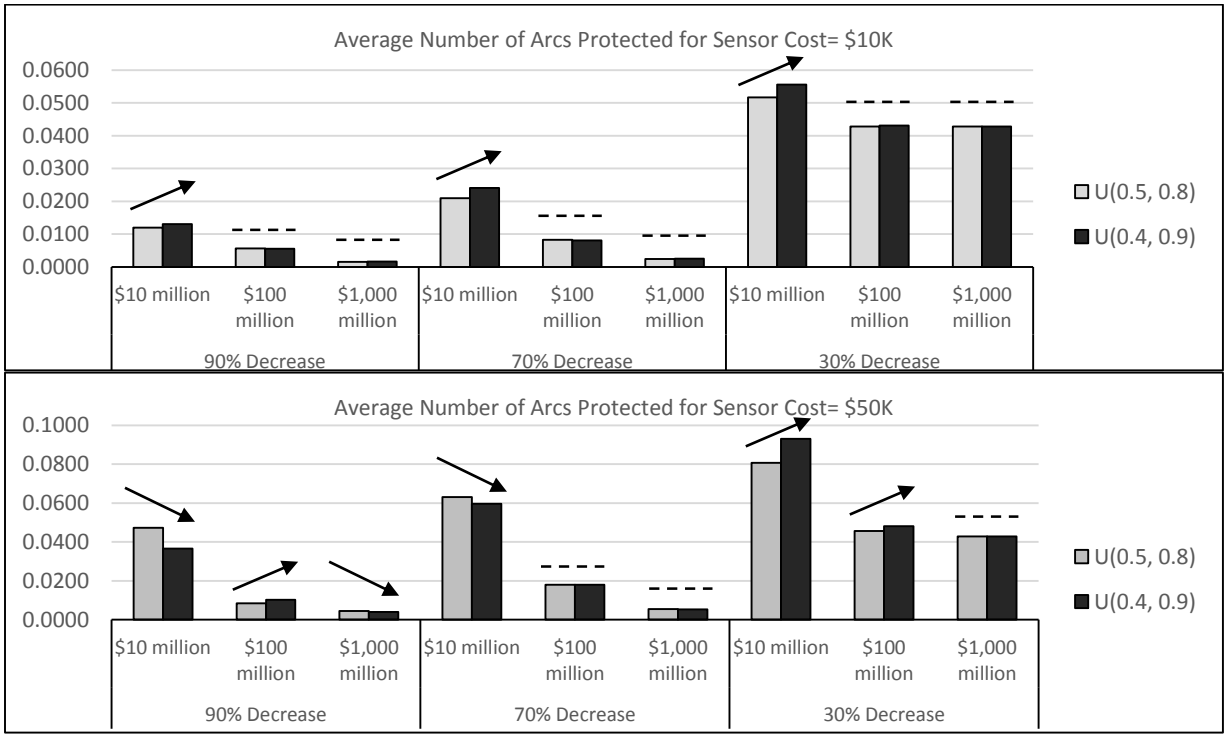

Figure B. 28 The average attack success probabilities for different types of distributions with different variances, when deterrence function's shape parameters are (α=0.5, β=0.5)

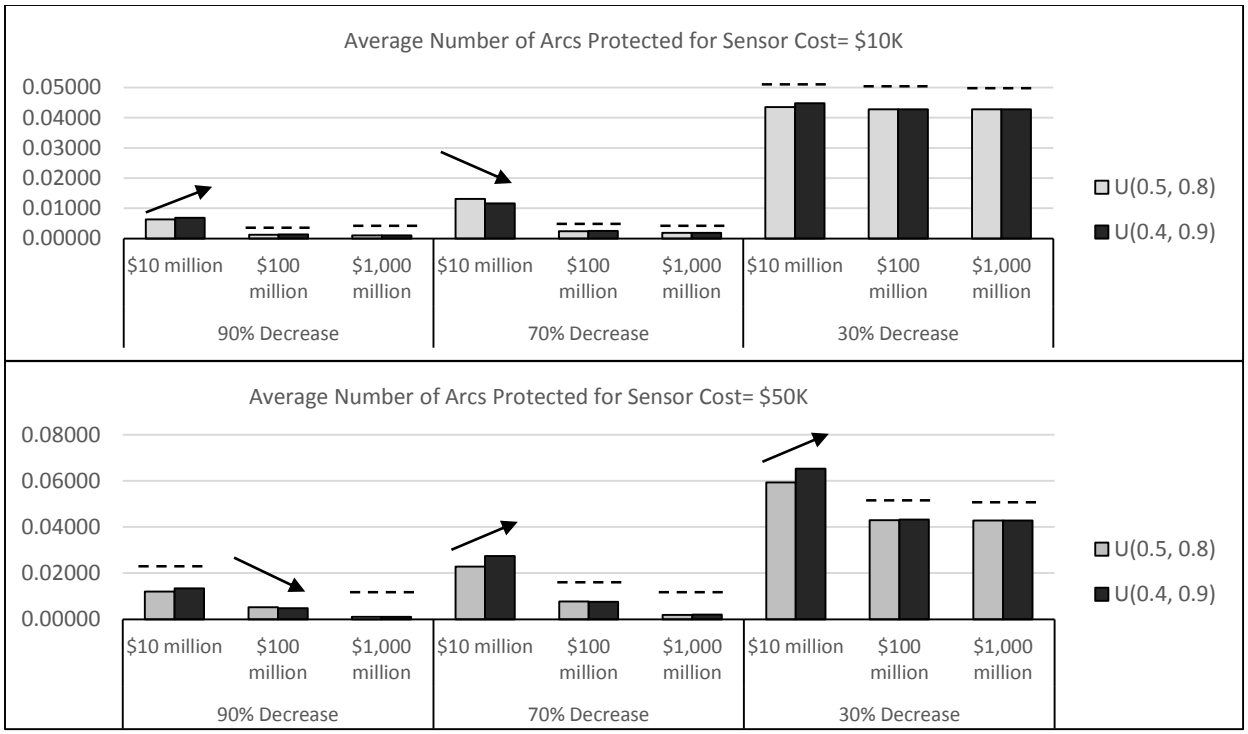

Figure B. 29 The average attack success probabilities for different types of distributions with different variances, when deterrence function's shape parameter are (α=0.2, β=0.8)

