sensors

MDPI

Article

Game Theoretic Honeypot Deployment in Smart Grid

Panagiotis Diamantoulakis [1], **Christos Dalamagkas** [2], **Panagiotis Radoglou-Grammatikis** [3], **Panagiotis Sarigiannidis** [3,*] **and George Karagiannidis** [1]

1   Department of Electrical and Computer Engineering, Aristotle University of Thessaloniki, 54124 Thessaloniki, Greece; padiaman@auth.gr (P.D.); geokarag@auth.gr (G.K.)
2   Testing, Research and Standards Centre, Public Power Corporation S.A., 15351 Athens, Greece; c.dalamagkas@dei.com.gr
3   Department of Electrical and Computer Engineering, University of Western Macedonia, 50100 Kozani, Greece; pradoglou@uowm.gr
*   Correspondence: psarigiannidis@uowm.gr

check for updates

Abstract: The smart grid provides advanced functionalities, including real-time monitoring, dynamic energy management, advanced pricing mechanisms, and self-healing, by enabling the two-way flow of power and data, as well as the use of Internet of Things (IoT) technologies and devices. However, converting the traditional power grids to smart grids poses severe security challenges and makes their components and services prone to cyber attacks. To this end, advanced techniques are required to mitigate the impact of the potential attacks. In this paper, we investigate the use of honeypots, which are considered to mimic the common services of the smart grid and are able to detect unauthorized accesses, collect evidence, and help hide the real devices. More specifically, the interaction of an attacker and a defender is considered, who both optimize the number of attacks and the defending system configuration, i.e., the number of real devices and honeypots, respectively, with the aim to maximize their individual payoffs. To solve this problem, game theoretic tools are used, considering an one-shot game and a repeated game with uncertainty about the payoff of the attacker, where the Nash Equilibrium (NE) and the Bayesian NE are derived, respectively. Finally, simulation results are provided, which illustrate the effectiveness of the proposed framework.

1. Introduction

The recent adoption of innovative Internet of Things (IoT) technologies and products led to the evolution of several domains of critical infrastructures, including health, transportation, and utilities. Power grids, in particular, have been enhanced with Information and Communication Technologies (ICT) at operational and resiliency level with new smart functionalities, including real-time monitoring, smart management, smart customer billing, and provisioning of resources to normalize fluctuations and address unexpected events. Smart meters, phasor measurement units, smart relays, remote terminal units (RTUs), and Programmable Logic Controllers (PLCs) are only a few of the IoT devices that are utilized by energy operators in order to convert traditional power grids to smart grids.

However, the introduction of all these new IoT devices has side effects, including an increasing attack surface. According to the Cisco Annual Internet Report for 2018–2023 [1], it is estimated that Distributed Denial of Service (DDoS) attacks will double to 15.4 million by 2023, which is expressed in 14% Compound Annual Growth Rate (CAGR). The statistics coming from the energy sector are also worrisome. According to LNS Research, 53% of industrial stakeholders have reported experiencing a cyberattack in the last 12 months [2] and "76% of energy executives cited business interruption as the most impactful cyber loss scenario for their organization" [3]. It is evident that even though the

research on cybersecurity is progressing rapidly and the market stakeholders pursue the adoption of new cybersecurity products, cyber threats have an increasing trend.

The research community has provided innovative solutions to tackle cyber threats in the critical infrastructure and the energy domain, including intrusion detection systems and threat information sharing platforms that leverage Artificial Intelligence (AI) and modern cryptography techniques. The H2020-DS-SC7-2017 SPEAR: Secure and PrivatE smArt gRid project is a research project, funded by the European Commission, intends to provide a complete cybersecurity solution for modern smart grids by integrating AI-enabled anomaly detection, visual analytics, reputation schemes, forensic investigation frameworks, and deception mechanisms [4].

