Computer Networks 55 (2011) 1168–1180

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

OREN: Optimal revocations in ephemeral networks

Igor Bilogrevic *, Mohammad Hossein Manshaei, Maxim Raya, Jean-Pierre Hubaux

Laboratory for Computer Communications and Applications 1, EPFL, Switzerland

ARTICLE INFO

Article history:
Received 31 July 2010
Received in revised form 22 November 2010
Accepted 24 November 2010
Available online 3 December 2010
Responsible Editor: A. Orda

Keywords:
Game theory
Wireless security
Ephemeral networks
Social optimum
Revocations

ABSTRACT

Public-key certificates allow a multitude of entities to securely exchange and verify the authenticity of data. However, the ability to effectively revoke compromised or untrustworthy certificates is of great importance when coping with misbehavior. In this paper, we design a fully distributed local certificate revocation scheme for *ephemeral* networks – a class of extremely volatile wireless networks with short-duration and short-range communications – based on a game-theoretic approach. First, by providing incentives, we can guarantee the successful revocation of the malicious nodes even if they collude. Second, thanks to the records of past behavior, we dynamically adapt the parameters to nodes' reputations and establish the optimal Nash equilibrium (NE) on-the-fly, minimizing the social cost of the revocation. Third, based on the analytical results, we define *OREN*, a unique optimal NE selection protocol, and evaluate its performance through simulations. We show that our scheme is effective in quickly and efficiently removing malicious devices from the network.

1. Introduction

The emerging availability of wireless devices able to communicate directly with other peers is opening new ways for people to interact and exchange information [1–3]. The absence of a centrally-managed infrastructure, however, makes it harder to cope with misbehavior. In the literature, a considerable effort is being devoted to the analysis of security mechanisms performed by self-interested agents [4,5]. In particular, the revocation of compromised public-key certificates is a very important primitive for environments where authentication is required.

In ephemeral networks, the short-lived and heterogeneous contacts among nodes (potentially unbeknownst to each other) make it imperative to address the revocation issue in a distributed and efficient way. One step in this direction has been taken by Raya et al. [6] through their game-theoretic local certificate revocation protocol RevoGame. Their model, however, has some limitations. First, it is often difficult to obtain correct estimates of crucial parameters very frequently and thus the outcome of the revocation could be unpredictable. Second, the dynamic kind of games used by their model assumes that each node can observe the actions of the others before taking its own decision, which is not always be feasible in ephemeral environments. For example, the duration of the related public-key operations, such as signature verification and generation, might take an excessive amount of time.

In this paper, we design a substantially improved and extended local certificate revocation framework for ephemeral networks. With respect to [6], our contribution is fourfold. First of all, we consider revocations in which nodes take actions simultaneously, i.e. they do not know others' decisions before taking their own, as it might take too much time in practice and the nodes might have already lost contact. Second, we provide incentives that stimulate participation and guarantee a successful revocation of malicious nodes even when they collude or when the parameter estimations are difficult. Third, by

* Corresponding author. Address: EPFL-IC-LCA, Station 14, CH-1015 Lausanne, Switzerland. Tel.: +41 21 693 66 21; fax: +41 21 693 66 10.
E-mail addresses: igor.bilogrevic@epfl.ch (I. Bilogrevic), hossein.manshaei@epfl.ch (M.H. Manshaei), maxim.raya@gmail.com (M. Raya), jean-pierre.hubaux@epfl.ch (J.-P. Hubaux).

1389-1286/$ - see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.comnet.2010.11.010

considering the past behavior of devices as their reputation, we are able to allow for personalized and dynamic costs that depend on the behavior of each node in past games. Fourth, as each device could potentially have a different reputation, we design a fully distributed on-the-fly NE selection protocol, *OREN*, that establishes, if more than one NE exist, the best course of action for each player with the least social cost. Simulation results finally show that our analytical framework is effective in removing the misbehaving nodes' certificates through the socially optimal NE of the revocation game.

The paper is organized as follows. After discussing the related work in Section 2, we present our system model in Section 3. We describe the revocation process in Section 4 and we perform the game theoretic analysis in Section 5. We devote Section 6 to the design of the socially optimal Nash equilibrium selection protocol *OREN* and we evaluate its performance through simulations in Section 7. We conclude the paper in Section 8.

2. Related work

Li et al. [7] propose a key management model based on a *web of trust*, where nodes sign each other's certificates without any trusted third party. Revocation is performed by a single node that broadcasts the revocation request to all two-hop neighbors, who then add the accused node's certificate to their blacklists. However, the communication overhead related to blacklist exchange and the trust assumptions derived from indirect chains of certificates could lead to security compromises when dealing with nodes without previous first-hand knowledge. A "virtual" CA is envisaged by Luo et al. [8], where no single node is trusted to issue certificates on its own, but any k trusted nodes together are allowed to issue and revoke certificates. Assuming a system-wide fixed value for k, new nodes wishing to enter the network are forced to migrate in places where at least k already trusted devices are willing to sign the public/private key pair of the newcomer.

Chinni et al. [9] propose a hierarchical trust model where a trusted third party (CA) is responsible for the generation of public-key certificates but revocation is delegated to nodes. The authors suggest a method to deal with misbehaving devices by minimizing their trust level among the neighbors based on the quality of service they provide but, at the same time, they allow the trust to be regained and therefore the certificate renewal interval can be extended. Similarly, Arboit et al. [10] perform a game-theoretic security analysis and compute a trust threshold value by taking into account the reputations of both the accused and accusing nodes. An accusation made by a node with a low reputation, i.e. a node that has many pending accusations on itself, has a lower weight than the accusation by a node with a higher reputation (with fewer pending accusations). A revocation is successful if the sum of weighted accusations is greater than a threshold value, and the revoked certificate is completely useless for further interactions.

Reputation mechanisms and their applications in mobile ad hoc networks have also been studied by Michiardi and Molva [11]. Their *CORE* reputation scheme naturally excludes nodes from the network, if they do not contribute to its functioning, by lowering their reputations, whereas cooperating nodes can operate and request more services, as their reputation is increased for every service their provide to the community.

In [6], Raya et al. 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 as the game model is a dynamic complete information game. As stated in Section 1, the estimation of several game parameters, such as the number of detectors and the number of required voters, coupled with the sequential strategic behavior, are some of the limiting factors addressed in this work. Incentives for revocations in ad hoc networks are analyzed by Reidt et al. [12], although only the self-sacrifice of one node could lead to the revocation of a malicious node's certificate.

3. System model

We consider an ephemeral network with short-duration (1–10 s), short-range (10–100 m) contacts that can take place both in licensed and unlicensed frequency bands. We only require the wireless devices to be able to establish 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 [13]) have integrated public-key certificates for connecting to secure HTTPS servers on the Internet or for authenticating themselves on protected enterprise IEEE 802.11 WLAN networks.

We consider that a trusted third party (or parties) exists in such networks and that each mobile node is pre-loaded with public-key certificates issued by a CA, that are used both for periodically advertising their presence (by broadcasting a signed beacon message) and for signing all sent messages. In order to allow for integrity and authenticity checks, we assume that only signed messages will be considered. The unique certificate serial number [14] serves as a *unique ID* that distinguishes each device in a given revocation process. We also assume that each node has more than one certificate in the initial deployment phase, in order to allow for location privacy protection and to avoid the possibility of being tracked and identified over time [15,16].

3.1. Certificate management

We assume that each node i has a *reserve* R_i containing all valid certificates, a *counter* u_i^- which measures the number of valid certificates within R_i that can be used for revocations, and a *tamper-resistant* device, such as a smart-card, where the revocation protocols are executed. The counter and reserve can be updated and signed either by a CA or by the tamper-resistant device but not by the node itself.

