ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Ecole Polytechnique Fédérale de Lausanne (EPFL)
School of Computer & Communication Sciences
Laboratory for computer Communications and Applications
(LCA1)

Master of Science Thesis

Revocation Games in Ephemeral Networks

by

Igor Bilogrevic
igor.bilogrevic@epfl.ch

Supervisors
Prof. Jean-Pierre Hubaux
Dr. Mohammad Hossein Manshaei
Dr. Maxim Raya

Lausanne, 2009

Abstract

An *ephemeral* network is usually defined by the very short-lived and heterogeneous nature of interactions among self-organizing wireless devices. The wide penetration in everyday gadgets of radio technologies operating in unlicensed frequency spectrum, such as Bluetooth or 802.11 WLANs, accentuates the risk involved in communicating with unknown nodes, especially in hostile environments. Thus, misbehavior in ephemeral networks poses a serious threat to both well-behaving nodes and the network itself. The lack of centralized infrastructure and control makes such networks vulnerable to abuses, resulting in local service degradations and interruptions. Due to the short-lived and heterogeneous contacts among nodes, the reputation mechanisms based on repeated interactions are hard to establish and thus local revocation schemes seem to better cope with the highly volatile network model. In this report, we present a fully distributed scheme for local revocation of public-key certificates using a game-theoretic approach, in which each node selfishly decides on its actions and where, for each action, there is an associated cost and benefit. By providing incentives, dynamic costs and thanks to the history of previous behavior, our payoff model establishes the best course of actions for all the involved devices on-the-fly, such that the resulting revocation generates the least cost for the collectivity of players, i.e. a successful revocation that is also socially optimal. Based on the analytical results, we then formally define such algorithm and evaluate its performance through simulations. We show that our scheme is both accurate and effective in quickly removing malicious devices from the network.

Acknowledgements

I would like to express my sincere gratitude to Mohammad Hossein Manshaei, Maxim Raya, Jean-Pierre Hubaux and Mathias Humbert for their precious contributions to this work. To M. H. Manshaei, who first introduced me to the *theory of games* and helped by providing excellent guidelines for the subsequent modeling of wireless networks based on that theory. To M. Raya, for contributing with valuable insights and feedback on this thesis from the beginning. To Jean-Pierre Hubaux, who helped adjusting the focus on the true problem of certificate revocations when the theoretical findings steered my attention away from the issue at stake. Finally, I would like to especially thank Mathias Humbert for his professional and friendly support throughout the months that resulted in the writing of this thesis.

Contents

Chapter 1

Introduction

In the last few years, the transition from wired to wireless mobile networks is a reality towards which both service providers and customers are migrating to. A recent study [17] shows that more than one-fourth of wireless customers in the U.S. have already abandoned the wired landline and are using exclusively wireless devices for their communication needs. The centrally-managed infrastructure owned by the service provider allows the end-users to benefit from a wide palette of services but, at the same time, limits their mobility and freedom of choice. Wireless capability, embedded in everyday devices, could be the *Panacea* to such constraints since it allows direct communication among different nodes, independently of the service provider, but the security concerns become even stronger. The dynamic network topology and frequent neighbor changes make it imperative to act both *proactively* and *reactively* with respect to potential malicious behavior [24]. In other words, an efficient defense against misbehavior in short-lived connections with potentially unknown partners has to encompass both detection and reaction mechanisms.

To date, public key certificates are typically created either by a trusted third party called *certification authority (CA)*, or by the node themselves in a distributed fashion, like in *PGP* [25]. The goal of such certificates is to allow the nodes to be able to uniquely identify and authenticate themselves and their messages while communicating. In fully open networks, where nodes are not subject to access controls by a third authority, distributed key management schemes have been studied and solutions have been proposed in [12, 3]. On the other hand, when globally verifiable public key certificates are needed prior to joining the network, the signature of the trusted CA on individual's public-key certificates is the best option. Therefore, such prerequisite makes the availability of valid certificates extremely important, especially when the mobility of the nodes imposes a sporadic contact with the issuing authority. As it is the case for ephemeral networks, a node without a valid certificate is completely denied participation, at least until the next time it connects with the accredited issuer.

Although a wireless device might not act selfishly or maliciously at first, there are circumstances in which this could not be true anymore. After some period of operation, the power management policies could for instance force a previously cooperative and well-behaving wireless node to suddenly become selfish. This could arise if the battery of the device starts to run out or, in the more adverse case, if another device gains control of the first one. The issue of node misbehavior detection is a central part of the *proactive* security aspect in mobile networks and has been addressed by various authors in [19, 14]. Thus, an efficient misbehavior detection mechanism is the *sine qua non* condition for a performing and clear-cut *reaction* system.

A solution to limit the abuses of efficient reaction schemes in presence of malicious nodes is achieved by the use of *reputation systems*, a set of techniques that considers the past behavior in order to determine the trustworthiness of a node [20]. Such reputations are usually built on the outcomes of repeated interactions and their value is stored either on a tamper-proof device on the node itself [13] or distributed to its neighbors [4]. Nevertheless, due to the very short-lived and heterogeneous nature of the contacts in ephemeral networks, such entries are hard to develop and maintain. Moreover, reputations are a natural means of disregarding misbehaving nodes but they can be redeemed. On the other hand, revocations are usually final.

In this report, we develop a local certificate revocation scheme for misbehaving nodes in ephemeral networks. By introducing the network participants as players in a game theoretic way, we are able to model their actions in a potentially hostile environment without having to assume any kind of cooperation among the different parties. The most commonly cited methods for revoking certificates in a multi-party environment are i) *vote* [22, 1] and ii) *suicide* [16]. We include both of them and we also add the possibility of *abstaining*, i.e. not taking any action but expecting others to perform the revocation. Moreover, we provide an efficient incentive to stimulate players to participate in the certificate revocation process through rewards. It is worth mentioning that the relationship between costs and benefits depends both on the kind of actions taken by the players and by the outcome of the revocation procedure. We then extend our model to include the past behavior and we establish conditions that guarantee a successful revocation of the misbehaving node's certificate. Since each device could potentially have a different past behavior, we determine the best course of actions for all the participants that will result in a successful revocation with a minimal cost, i.e. a unique outcome that is also socially optimal.

The rest of the report is organized as follows. In Chapter 2 we introduce the system model, the settings in which a public-key certificate revocation process takes place and we define the associated game theoretic framework that will be used throughout the report. We begin by an elementary model in which we only consider the costs associated with the certificate management for each node and then we establish the plausible outcomes represented by the Nash equilibria of the games. Chapter 3 is devoted to a more complex model of revocation games that includes both the rewards for the participating nodes and the history of their previous payoffs. By providing incentives for collaboration, we show that a successful revocation of a malicious node's certificate is guaranteed. Moreover, the incentive-based approach and the reputation-inspired variable costs allow us to refine even more the predictions of the outcome of such games. The introduction of two optimality concepts allows us to identify, in a distributed manner, a unique Nash equilibrium that is also socially optimal. Afterwards, in Chapter 4 we show through simulations that our unique optimal Nash equilibrium selection algorithms are both effective in removing the malicious node's certificate and with minimal message overhead. Finally, we give our concluding remarks in Chapter 5.

Related Work

Public-key management schemes for mobile wireless networks have been proposed in various forms. There are three main approaches: i) *fully distributed* key management, ii) *central-authority* management achieved when a trusted CA creates and revokes certificates and a iii) *combination* of the previous methods in which the CA issues the certificates but the nodes can revoke them independently.

The fully distributed approach has been studied by several authors. In [12] and similarly in [3], the certificates are generated, stored and distributed by the nodes, who maintain a local repository of the certificate that they already have. Prior to communicating, the nodes exchange their repositories and look for certificate chains in the merged data set. The main assumption is that nodes do not create false certificates for unknown peers if they believe that the keys do not belong to those peers. However, since the validation of other's certificates is based on individual beliefs, even a single misbehaving node could sign certificates for other such devices and thus the robustness of such scheme is still to be determined.

A trusted third party is required for the generation and revocation of public-key certificates in [19] and envisaged in [4]. Rather than completely revoking, the authors suggest a method to deal with misbehaving devices by disregarding their messages or by minimizing their trust level among the neighbors. In [19] an ignored certificate cannot be restored while in [4] the trust can be regained and the certificate renewal interval can be extended.

The combination of a trusted certificate issuer and distributed revocation ability is a topic that has been developed in [1, 18]. The former study revokes the malicious node's certificate based on a trust threshold value computed by taking into account the reputations of both the accused and accusing nodes through weighted accusations. If the sum of such weighted accusations is greater than a threshold value, the certificate is revoked and is completely useless for further interactions. In [18], the authors take a game-theoretic approach for certificate revocations in ephemeral networks by extending the possibility of revocation just by a single node's decision, in addition to the aggregate voting scheme. The interactions among the well-behaving nodes are visible to all of them since the game model is a dynamic complete information game. Since every revocation game is modeled as a cost game, without giving incentives for participation the revocation is achieved only by the last players of the game. An important problem with this solution is that some of the last nodes that should participate in the game might move out of communication range before its end and thus invalidate the revocation process.

In our work, we take a different approach than in [18]. First of all, we consider revocations in which nodes take actions simultaneously, i.e. they are unable to decrypt other's decisions before taking their own, since it might take too much time in practice and the nodes might have already lost contact. The participants do not know *a priori* the strategies of the others and they cannot wait for the last players simply because there is no notion of first or last players in simultaneous games. Second, by considering the past behavior of all the participants, we are able to allow for personalized costs, depending on the behavior of each node in past games. A node that has behaved correctly, i.e. no or little abuse of the revocations, is more motivated to take decisive actions against the misbehaving device since the price to pay would be lower than for a node that has not behaved well previously. In a sense, this reflects a reputation-like system. Finally, by designing a distributed on-the-fly Nash equilibrium computation algorithm that is also socially optimal, we are able to guarantee the unique most efficient outcome for the collectivity of the players.

A Note on Game Theory

The theory of games or *game theory* is defined as "the study of multiperson decision problems" [8] and it first appeared in the fields of economics and politics, two natural environments in which a formal tool for decision-making could be applied. The essence of game theory is that the participants (or *players*) of such processes can take different actions and the payoff (or *utility*) that each one of them obtains depends on the outcome of the *game*, his own action and the actions of other players [2]. In computer science, it first started to emerge as static wireless sensor networks (WSNs) began to spread and then it made its way in mobile ad hoc environments such as pervasive and ephemeral networks. In such settings, a multi-party decision could be taken, for instance, for determining the participants in message forwarding processes when there are multiple and redundant nodes or, as in this report, to determine the best course of action for each participant in a revocation scheme, in case a misbehaving node was positively detected.

Chapter 2

Revocations with Costs

Ephemeral networks are formed by autonomous mobile wireless devices with self-organizing capabilities, a very limited communication range and important power and bandwidth constraints. Clearly, such limitations impose that every interaction among neighboring nodes is carefully planned in order to maintain a sufficient level of throughput and overall performance. For instance, devices that are running out of battery could exhibit sometimes what is called a *selfish* behavior, i.e. they might refuse to communicate with neighboring nodes in order to save resources, or a *malicious* behavior by which they deliberately inject false information. In wireless ad hoc, ephemeral and pervasive networks these are crucial issues and methods to deal with such selfish nodes have been discussed in [14, 24, 21].

In this Chapter we deal with a similar challenge, namely the issue of removing nodes that exhibit some form of misbehavior in the network, such that the other devices in communication range are willing to sacrifice part of their *wealth* in order to remove it. The wealth in our case is the quantity of valid public-key certificates that each node has at its disposal at any given time. In the following sections, we define the system model and establish the rational outcomes of such revocation process through the game-theoretic concept of *Nash equilibrium*, defined in Section 2.3.1.

2.1 System Model

2.1.1 Network Model

The underlying network model in this report is that of an ephemeral and pervasive type, i.e. a network with short-duration (1-10 sec), short-range (10-100 m) and heterogeneous contacts among nodes who are likely to exchange (some) data spontaneously, even without previous knowledge of the other peers [15]. We allow the communication to take place both in licensed and unlicensed frequency bands as long as the wireless devices are able to establish a direct communication among themselves.

Furthermore, we assume that all devices are powerful enough to run public-key cryptographic algorithms. This assumption is based on the evidence that most of today's smartphones (and future cell phones [10]) have integrated public-key certificates for connecting to secure HTTPS servers on the Internet or to authenticate themselves on protected enterprise 802.11 WLAN networks. Moreover, we consider that a trusted third party (or parties) exist in such networks and that each mobile node is pre-loaded *public-key certificates* (or *pseudonyms*) signed by such CA. The certificate serial number serves as *unique ID* that distinguishes each device in a given revocation process. We explicitly state that each node has with more than one certificate in the initial deployment phase, supported by the trends to ensure the location privacy (by synchronized pseudonym changes) and avoid the possibility of being tracked and identified over time [11, 23]

After the initial deployment, we do not assume an always-on connection with the central authority anymore but we do assume that nodes will reconnect with the respective CA sporadically (from a few hours to a few days). During the successive reconnection, the CA will then be able to renew their credentials and verify their past behavior in an appropriate way. Since the description of the behavior verification process by the CA is outside the scope of this report, we do not develop it here. It is clear that the logistic costs associated with the certificate management (by the CA) and frequent pseudonym changes (by the nodes) could make the limited reserve of valid certificates a critical resource. In order to allow for integrity and authenticity checks, we assume that a node is able to send messages iff it can sign them with a valid certificate.

2.1.2 Opponent Model

The opponent considered in our setting could potentially be any device described in Section 2.1.1, i.e. a mobile wireless node with exactly the same characteristics as the other benign nodes. We allow the misbehavior to be both of selfish and malicious kind. An opponent could either be intentionally and systematically refusing to cooperate with other nodes (and thus behaving selfishly) or it could inject false information in the network and try to disrupt its correct operation (acting maliciously). For instance, by sending undesired advertisements or by hijacking other nodes with the intent to subvert them to its own advantage, a misbehaving node could be accused by its neighbors and a revocation process against it could be initiated.

2.1.3 Reaction Model

In our model, we assume that all nodes in the network have the necessary features to detect a potentially hostile or misbehaving node. In our work, we are concerned with the *reaction* of a set of nodes, once a misbehaving node has been identified, and the best course of action for the revocation of the its certificate revocation. Therefore, it is not our intent to develop a misbehavior *detection* system. References on the latter aspect can be found in [19, 14].

2.2 Game-Theoretic Model

This section delineates the game-theoretic model that we use throughout the rest of the report. The main reason for the interest in game theory for modeling the certificate revocation process is that it allows the nodes to independently and selfishly decide on the best action to take by knowing, however, that the "price to pay" for each individual decision depends on other nodes' decisions as well. In this first *cost* model, the "price to pay" is only the cost that is associated with the revocation decision. The unit in which we measure this cost is, not surprisingly, in *public-key certificates* since every sent message send contains the digital signature of its creator.

The cost that well-behaving nodes might face in order to revoke a malicious node might sometimes be even greater than the cost induced by the latter node. In this scenario, it might be more appropriate for the formers not to revoke the malicious device (e.g. when the bogus information does not preclude the network from functioning or is not judged to be very disturbing).

2.2.1 Players, Strategies and Payoffs

With the ideas presented in Section 2.2 we are now able to formally define what is called a *revocation game.* In order to characterize the game, we need to specify the set of *players* (the nodes involved in the revocation process), the set of *strategies* (the actions that each node can take) and the set of *payoffs* (in this chapter the payoffs correspond to the negative of the costs).

Players The set of wireless nodes $\mathcal{P} = \{P_i\}_{i=1}^{n}$ that are in communication range with both the accused node and the device that initiated the revocation process.

Strategies The set of strategies that can be taken by each node in a revocation process is $\mathcal{S} = \{S_i\}_{i=1}^{n}$. In our work, we define as $S_i = \{$*abstain, vote, self-sacrifice*$\}$ the set of possible strategies for each player i, where *abstain* means that the node does not take any action against the accused device but simply expects others to revoke it, *vote* stays for the voting action that would result in a successful revocation if and only if (iff) there is a sufficient number n_v of total voters, and finally *self-sacrifice* which stands for the ability of a player to commit suicide and at the same time to revoke the accused node. We stress here that since only one *sacrifice* strategy is sufficient to revoke the accused node's certificate, the cost of such strategy should be carefully determined in order to avoid abuses. We therefore devote Section 3.4 solely to the optimization of the self-sacrifice cost function.

Payoffs Since the costs associated with the revocation decisions depend both on the individual strategies and on the ultimate game outcome (*successful revocation* or *nothing*), each player gets an individual payoff $u_i = benefit - cost$. The set of the individual payoffs is $\mathcal{U} = \{u_i\}_{i=1}^{n}$ and, in the cost game here defined, the payoffs correspond to the negative of the costs associated with the revocation game (or $benefits = 0$). We note the presence of the *attack-induced cost* of the malicious node (in case it is not revoked by the other players) as c and we account for it through the parameter k in Table 2.1:

$$k = \begin{cases} 1, & \text{if successful revocation} \\ 0, & \text{if unsuccessful revocation} \end{cases} \tag{2.1}$$

The costs that correspond to the three strategies A ,V and S, are as follows:

(a) *Abstain*: if a player i decides not to take any action in a game and expects the other players to revoke the accused node, the cost for i in this case is 0.