Even though security mechanisms like signature-based and behavioral-based anomaly detection dominate in the cybersecurity domain, honeypots are emerging as an alternative strategy to trap intelligent cyberattackers that bypass traditional security measures. A first widely accepted definition of honeypots is provided by Spitzner [5]: "A honeypot is a decoy computer resource whose value lies in being probed, attacked, or compromised." Honeypots are deployed by organizations to disorient cyberattackers that target the infrastructure in production and persuade them to attack the honeypots rather than the real infrastructure. This can serve multiple purposes: either to prevent attacks against the valuable assets or to collect intelligence about the attacker's activity. These deployment options are known as production and research honeypots, respectively [6].

A major drawback of honeypots is that, during their operation, they reserve resources in a constant manner, regardless of the attacker's activity, if any. Therefore, a large number of honeypots may lead to resource wastage, while a small number of honeypots may result to inefficient defenses to potential cyberattackers, thus resources are also wasted in this case as the invested resources do not accomplish their purpose. This practical quandary that security engineers face with honeypot orchestration is an active research issue, and game theory has been proposed to enable dynamic configuration of honeypots, by providing the optimal strategy for the defender, taking into account that the adversary is rational and tries to maximize his payoff. Our research aims to address the issue of honeypot orchestration by focusing on smart grid systems and considering their unique characteristics [7].

1.1. Related Works & Motivation

Game theory and its potential applications have been thoroughly studied in the context of cyber security [8] and honeypot deployment [9,10], although there is a lack of realistic schemes. The following paragraphs provide an overview of frameworks related to honeypot deployment and orchestration that were considered for our work.

Denial of Service (DoS) and Distributed DoS (DDoS) attack scenarios gain significant attention in the literature as their detection and mitigation is still an open research issue in the domain of cybersecurity. Thus, many of the existing game theory models focus on such type of attacks and provide specific strategies to confront such threats [11]. In more detail, Ceker et al. [12] have proposed a deception-based defense framework to tackle DoS attacks as well as threats that may employ unconventional stealth methods. The proposed framework provides a game-theoretical approach to model the interaction between the defender and the attacker, while a proactive deception mechanism is employed in this dynamic game to confuse the attacker about the defender's profile. The deception mechanism is based on a Bayesian signaling game of incomplete information, and the perfect Bayesian Equilibrium is utilized as a solution of the proposed framework that takes into consideration resource constraints. The analytical results study the relation between invested resources, processing cost, and the desired security level. Even though the proposed game provides a dynamic framework that scales to other kinds of attacks, except DoS, it is highlighted by the authors that several limitations apply, one of them is that legitimate users may be blocked by the defender, while the defender cost is constant and could be converted to a dynamic function that reflects the implications of the decided actions in a more realistic way.

Wang et al. [13] investigated the deployment of honeypots in an Advanced Metering Infrastructure (AMI), a typical network architecture utilized by Distribution System Operators (DSO) to obtain

measurements from smart meters in the modern smart grid. The proposed game aims to address DDoS attacks in the aforementioned network topology, and to this aim, they introduce a Bayesian game model to find the equilibrium between legitimate users and attackers. An AMI network with four service providers, 10 honeypots, and two anti-honeypots is simulated via OPNET to obtain evaluation results, which indicate the optimal number of honeypots to be deployed with the given parameters when a balance between detection rate and energy consumption is achieved. It is also highlighted by the authors that the effectiveness of the defense strategy does not necessarily improve when more honeypots are deployed.

The promising and innovative concept of Software-Defined Networks (SDN) is adopted in [14] to propose a game-theoretic framework that estimates the optimal strategies for both defenders and attackers, considering the balance between energy consumption and detection rate. As highlighted by the authors, the centralized nature of SDN makes the architecture susceptible to (D)DoS attacks, and the proposed model aims to deploy a defense mechanism against such attacks. Moreover, anti-honeypot attacks and pseudo-honeypot game strategies are introduced in this research to model and tackle DDoS attacks, respectively, resulting in several Bayesian Nash solutions. To evaluate the proposed model, a realistic testbed was constructed with hosts, attackers, and OpenFlow switches. The experimental results outperform in terms of performance in energy consumption and detection rate.