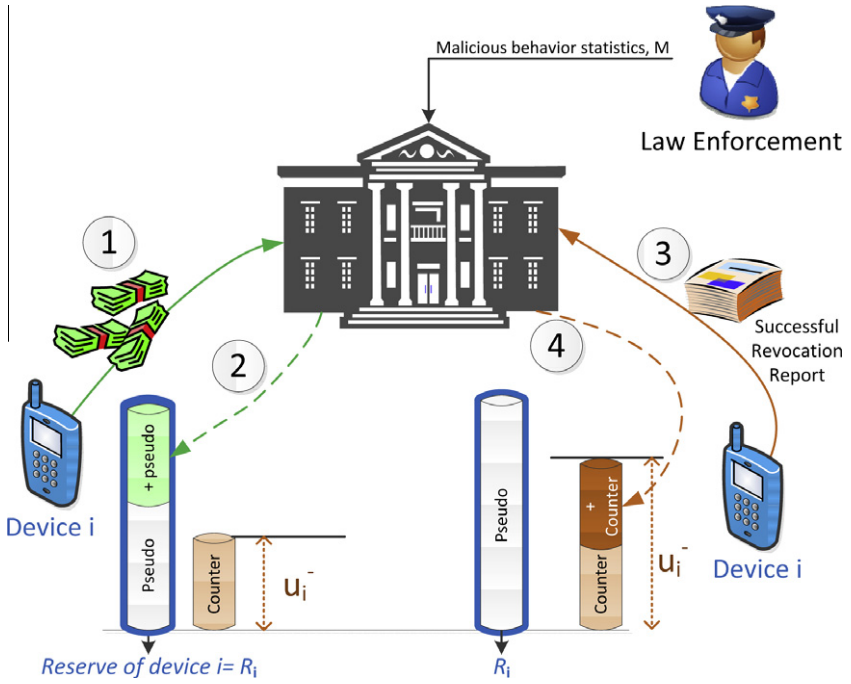

Fig. 1. Example scenario of a certificate update by the CA. Device *i* buys some certificates (step 1) and the CA only updates its *reserve* (step 2). Device *i*, after having actively participated in a revocation process, sends its revocation report to the CA (step 3), which updates both *i*'s counter u_i^- and *reserve* (step 4). Note that the CA sets the system parameter M/N based on periodic malicious behavior statistics, gathered by the law enforcement authorities.

After the initial deployment, we do not assume an always-on connection with the central authority, but we do assume that nodes will reconnect with the CA sporadically (from every few hours to every few days) through a direct connection or a pre-deployed infrastructure managed by the CA. During the successive connections, the CA will renew nodes' credentials by updating the counter u_i^- and/or reserve R_i, after having verified their past behavior in an appropriate way (e.g., the judgment system presented in [12]).

Nodes can thus obtain valid certificates by either (a) buying them from the CA (Fig. 1, step 1 and 2) or (b) by revoking malicious nodes, as a reward for the useful service provided to the community (Fig. 1, step 3 and 4). Note that when buying certificates, only the reserve is updated by the CA with new certificates for location privacy protection (+pseudo), whereas by revoking malicious devices, both reserve and counter are updated by the same amount (+counter). By definition, the level of the reserve cannot be lower than the counter and when the former reaches the latter (due to frequent pseudonym changes for instance), a node would have to renew its certificates in order to continue ensuring its location privacy. When a revocation occurs, the revocation protocol updates the values of R_i and u_i^- in all participating nodes by using the tamper-resistant device. This will be discussed in more detail when we define our revocation protocol in Sections 4 and 5.

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.

3.2. Threat model

The attacker could potentially be any wireless device with exactly the same characteristics as the other benign nodes. Examples of misbehavior include, for instance, disseminating false information in the network, sending undesired advertisements or hijacking other nodes with the intent to subvert them to the attacker's advantage. We assume that multiple attackers can also collude in order to revoke benign nodes.

4. Revocation process

The revocation procedure begins when a node detects the presence of a misbehaving peer (node m) and decides to accuse it. Note that for each accused node m, there is one revocation process and each node can participate in at most one at any given time, even though there could be many processes running in parallel. For simplicity and without loss of generality, in this paper we consider one revocation only. Moreover, we focus on the *reaction* [17] of a set of nodes once a malicious node has already been detected, rather than on the detection mechanism itself. References on the latter aspect can be found in [18,19].

The action that each device can take in a revocation process is either *abstain*, *vote* or commit *self-sacrifice*. By abstaining, the node does not take any *active*[1] role but

[1] By active we mean nodes that have either *voted* or committed *self-sacrifice* in the revocation process.

expects the other peers to eventually remove the accused node from the network. Voting against the incriminated node is decisive but a single vote is usually not sufficient for a successful revocation. There should be at least n_v votes in order to perform the revocation. The determination of this important parameter is performed in Section 5.2. Yet another possibility is obtained by allowing a single node to entirely revoke the certificate of the misbehaving node [20]. At the same time, however, the node performing the revocation has to sacrifice a considerable amount of its own certificates as well, in order to limit abuses. We call this powerful but expensive strategy the *self-sacrifice*. We devote Section 5.4 to the fine tuning of the self-sacrifice cost function.

The sequence of events encountered in each revocation process is shown in Fig. 2 and described hereafter. We assume that there is a set of $N = n + M$ nodes in communication range, where n is the number of benign nodes and M is the number of estimated malicious ones. M could also represent the estimated power of the colluding attackers, and in this case M/N could be set by the CA to a high value in case of a conservative attitude and repeated collusion attacks by malicious nodes. For instance, statistics on nodes' behavior (gathered periodically by the law enforcement authorities) can be used by the CA to set the M/N value according to the expected power of colluding attackers. In the set n of benign nodes there is one device, called *initiator*, that broadcasts (1) the *revocation request* against an accused node m, (2) its *signed counter*, (3) the attack-induced cost parameter c and (4) the parameter M/N (signed by the CA) to all peers, called *participants*, that are in communication range with both the initiator and the accused node. The participants respond to the request by broadcasting their own signed counters, such that all parties are aware of the respective amounts of valid certificates. When the accused node receives the revocation request against it, a signed message containing its own counter is generated by its tamper-resistant module and broadcast as well. Once all the n benign nodes have complete knowledge of each others' counters and M, they do not need to communicate anymore and the off-line distributed revocation process (described in Section 6) begins. Our protocols then define the unique outcome and the individual actions for all devices.

In order to prevent any abuse of benign nodes and encourage participation in revocations against malicious

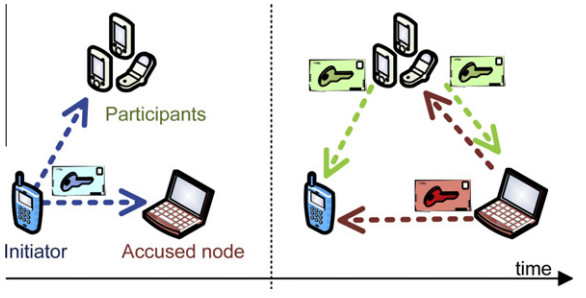

Fig. 2. Revocation process sequence of events: first, the initiator broadcasts the accusation and his signed counter and then participants and accused node broadcast their own counters.

Table 1
List of symbols.

Symbol	Definition
N	Total number of nodes in comm. range (benign + malicious)
M	Number of malicious nodes in comm. range
R_i	Reserve of valid certificates of node i
b	Benefit for voting
B	Benefit for self-sacrificing
c	Cost of non revocation of malicious node
$C_{s,i}$	Cost of self-sacrificing for player i
$f(M/N)$	Risk of attack by colluding malicious nodes for self-sacrificing
$e(M/N)$	Risk of attack by colluding malicious nodes for voting
k	If successful revocation $k = 1$, otherwise $k = 0$
m	Subscript used for the malicious node
n_v	Number of votes required for the revocation
u_i^-	Counter of player i's valid certificates for revocations
v	Cost of voting
$\gamma(s_{-i})$	Sum of counters of players (other than i)that vote

devices, we need to assign *costs* and *benefits* for every action performed by a participant in any revocation procedure (Table 1). We express these in number of certificates because they are a vital (required to sign messages) and limited resource in our network. For instance, we assume that for any participant i, casting a vote has a cost of $v + e(M/N)$, where $v \geqslant 0$ is a fraction of the counter set by the CA and $e(M/N) \geqslant 0$ is a function that represents the risk of a retaliation attack by colluding malicious peers against a node that chooses to cast a vote. Similarly, a self-sacrifice costs $c_{s,i} + f(M/N)$, where $c_{s,i} \geqslant 0$ is the individual cost for the self-sacrifice action and $f(M/N) \geqslant 0$ is a function that models the risk of a retaliation attack by colluding malicious peers against a node that performs a self-sacrifice. The two collusion risk functions are characterized in Section 5.3.