(b) *Vote*: to cast a vote does imply a cost since this action can determine the revocation of the accused node and thus should not come for free, in order to avoid potential abuses of the revocation process by colluding misbehaving nodes. We define v as the cost of voting and we bound in by $[0, 1]$ since it seems reasonable to assume that it should not exceed the cost for a self-sacrifice, since only one of the latter is completely sufficient for the revocation whereas more than one vote is needed for the same outcome ($n_v > 1$ votes are needed for a successful revocation).

(c) *Self-sacrifice*: since the annulment of one's own certificate is sufficient to revoke the accused node's certificate as well, we define the cost for the self-sacrifice strategy to be 1 (one valid certificate).

2.3 Revocation Games with Costs

We model the revocation game G as a finite n-player static (simultaneous) game of complete information [7], where the static type reflects the simultaneous decision-making process in which the wireless nodes are forced to vote "at the same time",

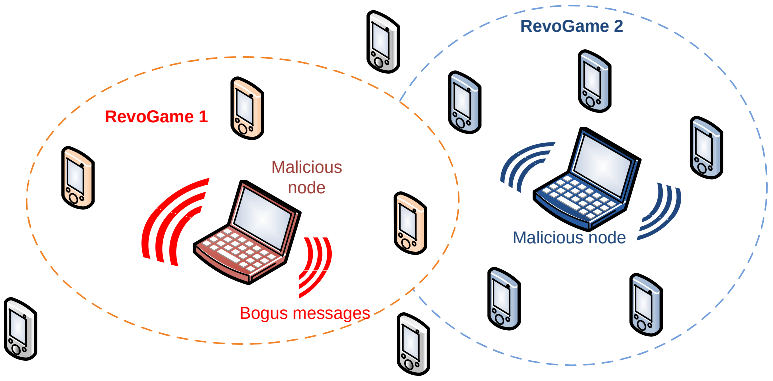


Figure 2.1: Pervasive network scenario in which two simultaneous revocation games (RevoGame 1 and RevoGame 2) are occurring against two malicious nodes. All players are under the same radio coverage area and, as we can see, each can participate to *at most one* game.

without having the possibility to overhear or to know the decision of the other nodes beforehand. The key concept here is that every node chooses his strategy in order to minimize its own costs. From the results of [18], we have seen that the sequential revocation process and the time needed for the decryption of the other nodes' decisions while still playing might cause an unpredictable game outcome due to some of the last nodes going out of communication range while still playing the game. We thus take the simultaneous approach such that the issue of sequential voting and on-the-fly decryption is not present.

The usual representation of a *static* game is in the *normal* (or *strategic*) form. The visually appealing representation for the *two-player* revocation game is shown in Table 2.2, where each row corresponds to one of the three possible strategies for player one and each column to a possible strategy for player two. In each cell we then have the payoffs that the first and second player get at the end of the game if they choose the corresponding strategy. In Table 2.2 for instance, if the game were to end by the *self-sacrifice* of player one and the *abstention* by player two (the (S, A) strategy profile), player one would incur in a cost of 1 (since he would lose one valid public-key certificate) and player two would not have to pay any cost since the malicious node would have been revoked by player one without any action taken by player two. Furthermore, we assume that for each accused node, there is one revocation game initiated by one of the neighboring nodes. If several nodes are accused, there could be as many independent revocation games in parallel, where each node can participate to at most one game at any given time (Figure 2.1). Without loss of generality, we provide the analysis for a single revocation game.

Definition 2.1. *A* revocation game *of complete information is expressed by* $G_n =$

	Abstain	***Self-sacrifice***	***Vote***
Cost	**(1-k) · c**	**1**	**v + (1-k) · c**

Table 2.1: Costs associated with the possible strategies. When the revocation is successful we have $k = 1$, otherwise $k = 0$.

$\{\mathcal{P}, \mathcal{S}, \mathcal{U}\}$, where $\mathcal{P}$ is the set of all the players $\mathcal{P} = \{P_i\}_{i=1}^{n}$, $\mathcal{S}$ is the strategy set and $\mathcal{U}$ is the payoff set. A strategy s_i of the strategy subset S_i is either Abstain, Vote *or* Self-sacrifice*, i.e. $s_i \in S_i = \{A, V, S\}$. The possible outcomes of the revocation game are either the* successful revocation *(k = 1) of the malicious node or* nothing *(k = 0). All players have the same complete knowledge about all parameters of the game.*

2.3.1 Solutions & Nash Equilibria of the Game

We introduce here the main concepts used for the analysis of the possible outcomes in revocation games. For a detailed analysis of other concepts of game theory one can look in [7, 8]. The most important idea for our work is that of a *Nash equilibrium*, which represent the most probable outcome in a game where all participants are rational and selfish, i.e. they play with the intent of maximizing their own payoff (or minimizing their cost). We define the Nash equilibrium as follows:

Definition 2.2. *In a n-player static game of complete information $G_n = \{\mathcal{P}, \mathcal{S}, \mathcal{U}\}$, a strategy profile $s^* = (s_1^*, s_2^*, \ldots, s_n^*)$ is a pure-strategy* Nash equilibrium *(NE) if the strategy s_i^* is such that*

$$u_i(s_1^*, \ldots, s_i^*, \ldots, s_n^*) \geq u_i(s_1^*, \ldots, s_i, \ldots, s_n^*), \quad \forall s_i \in S_i \tag{2.2}$$

In other words, the equilibrium strategy s_i^* solves

$$\max_{s_i \in S_i} u_i(s_1^*, \ldots, s_{i-1}^*, s_i, s_{i+1}^* \ldots, s_n^*) \quad \forall i \tag{2.3}$$

That is, no player i is better off deviating from his equilibrium strategy s_i^* given that the other players chose their respective s_{-i}^*.

A mixed-strategy *NE is analog to the pure strategy here defined, where instead of allowing only one possible strategy for each player we relax the condition and include the possibility to play any of the possible strategies with a finite probability. For instance, $s^* = (\sigma_1^*, \ldots, \sigma_n^*)$ is a mixed-strategy NE if the distribution $\sigma_i^* = (p_i^a, p_i^v, p_i^s)$, is such that*

$$u_i(\sigma_1^*, \ldots, \sigma_i^*, \ldots, \sigma_n^*) \geq u_i(\sigma_1^*, \ldots, \sigma_i, \ldots, \sigma_n^*), \quad \forall i, \forall \sigma_i \tag{2.4}$$

		Player 2		
		A	V	S
Player 1	A	(-c, -c)	(-c, -c-v)	(0, -1)
	V	(-c-v, -c)	(-v, -v)	(-v, -1)
	S	(-1, 0)	(-1, -v)	(-1, -1)

Table 2.2: 2-player cost game representation in the *normal* form.

where p_i^k *denotes the probability that player* i *plays strategy* k.

We see that by conforming to a strategy profile that is a NE, each node has no incentive to deviate from its strategy since even if it were given the opportunity to do so after the others have already played, the change would not bring him a better payoff

A concept related to the NE is that of the *best response* function, defined hereafter:

Definition 2.3. *A best response function for player* i *is a function* $br : s_{-i} \rightarrow s_i$ *such that it maximizes* i*'s expected payoff, given the strategies of other players* s_{-i}. *Formally, it is defined as*

$$br_i(s_{-i}) = \arg\max_{s_i \in \{A,V,S\}} u_i(s_i, s_{-i}), \qquad \forall i, \forall s_{-i} \tag{2.5}$$

We deduce that a strategy profile s^* is a NE iff it is the set of mutual best responses of all players of the game.

Another useful definition is provided by the *Pareto-optimal* NE which provides greater payoffs than any other NE, to all players. If, for instance, we have two NE profiles s^* and s^{**} with $u_i(s^*) \geq u_i(s^{**}), \forall i$ and strictly greater for at least one i, then s^* is a Pareto-optimal NE profile and thus it is the most appealing to all players since it gives greater payoffs to all of them.

2.3.2 2-Player Revocation Game

Before tackling the issue of a general finite n-player revocation game, we first focus on the different NE that arise in the 2-player game of Table 2.2 for different values of c and v, where the row player is *player 1*, the column player is *player 2* and the number of votes needed to revoke the malicious node is $n_v = 2$. This allows us to develop an intuition about the way the outcomes of the game are derived. For each of the following theorems, we give the relative proof by simply applying the definitions of Nash equilibrium and best response function.

Theorem 2.1. *For* $c < v < 1$, *the 2-player static game* G_2 *has one pure strategy Nash equilibrium* (A, A).

Proof. Since $-c > -v$ and $-c > -1$, (A, A) is the only pure strategy NE. □

Theorem 2.2. *For $v < c < 1$, the 2-player static game G_2 has two pure strategy NE (A, A) and (V, V) and one mixed strategy NE (σ_1, σ_2), where $\sigma_1 = \sigma_2 = (p_i^a, p_i^v, p_i^s) = (\frac{1-v}{c}, \frac{v}{c}, 0)$. Moreover, (V, V) is Pareto-optimal with respect to (A, A).*

Proof. For the pure strategies NE, since $-c > -v$ but $-c < -v$ we have that (A, A) and (V, V) are the pure strategy NE. By inspection we see that the payoffs corresponding to the strategy (V, V) are Pareto-optimal with respect to (A, A). In the mixed strategy NE, let p_i^k denote the probability that player i plays strategy k and $\sigma_i = (p_i^a, p_i^v, p_i^s)$. For player i to be indifferent between the three strategies *abstain*, *vote* and *self-sacrifice* we need that $u_i(A, \sigma_{-i}) = u_i(V, \sigma_{-i}) = u_i(S, \sigma_{-i})$, for $i = 1, 2$. Given that

$$\begin{cases} u_i(A, \sigma_{-i}) = -c(p_{-i}^a + p_{-i}^v) \\ u_i(V, \sigma_{-i}) = -v(p_{-i}^v + p_{-i}^s) - (v + c)p_{-i}^a \\ u_i(S, \sigma_{-i}) = -1 \\ p_{-i}^a + p_{-i}^v + p_{-i}^s = 1 \end{cases}$$

we obtain the probabilities for player $-i$'s strategies σ_2

$$\begin{cases} p_2^a = \frac{1-v}{c}, \qquad p_2^v = \frac{v}{c}, \qquad p_2^s = 1 - \frac{1}{c} \rightarrow 0 \end{cases}$$

Since the 2-player static game G_2 is symmetric, the same probabilities apply to both player 1 and 2, hence $\sigma_1 = \sigma_2 = (\min(1, \frac{1-v}{c}), \frac{v}{c}, 0)$. Thus, the mixed strategy NE is (σ_1, σ_2). □

Given the pure strategy NE of Theorem 2.2, we can represent the best response functions for player *one* and player *two* as in Figure 2.2. We see that whenever $p_i^a > (1 - v)/c$, the best response for player j is to *abstain* (or $p_j^a = 1$) and, since $p_j^s = 0$, to *vote* otherwise (or $p_j^a = 0$). Seen from a different perspective, when c diminishes, p_i^a grows and the mixed strategy NE approaches the pure strategy (A,A). As a result, the most probable NE would be (A,A) since the cost of the malicious node still remaining in the system is lower.

Theorem 2.3. *For $v < 1 < c$, the 2-player static game G_2 has three pure strategy NE (S, A), (A, S), (V, V) and one mixed strategy NE (σ_1, σ_2) where $\sigma_1 = \sigma_2 = (p_i^a, p_i^v, p_i^s) = (\frac{1-v}{c}, \frac{v}{c}, 1 - \frac{1}{c})$ where p_i^k denotes the probability that player i plays strategy k.*

Proof. For the pure strategies NE, since $v < 1$ and $c > 1$ we have that (S, A), (A, S) and (V, V) are the NE. In the mixed strategy NE, we refer to the proof of Theorem 2.2 and we conclude that (σ_1, σ_2) is the NE with

$$\begin{cases} p_2^a = \frac{1-v}{c}, \qquad p_2^v = \frac{v}{c}, \qquad p_2^s = 1 - \frac{1}{c} \end{cases}$$

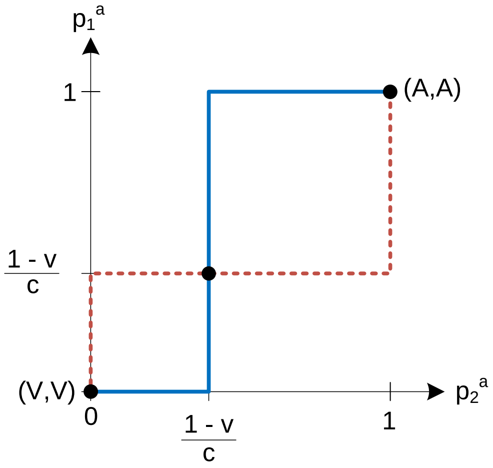


Figure 2.2: Best response strategies for the 2-player revocation game with fixed costs, where the continuous line represents the best response function of player *one* and the dashed line the best response function of player *two*. The NE are at the intersections between the two best response functions.

□

2.3.3 n-player Revocation Game

In the previous subsection we showed that the 2-player static game has one or more pure strategy Nash equilibria for each combination of the cost parameters. In this section we extend the revocation game to a finite number n of players, assuming the same possible strategies and costs for each player as in Table 2.1.

By definition, the costs of each player depend on the outcome of the game (successful revocation or no revocation), which, in return, depends directly on the strategies chosen by all the players. With this in mind, let G_n define the n-player static revocation game from Section 2.2, where the strategy of each player is either *abstain*, *vote* or *self-sacrifice*.

From 2- to 3-player Static Game

In order to better understand the dynamics of the game, let us consider briefly the 3-player revocation game G_3 and its NE, assuming that the revocation occurs by at least one self-sacrifice or by the majority voting rule (= 2 here). The *normal* form representation of such game is given in Table 2.3, where player 1 chooses the row, player 2 the column and player 3 the matrix.

The pure strategy Nash equilibria of the 3-player revocation game with fixed costs are as follows:

	A	V	S
A	(-c, -c, -c)	(-c, -v-c, -c)	(0, -1, 0)
V	(-c-v, -c, -c)	(-v, -v, 0)	(-v, -1, 0)
S	(-1, 0, 0)	(-1, -v, 0)	(-1, -1, 0)

	A	V	S
A	(-c, -c, -c-v)	(0, -v, -v)	(0, -1, -v)
V	(-v, 0, -v)	(-v, -v, -v)	(-v, -1, -v)
S	(-1, 0, -v)	(-1, -v, -v)	(-1, -1, -v)

	A	V	S
A	(0, 0, -1)	(0, -v, -1)	(0, -1, -1)
V	(-v, 0, -1)	(-v, -v, -1)	(-v, -1, -1)
S	(-1, 0, -1)	(-1, -v, -1)	(-1, -1, -1)

Table 2.3: 3-player cost game representation in normal form.

- $c < v < 1$. The unique pure strategy NE is (A, A, A), i.e. all players abstain.

- $v < c < 1$. NE are (A, A, A), (V, V, A), (V, A, V) and (A, V, V). By inspection we can see that (A, A, A) is Pareto-suboptimal and thus we can consider only the strategies that result in the revocation of the malicious node by majority voting.

- $v < 1 < c$. NE are all combinations of strategies consisting of *one self-sacrifice* and *two abstentions* or *two votes* and *one abstention*. Any of these combinations results in the malicious node being revoked.

The proof of these NE is similar to the ones shown in Section 2.3.1. For brevity, we leave them to the interested reader.

Finite n-player Static Game

In order to extend the number of players from 3 to n, let n_v define the number of votes needed for the revocation as

$$n_v = \lfloor \frac{n}{2} \rfloor + 1 \tag{2.6}$$

In this case, the strict majority of the players is needed in order to revoke a node. We now show the existence of the following pure strategy NE in the n-player static revocation game $G_n = \{\mathcal{P}, \mathcal{S}, \mathcal{U}\}$.

Theorem 2.4. *For $c < v < 1$, the n-player static game G_n has a unique pure strategy NE profile $(A, A, \ldots, A)$.*

Proof. The payoffs corresponding to the strategy profile $s^* = (s_1^*, \ldots, s_i^*, \ldots, s_n^*)$ are $u = (-c, -c, \ldots, -c)$, i.e. each player pays the cost of the malicious node still remaining in the system after the game ends. We focus on player i, where $s_i^* = A$ and $u_i(s_1^*, \ldots, s_i^*, \ldots, s_n^*) = -c$. In order for $s_i^* = A$ to be his best response strategy, given the other player's strategies $(s_1^*, \ldots, s_{i-1}^*, s_{i+1}^*, \ldots, s_n^*)$, we require that $u_i(s_1^*, \ldots, s_i^*, \ldots, s_n^*) \geq u_i(s_1^*, \ldots, s_i, \ldots, s_n^*)$, for all $s_i \in S_i$. The payoffs are as follows:

$$u_i(s_1^*, \dots, A, \dots, s_n^*) = -c \tag{2.7}$$
$$u_i(s_1^*, \dots, V, \dots, s_n^*) = -c - v \tag{2.8}$$
$$u_i(s_1^*, \dots, S, \dots, s_n^*) = -1 \tag{2.9}$$

As it can be seen, the highest payoff for player i is given for the strategy $s_i^* = A$.

