DIPLOMARBEIT

A Dynamic Defender-Attacker Optimization Model: Modeling Different Attackers as Exogenous Forces

Ausgeführt am Institut für
Wirtschaftsmathematik
der Technischen Universität Wien

unter der Anleitung von
Ao.Univ.Prof. Dipl.-Ing. Dr.techn. Gernot Tragler
und Projektass. Mag.rer.nat. Dr.techn. Dieter Grass

durch
Roman Wanek
Dr.-Natterergasse 2-4/4/18
1020 Wien

Wien, November 2011 _____

Abstract

Based on the ideas of a game theoretical model presented in the paper "The Timing and Deterrence of Terrorist Attacks due to Exogenous Dynamics" by Kjell Hausken and Jun Zhuang (forthcoming in the Journal of the Operational Research Society), in this thesis a nonlinear optimal control model will be formulated, which is linked to an ongoing conflict in Colombia. In this framework, the decision maker has to decide whether to invest a (normalised) budget into the security level of an asset he tries to defend against an attacker or directly into the asset in form of repairs or upgrades. In theoptimal control formulation presented in this thesis, the second player of the game theoretical model will be replaced by an exogenous factor in form of a "reaction function". This nonlinear optimal control model then will be solved by applying Pontryagin's Maximum Principle.

The main goal of this thesis is to analyze how different kinds of attackers affect the model's results and optimal solutions. In a first step, strictly monotone and strictly convex (concave) reaction functions will be applied. For a given set of parameters values, which describes a well-organized attacker, the problem will be solved and a sensitivity analysis will be carried out. In an extension, more complex, convex-concave (concave-convex) reaction functions will be used to analyze how they affect the model's outcome.

Acknowledgements

First of all, I would like to thank Prof. Dr. Gernot Tragler, who introduced me to the topic of terror-models and made it possible to write this thesis. Inviting me to different meetings with his colleagues ultimately aroused my interest in this topic. I also want to thank my advisor Dr. Dieter Grass, who showed much patience with me while providing great help with his toolbox. Without him I would still be sitting here, calculating stable paths with a pencil on a paper.

Of course I also want to thank all my friends. The ones I had before and the ones I met during my studies. More important than helping me when I was facing mathematical problems, is the time I was able to spend with them together, which made studying much more than just learning.

Last but not least I want to thank my family. Without them I would not be, where I am now.

Contents

Chapter 1
Introduction

1.1 The Colombian Pipeline War

Located in the North of South America, the Republic of Colombia with its approximately forty million people living in this second-most populous country after Brazil is facing a civil war since the mid-sixties and therefore for almost fifty years. Since this work does not comment on the political or historical situation of Colombia or the causes for the war, it should only be mentioned that the main parties of this armed conflict are:

- the government or rather the police and military forces of Colombia,
- the AUC (Autodefensas Unidas de Colombia or United Autodefenses of Colombia): a union of paramilitary rightist groups fighting the leftist rebels in Colombia and civilians they see close to the rebels,
- the FARC (Fuerzas Armadas Revolucionarias de Colombia or Revolutionary Armed Forces of Colombia): a leftist guerilla movement, which also caused many civilian casualties, fighting against the colombian government, and
- the ELN (Ejército de Liberación Nacional or National Liberation Army): another leftist guerilla movement fighting the colombian government but also being in conflict with the FARC who even declared war to the ELN in December 2006 lasting until December 2009.

The latter three groups are classified as terrorist organizations by the European Union (see [3]).

As mentioned above, this work will not comment on the possible causes of the civil war. However, it is undoubtedly clear that the civilian population of Colombia has suffered severe damages in the course of this conflict as the following example will show.

In 1983, the U.S.-based corporation Occidental Petroleum discovered an onshore oil field in the Northeast of Colombia named Caño Limón, which turned out to be the second largest in Colombia. After the discovery, an oil pipeline, the Caño Limón–Coveñas pipeline, with a length of 780 kilometres was built reaching from the Arauca Departement to the Carribean port of Coveñas in the Northwest. Construction took three years and in 1986, the pipeline was opened and production started.

For Colombia, oil soon became the most valuable export product ahead of coffee and coal. The country even became one of the largest foreign suppliers of oil to the United States, whose interest in the pipeline was huge since they tried to diversify their sources of oil. Of course, also the leftist rebels were aware of the enormous importance of the pipeline to the state. Hence they took advantage of the fact that a 780 kilometre long pipeline was on the one hand very easy to spot and on the other hand, because of its length, almost impossible to defend. They started attacking the pipeline.

The bombings of the pipeline not only caused severe economical damage because of non-performance but also affected nearby residents in many ways: not only did the spilled oil contaminate their drinking water, it also caused damage to the farming land, not to speak of the fear of falling victim to the rebel groups.

In 2001, when the pipeline was closed for over 200 days of the year due to 170 attacks (see Table 1.1), the army decided to increase security efforts and added three batallions to the two already stationed along the pipeline. As one can see in Table 1.1, the attacks on the Caño Limón Pipeline decreased dramatically in the following year. After the U.S. government had decided in 2003 to provide over 90 million dollar, which were for the most part invested in military assistance to protect their oil interests in Colombia, the number of attacks fell to a tenth of 2001 in 2004. It was finally possible to reduce the harm of the Colombian people living near the pipeline and the number of attacks on the pipeline, which sum up to 950 bombings since the 1980's.

	2001	2002	2003	2004
Caño Limón – Coveñas	170	41	34	17
All Pipelines	263	74	179	103

Table 1.1: Attacks on Oil Pipelines 2001-2004 (source: [4])

1.2 Game Theory in Defender-Attacker Models

In recent years much research has been conducted on the field of attacker-defender models, and many papers have been published. Since this thesis presents an optimal control model, two examples of a game-theoretic approach will be of special interest in this section. They will help to get some insights on defender-attacker models and to understand some of the basic ideas, which will then be transformed to formulate a corresponding optimal control model.

1.2.1 "The Timing and Deterrence of Terrorist Attacks due to Exogenous Dynamics"

The paper, written by Kjell Hausken and Jun Zhuang (see [5]), deals with a counter-terrorism two-stage game that is repeated over T periods. In this model, two players participate in a game where one player, the defender, moves first and the second player, the attacker, moves second, given the information on the defender's strategy. Given some kind of asset, a collection of assets or even an entire infrastructure, the defender's goal is to maximize his/her utility, which depends on the valuation of the asset and the applied defensive measures.

The defender and attacker both choose their effort in protecting and attacking the asset, d_t and A_t (both ≥ 0), facing unit costs for the chosen effort, b_t and B_t respectivly. The defender's valuation of the asset equals v_t, the attacker's V_t accordingly. In addition, c_t describes an "inherent defense level", which is interpreted by the authors as a "carried-over defense from history". Furthermore, depending on the defender's effort of protecting the asset, d_t, and the attacker's effort to damage it, A_t, the probability of a successful attack and damage to the asset consequently is described by $P(d_t, A_t) = \frac{A_t}{A_t+d_t+c_t}$. This so-called "contest success function" is based on the work of S. Skaperdas (see [7]) with the extension that the variable c_t makes sure that previous decisions of the defender do have an effect on current decisions.

Given the variables, both players of the game try to maximize their expected utility:

$$u_t(d_t, A_t) = [1 - P_t(d_t, A_t)]v_t - b_t d_t \quad \text{for the defender,}$$
$$U_t(d_t, A_t) = P_t(d_t, A_t)V_t - B_t A_t \quad \text{for the attacker.}$$

As one can see, the utility functions both consist of two terms, one in form of a benefit, the other in form of costs. Solving this two-stage game basically led to four different Subgame Perfect Nash Equilibria depending on the ratios of the defender's and attacker's valuations of the asset, the unit costs for defending and attacking, and of course the effort of the defender. In the first case, the attacker does not attack at all despite zero effort of the defender. This behavior is optimal for the attacker, because in this case his valuation of the asset is small compared to the attack costs and the historical defense level.

However, with increasing attacker's valuation of the asset, V_t, the defender, in the second case, gets forced to raise his effort above zero to deter the attacker leading to the third case, where both players choose efforts greater than zero leading to a defense/attack-equilibrium. Finally, in the fourth case, the attacker's valuation of the asset gets too high and the defender removes his defense.

1.2.2 "Defending against multiple different attackers"

In this work by Kjell Hausken and Vicki M. Bier (see [6]), the authors basically extend the model described in the previous section. Here, one defender of an asset faces n heterogenous attackers. To quote an example for two heterogenous attackers, they mention a defender's computer security efforts. In this case, the defender may defend his infrastructure against highly educated, professional hackers and so-called "script-kiddies", mostly adolescents without any basic knowledge of computer security, who only use pre-assembled instruction to hack external computer systems and networks.

Furthermore, the authors expand their research to three different game-theoretical scenarios. They analyze a game, in which all participants move simultaneously, a two-stage game, in which the defender moves first, and a two-stage game in which the attacker moves first.

In this model, every attacker is assigned with his/her own valuation of the asset and his/her own unit attack costs. The probability functions G_i (contest success functions) of attacker i to destroy the asset are interpreted as fractions of the asset the participants of the game compete for. Despite this different interpretation, these functions (G_i for attacker i and g for the defender) have the same ratio form as in the above sketched model. According to the ideas of [5], the players again try to maximize their utility function consisting of a benefit and a cost term.

Apart from results similar to those of the model described in the previous section, with unit costs for defending and attacking and the valuation of the assets affecting the model's

equilibrium levels, there are also other interesting results, which are based on the number of players. For example, it is possible that one of the attackers is extremely strong, and therefore will reclaim a big part of the asset, so that the other attackers withdraw from the contest. On the other hand, the defender is likely to withdraw from the contest if she faces many strong attackers or if the attacker moves first.

1.3 The Idea

As one can conclude given these two examples, defender-attacker models in game theory are very interesting to analyze due to the dynamic structure of the models. However, optimal solutions of this game-theoretic approach always imply that participants of the game behave in a rational way, trying to maximize their utilities. However, in recent years the world had to face attackers who acted based upon political reasons. The ways in which attackers retaliated could no longer be described as rational. It seems likely to mention the war in Afghanistan and the attackers methods of suicide bombings as an example of such an irrational way of conflict.

In this thesis, the goal will be to formulate an optimal control model roughly based on the ideas of the above game-theoretical models. In contrast to [5] and [6], the attackers will influence the model as exogenous forces in form of reaction functions responding to the decision maker's level of security. It will then be analyzed how a decision maker's optimal control policy changes, as she faces different kinds of attackers.

Chapter 2
The Model

In this chapter the optimal control model will be introduced in a general formulation. It will be formulated as a two-state model with one control. Besides providing interpretations for the functions used in this model, the connections to the game-theoretical models introduced in Chapter 1 will also be mentioned.

2.1 State and Control Variables

Just like in the models described in the introduction, consider an asset a decision maker (state, corporation, group,...) wishes to defend against some kind of attacker. Such an asset could be a building, an important area (in context of raw materials one may think of oil fields or gold mines), or a whole infrastructure. Similar to [5], the defender values this asset with the state variable y. This state of the optimal control model can be seen as the accumulated value of money the defender assigns to the asset. Since in this model the value will be of monetary nature, it isn't unlikely to assume that an attacker is aware of the value an asset has for the defender (compare the oil field example from the introduction).

Every time period (say a year for example), the defender faces a potential assault by an attacker, which causes the asset to take damage reducing its value. In terms of the "Pipeline War"-example from the introduction, this reduction in the value of the asset equals the production downtimes if the pipeline cannot transport oil. To keep this model simple, a probability function will be omitted and it will be assumed that every attack is successful. Nevertheless, similar to the contest success function, which was used in the work of [5], [6], [7] and which was influenced by the "inherent defense level", a function will be used in our optimal control model, which will be based on the dynamic analogue of the historic defense level. However, introducing a probability function describing whether

an attack is successful or not could be the objective of further work.

Following the examples froma above, the defender tries to prevent the asset from taking damage. For this purpose she is able to raise the security level x of the asset. This second state variable of the optimal control model could be interpreted as equipment of the army, the quantitiy of security forces, or the possibility of infrastructure to obtain information of following attacks. The security level x takes values in $[0, 1)$ with 0 meaning that the asset is completely unsecured and 1 reflecting perfect security and therefore the ability to avoid damage completely. This case of perfect security of course seems very unlikely, since no one can ever guarantee to secure some asset perfectly. That is why the model later on will be formulated in a way which implies that this boundary case will not occur. In this model, x takes the role of the "inherent defense level" c_t of the model in [5]. It is the dynamic analogue to the discrete expression c_t influencing the situation for the defender in a positive way. To increase the security level, the decision maker is able to invest a share $u \in [\overline{u}, 1]$ of a given budget that will be normalised to 1. x will then be increased by a concave function f depending on the current level of x and u. It can be seen as the effectiveness of investing into the security level and describes the increase of security given a certain level of investement and current security. In this context, $\overline{u}$ can be seen as some kind of minimum security effort. To avoid numerical problems in computing solution paths later on, the case $u \in [0, 1]$ will be realized by setting $\overline{u}$ not to 0 but to a positive level close to zero, $\overline{u} = 0.0001$. Of course, the security level x will not stay at the same level for all times. It can also be reduced by a depreciation rate $\delta \in [0, 1]$. The interpretation of this rate could be loss of equipment due to abrasion or the loss of military forces due to the limited time soldiers are assigned to certain spots of conflict, but it can also be seen as indirect depreciation because of advancements in the attacker's capabilities.

The remainder of the budget which is not invested in x, $1 - u$, will be directly invested into the asset leading to an increase of its value y. This investement can be interpreted as repairs, better equipment, or better infrastructure. In relation to the pipeline example one may think of measures to increase the transport capacity of the pipeline, which would directly result in a higher value for the defender since she can make more money delivering more oil. Similar to the security level x, the value of the asset y can be increased by a linear or nonlinear function g depending on the share of the budget invested in y, $1 - u$. In addition, the value of the asset will be reduced because of the periodic attacks of the opponent denoted by a function μ (see the next section for details).

As one can see in this dynamic formulation of a defender-attacker model, the defender faces the decision wether to invest into security or the value of the asset, leaving him/her

with a trade-off between security and wealth.

2.2 Interpretation of the Remaining Functions

In this section, I will provide a brief overview of the five functions that will be used in the optimal control model.

As mentioned in the previous section, the value of the asset y will be reduced by successful attacks of the opposing force. This reduction is taken into account by a *damage function* μ, which depends on the so-called *attack-intensity function* v, which itself depends on the states x and y. The *attack-intensity function* $v(x, y)$ will be introduced later in Section 2.3, because it will play a crucial role in modeling the attacker's behavior. For now it should only be mentioned that v represents how many people or which equipement the attacker uses for his/her attacks and therefore how much damage she can possibly cause.

One more note is in order. Of course, x, y and u depend on time t, so $x = x(t)$, $y = y(t)$, and $u = u(t)$. However, for the ease of exposition, the time argument will mostly be omitted.

According to the models in the preface, the objective function consists of two terms, one being a benefit function and one influencing the objective value in a negative way. The beneficial term will be called the *wealth function* W depending on the value of the asset y. It can be seen as the benefit of a high-valued asset. Say, for example, that investing into the value of the pipeline and therefore raising the transport capacity results in overall positive effects for the whole country because of increased tax income due to increased oil sales. Hence, this wealth function combines all positive effects caused by investement in the asset. In contrast to the benefit function, the *harm function* D combines overall negative effects caused by a damage and the simultaneous reduction of the value of the asset. This harm relates to the spilled oil and the damage for nature and people. It depends on the damage function μ.

Summing up, it is now possible to formulate the objective function and the two state dynamics and to set up a general formulation of the optimal control model. As explained in the previous section, the state variable x can be increased by a concave function $f(u, x)$ and is decreased by the depreciation rate δ, leading to:

$$\dot{x} = f(u, x) - \delta x.$$

The state variable y profits from direct investements $1 - u$, in form of a function $g(1 - u)$,

but also suffers from damage caused by the attacker, μ, which depends on the *attack intensity* $v(x, y)$:

$$\dot{y} = g(1 - u) - \mu(v(x, y)).$$

Finally, the objective function consists of positive overall effects $W(y)$ minus the negative overall effects $D(\mu)$:

$$W(y) - D(\mu(v(x, y))).$$

All these assumptions yield the general formulation of the optimal control model:

$$\max_{u(t)} \quad \int_0^\infty e^{-rt}(W(y(t)) - D(\mu(v(x(t), y(t)))))dt$$

s.t.

$$\begin{aligned}
\dot{x}(t) &= f(u(t), x(t)) - \delta x(t) \\
\dot{y}(t) &= g(1 - u(t)) - \mu(v(x(t), y(t))) \\
x(0) &= x_0 \in [0, 1) \\
y(0) &= y_0 > 0 \\
u(t) &\in [\overline{u}, 1] \qquad \forall t.
\end{aligned}$$

This formulation will be augmented by the use of specifications for the functions in the next section.

2.3 Functional Specification and Properties

This section deals with a detailed description of the functions that will be used in the expressions of the previous section.

Starting with the *wealth function* $W(y)$, one may expect a raise of wealth if the value of the asset increases due to direct investements. A positive first derivative W' with respect to y takes this assumption into account. To keep the model as simple as possible, a linear function meeting this requirement is used: $W(y) = by$ with $b > 0$. This formulation implies that every unit y of the value of the asset generates b monetary units of wealth. Similarly, the *investement function* for the asset, $g(1 - u)$, relies on this basic form, too: $g(1 - u) = d(1 - u),\ d > 0$. Therefore, assuming the decision maker invests all of her budget into the asset (i.e. $u = 0$), she can add at most d units of value to the asset (via repairs or improvements) per unit of time. As already mentioned, to avoid numerical problems the case $u = 0$ later on will be substituted by $u = 0.00001$, hence decreasing the maximal raise of value only a little bit.

With the *effectiveness function* $f(u, x)$ things become a little more complicated. Investing a share u of the normalized budget should have positive effects on the security level, implying $\frac{\partial f}{\partial u} > 0$. However, it would not be very realistic to assume that, if the security level is already very high (e.g. close to 1), additional units of money invested do have the same effect on the security level. As a result, the assumption of diminishing returns of the investment seems obvious, suggesting the dependence on u to be of the form u^α with $0 < \alpha < 1$. In addition, assume that if the security level is already high, it is harder, or to say more expensive, to raise the security level even further. This fact will be captured by a negative first derivative of f with respect to x. A simple function, which meets all these assumptions, is $f(u, x) = cu^\alpha(1 - x)$.

The *harm function* $D(\mu)$ is modeled as $D(\mu) = k\mu^\sigma$ with $k > 0$. This functional form implies a positive first derivative leading to an increase in harm, if the damage done to the asset increases. Depending on the choice of σ, D will be a convex or concave function, but since we want the first derivative to be positive, at least the condition $\sigma > 0$ must be satisfied. Similar to the parameter b of the *wealth function*, k describes the monetary units of harm done for every unit of value, which is lost due to attacks.

The *attack intensity* $v(x, y)$ should be of multiplicative form $v(x, y) = h(x)p(y)$, with $\lim_{y\to 0^+} p(y) = 0$, because it is assumed that the attack intensity converges to zero if $p(y)$ converges to zero, implying a high interest of the attacker to damage valuable assets. As one can see, the attack intensity is assumed to depend on the current security level x and the value of the asset y. Since one may expect that attacks become more intense the more valuable the asset is to the defender, $p(y) = y^\beta$ with $\beta \geq 1$ seems to be a fitting choice for the second factor. The first factor, $h(x)$, will be called the *reaction function* of the attacker, which takes values in $[0, 1]$. It will play a crucial role in modeling the attacker's behavior (see Section 2.6, Figure 2.1 on Page 22, and Figure 5.1 on Page 60), and its particular form will depend on the chosen type of attacker. As it was mentioned in Section 1.3, "The Idea", the attacker should not only be modeled as a rational type who is deterred by a high security level, but there should also be an irrational type of attacker, who may be attracted by a high security level for his/her purpose. This distinction between rational and irrational behavior leads to different types of attackers who can be classified according to one of the following categories:

1. "deterred" type:
   This type of attacker has a high and increasing initial level of intensity of attacks if the security level is low. At a certain level of x, the attacker gets deterred and decreases his/her attacks. (The reader may remember the Pipeline-War example, where the attacks drastically decreased after a raise of the troops assigned to the

pipeline.)

2. "aggressive" type:
   This type of attacker has a low initial level of intensity of attacks. However, the higher the security level becomes, the more the attacker thinks it is worth attacking the asset. This type of attacker can be seen as a political aggressor seeking to strike with fear in the population: attacking a highly secured asset will successfully make people feel insecure.

3. "provoking" type:
   This type of attacker has a high but decreasing initial level of attack intensity. When x reaches a certain level, the sign of the first derivate of the reaction function changes and the attacker increases her/his attacks. This can be interpreted as the attacker realizing that the asset at this certain level of x becomes so important to the defender that she reassesses the situation and starts increasing her attack intensity.

Finally, the *damage function* μ is assumed to increase if attacks of the opponent become more intense. Thus, $\mu'(v)$ should be greater than zero. Again, relying on a simple form seems adequate: $\mu(v(x,y)) = av^\gamma = ah(x)^\gamma p(y)^\gamma$ with $\gamma,\ a > 0$. Checking the derivative of μ with respect to y, $\mu_y = a\gamma v^{\gamma-1} v_y$, one can see that all the assumptions made so far are taken into account. From $v_y = \beta y^{\beta-1} h(x) \geq 0$ (since $h(x)$ will be chosen in a way that $h(x) \geq 0\ \forall x \in [0,1)$) it follows that $\mu_y \geq 0$. Consequently, an increase in the asset's value leads to an increase in the attack intensity ($v_y \geq 0$!), which then leads to a higher damage done to the asset. So μ can be interpreted as follows: given a certain level of value of the asset, an attacker aims to destroy $p(y)^\gamma$ units of this value (if this expression is greater than y itself, it can be seen as the goal to fully destroy the asset). However, based on the type of attacker, this goal of damage will be reduced by the *reaction function* $h(x)^\gamma \in [0,1]$ and therefore can also be seen as some kind of probability. Finally, the damage $h(x)^\gamma p(y)^\gamma$ will be multiplied with the *capability factor* a, which depends on the skills of the attacker.

All the properties assumed in this section lead to the general model:

$$\max_u \quad \int_0^\infty e^{-rt}(by - k(a(h(x)y^\beta)^\gamma)^\sigma)dt \tag{2.1}$$

s.t. (2.2)

$$\dot{x} = cu^\alpha(1-x) - \delta x \tag{2.3}$$

$$\dot{y} = d(1-u) - a(h(x)y^\beta)^\gamma \tag{2.4}$$

$$x(0) = x_0 \in [0,1) \tag{2.5}$$

$$y(0) = y_0 > 0 \tag{2.6}$$

$$0 < \overline{u} \leq u \leq 1 \tag{2.7}$$

$$a, b, c, d, k, r > 0 \tag{2.8}$$

$$0 < \delta < 1 \tag{2.9}$$

$$\alpha > 0 \tag{2.10}$$

$$\beta \geq 1 \tag{2.11}$$

$$\gamma > 0 \tag{2.12}$$

$$\sigma > 0 \tag{2.13}$$

NOTE: Restrictions to the exponents just meet the assumptions of Section 2.3. The exact values will be chosen according to the requirements of the second derivatives.

2.4 Applying Pontryagin's Maximum Principle

The optimal control problem will be solved by applying Pontryagin's Maximum Principle (see, e.g., [1]). To formulate the necessary optimality conditions we first state the Hamiltonian H in *current-value* notation with λ_1, λ_2 denoting the *adjoint* or *costate variables*:

$$H(x,y,u,\lambda_0,\lambda_1,\lambda_2) = \lambda_0\left(by - k(a(h(x)y^\beta)^\gamma)^\sigma\right) + \lambda_1(cu^\alpha(1-x) - \delta x)\ldots \\ \ldots + \lambda_2(d(1-u) - a(h(x)y^\beta)^\gamma).$$

Although generally λ_0 cannot be set to 1 (see [2] for a counterexample), this thesis will only analyze the normal case (i.e. $\lambda_0 = 1$). Next, because of the control constraints it is necessary to state the Lagrangian

$$L(x,y,u,\lambda_1,\lambda_2,\mu_1,\mu_2) = H(x,y,u,\lambda_1,\lambda_2) + \mu_1(u-\overline{u}) + \mu_2(1-u).$$

The necessary conditions derived from Pontryagin's Maximum Principle become (see [1]):

$$L_u = \alpha\lambda_1(1-x)cu^{\alpha-1} - d\lambda_2 + \mu_1 - \mu_2 = 0 \tag{2.14}$$

$$\dot{\lambda_1} = r\lambda_1 - L_x \tag{2.15}$$

$$= \lambda_1(r + cu^\alpha + \delta) + \frac{h'(x)}{h(x)}\gamma\left[k\sigma\left(a(h(x)y^\beta)^\gamma\right)^\sigma + \lambda_2 a(h(x)y^\beta)^\gamma\right] \tag{2.16}$$

$$\dot{\lambda_2} = r\lambda_2 - L_y \tag{2.17}$$

$$= r\lambda_2 - b + \frac{\beta\gamma\left[k\sigma(a(h(x)y^\beta)^\gamma)^\sigma + a\lambda_2(h(x)y^\beta)^\gamma\right]}{y} \tag{2.18}$$

$$\mu_1 \geq 0, \quad \mu_1(u-\overline{u}) = 0 \tag{2.19}$$

$$\mu_2 \geq 0, \quad \mu_2(1-u) = 0 \tag{2.20}$$

with the *first-order condition* (2.14), *adjoint equations* (2.16) and (2.18), and the *complementary slackness condition* (2.19) and (2.20). The derivation and analysis of the canonical system now has to be divided into the case of an interior solution (i.e. $u \in (\overline{u}, 1)$) and the case of a boundary solution.