If the revocation is successful, the CA provides rewards for voting and committing self-sacrifice, which are b and B, respectively. The abstain strategy, on the contrary, does not have a cost or benefit because it does not contribute the revocation. If the revocation is not successful, the benefits are not distributed. Moreover, a failed attempt and the wasted effort of the community is computed by adding the attack-induced cost value c for all participants, which is estimated by the *initiator* and broadcast together with the revocation request at the beginning of the process.

After each revocation procedure, a report – containing all the *unique IDs* of nodes involved in the process together with the associated action – is compiled by all nodes and stored. At the next possible occasion, each participating node sends the report to the CA who then verifies, in a suitable way, the past behavior of the accused node and decides whether to permanently revoke the certificate or not. In case the accusation was unfunded, the CA can also punish nodes that have disseminated false accusations. Finally, depending on the action taken by each device, the CA rewards the participants with fresh certificates and updates the reserves and counters, which then enable the participants to continue operating in the network.

Clearly, if a device is seldom required to participate in revocation procedures, its counter does not evolve as

quickly as that of the frequent participants and thus the CA does not need to renew its credentials due to revocations. However, all nodes will have to periodically renew their certificates when the level of the reserve reaches the value of the counter, in order to prevent eavesdroppers from tracking their location.

Although the revocation protocols are run in a tamper-resistant device and certificates are updated by a CA, there could still be several possible combinations of actions by which each revocation procedure might end. Moreover, as the costs for each node depend both on the individual action (performed by that node) and on the outcome of the revocation itself (whether the accused node is revoked or not), a game-theoretic framework is well adapted to model and analyze such strategic situations. Furthermore, if more than one solution exists, game theory provides means for all parties to converge to the socially optimal one, which maximizes the aggregated benefits of the community of nodes. Sections 5 and 6 are devoted to the application of game theory to local revocations.

5. Game-theoretic analysis

In this section, we present our game-theoretic framework and the analytical results. First, we consider revocation games where payoffs depend on the current strategies and game outcome only. Afterwards, we extend the framework to include nodes' past behavior in the computations of payoffs, strategies and outcomes by considering the counter as the indicator of a node's reputation.

We define a non-cooperative static *revocation* game as $\mathsf{G}_n = \{\mathcal{P}, \mathcal{S}, \mathcal{U}\}$, where $\mathcal{P} = \{P_i\}_{i=1}^n$ is the set of the n wireless players as described in Section 3, $\mathcal{S} = \{S_i\}_{i=1}^n$ is the strategy set and $\mathcal{U} = \{u_i\}_{i=1}^n$ the payoff set. Moreover, we assume the game to be of complete information, i.e. every node has complete knowledge about the payoff functions and the counters of all participants. This assumption is based on the fact that the game parameters are either defined in advance on a system-level scale or they are completely defined by the information exchanged during the revocation process itself. More often than not, security decisions are made on implicit assumptions about the strength of the attacker, but here we need to commensurate the response of benign players to quantitative values of the current costs and benefits of the game. Therefore, we assume such values to be known to all participants before the actual game takes place.

Strategies. The strategies available for each player i are either *abstain* (A), *vote* (V), or commit *self-sacrifice* (S). Each strategy has an associated benefit and cost that depends on the successful or unsuccessful revocation of the certificate as well.

Payoffs. The payoff function u_i of player i is defined as the difference between *benefits* and *costs*, expressed in public-key certificates and is shown in Table 2.

The quantity of valid certificates, available for revocation purposes, is defined as u_i^- for each player i, whereas the accused node m has u_m^-. According to Section 3, we refer to it as the *counter*, which is updated after each game as the sum of the previous value of the counter and the current payoff, i.e. $u_i^- \leftarrow u_i^- + u_i$, such that it is accumulated over time. The evolution of u_i^- depends therefore on the way nodes participate in revocation games and on their past behavior.

Table 2
Payoff u_i of player i after the end of a revocation game, given the strategy s_i. If the revocation was successful, we have $k = 1$ and otherwise $k = 0$.

	Abstain	Self-sacrifice	Vote
Cost	$(1-k)\cdot c$	$c_{s,i} + f(M/N)$	$v + e(M/N) + (1-k)\cdot c$
Benefit	0	B	$k \cdot b$
Payoff u_i	$-(1-k)\cdot c$	$B - c_{s,i} - f(M/N)$	$k\cdot b - v - e(M/N) - (1-k)\cdot c$

Game solutions. A widely adopted solution concept in game theory is the *Nash equilibrium (NE)*, a strategy set $s^* = \{s_i^*\}_{i=1}^n$ from which no node has incentive to unilaterally deviate, given that all other players conform to it. In this paper, we focus on Nash equilibria as the rational outcome for any revocation game G_n. Although computing any NE is PPAD hard [21], the fine tuning performed in Section 5.4 allows nodes to substantially reduce the number of such computations by considering only efficient strategy profiles that result in a successful revocation.

5.1. Revocations with Payoffs

Let G_n^f be an n-player revocation game, where benefit and cost values of Table 2 are fixed for all players ($c_{s,i} = c_s$). Initially, we assume that the number of votes required to revoke a certificate is a fixed value n_t. We now establish the solutions of G_n^f by means of the NE strategies which define, for each player, the strategy to adopt in order to achieve the desired outcome.

Lemma 1. *In G_n^f, for $(B = c_s) \wedge (b > v)$, the n-player static game G_n has a unique pure strategy NE profile $s^* = (V, \ldots, V)$, i.e. all players vote and the accused node is revoked.*

Proof. By definition, we know that a strategy profile s is a NE iff no single player has incentive to unilaterally deviate from his equilibrium strategy s_i^*, given the strategies of other players s_{-i}. If we consider the payoff for any player i corresponding to the strategy profile $s^* = (V, \ldots, V)$ we have that

$$
\begin{aligned}
&s_i = A \qquad u_i(V, \ldots, A, V, \ldots, V) = 0,\\
&s_i^* = V \qquad u_i(V, \ldots, V, \ldots, V) = b - v - e(M/N),\\
&s_i = S \qquad u_i(V, \ldots, S, V, \ldots, V) = B - c_s - f(M/N).
\end{aligned}
$$

Given the conditions of the Lemma, $b - v - e(M/N) > 0 - f(M/N)$ and thus for any $s_i \neq s_i^*$, the corresponding payoff is lower than if $s_i = s_i^*$. □

Intuitively, as the payoff for voting is strictly greater than for self-sacrificing, all players are better off voting and revoking the certificate.

Lemma 2. *In G_n^f, for $(B = c_s) \wedge (b < v)$, if $f(M/N) < c$ then the NE are all strategy profiles s^* that have exactly one self-sacrifice and $n-1$ abstentions. If $f(M/N) \geqslant c$, then the strategy profile all-abstain is a NE.*

Proof. We consider the strategy profile s^* with *one* self-sacrifice and $n-1$ abstentions. In this case, the payoffs are $u = (B - c_s - f(M/N), 0, \ldots, 0) = (-f(M/N), \ldots, 0)$, where the self-sacrificing player i could be any of the n players. The payoffs are

$$\begin{aligned}
&\text{if } s_i^* = S : u_i(A, \ldots, s_i^*, A, \ldots, A) = 0 - f(M/N),\\
&\qquad u_i(A, \ldots, A, \ldots, A) = -c,\\
&\qquad u_i(A, \ldots, V, A, \ldots, A) = -v - e(M/N) - c,\\
&\text{if } s_i^* = A : u_i(S, A \ldots, s_i^*, \ldots, A) = 0,\\
&\qquad u_i(S, A, \ldots, V, A, \ldots, A) = b - v - e(M/N),\\
&\qquad u_i(S, A \ldots, S, A, \ldots, A) = 0 - f(M/N).
\end{aligned}$$

For $s_i^* = S$, $u_i(A, \ldots, A) = -c < u_i(s_i^*, A, \ldots, A) = -f(M/N)$ if and only if $f(M/N) < c$. For $s_i^* = A$, $u_i(S, A, \ldots, A) = 0 > u_i(S, A, \ldots, S, A, \ldots, A) = -f(M/N)$ for all $f(M/N) > 0$.