Al-Shaer et al. [15] proposed a different approach, compared to the previously mentioned references, that is based on the hypergame theory. The main motives of this perspective are the capabilities that are offered in terms of defense strategies for both proactive and reactive approaches as well as the limited contribution in the literature regarding mature and well-structured mathematical frameworks listing the hypergame concept. In the proposed work, an attack–defense model is structured with subjective beliefs in a dynamic environment, in which the defender tries to manipulate the attacker's belief utilizing deception techniques. Hypergame theory provides the ability to estimate the decision of each player and the impact that the uncertainty has on the expected utility. The deception model is studied by modeling a Stochastic Petri Net and the results deliver insightful findings that relate the perceptions by different players (i.e., an attacker or a defender) with their chosen optimal strategies and the corresponding utilities.

A Partially Observable Stochastic Game (POSG) was introduced in [16] that applies in situations where each player has partial information about the environment. In particular, the authors develop a POSG-based game theoretic framework to optimize honeypot deployment that assumes literal movement of the attacker in a computer network. The attacker and the defender are placed on a graph, in which nodes represent network hosts and the edges represent attacks against other hosts, with each attack incurring an associated cost. In this context, the attacker tries iteratively to attack hosts, while the defender chooses the edges that will act as honeypots. The experimental results prove that the POSG model was able to generate near-optimal deployment strategies as well as realistic and scalable networks of multiple hosts.

The authors of [17,18] proposed a game-theoretic framework that focuses on Cyber-Physical system (CPS) honeypots, with both low and high interaction. The proposed model is specifically used to deploy defensive mechanisms against Advanced Persistent Threats (APTs) in CPS and considers limited resources for honeypot allocation and human analysis as well as incomplete information for the players. Simulation results prove that the proposed model succeeds to maximize the defender's payoff and provides multiple Bayesian equilibria.

The authors of [19,20] used game theory to study various attacks and defense scenarios in networks with honeypots. Specifically, they utilize a Bayesian model to adequately reflect the defender's imperfect knowledge of user behavior (i.e., normal or malicious), thus forming a Bayesian signaling game of incomplete information. A one-shot game model is presented in order to determine how the defender should react to different user behaviors. Moreover, the authors provided a repeated version of this game that enables the players to update their opinions under a Bayes rule. Finally, mathematical analysis, as well as simulations, are used to find the equilibria and further evaluate the

model. The results suggest that when the defender is facing attacks with high frequency, the best action is to massively deploy honeypots. Otherwise, in the case of low-frequency attacks, the defender can mix up their strategy.

Finally, Bilinski et al. in [21] investigated the Nash Equilibrium (NE) of a honeynet system, in which the defender aims to protect a number of network hosts and has a fixed set of resources, therefore can defend only a limited number of hosts. On the contrary, the attacker can attack a specific number of hosts concurrently, although no cost is incurred to the adversary for each attack. In this context, the attacker is considered the winner if they attack a real host and not a honeypot, otherwise the defender wins. The analysis of the proposed model concludes that the value of a host is inversely proportional to the probability of the host to being attacked. However, certain limitations are remarked, including the fact that the attacker's activity is not limited by a cost function and that the proposed game assumes that the attacker wins the game if it attacks any host which is not a honeypot as well as that the number of served real devices is fixed, despite the fact that limited resources have been assumed. Finally, a similar scenario has been investigated in [22], assuming though that the defender has complete information about the attacker's payoff, a cost function for the attacker, and fixed number of served real devices, which has led to the formulation of a Stackelberg game. Moreover, in contrast in [21], the payoff of the attacker has been considered to be an increasing function of the number of attacked real devices.