Since the payoffs of all the n players are the same as for player i, it follows that for all players i, $s^* = (s_1^*, \dots, s_i^*, \dots, s_n^*) = (A, \dots, A)$ is the unique pure strategy NE of this game. □

Theorem 2.5. *For $v < c < 1$, the n-player static game G_n has pure strategy NE that are all strategy profiles s^* that include (a) n_v votes with $n - n_v$ abstentions and (b) all abstentions.*

Proof. We will first concentrate on part (a) and then we will prove part (b). We assume that, given the s_{-i}^* strategies of the other players, s_i^* could either be A or V for each player i, depending on whether he is one of the n_v voters or $n - n_v$ abstainers in the sequence under consideration. Therefore, we have two cases for all player i:

$$\text{if } s_i^* = A : u_i(s_1^*, \dots, s_i^*, \dots, s_n^*) = 0 \qquad \text{if } s_i^* = V : u_i(s_1^*, \dots, s_i^*, \dots, s_n^*) = -v \tag{2.10}$$
$$u_i(s_1^*, \dots, V, \dots, s_n^*) = -v \qquad u_i(s_1^*, \dots, A, \dots, s_n^*) = -c \tag{2.11}$$
$$u_i(s_1^*, \dots, S, \dots, s_n^*) = -1 \qquad u_i(s_1^*, \dots, S, \dots, s_n^*) = -1 \tag{2.12}$$

We see that, for all player i, any strategy $s_i \neq s_i^*$ results in a lower payoff for him. Thus, no player has an incentive to deviate from his equilibrium strategy and therefore any strategy profile s^* that is a combination of n_v votes and $n - n_v$ abstentions is a NE.

For part (b) of the theorem, we already know that $u(A, \dots, A) = (-c, \dots, -c)$ and thus any deviation from that strategy would result in a lower payoff for the deviating player and therefore our result. □

Theorem 2.6. *For $v < 1 < c$, the n-player static game G_n has pure strategy NE that are all strategy profiles s^* that include (a) one self-sacrifice with $n - 1$ abstentions and (b) n_v votes and $n - n_v$ abstentions. The malicious node is revoked by any of the NE.*

Proof. For part (a) we assume that, given the s_{-i}^* strategies of the other players, s_i^* could either be S or A for each player i, depending on whether he is *the* self-sacrificer or one of the $n-1$ abstainers in the sequence under consideration. Therefore, we have two cases for all player i:

$$\text{if } s_i^* = S : u_i(s_1^*, \ldots, s_i^*, \ldots, s_n^*) = -1 \qquad \text{if } s_i^* = A : u_i(s_1^*, \ldots, s_i^*, \ldots, s_n^*) = 0 \tag{2.13}$$

$$u_i(s_1^*, \ldots, A, \ldots, s_n^*) = -c \qquad u_i(s_1^*, \ldots, S, \ldots, s_n^*) = -1 \tag{2.14}$$

$$u_i(s_1^*, \ldots, V, \ldots, s_n^*) = -c - v \qquad u_i(s_1^*, \ldots, V, \ldots, s_n^*) = -v \tag{2.15}$$

We see that, for all player i, any strategy $s_i \neq s_i^*$ results in a lower payoff for him. Thus, no player has an incentive to deviate from his equilibrium strategy and therefore any strategy profile s^* that includes *one* self-sacrifice and $n-1$ abstentions is a NE.

For part (b), we refer to Theorem 2.5, where it can be seen that, for $v < 1 < c$, a strategy profile s^* that is a combination of n_v votes and $n - n_v$ abstentions is a NE. □

2.4 Summary

In this Chapter we have introduced our revocation games with fixed costs and explained what are the conditions in which such revocation takes place. Thanks to the game-theoretic concepts of *Nash equilibrium* and *best response function*, we have been able to analyze the outcomes and predict the actions taken by each player in our cost-only model.

The rational outcomes of the game, the NE, have shown that the revocation of the malicious node is not always guaranteed, even with the plausible assumption that $v < c < 1$, since the strategy profile (A,...,A) was a NE just as well as the other equilibria that resulted in the successful revocation of the malicious node's public-key certificate. Interesting also was the fact that, in the equilibria with successful revocation, we didn't find any costly action, i.e. vote or self-sacrifice, in excess than what was strictly needed. In other words, in the vote-only NE, we didn't find more than n_v votes (strictly needed for the revocation) nor more than 1 self-sacrifice. This favorable feature that limited the unnecessary waste of valid certificates also brought a less desirable aspect of such NE: for almost all combinations of v and c we had *more* than one NE. This means that in order for the game to end in a unique way, predictable by all the players, we would need a mechanism that specifies exactly which one of the possible NE to choose. Clearly, each selfish player would want that unique NE to be the one that favors him the most, but this would create a situation in which a unique NE across all the players would be impossible to establish.

Chapter 3

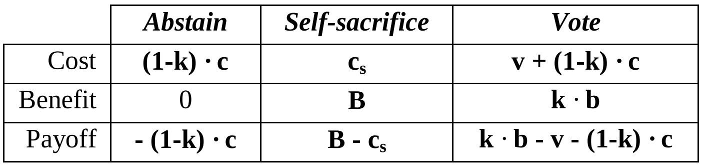
Revocations with Payoffs, Past Behavior & Social Welfare

In [18] the authors developed a cost model for the dynamic revocation games of complete information with n players. In order to include the possibility of the players not knowing beforehand the strategies adopted by other players, we then extended this initial model to the n-player static games of complete information in Chapter 2 of this report, where players chose their actions simultaneously. At the same time, we have established the Nash equilibria and drawn different conclusions.

Although interesting, the cost model is unable to capture an important aspect of a different version of the same game: the $benefits$ that players who are actively* participating in the revocation game could receive in case the malicious node is effectively and correctly revoked from the system. These rewards could serve as incentives to motivate the players to actively participate towards the revocation and could be decisive when multiple outcomes are possible.

In this Chapter, we develop a payoff model of the revocation game in which actively participating players receive a fixed benefit from the central authority to compensate for their costs when the revocation of the malicious node is successful. Next, we include the history of previous payoffs in the model and analyze the behavior of the players in a scenario where the cost of self-sacrificing is variable. The reason behind such choice is that we would like to have a model in which players with a high reserve are more willing to sacrifice themselves, since the cost of such action does not preclude their ability to continue operating in the network and leaves the others with sufficient certificates. Moreover, we define a way to coordinate on a unique socially optimal NE in case more than one NE are present

*By actively we mean players that either *vote* or *self-sacrifice*



	Abstain	***Self-sacrifice***	***Vote***
Cost	**(1-k) · c**	**c_s**	**v + (1-k) · c**
Benefit	0	**B**	**k · b**
Payoff	**- (1-k) · c**	**B - c_s**	**k · b - v - (1-k) · c**

Table 3.1: Payoffs associated with the possible strategies where $c_s = 1$ in the fixed costs model. If the revocation of the malicious node's certificate is successful we have $k = 1$, otherwise $k = 0$.

in the game and we design the algorithm that realizes that idea.

The rest of the Chapter is organized as follows. In Section 3.1 we present the general game model and in Section 3.2 we describe the payoff model of the n-player static revocation game with fixed costs, by looking at the respective NE for different combination of benefit and cost parameters. Section 3.3 is devoted to the static revocation games with previous payoffs and variable self-sacrificing cost, with some examples of possible scenarios and the respective NE. In Section 3.4 we optimize the parameters used by the variable self-sacrifice cost function and in Section 3.5.1 we present and implement a mechanism to select a unique socially optimal NE. After a brief description of the complexity of our payoff model in Section 3.6, we summarize the main results of this Chapter in Section 3.7.

3.1 Game-Theoretic Model

Let us define the revocation game with payoffs as $G_n^p = \{\mathcal{P}, \mathcal{S}, \mathcal{U}\}$, where $\mathcal{P}$ is the set of all the players $\mathcal{P} = \{P_i\}_{i=1}^n$, $\mathcal{S}$ is the strategy set and $\mathcal{U}$ is the payoff set. As usual, a strategy s_i of the strategy subset S_i is either *Abstain, Vote* or *Self-sacrifice*, i.e. $s_i \in S_i = \{A, V, S\}$. The possible outcomes of the game are either (a) *successful revocation* (k = 1) of a public key certificate of the malicious node or (b) *nothing* (k = 0). The costs and *benefits* associated with each of the possible actions depend on the outcome of the game and are summarized in Table 3.1. For instance, in the fixed cost model the cost of voting is $v \in [0, 1]$, the cost of self-sacrificing is $c_s = 1$ and the cost of the malicious node remaining in the system after the game ends is $c \in [0, 1]$.

3.2 Revocation Games with Payoffs & Fixed Costs

We describe here the payoff model of the revocation game, where costs and benefits for each of the possible actions are fixed for all players. Like we did in

S_3 = A

	A	**V**	**S**
A	(- c, - c, - c)	(- c, -v – c, - c)	(0, B – 1, 0)
V	(- v - c, - c, - c)	(b - v, b – v, 0)	(b - v, B – 1, 0)
S	(B - 1, 0, 0)	(B - 1, b – v, 0)	(B - 1, B – 1, 0)

S_3 = V

	A	**V**	**S**
A	(- c, - c, - c - v)	(- c, - c, - c - v)	(- c, - c, - c - v)
V	(b - v, 0, b - v)	(b - v, 0, b - v)	(b - v, 0, b - v)
S	(B - 1, 0, b - v)	(B - 1, 0, b - v)	(B - 1, 0, b - v)

S_3 = S

	A	**V**	**S**
A	(0, 0, B - 1)	(0, 0, B - 1)	(0, 0, B - 1)
V	(b - v, 0, B - 1)	(b - v, 0, B - 1)	(b - v, 0, B - 1)
S	(B - 1, 0, B - 1)	(B - 1, 0, B - 1)	(B - 1, 0, B - 1)

Table 3.2: Payoffs for the 3-player revocation game with fixed costs, where two votes (majority) are needed for the revocation of the malicious node. S_3 refers to the current strategy adopted by player three.

the previous Chapter for the cost model, we start by delineating the NE in the 3-player game and then we generalize to the n-player static revocation game of complete information.

3.2.1 3-player Game

The strategic representation of 3-player revocation game with payoffs G_3^p is shown in Table 3.2, where player *one* chooses rows, player *two* chooses columns and player *three* chooses matrices. The pure strategy Nash equilibria in such game depend on the relationship between the benefits and costs and, by inspection, they are:

- For $B = 1 \wedge b > v$. The unique pure strategy NE is the strategy profile is (V,V,V).

- For $B = 1 \wedge b < v$. The pure strategy NE profiles involve at least one self-sacrifice and abstentions for the other players.

- For $(B < 1 \wedge b < v) \wedge (B - 1 > b - v > -c)$. The pure strategy NE involve exactly one self-sacrifice and two abstentions.

- For $(B < 1 \wedge b < v) \wedge (b - v > B - 1 > -c)$. The pure strategy NE involve combinations of (a) one self-sacrifice with two abstentions and (b) two votes with one abstention.

It can be noticed that, except for the first case, there are multiple pure strategy NE and *no* possible Pareto-optimal strategy profiles that could reduce the plausible choices of the players. Since the players choose their actions simultaneously, this could be an issue because they should then agree to play exactly one particular NE in a given game. Considering the fact that we do not assume any kind of coordination between the players, there could be a scenario in which two players choose a NE strategy s_1^* but the third player chooses a different NE s_2^*, yielding a suboptimal payoff for all parties.

In order to mitigate the effects of the lack of coordination, players could choose a NE strategy profile s^* that yields the biggest individual expected payoff when there is increasing uncertainty about the actions of other players. If there are several NE profiles that give the same payoffs and, among those, there is one for which all individual payoffs u_i are independent on the coordination with other players, then all players should converge to that particular NE, which then becomes the *risk-dominant* NE.

In the 3-player revocation game G_3^p described in Table 3.2, there are several NE depending on the benefit parameters combinations. Among these NE, however, it appears that there are no risk-dominant strategies. If we consider the case $(B < 1 \wedge b < v) \wedge (B - 1 > b - v > -c)$, we see that it is impossible to say whether one NE is less risky than the other two without additional information about the players and their behavior. Therefore, we leave the investigation of risk-dominant NE for future analysis. We provide, however, a selection algorithm based on social welfare in Section 3.5.1.

3.2.2 n-player Game

We are now able to perform the Nash equilibria analysis in the finite n-player static revocation game with payoffs G_n^p. As usual, we prove the following NE by showing that each player i has no incentive to deviate from his best response strategy s_i^*, provided that the others conform to their own.

In order to extend the number of players from 3 to n, let n_v define the number of votes needed for the revocation as the majority of players, i.e. $n_v = \lfloor n/2 \rfloor + 1$. We note that n_v could also be determined dynamically based on the game parameters. Due to lack of time, we intend to explore that possibility in a future work.

Theorem 3.1. *For $(B = 1) \wedge (b > v)$, the n-player static game G_n^p has a unique pure strategy NE profile $s^* = (V, V, \dots, V)$, i.e.all players vote. The outcome of the game is the revocation of the malicious node.*

Proof. In G_n^p the payoffs corresponding to the strategy profile $s^* = (V, V, \dots, V)$ are $u = (b - v, \dots, b - v)$, i.e. they are the benefit minus the cost of voting for all the n players. By looking at any player i, we see that $s_i = V$ indeed solves the maximization problem described in the definition (2.2), i.e. the NE. Formally, we have

$$s_i = A \qquad u_i(V, \ldots, A, V, \ldots, V) = 0 \tag{3.1}$$

$$s_i^* = V \qquad u_i(V, \ldots, V, \ldots, V) = b - v \tag{3.2}$$

$$s_i = S \qquad u_i(V, \ldots, S, V, \ldots, V) = B - 1 \tag{3.3}$$

and therefore we see that for any $s_i \neq s_i^* = V$, the payoff u_i is strictly smaller than if $s_i = s_i^*$, for all players i. Thus, the strategy profile $s^*(V, \ldots, V)$ is the unique pure strategy NE. □

Theorem 3.2. *For $(B = 1) \wedge (b < v)$, the n-player static game G_n^p has pure strategy NE that are all strategy profiles s^* that include at least one self-sacrifice and all others abstain. The outcome of the game is the revocation of the malicious node.*

Proof. For the proof, we start by looking at the case where there is *only* one self-sacrifice and $n-1$ abstentions. In this case, the payoffs are $u = (B - 1, 0, \ldots, 0) = (0, \ldots, 0)$, where the self-sacrificing player could be any of the n players. Assuming that all players other than i choose their s_{-i}^*, we have that s_i^* could be either S or A, depending on the sequence under consideration. The payoffs are

$$\text{if } s_i^* = S : u_i(A, \ldots, s_i^*, A, \ldots, A) = 0 \tag{3.4}$$

$$u_i(A, \ldots, A, \ldots, A) = -c \tag{3.5}$$

$$u_i(A, \ldots, V, A, \ldots, A) = -v - c \tag{3.6}$$

$$\text{if } s_i^* = A : u_i(s_1^*, \ldots, s_i^*, \ldots, s_n^*) = 0 \tag{3.7}$$

$$u_i(s_1^*, \ldots, V, s_{i+1}^*, \ldots, s_n^*) = b - v \tag{3.8}$$

$$S, s_{i+1}^*, \ldots, s_n^*) = 0 \tag{3.9}$$

We see that if player i is the only sacrificing participant, he has no incentive to deviate from this strategy and if, on the other hand, he is one of the $n-1$ abstainers, his payoffs are equivalent ($= 0$) for both self-sacrificing and abstaining. By symmetry of the payoffs, any strategy profile s^* that includes at least one self-sacrifice and all other abstentions is a NE. □

Theorem 3.3. *For $[(B < 1 \wedge b < v)] \wedge [(B - 1 > b - v > -c)]$, the n-player static game G_n^p has pure strategy NE that are all strategy profiles s^* that include exactly one self-sacrifice and $n-1$ abstentions. The outcome of the game is the revocation of the malicious node.*

Proof. In this proof, we choose one strategy profile $s^* = (s_1^*, \ldots, s_n^*)$ that we claim is a pure strategy NE and then, by symmetry of the payoffs, we extend it to any such profile as long as it has *exactly* one self-sacrifice and $n-1$ abstentions. First, consider the strategy profile $s^* = (S, A, \dots, A)$. We see that $s_1^* = S$ and $s_j^* = A$, $\forall j \in [2, \dots, n]$. We now consider all possible strategies for player one, given the other $n-1$ strategies, and all possible strategies for a player j, given the other $n-1$ strategies.