We see that if player i is the only sacrificing participant, he has no incentive to deviate from this strategy if the risk of retaliation is low ($f(M/N) < c$). In this case, any strategy profile s^* with exactly *one* self-sacrifice and $n-1$ abstentions is a NE. If, on the other hand, the risk of retaliation is high, he would prefer to abstain and thus the *all-abstain* strategy profile would be a NE. □

In other words, if the risk of retaliation by colluding malicious nodes is higher than the attack induced cost, then the benign nodes would prefer not to revoke the misbehaving device.

Lemma 3. *In* G_n^f, *for* $[(B < c_s) \wedge (b < v)] \wedge [B - c_s - f(M/N) > b - v - e(M/N)]$, *if* $f(M/N) < B - c_s + c$ *then the NE are all strategy profiles that have exactly one self-sacrifice and* $n-1$ *abstentions. If* $f(M/N) > B - c_s + c$ *then the strategy profile all-abstain is a NE.*

Proof. Similar to Lemma 2, we consider the strategy profile s^* with *one* self-sacrifice and $n-1$ abstentions. The payoffs are $u = (B - c_s - f(M/N), 0, \ldots, 0)$, where the self-sacrificing player i could be any of the n players. Then

$$\begin{aligned}
&\text{if } s_i^* = S : u_i(A, \ldots, s_i^*, A, \ldots, A) = B - c_s - f(M/N),\\
&\qquad u_i(A, \ldots, A, \ldots, A) = -c,\\
&\qquad u_i(A, \ldots, V, A, \ldots, A) = -v - e(M/N) - c,\\
&\text{if } s_i^* = A : u_i(S, A \ldots, s_i^*, \ldots, A) = 0,\\
&\qquad u_i(S, A, \ldots, V, A, \ldots, A) = b - v - e(M/N),\\
&\qquad u_i(S, A \ldots, S, A, \ldots, A) = B - c_s - f(M/N).
\end{aligned}$$

For $s_i^* = S$, $u_i(A, \ldots, A) = -c < u_i(s_i^*, A, \ldots, A) = B - c_s - f(M/N)$ if and only if $f(M/N) < B - c_s + c$. For $s_i^* = A$, $u_i(S, A, \ldots, A) = 0 > u_i(S, A, \ldots, S, A, \ldots, A) = B - c_s - f(M/N)$ for all $f(M/N) > B - c_s$, which is always the case, assuming $B < c_s$. The Lemma follows. □

Even though both payoffs are negative, if self-sacrificing is still better than voting and the retaliation risk is contained, then the revocation is performed by only one player, because it is in the best interest of all other players to avoid wasting certificates and thus to abstain.

Lemma 4. *In* G_n^f, *for* $[(B < c_s) \wedge (b < v)] \wedge [b - v - e(M/N) > B - c_s - f(M/N)]$, *if* $e(M/N) < b - v + c$ *then the NE are all strategy profiles that have (a) one self-sacrifice with* $n-1$ *abstentions and (b)* n_v *votes with* $n - n_v$ *abstentions. If* $e(M/N) \geqslant b - v + c$ *then (b) is not anymore a NE. The accused node is revoked by any NE.*

Proof. For the case (a), the proof is analogous to the one of Lemma 2. For the case (b), we consider the strategy profile s^* that has exactly n_v votes and $n - n_v$ abstentions. Without loss of generality, we assume that the first n_v players vote and the remaining players abstain. We refer to a voting player as i and to an abstaining player as j.

$$\begin{aligned}
&\text{If } s_1^* = V : u_1(s_1^*, \ldots, V, A, \ldots, A) = b - v - e(M/N),\\
&\qquad u_1(A, V, \ldots, V, A, \ldots, A) = -c,\\
&\qquad u_1(S, V, \ldots, V, A, \ldots, A) = B - c_s - f(M/N),\\
&\text{If } s_n^* = A : u_1(V, \ldots, V, A, \ldots, s_n^*) = 0,\\
&\qquad u_n(V, \ldots, V, A, \ldots, V) = b - v - e(M/N),\\
&\qquad u_n(V, \ldots, V, A, \ldots, S) = B - c_s - f(M/N).
\end{aligned}$$

According to the conditions of the Lemma, we have that $s_i = V$ is better than $s_i = S$ for any voting player i. Similarly, we see that $s_i = V$ is also better than $s_i = A$ if and only if $b - v - e(M/N) > -c$, or if $e(M/N) < b - v + c$. Moreover, $s_j = A$ is better than $s_j = V$ or $s_j = S$ for any abstaining player j. Therefore, the strategy profile s^* with exactly n_v votes and $n - n_v$ abstentions is a NE if and only if $e(M/N) < b - v - c$, otherwise s^* is not a NE. □

Intuitively, if the risk of retaliation for a voting node is contained, the revocation could also be performed by the strict minimum number of voters n_v, without any self-sacrifice. If the risk is higher, then no voting strategy profile is a NE.

Most of the NE defined by the precedent lemmas guarantee the revocation of the accused node's certificate. However, when costs are greater than benefits, the rational strategies do not predict any unnecessary waste of valid certificates by the players. Only the strict minimal number of voters n_v or exactly *one* self-sacrifice is selected as NE of the game. The main drawback is, however, that in all cases we have more than one possible NE by which the game could end. If active players bear a positive cost, those who abstain benefit from the effort of the others without having to pay for it. Thus, every node would prefer to be one of the abstaining players and enjoy the benefits without contributing to the well-being of the community. The decision about which player should choose which strategy is addressed in the following subsections, by taking into account the past behavior of each node when computing individual payoffs. We first discuss the number of votes n_v and then we focus on self-sacrifice costs $c_{s,i}$.

5.2. Dynamic vote

Previously, we assumed that n_v was a fixed value, e.g. the *majority* of players, as we did not consider reputations. By accounting for past behavior, however, we can determine the number of necessary votes for a successful revocation depending on the device that actually uses the *vote* strategy and the reputation of the accused node. For instance, one vote by a node with a higher reputation than

the accused might be enough to successfully revoke the certificate (thus $n_v = 1$), whereas several nodes might need to vote if their counter is not greater than the one of the accused device ($n_v > 1$).

We now assume that a revocation is successful when (a) $\sum_{i:s_i=V} u_i^- \geqslant u_m^-$, i.e. if the sum of counters of the players that vote is greater than the accused node's counter, or when (b) there is at least one self-sacrificing player. We see that, for any given strategy profile $s = \{s_i\}_{i=1}^n$, the actual reputation of the nodes performing the vote strategy determines n_v. For simplicity of future notation, for each strategy profile $s_{-i} = (s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_n)$, we define the sum of counters of all players k (other than i) that choose to *vote* as

$$\gamma(s_{-i}) = \sum_{k \neq i : s_k = V} u_k^-.$$

5.3. Retaliation attack cost functions

For each revocation game against a malicious node, there is a risk that the accused nodes might collude and/or respond to the revocation by accusing the benign nodes. The more malicious nodes are present in a given area, the more costly (or risky) it becomes for benign nodes to revoke them. Each participant in the revocation game has two decisive actions (vote or commit self-sacrifice) that have different strengths: one vote is usually not sufficient for a revocation, as opposed to one self-sacrifice which is entirely sufficient. Thus, the self-sacrifice strategy is more risky to adopt because it is very easy for the malicious nodes to identify the unique player that committed self-sacrifice and retaliate against it. Therefore, we assume that $0 < e(M/N) < f(M/N)$.