2.4.1 Interior Case $u \in (\overline{u}, 1)$

In the case of an interior solution, the complementary slackness conditions (2.19) and (2.20) imply $\mu_1 = \mu_2 = 0$. Thus, the Lagrangian reduces to the Hamiltonian. As a first step it will be useful to derive further necessary conditions for optimal solutions of the model. The necessary Legendre-Clebsh condition for maximizing optimal control problems will meet this task:

$$\begin{aligned} H_{uu} &= \alpha(\alpha-1)\lambda_1(1-x)cu^{\alpha-2} \leq 0 \\ &\Leftrightarrow \alpha(\alpha-1)\lambda_1(1-x)c\frac{1}{u^{2-\alpha}} \leq 0. \end{aligned} \tag{2.21}$$

This condition holds with strict inequality (implying a unique control value) for

- $0 \leq x < 1, c > 0$, $\alpha > 1$ and $\lambda_1 < 0$ as well as
- $0 \leq x < 1, c > 0$, $0 < \alpha < 1$ and $\lambda_1 > 0$.

These conditions for an optimal solution, especially the second, will become more important in the subsequent analysis. Note that this is the place where numerical problems occur if $u = 0$ would be admissible yielding a singularity in (2.21).

In addition, the Arrow sufficiency condition for infinite time horizon problems (see [1]) requires the maximized Hamiltonian $H^*(x, y, \lambda_1, \lambda_2) = \max_u H(x, y, u, \lambda_1, \lambda_2)$ to be concave in the state variables x and y for all t, λ_1, and λ_2. Since the Hamiltonian is a multidimensional function in x, y, u, λ_1, and λ_2, the second derivative of H^* corresponds to the Hessian of H^*, which is given by

$$D^2 H^*_{x,y} = \begin{pmatrix} \frac{\partial^2 H}{\partial x^2} & \frac{\partial^2 H}{\partial x \partial y} \\ \frac{\partial^2 H}{\partial y \partial x} & \frac{\partial^2 H}{\partial y^2} \end{pmatrix}.$$

Concavity of H^* with respect to the state variables in the multidimensional follows from the negative semi-definiteness of $D^2 H^*_{x,y}$, which is given if the quadratic form

$$(x, y) D^2 H^*(x, y)^T$$

is lesser or equal to 0 for all $(x, y) \neq 0$. Solving this inequality yields (the star of the maximized Hamiltonian will be omitted)

$$\begin{aligned} (x, y) \begin{pmatrix} \frac{\partial^2 H}{\partial x^2} & \frac{\partial^2 H}{\partial x \partial y} \\ \frac{\partial^2 H}{\partial y \partial x} & \frac{\partial^2 H}{\partial y^2} \end{pmatrix} (x, y)^T &\leq 0 \\ \left(x \frac{\partial^2 H}{\partial x^2} + y \frac{\partial^2 H}{\partial y \partial x}, x \frac{\partial^2 H}{\partial x \partial y} + y \frac{\partial^2 H}{\partial y^2} \right) (x, y)^T &\leq 0 \\ x^2 \frac{\partial^2 H}{\partial x^2} + xy \frac{\partial^2 H}{\partial y \partial x} + xy \frac{\partial^2 H}{\partial x \partial y} + y^2 \frac{\partial^2 H}{\partial y^2} &\leq 0 \end{aligned}$$

and because of $\frac{\partial^2 H}{\partial y \partial x} = \frac{\partial^2 H}{\partial x \partial y}$ it follows

$$x^2 \frac{\partial^2 H}{\partial x^2} + y^2 \frac{\partial^2 H}{\partial y^2} + 2xy \frac{\partial^2 H}{\partial y \partial x} \leq 0. \tag{2.22}$$

This sufficient condition (2.22) has to be satisfied along the optimal paths, but due to the complexity of the functional forms it is not possible to derive conditions on parameters at this point.

Given $\mu_1 = \mu_2 = 0$, solving equation (2.14) yields an expression for the optimal control depending on the state variable x and the costates λ_1 and λ_2:

$$\tilde{u} = \left(\frac{d\lambda_2}{\alpha \lambda_1 c (1 - x)} \right)^{\frac{1}{\alpha - 1}}. \tag{2.23}$$

Combining equations (2.16) and (2.18) and the system dynamics (2.3) and (2.4) yields, after substituting $\tilde{u}$ for u, the canonical system of the optimal control problem. For the sake of simplicity define

$$K(x,y) := \left[k\sigma(a(h(x)y^{\beta})^{\gamma})^{\sigma} + \lambda_2 a(h(x)y^{\beta})^{\gamma}\right]. \tag{2.24}$$

The canonical system then becomes

$$\dot{x} = c\tilde{u}^{\alpha}(1-x) - \delta x \tag{2.25}$$

$$\dot{y} = d(1-\tilde{u}) - a(h(x)y^{\beta})^{\gamma} \tag{2.26}$$

$$\dot{\lambda_1} = \lambda_1(r + c\tilde{u}^{\alpha} + \delta) + \frac{h'(x)}{h(x)}\gamma K(x,y) \tag{2.27}$$

$$\dot{\lambda_2} = r\lambda_2 - b + \frac{\beta\gamma}{y}K(x,y). \tag{2.28}$$

2.4.2 Boundary Case $u = \overline{u}$ or $u = 1$

In the case of a boundary solution $u = \overline{u}$, the complementary slackness condition (2.20) yields $\mu_2 = 0$. Hence, the first order condition becomes

$$L_u = \alpha\lambda_1(1-x)c\overline{u}^{\alpha-1} - d\lambda_2 + \mu_1 = 0 \tag{2.29}$$

yielding an analytical expression for the Lagrange multiplier

$$\mu_1 = d\lambda_2 - \alpha\lambda_1(1-x)c\overline{u}^{\alpha-1}. \tag{2.30}$$

The state dynamics (2.3) and (2.4) and adjoint equations (2.16) and (2.18), which give the canonical system, then read as follows:

$$\dot{x} = c\overline{u}^{\alpha}(1-x) - \delta x \tag{2.31}$$

$$\dot{y} = d(1-\overline{u}) - a(h(x)y^{\beta})^{\gamma} \tag{2.32}$$

$$\dot{\lambda_1} = \lambda_1(r + c\overline{u}^{\alpha} + \delta) + \frac{h'(x)}{h(x)}\gamma K(x,y) \tag{2.33}$$

$$\dot{\lambda_2} = r\lambda_2 - b + \frac{\beta\gamma}{y}K(x,y) \tag{2.34}$$

On the other hand, the boundary case $u = 1$ implies, because of the complementary slackness condition (2.19), $\mu_1 = 0$. The canonical system therefore reads as (the first order condition in this case is not relevant since the solution at the upper boundary is not

admissible, see Section 2.5)

$$\dot{x} = c(1-x) - \delta x \tag{2.35}$$

$$\dot{y} = -a(h(x)y^{\beta})^{\gamma} \tag{2.36}$$

$$\dot{\lambda_1} = \lambda_1(r + c + \delta) + \frac{h'(x)}{h(x)}\gamma K(x,y) \tag{2.37}$$

$$\dot{\lambda_2} = r\lambda_2 - b + \frac{\beta\gamma}{y}K(x,y) \tag{2.38}$$

2.5 Steady States of the General Model

A first step in the analysis of a nonlinear optimal control model is to find points $\hat{x},\ \hat{y},\ \hat{\lambda_1},\ \hat{\lambda_2}$ of the canonical systems

- (2.25)-(2.28) for the interior case,
- (2.31)-(2.34) for the boundary case $u = \overline{u}$, and
- (2.35)-(2.38) for the boundary case $u = 1$,

which stay at their level for all times, meaning the derivative with respect to t equals zero. Such points are called *steady states* or *stationary points*. Therefore, the first task will be to solve the system of the four equations

$$\dot{x} = 0$$
$$\dot{y} = 0$$
$$\dot{\lambda_1} = 0$$
$$\dot{\lambda_2} = 0$$

simultaneously. Since the equations in the interior case are pretty complex, one cannot expect to obtain analytical solutions for $x,\ y\ ,\ \lambda_1$, and λ_2. However, the system of four equations can be reduced to a system of two equations both depending on the state variables x and y. By plotting isoclines $\dot{y}(x,y) = 0$ and $\dot{\lambda_1}(x,y) = 0$ it will then be possible to detect *steady states* by identifying the intersection points of these two curves.

2.5.1 Interior Case $u \in (\overline{u}, 1)$

By setting $\dot{\lambda_2}$ in equation (2.28) equal to 0 and solving for λ_2, it is possible to obtain an analytical expression for λ_2 depending on the two state variables:

$$\lambda_2 = \lambda_2(x, y) = \frac{by - \beta\gamma\sigma k(a(h(x)y^\beta)^\gamma)^\sigma}{ry + \beta\gamma a(h(x)y^\beta)^\gamma}. \tag{2.39}$$

Next, $\dot{x}$ in equation (2.25) is set to 0 and solved for λ_1:

$$\dot{x} = 0 \Rightarrow c\left[\left(\frac{d\lambda_2}{\alpha\lambda_1 c(1-x)}\right)^{\frac{1}{\alpha-1}}\right]^\alpha (1-x) = \delta x \tag{2.40}$$

$$\left(\frac{d\lambda_2}{\alpha\lambda_1 c(1-x)}\right)^{\frac{1}{\alpha-1}} = \left(\frac{\delta x}{c(1-x)}\right)^{\frac{1}{\alpha}} \tag{2.41}$$

$$\lambda_1^{\frac{1}{1-\alpha}} = \left(\frac{d\lambda_2}{\alpha c(1-x)}\right)^{\frac{1}{1-\alpha}} \left(\frac{\delta x}{c(1-x)}\right)^{\frac{1}{\alpha}}. \tag{2.42}$$

Note that the number of solutions for λ_1 obtained by this equation depends on the exponent on the left hand side of the equation, $\frac{1}{1-\alpha}$. Nevertheless, the above equation can be solved resulting in solutions $\lambda_{1,i} = \lambda_{1,i}(x, y)$, which, in addition to (2.39), can be used to reduce the four-dimensional canonical system to two dimensions. After substituting the parameters for the base case, this two-dimensional system will be analyzed further.

2.5.2 Boundary Case $u = \overline{u}$ or $u = 1$

In the case $u = \overline{u}$, steady states of the canonical system have to meet the equations

$$\dot{x} = c\overline{u}^\alpha(1-x) - \delta x = 0 \tag{2.43}$$

$$\dot{y} = d(1-\overline{u}) - a(h(x)y^\beta)^\gamma = 0 \tag{2.44}$$

$$\dot{\lambda_1} = \lambda_1(r + c\overline{u}^\alpha + \delta) + \frac{h'(x)}{h(x)}\gamma K(x, y) = 0 \tag{2.45}$$

$$\dot{\lambda_2} = r\lambda_2 - b + \frac{\beta\gamma}{y}K(x, y) = 0. \tag{2.46}$$

Equation (2.43) yields

$$x_{\overline{u}} = 1 - \frac{\delta}{c\overline{u}^\alpha + \delta}$$

implying

$$\begin{aligned} d(1-\overline{u}) - a(h(x_{\overline{u}})y^{\beta})^{\gamma} &= 0 \\ \lambda_1(r + c\overline{u}^{\alpha} + \delta) + \frac{h'(x_{\overline{u}})}{h(x_{\overline{u}})}\gamma K(x,y) &= 0 \\ r\lambda_2 - b + \frac{\beta\gamma}{y}K(x,y) &= 0. \end{aligned}$$

Solving these equations results in an equilibrium solution at the boundary of the control region in analytical form

$$\begin{aligned} x_{\overline{u}} &= 1 - \frac{\delta}{c\overline{u}^{\alpha} + \delta} \\ y &= \left(\frac{1}{h(x_{\overline{u}})}\left(\frac{d(1-\overline{u})}{a}\right)^{\frac{1}{\gamma}}\right)^{\frac{1}{\beta}} \\ \lambda_1 &= -\frac{h'(x_{\overline{u}})}{h(x_{\overline{u}})}\frac{1}{r + c\overline{u}^{\alpha} + \delta}\gamma K(x,y) \\ \lambda_2 &= \frac{by - \beta\gamma\sigma k(a(h(x_{\overline{u}})y^{\beta})^{\gamma})^{\sigma}}{ry + \beta\gamma a(h(x_{\overline{u}})y^{\beta})^{\gamma}} \end{aligned}$$

with

$$K(x,y) = \left[k\sigma(a(h(x_{\overline{u}})y^{\beta})^{\gamma})^{\sigma} + \lambda_2 a(h(x_{\overline{u}})y^{\beta})^{\gamma}\right].$$

However, in the boundary case $u = 1$, equation (2.36) of the corresponding canonical system would imply

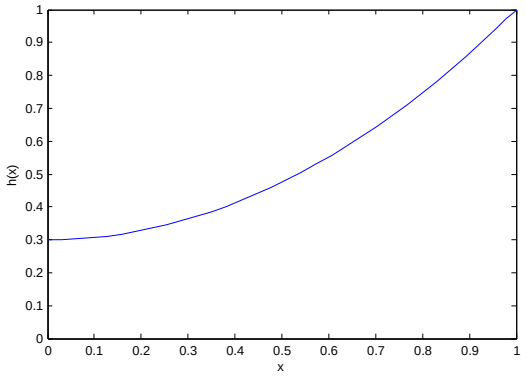
$$\dot{y} = -a(h(x)y^{\beta})^{\gamma} = 0.$$

Since parameter a will be chosen greater than zero and $h(x)$ will be constructed in a way so that $h(x) > 0$ for $0 \leq x < 1$, this equation would only be satisfied for $y = 0$. This solution however, is not admissible since it describes an asset of no worth or a destroyed asset, so to speak.

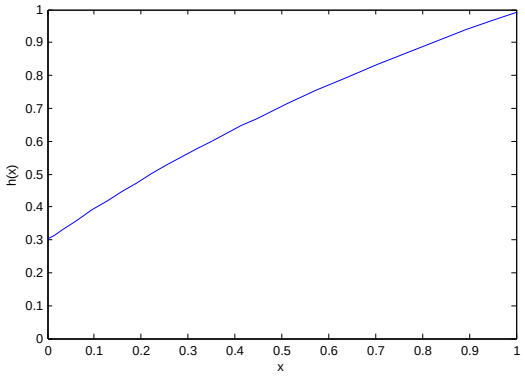
2.6 Reaction Functions of the Attacker

This section will briefly deal with the different types of attackers and how different functional forms $h(x)$ for the attacker's reaction functions will be derived. The reaction function $h(x)$ describes how an attacker reacts to a certain level of security built over time by the defender. As already mentioned, a difference will be made between a *rational* attacker, who retreats given a high security level x, and an *irrational* attacker, whose

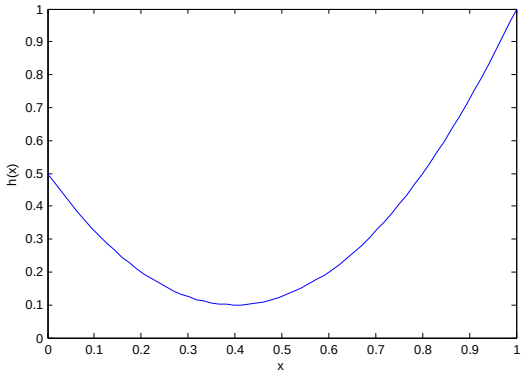
motive is a political one trying to spread fear. This kind of attacker takes advantage of a high security level, since people will get more scared if the attacker succeeds in destroying a well secured asset.



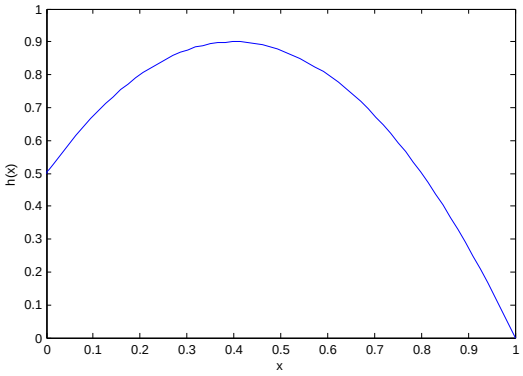
(a) aggressive type, convex: h_{aconv}



(b) aggressive type, concave: h_{aconc}



(c) provoking type: h_p



(d) deterred type: h_d

Figure 2.1: The reaction functions of the different types of attacker

The illustrations in Figure 2.1 show the qualitative characteristics of the functions $h(x)$. Referring to the *deterred* and *provoking* types, for the sake of simplicity of a base case analysis, at first simple (e.g. strictly concave/convex) functions will be used. In an extension, convex-concave or concave-convex functions are considered, respectively, to analyze how an inflexion point may influence the solution of the optimal control problem (see Chapter 5 starting on Page 60).

The monotonically increasing functions $h(x)_{aconv}$ and $h(x)_{aconc}$ of the aggressive, irrational attacker are constructed given the assumptions of a standard-attack level of 0.3 at a security level of $x = 0$ and 1 at $x = 1$. The functions are based on the convex/concave standards of a quadratic function and the logarithm, modified to meet the assumptions.

Using additional conditions given by theoretical assumptions, it is possible to solve a

system of equations derived from a general quadratic function $f(x) = ax^2 + bx + c$ and obtain functions for the rational attacker, the so-called *deterred* type. In addition to a standard attack level of 0.5 at $x = 0$ it is assumed that the deterred type decreases his/her attacks, if the security level raises above $x = 0.4$, leading to an attack level of 0, if the asset is optimally secured (i.e. $x = 1$). The peak of his/her attacks will be chosen to be at a level of 0.9 for $x = 0.4$, leading to the condition $h'_d(0.4) = 0.9$.

Similarly, the irrational *provoking* type is constructed, who retreats if the security level is increased at low levels but then starts increasing her/his attacks thinking that it is worth attacking an asset so important to the defender or trying to spread fear. This attacker also will be assumed to have a standard attack level of 0.5. Similar to the deterred type, she is assumed to have her change of mind at $x = 0.4$ with an attack level of 0.1 leading to the condition $h'_p(0.4) = 0.1$. Since this aggressive attacker is not assumed to retreat after this crossing, her attack level at $x = 1$ will be set to 1.

Applying these conditions to calculate functions $h(x)$ leads to:

$$\begin{aligned} h(x)_{aconv} &= 0.7x^2 + 0.3 \\ h(x)_{aconc} &= \ln(x+1) + 0.3 \\ h(x)_d &= -2.5x^2 + 2x + 0.5 \\ h(x)_p &= 2.5x^2 - 2x + 0.5 \end{aligned}$$

implying ($v(x, y) = h(x)y^\beta$)

$$\begin{aligned} v(x,y)_{aconv} &= (0.7x^2 + 0.3)y^\beta \\ v(x,y)_{aconc} &= (\ln(x+1) + 0.3)y^\beta \\ v(x,y)_d &= (-2.5x^2 + 2x + 0.5)y^\beta \\ v(x,y)_p &= (2.5x^2 - 2x + 0.5)y^\beta. \end{aligned}$$

Chapter 3
Base Case Analysis

3.1 Base Case Parameters

Before starting the numerical analysis, the exact values of all parameters have to be chosen. Since this work is heavily based on modeling the attacker's behavior, the parameters will be chosen in this context freely without relying on any empirical data. Basically, there are two kinds of parameter sets: the first parameter set consists of the exponents $\alpha, \beta, \gamma, \sigma$, describing qualitative influences on reaction and outcome functions of the model. The second parameter set a, b, c, d, k, δ, r consists of scaling parameters.

First, the exponents will be chosen based on the behavior of the attacker we want to model and the influence on the functions linked to this particular behavior. Additionally, parameter α will be set to 0.5, which means that the decision maker faces a concave money-input function. This seems to be a quite realistic assumption, since one may expect that the effect of an additional unit of money spent on the security level is lower than the effect of the current unit.

Parameters β and γ will both be set to 1 for the base case, since this level on the one hand reduces the complexity and therefore the computing time of the model, and on the other hand meets the intention of nonnegative first derivatives of functions $v(x, y)$ and $\mu(v(x, y))$. Finally, σ will be set to 0.5 for the same reason as α: the decrease in the objective funtion should be concave. To interpret this circumstance, one may think of a building generating a high level of wealth for society, a hospital. If an attacker destroys most of a hospital, every unit more that will be lost does not affect the decrease of wealth that much, because the hospital was hardly able to operate at normal levels already after the first attack.

For the base case, the discount rate r will be set to a common level of 0.05. The deprecia-

tion rate of the securitiy level x, δ, will initially be set to a fairly low level of 0.2. Referring to Section 2.1, the interpretation of the depreciation rate now means that every time unit (a year in this thesis) a fifth of the equipment that somehow generates a certain level of security has to be exchanged, which furthermore means that every $\frac{1}{\delta} = 5$ years, the whole equipement gets changed. In terms of technical advancements these days, 5 years seem to be a fairly realistic rate if one just thinks of recent events of governments and companies being hacked. Especially in the so-called "Cyber-War" it seems indispensable to renew security software on computer systems or the level of knowledge of the system administrators quite often.

Parameter c will be set to 1 in the base case, because in the beginning the focus lies on the behavior of the attacker and the corresponding optimal control of the decision maker to cover the basic dynamics of this model, without considering something like increase or decrease in currency. Parameter d will be set to 1, meaning that the decision maker can restore one monetary unit of value of the asset if she invests her whole budget into the asset.

After these assumptions, parameters a, b, and k still have to be chosen. The *capability factor* of the attacker, a, will be set to a fairly high level of 2 implying that the defender faces assaults by a well-organized, capable attacker. For the base case analysis, choosing the levels of b and k will be based on balancing the expressions they show up in, namely the objective function. Parameter b will be set to 2, which implies that every unit of value of the asset generates two units of wealth. Parameter k will be set to 1.5, leaving the decision maker with an asset that causes 1.5 monetary units of decrease in the objective function for every unit of value being destroyed.

For a better overview, all parameter values for the case base are summarized in Table 3.1.

Parameter	a	b	c	d	k	r	α	β	γ	δ	σ	$\overline{u}$
Value	2	2	1	1	1.5	0.05	0.5	1	1	0.2	0.5	0.00001

Table 3.1: Parameters for the Base Case

Given these parameter values, the functions become

$$\begin{aligned} f(u,x) &= \sqrt{u}(1-x) \\ g(1-u) &= 1-u \\ W(y) &= 2y \\ D(\mu) &= 1.5\sqrt{\mu} \\ \mu(v) &= 2v \end{aligned}$$

leading to the following base case formulation of our optimal control problem:

$$\max_u \int_0^\infty e^{-0.05t}(2y - 1.5\sqrt{2h(x)y}dt \tag{3.1}$$

s.t. (3.2)

$$\dot{x} = \sqrt{u}(1-x) - 0.2x \tag{3.3}$$

$$\dot{y} = 1 - u - 2h(x)y \tag{3.4}$$

$$x(0) = x_0 \in [0, 1) \tag{3.5}$$

$$y(0) = y_0 > 0 \tag{3.6}$$

$$u \in [0.00001, 1]. \tag{3.7}$$

3.2 The Canonical Systems for the Base Case

Following Section 2.4 on Page 15, the base case model will now be solved for an interior solution by applying Pontryagin's Maximum Principle, starting with formulating the current-value Hamiltonian for the normal case $\lambda_0 = 1$:

$$H(x, y, u, \lambda_1, \lambda_2) = 2y - 1.5\sqrt{2h(x)y} + \lambda_1(\sqrt{u}(1-x) - 0.2x) + \lambda_2(1 - u - 2h(x)y).$$

(Recall that the Lagrangian equals the Hamiltonian in the interior case.) The necessary optimality conditions derived from the Maximum Principle are

$$H_u = \frac{\lambda_1(1-x)}{2\sqrt{u}} - \lambda_2 = 0 \tag{3.8}$$

$$\dot{\lambda_1} = \lambda_1(\sqrt{u} + 0.25) + \frac{h'(x)}{h(x)}\left[0.75\sqrt{2yh(x)} + \lambda_2 2yh(x)\right] \tag{3.9}$$

$$\dot{\lambda_2} = 0.05\lambda_2 - 2 + \frac{0.75\sqrt{2yh(x)}}{y} + 2\lambda_2 h(x). \tag{3.10}$$

Solving (3.8) with respect to u leads to the candidate solution for the optimal control

$$u^* = \left(\frac{\lambda_1(1-x)}{2\lambda_2}\right)^2. \tag{3.11}$$

The Legendre-Clebsh condition becomes

$$H_{uu} = \frac{\lambda_1(x-1)}{4u^{\frac{3}{2}}} < 0. \tag{3.12}$$

Since $-1 \leq (x-1) < 0$ (the case of perfect security $x = 1$ will not be taken into account) and $u^{\frac{3}{2}} > 0 \forall u \in (\overline{u}, 1]$, it follows that $H_{uu} < 0 \Leftrightarrow \lambda_1 > 0$.