$$\text{For } s_1^* = S : u_1(s_1^*, A, \dots, A) = B - 1 \tag{3.10}$$

$$u_1(A, \dots, A) = -c \tag{3.11}$$

$$u_1(V, A \dots, A,) = -v - c \tag{3.12}$$

$$\text{For } s_j^* = A : u_j(S, A, \dots, s_j^*, \dots, A) = 0 \tag{3.13}$$

$$u_j(S, A, \dots, V, \dots, A) = b - v \tag{3.14}$$

$$u_j(S, A, \dots, S, \dots, A) = B - 1 \tag{3.15}$$

As it can be seen, no player i wants to choose a strategy $s_i \neq s_i^*$, since this would not give him a higher payoff. Thus, due to the symmetry of the payoffs for all players, any strategy profile s^* that has *exactly* one self-sacrifice and $n-1$ abstentions is a pure strategy NE. □

Theorem 3.4. *For $[(B < 1) \wedge (b < v)] \wedge [(b - v > B - 1 > -c)]$, the n-player static game G_n^p has pure strategy NE that are all strategy profiles s^* that include (a) one self-sacrifice with $n-1$ abstentions and (b) n_v votes with $n - n_v$ abstentions. The outcome of the game is the revocation of the malicious node.*

Proof. For part (a) of the theorem, the proof is analog to the one of Theorem 3.3 and thus we will concentrate on part (b) here. In this sense, let us choose the strategy profile $s^* = (V, \dots, V, A, \dots, A)$ that has n_v voters and $n - n_v$ abstainers. The payoffs that correspond to s^* are $u = (b - v, \dots, b - v, 0, \dots, 0)$, where the first group $(b - v)$ belongs to the n_v voters and the second group (0) to the $n - n_v$ abstainers. We now distinguish between two sets of players in s^*: g_v is the set of the n_v players that voted and g_a is the set of the $n - n_v$ players that abstained. A further assumption is that player i belongs to g_v and player j to g_a. We are now able to solve the maximization problem of equation (2.5) for all players i and j.

$$\text{if } s_i^* = V : \quad u_i(V, \dots, s_i^*, A, \dots, A) = b - v \tag{3.16}$$

$$u_i(V, \dots, A, A, \dots, A) = -c \tag{3.17}$$

$$u_i(V, \dots, S, A, \dots, A) = B - 1 \tag{3.18}$$

$$\text{if } s_j^* = A : \quad u_j(V, \dots, V, s_j^*, \dots, A) = 0 \tag{3.19}$$

$$u_j(V, \dots, V, V, A \dots, A) = b - v \tag{3.20}$$

$$u_j(V, \dots, V, S, A, \dots, A) = B - 1 \tag{3.21}$$

We see that, for any player i of the g_v set, his best response strategy is to vote, given that the other players conform to their own best responses. The same argument holds for any player j of the g_a set, since he is better off abstaining than by choosing any other strategy, i.e. $s_j^* = A$. Therefore, due to the symmetry of the payoffs, all strategy profiles that include (a) *one* suicide with $n-1$ abstentions and (b) n_v votes with $n - n_v$ abstentions are NE. □

3.2.3 Considerations on the Payoff Model with Fixed Costs

The theorems shown so far for the payoff model of the n-player static revocation game depend on the relationship between benefit and cost parameters. The main consequence of the addition of benefits in case of a successful revocation is that the malicious node is always revoked at the equilibria, as opposed to the cost model in which the revocation of the malicious node was not guaranteed for the case where $c < v < 1$.

The other important facts that emerge from the consideration of the payoff model with no previous history are the following:

- If benefits are equal to the costs, any strategy that revokes the malicious node is a NE. In the case where the majority voting rule applies, it means that any strategy that has at least n_v votes or at least *one* self-sacrifice is a NE.
- If benefits for voting are greater than the respective costs ($B = 1 \wedge b > v$), the NE is unique and it consists of the *all-vote* strategy.
- If benefits for voting are smaller than the respective costs ($B = 1 \wedge b < v$), any strategy that revokes the malicious node by at least *one* self-sacrifice and all other abstentions is a NE.

3.3 Adaptive Revocation Games with History

In the previous Section, we analyzed the payoff model of the static revocation game of complete information G_n^p and we found the relative pure strategy NE. This model was only based on the current game and the payoff functions did not include the history of the previous payoffs, i.e. the number of keys that each player had before he started the current game. Yet another character that was missing in the first payoff model is the idea of a variable cost of self-sacrificing. There could be a situation in which a node has to choose a strategy but it has very few keys left. In such scenario, the cost of self-sacrificing should be greater than the cost of the same strategy when the node has still many keys left since in the former case the risk of remaining without any valid certificate would be greater than in the latter case.

We now extend the initial payoff model of Section 3.2 to include the history of the previous payoffs and the variable self-sacrifice cost.

3.3.1 Previous Payoffs

Let u_i^- define the number of keys that each node has prior to entering the game. We define the new payoff function u_i with previous payoffs as

$$u_i = u_i^- + \text{benefit} - \text{cost} \tag{3.22}$$

and we refer to it hereafter as "payoffs with history".

In a nutshell, the new payoff function is identical to the one defined in Table 3.1 but with the addition of the previous payoffs u_i^- for all players. As it can be noticed, the NE defined in Section 3.2 *do not change* for the payoffs with history. Since u_i^- is a player specific constant value, each player's best response function is not affected. By consequence, we will not discuss the NE of the n-player static revocation game any further as they have been already shown in Section 3.2.

3.3.2 Variable Cost for Self-sacrifice

Up to now, we have considered only fixed costs and benefits for all players. Without the notion of the history of previous payoffs u_i^-, we have focused on the pure strategy NE for different combination and relationship between cost and benefit parameters. The payoffs with history as defined by equation 3.22 allow us to consider the idea that the cost of self-sacrificing should somehow depend on the reserve of keys that each player has left, i.e. it should depend on u_i^-. It appears reasonable to assume that when u_i^- is high, player i probably participated correctly in previous games, i.e. no or little abuse of voting of self-sacrifice against benign players. Thus, he should not be charged too much for self-sacrifice. On the other hand, if u_i^- is low then self-sacrificing should be used with extreme precaution because once the last keys are depleted, the node would not be able to operate until the next time it establishes contact with the central authority. Hence, the greater cost would penalize and quickly remove malicious nodes from the system as well as limit its abuses.

To reformulate this idea into operational terms, we first define the variable cost of self-sacrificing as $c_{s,i}$ and then we consider several functions of u_i^- that could be appropriate to model it. In Figure 3.3.2 we plotted three functions:

(a) $c_{s,i} = 1/u_i^-$. The cost $c_{s,i}$ is inversely proportional to the reserve u_i^-. For low or high u_i^- the cost is very different. When $u_i^- = 1 \rightarrow c_{s,i} = 1$, a self-sacrifice would mean a complete temporary exclusion of node i from the system.

(b) $c_{s,i} = \max(h - g \cdot u_i^-, 0)$. The cost decreases linearly with the reserve with a slope of $-g$.

(c) $c_{s,i} = \max(h - a \cdot (u_i^-)^2, 0)$. The cost decreases like the negative square function of the reserve, meaning that $c_{s,i}$ is relatively high for an initial range of values u_i^- and then decreases rapidly for greater u_i^-.

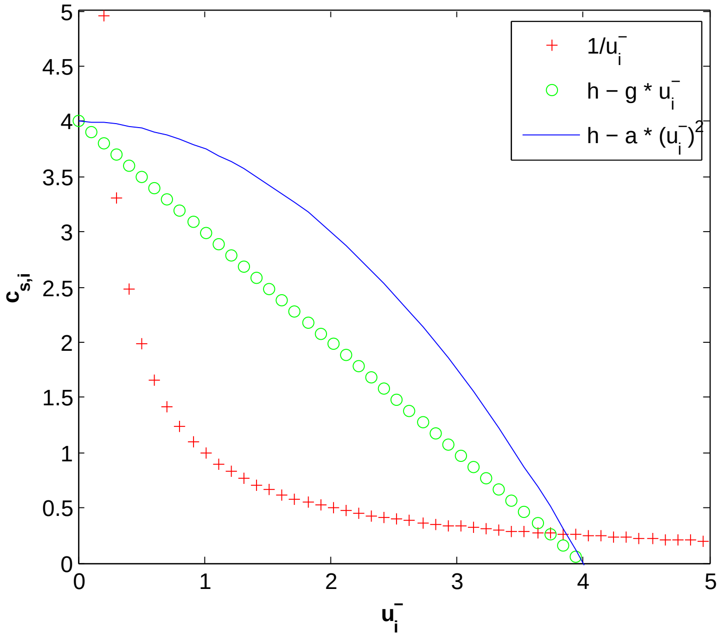


Figure 3.1: The cost of self-sacrificing $c_{s,i}$ vs. the previous payoffs u_i^- for three different functions ($h = 4$, $g = 1$ and $a = 1/4$).

Any of the three proposed models has the desired behavior but some put more or less weight on the quantity of keys u_i^- that are left. In our analysis, we consider the three functions and analyze their behavior for different values of the coefficients.

3.3.3 2-player Game with Previous Payoffs & Variable Cost

In order to understand the impact of previous history and cost variability, we start by looking at the 2-player version of the static revocation game with payoffs G_2^p, in which we include the previous payoffs u_i^- and the variable cost of self-sacrifice $c_{s,i}$. Moreover, we define such game to be *collaborative* for the voting-based strategies, meaning that players are better off collaborating when voting and removing the malicious node than leaving it in the system. In other words, we define $b - v > -c$. Assuming that the vote of the majority is needed for the revocation, both players would have to vote or at least one would have to self-sacrifice in order to revoke the malicious node. The payoff matrix of the game is shown in Table 3.3.

We know that the best response strategy of player i, given the strategies s_{-i} of the other players, is defined as

$$br_i(s_{-i}) = \arg\max_{s_i \in S_i} u_i(s_i, s_{-i}) \tag{3.23}$$

	A	**V**	**S**
A	$(u_1^- - c, u_2^- - c)$	$(u_1^- - c, u_2^- -v - c)$	$(u_1^-, u_2^- + B - c_{s,2})$
V	$(u_1^- - v - c, u_2^- - c)$	$(u_1^- + b - v, u_2^- + b - v)$	$(u_1^- + b - v, u_2^- + B - c_{s,2})$
S	$(u_1^- + B - c_{s,1}, u_2^-)$	$(u_1^- + B - c_{s,1}, u_2^- + b - v)$	$(u_1^- + B - c_{s,1}, u_2^- + B - c_{s,2})$

Table 3.3: Payoffs for the 2-player static revocation game with previous payoffs and variable cost for the self-sacrifice.

For instance, if we consider the 2-player game of Table 3.3 with $c_{s,i} = 1/u_i^-$, we can compute the best response strategies of player i for all possible strategies of player j and we obtain:

$$br_i(A) = \arg\max_{s_i \in \{A,V,S\}} u_i(s_i, A) = \begin{cases} A \text{ if } u_i^- < \frac{1}{B+c} \\ S \text{ otherwise} \end{cases} \tag{3.24}$$

$$br_i(V) = \arg\max_{s_i \in \{A,V,S\}} u_i(s_i, V) = \begin{cases} V \text{ if } u_i^- < \frac{1}{B-b+v} \\ S \text{ otherwise} \end{cases} \tag{3.25}$$

$$br_i(S) = \arg\max_{s_i \in \{A,V,S\}} u_i(s_i, S) = \begin{cases} A \text{ if } b < v \wedge u_i^- < \frac{1}{B} \\ V \text{ if } b > v \wedge u_i^- < \frac{1}{B-b+v} \\ S \text{ if } (b > v \wedge u_i^- > \frac{1}{B-b+v}) \cup (b < v \wedge u_i^- > \frac{1}{B}) \end{cases} \tag{3.26}$$

Similarly, when $c_{s,i} = h - g \cdot u_i^- > 0$ we have

$$br_i(A) = \begin{cases} A \text{ if } u_i^- < \frac{h-c-B}{g} \\ S \text{ otherwise} \end{cases} \tag{3.27}$$

$$br_i(V) = \begin{cases} V \text{ if } u_i^- < \frac{b-v-B+h}{g} \\ S \text{ otherwise} \end{cases} \tag{3.28}$$

$$br_i(S) = \begin{cases} A \text{ if } b < v \wedge u_i^- < \frac{h-B}{g} \\ V \text{ if } b > v \wedge u_i^- < \frac{b-v-B+h}{g} \\ S \text{ if } (b > v \wedge u_i^- > \frac{b-v-B+h}{g}) \cup (b < v \wedge u_i^- > \frac{h-B}{g}) \end{cases} \tag{3.29}$$

Finally, if $c_{s,i} = h - a \cdot (u_i^-)^2 > 0$, the best response functions are

$$br_i(A) = \begin{cases} A \text{ if } u_i^- < \sqrt{\frac{h-c-B}{a}} \wedge h > c + B \\ S \text{ if } u_i^- > \sqrt{\frac{h-c-B}{a}} \end{cases} \tag{3.30}$$

$$br_i(V) = \begin{cases} V \text{ if } u_i^- < \sqrt{\frac{b-v-B+h}{a}} \wedge h > B + v - b \\ S \text{ if } u_i^- > \sqrt{\frac{b-v-B+h}{a}} \end{cases} \tag{3.31}$$

$$br_i(S) = \begin{cases} A \text{ if } b < v \wedge (u_i^- < \sqrt{\frac{h-B}{a}} \wedge h > B) \\ V \text{ if } b > v \wedge (u_i^- < \sqrt{\frac{b-v-B+h}{a}} \wedge h > B + v - b) \\ S \text{ if } (b > v \wedge u_i^- > \sqrt{\frac{b-v-B+h}{a}}) \cup (b < v \wedge u_i^- > \sqrt{\frac{h-B}{a}}) \end{cases} \tag{3.32}$$

As it can be noticed, when player two chooses to *abstain*, player one's best response strategy is either to *abstain* or to *self-sacrifice*, but he should not *vote* in any case. Indeed, $u_1(V, A)$ is the lowest among all possible payoffs given player two's abstention. Moreover, the choice between abstain or self-sacrifice for player one depend on his reserve of keys that is still left: if he has enough keys ($u_1^- >$ thresholds), he should definitely self-sacrifice and, if not, he should abstain. When player two chooses to *vote*, player one's choices are limited to either vote himself or to self-sacrifice. Since we assumed a collaborative voting game, i.e. $b - v > -c$, this comes naturally since voting brings him always a better payoff than abstaining. Finally, if player two chooses to *self-sacrifice*, player one has all three strategies at his disposal, depending on the relationship between the cost and benefit parameters and his reserve u_1^-.

Having considered the cost functions and best responses when $c_{s,i} > 0$, we now list them for $c_{s,i} = 0$, according to the definitions of Section 3.3.2.

$$br_i(A) = S \tag{3.33}$$

$$br_i(V) = \begin{cases} V \text{ if } b > v \wedge b - v > B \\ S \text{ otherwise} \end{cases} \tag{3.34}$$

$$br_i(S) = \begin{cases} V \text{ if } b > v \wedge b - v > B \\ S \text{ if } (b > v \wedge b - v < B) \cup b < v \end{cases} \tag{3.35}$$

In order to make sure that the threshold values for u_i^- of the different best response functions are always positive, we have to define the minimal value for the parameter h in the linear and square functions. We can see that if

$$h > \max(B + c, B - b + v, B) = B + c \tag{3.36}$$

then all threshold values are positive and thus all possible strategies present in the best response functions are available for each player.

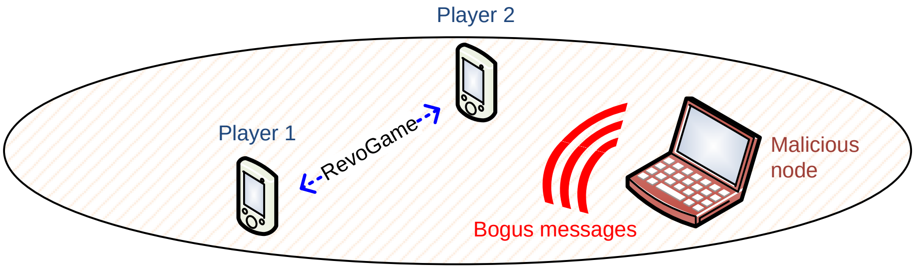


Figure 3.2: Two well-behaving nodes (player one and player two) start a revocation game against the malicious node, once the bad behavior has been identified. All nodes are in communication range with each other.

3.3.4 Numerical Example of the 2-player Game

As we have seen, the best response functions found in Section 3.3.3 often depend on more than just one parameter and the interpretations in such a general scenario are far from being trivial. For this reason, we develop here a simple situation in which there are two nodes that start playing the revocation game with previous payoffs and variable cost from Table 3.3.

The two well-behaving nodes (player *one* and player *two* hereafter) and one malicious node are all in communication range with each other, but initially player one and player two are not aware of the malicious nature of the third node. At a certain point in time, however, one of the two players somehow registers the presence of the malicious node and starts the revocation game. Figure 3.2 illustrates this scenario.