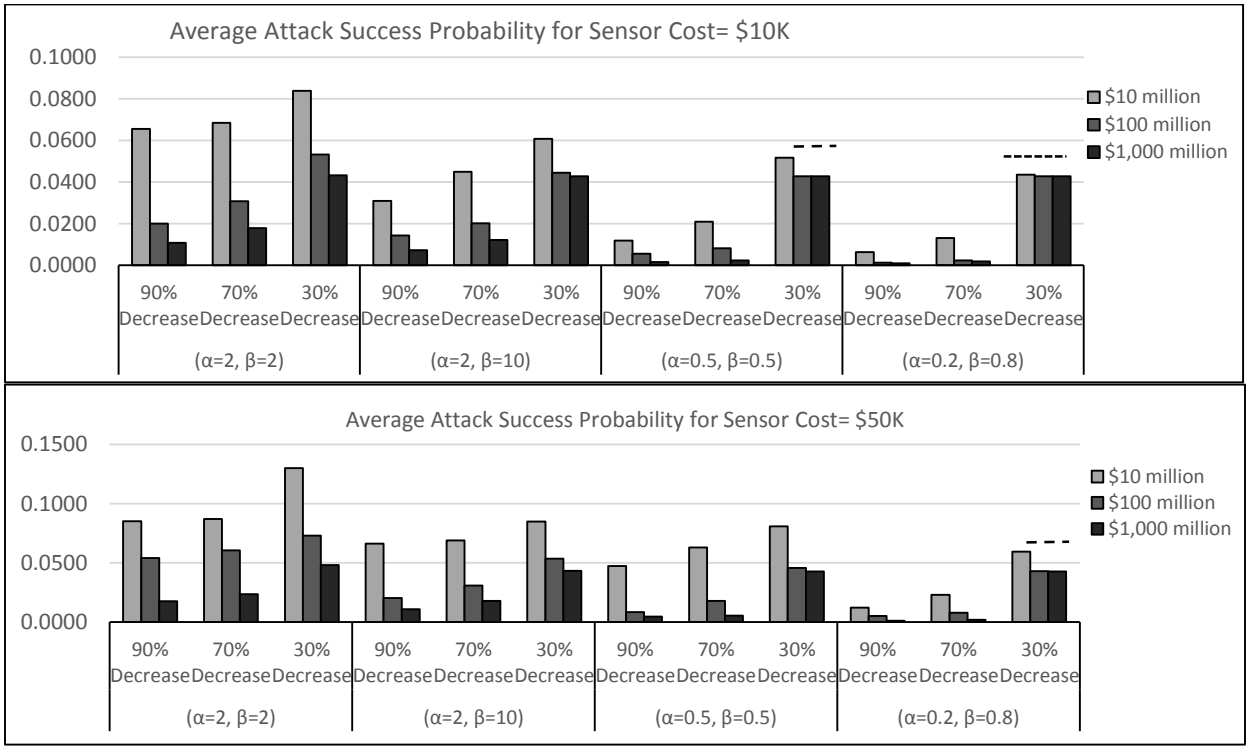

Figure B. 30 The average attack success probabilities for different target values, when p_{ij} is generated from Uniform(0.5,0.8)

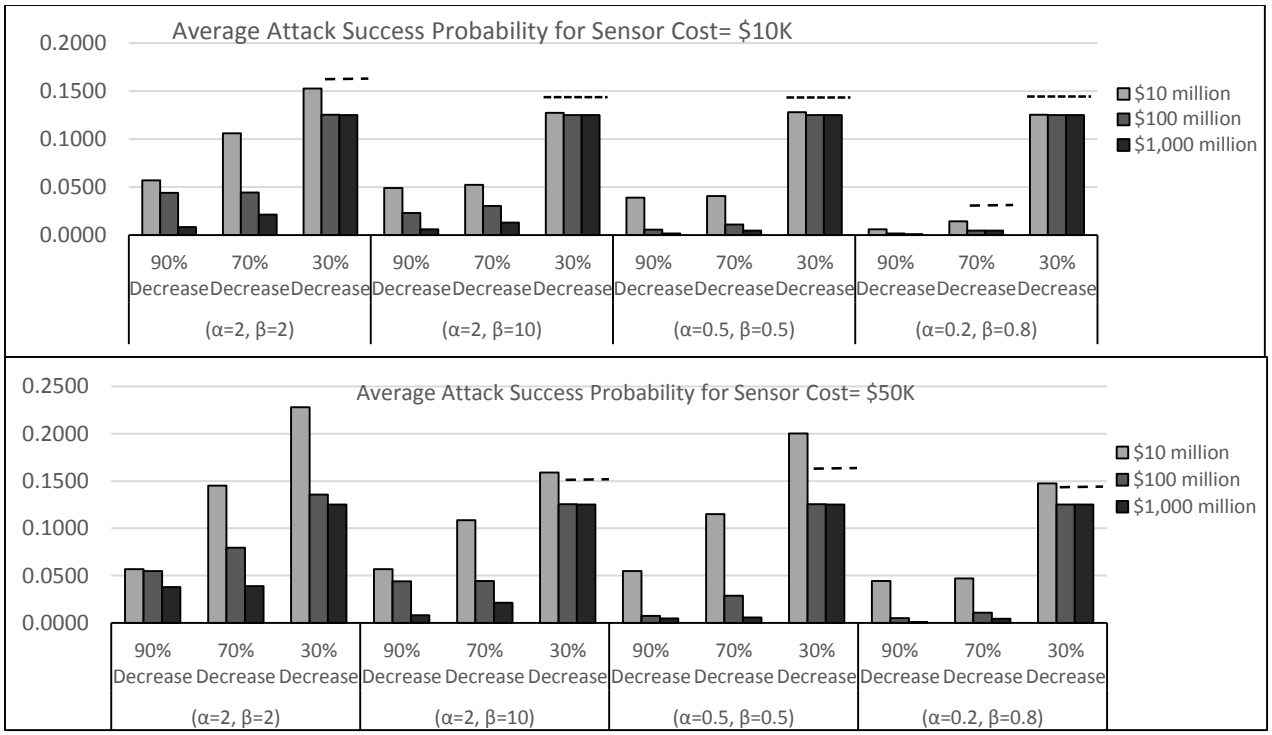

Figure B. 31 The average attack success probabilities for different target values, when pij is generated from Uniform(0.7, 1)