We choose $f(M/N) = M/N$ and $e(M/N) = z \cdot M/N$, $0 < z \ll 1$, to model the retaliation attack cost functions in our games. They assure that in each revocation game, if M/N is high, the nodes will carefully consider their actions before committing to them.

5.4. Self-sacrifice cost function

If we consider the self-sacrifice strategy, we know that only *one* such strategy is sufficient to revoke the accused node. Thus, the extreme power associated with its use should depend on the past behavior of each node. We make the plausible assumption that a node with a high counter has most likely behaved correctly in the past and did not abuse the revocations, whereas a node with a low counter has probably misbehaved. The well-behaving node has a better reputation and should be given a greater incentive to perform the self-sacrifice. The misbehaving node should have to pay an extremely high price for self-sacrificing, which would ultimately deplete its counter and remove it automatically from the network. This would limit the abuse and ensure that misbehavior is quickly extinguished.

We model the self-sacrifice cost $c_{s,i}$ by a linear function of the counter u_i^-, i.e. $c_{s,i} = h - g \cdot u_i^-$. We tested several concave and convex functions for which the cost decreases monotonically with the counter. We chose the linear model because it provides a good balance between the higher costs determined by a concave function and the lower costs dictated by a convex one. The two parameters of $c_{s,i}$ to fine tune are $h > 0$ and $g > 0$. We begin by delineating the best response functions for a player i, assuming that $b - v - e(M/N) > -c$, i.e. the payoff for a successful vote is greater than the cost of abstaining in case the accused node is not revoked. The NE profiles are then obtained by the set of mutual best responses. The following lemmas define the scenarios where (1) the revocation does not succeed even if i votes, (2) the revocation succeeds if i votes and (3) the revocation succeeds even if i abstains.

Lemma 5. *If s_{-i} is such that $u_i^- + \gamma(s_{-i}) < u_m^-$ and in absence of a self-sacrifice, the best response function for any player i is defined as*

$$br_i(s_{-i}) = \arg\max_{s_i \in \{A,V,S\}} u_i(s_i, s_{-i}) = \begin{cases} A & \text{if } u_i^- < \tau_1, \\ S & \text{otherwise}, \end{cases}$$

where $\tau_1 = \frac{h - B - c + f(M/N)}{g}$.

Proof. We look at the payoff functions for the different possible s_i, given all s_{-i} that respect the condition of the lemma.

$$\begin{aligned} &s_i = A \quad u_i(A, s_{-i}) = -c, \\ &s_i = V \quad u_i(V, s_{-i}) = -c - v - e(M/N), \\ &s_i = S \quad u_i(S, s_{-i}) = B - h + g \cdot u_i^- - f(M/N). \end{aligned}$$

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 $B - h + g \cdot u_i^- - f(M/N) > -c$ we have that the best response of player i is to *abstain* if $u_i^- < \frac{h - c - B + f(M/N)}{g}$ and to *self-sacrifice* otherwise. □

Lemma 6. *If s_{-i} is such that $u_i^- + \gamma(s_{-i}) \geqslant u_m^-$ and in absence of a self-sacrifice, the best response function for any player i is defined as*

$$br_i(s_{-i}) = \begin{cases} V & \text{if } u_i^- < \tau_2, \\ S & \text{otherwise}, \end{cases}$$

where $\tau_2 = \frac{h - B - v + b - e(M/N) + f(M/N)}{g}$.

Proof. The proof is analogous to the one of Lemma 5. □

Lemma 7. *If s_{-i} is such that $\gamma(s_{-i}) \geqslant u_m^-$ or it has at least one self-sacrifice, the best response function for any player i is defined as*

$$br_i(s_{-i}) = \begin{cases} A & \text{if } b - v < e(M/N) \wedge u_i^- < \tau_3, \\ V & \text{if } b - v > e(M/N) \wedge u_i^- < \tau_2, \\ S & \text{if } (b - v < e(M/N) \wedge u_i^- \geqslant \tau_3), \\ & \cup (b - v > e(M/N) \wedge u_i^- \geqslant \tau_2), \end{cases}$$

where $\tau_3 = \frac{h - B + f(M/N)}{g}$.

Proof. The proof is analogous to the one of Lemma 5. □

Thanks to the best response functions, we can already fine tune h such that $\min(\tau_1,\tau_2)>0$ as $u_i^- \geqslant 0$, which yields $h > B + c - f(M/N)$. In addition, we are now able to impose the following three conditions on the game parameters:

(1) *Positive cost*. We want that $c_{s,i} + f(M/N) > 0$ for all players P_i, otherwise it would encourage the abuse of self-sacrifice by malicious against benign nodes.

$$c_{s,i} = h - g \cdot u_i^- + f(M/N) > 0, \quad \forall i = 1 \ldots, n,$$

which is equivalent to

$$\begin{aligned} &c_{s,i} = h - g \cdot \max_i u_i^- + f(M/N) > 0, \\ &\frac{h + f(M/N)}{\max_i u_i^-} > g. \end{aligned} \tag{1}$$

(2) *Guaranteed revocation*. Considering s_{-i} of Lemma 5, we do not want *abstain* to be a best response for at least one player, otherwise the accused node would not be revoked. In other terms, we need that

$$\begin{aligned} &\max_i u_i^- > \frac{h - B - c + f(M/N)}{g}, \\ &g > \frac{h - B - c + f(M/N)}{\max_i u_i^-}. \end{aligned} \tag{2}$$

This requirement is essential if we want to protect ourselves in case the estimation of the cost parameters associated with the attack of the accused node is difficult or prone to errors.

(3) *System-wide efficiency*. Considering s_{-i} of Lemma 7, we do not want *self-sacrifice* to be a best response. The malicious node would be revoked anyway, even if i abstains (and thus does not incur in any costs). We can guarantee this by setting the largest threshold of the game lower than the maximum counter.

(a) If $b - v < e(M/N)$:

$$\begin{aligned} &\max_i u_i^- < \tau_3, \\ &g < \frac{h - B + f(M/N)}{\max_i u_i^-} = \tau_4. \end{aligned} \tag{3}$$

(b) If $b - v \geqslant e(M/N)$:

$$\begin{aligned} &\max_i u_i^- < \tau_2, \\ &g < \frac{h - B - v + b - e(M/N) + f(M/N)}{\max_i u_i^-} = \tau_5. \end{aligned} \tag{4}$$

By merging the upper bounds (1), (3), (4) and the lower bound (2) we have.

- if $b - v < e(M/N)$:

$$\frac{h - B - c + f(M/N)}{\max_i u_i^-} < g < \tau_4,$$

- if $b - v \geqslant e(M/N)$:

$$\frac{h - B - c + f(M/N)}{\max_i u_i^-} < g < \tau_5.$$

In addition to the conditions (1)–(3) expressed previously, in the NE selection protocol *OREN* defined in Section 6 we require the existence of at least one NE strategy profile. Thanks to bounds on the cost parameters h and g, we state the following Theorem for $b - v < e(M/N)$ (when $b - v > e(M/N)$, the solution is trivial because there is always a unique NE, according to Lemma 1):

Theorem 1. *In* G_n, *for* $b - v < e(M/N)$, *there is always 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. 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 5.4 for h and g, we show that s^* is always a NE.