We consider four versions of the same revocation game but with different previous payoffs u_i^-. As we can already see in Figure 3.3, the decision thresholds for the linear and square cost functions are relatively high with respect to the inverse function. In this context, for the first game G_2^I we assume a relatively large number of remaining keys for each player whereas in the second game, G_2^{II}, player one has still more than enough keys left but player two is running out even with the $c_{s,i}$ inverse function. The third game, G_2^{III}, has player one low on keys but player two still enough and in the last game, G_2^{IV}, both players are low on keys for all cost functions. A visual comparison of the payoffs is shown in Figure 3.3 and the exact values of the other parameters are the following:

- For all games: $h = 4 > B = g = 1 > c = 0.5 > v = 0.3 > a = 0.25 > b = 0.2$.
- G_2^I: $u_1^- = 3 > u_2^- = 2$.
- G_2^{II}: $u_1^- = 1.5 > u_2^- = 0.8$.

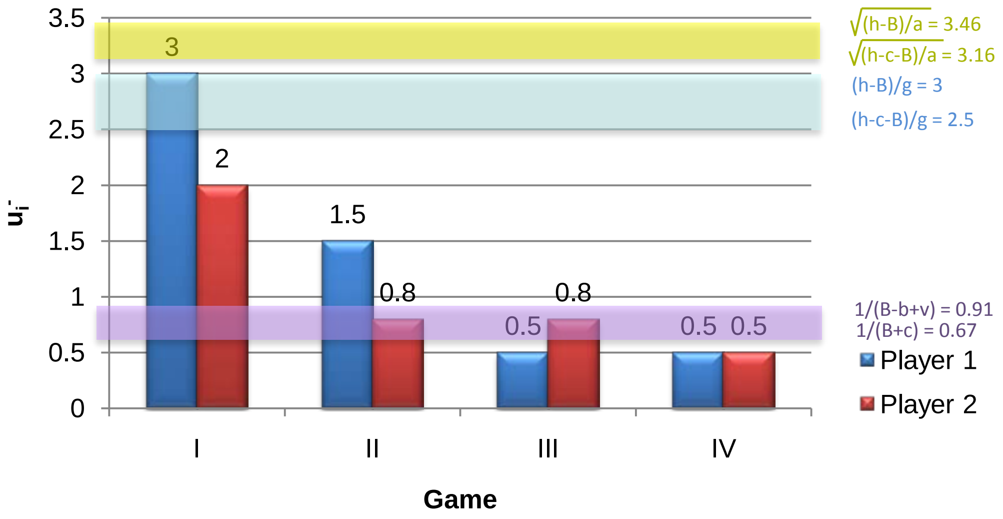


Figure 3.3: Previous payoff functions u_i^- for the four revocation games G_2^I, G_2^{II}, G_2^{III} and G_2^{IV}. The shaded horizontal regions represent the threshold intervals for each of the three $c_{s,i}$ cost functions (violet for the inverse, blue for the linear and yellow for the square function).

	A	**V**	**S**
A	(2.5, 1.5)	(2.5, 1.2)	(3, 2.5)
V	(2.2, 1.5)	(2.9, 1.9)	(2.9, 2.5)
S	(3.67, 2)	(3.67, 1.9)	(3.67, 2.5)

Table 3.4: Payoffs for the 2-player static revocation game G_2^I when $c_{s,i} = 1/u_i^-$.

- G_2^{III}: $u_1^- = 0.5 < u_2^- = 0.8$.
- G_2^{IV}: $u_1^- = u_2^- = 0.5$.

With the given numerical values, we are able to compute each player's best response strategies and therefore the NE of the four games.

G_2^I Nash Equilibria

We start by delineating each player's best response strategies according to the respective payoffs and cost functions.

$\mathbf{c_{s,i} = 1/u_i^-}$ The payoffs are shown in Table 3.4 and the best responses are:

$$br_1(A) = S \qquad br_2(A) = S \tag{3.37}$$

$$br_1(V) = S \qquad br_2(V) = S \tag{3.38}$$

$$br_1(S) = S \qquad br_2(S) = S \tag{3.39}$$

Since the NE are the mutual best responses, the unique pure strategy NE in this case is the profile $s^* = (s_1^*, s_2^*) = (S, S)$, i.e. both player sacrifice themselves and the malicious node is revoked. The payoffs corresponding to s^* are $u = (3.67, 2.5)$.

$\mathbf{c_{s,i} = h - g \cdot u_i^-}$ The best responses in this case are:

$$br_1(A) = S \qquad br_2(A) = A \tag{3.40}$$

$$br_1(V) = S \qquad br_2(V) = V \tag{3.41}$$

$$br_1(S) = A \cup S \qquad br_2(S) = A \tag{3.42}$$

The unique NE strategy profile is $s^* = (S, A)$ with $u = (3, 2)$, where player one sacrifices himself and player two abstains. This reflects the situation in which they were before starting the game, since player one had still a largely sufficient reserve of keys but player two's reserve was below the two limiting thresholds, i.e. $u_2^- < (h - B - c)/g$. Thus, the choice to sacrifice for player one and to abstain for player two appears a very rational decision.

$\mathbf{c_{s,i} = h - a \cdot (u_i^-)^2}$ The best responses are:

$$br_1(A) = A \qquad br_2(A) = A \tag{3.43}$$

$$br_1(V) = V \qquad br_2(V) = V \tag{3.44}$$

$$br_1(S) = A \qquad br_2(S) = A \tag{3.45}$$

This situation reflects the behavior of the players when both u_i^- are below all thresholds. There are two NE strategy profiles (A, A) and (V, V) with $u_{(A,A)} = (2.5, 1.5)$ and $u_{(V,V)} = (2.9, 1.9)$. Clearly, the unique Pareto-optimal NE is the profile $s^* = (V, V)$, i.e. the unique rational strategy choice.

G_2^{II} Nash Equilibria

$\mathbf{c_{s,i} = 1/u_i^-}$ As usual, the best response functions are:

$$br_1(A) = S \qquad br_2(A) = S \tag{3.46}$$

$$br_1(V) = S \qquad br_2(V) = V \tag{3.47}$$

$$br_1(S) = S \qquad br_2(S) = A \tag{3.48}$$

The unique pure strategy NE is $s^* = (S, A)$ with payoffs $u_{(S,A)} = (0.83, 0.8)$.

$\mathbf{c_{s,i} = h - g \cdot u_i^-}$ Since all u_i^- are below the thresholds, the best responses are equivalent to ones found in Section 3.3.4 for $c_{s,i} = h - a \cdot (u_i^-)^2$. Therefore, the NE are the same and the unique Pareto-optimal NE profile is $s^* = (V, V)$ with $u = (1.4, 0.7)$.

$\mathbf{c_{s,i} = h - a \cdot (u_i^-)^2}$ Like in the previous case, the unique Pareto-optimal NE profile is still $s^* = (V, V)$ with $u = (1.4, 0.7)$.

G_2^{III} Nash Equilibria

$\mathbf{c_{s,i} = 1/u_i^-}$ The best responses are:

$$br_1(A) = A \qquad br_2(A) = S \tag{3.49}$$

$$br_1(V) = V \qquad br_2(V) = V \tag{3.50}$$

$$br_1(S) = A \qquad br_2(S) = A \tag{3.51}$$

In this case, we have two pure strategy NE: (A,S) and (V,V). The first NE would result in the payoffs $u_{(A,S)} = (0.5, 0.55)$ and the second in $u_{(V,V)} = (0.4, 0.7)$. We can deduce that the final choice between one NE profile will depend on the level of selfishness and the will to take risks of the nodes. If player one chooses to vote, he will be sure that no matter the NE choice of player two, player one will get a payoff of 0.4 and this seems to be his safest strategy. Player two, on the other hand, has the same dilemma since if he chooses to self-sacrifice, he will be sure that he will get at least a payoff 0.55. From the analysis, the safest strategy for both players would be (V,S), which would yield the payoffs $u_{(V,S)} = (0.4, 0.55)$. Even though (V,S) is not a NE, in case of increasing uncertainty and node selfishness this *risk-dominant* strategy would probably be the less costly for both players. We will discuss the unique NE selection criteria in Section 3.5.1.

$\mathbf{c_{s,i} = h - g \cdot u_i^-} \quad \cup \quad \mathbf{c_{s,i} = h - a \cdot (u_i^-)^2}$ The unique Pareto-optimal NE profile is $s^* = (V, V)$ with $u = (0.4, 0.7)$.

G_2^{IV} Nash Equilibria

In this game, all u_i^- are below all thresholds for all $c_{s,i}$. Therefore, the best response functions and NE are the same for all $c_{s,i}$ and they are:

$$br_1(A) = A \qquad br_2(A) = A \tag{3.52}$$

$$br_1(V) = V \qquad br_2(V) = V \tag{3.53}$$

$$br_1(S) = A \qquad br_2(S) = A \tag{3.54}$$

The unique Pareto-optimal NE profile is $s^* = (V, V)$ with $u = (0.4, 0.4)$.

3.3.5 n-player Game with Previous Payoffs & Linear Cost

In the 2-player game described in Section 3.3.3 we have found the best response functions $br_i(s_{-i})$ for any of the two players. We now use these results to develop the n-player game G_n^{pp} with previous payoffs and variable cost of self-sacrifice, assuming $b - v > -c$. As usual, we fix the number of votes needed for the revocation of the malicious node to n_v. In absence of proofs supporting a more complex model, we express the relationship between reserve of valid keys u_i^- and the self-sacrifice cost $c_{s,i}$ with the linear function $c_{s,i} = h - g \cdot u_i^- > 0$.

In the 2-player game, whenever player *two* abstains, the outcome of the game is that the malicious node remains in the system except if player *one* self-sacrifices. Assuming we are player *one* and $n_v = 2$, if player *two* chose to abstain our best response would be defined as in Equation (3.27).

Since payoffs are only determined by our strategy and the outcome of the game, we will prove that $br_1(A) = br_i(s_{-i})$ for any sequence of strategies s_{-i} in the n-player game, as long as s_{-i} is composed by at most $n_v - 2$ votes and *all other* abstentions. For instance, $br_i(s_{-i}) = br_1(A)$ for any combination of $s_{-i} = (A, A, \ldots, A)$ up to $s_{-i} = (A, \ldots, A, V, \ldots, V)$, as long as the number of votes is smaller or equal than $n_v - 2$. By analogy, we have that $br_i(s_{-i}) = br_1(V)$ for any s_{-i} that has exactly $n_v - 1$ votes and *all other* abstentions. The last case, $br_i(s_{-i}) = br_1(S)$, holds for any s_{-i} that has *at least one* self-sacrifice.

By grouping these statements and assuming that $b - v > -c$, we are able to obtain the best response functions for the n-player static revocation game G_n^{pp} with previous payoffs and variable cost of self-sacrifice.

Lemma 3.1. *In G_n^{pp}, if s_{-i} is a combination of at most $n_v - 2$ votes and all other abstentions, the best response function for any player i is defined as*

$$br_i(s_{-i}) = \arg\max_{s_i \in \{A,V,S\}} u_i(s_i, s_{-i}) = \begin{cases} A \text{ if } u_i^- < \frac{h-B-c}{g} \\ S \text{ otherwise} \end{cases} \tag{3.55}$$

Proof. In order to prove the theorem, we look at the payoff functions for the different possible s_i, given all s_{-i} that respect the condition of the theorem.

$$s_i = A \qquad u_i(A, s_{-i}) = u_i^- - c \tag{3.56}$$

$$s_i = V \qquad u_i(V, s_{-i}) = u_i^- - c - v \tag{3.57}$$

$$s_i = S \qquad u_i(S, s_{-i}) = u_i^- + B - h + g \cdot u_i^- \tag{3.58}$$

From the above equations we know that the strategy *vote* will never be a best response since the associated payoff is always lower than the one given by *abstain*. The only choice is then between the strategy S and A. Solving the inequality $B - h + g \cdot u_i^- > -c$ we have that the best response of player i is to *abstain* if $u_i^- < \frac{h-c-B}{g}$ and to *self-sacrifice* otherwise. □

Lemma 3.2. *In G_n^{pp} and assuming $b - v > -c$ (collaborative voting game), if s_{-i} is a combination of exactly $n_v - 1$ votes and all other abstentions, the best response function for any player i is defined as*

$$br_i(s_{-i}) = \arg\max_{s_i \in \{A,V,S\}} u_i(s_i, s_{-i}) = \begin{cases} V \text{ if } u_i^- < \frac{h-B-v+b}{g} \\ S \text{ otherwise} \end{cases} \tag{3.59}$$

Proof. From the formulation of the theorem we know that $b - v > -c$ and therefore we already exclude the *abstain* strategy. The choice is then between S and V. The list of the payoffs for these strategies gives

$$s_i = V \qquad u_i(V, s_{-i}) = u_i^- + b - v \tag{3.60}$$

$$s_i = S \qquad u_i(S, s_{-i}) = u_i^- + B - h + g \cdot u_i^- \tag{3.61}$$

By solving the inequality $B - h + g \cdot u_i^- < b - v$ we obtain that $br_i(s_{-i}) = V$ if $u_i^- < \frac{b-v-b+h}{g}$ and $br_i(s_{-i}) = S$ otherwise. □

Lemma 3.3. *In G_n^{pp}, if s_{-i} is composed of at least one self-sacrifice or at least n_v votes, the best response function for any player i is defined as*

$$br_i(s_{-i}) = \arg \max_{s_i \in \{A,V,S\}} u_i(s_i, s_{-i}) = \begin{cases} A \ \textit{if}\ b < v \wedge u_i^- < \frac{h-B}{g} \\ V \ \textit{if}\ b > v \wedge u_i^- < \frac{h-B-v+b}{g} \\ S \ \textit{if}\ (b > v \wedge u_i^- > \frac{h-B-v+b}{g}) \cup (b < v \wedge u_1^- > \frac{h-B}{g}) \end{cases} \tag{3.62}$$

Proof. First of all, we list the payoff functions for all possible strategies s_i as

$$s_i = A \qquad u_i(A, s_{-i}) = u_i^- \tag{3.63}$$

$$s_i = V \qquad u_i(V, s_{-i}) = u_i^- + b - v \tag{3.64}$$

$$s_i = S \qquad u_i(S, s_{-i}) = u_i^- + B - h + g \cdot u_i^- \tag{3.65}$$

Next, we consider that $b < v$ and therefore we can already exclude the strategy *vote* as possible best response. Therefore the choice is between A and S. The solution to the inequality $B - h + g \cdot u_i^- > 0$ tells us that $br_i(s_{-i}) = S$ if $u_1^- > \frac{h-B}{g}$ and $br_i(s_{-i}) = A$ otherwise. On the other hand, when $b > v$ we can already exclude the strategy *abstain* as possible best response, which leaves us the choice between S or V. By solving the inequality $B - h + g \cdot u_i^- > b - v$ we obtain that $br_i(s_{-i}) = S$ if $u_i^- > \frac{h-B-v+b}{g}$ and $br_i(s_{-i}) = V$ otherwise. □

It is important to note that the *self-sacrifice* strategy can only be chosen if the final payoff $u_i(S, s_{-i})$ is greater than zero, i.e. if $u_i(S, s_{-i}) = u_i^- + B - c_{s,i} > 0$. In the linear cost function game, this is equivalent to

$$u_i^- > \frac{h - B}{g + 1} \tag{3.66}$$

3.4 Linear Cost Function Parameter Optimization

We are now ready to develop the linear self-sacrifice cost function even further by giving bounds on the required parameters such that there is no or little redundancy in the revocation process. In other words, we avoid unnecessary operations, such as having more than one self-sacrifice in a game, and we derive upper and lower bounds of the linear cost function parameters.

In Figure 3.3.2 and from the definition of the linear cost function of Section 3.3.5, we can see that the linear function has two parameters as usual: h is the y-intercept and g the slope. We now bound these values such that there is no or little redundancy in the revocation process, i.e. no unnecessary votes or more than one self-sacrifice in a NE strategy profile.

3.4.1 Y-intercept parameter h

We know that the threshold values of the best response functions need to be positive and therefore we have

$$\begin{aligned} h &> \max(B, B+c, B-b+v) = B+c && (3.67)\\ &> B+c && (3.68)\end{aligned}$$

3.4.2 Slope parameter g

First of all, we want that $c_{s,i} > 0$ for all players P_i, $i = 1\dots,n$. In mathematical terms, we need that

$$c_{s,i} = h - g \cdot u_i^- > 0, \qquad \forall i = 1\dots,n \tag{3.69}$$

which is equivalent to

$$\begin{aligned} c_{s,i} = h - g \cdot \max_i u_i^- &> 0 && (3.70)\\ \frac{h}{\max_i u_i^-} &> g && (3.71)\end{aligned}$$

Then, we want that the following conditions are met for a player i^* that has the highest u_i^-, i.e. a player who satisfies $i^* = \arg\max_i u_i^-$.

1. <u>*Guaranteed revocation*</u>. No *abstain* strategy is a best response to all s_{-i} that have *no self-sacrifice* or at most $n_v - 2$ votes. In other terms, we need that

$$\begin{aligned} \max_i u_i^- &> \frac{h-B-c}{g} && (3.72)\\ g &> \frac{h-B-c}{\max_i u_i^-} && (3.73)\end{aligned}$$

2. <u>*System-wise efficiency*</u>. At most *one self-sacrifice* strategy is present in each NE profile or, in other words, we do not allow $br_i(s_{-i}) = S$, if s_{-i} already has one or more *self-sacrifices*. We can guarantee this by setting the maximum payoff of the game lower than the largest threshold.