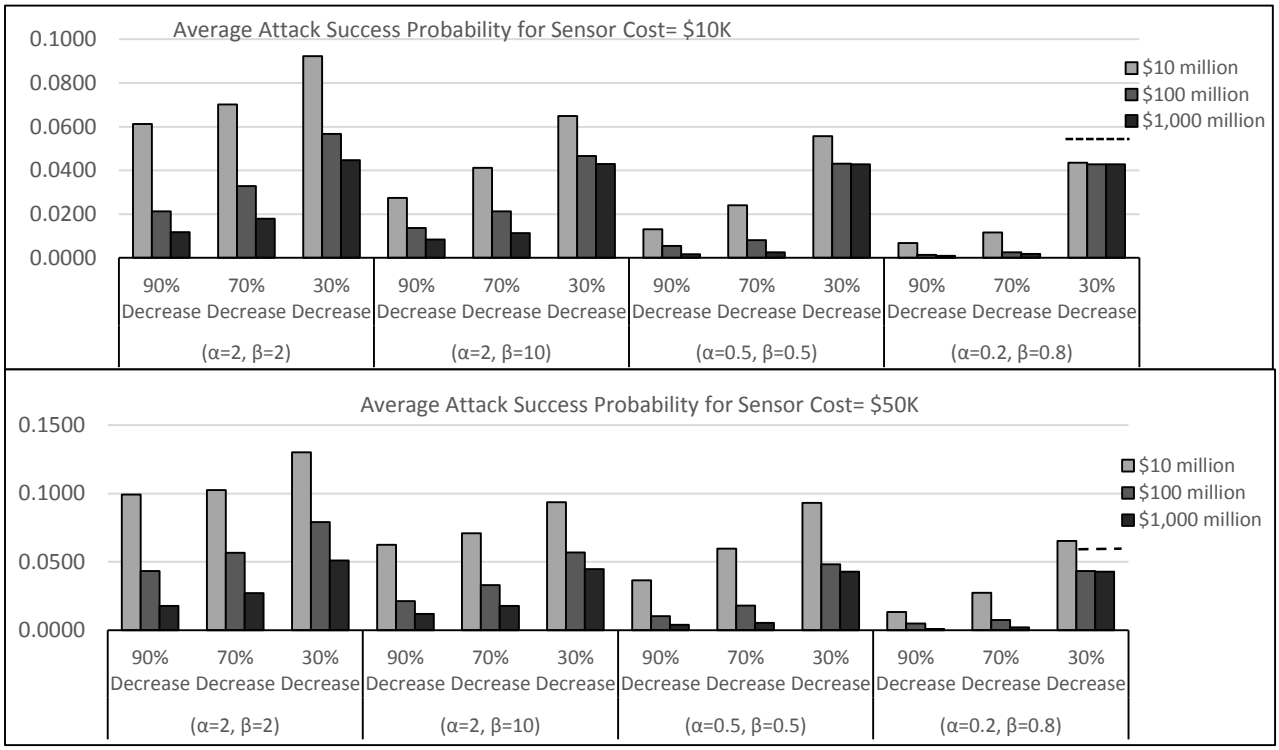

Figure B. 32 The average attack success probabilities for different target values, when p_{ij} is generated from Uniform(0.4, 0.9)

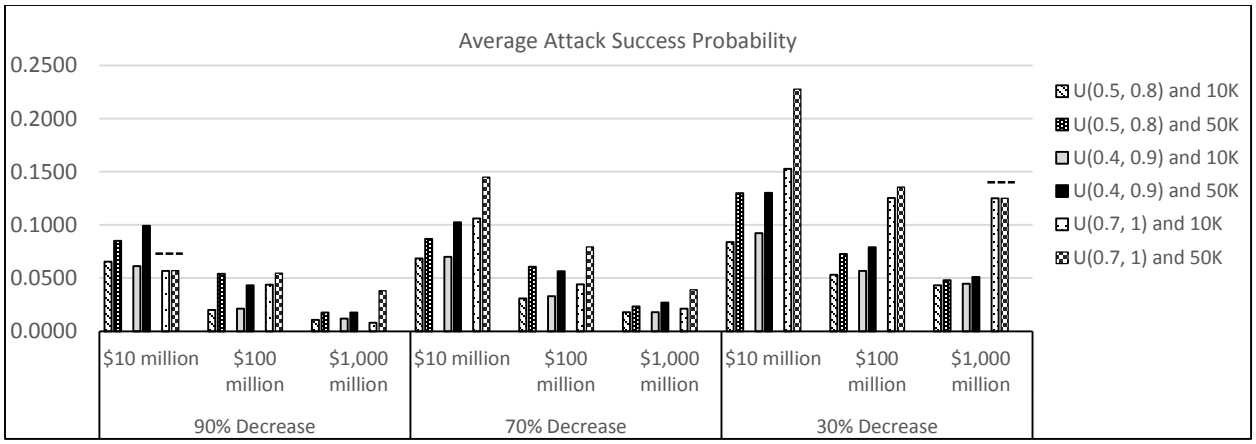

Figure B. 33 Comparison of the average attack success probabilities for different sensor costs, when deterrence function's shape parameters are (α=2, β=2)

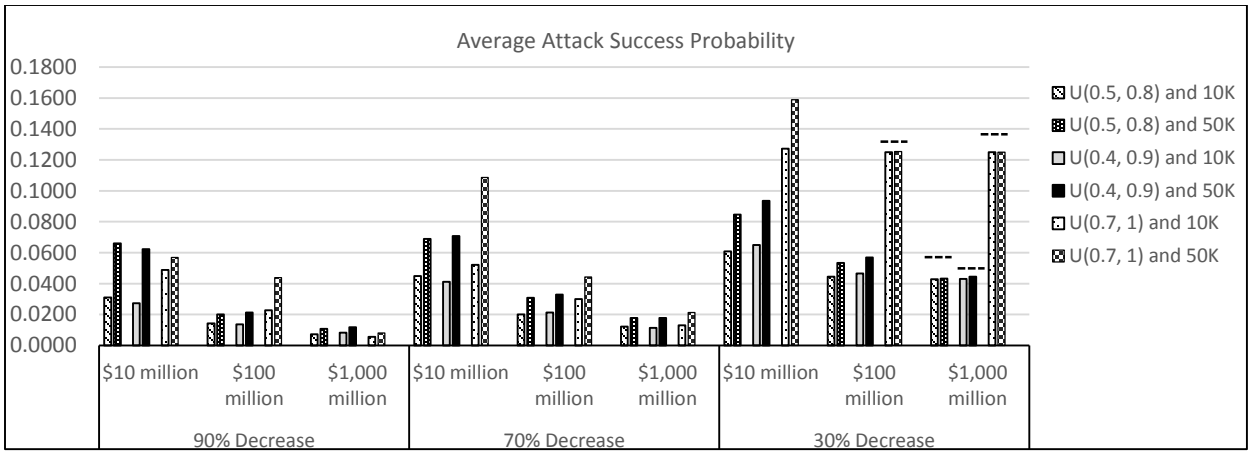

Figure B. 34 Comparison of the average attack success probabilities for different sensor costs, when deterrence function's shape parameters are (α=2, β=10)