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:

$$\begin{aligned} &u_{P_A}(A, s_{-i}) = u_{P_A,(A,s_{-i})} = 0, \\ &u_{P_A}(V, s_{-i}) = u_{P_A,(V,s_{-i})} = b - v - e(M/N), \\ &u_{P_A}(S, s_{-i}) = u_{P_A,(S,s_{-i})} = B - c_{s,P_A} - f(M/N). \end{aligned}$$

Here, we can already exclude the second possibility as the corresponding payoff is always smaller than the other two. Moreover, we can see that

$$\begin{aligned} &u_{P_A,(S,s_{-i})} - u_{P_A,(A,s_{-i})} \\ &= B - c_{s,P_A} - f(M/N) \overset{(a)}{<} B - h + \frac{h - B + f(M/N)}{\max_i u_i} \cdot u_{P_A}^- \\ &\quad - f(M/N) = \left(1 - \frac{u_{P_A}^-}{\max_i u_i}\right)(B - h - f(M/N)) \\ &\quad \overset{(b)}{<} \underbrace{\left(1 - \frac{u_{P_A}^-}{\max_i u_i}\right)}_{>0}(B - B - c + f(M/N) - f(M/N)) \\ &= \left(1 - \frac{u_{P_A}^-}{\max_i u_i}\right)(-c) < 0 \rightarrow u_{P_A,(S,s_{-i})} < u_{P_A,(A,s_{-i})}, \end{aligned}$$

where *(a)* follows from the lower bound (3) and *(b)* from the fine tuning of h, i.e. $h > B + c - f(M/N)$. Therefore, no player P_A has incentive to unilaterally deviate from his equilibrium strategy *abstain*.

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

$$\begin{aligned} &u_{P_S}(A, s_{-i}) = u_{P_S,(A,s_{-i})} = -c, \\ &u_{P_S}(V, s_{-i}) = u_{P_S,(V,s_{-i})} = -c - v - e(M/N), \\ &u_{P_S}(S, s_{-i}) = u_{P_S,(S,s_{-i})} = B - c_{s,P_S} - f(M/N). \end{aligned}$$

Again, to *vote* is not an option for P_S since the strategy *abstain* would always give him a better payoff. Furthermore, we have

$$
\begin{aligned}
&u_{P_S,(S,s_{-i})} - u_{P_S,(A,s_{-i})} \\
&= B - c_{s,P_S} - f(M/N) + c \\
&= B - h + g \cdot u^-_{P_S} - f(M/N) + c \overset{(c)}{>} B - h \\
&\quad + \frac{h - B - c + f(M/N)}{\max_i u_i^-} \cdot u^-_{P_S} - f(M/N) + c \overset{(d)}{=} B - h \\
&\quad + \frac{h - B - c + f(M/N)}{u^-_{P_S}} \cdot u^-_{P_S} - f(M/N) + c = 0,
\end{aligned}
$$

where *(c)* follows from the lower bound (2) and *(d)* from $u^-_{P_S} = \max_i u_i^-$. Summing up, we have that

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

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. □

6. Social welfare and protocols

In this section, we describe the method that we use to select a single NE, in case more are present, with the related protocols. The underlying principle is that of the *price of anarchy* [22], 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:

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

$$\text{Egalitarian}: \ \omega(s) = \min_i u_i(s).$$

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

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

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^*

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

The idea is that it gives a measure of how well selfish players (NE) perform compared to the social optimum. To solve the issue and help players make consistent decisions, i.e. to select 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^*, because we are interested in selecting one NE that is optimal with respect to the given ω. Consequently, all players will be able to make independent, but mutually consistent, decisions about a unique NE.

We now describe the unique optimal NE selection protocol *OREN* that is run during the revocation process, as described in Section 4.

First of all, each player computes all NE as the first step of the OREN protocol. Knowing the optimized game parameters, nodes can use heuristics to immediately discard all strategy combinations that do not result in a revocation or that are inefficient, thus reducing the time required for the NE computations. If more than one NE exists, the second protocol OptNE is executed and the set G of all NE satisfying the optimality criteria (utilitarian → egalitarian or *vice versa*) defined by the variable *firstOptCond* is determined. We choose the *utilitarian* criteria first because it compares the aggregate utilities of all players at once, as opposed to the one-to-many comparison of each utility, for all NE, done by the *egalitarian* criteria. The first protocol 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 selects one optimal NE from the set G at random and broadcasts it to all participants. The final output of the two protocols is the unique socially optimal NE profile s^*. By agreeing on this NE, all players are guaranteed not to pay the extra cost c that would result from the failed revocation and to receive rewards from the CA.

Protocol 1: OREN

```
1: AllNE={s|s ∈ NE}
2: if |AllNE| = 1 then
3:     s*= getNext(AllNE)
4: else
5:     G = OptNE(utilitarian, AllNE)
6:     if |G| = 1 then
7:         s*= getNext(G)
8:     else
9:         G = OptNE(egalitarian, AllNE)
10:        if |G| = 1 then
11:            s*= getNext(G)
12:        else
13:            if thisNodeID = initiatorID then
14:                s*= InitiatorSelectOpt(G)
15:                Broadcast(s*)
16:            else
17:                s*= ReceiveOpt(initiatorID)
18:            end if
19:        end if
20:    end if
21: end if
```

Protocol 2: OptNE(*firstOptCond*, *AllNE*)

```
1: if firstOptCond="utilitarian" then
2:     ω1(s) = Σ_{i=0}^{n} u_i(s)
3:     ω2(s) = min_i u_i(s)
4: else
5:     ω1(s) = min_i u_i(s)
6:     ω2(s) = Σ_{i=0}^{n} u_i(s)
7: end if
8: G1 = {s|s = argmax_{s∈AllNE}[ω1(s)]}
9: if |G1| = 1 then
```

Protocol 2 (*continued*)

Protocol 2: OptNE(*firstOptCond, AllNE*)

10: $G = G_1$
11: **else**
12: $G_2 = \{s | s = argmax_{s \in G_1}[\omega_2(s)]\}$
13: $G = G_2$
14: **end if**
15: **return** G

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

7. Performance evaluation

We implemented and simulated the optimal NE selection protocol *OREN* in *Matlab*, assuming a single attacker, although there could be as many attackers as revocation games running in parallel. We run 10 iterations for each number of players between 2 and 15, as we assume a highly mobile environment and short-range communications. The confidence interval is 95%. As in Section 5.4 for the system-wise efficiency of the self-sacrifice cost $c_{s,i}$, we assume here that $b - v < e(M/N)$ in order to avoid any unnecessary effort due to the use of the vote strategy as well. The exact game parameters are:

- $u_i^- \in [0, 10]$ uniformly at random, where we use the same maximum value through all subsequent simulations.
- $h = 4.5 > B = 1 > c = 0.5 > v = 0.3 > b = 0.2$ [certificates], $z = 0.25$.
- $g = \frac{2(h-B+f(M/N))-c}{2 \cdot \max_i u_i^-}$ is the middle point between the lower (2) and upper bounds (3) to the slope of $c_{s,i}$. The ratio of malicious/total nodes is $M/N = 0$ and $M/N = 0.3$.

The main results are discussed in the following subsections.

7.1. Number of Nash equilibria

In Fig. 3 we see that by using the dynamic vote, the number of vote NE is only 1/25 of the number obtained when using the majority vote for 15 players. This comes from the fact that there are fewer combinations of players whose aggregate votes would result in a successful revocation, compared to any combination of the majority of players in the other case. The impact of the presence of colluding malicious nodes that could retaliate against the players is negligible.

We notice that the number of self-sacrifice NE is the same in both systems, because the self-sacrifice strategy is limited to the one or two players that have the highest counter and does not depend on the voting scheme being used.

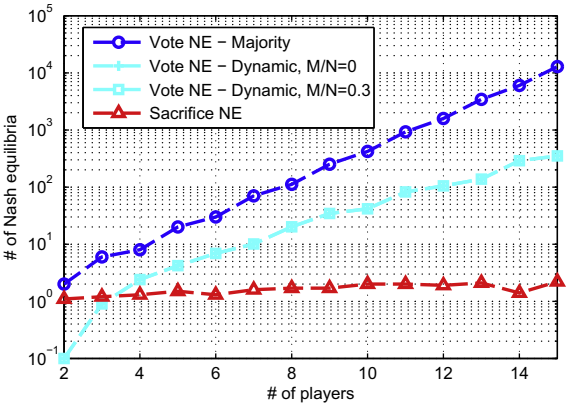

Fig. 3. Average number of Nash equilibria.

7.2. Number of votes for revocation

Fig. 4 shows the number of players that are required to vote in order to revoke the accused node's certificate. For the majority vote, the number of votes increases with the total number of players, irrespective of their reputations.