Using the parameters in Table 3.1 in the general canonical system (2.25)-(2.28) on Page 18 yields the canonical system for the base case after defining

$$K(x,y) := 0.75\sqrt{2yh(x)} + \lambda_2 2yh(x).$$

$$\dot{x} = \sqrt{\frac{\lambda_1^2(1-x)^2}{4\lambda_2^2}}(1-x) - 0.2x \tag{3.13}$$

$$\dot{y} = 1 - \frac{\lambda_1^2(1-x)^2}{4\lambda_2} - 2yh(x) \tag{3.14}$$

$$\dot{\lambda_1} = \lambda_1 \left(0.25 + \frac{\lambda_1(1-x)}{2\lambda_2}\right) + \frac{h'(x)}{h(x)}K(x,y) \tag{3.15}$$

$$\dot{\lambda_2} = \lambda_2(0.05 + 2h(x)) + 0.75\frac{\sqrt{2yh(x)}}{y} - 2. \tag{3.16}$$

3.3 Steady States

As mentioned in Section 2.5 on Page 19, one has to solve the system $\dot{x} = 0$, $\dot{y} = 0$, $\dot{\lambda_1} = 0$, and $\dot{\lambda_2} = 0$ simultaneously to determine the equilibrium points ($EP_i = (\hat{x^i}, \hat{y^i}, \hat{\lambda_1^i}, \hat{\lambda_2^i})$). Following the calculations of Section 2.5 for the interior case yields

$$\lambda_2(x,y) = \frac{2y - 0.75\sqrt{2yh(x)}}{y(0.05 + 2h(x))} \tag{3.17}$$

$$\lambda_{1_{1,2}}(x,y) = \pm\frac{0.4\lambda_2 x}{(1-x)^2}. \tag{3.18}$$

Finally, with these expressions the two-dimensional system becomes:

$$\dot{y} = 1 - \frac{\lambda_{1,i}(x,y)^2(1-x)^2}{4\lambda_2(x,y)} - 2yh(x) \tag{3.19}$$

$$\dot{\lambda_1} = \lambda_{1,i}(x,y)\left(0.25 + \frac{\lambda_{1,i}(x,y)(1-x)}{2\lambda_2(x,y)}\right) + \frac{h'(x)}{h(x)}K(x,y). \tag{3.20}$$

Graphically, the detection of the steady states of the canonical system now comes down to plotting the zero isoclines of $\dot{y}$ and $\dot{\lambda_1}$. The intersection points of these isoclines depict the candidate steady states of the optimal control problem. The blue curve represents $\dot{y} = 0$, and the purple and red curves correspond to $\dot{\lambda_1} = 0$, with the two different colors

referring to the two solutions of (3.18). Note that the intersection point at $x = 0$, i.e. the steady state in Figure 3.1, is not admissible, since the control value in this equilibrium equals $u = 0$.

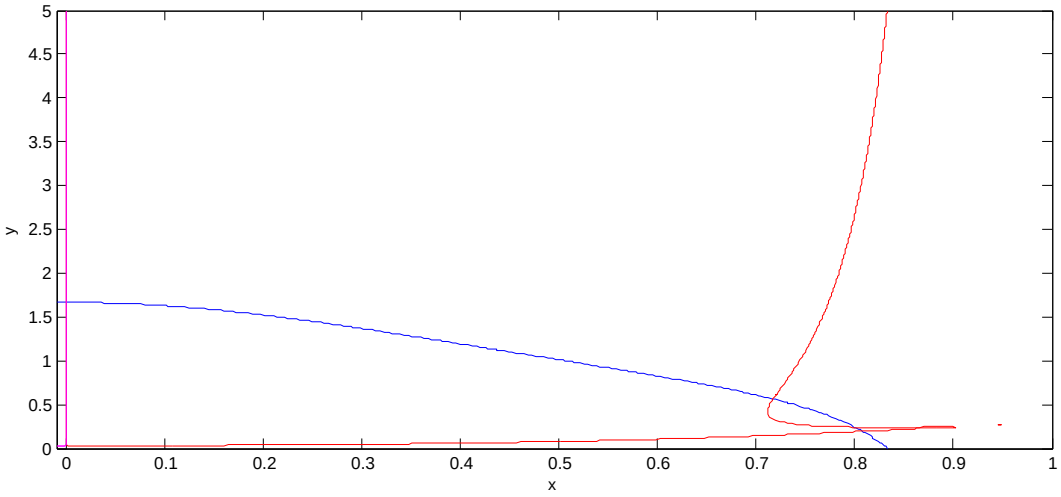


Figure 3.1: The zero-isoclines of the *aconv*-model

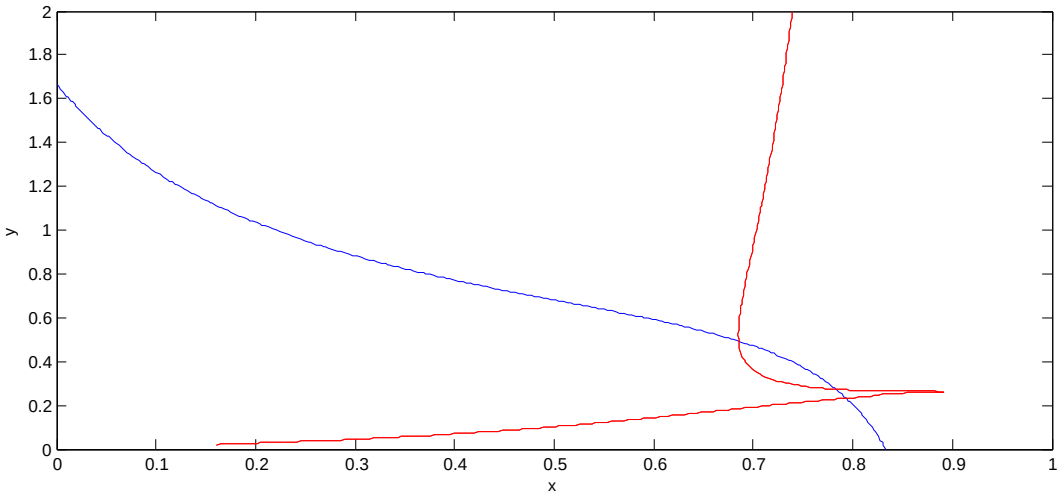


Figure 3.2: The zero-isoclines of the *aconc*-model

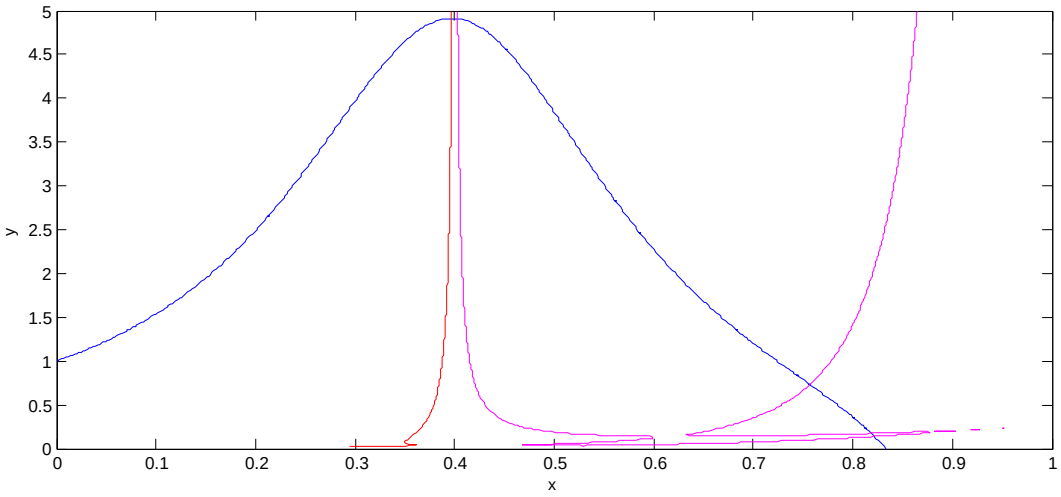


Figure 3.3: The zero-isoclines of the *provoking*-model

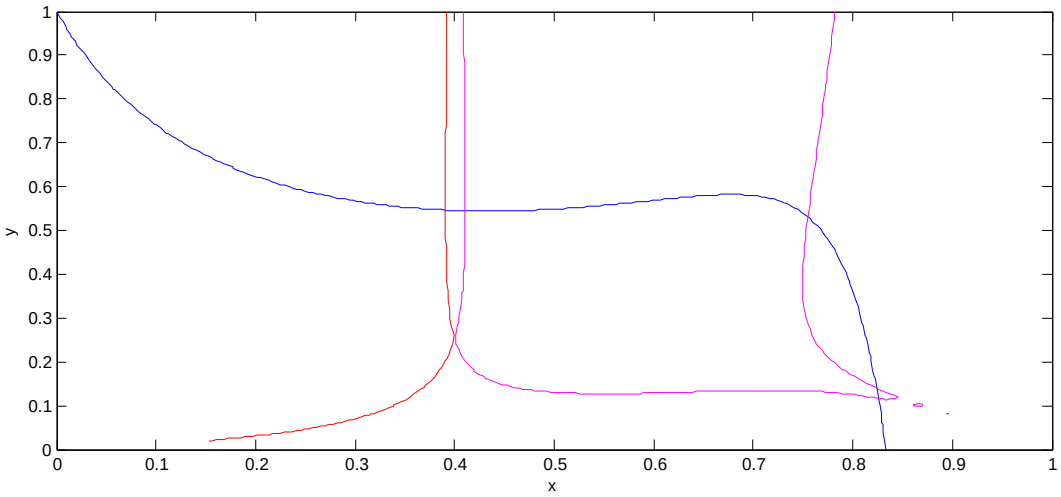


Figure 3.4: The zero-isoclines of the *deterred*-model

In addition, according to the calculations in Section 2.5, the equilibrium point at the boundary of the control region reads as

$$
\begin{aligned}
x_{\overline{u}} &= 1 - \frac{0.2}{0.00001^{\frac{1}{2}} + 0.2} = 0.0015565 \\
y &= \frac{1}{h(x_{\overline{u}})}\left(\frac{1 - 0.00001}{2}\right) \\
\lambda_1 &= -\frac{h'(x_{\overline{u}})}{h(x_{\overline{u}})}\frac{1}{0.253162278}K(x,y) \\
\lambda_2 &= \frac{2y - 0.75\sqrt{(2h(x_{\overline{u}})y)}}{0.05y + 2h(x_{\overline{u}})y} \\
&\text{with} \\
K(x,y) &= \left(0.75\sqrt{2h(x_{\overline{u}})y} + \lambda_2 2h(x_{\overline{u}})\right),
\end{aligned}
$$

and the Lagrange multiplier

$$\mu_1 = \lambda_2 - 0.5(1 - 0.0015565)0.00001^{-0.5}\lambda_1.$$

To verify the results in terms of the number of equilibria and to obtain exact equilibrium values, one has to solve the canonical system numerically too, which, in this thesis, is done by using the OcMat Toolbox[1] for Matlab.

As one can see in Table 3.2, all equilibrium points detected in the graphical illustrations in Figures 3.1-3.4 of the system can be found. However, because of the concavity of the control or, to be exact, the parameter α and the possibility of multiple solutions when extracting roots, one has to recheck the solutions obtained to verify that the necessary optimality conditions $H_u = 0$ and $H_{uu} < 0$ for the interior case, and $H_u < 0$ for the boundary case are satisfied. The calculated steady states, which are depicted in bold in Table 3.2, are therefore the only admissible ones satisfying Pontryagin's Maximum Principle.

[1] see http://orcos.tuwien.ac.at/research/ocmat_software

		EP_1	EP_2	EP_3	EP_4	EP_5	EP_6
$h(x)_{aconv}$	$\hat{x}$	0.80779	0.79987	**0.015565**	0.71708		
	$\hat{y}$	0.19394	0.24137	**1.6657**	0.56296		
	$\hat{\lambda_1}$	-0.53235	-0.68735	**-0.89841**	-2.2277		
	$\hat{\lambda_2}$	-0.06087	0.086043	**2.383**	0.62167		
	$\hat{u}$	0.7065	0.6390	**0.00001**	0.2570		
	H_u	0	-0.1721	**-142.2224**	-1.2433		
	H_{uu}	0.043081	0.067328		1.209670		
$h(x)_{aconc}$	$\hat{x}$	0.68516	0.78296	**0.015565**	0.79337		
	$\hat{y}$	0.49313	0.27294	**1.585**	0.23203		
	$\hat{\lambda_1}$	-1.0296	-0.35835	**-36.8965**	-0.28781		
	$\hat{\lambda_2}$	0.37239	0.053898	**2.2424**	-0.03872		
	$\hat{u}$	0.1894	0.5206	**0.00001**	0.5897		
	H_u	-0.74477	-0.107797	**-5745.2816**	0		
	H_{uu}	0.98291	0.05176986		0.032829		
$h(x)_p$	$\hat{x}$	0.81849	**0.39692**	0.82165	0.75681	0.40322	0.015565
	$\hat{y}$	0.17346	**4.9122**	0.13872	0.73233	4.9074	1.065
	$\hat{\lambda_1}$	-1.1683	**3.2274**	-0.91915	-6.9189	-3.348	33.3196
	$\hat{\lambda_2}$	0.11756	**7.3932**	-0.08896	1.3518	7.3928	1.3103
	$\hat{u}$	0.8134	**0.0173**	0.8489	0.3874	0.0183	0.00001
	H_u	-0.23512	**0**	0	-2.7035	-14.785502	5185
	H_{uu}	0.07226	**-213.341**	0.052394	1.74482	202.4164	
$h(x)_d$	$\hat{x}$	0.39085	**0.8237**	0.82557	**0.75485**	**0.41056**	**0.015565**
	$\hat{y}$	0.54653	**0.14059**	0.11623	**0.53037**	**0.54494**	**0.94245**
	$\hat{\lambda_1}$	-0.14558	**1.1117**	0.92624	**3.647**	**0.16283**	**-26.2451**
	$\hat{\lambda_2}$	0.34552	**0.10488**	-0.08534	**0.72588**	**0.3445**	**1.0838**
	$\hat{u}$	0.0165	**0.8731**	0.8960	**0.3793**	**0.0194**	**0.00001**
	H_u	-0.69103	**0**	0.17068	**0**	**0**	**-4086.2019**
	H_{uu}	10.4905	**-0.06006**	-0.04762	**-0.95698**	**-8.87634**	

Table 3.2: Steady States for the Base Case Computed with the OcMat Toolbox

3.4 Stability of the Steady States

The next step is to determine the stability of the steady states, i.e. analyzing how small influences in the initial values may affect the corresponding equilibrium levels. Determination of the stability of a steady state is based on linearising the system in an equilibrium and using results from calculus (see [2]). In the end, the eigenvalues of the Jacobian

$$J = \begin{pmatrix} \frac{\partial \dot{x}}{\partial x} & \frac{\partial \dot{x}}{\partial y} & \frac{\partial \dot{x}}{\partial \lambda_1} & \frac{\partial \dot{x}}{\partial \lambda_2} \\ \frac{\partial \dot{y}}{\partial x} & \frac{\partial \dot{y}}{\partial y} & \frac{\partial \dot{y}}{\partial \lambda_1} & \frac{\partial \dot{y}}{\partial \lambda_2} \\ \frac{\partial \dot{\lambda_1}}{\partial x} & \frac{\partial \dot{\lambda_1}}{\partial y} & \frac{\partial \dot{\lambda_1}}{\partial \lambda_1} & \frac{\partial \dot{\lambda_1}}{\partial \lambda_2} \\ \frac{\partial \dot{\lambda_2}}{\partial x} & \frac{\partial \dot{\lambda_2}}{\partial y} & \frac{\partial \dot{\lambda_2}}{\partial \lambda_1} & \frac{\partial \dot{\lambda_2}}{\partial \lambda_2} \end{pmatrix}$$

of the canonical system, evaluated at the equilibrium point $\hat{x^i}$, $\hat{y^i}$, $\hat{\lambda_1^i}$, and $\hat{\lambda_2^i}$ play a crucial role. The eigenvalues are the roots of the characteristic polynomial, which is given by $\chi(\omega) = \det(\omega \mathbb{1}_n - \hat{J})$ with the unit matrix $\mathbb{1}_n$ of dimension $n = 4$ and $\hat{J}$ the Jacobian evaluated at the equilibrium point. Given the specific form of the canonical system, the Jacobian in this model slightly reduces to

$$\begin{pmatrix} \frac{\partial \dot{x}}{\partial x} & 0 & \frac{\partial \dot{x}}{\partial \lambda_1} & \frac{\partial \dot{x}}{\partial \lambda_2} \\ \frac{\partial \dot{y}}{\partial x} & \frac{\partial \dot{y}}{\partial y} & \frac{\partial \dot{y}}{\partial \lambda_1} & \frac{\partial \dot{y}}{\partial \lambda_2} \\ \frac{\partial \dot{\lambda_1}}{\partial x} & \frac{\partial \dot{\lambda_1}}{\partial y} & \frac{\partial \dot{\lambda_1}}{\partial \lambda_1} & \frac{\partial \dot{\lambda_1}}{\partial \lambda_2} \\ \frac{\partial \dot{\lambda_2}}{\partial x} & \frac{\partial \dot{\lambda_2}}{\partial y} & 0 & \frac{\partial \dot{\lambda_2}}{\partial \lambda_2} \end{pmatrix}.$$

The eigenvalues for our model were computed with the OcMat Toolbox of Matlab and can be found in the Appendix (see Table B.1 on Page 78). Since there are no zero or purely imaginary eigenvalues of $\hat{J}$, the stationary points are all hyperbolic. This is important, since the Hartman-Grobman Theorem (see [1]) therefore can be stated, which implies that the system is equivalent to its linear approximation in a small neighborhood of an equilibrium.

Chapter 4
Sensitivity Analysis and Optimal Paths

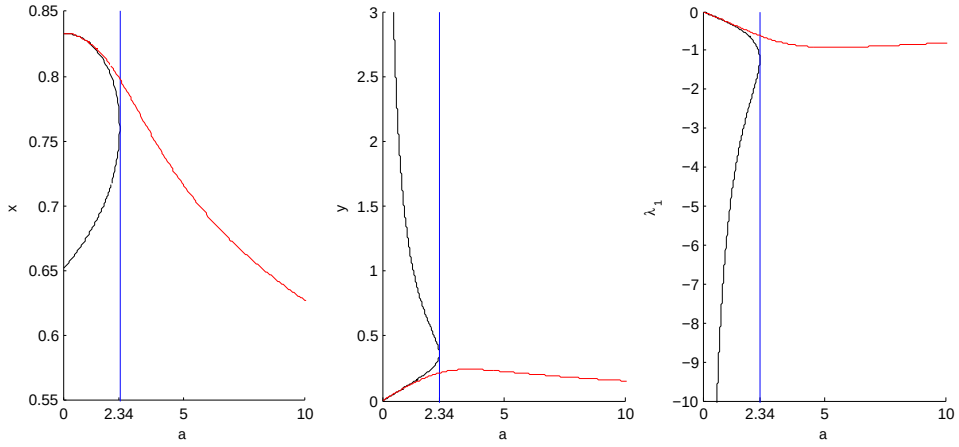
The topic in this section is the question how slight changes in the model parameters affect equilibrium values of the security level x and the value of the asset y. To accomplish this task using Matlab, every iteration (i.e. every step increasing the parameter value a bit) a Newton search was applied to the canonical system with new parameter values, where the initial solution was provided by the solution of the previous step. The structure will be as follows: the analysis will be divided into the sensitivity of the admissible steady states exhibting a two-dimensional stable manifold (the ones, which will be interesting when calculating the optimal paths), and the boundary equilibria, which can be found on Page 48 (Figure 4.16). Additionally, the sensitivity of the non-admissible steady states will also be depicted.

4.1 Attackers with Different Capabilities

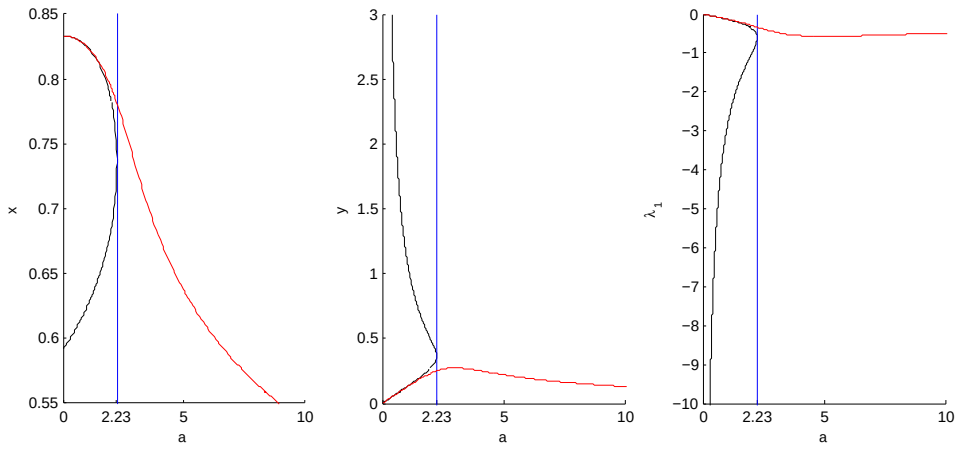
Recalling the damage function $\mu(v(x,y)) = av(x,y)^\gamma = ah(x)^\gamma p(y)^\gamma$, one can see that the damage an attacker can inflict on an asset basically equals a standard level $p(y)^\gamma$ multiplied with some positive number $h(x)^\gamma$ and the capability factor of the attacker. The explanation for the term $p(y)^\gamma$ was the increased attack efforts of the attacker due to the attack intensity function $v(x,y)$ if the asset has a high value. The expression $ap(y)^\gamma$ can be seen as potential damage, which will be reduced by the defender's level of security x, because $h(x)$ was chosen to take values between 0 and 1. An attacker with the capabilities (say because of more equipement or well trained people) to launch heavier attacks can now be expressed as an attacker with a higher *capability factor* a.

For the models with strictly monotone reaction functions, Figures 4.1(a) and 4.1(b) depict the sensitivity of the equilibrium levels in the interior of the control region to changes in

parameter a. As one can see, in every model there exists a *blue-sky bifurcation*, a point where the number of steady states suddenly changes. Depending on the point of view, this means that two steady states converge towards each other until they vanish or that two steady states suddenly appear at a certain parameter value. Based on this phenomenon is the name of this bifurcation: steady states appear out of the *blue sky*.



(a) Sensitivity diagram of the non-admissble steady states with respect to a for the *aconv*-model



(b) Sensitivity diagram of the non-admissble steady states with respect to a for the *aconc*-model

Figure 4.1: Sensitivity diagram of the non-admissible steady states for the *aconv* and *aconc*-models with respect to a

It is obvious that the bifurcation basically seperates the model dynamics into two areas. In the simple aggressive models with strictly monotone reaction functions (Figures 4.1(a) and 4.1(b)), the models both exhibit high and low steady states left to the bifurcation

value of 2.34 and 2.23. In addition, one can see the trade-off effect on which the model is based: with a high steady state value of the security level x there comes a lower level of y and vice versa. This circumstance is based on the model formulation, because the decision maker can possibly invest in x or y. As the attacker's capabilities rise, i.e. the parameter crosses the *blue-sky* threshold, the number of steady states reduces to one, converging to a low level of x with a low level of y at the same time. The trade-off effect vanishes, because in this case the attacker causes so much damage to the asset, that the defender fully concentrates on repairs (i.e. investing everything into the asset), which lets the security level decrease due to depreciation. However, it is important to mention that these considerations are only of hypothetic value, because the interior steady states never become admissible as the value of the first costate is negative over the whole parameter area and only converges towards zero but never crosses it. So the boundary equilibrium has to be analyzed (see Figure 4.16 on Page 48). As it turns out, in both, the *aconv*- and *aconc*-model, the Lagrange multiplier of the boundary equilibrium converges to, but stays above zero, which means that this remains the only admissible solution.