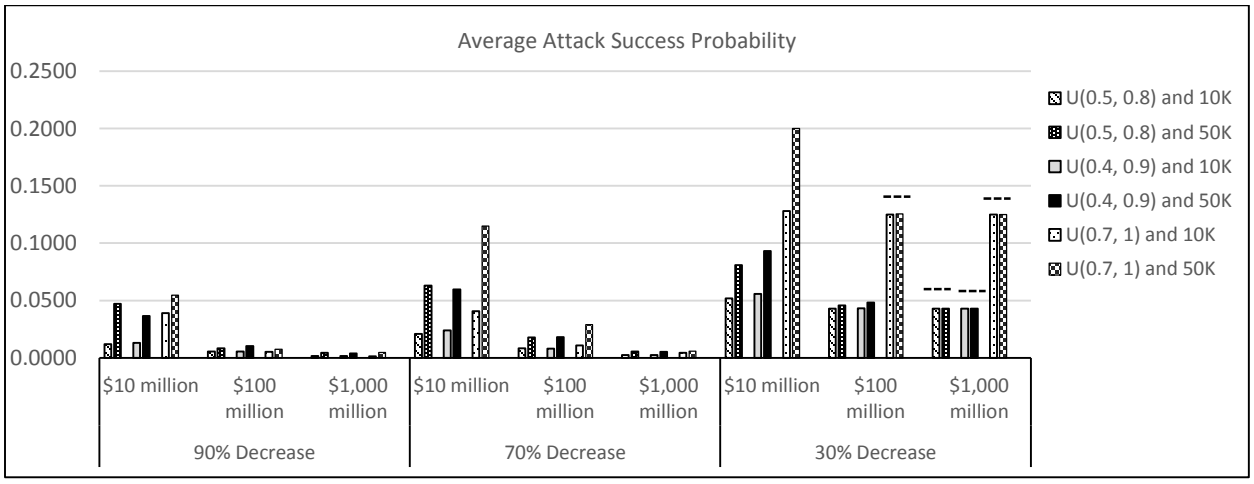

Figure B. 35 Comparison of the average attack success probabilities for different sensor costs, when deterrence function's shape parameters are (α=0.5, β=0.5)

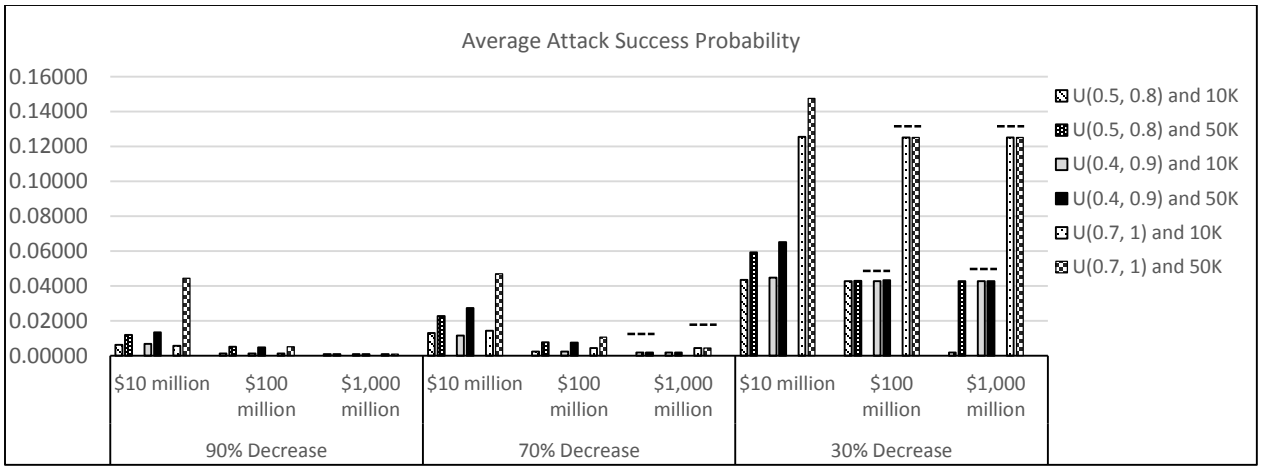

Figure B. 36 Comparison of the average attack success probabilities for different sensor costs, when deterrence function's shape parameters are (α=0.2, β=0.8)

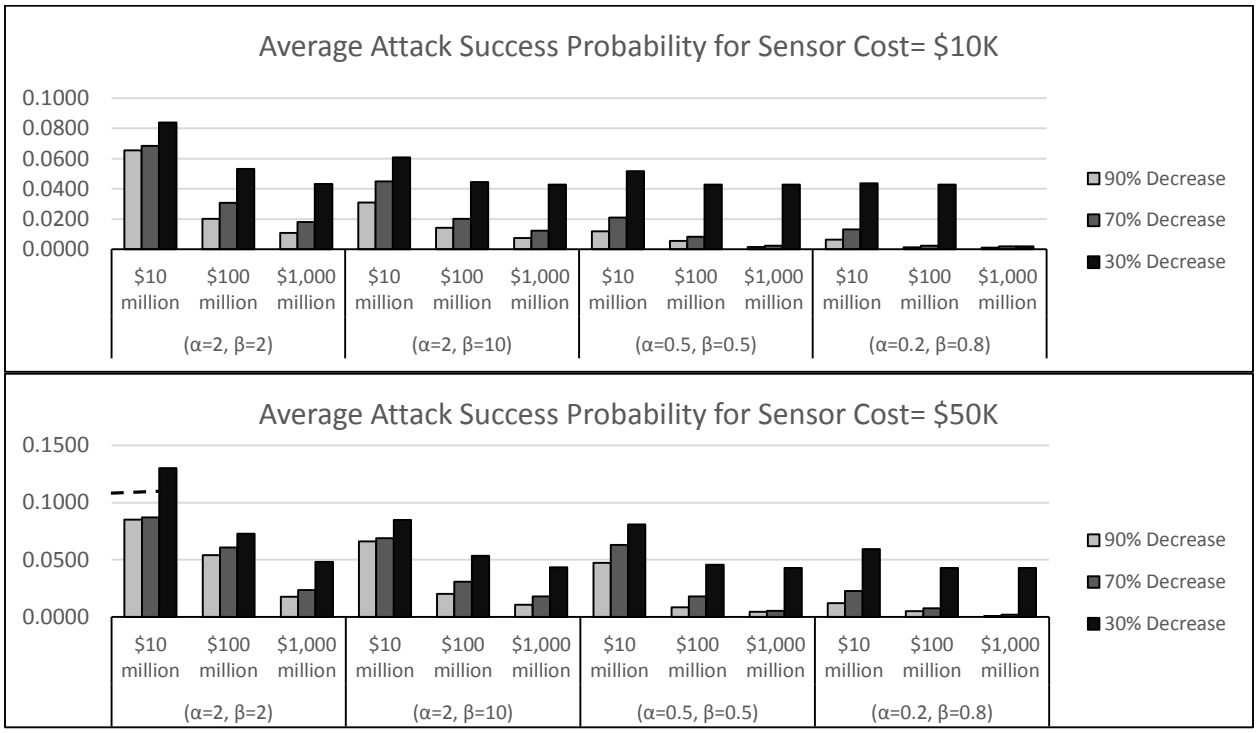

Figure B. 37 The average attack success probabilities for different defensive investment effectiveness, when p_{ij} is generated from Uniform(0.5, 0.8)