1.2. Contribution

In this paper, game theory is used to model the interaction between an attacker and a defender, who makes use of honeypots to mitigate the impact of attacks within a smart grid. Taking into account the trade-off between connectivity and security, which is an important challenge in the smart grid, a novel framework is proposed according to which the defender has the option to periodically substitute part of the real devices with honeypots, e.g., for a portion of time, with the aim to deceive the attacker. More specifically, the defender optimizes the number of connected real devices and honeypots, taking into account the attacker's preferences. First, we focus on one encounter between the attacker and the defender, which is solved by using the concept of NE. Moreover, an alternative optimization framework is proposed for the case that the NE does not exist. Next, we extend the analysis considering a more sophisticated attacker, who randomizes its strategy, by attacking a random number of hosts, while also considering a repeated game and uncertainty about the attacker's payoff parameters. In this case, the interaction between the attacker and the defender is modeled as a multi-stage Bayesian game and the Bayesian NE is derived. Moreover, a rule to update the defender's belief about the type of the attacker is also provided. Finally, simulation results are provided to illustrate the effectiveness of the proposed framework.

1.3. Structure

The rest of the paper is organized as follows. The system model for the strategies and payoffs of the attacker and the defender is introduced in Section 2. In Section 3, the NE in the case of a one-shot game is derived, while the case that the NE does not exist is also discussed. In Section 4, the results of Section 3 are extended to the case of repeated games with uncertainty about the type of the attacker. Simulation results are given and discussed in Section 5. Finally, conclusions are summarized in Section 6.

2. System Model

A defending system is considered within a smart grid, hereinafter termed as a defender, that protects a collection of hosts from a potential attacker by using honeypots, which are able to detect unauthorized accesses, collect evidence, and help hide the real devices [13]. The honeypots are designed to mimic common services of the smart grid, including Industrial Control System (ICS) devices, smart meters, and smart appliances, among others [7]. Figure 1 depicts the most common

locations of attack threats and honeypots as well as real-life applications of the proposed model. In more detail, honeypots could be deployed in Supervisory Control and Data Acquisition (SCADA) networks, located in smart factories, power plants, and Distributed Energy Resources (DERs), to mimic various ICS devices, including Programmable Logic Controllers (PLCs), sensors, and smart relays, among others [23]. Moreover, honeypots could be deployed in substations owned by Transmission System Operators (TSO) or Distribution System Operators (DSO) to emulate more advanced ICS devices, including Remote Terminal Units (RTUs) and Phasor Measurement Units (PMUs). Finally, honeypots could be applicable in smart buildings to emulate smart appliances and energy meters or in Advanced Metering Infrastructures (AMIs), operated by DSOs, to emulate smart meters [24]. It is assumed that the defender has a fixed set of resources and, as a result, is only able to defend a limited number of hosts [21].
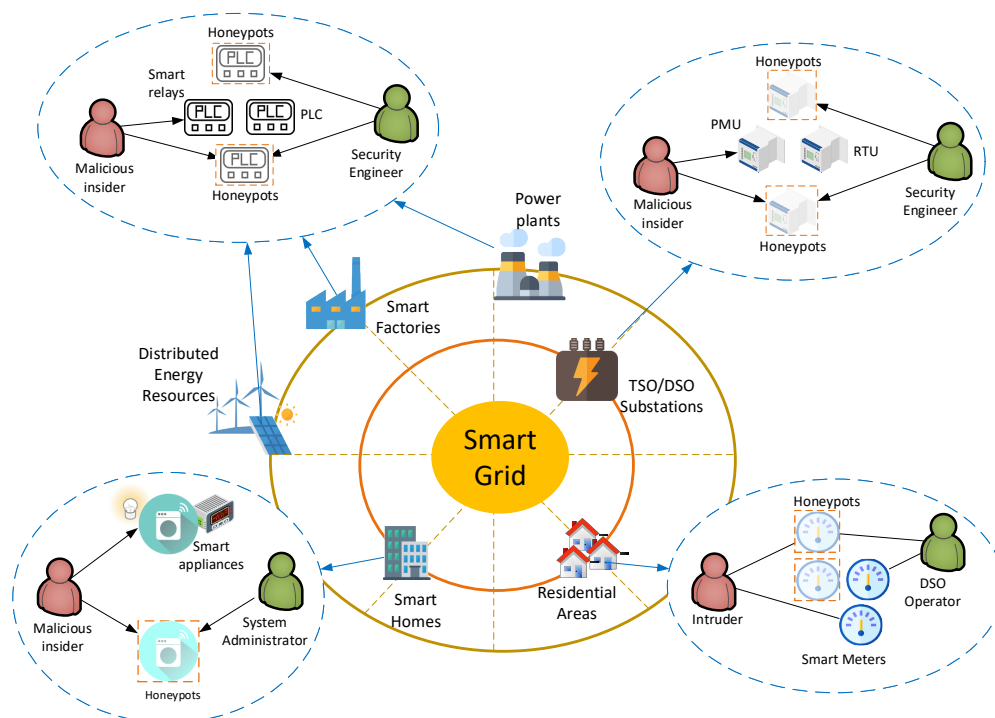