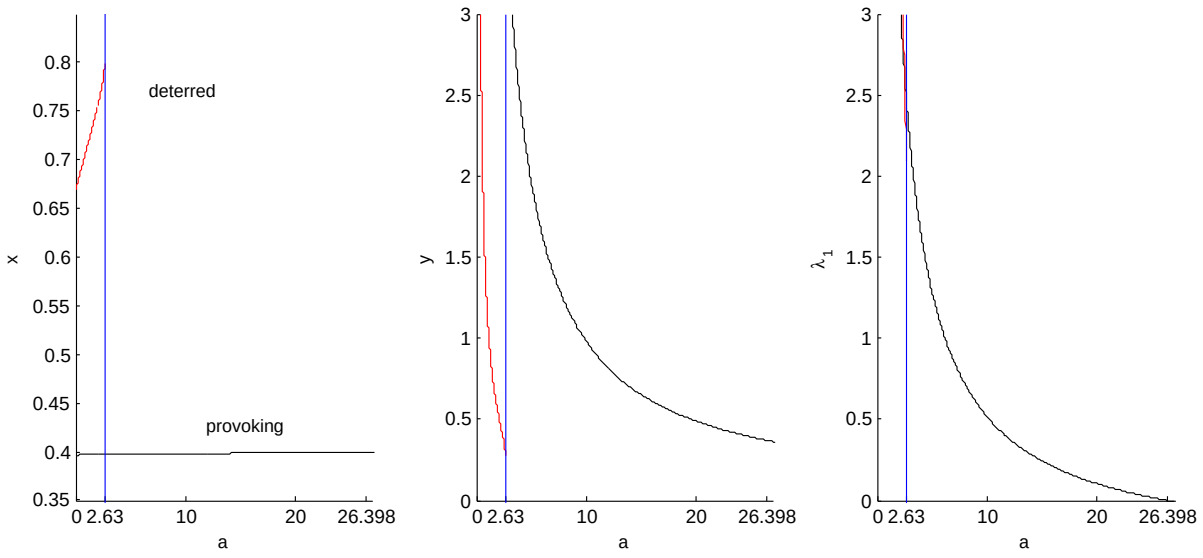
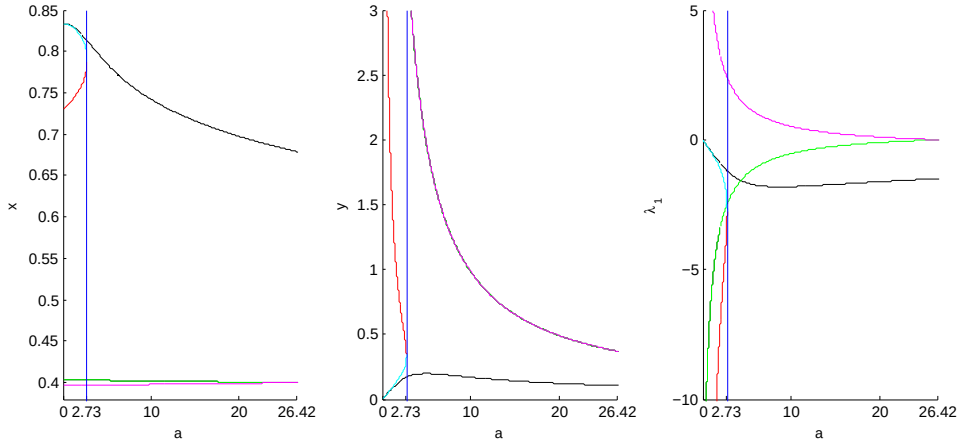


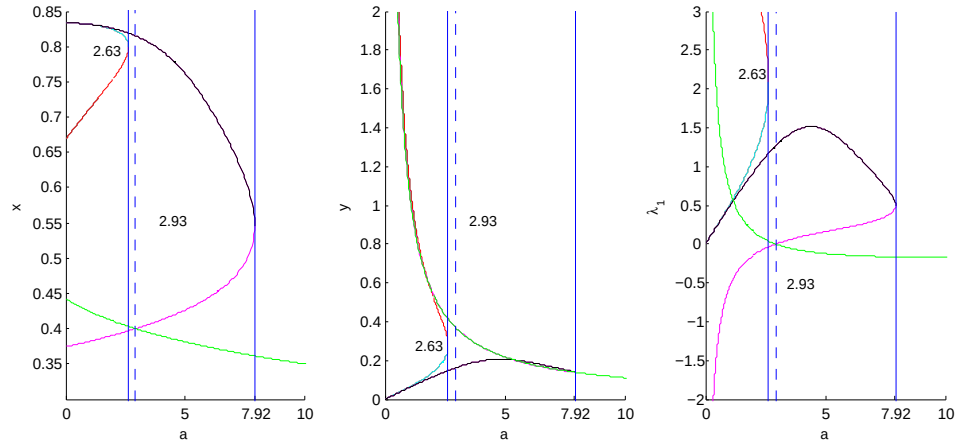
Figure 4.2: Sensitivity diagram of the admissible steady states with two-dimensional stable manifold of the *deterred* and *provoking* models with respect to a

In Figure 4.2, the changes of stationary levels of the *provoking* and *deterred* models can be observed. At the bifurcation value of 2.63, the admissible steady state of the *deterred* model vanishes, while at parameter value $a = 26.398$ in the *provoking* model the only admissible steady state becomes non-admissible, because the costate λ_1 changes its sign. To answer the question, which other steady states in these cases possibly satisfy the

necessary optimality conditions of positivity of the first costate, Figure 4.3 illustrates the developement of the other stationary points.



(a) Sensitivity diagram with respect to a for the *provoking*-model including non-admissible steady states (purple is the admissible steady state)



(b) Sensitivity diagram with respect to a for the *deterred*-model including non-admissible steady states (purple is the admissible steady state exhibiting a two-dimensional stable manifold)

Figure 4.3: Sensitivity diagram for the *provoking* and *deterred* models with respect to a including non-admissible steady states

As one can see, in the *provoking* model at the critical value of about 26.4 the second, lower steady state (corresponding to the green curve) changes its costate sign, too, which leaves it being the only one with a positive value of λ_1 and therefore the only possible admissible steady state. In the *deterred* model, one can see that after the bifurcation value of 2.63, where the admissible solutions vanish, the high, purple and green steady states are the only admissible until a reaches the value of 2.93, where only the purple steady states satisfy the necessary conditions. However, these purple steady states vanish at another bifurcation point occuring at $a = 7.92$. Therefore, the only candidate which may be an admissible steady state is the one at the boundary of the control region. Checking Figure 4.16(a) on Page 48, one can verify that this boundary equilibrium indeed remains the only admissible one after $a = 7.92$, since the corrsponding Lagrange multiplier is positive.

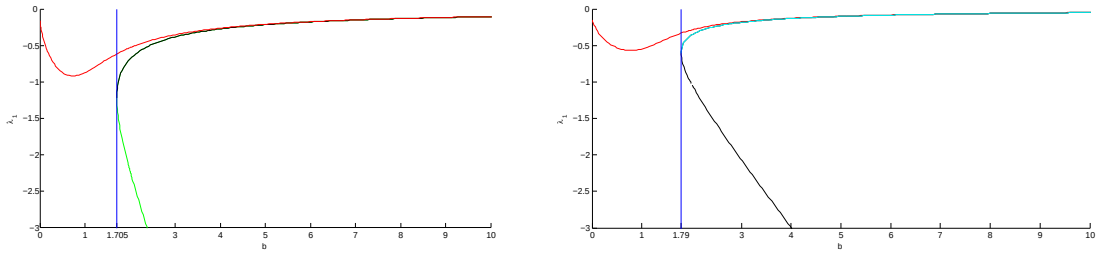
Comparing the four models, one can see that the overall developement of the steady state levels of x and y follow the same movement: left to the blue sky bifurcations, the stationary levels of security and value of the assets heavily depend on the relation of x and y. This is the area where a decision maker has the choice to invest in security, too, because the attacker's damage is, due to the low capability factor, not so high. However, right to the bifurcation points, security levels in general converge to low levels, because the defender faces attacks so heavy that she fully has to invest into the asset (or to say repair the asset) and has no money left for security expenditures. The ongoing depreciation of x then yields the reduction.

4.2 Assets Important to Society

In terms of the state as a decision maker, in this model one may think of assets, which have even more influence on the people of a country. Recalling the example of an oil pipeline from the introduction, it is undoubtedly clear that tax incomes from oil sales can generate wealth in different ways. Nevertheless, examples of assets can be found, which generate even more wealth for society. As a simple example, one can think of hospitals. In their function as health care facilities, people in some region would suffer much more and directly because of the damage of a hospital than the loss of income due to oil sales. Looking at the wealth function $W(y) = by$, it is possible to describe this circumstance with a raise of the parameter b. In the context of a hospital, b can be seen as a the units of wealth every unit of y generates, whereas an increasing level of y can be interpreted as new machines in the hospital or even new departements.

Figure 4.4 again shows that none of the interior non-admissible solutions of the *aconv-*

and *aconc*-models become admissible, since the first costates stay negative for all values of b considered here.

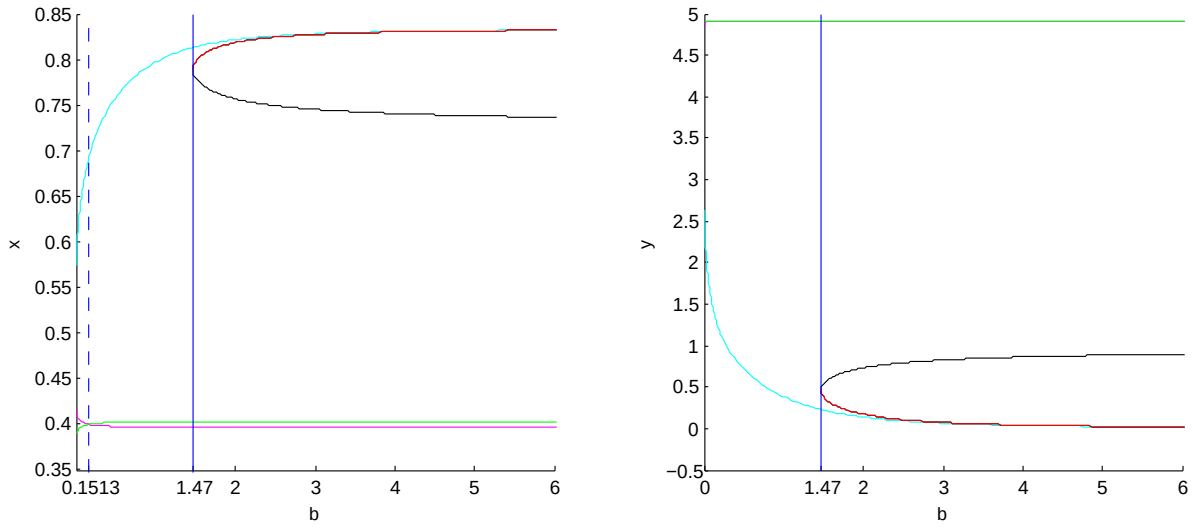


(a) Sensitivity diagram with respect to b for the *aconv*-model

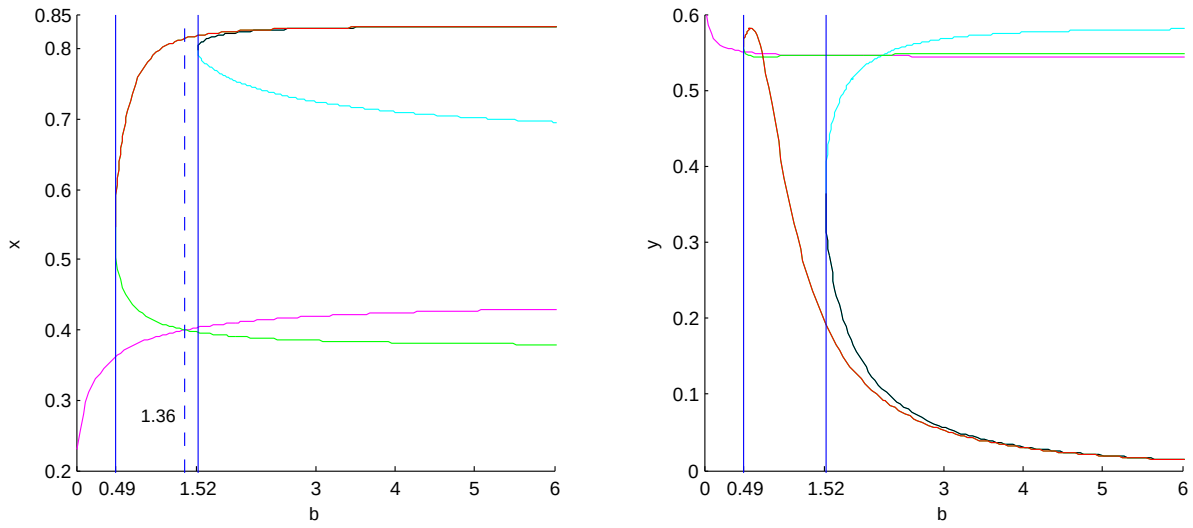
(b) Sensitivity diagram with respect to b for the *aconc*-model

Figure 4.4: Sensitivity diagram of non-admissible steady states for the *aconv*- and *aconc*-models with respect to b

Figure 4.5 illustrates further sensitivity analyses of the steady states with respect to b. The purple equilibrium in the *provoking*-model barely changes as parameter b increases. Again, the trade-off structure of this model can be observed in Figure 4.5(a). Checking Figure 4.6, one is finally able to see that this purple, interior steady state remains the only admissible for parameter changes in b, since the costates of all the others points stay below zero. However, at $b = 0.1513$ and $x = 0.4$ the intersection point of the green and purple line shows that admissibility changes.



(a) Sensitivity diagram of the *provoking*-model with respect to b including non-admissible steady states (purple is the admissible steady state)



(b) Sensitivity diagram of the *deterred*-model with respect to b including non-admissible steady states (blue is the admissible steady state exhibiting a two dimensional stable manifold)

Figure 4.5: Sensitivity diagram of the *provoking*- and *deterred*-models with respect to b including non-admissible steady states

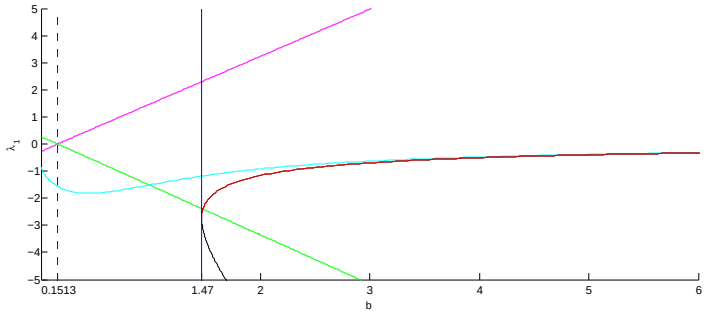


Figure 4.6: Sensitivity of the first costate of the *provoking*-model with respect to b (purple is the admissible steady state)

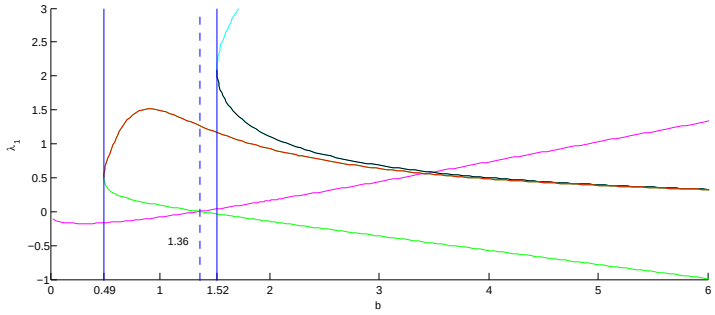


Figure 4.7: Sensitivity of the first costate of the *deterred*-model with respect to b (blue is the admissible steady state exhibiting a two-dimensional stable manifold)

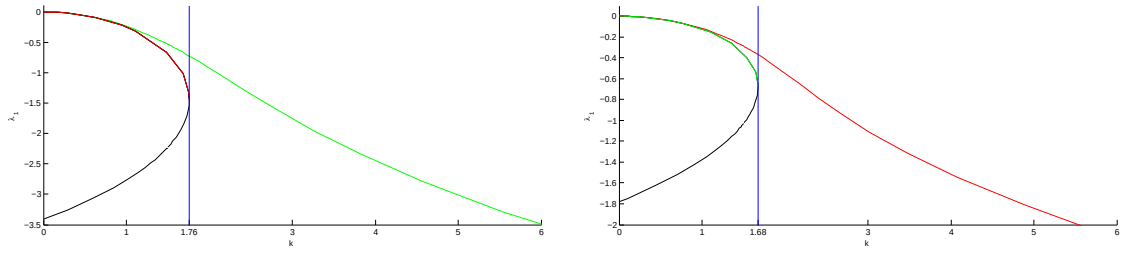
In the *deterred*-model (Figure 4.5(b)), now there exists a second bifurcation threshold, where the admissible blue steady state vanishes. For parameter values greater than 1.52, this steady state remains admissible, but for values between 0.4975 and 1.52 Figure 4.7 shows that the red and green (or purple) steady states remain admissible. Again, the intersection of the green and purple lines at $x = 0.4$ is observable.

This intersection point of the low steady states, which always occurs at $x = 0.4$ is very interesting. This level of security was chosen to be the point where the reaction functions in the *provoking*- and *deterred*-models took their minimum or maximum, respectivly.

4.3 Sensitive Assets

Thinking of nuclear or hydroelectric power plants, it is obvious that valuable assets, which are of big use for people may on the other hand turn into devastating places once they are damaged. The fallout of a damaged nuclear power plant or the masses of water if the

dam of a hydroelectric power plant gets damaged can make whole regions uninhabitable for years or even decades. This potential to cause severe harm given the damage can be covered by the parameter k of the harm function $D(\mu(.)) = k\mu^{\sigma}$.



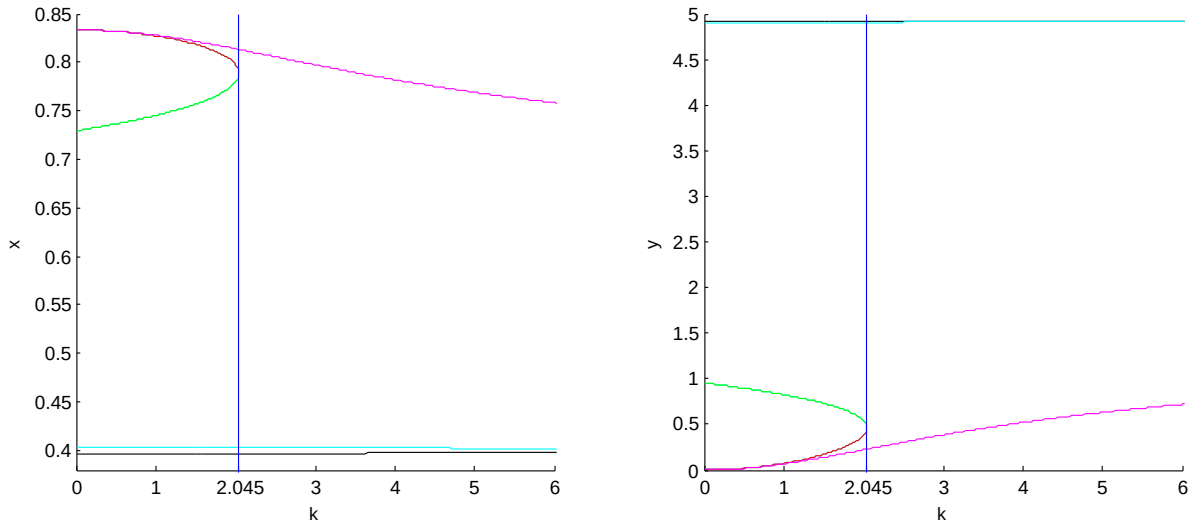
(a) Sensitivity diagram with respect to k for the *aconv*-model

(b) Sensitivity diagram with respect to k for the *aconc*-model

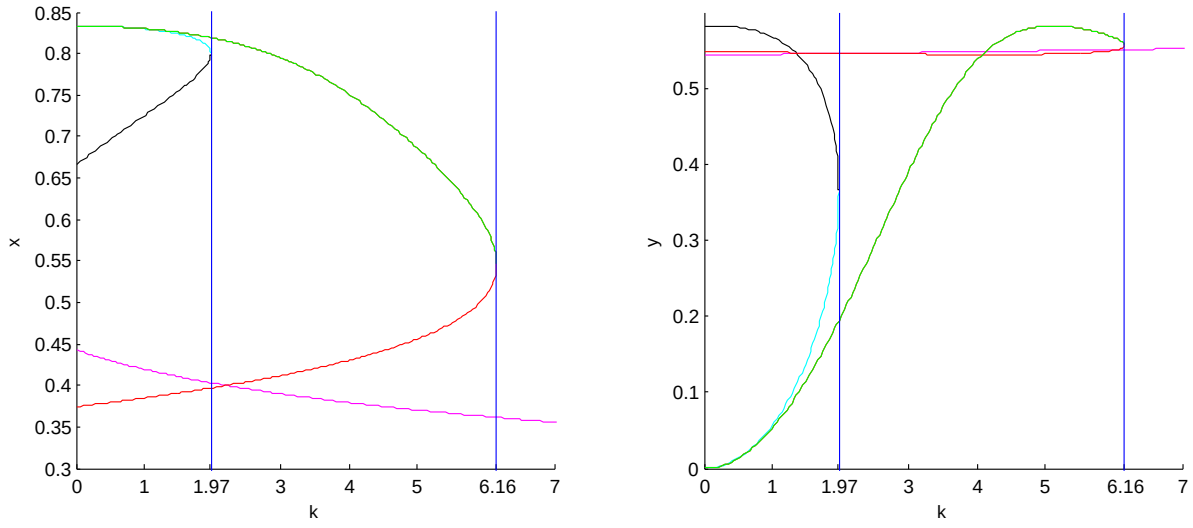
Figure 4.8: Sensitivity diagram of non-admissible steady states for the *aconv*- and *aconc*-models with respect to k

First, Figure 4.8 again shows that in the *aconv*- and *aconc*-models, the steady states at the boundary of the control region can be the only admissible ones when varying k, since none of the interior ones exhibit costate values above zero.

In the *provoking*-model, (Figure 4.9(a)), again there is one bifurcation threshold. In the *deterred*-model (Figure 4.9(b)) there are two blue-sky bifurcations at 1.97 and 6.16. In Figure 4.9(b), the intersection point at $x = 0.4$ can be found, too, and since the costate of the purple steady state remains negative after the second bifurcation, the boundary equilibrium remains the only admissible one.



(a) Sensitivity diagram of the *provoking*-model with respect to k including non-admissible steady states (black is the admissible steady state)



(b) Sensitivity diagram of the *deterred*-model with respect to k including non-admissible steady states (black is the admissible steady state exhibiting a two-dimensional stable manifold)

Figure 4.9: Sensitivity diagram of the *provoking*- and *deterred*-models with respect to k including non-admissible steady states

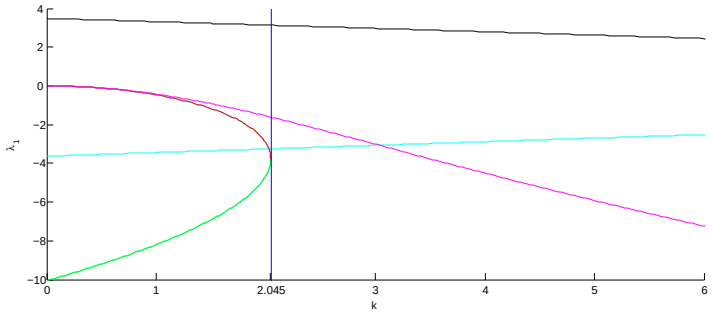


Figure 4.10: Sensitivity of the first costate of the *provoking*-model with respect to k (black is the admissible steady state)

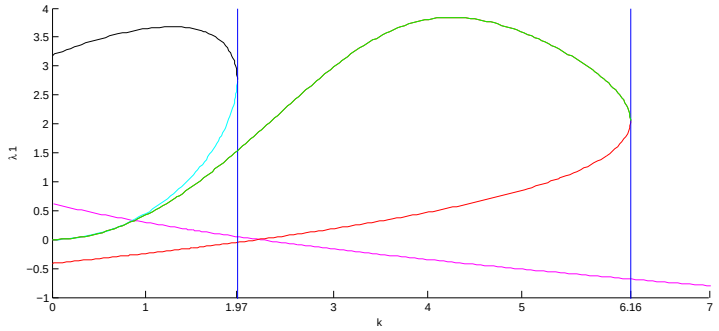
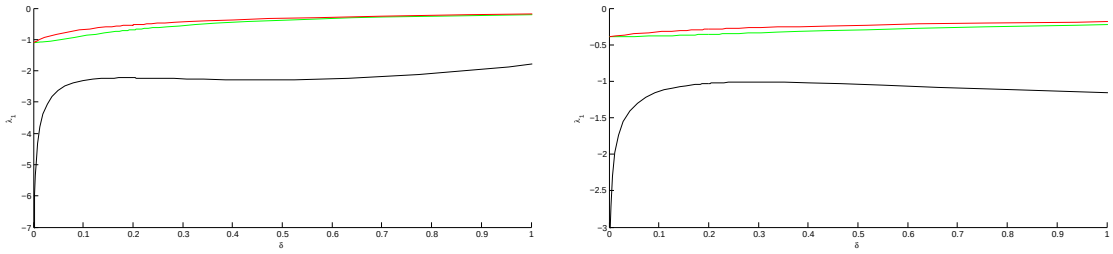


Figure 4.11: Sensitivity of the first costate of the *deterred*-model with respect to k (black is the admissible steady state exhibiting a two-dimensional stable manifold)

It is interesting to see that an increase in parameter k not automatically comes with a decrease in y (as it could be observed when increasing parameter a). To interpret how and why state variables react to k, one may look at the evolution of the green steady state in Figure 4.9(b) on Page 42. As k increases, the security level x gets reduced but simultaneously the value of the asset rises. In this case the decision maker reduces his/her investment in the security of the asset, which is based on the fact that she tries to compensate the possible harm by investing into the asset, and therefore increases the possible wealth. However, in contrast to increasements in parameter a, the attacker suffers from his/her restricted capabilities and cannot inflict more damage to the asset. That is why the investment can be preserved in contrast to the case of changes in a, where the dynamics of y stay at negative levels due to the high value of a.