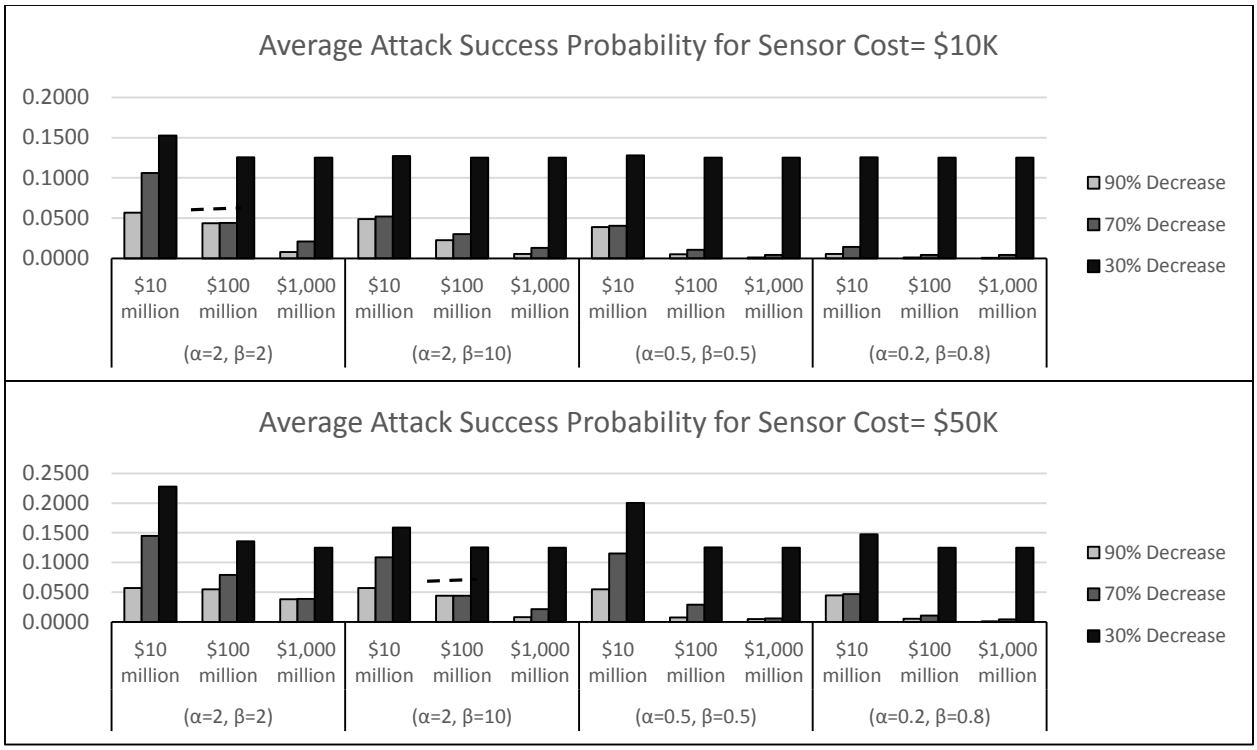

Figure B. 38 The average attack success probabilities for different defensive investment effectiveness, when p_{ij} is generated from U(0.7, 1)

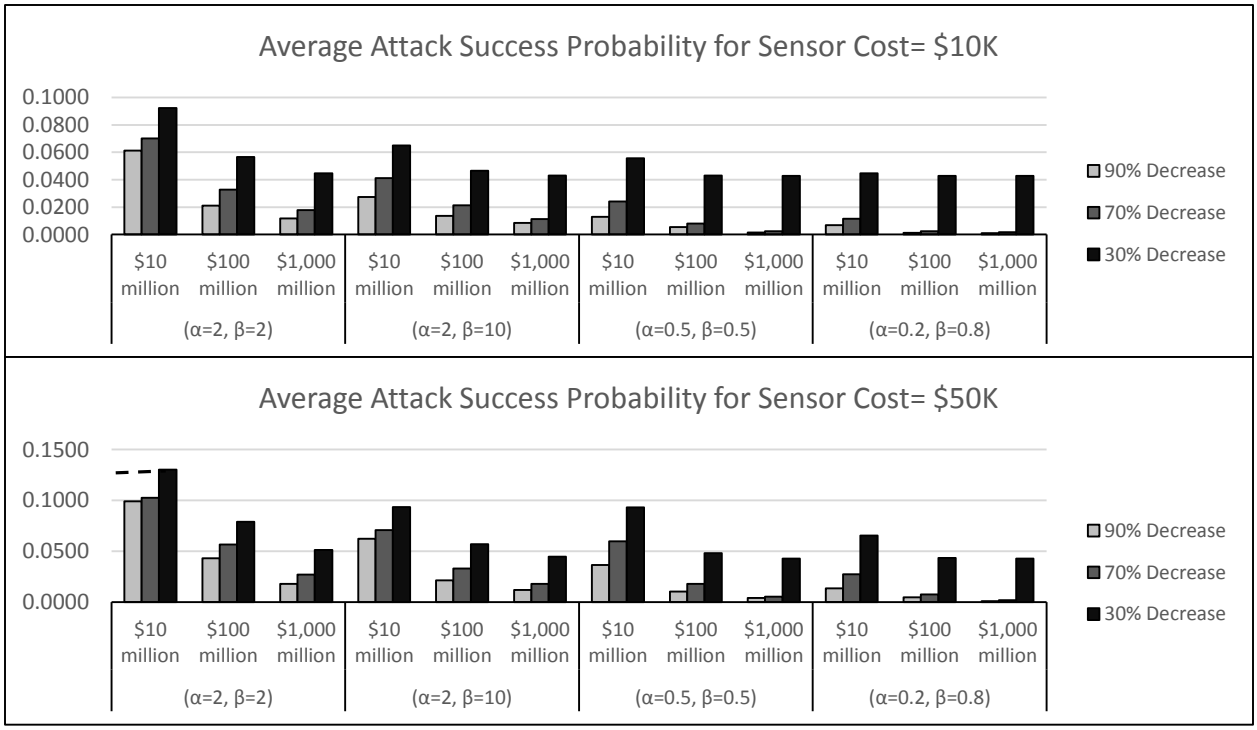

Figure B. 39 The average attack success probabilities for different defensive investment effectiveness, when p_{ij} is generated from U(0.4, 0.9)