(a) If $b < v$:

$$\max_i u_i^- < \frac{h-B}{g} \tag{3.74}$$

$$g < \frac{h-B}{\max_i u_i^-} \tag{3.75}$$

(b) If $b > v$:

$$\max_i u_i^- < \frac{h-B-v+b}{g} \tag{3.76}$$

$$g < \frac{h-B-v+b}{\max_i u_i^-} \tag{3.77}$$

Bounds for g

Finally, by merging the upper bounds (3.71), (3.75), (3.77) and the lower bound (3.73) we obtain that

- if $\mathbf{b} < \mathbf{v}$:

$$\frac{h-B-c}{\max_i u_i^-} < g < \frac{h-B}{\max_i u_i^-} \tag{3.78}$$

- if $\mathbf{b} > \mathbf{v}$:

$$\frac{h-B-c}{\max_i u_i^-} < g < \frac{h-B-v+b}{\max_i u_i^-} \tag{3.79}$$

In the end, we see that the value of the slope g changes from game to game, depending on the maximum value of u_i^- at each time. It also means that the thresholds are not stationary either.

3.4.3 Nash Equilibria with Linear Cost

In Section 3.3.5 we have given the theorems that define the best response functions for each player in the n-player revocation game G_n^{pp}. We will prove here that there exists *at least* one NE profile s^* in such game as well. This result is of extreme importance since it will be a necessary requirement for our unique optimal NE selection algorithm that we present in Section 3.5.1

Claim 3.1. *In G_n^{pp} and assuming $b - v > -c$ (collaborative voting game) and $b < v$, there exists a pure strategy NE profile s^* with exactly one self-sacrifice and $n-1$ abstentions. Moreover, the player that commits self-sacrifice is the one with the largest u_i^-.*

Proof. By definition, a *Nash equilibrium* strategy profile s^* is such that no player could achieve a better individual payoff by unilaterally deviating from s^* while the others comply to it. Let us consider the strategy profile $s = (A, \ldots, A, S, A, \ldots, A)$, where the only S strategy is adopted by the player with the largest u_i^- (we call him P_S) and all the remaining $n-1$ players adopt the strategy *abstain* (we refer to any of these players as P_A). Using the bounds found in Section 3.4 for h and g, we will show that s^* is always a NE in all such G_n^{pp}.

First, let us analyze the individual payoffs for each player and for all his possible strategies, given the strategies of the other $n-1$ players.

(a) For any P_A:

$$u_{P_A},(A, s_{-i}) = u_{P_A,(A,s_{-i})} = u_{P_A}^- \tag{3.80}$$

$$u_{P_A},(V, s_{-i}) = u_{P_A,(V,s_{-i})} = u_{P_A}^- + b - v \tag{3.81}$$

$$u_{P_A},(S, s_{-i}) = u_{P_A,(S,s_{-i})} = u_{P_A}^- + B - c_{s,P_A} \tag{3.82}$$

Here, we can already exclude the second possibility (3.81) since the corresponding payoff is always smaller than the other two. We are left with $u_{P_A,(A,s_{-i})}$ and $u_{P_A,(S,s_{-i})}$ and we can see that

$$u_{P_A,(S,s_{-i})} - u_{P_A,(A,s_{-i})} = -c_{s,P_A} < 0 \tag{3.83}$$

$$u_{P_A,(S,s_{-i})} < u_{P_A,(A,s_{-i})} \tag{3.84}$$

Therefore, no player P_A has incentive to unilaterally deviate from his equilibrium strategy *abstain*.

(b) For P_S, where $u_{P_S}^- = \max_i u_i^-$:

$$u_{P_S},(A, s_{-i}) = u_{P_S,(A,s_{-i})} = u_{P_S}^- - c \tag{3.85}$$

$$u_{P_S},(V, s_{-i}) = u_{P_S,(V,s_{-i})} = u_{P_S}^- - c - v \tag{3.86}$$

$$u_{P_S},(S, s_{-i}) = u_{P_S,(S,s_{-i})} = u_{P_S}^- + B - c_{s,P_S} \tag{3.87}$$

Again, to *vote* is not an option for P_S since the strategy *abstain* would always give him a better payoff. Like in the previous case, have to analyze $u_{P_A,(A,s_{-i})}$ and $u_{P_A,(S,s_{-i})}$ and we obtain

$$u_{P_S,(S,s_{-i})} - u_{P_S,(A,s_{-i})} = B - c_{s,P_S} + c \tag{3.88}$$

$$= B - h + g \cdot u_i^- + c \tag{3.89}$$

$$\overset{(a)}{>} B - h + \frac{h - B - c}{\max_i u_i^-} \cdot u_{P_S}^- + c \tag{3.90}$$

$$\overset{(b)}{=} B - h + \frac{h - B - c}{u_{P_S}^-} \cdot u_{P_S}^- + c \tag{3.91}$$

$$= 0 \tag{3.92}$$

where (a) follows from the lower bound (3.73) and (b) from $u_{P_S}^- = \max_i u_i^-$. Summing up, we have that

$$u_{P_S,(S,s_{-i})} - u_{P_S,(A,s_{-i})} > 0 \quad \text{or} \tag{3.93}$$

$$u_{P_S,(S,s_{-i})} > u_{P_S,(A,s_{-i})} \tag{3.94}$$

Therefore, P_S has no incentive to unilaterally deviate from his equilibrium strategy S.

In the end, no player is better off deviating from his equilibrium strategy and thus s^* is a Nash equilibrium in any n-player revocation game G_n^{pp}. □

3.5 Social Welfare & NE Selection

At this point, we have seen that both in the fixed and variable cost models the pure strategy NE are not always unique. In practical terms, it means that there are situations in which either one of the possible strategy profiles could be chosen as the NE of the game. What is missing, however, is a way to enforce the choice of exactly one such NE for all the players in the game. Indeed, only if all players make a consistent decision about one particular NE, the game ends in an optimal and predictable fashion. Nevertheless, we do not assume any kind of coordination among players.

The method that we use to select a single NE, in case more are present, is based on the principle of the *price of anarchy*, which takes into account the utility of all players or, in other words, the *social welfare* function ω. There are different kinds of these functions and two among them are the *utilitarian* and *egalitarian* functions:

$$\text{Utilitarian: } \omega(s) = \sum_{i=0}^{n} u_i(s) \tag{3.95}$$

$$\text{Egalitarian: } \omega(s) = \min_{i} u_i(s) \tag{3.96}$$

By maximizing $\omega(s)$ over all possible strategy profiles $s = (s_1, \ldots, s_n) \in S$, we achieve the *social optimum* welfare

$$\text{Social Optimum } = \max_{s \in S} \omega(s) \tag{3.97}$$

The price of anarchy (PoA) is then defined as the ratio of the social optimum welfare to the welfare of the worst NE strategy profile s^*

$$\text{PoA } = \frac{\text{Social Optimum}}{\min_{s^* \in \text{NE}} \omega(s^*)} \tag{3.98}$$

The idea is that it gives a measure of how well selfish players (NE) perform compared to the social optimum.

As an example, in the 2-player games described in Section 3.3.3, we see that the game G_2^{III} has two pure strategy NE (A, S) and (V, V) with $u_{(A,S)} = (0.5, 0.55)$ and $u_{(V,V)} = (0.4, 0.7)$ but none of them is Pareto-optimal with respect to the other. To solve the issue and help players make consistent decisions, i.e. both players choose exactly the same NE strategy, we use the notion of social optimum but in a slightly different way. We do not try to maximize the welfare function ω over all possible profiles s but only over the NE profiles s^*, since we are interested in selecting one NE that is optimal with respect to the given ω. When there is prior agreement upon the social welfare model, both players are able to make independent but mutually consistent decisions that will ultimately select a unique NE. The choice then between the *egalitarian* and the *utilitarian* functions depends on the idea of social welfare: if we take the sum of all individual payoffs as social welfare, then we would choose the utilitarian function; if we think that the best is when everybody has a more uniform quantity of keys left, then we would choose the egalitarian function.

In order to better visualize the NE selection process using the modified social optimum, we refer back to the G_2^{III} game.

$$\textbf{Utilitarian model} \tag{3.99}$$

$$\text{Social Optimum } = 0.4 + 0.7 = 1.1 \qquad \text{with NE } s^*_{\text{util}} = (A, S) \tag{3.100}$$

$$\textbf{Egalitarian model} \tag{3.101}$$

$$\text{Social Optimum } = 0.5 \qquad \text{with NE } s^*_{\text{egal}} = (V, V) \tag{3.102}$$

As it can be noticed, any of the two welfare functions removed the corresponding suboptimal NE and left us with a unique NE profile s^*. In this case, there is no uncertainty about which NE profile to choose since, depending on the social welfare model, we are left with only one NE.

3.5.1 Unique Optimal NE Selection Algorithms

We now describe the sequence of event that are encountered in a revocation game and afterwards we define the unique NE selection algorithms more formally. We assume that each node i has a unique ID variable called *thisNodeID* (the serial number of the valid certificate that is being used) and a reserve of keys $u_i^- > 0$.

Once the malicious node has been identified, a well-behaving node starts a revocation game and sets the game variable *initiatorID* equal to his own *thisNodeID*. At this point, all participating nodes broadcast their own 2-tuple (u_i^-, *thisNodeID*) so that each player knows the reserve of keys and the unique ID of all participants. All NE computations are then completely distributed and no other messages need to be transmitted.

Once the NE have been computed, we start the optimal NE selection procedure, which is based on two algorithms: NESelect and OptNE. The inputs to the second algorithm are the *first optimality criteria* and *all* NE profiles; the output is a set G of *optimal NE profiles*. The first algorithm then looks whether this set is a singleton or not and if so, it outputs the unique optimal NE profile s^*, otherwise it changes the optimality criteria and restarts. If this process ends up with G having more than one optimal NE as well, the player that initiated the revocation game is then asked to select one NE from the set G at random and to broadcast it to all participants. The final output of the two algorithms is the unique socially optimal NE profile s^*.

Algorithm 1 NESelect.

```
$AllNE = \{s | s \in NE\}$
if $|AllNE| = 1$ then
    $s^* = getNext(AllNE)$
else
    $G$ = $OptNE(utilitarian, AllNE)$
    if $|S| = 1$ then
        $s^* = getNext(G)$
    else
        $G$ = $OptNE(egalitarian, AllNE)$
        if $|S| = 1$ then
            $s^* = getNext(G)$
        else
            if thisNodeID = initiatorID then
                $s^* = SelectRandom(G)$
                $Broadcast(s^*)$
            else
                $s^* = ReceiveOpt(initiatorID)$
```

Algorithm 2 OptNE(*firstOptCond, AllNE*).

```
if $firstOptCond$ = "utilitarian" then
    $\omega_1(s) = \sum_{i=0}^{n} u_i(s)$
    $\omega_2(s) = \min_i u_i(s)$
else
    $\omega_1(s) = \min_i u_i(s)$
    $\omega_2(s) = \sum_{i=0}^{n} u_i(s)$
$G_1 = \{s | s = \arg\max_{s \in AllNE}[\omega_1(s)]$
if $|G_1| = 1$ then
    $G = G_1$
else
    $G_2 = \{s | s = \arg\max_{s \in G_1}[\omega_2(s)]$
    $G = G_2$
return $G$
```

The function *getNext(.)* takes the next in line element of (.), *SelectRandom(.)* chooses one element of (.) at random, *Broadcast(.)* sends a broadcast message with the element (.) to all neighbors and *ReceiveOpt(.)* waits for the broadcasted element sent by the node with the (.) ID.

We devote Chapter 4 to the performance analysis based on simulations of the two algorithms NESelect and OptNE.

3.5.2 Parameter effect on Example Games

We are now able to test the parameter bounds and equilibrium selection algorithms found earlier to see how they perform in some typical example games. In the 2-player game, we analyze the same four scenarios that have been studied in Section 3.3.3. The revocation of the malicious node is performed when there is at least one *self-sacrifice* or with at least n_v *votes*.

2-Player games

The parameters of the 2-player games G_2^{pp} are the following

- For all games: $h = 4 > B = 1 > c = 0.5 > v = 0.3 > b = 0.2$ and $n_v = 2$.
- G_2^I: $u_1^- = 3 > u_2^- = 2$.
- G_2^{II}: $u_1^- = 1.5 > u_2^- = 0.8$.
- G_2^{III}: $u_1^- = 0.5 < u_2^- = 0.8$.
- G_2^{IV}: $u_1^- = u_2^- = 0.5$.

We also define the three thresholds values appearing in the best response functions as

$$tr_1 = \frac{h - B - c}{g} \tag{3.103}$$

$$tr_2 = \frac{h - B - v + b}{g} \tag{3.104}$$

$$tr_3 = \frac{h - B}{g} \tag{3.105}$$

The slope parameter g is chosen as the middle point between the lower and upper bounds. For $b < v$ it is

$$\frac{h - B - c}{\max_i u_i^-} < g < \frac{h - B}{\max_i u_i^-} \tag{3.106}$$

$$g = \frac{2(h - B) - c}{2 \cdot \max_i u_i^-} \tag{3.107}$$

We refer the reader to Figure 3.4 for a representation of the different previous payoffs and thresholds for each game.

G_2^I Nash Equilibria

We have that $0.83 < g < 1$ and thus we choose the middle point $g = \frac{0.83+1}{2} \approx 0.92$. Then, the threshold values are $tr_1 = 2.72$, $tr_2 = 3.15$ and $tr_3 = 3.26$.

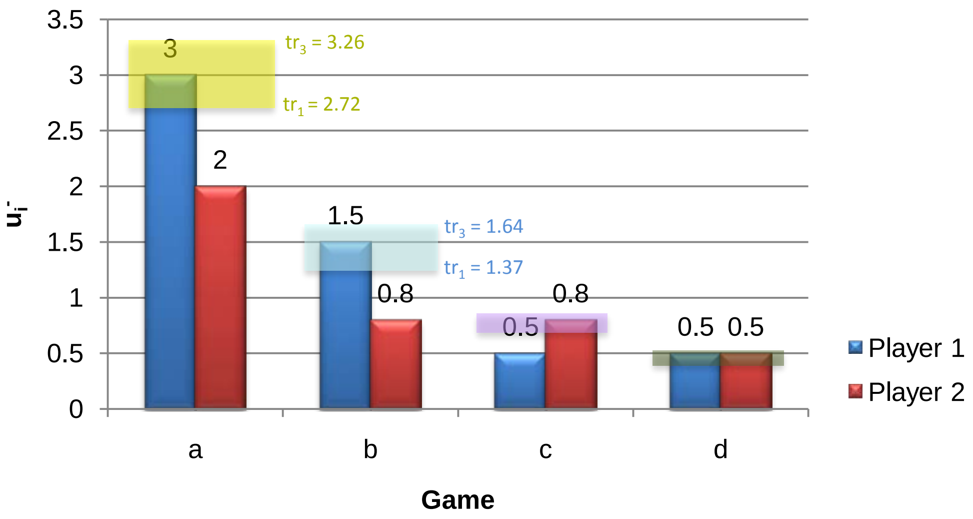


Figure 3.4: Previous payoffs in the different 2-player games with the respective threshold intervals (yellow, blue, violet and green).

We are now able to compute the best response functions of both players. We obtain

$$br_1(A) = S \qquad br_2(A) = A \tag{3.108}$$

$$br_1(V) = V \qquad br_2(V) = V \tag{3.109}$$

$$br_1(S) = A \qquad br_2(S) = A \tag{3.110}$$

The NE are then (S, A) and (V, V) with $u_{(S,A)} = (2.76, 2)$ and $u_{(V,V)} = (2.9, 1.9)$. Applying the NE selection algorithm defined in Section 3.5.1 we identify the unique NE profile $s^* = (V, V)$.

G_2^{II} Nash Equilibria

As we did before, $1.67 < g < 2$ and thus we choose $g = \frac{3.67}{2} \approx 1.83$. The threshold values are $tr_1 = 1.37$, $tr_2 = 1.58$ and $tr_3 = 1.64$. The best response functions are

$$br_1(A) = S \qquad br_2(A) = A \tag{3.111}$$

$$br_1(V) = V \qquad br_2(V) = V \tag{3.112}$$

$$br_1(S) = A \qquad br_2(S) = A \tag{3.113}$$

The NE are the same as in G_2^I: (S, A) and (V, V) with $u_{(S,A)} = (1.245, 0.8)$ and $u_{(V,V)} = (1.4, 0.7)$. The unique socially optimal NE profile is $s^* = (V, V)$.

G_2^{III} Nash Equilibria

The slope is bounded by $3.125 < g < 3.75$ and thus $g = 3.44$. The thresholds are $tr_1 = 0.73$, $tr_2 = 0.84$ and $tr_3 = 0.87$. The best responses are

$$br_1(A) = A \qquad br_2(A) = S \tag{3.114}$$
$$br_1(V) = V \qquad br_2(V) = V \tag{3.115}$$
$$br_1(S) = A \qquad br_2(S) = A \tag{3.116}$$

and the NE are (A, S) and (V, V) with $u_{(A,S)} = (0.5, 0.55)$ and $u_{(V,V)} = (0.4, 0.7)$. The optimal NE is $s^* = (V, V)$.