4.4 Maintenance-Intensive Security Measures

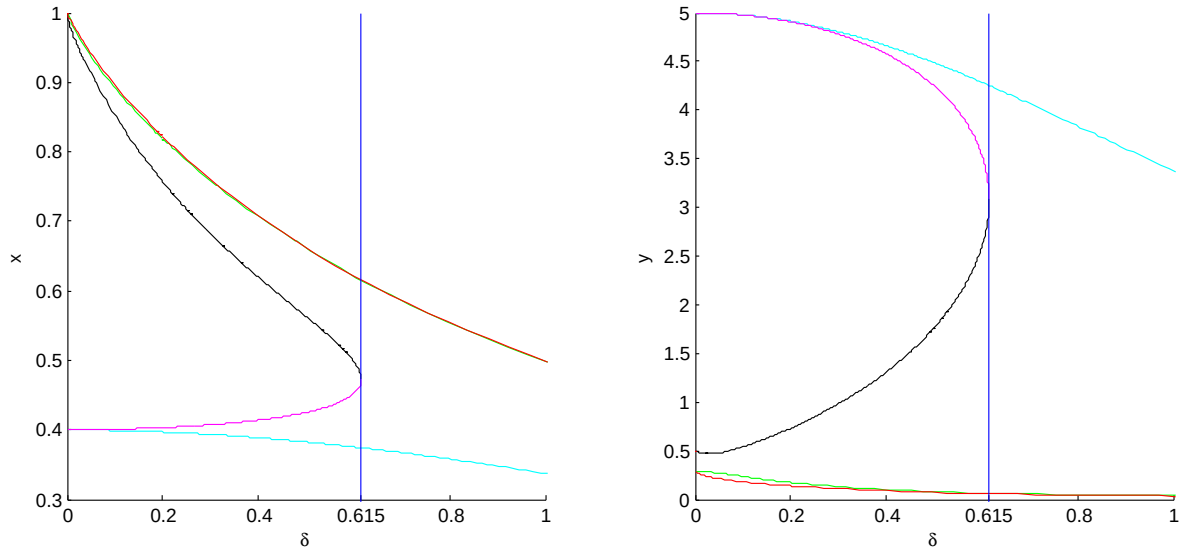
In the introduction, the raise of the security level happened through an increase in the number of soldiers assigned to protect the pipeline. Military force, in both ways human and mechanical, is a security measure that can be seen as relatively sustainable: soldiers can be assigned to certain duties for several years and also technical equipement can be applied a long time. However, reading today's newspapers it is more and more common to come across the words "Cyber War". Due to the technical advancements and the important role of computers, these-days conflicts dislocate to a non-physical area. Of course, computer systems or big networks are very complicated to protect against attackers one cannot even see. That is why on the one hand, people need to be trained well and educated constantly, and on the other hand, equipment (hardware but especially software) needs to be updated often. This fast-paced development on the IT sector causes a high depreciation of security if it is based on computer systems, which leads to an increased value of δ. Looking at Figure 4.12 and using the same argument for the models with strictly monotone increasing reaction function one can argue that no interior equilibrium solution turns out to be admissible.



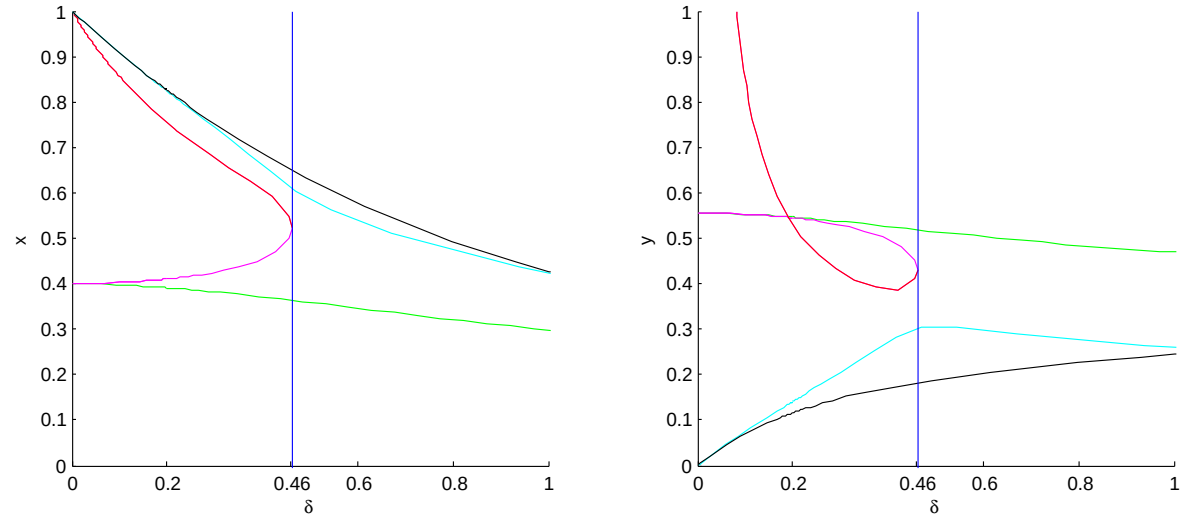
(a) Sensitivity diagram with respect to δ for the *aconv*-model

(b) Sensitivity diagram with respect to δ for the *aconc*-model

Figure 4.12: Sensitivity diagram of non-admissible steady states for the *aconv*- and *aconc*-models with respect to δ



(a) Sensitivity diagram with respect to δ for the *provoking*-model including non-admissible steady states (blue is the admissible steady state)



(b) Sensitivity diagram with respect to δ for the *deterred*-model including non-admissible steady states (red is the admissible steady state exhibiting a two-dimensional stable manifold)

Figure 4.13: Sensitivity diagram of the *provoking*- and *deterred*-models with respect to δ including non-admissible solutions

As it could be expected, maintenance-intensive security measures generally lead to reduced steady state values of x. However, it is interesting to see that the development of the steady state levels does not always have to look the same. For example, in Figure 4.13(b) one can see that maintenance-intensive security measures generally lead to reduced equilibrium levels of x, but checking the sensitivity of y it is noticeable that the equal qualitative development of x does not result in an equal qualitative behavior of y: the black, blue, and red equilibrium paths of x decrease, but the correlating lines in the (δ,y)-plane do not exhibit the same behavior. Here, the black and blue path increase and the red decreases. Checking Figure 4.14, it is obvious that this fact is based on the different equilibrium levels of the control u. In the red case, the equilibrium control levels grow with increasing δ, whereas in the black and blue cases control values decrease, which implies that in the red case the loss of security due to the high depreciation rate is compensated with higher expenditures on x, whereas in the black and blue cases the expenditures on x decrease and therefore extra money can be put into the asset, directly leading to the increasing levels of y.

In Figure 4.13(b) the red line, corresponding to the steady state exhibiting a two-dimensional stable manifold, vanishes at the bifurcation value of 0.463. In this case the two high steady states remain the only admissible ones (see figure 4.15).

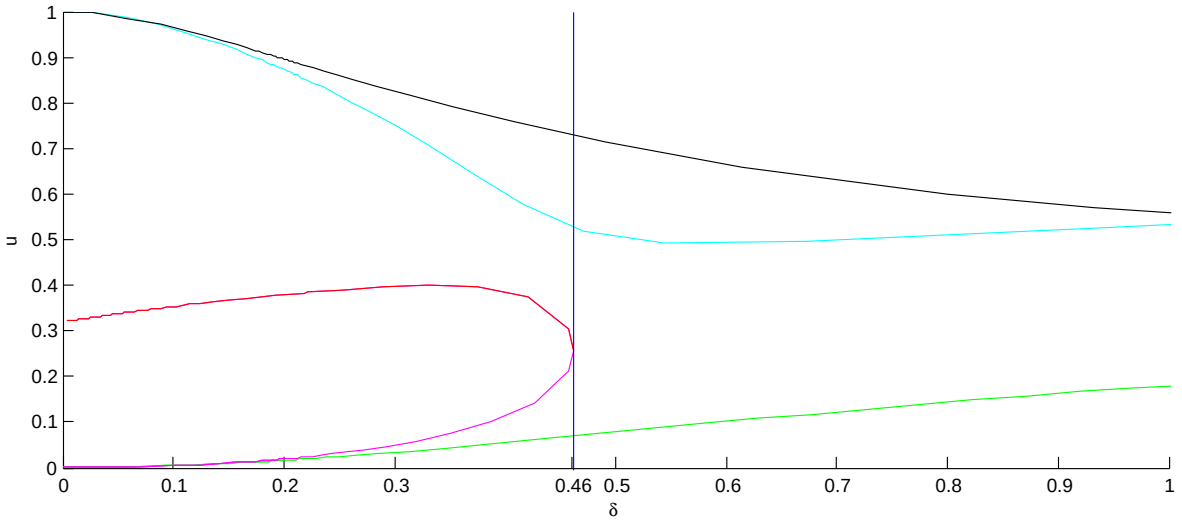


Figure 4.14: Sensitivity of the control to δ in the *deterred*-model (red is the admissible solution exhibiting a two-dimensional stable manifold)

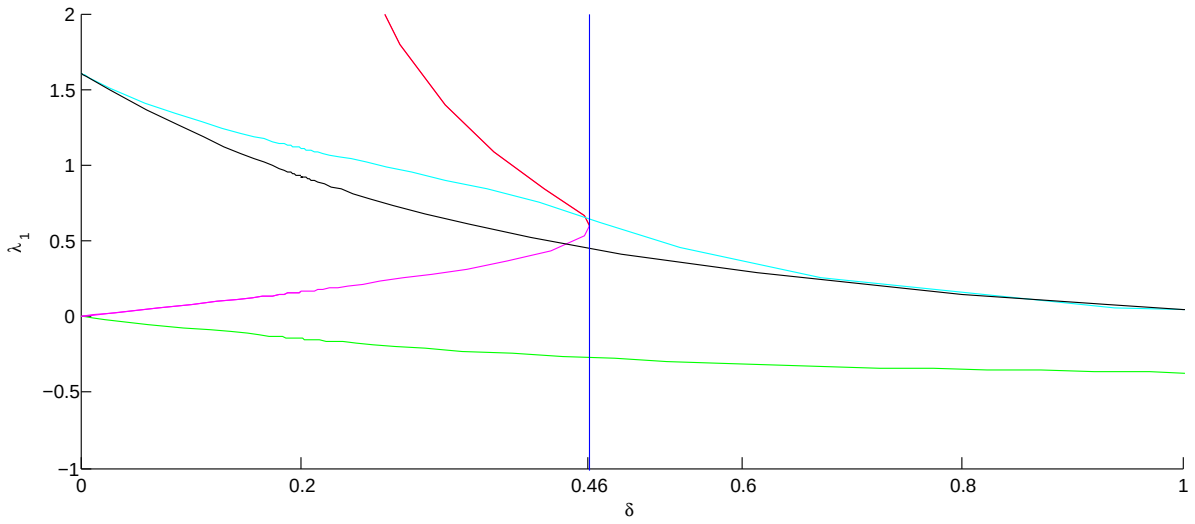
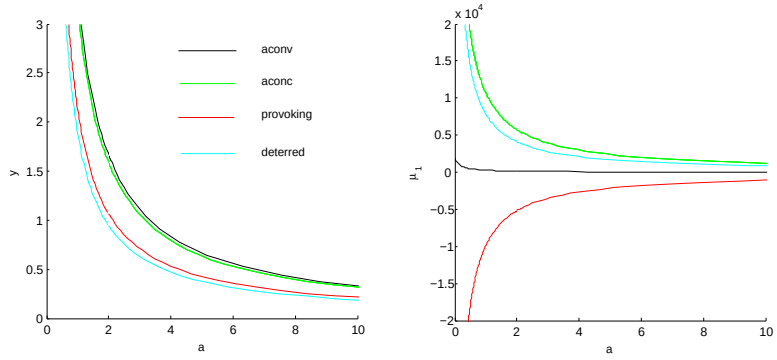


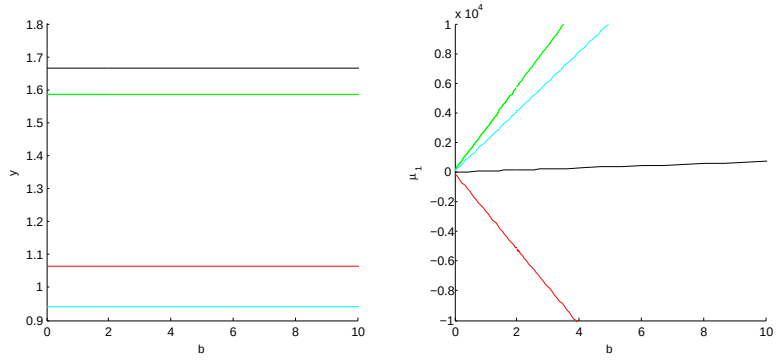
Figure 4.15: Sensitivity of the first costate of the *deterred*-model with respect to δ (red is the admissible steady state)

4.5 Sensitivity of the Boundary Equilibrium

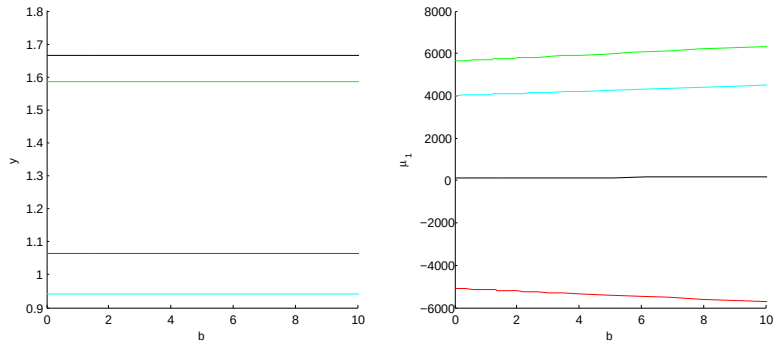
In addition to the sensitivity analysis of the steady states in the interior of the control region, for the sake of completeness also the boundary equilibria are analyzed in Figure 4.16. The main result of this analysis is the answer to the question if one of the boundary steady states become admissible or non-admissible as parameters change. As one can see, in every model the Lagrange multiplier does not change its sign, which implies that the stationary point at the boundary of the control region stays admissible in the *aconv*-, *aconc*-, and *deterred*-models, but non-admissible in the *provoking*-model.



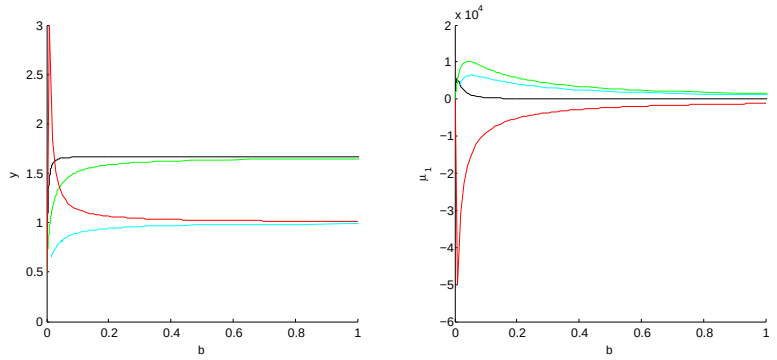
(a) Sensitivity with respect to a



(b) Sensitivity with respect to b



(c) Sensitivity with respect to k



(d) Sensitivity with respect to δ

Figure 4.16: The sensitivity of the boundary equilibrium

4.6 Long-Run Optimal Solutions

In this section, the calculated equilibria will be checked looking for candidates for long-run optimal solutions. In a next step, trajectories converging towards the selected candidates will be computed using the BVP approach (see [1]).

In Section 2.4 on Page 15, based on the Legendre-Clebsh condition, the constraint $\lambda_1 > 0$ for the base case parameter $\alpha = 0.5$ was identified to be necessary for the concavity of the Hamiltonian in the interior of the control region. In case of a boundary equilibrium, however, the Legendre-Clebsh condition cannot be used. In this case, the value of the Hamiltonian H should decrease given a slight increase in the control u. Mathematically spoken, this means that

$$\exists \epsilon > 0 : H_u < 0, \ \forall u : u - \overline{u} < \epsilon.$$

Because $L_u = H_u + \mu_1 - \mu_2$ has to be equal to zero for an admissible steady state, the condition above implies that μ_1 has to be greater than zero, which satisfies the complementary slackness condition.

Using the first condition, one can see that for the two simple models, *aconv* and *aconc* with monotonically increasing reaction functions $h(x)$, none of the calculated equilibrium points in the interior of the control region are candidates for long-run optimal solutions. However, both models also exhibit steady states (EP_3) at the boundary of the control region with $H_u < 0$, making these two equilibrium points candidates for long-run optimal solutions. In the *provoking*-model, equilibrium $EP_2 = (0.39692, 4.9122, 3.2274, 7.3932)$ is the only equilibrium in the interior of the control region which satisfies the positivity of λ_1. Since this equilibrium also exhibits a two-dimensional stable manifold (see Table B.1), it is a candidate for a long-run optimal solution. In this model, the boundary equilibrium is not taken into account since $H_u > 0$, which implies that the Lagrange multiplier $\mu_1 < 0$. In the *deterred*-model, it turns out that there exist three possible candidates for long run solutions in the interior of the control region (EP_2, EP_4, EP_5), but checking Table B.1, one can immediately see that only EP_4 is a candidate for a long-run optimal solution, since this is the only equilibrium exhibiting a two-dimensional stable manifold. In contrast to the *provoking*-model, in this model the boundary equilibrium comes into consideration to be an additional candidate since $H_u < 0$.

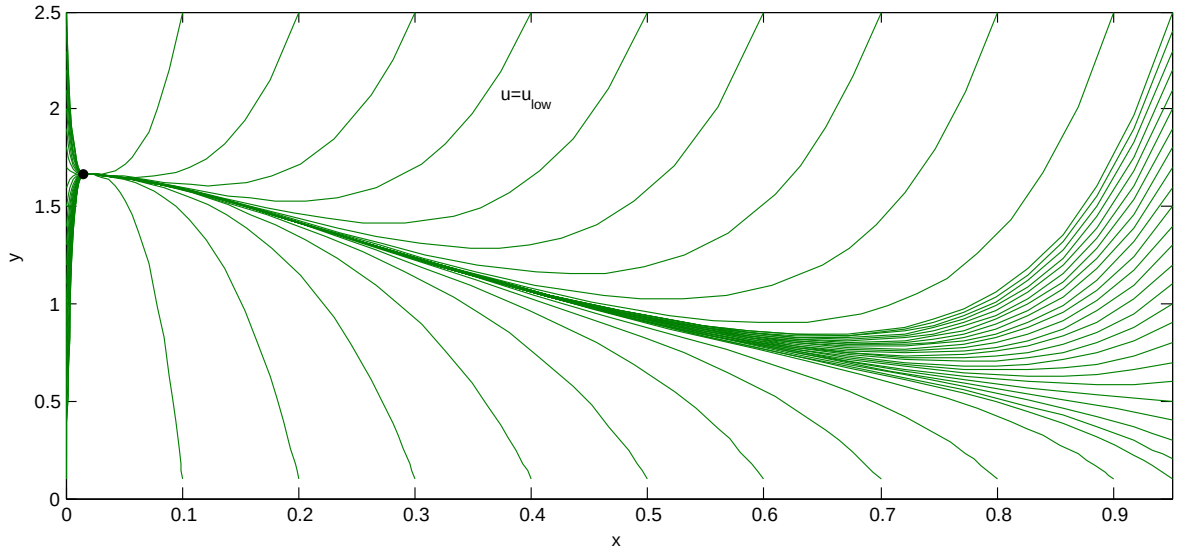


Figure 4.17: The phase portrait of the *aconv*-model

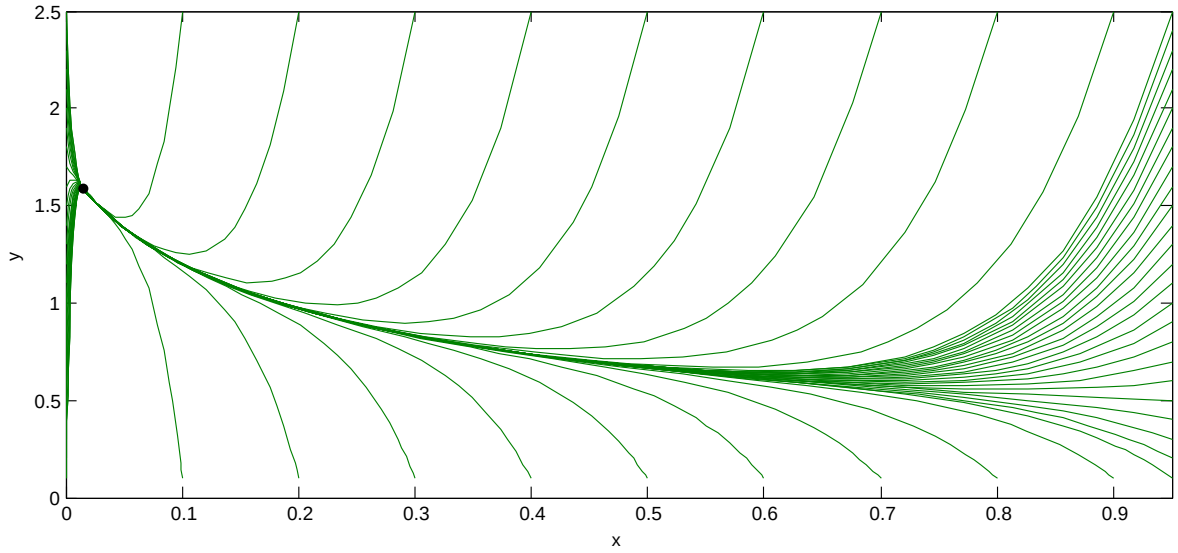
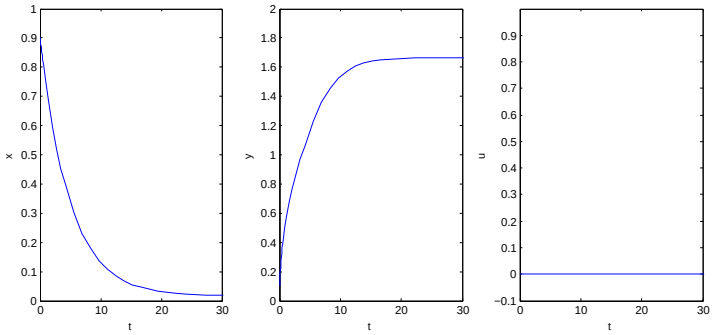
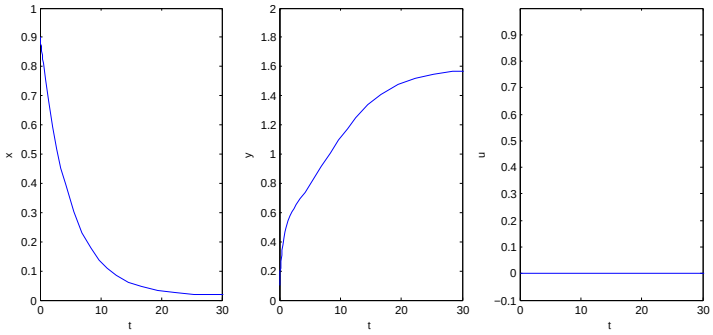


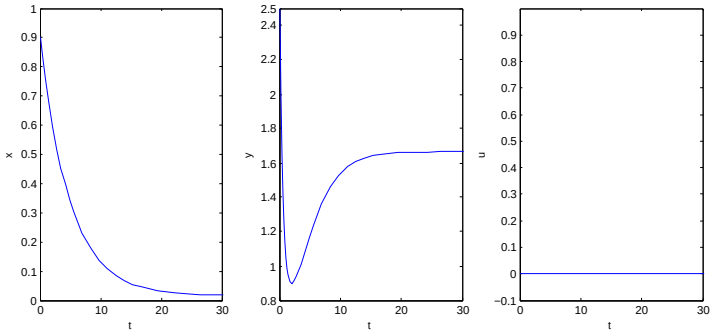
Figure 4.18: The phase portrait of the *aconc*-model



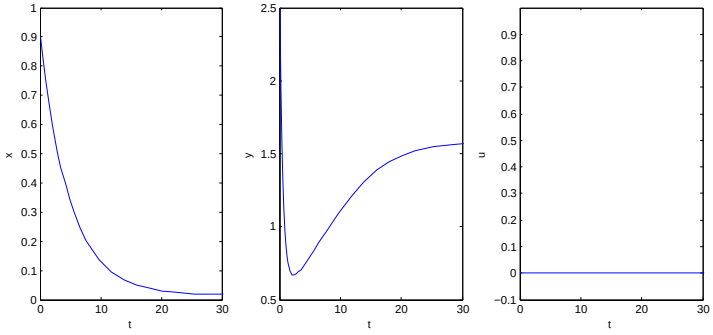
(a) The time path for inital value (0.9/0.1) of the *aconv*-model



(b) The time path for inital value (0.9/0.1) of the *aconc*-model



(c) The time path for inital value (0.9/2.5) of the *aconv*-model



(d) The time path for inital value (0.9/2.5) of the *aconc*-model

Figure 4.19: The time paths of the *aconv*- and *aconc*-models for initial values (0.9/0.1) and (0.9/2.5)

As one can see, both of the phase portraits (Figures 4.17 and 4.18 on Page 50) for the simple models with aggressive attackers look pretty much the same. As it could be expected, given the model formulation, the optimal policy in these models is to fully invest directly into the asset (which can be seen because of the green color of the paths, implying a control value at the lower boundary of the control region). The control value at the boundary of the control region over the whole solution path implies that security efforts are reduced to a minimum and the whole budget is invested into the asset. The exemplary time paths of the solutions on Page 51 show that this policy causes security to decrease over time due to depreciation. If one remembers how the security level influences the model dynamics, this result will be no suprise. Recalling the dynamics for the value of the asset y,

$$\dot{y} = d(1-u) - a(h(x)y^{\beta})^{\gamma},$$

one can see that an increasing security level given this kind of aggressive attacker influences the model only in a negative way, since the value of the asset will be reduced the higher security measures x get ($h(x) > 0\,, \forall x > 0$). This leaves the decision maker with no other choice than investing everything possible into the asset, or to say repair the damages done by the attacker, leading to an ever decreasing security level resulting in a decreasing reaction function, which ultimately leads to a poorly secured but fairly valuable asset. However, Figures 4.17 and 4.18 show that the evolution of the solution strongly depends on how valuable the asset is given a certain level of security. Starting at the same security level of 0.9 but different values of the asset of 0.1 and 2.5, in the first case the value gets built up monotonously, while in the second case the value gets reduced non-monotonously. Figure 4.19 illustrates this behavior. Of course, this kind of attacker does not seem quite realistic. However, it is possible to obtain some interesting results of the model and analyze whether the outcome is what one would expect.