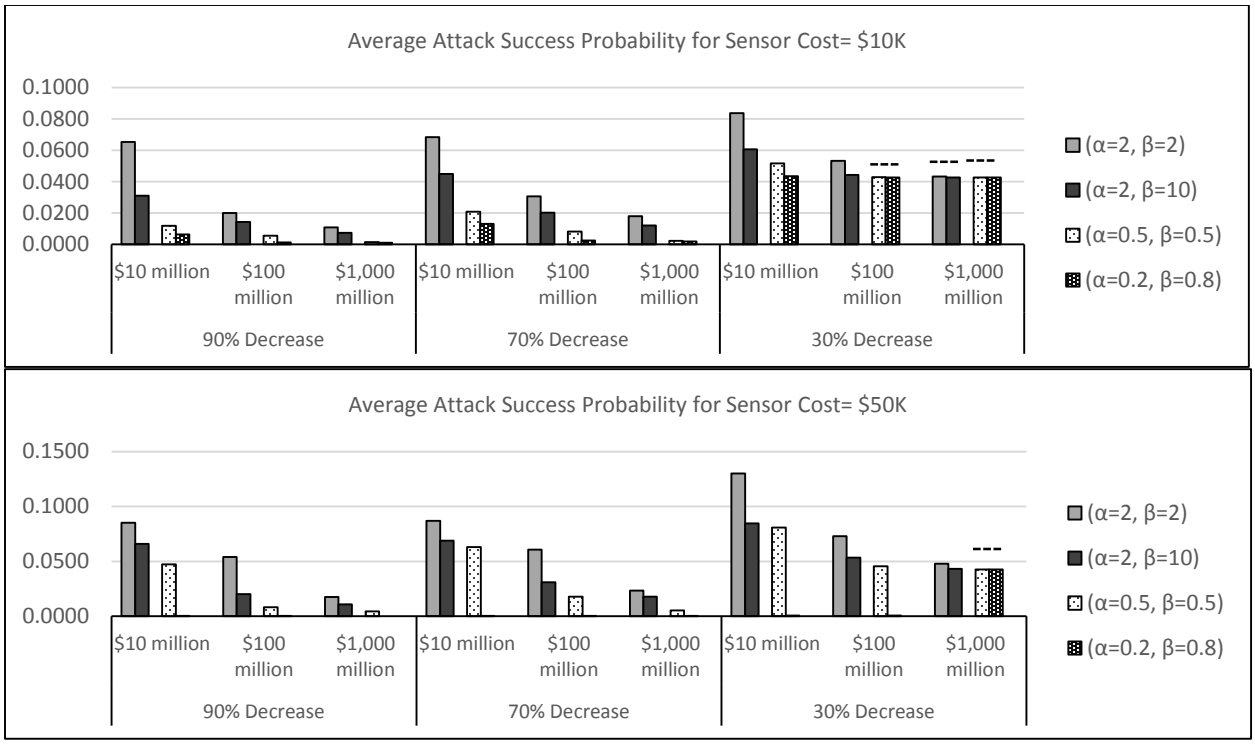

Figure B. 40 The average attack success probabilities for different shape of deterrence function, when p_{ij} is generated from Uniform(0.5, 0.8)

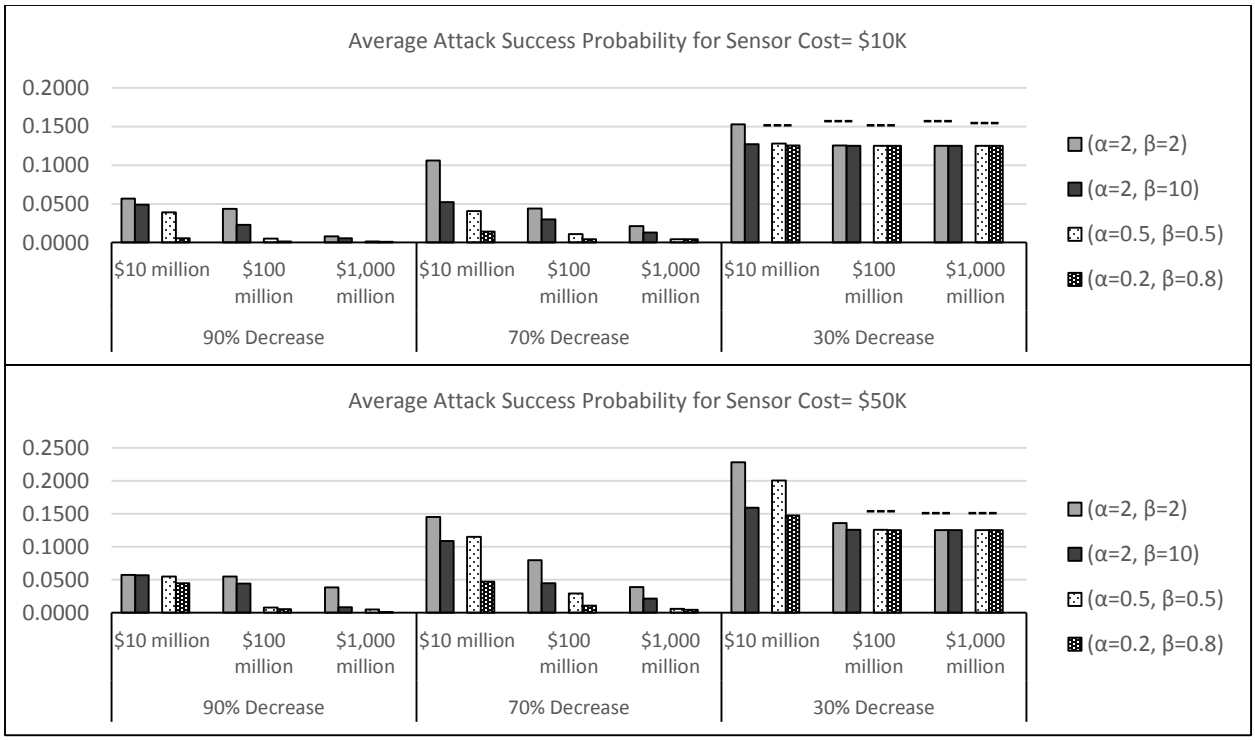

Figure B. 41 The average attack success probabilities for different shape of deterrence function, when p_{ij} is generated from Uniform(0.7, 1)