With the dynamic vote, on the contrary, we see that the number of votes tends to decrease as the number of players increases. Thanks to the greater diversity of counters as the number of players increases, it becomes easier to find few players with high counters (or reputations), such that the vote NE becomes socially less costly. If the game were to end by voting, only these few players would need to vote, compared to the greater number of players needed by the majority and the consequently higher social cost.

7.3. Type of selected Nash equilibrium

Fig. 5 shows the percentage of *vote* NE that have been selected as the unique optimal NE by the protocols for, respectively, majority and dynamic votes. The percentage of selected optimal *self-sacrifice* NE is simply the difference between 100% and the vote NE selection percentage.

With majority votes, the vote NE is dominant in games with less than 4 players, whereas with 4 players and more, the self-sacrifice takes over. This is justified by the social

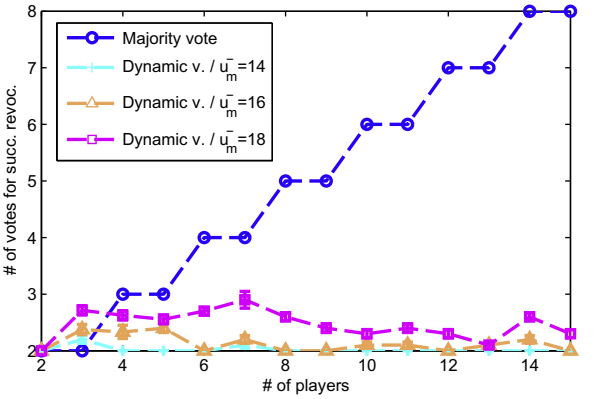

Fig. 4. Number of votes required for a successful revocation.

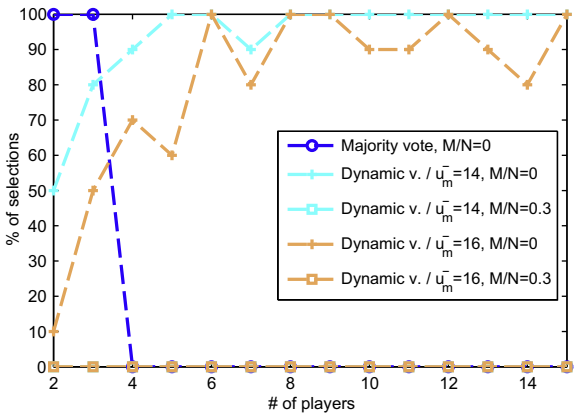

Fig. 5. Percentage of vote Nash equilibrium selections.

optimality criteria as the vote NE will be less socially costly than the sacrifice if and only if $(b - v) \cdot n_v > -c/2$. For our parameters, we have that the inequality holds if $n_v \leqslant 2$, meaning that up to three players, a vote is less costly as the majority is $n_v = 2$, and afterwards it becomes more costly and therefore the self-sacrifice strategy is selected.

With dynamic votes, we see that for relatively low u_m^-, the vote NE is dominant with respect to the self-sacrifice because very few players are needed to vote and, as explained earlier, the vote is more socially optimal if and only if the two most wealthy players are sufficient to revoke the accused node. When u_m^- increases, more players would be needed for the revocation by vote and if most of them have a relatively low u_i^-, it might not even be feasible. In this case, the self-sacrifice strategy would be the only option. Finally, we see that by increasing the number of players, there are more chances of finding players with relatively high u_i^- and thus revocation by vote would be less costly than self-sacrifice.

When the number of colluding malicious nodes increases, the revocation is done by self-sacrifice. Given our parameters, it is socially less costly to risk the revocation of one benign node that committed self-sacrifice than two devices that voted.

7.4. Optimality criteria

Fig. 6 shows the behavior of the revocation process with respect to the optimality criteria that is chosen. *OREN* uses two criteria for selecting the optimal NE: The *utilitarian*, which maximizes the sum of individual payoffs, and the *egalitarian*, which maximizes the minimum payoff among the participants. Additionally, the initiator of the revocation has the ability to select one NE among the set of optimal NE at the end of the computations, but only if several equivalent such equilibria exist.

As it can be seen, when the accused node has a relatively bad record of past behavior, i.e., a small u_m^-, there are several optimal NE that can be selected at the end of the revocation process. In this case, the initiator of the revocation process chooses one optimal NE (from the set of optimal NE that has been identified by each participant in the process) and instructs the other participants of this

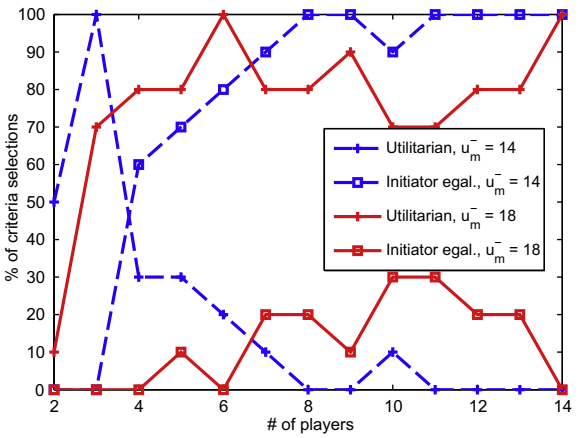

Fig. 6. Percentage of the different optimality criteria selections for the unique Nash equilibrium. The *utilitarian* criterion is the first to be evaluated in *OREN*, and the egalitarian NE selected by the initiator is the last criterion of *OREN*.

choice. However, when the accused device has a relatively good record of past behavior, i.e., a larger u_m^-, *OREN* finds the unique optimal NE autonomously, facilitating the successful revocation of the accused node in scenarios with high node mobility and unreliable communications.

7.5. Duration of simulation

Fig. 7 shows the average duration of the *OREN* protocol simulation, assuming that a dedicated hardware is available for the computations. This specialized hardware helps reducing the total time of heterogeneous computations by at least a factor of six [23] when compared to general purpose CPUs (with a processing power similar to that of current CPUs found on mobile devices). As it can be seen from Fig. 7, by using dedicated hardware it would take at most 1.5 s (on average) to determine the unique optimal NE for a revocation game with 10 players. Considering the ephemeral network model under examination, this result is satisfactory. However, as finding an optimal NE is hard in general [21], further research might be required in order to extend *OREN* to larger-scale networks.

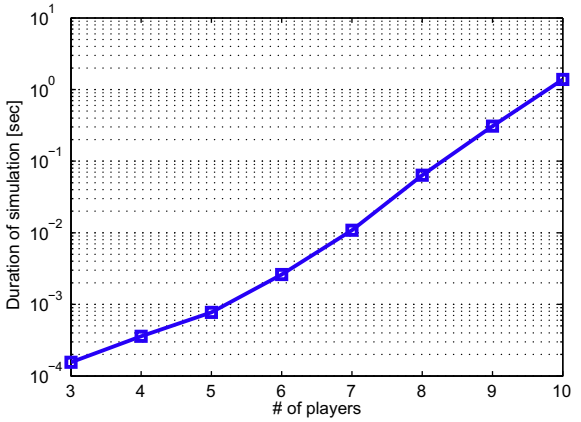

Fig. 7. Average duration of the *OREN* simulation, assuming that a dedicated hardware is available for the computations [23].

8. Conclusion

In this paper, we have designed a game-theoretic framework for local certificate revocation in ephemeral networks. First, the scheme makes use of incentives in order to guarantee the revocation of the malicious node even in presence of inaccurate estimation of the attack-induced cost. Second, the scheme makes also use of reputations, based on each node's past behavior, and we have optimized the game model such that the adapted cost parameters guarantee a successful revocation of the malicious node in the most socially efficient way.

Based on the analytical results, we have then designed a novel reputation-based on-the-fly local revocation scheme that establishes a unique optimal Nash equilibrium in a distributed fashion. Simulation results have illustrated that, by considering the past behavior of all parties involved in the process, our revocation protocols are effective in determining the unique most efficient outcome that is also socially optimal, i.e. that generates the least costs for the community of players.