From a mathematical point of view, it is easy to see that it makes almost no difference if the reaction function is a convex or concave one and, because of how x influences these models, the optimal control value will stay at the lower boundary despite parameter changes. The only difference, as the time paths on Page 51 show, is the slightly different behaviour at around $t = 10$ with $x \approx 0.1$. In the *aconv*-model, the value of the asset gets built up faster since the reaction function has smaller values. To illustrate the trade-off between wealth and security in these models, in Figure 4.20 the assumption was made that a decision maker has to invest at least 40% of his budget into the security level, now leaving him/her with a well-secured asset that does not have the same high value as before.

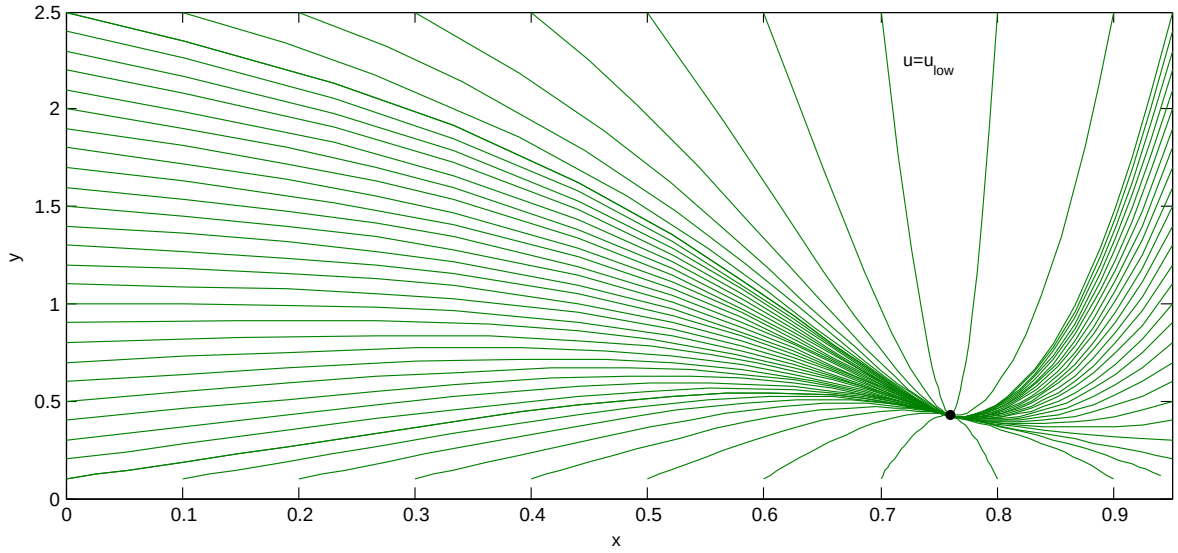


Figure 4.20: The *aconv*-model with minimum expenditures on security of 40 %

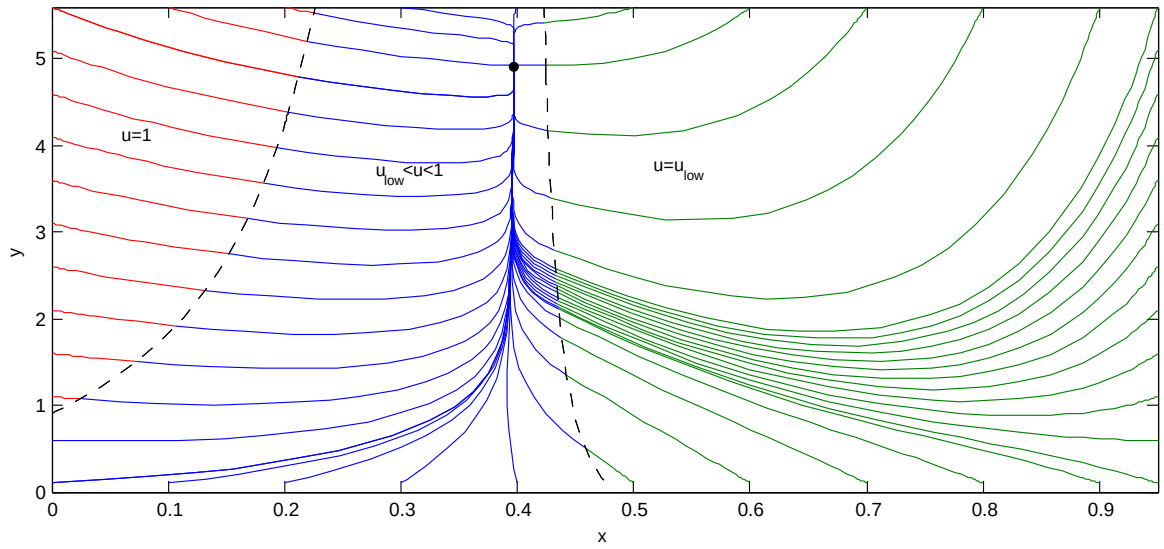


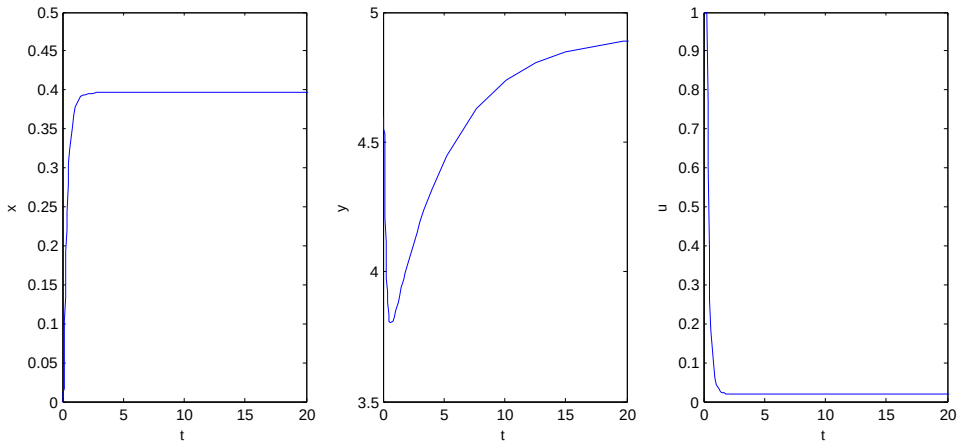
Figure 4.21: The phase portrait of the *provoking*-model

In the more complex *provoking*-model (Figure 4.21), which describes an aggressive attacker who increases his/her attacks at a certain level of security since he seeks to spread fear, the first thing one can notice is the long-run equilibrium at $x \approx 0.4$, which coincides with the minimum of the reaction function $h(x)$ of the attacker. In this model, in the long run, it is optimal to choose a policy which leaves the decision maker with an averagely secured asset. One can see that there exist two boundary curves, where either one of the control constraint becomes active. This basically divides the state space into three areas, where two fundamentally different policies have to be taken into account:

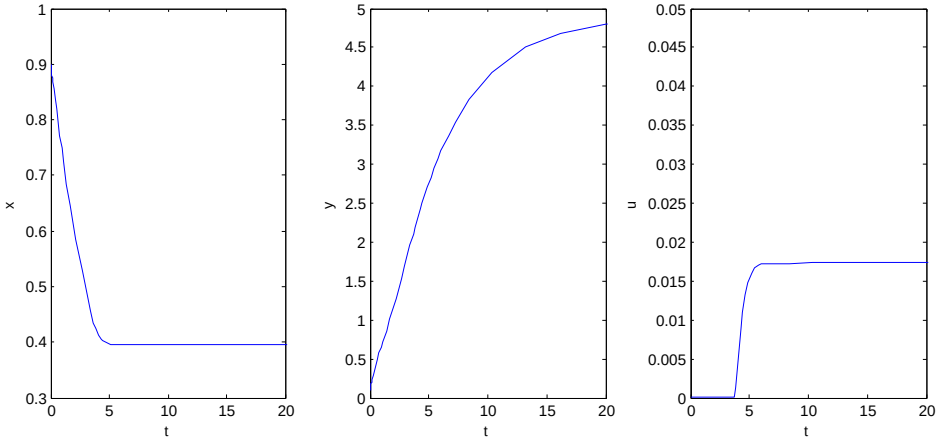
- Initial values in the red area imply a worthy asset which is poorly secured. As an example, in Figure 4.22(a) on Page 56 the time path for the solution with inital value (0,4.6) is depicted. In this case, the reaction function $h_p(x)$ is 0.5 implying a high value of the damage function $\mu(v(x, y))$, which results in a negative value of $\dot{y}$. Therefore, in the beginning it is optimal to fully invest into security (as can be seen at the time path of the control or the red part of the corresponding path in the phase portrait in Figure 4.21). This will cause the reaction function to decrease and $\dot{y}$ will increase over time. However, for some time $\dot{y}$ stays negative implying that the value of the asset will decrease, which can be seen along the red part of the solution path or the time path of $y(t)$ in Figure 4.22(a). At the boundary curve, the decision maker starts investing a huge share into the asset (implying that the control value decreases drastically in Figure 4.22(a)). Since the security level now is high enough so that the reaction function comes close to its minimum, the damage decreases leading to an increase in $\dot{y}$, which implies that value now can be built up until the path reaches the steady state.

- Initial values in the green area are basically divided into the ones with high security and low value (for example (0.9,0.1)), and high security and high value (0.9,5.6). From the different shape of the paths, one can see that the same policy may lead to different dynamics over time, which in detail can be seen in Figures 4.22(b) and 4.22(c) on Page 56. Starting at (0.9,0.1) implies that the decision maker faces an attacker with a high reaction function. This implies that the attacker does a lot of damage yielding the necessitiy to fully invest into the asset to compensate for these heavy attacks. Because of depreciation, this yields a decreasing security level. As security decreases, the attacker's reaction function gets smaller which yields increasing $\dot{y}$. Hence, the value of the asset can be built up as can be seen on the time path of y in Figure 4.22(b). On the other hand, following the path starting at (0.9,5.6), i.e. starting with a highly secured, valuable asset, the decision maker faces attacks which are too heavy to maintain or even build up the value of the

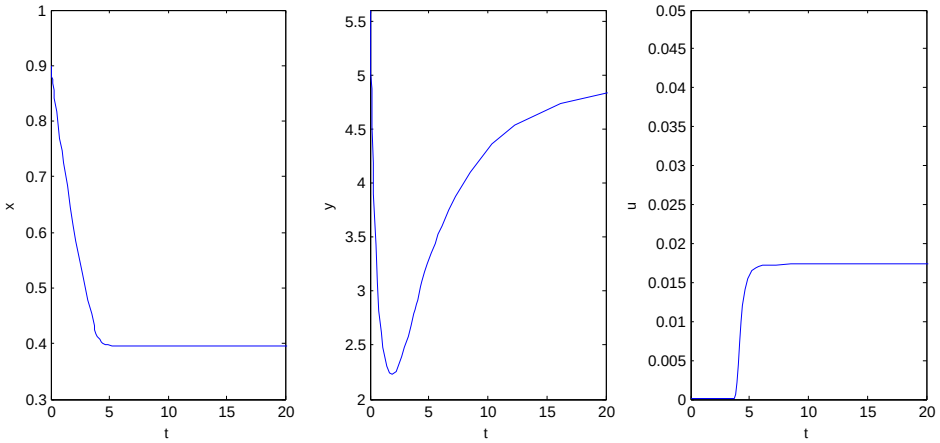
asset leading to a drastic decrease of y. After a short time in the time path of y, the strikes of the attacker become less powerful, because x was reduced to a level, which the attacker cannot use for politically motivated attacks anymore and therefore the value of the asset can be built up again. It is interesting to see that in this case the asset gets restored nearly to the initial value but with a security level low enough so the attacker does not get attracted to use a high security level for his purpose. This case reflects some kind of "fooling" strategy, where the defender restores the asset nearly to the old value but now keeps a lower security level so the attacker's attention is not drawn to the asset.



(a) The time path for the *provoking*-model for inital value (0/4.6)



(b) The time path for the *provoking*-model for inital value (0.9/0.1)



(c) The time path for the *provoking*-model for inital value (0.9/5.6)

Figure 4.22: The time paths for the *provoking*-model for different initial values

Before analysing the *deterred*-model, one has to "prove" at least numerically that one of the two admissible steady states exhibiting a two-dimensional stable manifold is the only candidate for a long-run optimal solution. Following [1], this is done by trying to continue the optimal solution along the line, which connects the two steady states exhibiting a two-dimensional stable manifold. In Figure 4.23, the black and red points are the stationary points exhibiting a two-dimensional stable manifold. Calculating the path starting at the red point leading to the boundary equilibrium yields the green path. The solution starting at the black equilibrium converging towards the red one cannot be calculated, which is a first indication that the black equilibrium at the boundary of the control region is the only long-run solution. To test if this suspicion proves right, the path starting at the green, admissible steady state, which exhibits a two-dimensional stable manifold into the red and black ones is computed, too. As one can see in Figure 4.24, the Hamiltonian along the purple path is smaller than the Hamiltonian along the path from the green to the black steady state, which ultimately supports the assumption that the black steady state is part of the long-run solution.

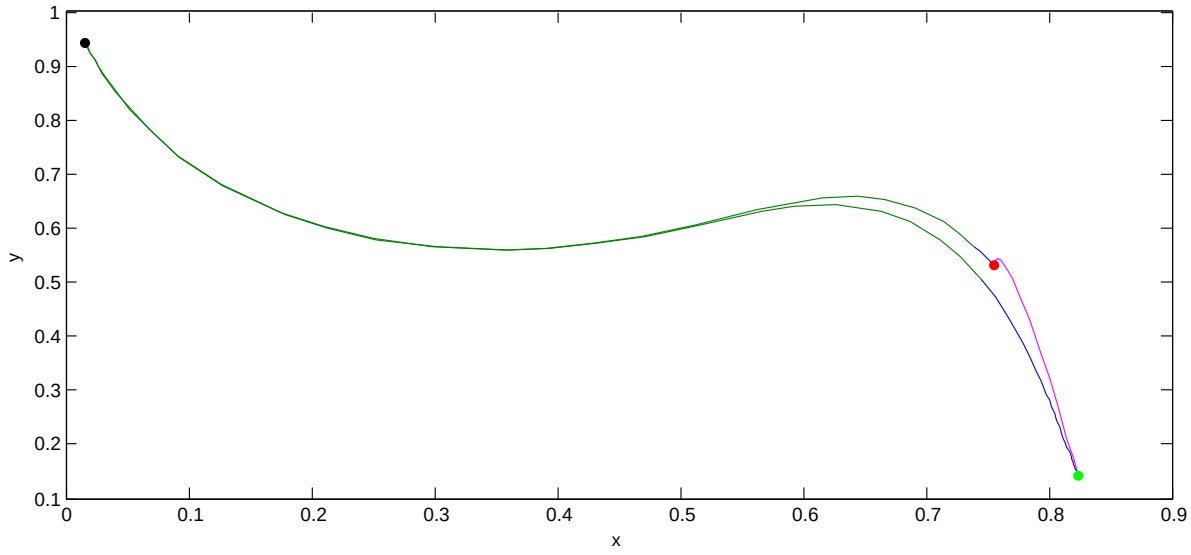


Figure 4.23: Looking for the only long-run optimal solution in the *deterred*-model

In the phase portrait of the *deterred*-model (Figure 4.25), one can see that results are quite unexpected. In this case, the reaction function $h_d(x)$ was 0.5 for $x = 0$, 0.9 for $x = 0.4$, and 0 for $x = 1$. So, one might expect that paths which start at a high security level lead to a steady state exhibiting a high security level, since in this case $h_d(x)$ would stay small over the whole path. Instead, the phase portrait shows that all paths lead to the steady state with low security with a boundary curve where the optimal control value

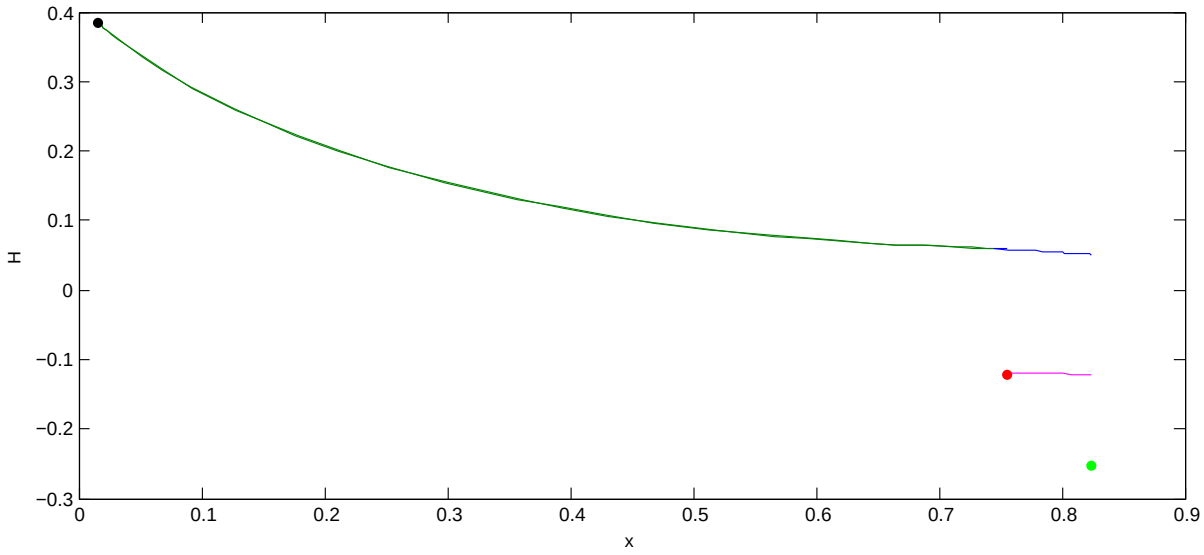


Figure 4.24: Hamiltonians along the paths in the *deterred*-model

even gets reduced to its minimum. To interpret this circumstance, one may look at the path starting at (0.9,2.6) and the corresponding plots of the time path in Figure 4.26 on Page 59. The initial value lies in the blue region where no control constraint is active yielding a control value in the interior of the control region. But as one can see, as the path converges to the steady state, both the security level x and the value of the asset y decrease initially. That is because on the one hand, security investments on this path are too small to even compensate for depreciation and on the other hand, investments in the asset are way to low to compensate for the damage caused by the attacker, i.e. $\dot{y}$ is less than zero. The negative effect of decreasing security leads to increased attacks due to the shape of the reaction function $h_d(x)$. As the control constraint becomes active after just two units of time, the whole budget is invested into the asset but the overall level of y still decreases until the decreasing security level finally yields a build-up of y at t approximately 8. This is mainly based on the choice of parameter d. As it was already mentioned, especially the decrease of y, although almost the whole budget is invested into it, comes from the negativity of the dynamics $\dot{y}$. This can either be based on a bad restore capability, d (i.e. the decision maker cannot build up value fast enough) or a high attack capability, a, of the attacker.

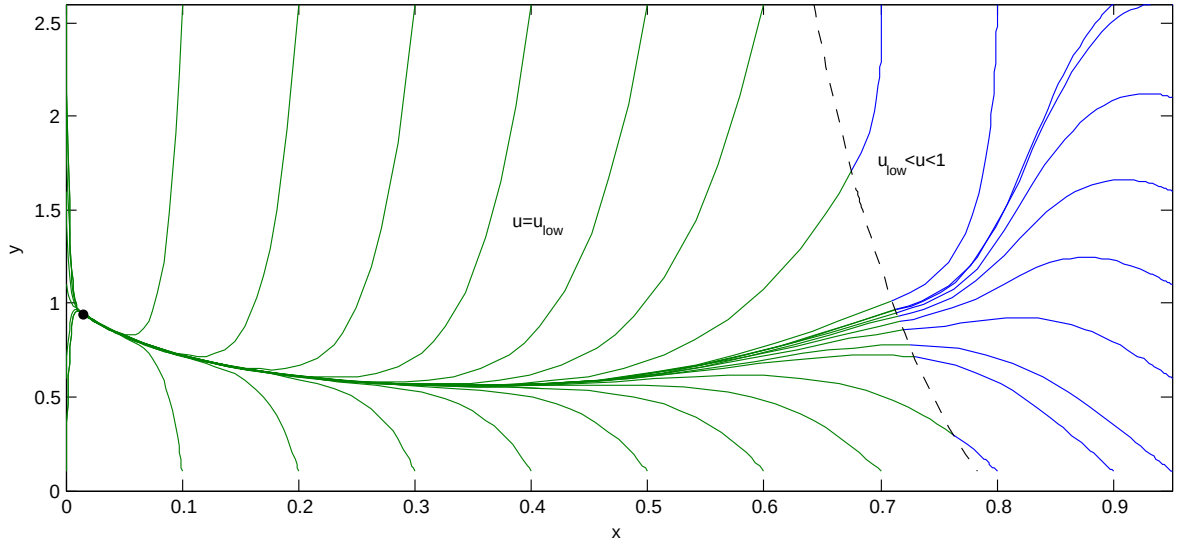


Figure 4.25: The phase portrait of the *deterred*-model

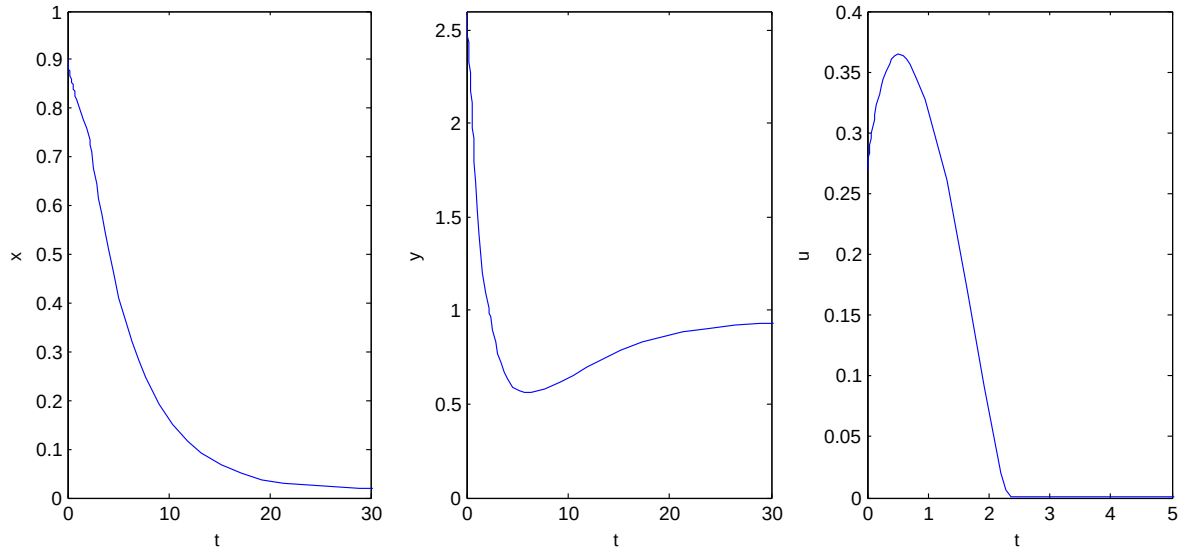


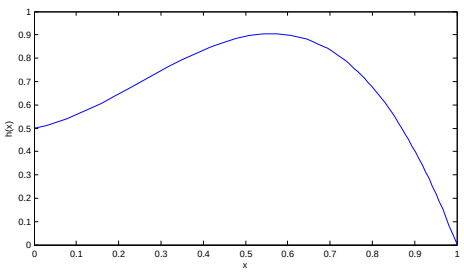
Figure 4.26: The time path of the *deterred*-model starting at the initial value (0.9/2.6)

Chapter 5
Convex-Concave Reaction Functions

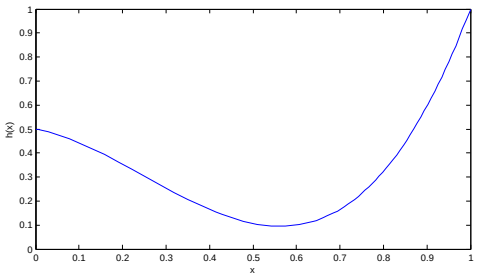
5.1 Deriving the Functions

In this chapter, so-called convex-concave or concave-convex reaction functions $h(x)$ will be introduced, instead of strictly convex (concave) functions to analyze if inflexion points have any impact on the optimal control or the optimal solution paths.