G_2^{IV} Nash Equilibria

As usual, $5 < g < 6$ and thus $g = 5.5$. The threshold values are $tr_1 = 0.45$, $tr_2 = 0.53$ and $tr_3 = 0.55$, while the best responses are

$$br_1(A) = S \qquad br_2(A) = S \tag{3.117}$$
$$br_1(V) = V \qquad br_2(V) = V \tag{3.118}$$
$$br_1(S) = A \qquad br_2(S) = A \tag{3.119}$$

The NE profiles are (S, A), (V, V) and (A, S) with $u_{(S,A)} = (0.25, 0.5)$, $u_{(V,V)} = (0.4, 0.4)$ and $u_{(A,S)} = (0.5, 0.25)$. The unique optimal NE is $s^* = (V, V)$.

3-Player Games

The main game parameters are the same as for the 2-player game defined earlier ($n_v = 2$). The previous payoffs in the new 3-player games are

- G_3^I: $u_1^- = 3 > u_2^- = 2.9 > u_3^- = 1$.
- G_3^{II}: $u_1^- = 3 > u_2^- = u_3^- = 1$.

Figure 3.5 shows the two scenarios.

G_3^I Nash Equilibria

According to the theorems of Section 3.3.5, the mutual best responses of the three players define the following NE profiles:

$$s_1^* = (A, S, A) \quad \rightarrow \quad u_{(A,S,A)} = (3, 2.56, 1) \tag{3.120}$$
$$s_2^* = (S, A, A) \quad \rightarrow \quad u_{(S,A,A)} = (2.76, 2.9, 1) \tag{3.121}$$
$$s_3^* = (V, V, A) \quad \rightarrow \quad u_{(V,V,A)} = (2.9, 2.8, 1) \tag{3.122}$$
$$s_4^* = (V, A, V) \quad \rightarrow \quad u_{(V,A,V)} = (2.9, 2.9, 0.9) \tag{3.123}$$
$$s_5^* = (A, V, V) \quad \rightarrow \quad u_{(A,V,V)} = (3, 2.8, 0.9) \tag{3.124}$$
$$\tag{3.125}$$

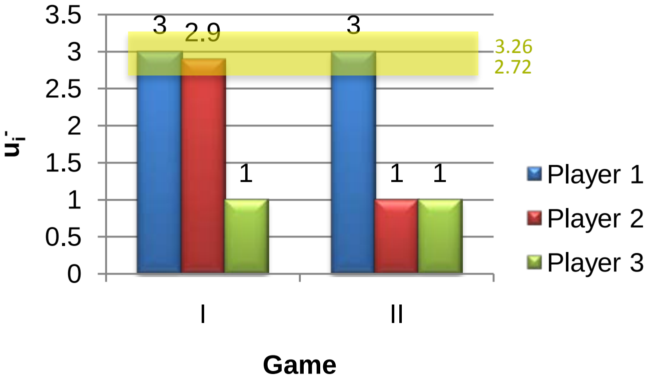


Figure 3.5: Previous payoffs in the different 3-player games with the respective threshold interval (yellow).

When identifying the unique optimal NE profile s^*, we follow the algorithm described in Section 3.5.1. First, we select the *utilitarian* function and choose all profiles s_j^* that are socially optimal NE: s_3^*, s_4^* and s_5^*. Next, we see that there is no unique such profile and therefore we select the most *egalitarian* among them, which is s_3^*. The unique optimal NE is thus the profile $s^* = (V, V, A)$.

G_3^{II} Nash Equilibria

Likewise, the NE profiles are:

$$s_1^* = (S, A, A) \quad \rightarrow \quad u_{(S,A,A)} = (2.76, 1, 1) \tag{3.126}$$

$$s_2^* = (V, V, A) \quad \rightarrow \quad u_{(V,V,A)} = (2.9, 0.9, 1) \tag{3.127}$$

$$s_3^* = (V, A, V) \quad \rightarrow \quad u_{(V,A,V)} = (2.9, 1, 0.9) \tag{3.128}$$

$$s_4^* = (A, V, V) \quad \rightarrow \quad u_{(A,V,V)} = (3, 0.9, 0.9) \tag{3.129}$$

$$\tag{3.130}$$

The NE selection algorithm dictates that we need to select the profiles s_2^*, s_3^* and s_4^*. Next, we see that there is more than one such profile and thus we select the most *egalitarian* but here again, we have two possible profiles: s_2^* and s_3^*. Therefore, we carry on with the algorithm which selects then the *egalitarian* optimality criteria in the first place. As a result, we are left with only one NE, s_1^*, which is then the unique optimal NE $s^* = (S, A, A)$.

3.6 n-player Model Complexity

Variable costs and previous payoffs are a natural extension to the initial fixed costs model. By adding benefits and dynamic parameters, we enriched the revocation games but at the expense of increased analytical complexity. Here we show that, despite the additional parameters, we are able to contain the size and time of computation of the best responses of the n-player static revocation game.

Already in the 2-player game, we have seen that an extensive list of all possible best responses was needed in order to ascertain the NE. If we wanted to go beyond the simple two player scenario to a finite n-player game, we would not be able to do so in a compact fashion, since we would need to list all possible best responses for all players and all combinations of strategies. However, since u_i depends only on the total *number* of players that choose a given strategy and not their order or identity, we are able to reduce the length of such list and therefore to accelerate the process of finding the best responses in a finite n-player revocation game.

In order to understand why this is important, let L define the number of entries necessary to extensively represent the total amount of best response strategies for the n-player revocation game. If each player's payoff depended on the order of the sequence of the other $n-1$ strategies, we would have

$$L_1 = n \cdot 3^{n-1} = \frac{n}{3} 3^n \rightarrow O(n \cdot 3^n) \tag{3.131}$$

Since in our revocation game the quantity L does not depend on the order of strategies but only on the *number* of each strategy $\{A, V, S\}$, we are able to reduce the number of entries necessary to

$$L_2 = n(\sum_{k_s=0}^{n-1} \sum_{k_v=0}^{n-1-k_s} 1) = n(\sum_{k_s=0}^{n-1} n - k_s) = \frac{n}{2}(n^2+n) = \frac{1}{2}(n^3+n^2) \rightarrow O(n^3) \tag{3.132}$$

where k_v is the number of players that choose to *vote* and k_s is the number of players who choose to *self-sacrifice*. Assuming $n = 10$, the number of entries for the best response strategies would be

$$L_1 = 10 \cdot 3^{10} = 590.490 \tag{3.133}$$

$$L_2 = 10 \cdot \frac{1.100}{2} = 5500 \tag{3.134}$$

where the ratio is $L_1/L_2 \approx 107$ for only 10 players.

We see that by keeping the payoffs dependent on the number rather than on the order of other player strategies, we are able to represent the best responses in a polynomial rather than exponential time and thus we could be able to compute the NE much faster. Unfortunately, this is not the case as we will see later on.

3.7 Summary

In this Chapter, we extended and enriched the static revocation games of complete information by adding, on top of the costs, the benefits for a successful revocation of a malicious node. The gradual development of the new model begun with the analysis of the simple payoff model with fixed costs, without any notion of previous history of games nor cost-variability. In this framework, we showed that in the n-player revocation game with fixed costs, the malicious node is always revoked by the well-behaving players, as long as the payoff for the *vote* or *self-sacrifice* strategies are greater than the cost of the malicious node still remaining in the system. Under this condition, if the reward for voting/self-sacrificing is greater than the reward for self-sacrificing/voting, the NE is unique and it is the *all-vote/all-self-sacrifice* strategy.

With the inclusion of the history of previous payoffs and the variable cost of self-sacrificing, the payoff game model acquired a more dynamic behavior since it allowed for the cost to depend on the actual reserve of keys that each player has still left prior to entering the current game. By the trade-off between aggressiveness and conservatism and without further proof of complexity, we chose to describe this individual cost by a simple linear function of each player's reserve of keys. After formally showing the best response strategies in the n-player revocation game with previous payoffs and variable (linear) cost, we then bounded the required parameters in order to achieve a system-wide efficient revocation of a malicious node, i.e. without generating more cost for the whole system than what is needed for a successful revocation. In addition to the bounds, we developed an algorithm that selects the unique optimal NE in case many are present, according to the social optimum welfare functions. We tested the new implementation on several 2- and 3-player revocation games and obtained promising results that will be further validate by simulations in the next Chapter.

We also found interesting the fact that the extension of our model to a finite n-player game would only require a polynomial amount of storage for the best response functions, compared to the exponential order in general. This is due to the fact that each player's payoffs do not depend on the order of the other strategies but just on their total number. However, as we will see, this does not imply that a unique optimal NE strategy profile can be found in polynomial time. Since each strategy profile could have different payoffs for different players, the search for an optimal NE requires an extensive listing of all best responses. Ultimately, the optimal NE search problem was shown to be NP-complete [9, 5, 6].

Chapter 4

Performance Evaluation

The analytical results achieved in Chapter 2 and 3 have proven to hold in the simple example games that have been discussed. Our intent to revoke the misbehaving node's public-key certificate by its neighbors has been fulfilled, as well as the unique determination of an optimal NE strategy profile. Even with many candidate NE, our algorithm has been able to select the socially optimal profile that would result in an efficient system-wide revocation and, at the same time, to preserve the assumption about the selfish nature of the nodes.

There are, however, aspects that the 2- and 3-players games considered so far have not been able to capture completely. For instance, what would be the behavior of the players when their number is greater than 3? Would they prefer more to sacrifice one node or to contribute to the voting together? And also: is the revocation always guaranteed, as it was in the analytical model? If so, were the nodes able to find one optimal NE in a unique manner or should the rely on the optimal selection by the revocation game initiator?

In this Chapter, we try to answer to these (and other) questions by looking at the result that have been provided through simulations of the payoff games defined in Chapter 3.

4.1 Simulation Environment

The game model that we tested was the payoff model with previous payoffs and variable (linear) cost of self-sacrifice. In Chapter 3 we called this game G_n^{pp}. The number of votes needed for revocation n_v has been set to the *majority* of the players, according to equation (2.6). The code that implemented the unique optimal NE selection algorithms NESelect and OptNE can be provided by the author upon request.

The simulations have been performed in *Matlab* software environment* on a Windows based PC (Core 2 Quad, 2.33 GHz) as follows. We run 10 iteration for each number of players between 2 and 9 with $b < v$. We then run 10 simulations for each number of players between 2 and 6 for the case $b = v$ and $b > v$. The main reason for this difference is that when $b = v$ or $b > v$, the predicted NE profiles are the optimal voting NE. One can show that the final payoff for this strategy would be greater than the payoff for the self-sacrifice optimal NE, due to the strict upperbound on g.

Players The number of players varied from 2 to 9. The role played by each of them is equal, i.e. there is no player with special abilities nor particular treatment with respect to the others.

Iterations The number of iterations for each number of players was set to 10. In other words, we performed 10 simulations for the 2-player game, other 10 simulations for the 3-player game and so on and so forth up to the 9-player game.

Previous Payoffs Since the nodes could have an undetermined number of valid certificates before entering a game, we modeled the distribution of previous payoffs u_i^- as *uniform* random variables in the interval $[0, \max u^-]$, where $\max u^- = 9.39$ was set for the simulations. At least one player always had $u_i^- = \max u^- = 9.39$.

Other Parameters The remaining fixed cost and benefit parameters are: $B = 1 > c = 0.5 > v = 0.3 > b = 0.2$ and $h = 4.5$. The slope parameter g was always the middle point between the upper and lower bounds for each iteration, as defined in Section 3.4.2. When needed, $b = v = 0.2$ and $b = 0.3 > v = 0.2$.

Tracked Data We kept track of the following relevant data through all iterations: all NE profiles, the optimal NE, previous payoffs and payoffs after the each game, the optimality criteria that was used to determine the optimal NE and the duration of each iteration.

4.2 Results Analysis

First of all, the result showed that the analytically established bounds on the game parameters are valid. In all simulations, the output of the unique optimal NE selection algorithms was indeed one such strategy profile. No strategy with more than one self-sacrifice or more than n_v votes was NE. We now examine more in detail the other interesting aspects of the simulations.

*Matlab R2007a developed by MathWorks, http://www.mathworks.com/products/matlab/

4.2.1 Results for $\mathrm{b} < \mathrm{v}$

Quantity of NE

Figure 4.1 we can notice the following. First, the number of the NE that result in a successful revocation of the misbehaving node's certificate by a *vote* strategy (exactly n_v votes and $n - n_v$ abstentions) grows exponentially with the number of players. This is explained by the fact that it is possible to have up to $\binom{n}{n_v}$ NE profiles with vote strategies and this number grows exponentially with n as shown here below:

$$\begin{aligned}
\binom{n}{n_v} &= C_n^{\lfloor n/2 \rfloor + 1} = \frac{n!}{(\lfloor n/2 \rfloor + 1)!(n - \lfloor n/2 \rfloor - 1)!} && (4.1)\\
&= \frac{n \cdot (n-1) \cdot \ldots \cdot (n - \lfloor n/2 \rfloor)}{(\lfloor n/2 \rfloor + 1)!} && (4.2)\\
&\overset{(a)}{\geq} \frac{n}{n/2+1} \cdot \frac{n-1}{n/2} \cdot \ldots \cdot \frac{n/2}{1} && (4.3)\\
&\overset{(b)}{=} \underbrace{\frac{2n}{n+2}}_{>1} \cdot \underbrace{\frac{2(n-1)}{n}}_{>1} \cdot \ldots \cdot \underbrace{\frac{n}{2}}_{>1} && (4.4)\\
&= \alpha^{n/2+1}, \quad \alpha > 1 && (4.5)
\end{aligned}$$

where (a) comes from the fact that $\lfloor n/2 \rfloor < n/2$, $(\forall n \geq 0)$, and (b) since $n \geq 3$, given that when $n = 2$ the only possibility is (V, V).

On the other hand, the number of NE with one self-sacrifice stays limited between one and two NE profiles. We can explain this by saying that there is always at least one such strategy (where the sacrificing node i is the one that has the highest u_i^-) but there might be other nodes with a high enough u_j^-, $(j \neq i)$, such that j's best response is above the required threshold as well.

As a last result, we have not found any NE that would result in a unsuccessful revocation of the misbehaving node and thus our efficiency and revocation guarantee requirements of Section 3.4 are fulfilled.

Selected NE Type

We notice an interesting aspect in Figure 4.2: the dominant optimal NE profile, selected by our algorithm, in 2- and 3-player games is obtained by *vote*, i.e. there are n_v votes and $n - n_v$ abstentions; on the other hand, in 4-9 player games the selected optimal NE is the *self-sacrifice* by one player. By looking at the simulation parameters we can explain this fact.

For our simulations, we had $v = 0.3 > b = 0.2$, which results in the payoff $u_j = u_j^- + b - v = u_j^- - 0.1$ for each player that has voted. On the other hand, we know that $B = 1 > c = 0.5$ and that gives a payoff $u_i = u_i^- + B - h + g \cdot u_i^-$,

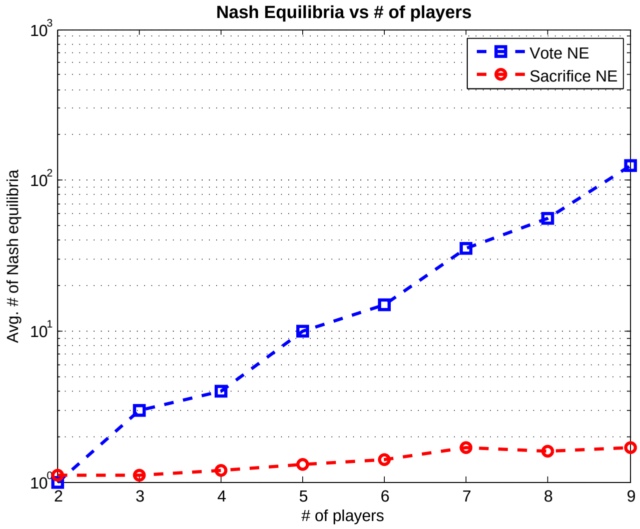


Figure 4.1: Average quantity of the different NE as a function of the number of players when $b < v$. It can be noticed that there are no NE strategy profile that would result in a non-revocation of the misbehaving node's certificate.

$i \neq j$. By developing the latter, we have the following expression for a player i that has $u_i^- = \max_j u_j^-$:

$$u_i = u_i^- + B - h + g \cdot u_i^- \overset{(a)}{=} u_i^- + B - h + \frac{2(h-B)-c}{2 \cdot u_i^-} \cdot u_i^- \tag{4.6}$$

$$= u_i^- - \frac{c}{2} = u_i^- - 0.25 \tag{4.7}$$

Now, the NESelect algorithm uses the *utilitarian* social optimum function first, i.e. the sum of individual payoffs, and then the *egalitarian* if needed. This means that the self-sacrifice NE would result in a better social optimum (the sum of individual payoffs would be greater) than the vote strategy if and only if $n_v \cdot (-0.1) < -0.25$, which happens when $n_v \geq 3$ or, equivalently, when $n \geq 4$.