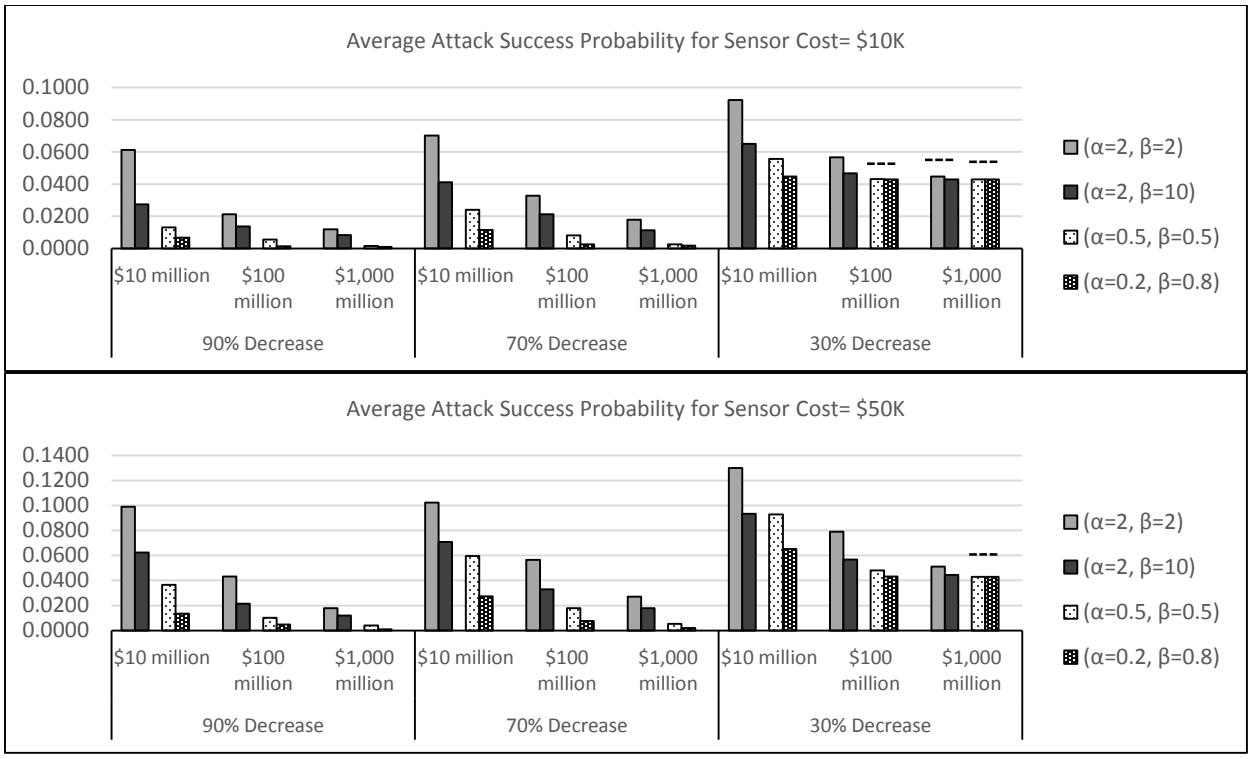

Figure B. 42 The average attack success probabilities for different shape of deterrence function, when p_{ij} is generated from Uniform(0.4, 0.9)

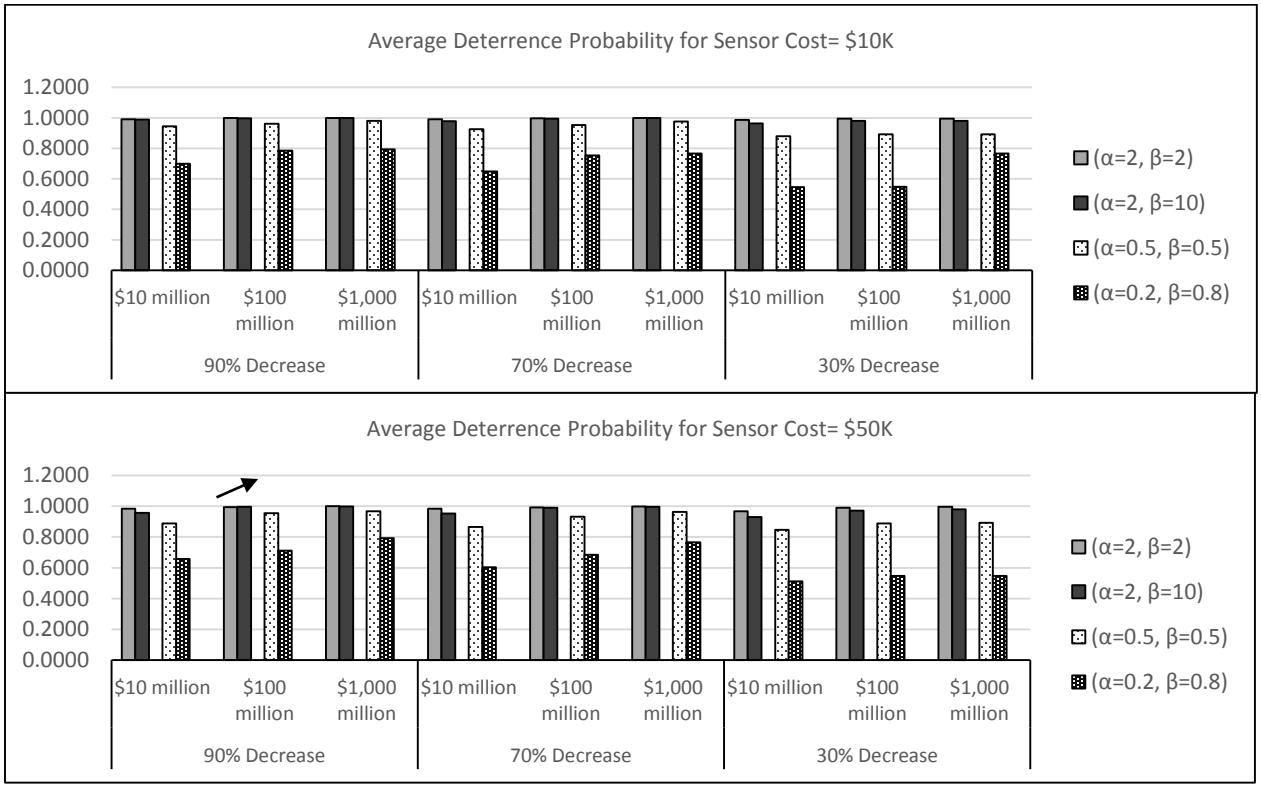

Figure B. 43 The average deterrence probabilities for different shape of deterrence function, when p_{ij} is generated from Uniform(0.5, 0.8)