Since one of the most simple functions with an inflexion point is a polynomial of degree 3, $h(x) = ax^3 + bx^2 + cx + d$, this will be the initial functional form. By stating four different conditions on $h(x)$, some related to the model itself, some of technical nature to obtain "good" functions, it is possible to derive the following functions for the *deterred* and *provoking* type, respectively. As one can see, the levels at $x = 0$ and $x = 1$ are the same as in the *provoking*- and *deterred*-models. The minimum and maximum, however, are slightly different from the other two functions, which will be taken into account when analyzing the phase portraits. Since in this chapter the shape of the functions is the esential part and not the values themselves, comparability is not hugely affected.



(a) *deterred* type: h_{dext}



(b) *provoking* type: h_{pext}

Figure 5.1: Different types of attacker for the extension

Stating the assumptions $h_{dext}(0) = 0.5$, $h_{dext}(1) = 0$, $h_{dext}(0.6) = 0.9$, and $h''_{dext}(\frac{124}{495}) = 0$, one can solve a system of four equations to calculate the functional form of $h(x)_{dext}$:

$$h(x)_{dext} = -\frac{55}{16}x^3 + \frac{31}{12}x^2 + \frac{17}{48}x + \frac{1}{2}.$$

Mirroring this function at $z(x) = 0.5$ yields $h(x)_{pext}$:

$$h(x)_{pext} = \frac{55}{16}x^3 - \frac{31}{12}x^2 - \frac{17}{48}x + \frac{1}{2},$$

resulting in the following reaction functions:

$$v(x,y)_{pext} = \left(\frac{55}{16}x^3 - \frac{31}{12}x^2 - \frac{17}{48}x + \frac{1}{2}\right) y^\beta$$
$$v(x,y)_{dext} = \left(\frac{-55}{16}x^3 + \frac{31}{12}x^2 + \frac{17}{48}x + \frac{1}{2}.\right) y^\beta$$

5.2 Steady States

Following Section 2.4 to formulate Pontryagin's Maximum Principle and Section 2.5 to calculate steady states, one is able to obtain the following equilibrium points (Table 5.1) of the canonical system. Again, the admissible stationary points are displayed bold. Comparing Table 5.1 with the steady states from the base case models (Table 3.2 on Page 31), one can see that the steady state in the *extended provoking*-model exhibit the same qualitative properties as in the base model. The only admissible steady state is located at the minimum value of x of the applied reaction function. Although in the *extended* model the stationary value of x is a bit higher, the steady state value of y is almost the same. This shows in a mathematical way what could be expected beforehand: the higher the threshold, where an attacker gets provoked to increase his/her attacks, the better for the decision maker.

In the *extended deterred*-model, much like in the case of the *provoking*-model, the usage of a concave-convex function does not have an impact on the number or location of stationay points. Again, there are two high and two low steady states, each time with one being admissible. Additionaly, there is an admissible steady state at $x \approx 0.77$, which is located between these four (in relation to x). Finally, the admissible boundary equilibrium also occurs in this case. However, it can be seen that the higher value of the maximum of the reaction function in this *extended* case (0.56 compared to 0.4 in the base model) influences the values of x of the two low steady states (EP_2 and EP_5 in Table 5.1) significantly.

For example, this higher maximum changes the stationary security level of the two high equilibrium points only about 0.15, while in the case of the two low equilibria the increase in the maximum point relates almost 1:1 to the increase of the low steady states. Due to the trade-off structure of the model, however, this higher security level yields a lower value of the asset.

		EP_1	EP_2	EP_3	EP_4	EP_5	EP_6
$h(x)_{pext}$	$\hat{x}$	0.76844	0.8266	**0.55402**	0.82764	0.5713	0.015565
	$\hat{y}$	1.0669	0.11857	**4.9172**	0.10064	4.8651	1.0124
	$\hat{\lambda_1}$	-14.7124	-1.2402	**8.5698**	-1.0506	-9.5542	6.7851
	$\hat{\lambda_2}$	2.5665	0.11278	**7.6916**	-0.094283	7.6839	1.2134
	$\hat{u}$	0.4405	0.9090	**0.0617**	0.9223	0.0710	0.00001
	H_u	-5.13296	-0.22555	**0**	0	-15.36787	1054.9
	H_{uu}	2.91306	0.06203	**-62.3030**	0.05111	54.0852	
$h(x)_{dext}$	$\hat{x}$	**0.80441**	0.53949	0.81713	**0.76922**	**0.5952**	**0.015565**
	$\hat{y}$	**0.24234**	0.5232	0.15756	**0.37724**	**0.50686**	**0.98789**
	$\hat{\lambda_1}$	**1.4584**	-0.3324	0.99879	**1.9653**	**0.45944**	**-6.4682**
	$\hat{\lambda_2}$	**0.17339**	0.32666	-0.10218	**0.34019**	**0.31622**	**1.1681**
	$\hat{u}$	**0.6766**	0.0549	0.7987	**0.4444**	**0.0865**	**0.00001**
	H_u	**0**	-0.65332	0.20437	**0**	**0**	**-1007.958**
	H_{uu}	**-0.128132**	2.975270	-0.063968	**-0.38276**	**-1.828274**	

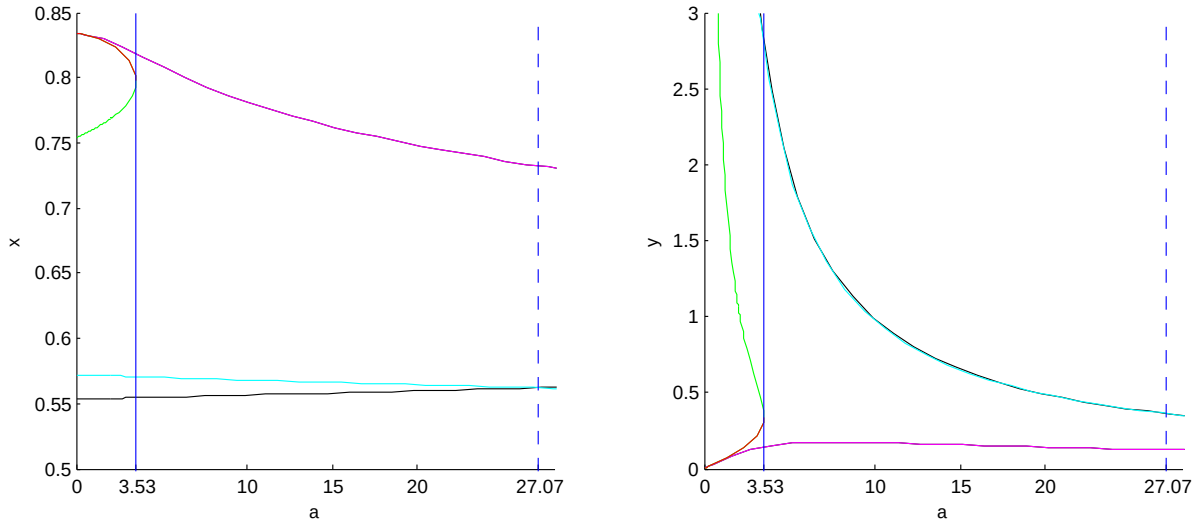
Table 5.1: Steady states for the *extension*

In addition, Appendix B on Pages 78 and 79 provides the eigenvalues of the steady states of the *extended* models.

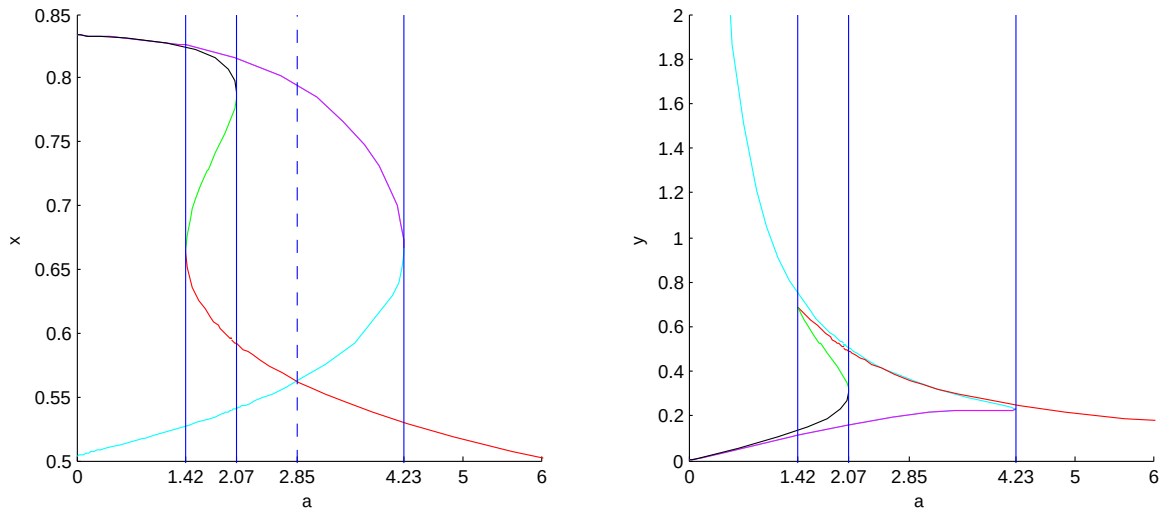
5.3 Sensitivity and Optimal Paths

5.3.1 Changes in the Sensitivity

In the case of a change of parameter a, one can see that, compared to the *provoking base*-model, the *extended*-model exhibits the same characteristics (see Figure 5.2). The significant difference lies in the smaller value of the bifurcation point. However, in the *extended deterred*-model one can see that in the analyzed parameter area there are two additional blue sky bifurcations. This is interesting, because the two thresholds of about 1.4152 and 2.065 set limits to a very small area, in which the admissible steady state at $(x = 0.76922, y = 0.37422)$, which in this model will also be a candidate for a long-run optimal solution exists. In addition, the new threshold at around 4.23 generates an area in which three steady states exist in the interior of the control region.

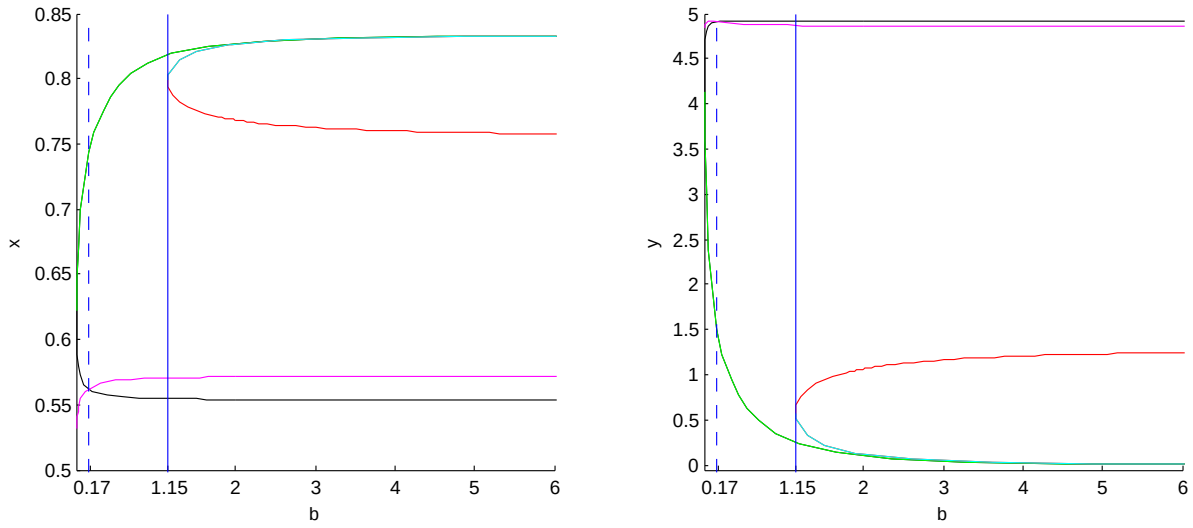


(a) Sensitivity diagram with respect to a for the *extended provoking*-model including non-admissible steady states (black is the admissible steady state)

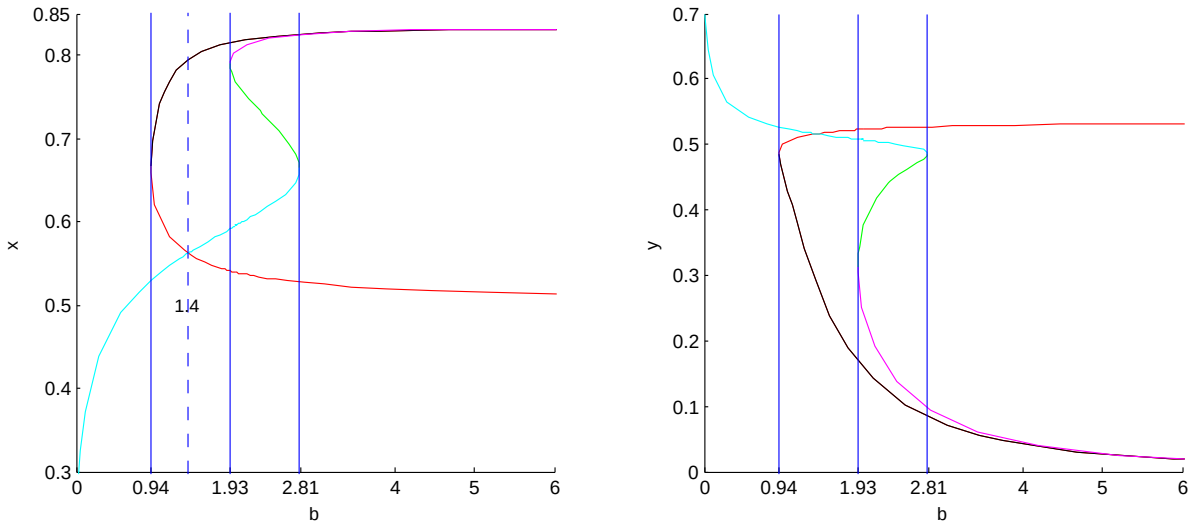


(b) Sensitivity diagram with respect to a for the *extended deterred*-model including non-admissible steady states (green is the admisible steady state exhibiting a two-dimensional stable manifold)

Figure 5.2: Sensitivity diagram of the *extended provoking*- and *deterred*-models with respect to a including non-admissible solutions

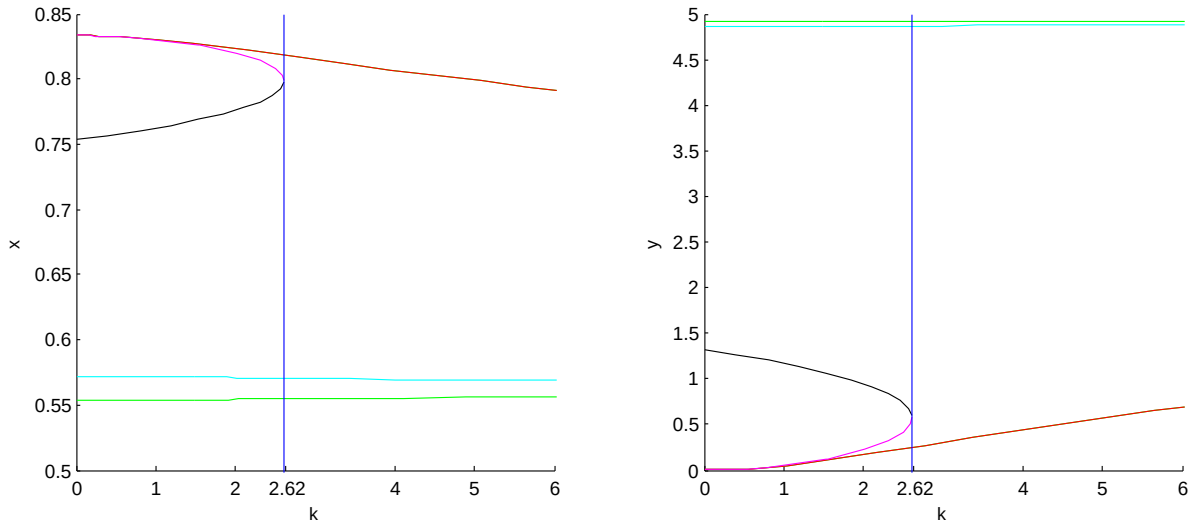


(a) Sensitivity diagram with respect to b for the *extended provoking*-model including non-admissible steady states (black is the admissible steady state)

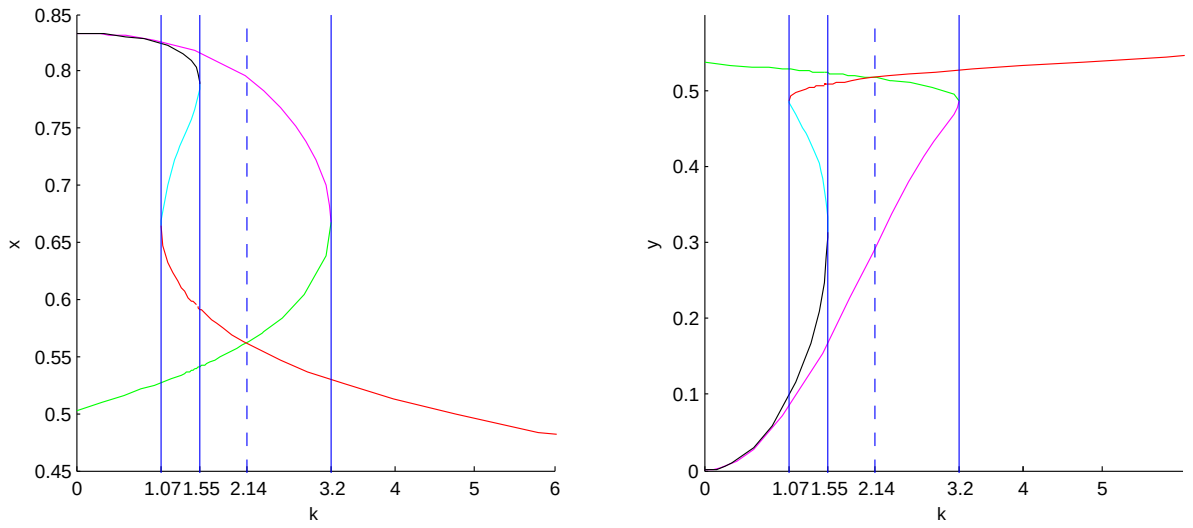


(b) Sensitivity diagram with respect to b for the *extended deterred*-model including non-admissible steady states (green is the admisible steady state exhibiting a two-dimensional stable manifold)

Figure 5.3: Sensitivity diagram of the *extended provoking*- and *deterred*-models with respect to b including non-admissible solutions



(a) Sensitivity diagram with respect to k for the *extended provoking*-model including non-admissible steady states (green is the admissible steady state)

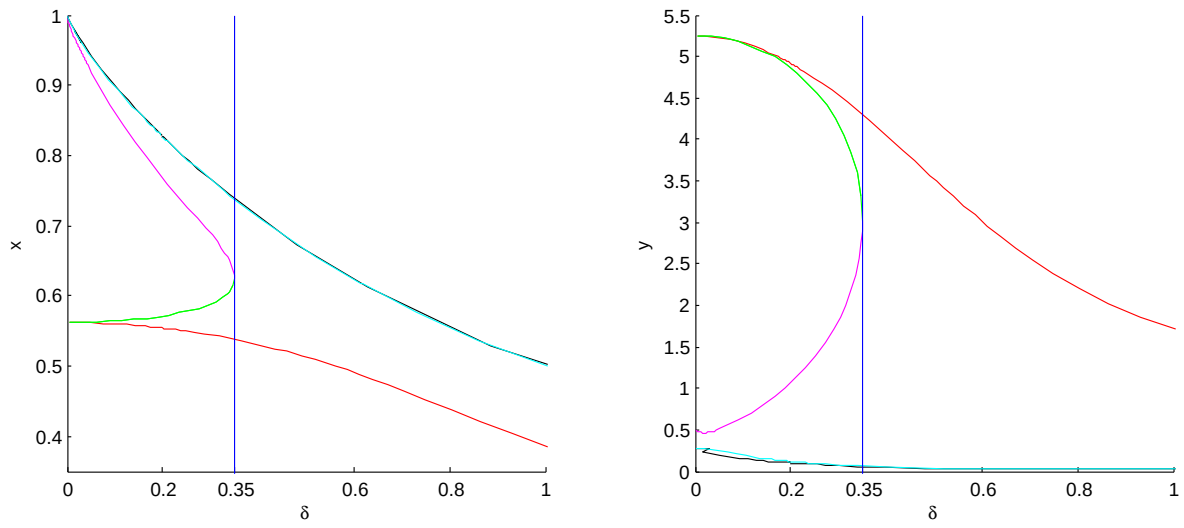


(b) Sensitivity diagram with respect to k for the *extended deterred*-model including non-admissible steady states (blue is the admisible steady state exhibiting a two-dimensional stable manifold)

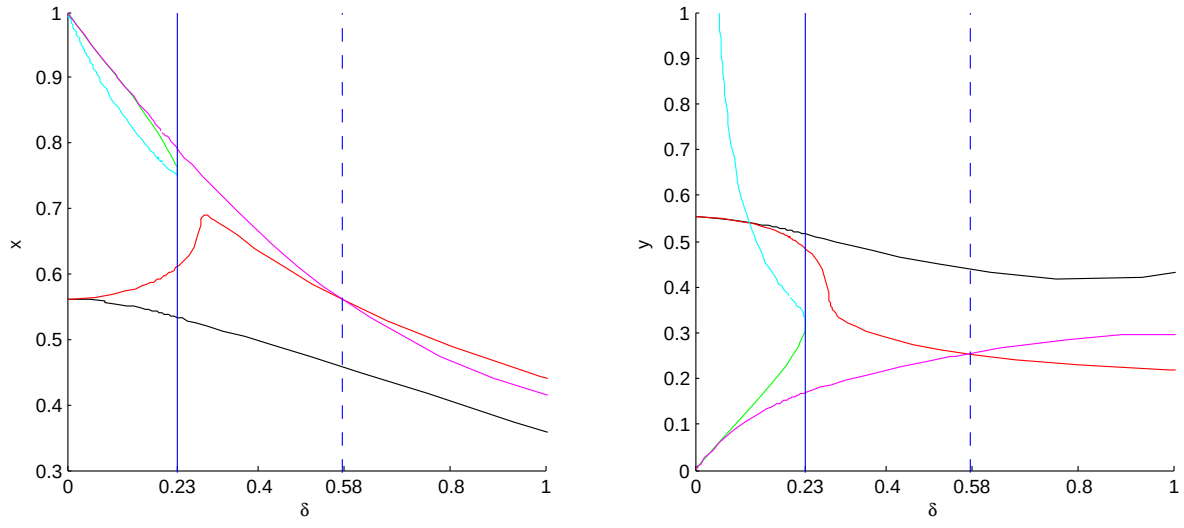
Figure 5.4: Sensitivity diagram of the *extended provoking*- and *deterred*-models with respect to k including non-admissible solutions

In the case of the changes of parameter b (Figure 5.3) and k (Figure 5.4), i.e. the asset generates more wealth or more harm if damaged, the situation follows the one in the case of changes in a. The *extended provoking*-model exhibits a slightly different blue sky bifurcation level, but overall the changes in steady state levels follow the same dynamics. In the *extended deterred*-model, however, an additional fold bifurcation yields the admissible equilibrium at $x = 0.76922$ only to exist in a small parameter interval.

In the case of parameter changes of δ, there is an interesting observation to be made. If one compares Figure 4.13(b) on Page 45 and Figure 5.5(b), one can notice that at the bifurcation level in the two cases different steady states are generated or to say they vanish if one starts the analysis at the base case value of $\delta = 0.2$. In the *deterred*-model the middle and one of the low steady states disappear at the bifurcation value of about 0.463. However in the *extended*-model it is the middle and one of the two high steady states, which vanish at the bifurcation point.