As part of future work, we intend to extend our game-theoretic model to other breeds of networks with similar characteristics, and to include role attribution to a subset of players, where hierarchy and past behavior will be considered while determining the outcome of the revocation games.

Acknowledgments

We would like to express our sincere gratitude to Tansu Alpcan, Georgios Theodorakopoulos, Mathias Humbert, Marcin Poturalski and to the anonymous reviewers who contributed to improve the quality of this work.

References

[1] AKAAKI. <http://www.aka-aki.com/> (accessed 20.07.2010).
[2] BlueStar*. <http://www.csg.ethz.ch/research/projects/Blue_star> (accessed 20.07.2010).
[3] Serendipity. <http://reality.media.mit.edu/serendipity.php> (accessed 20.07.2010).
[4] J. Katz, Bridging game theory and cryptography: recent results and future directions, in: TCC'08: Proceedings of the 5th Conference on Theory of Cryptography, Springer-Verlag, Berlin, Heidelberg, 2008, pp. 251–272.
[5] L. Buttyan, J. Hubaux, Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing, Cambridge University Press, 2008.
[6] M. Raya, M.H. Manshaei, M. Félegyhazi, J.-P. Hubaux, Revocation games in ephemeral networks, in: CCS'08: Proceedings of the 15th ACM Conference on Computer and Communications security, ACM, New York, NY, USA, 2008, pp. 199–210.
[7] R. Li, J. Li, H. Kameda, P. Liu, Localized public-key management for mobile ad hoc networks, in: GLOBECOM '04: Global Telecommunications Conference, vol. 2, pp. 1284–1289.
[8] H. Luo, P. Zerfos, J. Kong, S. Lu, L. Zhang, Self-securing ad hoc wireless networks, in: ISCC 2002: Proceedings of the Seventh International Symposium on Computers and Communications, pp. 567–574.
[9] S. Chinni, J. Thomas, G. Ghinea, Z. Shen, Trust model for certificate revocation in ad hoc networks, Ad Hoc Networks 6 (2008) 441–457.
[10] G. Arboit, C. Crépeau, C.R. Davis, M. Maheswaran, A localized certificate revocation scheme for mobile ad hoc networks, Ad Hoc Networks 6 (2008) 17–31.
[11] P. Michiardi, R. Molva, Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks, in: Advanced Communications and Multimedia Security: IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security, September 26–27, 2002, Portorož, Slovenia, Kluwer Academic, 2002, pp. 107–121.
[12] S. Reidt, M. Srivatsa, S. Balfe, The fable of the bees: incentivizing robust revocation decision making in ad hoc networks, in: CCS'09: Proceedings of the 16th ACM Conference on Computer and Communications security, ACM, New York, NY, USA, 2009, pp. 291–302.
[13] WPKI, Wireless public key infrastructure – specification. <http://www.signature.lt/KK/wPKI-specification.pdf> (accessed 20.07.2007).
[14] Ietf rfc 2459. (accessed 20.07.2010).
[15] M. Gruteser, D. Grunwald, Enhancing location privacy in wireless lan through disposable interface identifiers: a quantitative analysis, Mobile Networks and Applications 10 (2005) 315–325.
[16] A. Beresford, F. Stajano, Location privacy in pervasive computing, IEEE Pervasive Computing 2 (2003) 46–55.
[17] H. Yang, H. Luo, F. Ye, S. Lu, L. Zhang, Security in mobile ad hoc networks: challenges and solutions, IEEE Wireless Communications 11 (2004) 38–47.
[18] H. Yang, J. Shu, X. Meng, S. Lu, Scan: self-organized network-layer security in mobile ad hoc networks, IEEE Journal on Selected Areas in Communications 24 (2006) 261–273.
[19] S. Radosavac, J.S. Baras, I. Koutsopoulos, A framework for mac protocol misbehavior detection in wireless networks, in: WiSe'05: Proceedings of the 4th ACM Workshop on Wireless Security, ACM, New York, NY, USA, 2005, pp. 33–42.
[20] T. Moore, J. Clulow, S. Nagaraja, R. Anderson, New strategies for revocation in ad-hoc networks, in: ESAS'07: Proceedings of the 4th European Conference on Security and Privacy in Ad-Hoc and Sensor Networks, Springer-Verlag, Berlin, Heidelberg, 2007, pp. 232–246.
[21] C. Daskalakis, P.W. Goldberg, C.H. Papadimitriou, The complexity of computing a Nash equilibrium, Communications of the ACM 52 (2009) 89–97.
[22] T. Roughgarden, Selfish Routing and the Price of Anarchy, The MIT Press, 2005.
[23] A. Marongiu, P. Palazzari, V. Rosato, Parallel dedicated hardware devices for heterogeneous computations, in: Proceedings of the ACM/IEEE Supercomputing Conference (SC01), 2001.

Igor Bilogrevic is a research assistant and Ph.D student at the Laboratory for computer Communications and Applications (LCA1), at the Ecole Polytechnique Fédérate de Lausanne (EPFL), under the supervision of Prof. Jean-Pierre Hubaux. He earned his M.Sc. and B.Sc. in communication systems from EPFL in 2009 and 2007 respectively, with specialization in Wireless Communications. Igor's main areas of interest include wireless networks and, in particular, security and privacy issues thereof. http://people.epfl.ch/igor.bilogrevic.

Mohammad Hossein Manshaei earned his B.S. degree in electrical engineering and his M.S. degree in communication engineering from the Isfahan University of Technology (IUT), Iran, in 1997 and 2000, respectively. He earned another M.S. degree in computer science and his Ph.D. in computer science and distributed systems from the University of Nice Sophia-Antipolis, France, in 2002 and 2005, respectively. He completed his thesis work at INRIA Sophia- Antipolis. He currently works as a senior researcher and lecturer at the Laboratory for Computer Communications and Applications (LCA) in EPFL. His research interests include wireless networking, security and privacy, social networks, cognitive radios, and game theory. http://people.epfl.ch/manshaei.

Maxim Raya received his B.Eng. degree in Computer and Communications Engineering in 2002 from the American University of Beirut, Lebanon. He earned his Ph.D degree from EPFL in 2009. His research interests are in the area of security in wireless networks, and especially vehicular networks. He served in the program committee of VANET 2007.

Jean-Pierre Hubaux joined the faculty of EPFL in 1990. His research activity is focused on wireless networks, with a special interest in security and cooperation issues. In 1991, he designed the first curriculum in Communication Systems at EPFL. He was promoted to full professor in 1996. In 1999, he defined some of the main ideas of the National Competence Center in Research named "Mobile Information and Communication Systems" (NCCR/MICS). In this framework, he has notably defined, in close collaboration with his students, novel schemes for the security and cooperation in wireless networks; in particular, he has devised new techniques for key management, secure positioning, and incentives for cooperation in such networks. In 2003, he identified the security of vehicular networks as one of the main research challenges for real-world mobile ad hoc networks. In 2008, he completed a graduate textbook entitled "Security and Cooperation in Wireless Networks", with Levente Buttyan. Most of his current research activities revolve around privacy issues in mobile networks and are partially funded by Nokia. He is co-founder and chairman of the steering committee of WiSec (the ACM Conference for Wireless Network Security). He has served on the program committees of numerous conferences and workshops, including SIGCOMM, INFOCOM, MobiCom, MobiHoc, SenSys, WiSe, and VANET. Since 2007, he has been one of the seven commissioners of the Federal Communications Commission (ComCom), the "Swiss FCC". He held visiting positions at the IBM T.J. Watson Research Center and at UC Berkeley. He has been on the advisory board of Deutsche Telekom Laboratories (T-Labs) since their creation in 2004. He is a Fellow of both IEEE and ACM. He was born in Belgium, but spent most of his childhood and youth in Northern Italy. After completing his studies in electrical engineering at Politecnico di Milano, he worked 10 years in France with Alcatel, primarily in the area of switching systems architecture and software.