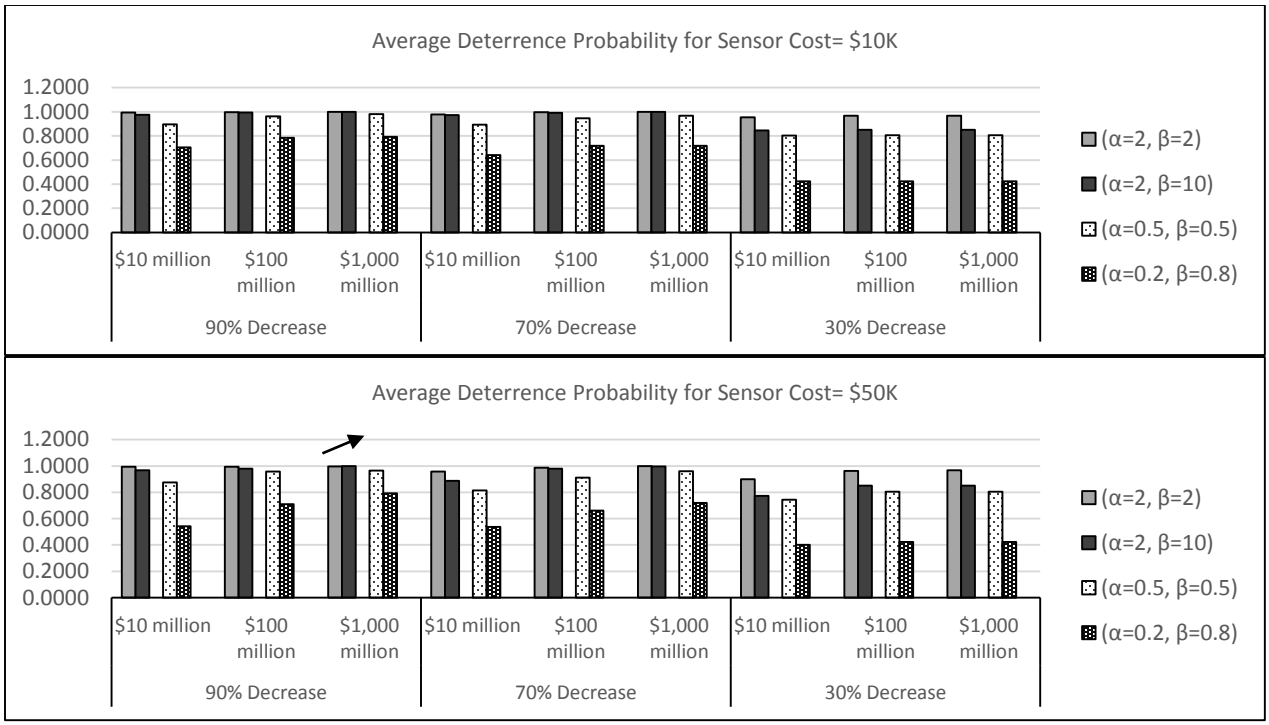

Figure B. 44 The average deterrence probabilities for different shape of deterrence function, when p_{ij} is generated from Uniform(0.7, 1)

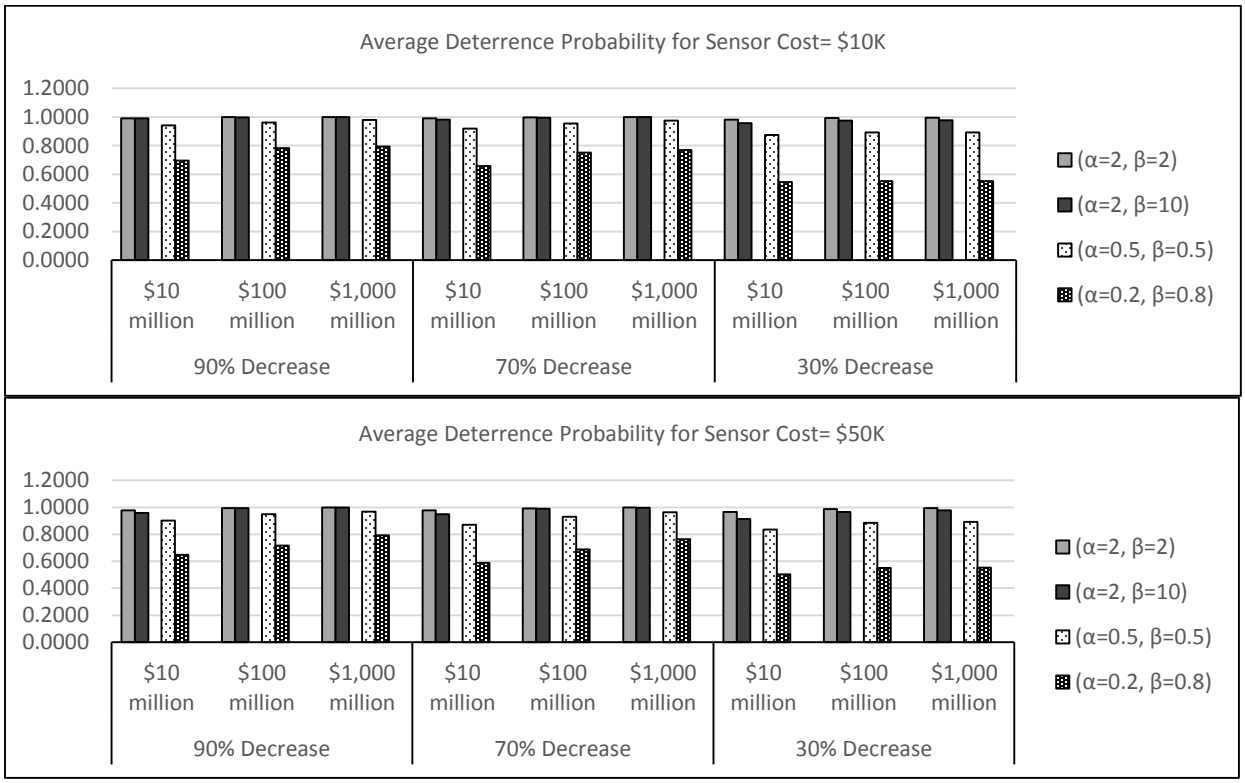

Figure B. 45 The average deterrence probabilities for different shape of deterrence function, when p_{ij} is generated from Uniform(0.4, 0.9)