(a) Sensitivity diagram with respect to δ for the *extended provoking*-model including non-admissible steady states (red is the admissible steady state)



(b) Sensitivity diagram with respect to δ for the *extended deterred*-model including non-admissible steady states (blue is the admisible steady state exhibiting a two-dimensional stable manifold)

Figure 5.5: Sensitivity diagram of the *extended provoking*- and *deterred*-models with respect to δ including non-admissible solutions

As it was shown, the extension to a concave-convex function in addition to the change of the location of the minimum of $h(x)$ in the *extended provoking*-model barely affects the steady state values or the sensitivity of the model. However, it could be noticed that the extension to a convex-concave function $h(x)$ in the case of the *deterred*-model does not only have an effect on steady state values but also changes the sensitivity of the model completely, whether it is the number of blue-sky bifurcations or the diversity of stationary points, which are generated at these thresholds.

5.3.2 Changes in the Optimal Paths

Again, with the necessary condition $\lambda_1 > 0$ and the first-order condition $H_u = 0$, EP_3 of the *pext*-model can be identified to be a candidate for a long-run optimal solution. In the *extended deterred*-model, steady states EP_1, EP_4, and EP_5 in addition to the boundary equilibrium must be taken into account. Checking Table B.2, looking for stationary points exhibiting a two-dimensional stable manifold, reveals that EP_4 and EP_6 of the *extended deterred*-model are fitting candidates. Comparing these candidates to the ones from the base model shows that the different shape of the reaction function in a first step does not affect the choice of steady states, which have to be considered as part of a long run solution.

Following Grass et al. (see [1]), again a BVP approach is used to calculate the solution paths in the *extended*-models, which is implemented in the OcMat Toolbox. Similar to the results of the sensitivity analysis, one can see that the solution paths of the *extended provoking*-model in Figure 5.6 exhibit the same overall behavior. Due to the different location of the minimum of the reaction function $h(x)$, the steady state has a different level, which shifts the area where no control constraint is active to the right, causing the area to grow, in which the control value lies at the upper boundary and the area to shrink, in which the control value lies at the lower boundary.

In the *extended deterred*-model (Figure 5.7), the same method as in the base model can be used to numerically "prove" that the steady state at the boundary of the control region is the only candidate for a long-run solution. As it can be seen, also in this case the different location of the maximum of $h_{dext}(x)$ results in the boundary curve being located more to the right, yielding a smaller area, in which no control constraint is active. It is further noticable, that the inflexion point at about 0.25 seems to have an impact on how the paths converge to the steady state. In the *deterred*-model (Figure 4.25 on Page 59), the paths in this area ($x \in (0.1, 0.3)$) converge in a convex way to the equilibrium point, whereas in the *extended*-model the paths follow a convex-concave shape. Comparing the

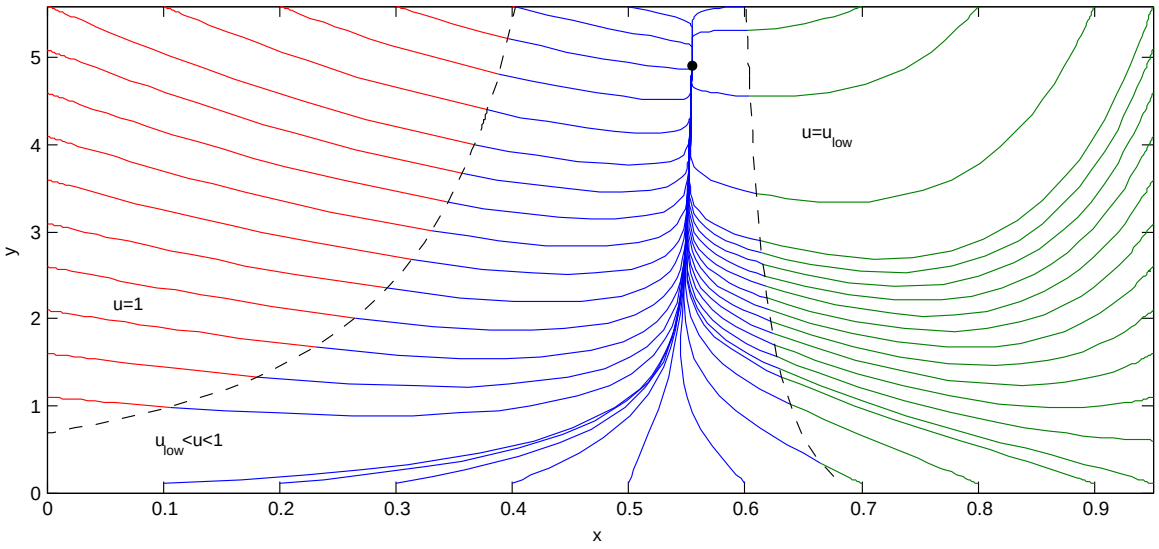


Figure 5.6: The phase portrait of the *extended provoking*-model

time paths for the initial value (0.9,2.6) in Figures 5.8(b) for the *extended* and Figure 4.26 on Page 59 for the base model, one can see that this difference in how the paths converge towards the steady state has a minimal impact on how the time path of y looks like. In addition, the smaller area of inactive control constraints is reflected in the short time the control in Figure 5.8(b) stays above its minimum level.

As it was shown in this chapter, the introduction of a concave-convex reaction function in the *extended provoking*-model barely has any effect concerning steady states or optimal paths. In this model, the difference in the location of the minimum of the reaction function played a bigger role yielding a change in the steady state values and therefore a change in control values along the optimal path.

However, on the other, hand the *deterred*-model was affected in different ways by the usage of a convex-concave reaction function and a different location of its maximum. The steady state levels, especially of the low stationary points, were affected more in relation to the *provoking*-model, the sensitivity in some cases changed completely and the solution paths converged slightly differently towards the equilibrium.

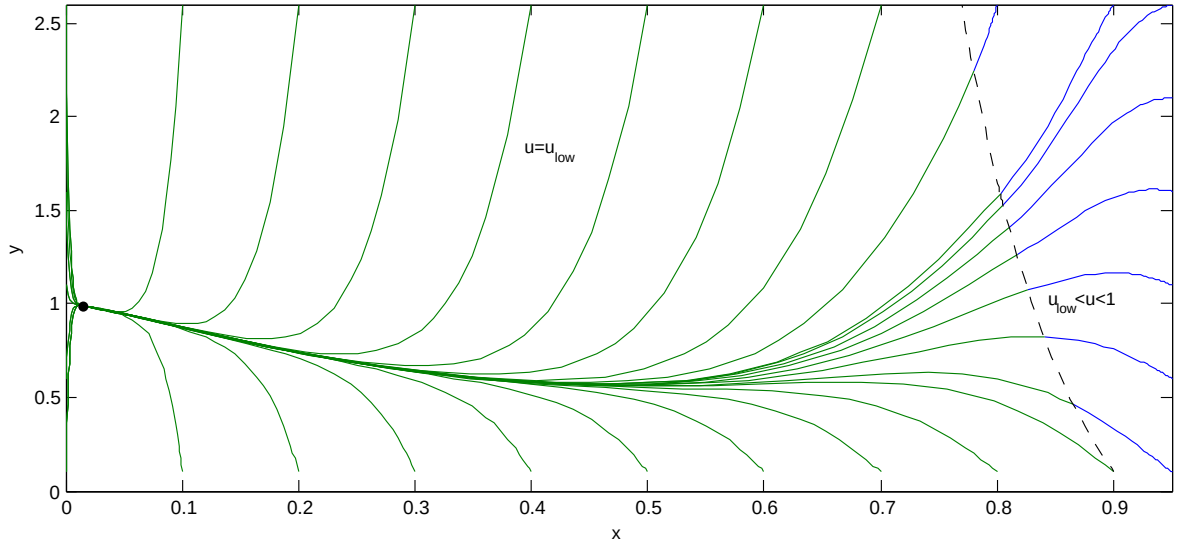
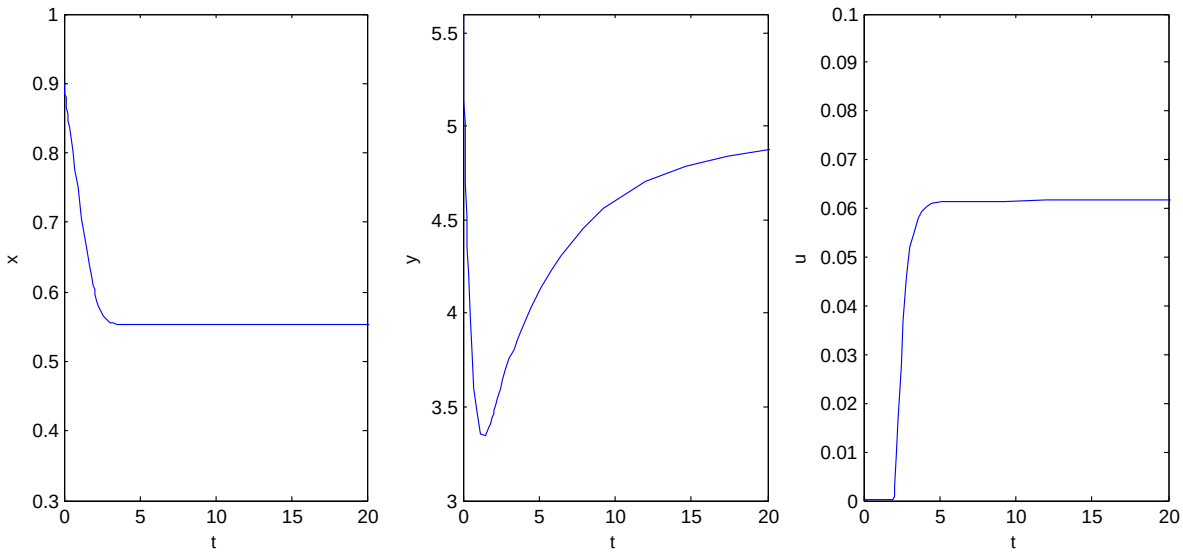
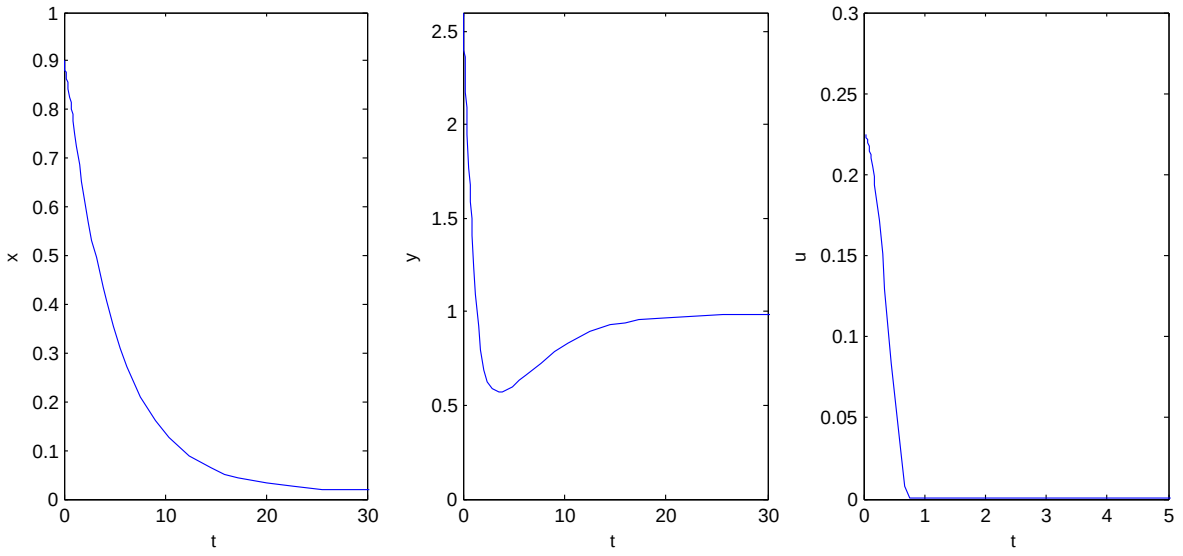


Figure 5.7: The phase portrait of the *extended deterred*-model



(a) The time path for the *extended provoking*-model for inital value (0.9/5.6)



(b) The time path for the *extended deterred*-model for inital value (0.9/2.6)

Figure 5.8: The time paths for the *extended*-models for different initial values

Chapter 6
Summary

6.1 Conclusion

The goal of this thesis was to formulate a nonlinear optimal control problem, which was based on the ideas of a game theoretical defender-attacker model by Kjell Hausken and Jun Zhuang. In this dynamic model, the defender became the decision maker trying to optimally invest a normalized budget into the security level of an asset she tries to defend, or directly into the asset. The second player, the attacker, was introduced as an exogenous force, namely a "reaction function", which depended on the security level of the asset. Together with a function describing the potential damage an attacker can inflict on an asset, it was possible to derive different kinds of attackers.

In a base case analysis parameter values were chosen to model a very capable, well organised attacker and it was assumed that the decision maker had limited ressources to restore damage to the asset. This was based on the attempt to point out the trade-off relation between the security level of the asset and the wealth it can generate.

Solving this base case model with Pontryagin's Maximum Principle led to different kinds of stationary points depending on how the attackers reaction function was modeled. Surprisingly, it turned out that in the case of a so-called "deterred" attacker the long run optimal solutions converged to a steady state at the boundary of the control region and not to a steady state in the interior of the control region. Additionally, a sensitivity analysis showed that this "deterred"-model was influenced by changes in parameter values in more ways than other models. Not only did steady state levels react more sensitive, it was also possible to observe multiple bifurcation threshold.

To analyse if the change from strictly convex (concave) to concave-convex or convex-concave functions has any impact on the model, two of the reaction functions of the

base case were extended this way. In addition, the points where these extended reaction functions took their minimum (or maximum) were changed. It turned out that effect of changing these extremal points of the reaction functions had a bigger effect on the models outcome than the introduction of inflexion points. Especially the "*deterred*"-model again turned out to be very sensitive to changes in parameter values, with admissible steady states existing only in very small parameter areas.

As it turned out, the attacker in the base case was modeled in a way, which often left the decision maker with the only choice to retreat and concentrate on repairing his/her asset. This was based on the negative dynamics of the value of the asset. This fact together with the observation that the "*deterred*"-model exhibited the most dynamic behavior leads to the assumption that it may be interesting to analyse this model in a framework, where the defender has more ressources to repair his/her asset and/or the attacker is not as strong as in the base case in this model. These two assumptions may most likely lead to multiple optimal solutions.

6.2 Extensions

Ending this thesis as it started, the connection to the game theoretical models should be carved out by suggesting some extensions which are based on the work of Hausken, Bier, and Zhuang ([5] and [6]).

6.2.1 Multiple Attackers

In relation to the paper "Defending against multiple different attackers" by Hausken and Bier (see [6]), the first extension of the optimal control problem formulated in this thesis could be the one of stating different attackers. Based on the basic idea of the model presented in this thesis to model the attacker's behavior by a reaction function, it is easy to implement the intention of Hausken and Bier ([6]) who consider a defender facing heterogenous attackers. As an example of heterogenous attackers, which was already used in the introduction of this thesis, the authors mention professional hackers and so-called "script-kiddies" on the field of computer security. These two types of attackers may be modelled by two different reaction functions $h_1(x), h_2(x)$ which exhibit different properties. For example, it is possible to state a reaction function of the *deterred*-type for the "script-kiddies", which has the threshold where they decrease their attacks already at a very low value of security level x. Aditionally, it is possible to replace the assumption

$h(1) = 0$ with $h(c) = 0$ with $c < 0$, which implies that the kiddies stop their attacks at all already at a lower level of security. In addition, the parameters in the damage function μ_i for the i-th attacker can be used to model the variability of different attackers even more. Since the damage caused to the asset in the dynamics of y now has to be added, the dynamics of y in the case of i different attackers becomes:

$$\dot{y} = g(1-u) - \sum_{i=1}^{n} \mu_i(v_i(x,y)).$$

The harm-function $D(\mu(v(x,y)))$ in this case then becomes a function depending on the overall damage, $\sum_{i=1}^{n} \mu_i$.

6.2.2 Additional Assets

Despite a significant increase in the complexity of solving such a model, adding dynamics for the security level and value of a second asset and corresponding control variables u_2 and u_3 to the model, expands the formulation to multiple assets. In this case, the decision maker tries to distribute the budget between two different assets by choosing control values for investements on the security level of asset 1 and asset 2, u_1, u_2, and the share u_3 of the budget which is invested in asset 1 implying that the rest of the budget, $1 - u_1 - u_2 - u_3$, will be invested in asset 2. Additionally, benefit and cost terms of the second asset have to be added to the objective function. This formulation, depending on the different kinds of attackers, allows a decision maker to respond to the question of finding an optimal defensive plan for multiple assets.

Chapter A
Base Case Models

A.1 The Base Model with $v = v(x, y)_{aconv}$

$$\max_{u} \quad \int_0^{\infty} e^{-0.05t} \left(2y - 1.5\sqrt{2y(0.7x^2 + 0.3)}\right) dt$$

$$\begin{aligned}
\dot{x} &= \sqrt{u}(1 - x) - 0.2x \\
\dot{y} &= 1 - u - 2y(0.7x^2 + 0.3) \\
x(0) &= x_0 \in [0, 1) \\
y(0) &= y_0 > 0 \\
&\quad u \in [\overline{u}, 1]
\end{aligned}$$

A.2 The Base Model with $v = v(x, y)_{aconc}$

$$\max_{u} \quad \int_0^{\infty} e^{-0.05t} \left(2y - 1.5\sqrt{2y(\ln(x + 1) + 0.3)}\right) dt$$

$$\begin{aligned}
\dot{x} &= \sqrt{u}(1 - x) - 0.2x \\
\dot{y} &= 1 - u - 2y(\ln(x + 1) + 0.3) \\
x(0) &= x_0 \in [0, 1) \\
y(0) &= y_0 > 0 \\
&\quad u \in [\overline{u}, 1]
\end{aligned}$$

A.3 The Base Model with $v = v(x, y)_d$

$$\max_u \quad \int_0^\infty e^{-0.05t}\left(2y - 1.5\sqrt{2y(-2.5x^2 + 2x + 0.5)}\right) dt$$

$$\begin{aligned}
\dot{x} &= \sqrt{u}(1-x) - 0.2x \\
\dot{y} &= 1 - u - 2y(-2.5x^2 + 2x + 0.5) \\
x(0) &= x_0 \in [0, 1) \\
y(0) &= y_0 > 0 \\
& u \in [\overline{u}, 1]
\end{aligned}$$

A.4 The Base Model with $v = v(x, y)_p$

$$\max_u \quad \int_0^\infty e^{-0.05t}\left(2y - 1.5\sqrt{2y(2.5x^2 - 3x + 1)}\right) dt$$

$$\begin{aligned}
\dot{x} &= \sqrt{u}(1-x) - 0.2x \\
\dot{y} &= 1 - u - 2y(2.5x^2 - 3x + 1) \\
x(0) &= x_0 \in [0, 1) \\
y(0) &= y_0 > 0 \\
& u \in [\overline{u}, 1]
\end{aligned}$$

A.5 The Base Model with $v = v(x, y)_{pext}$

$$\max_u \quad \int_0^\infty e^{-0.05t}\left(2y - 1.5\sqrt{2y(\frac{55}{16}x^3 - \frac{31}{12}x^2 - \frac{17}{48}x + \frac{1}{2})}\right)dt$$

$$\begin{aligned}
\dot{x} &= \sqrt{u}(1-x) - 0.2x \\
\dot{y} &= 1 - u - 2y(\frac{55}{16}x^3 - \frac{31}{12}x^2 - \frac{17}{48}x + \frac{1}{2}) \\
x(0) &= x_0 \in [0, 1) \\
y(0) &= y_0 > 0 \\
& u \in [\overline{u}, 1]
\end{aligned}$$

A.6 The Base Model with $v = v(x, y)_{dext}$

$$\max_u \quad \int_0^\infty e^{-0.05t}\left(2y - 1.5\sqrt{2y(\frac{-55}{16}x^3 + \frac{31}{12}x^2 + \frac{17}{48}x + \frac{5}{10})}\right)dt$$

$$\begin{aligned}
\dot{x} &= \sqrt{u}(1-x) - 0.2x \\
\dot{y} &= 1 - u - 2y(\frac{-55}{16}x^3 + \frac{31}{12}x^2 + \frac{17}{48}x + \frac{5}{10}) \\
x(0) &= x_0 \in [0, 1) \\
y(0) &= y_0 > 0 \\
& u \in [\overline{u}, 1]
\end{aligned}$$

Chapter B
Eigenvalues

	EP_1	EP_2	EP_3	EP_4	EP_5	EP_6
$h(x)_{aconv}$	-11.6749	0.1231 + 7.3186i	0.2532	1.1574 + 0.6799i		
	11.7249	0.1231 - 7.3186i	0.6503	1.1574 - 0.6799i		
	-1.1083	-1.0764	-0.6003	-0.9137		
	1.1583	0.9301	-0.2032	-1.3012		
saddle	✓	✓	✓	✓		
dim_{sm}	2	1	2	2		
$h(x)_{aconc}$	1.2299 + 0.6993i	0.0994 + 7.9125i	0.2532	-12.0440		
	1.2299 - 0.6993i	0.0994 - 7.9125i	0.6809	12.0940		
	-1.3977	-0.9660	-0.6309	-1.0273		
	-0.9621	0.8672	-0.2032	1.0773		
saddle	✓	✓	✓	✓		
dim_{sm}	2	1	2	2		
$h(x)_p$	0.0979 + 8.4474i	-3.1488	-12.6780	1.0863 + 0.4822i	0.0250 + 3.0670i	
	0.0979 - 8.4474i	3.1988	12.7280	1.0863 - 0.4822i	0.0250 - 3.0670i	
	-1.1696	-0.2000	-1.1732	-1.0363 + 0.2680i	-0.1999	
	1.0738	0.2500	1.2232	-1.0363 - 0.2680i	0.25	
saddle	✓	✓	✓	✓	✓	
dim_{sm}	1	2	2	2	1	
$h(x)_d$	-1.8077 + 0.1381i	0.0250 + 9.7407i	13.7783	-1.4630	0.0250 + 1.6856i	0.2532
	-1.8077 - 0.1381i	0.0250 - 9.7407i	-13.7954	-1.0489	0.0250-1.6856i	1.1110
	1.8577 + 0.1969i	-1.0945	-1.1095	1.0989	-1.7836	-1.0610
	1.8577 - 0.1969i	1.1445	1.2265	1.5130	1.8336	-0.2032
saddle	✓	✓	✓	✓	✓	✓
dim_{sm}	2	1	2	2	1	2

Table B.1: Eigenvalues for the Base Models

	EP_1	EP_2	EP_3	EP_4	EP_5	EP_6
$h(x)_{pext}$	0.9964	0.0487 +11.2785i	-2.6621	-15.0030	0.0244 + 2.4514i	
	0.8662	0.0487 -11.2785i	2.7121	15.0530	0.0244 - 2.4514i	
	-0.8813 + 0.4210i	1.1808	-0.1905	-1.1806	-0.1892	
	-0.8813 - 0.4210i	-1.1783	0.2405	1.2306	0.2405	
saddle	✓	✓	✓	✓	✓	
dim_{sm}	2	1	2	2	1	
$h(x)_{dext}$	0.0250+4.3379i	-1.6711+0.2278i	10.3502	-0.9883+0.7843i	1.7503	0.2532
	0.0250-4.3379i	-1.6711-0.2278i	-10.4661	-0.9883-0.7843i	0.0250+1.2839i	1.0623
	-0.7959	1.7211+0.3785i	-1.0084	1.0383+0.7843i	0.0250-1.2839i	-1.0123
	0.8459	1.7211-0.3785i	1.2244	1.0383-0.7843i	-1.7003	-0.2032
saddle	✓	✓	✓	✓	✓	✓
dim_{sm}	1	2	2	2	1	2

Table B.2: Eigenvalues for the Extended Models

List of Figures

List of Tables

Bibliography

[1] D. Grass, J.P. Caulkins, G. Feichtinger, G. Tragler and D.A. Behrens, *"Optimal Control of Nonlinear Processes - With Application in Drugs, Corruption and Terror"* Springer - Verlag Berlin Heidelberg 2008

[2] G. Feichtinger, R.F. Hartl, *"Optimale Kontrolle ökonomischer Prozesse - Anwendungen des Maximumsprinzips in den Wirtschaftswissenschaften"* Walter de Gruyter - Berlin - New York - 1986

[3] *"GEMEINSAMER STANDPUNKT 2008/586/GASP DES RATES vom 15. Juli 2008 zur Aktualisierung des Gemeinsamen Standpunkts 2001/931/GASP über die Anwendung besonderer Maßnahmen zur Bekämpfung des Terrorismus und zur Aufhebung des Gemeinsamen Standpunkts 2007/871/GASP"* - 16.07.2008

[4] C. Veilette *"CRS Report for Congress: Plan Colombia: A Progress Report"* 22.06.2005

[5] K. Hausken, J. Zhuang *"The Timing and Deterrence of Terrorist Attacks due to Exogenous Dynamics"* Journal of the Operational Research Society (forthcoming)

[6] K. Hausken, V.M. Bier *"Defending against multiple different attackers"* European Journal of Operational Research 211 (2011), 370-384

[7] S. Skaperdas *"Contest success functions"* Economic Theory 7 (1996), 283-290