Optimality Criteria

The NESelect algorithm defined in Section 3.5.1 states that, in the first place, we use the *utilitarian* → *egalitarian* sequence of social optima and, if necessary, in the opposite direction as well. We call the first sense (from left to right) the 1^{st} *criteria* and the opposite (from right to left) the 2^{nd} *criteria*. The situation is illustrated in Figure 4.3. It is straightforward to realize that, except for one iteration, the 1^{st} criteria was entirely sufficient in order to determine the optimal unique NE. This means that such NE could be found without having to go through the optimality process another time and, more importantly, that the nodes did

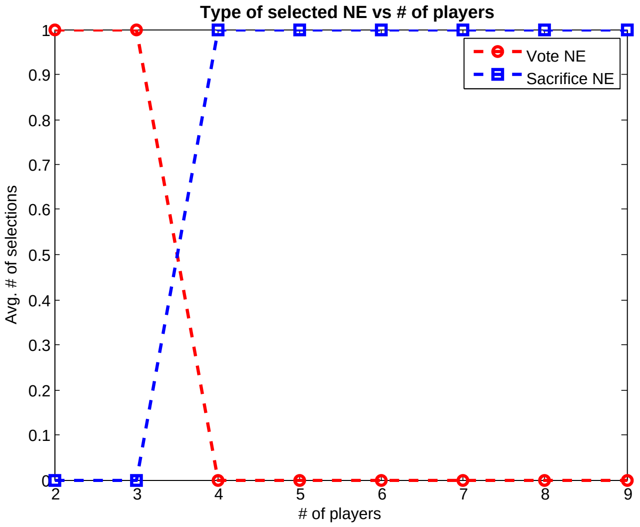


Figure 4.2: Average type of selected optimal NE as a function of the number of players when $b < v$. We notice that the vote NE (n_v votes and $n - n_v$ abstentions) is dominant for the 2-3 player games whereas the self-sacrifice NE is the choice for 4-9 player games.

not have to rely at all on the random optimal decision from the initiator of the revocation game.

Simulation Duration

Not surprisingly, the duration of the simulation for each game in the 2- to 9-player scenario was increasing exponentially with respect to the number of players. As stated in Chapter 3, the search for a socially optimum NE requires exponential time and thus this is a limitation of the current implementation of the selection algorithms. Figure 4.4 shows that this analytical result is validated empirically through our simulation. Nonetheless, one can notice that up to 5 players, the search and determination of the unique optimal NE takes less than 1 second, a time frame that is sufficient for taking a revocation decision in most of the ephemeral networks.

4.2.2 Results for $\mathrm{b} = \mathrm{v}$

In this case, we have $b = v = 0.2$, which translates in the unchanged payoffs for all voting players in a game. Hence the voting strategy is the unique type of NE that is chosen in all games, for all combination of previous payoffs. It also suggests that the multiplicity of such possible NE is greater than it was for the $b < v$ case, since now even for $n \geq 4$, a vote strategy will be the unique optimal

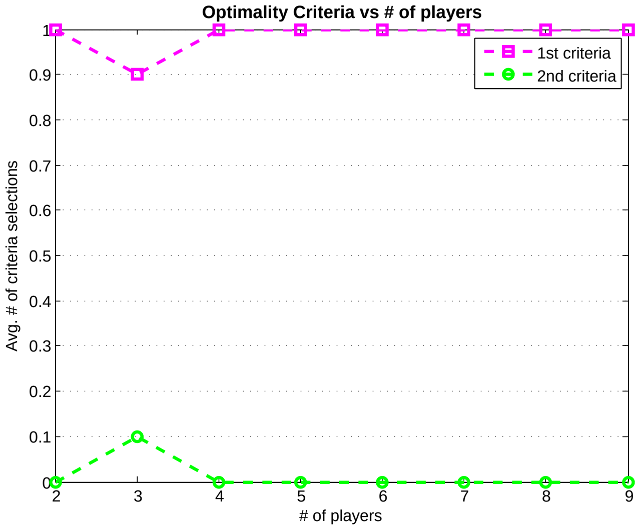


Figure 4.3: Average type of optimality criteria as a function of the number of players when $b < v$. We see that, except for one iteration, only the 1^{st} criteria was sufficient in all cases to determine the unique optimal NE profile.

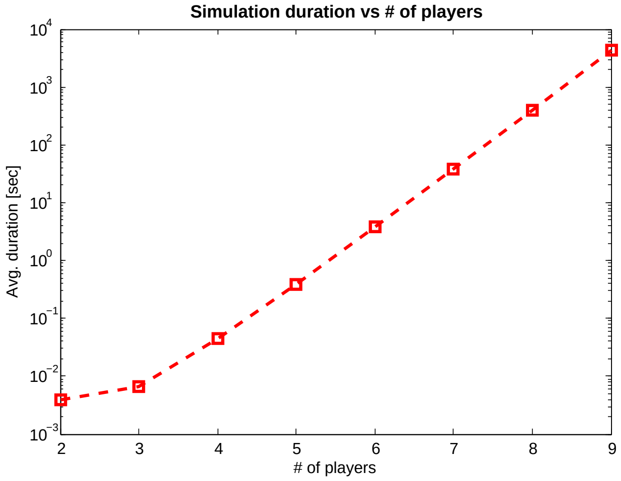


Figure 4.4: Average duration of the simulation as a function of the number of players. The exponential nature of the relationship between the search for an optimal NE and the number of players is clearly defined in this semi-log plot.

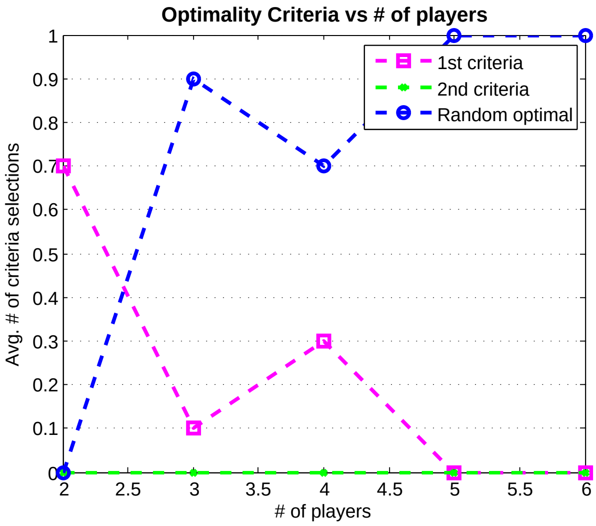


Figure 4.5: Average duration of the simulation as a function of the number of players when $\mathbf{b} = \mathbf{v}$. As the number of possible optimal NE grows exponentially and since they all have the same sum of individual payoffs, the chances to run through the entire NESelect algorithm are higher. This is confirmed by the *random* criteria being used more and more as the number of players grows.

NE.

The determination of which players exactly will perform the action and which will abstain is the unknown here. By looking at the optimality criteria, we can already see that all vote strategies will have the same sum of individual payoffs and thus the algorithm will proceed to the *egalitarian* criteria. Again, for the least happy player, there are multiply possible NE that would make him as happy as possible. For instance, if a player j has the minimum payoff (and thus is the one that will *not* vote), there are $\binom{n-1}{n_v}$ possible NE that would make no difference for him. As a consequence, there are high chances that the algorithm will need to run through the 2^{nd} criteria selection and maybe even the *random optimal* criteria, which is not envisaged. By observing Figure 4.5, we can see this trend as the number of players grows.

4.2.3 Results for b > v

In this case, the unique NE profile in all games will be the *all-vote* strategy, i.e. every player votes. This is in clear contrast with our intention to limit the unnecessary operations as stated in Section 3.4 but is in line with the selfish behavior of the nodes when considering solely their individual payoffs.

4.3 Summary

The intent of this Chapter was to test the unique optimal NE selection algorithms in possible scenarios that could arise in ephemeral and pervasive networks, where a misbehaving node was already recognized and the revocation process has just started.

In general, the results showed that the analytical model was indeed behaving correctly according to our requirements and successfully achieved its goal of determining the unique (socially optimal) NE profile for all players, in a distributed fashion.

The pros are, first of all, that the malicious node is always successfully revoked and, with a single exception, without the need for the initiator to determine the unique optimal strategy. The choice of the nodes was completely independent and they all selected the same equilibrium strategy. Moreover, we achieved the revocation without unnecessary waste of valid public-key certificate since all outcomes of the games had either exactly n_v votes or only 1 self-sacrifice, in a way that maximizes the overall social utility.

The negative points that we have found are, first of all, the duration of the simulation for a relatively small number of players and the limited scope of the voting strategy when the quantity of players increased. The first aspect could be improved by a more efficient code implementation and thus more players could potentially be accommodated. The latter feature is due essentially to the determination of the number of voters needed for a successful revocation, i.e. n_v was the majority. The challenge is here to develop a dynamic assignment of n_v as a function of some parameters used in the games, such that the social cost generated by the voters does not systematically exceed that of the self-sacrifice as soon as there are more than 3 players in the game.

When we nullify the cost for the voters ($b = v$), we see that the system evolves towards a social revocation decision that is more and more “randomized”. Since the self-sacrifice generates more social cost than the votes, the abundance of the latter strategies makes the unique NE selection process more difficult and, as a result, the random optimal NE is predominant in larger games. This could sometimes be undesirable.

The last aspect is quite obvious. When we incentive the voting strategies by providing a benefit that is greater than the cost ($b > v$), all players would prefer to vote (and get a strictly positive payoff) rather than abstaining (and getting nothing at best) or self-sacrificing (and having a negative payoff).

Chapter 5

Conclusion

The revocation of public-key certificates is an important aspect of information security. The integrity, authenticity and non-repudiation features of a message can be verified using these certificates. In case they get compromised (either by loosing or hijacking), the dangers of misuse of one's identity could become great. Moreover, if a wireless node get subverted and reprogrammed to act maliciously or very selfishly, it should definitely be denied to possibility to further interfere in the network. Due to the ephemeral and pervasive nature of the networks we analyzed, it is even more important to prevent such malicious nodes from damaging other networks in which they might connect in the future. Therefore, the revocation of public-key certificates is an extremely important measure to achieve this goal.

In this thesis, we developed a local certificate revocation scheme by using a game theoretic approach. The selfish and rational assumption about the individual nodes reflects their potentially different owners and thus their selfish nature. With this framework, we first created a cost model for the revocation process, where each action taken in order to revoke the malicious node had an associated cost expressed in public-key certificates. Since all messages need to be digitally signed, the limited number of valid certificates would deter nodes from abusing the system because otherwise they would be unable to communicate anymore. Our analysis showed that the revocation of the malicious node is not always guaranteed but, when it is, it does not generate any unnecessary actions that would result in a higher cost for the participants.

Afterwards, we enhanced the cost model by considering some reward for active participants in case of a successful revocation. This incentive towards participation proved to be very effective. Furthermore, we included in the initial model the history of previous behavior through the reserve of valid certificates of each node. Like in real world, the well-behaving individuals should receive a benefit when performing a costly but good action, in order to compensate for the effort; on the other hand, the malicious or dishonest devices should be punished. In order to cope with recidivism by insisting malicious or very compromised well-behaving nodes, we implemented the idea of a variable cost of the self-sacrifice action: the better you behave, the lower the cost for such drastic action is and *vice versa*. With these features, all possible outcomes of the revocation games guaranteed now a successful revocation of the malicious node. The issue that emerged with this first extension is the multitude of such possible game outcomes and the difficulty of coordinating to one specific equilibrium by all the selfish nodes.

In order to solve this issue, we developed a unique Nash equilibrium selection algorithm based on our payoff model with previous payoffs and variable self-sacrifice costs. The unique feature is that we take into account the social welfare in addition to the individual payoffs, by selecting the socially optimal game outcome in case more were present. The simulations results validated our analytical model and provided some further insights on the vote-based and self-sacrifice strategies. By relaxing the constraint on the number of voters (majority) to allow for a more dynamic number (based, for example, on the sum of payoffs of the players with respect to the accused node), it might be possible to exploit the vote strategy in more cases than what is currently done.

Therefore, our opinions is that for future improvements on this work one could consider, among other aspects, a dynamic number of voters, a more efficient implementation of the unique optimal NE selection algorithms, an optimization of the benefit parameters related to the different strategies and finally an improved simulation setting that would implement realistic traffic and interference parameters encountered in real-world environments.

Bibliography

[1] G. Arboit, C. Crépeau, C. R. Davis, and M. Maheswaran. A localized certificate revocation scheme for mobile ad hoc networks. *Ad Hoc Networks*, 6, 2008. [cited at p. 2, 3]

[2] L. Buttyán and J.-P. Hubaux. *Security and Cooperation in Wireless Networks*. Cambridge University Press, 2008. [cited at p. 4]

[3] S. Capkun, L. Buttyán, and J.-P. Hubaux. Self-organized public-key management for mobile ad hoc networks. *IEEE Transactions on Mobile Computing*, 2(1), 2003. [cited at p. 1, 3]

[4] S. Chinni, J. Thomas, G. Ghinea, and Z. Shen. Trust model for certificate revocation in ad hoc networks. *Ad Hoc Networks*, 6, 2008. [cited at p. 2, 3]

[5] V.t Conitzer and T. Sandholm. New complexity results about nash equilibria. *Games and Economic Behavior*, 63(2), 2008. Second World Congress of the Game Theory Society. [cited at p. 47]

[6] C. Daskalakis, P. W. Golfberg, and C. H. Papadimitriou. The complexity of computing a nash equilibrium. In *ACM STOC '06*, 2006. [cited at p. 47]

[7] D. Fudenberg and J. Tirole. *Game Theory*. The MIT Press, 1991. [cited at p. 10, 12]

[8] R. Gibbons. *A Primer in Game Theory*. Financial Times / Prentice Hall, 1992. [cited at p. 4, 12]

[9] I. Gilboa and E. Zemel. Nash and correlated equilibria: Some complexity considerations. Discussion Papers 777, Northwestern University, Center for Mathematical Studies in Economics and Management Science, 1988. [cited at p. 47]

[10] WPKI Project Group. Wpki main specification. Rev. 2.2, http://www.wpki.net/files/WPKI%20Main%20Specification%202.2.pdf, 2009. [cited at p. 8]

[11] M. Gruteser and D. Grunwald. Enhancing location privacy in wireless lan through disposable interface identifiers: A quantitative analysis. *Mobile Networks and Applications*, 10, 2005. [cited at p. 8]

[12] J.-P. Hubaux, L. Buttyan, and S. Capkun. The quest for security in mobile ad hoc networks. In *ACM MobiHOC*, 2001. [cited at p. 1, 3]

[13] C. Y. Liau, X. Zhou, S. Bressan, and K.-L. Tan. Efficient distributed reputation scheme for peer-to-peer systems. In *HSI 2003 - LNCS*, volume 2713/2003. Springer Berlin / Heidelberg, 2003. [cited at p. 2]

[14] S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *ACM MobiCOM*, 2000. [cited at p. 2, 7, 9]

[15] S. Moloney and P. Ginzboorg. Security for interactions in pervasive networks: Applicability of recommendation systems. *ESAS 2004 - LNCS*, 3313, 2005. [cited at p. 8]

[16] T. Moore, J. Clulow, S. Naharaja, and R. Anderson. New strategies for revocation in ad-hoc networks. In *ESAS 2007 - LNCS*, volume 4572. Springer Berlin / Heidelberg, 2007. [cited at p. 2]

[17] J.D. Power and Associates. U.S. wireless contract regional customer satisfaction index (csi) study. Press release, October 2008. [cited at p. 1]

[18] M. Raya, M. H. Manshaei, M. Felegyhazi, and J.-P. Hubaux. Revocation games in ephemeral networks. In *ACM CCS*, 2008. [cited at p. 3, 4, 11, 19]

[19] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux. Eviction of misbehaving and faulty nodes in vehicular networks. *IEEE Journal on Selected Areas in Communications*, 25(8), 2007. [cited at p. 2, 3, 9]

[20] P. Resnick, R. Zeckhauser, E. Friedman, and K. Kuwabara. Reputation systems. *Communications of the ACM*, 43(12), 2000. [cited at p. 2]

[21] G. Theodorakopoulos and J. S. Baras. A game for ad hoc network connectivity in the presence of malicious users. In *IEEE Global Telecommunications Conference*, 2006. [cited at p. 7]

[22] G. Theodorakopoulos and J. S. Barras. On trust models and trust evaluation metrics for ad hoc networks. *IEEE Journal on Selected Areas in Communications*, 24(2), 2006. [cited at p. 2]

[23] K. Wrona. Distributed security: Ad hoc networks & beyond. In *Ad Hoc Network Security, Pampas Workshop*, 2002. [cited at p. 8]

[24] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang. Security in mobile ad hoc networks: Challenges and solutions. *IEEE Wireless Communications*, 2004. [cited at p. 1, 7]

[25] P. Zimmerman. *The Official PGP User's Guide.* MIT Press, 1995. [cited at p. 1]