Figure 1. Depiction of various threats and possible honeypot deployments in smart grids.

Considering the proposed system model, the corresponding attack model ensembles a wide range of attack scenarios, especially those that target specific vulnerable network assets and in which the adversary has to choose between assets in the operational environment and honeypots. In more detail, DoS attacks are very common in smart grid applications and include a variety of attacks, such as buffer overflow, flooding, and amplification attacks, among others, that aim to render a remote service inaccessible to legitimate users. By its definition, the proposed system model aggregates possible multiple adversaries to a single entity, therefore the attack model also considers DDoS attacks, where multiple systems launch orchestrated attacks against a single host. Finally, False Data Injection Attacks (FDIAs) can also be considered for the attack model as they target specific assets in a smart grid. FDIAs aim to tamper control systems with falsified data that can manipulate the decision of automation systems, with severe consequences ranging from the destruction of smart grid equipment to grid fluctuations, instabilities, and financial loses [25].

Let $N \leq N_{\max}$ denote the total number of hosts within a block of IP addresses, with the value of N being controlled by the defender. Additionally to the total number of hosts, the defender can also control which of them are used by real devices and honeypots, with the aim to mitigate the impact of potential attacks without unnecessarily increasing the related costs. It is highlighted that in the

considered scenario, the defender has the option to increase the number of honeypots by disconnecting real devices (each of which for a portion of time), if this further assists on further mitigating the impact of potential attacks. This approach aims at exploring the potential security gains of "hiding" some of the real devices and substituting them with honeypots. In general, the defender's decision is affected by several parameters, such as the deployment costs; the benefit of capturing an attack with a honeypot; the cost of having a number of real devices under attack; and the trade-off between increasing the number of real devices that are connected to the smart grid at each time slot, the level of security, which increases with the number of utilized honeypots, and the implementation cost.

The attacker set of strategies determines whether or not to attack a host. Thus, the attacker's decision depends on the trade-off between the benefit acquired when attacking a real device and the cost of attacking a honeypot.

For the t-th interval, let $s_{\mathrm{D},i}[t] \in \{1, -1\}$ be equal to 1 when the i-th host is used by a real device and equal to -1 when it is used by a honeypot. On the other hand, regarding the set of strategies of the attacker, let $s_{\mathrm{A},i}[t] \in \{1, 0\}$ be equal to 1 when the attacker attacks the j-th host and equal to 0 when the j-th host is not attacked. For the sake of clarity, the notation is given in Table 1.

Table 1. Notation.

Parameter	Definition
A	attacker
D	defender
$s_{\mathrm{A},i}$	strategy of the attacker for the i-th host
$s_{\mathrm{D},i}$	strategy of the defender for the i-th host
N_{r}	number of real devices
N_{max}	total number of available hosts
N	sum of connected real devices and honeypots
a_i	different terms' weights of attacker's payoffs
d_i	different terms' weights of defender's payoffs
θ	portion of the number of hosts (N) that are honeypots
ϕ	portion of the number of hosts (N) that are attacked
ϕ_{m}	the maximum portion of the number of hosts (N) that are attacked
U_{i}	payoff of player i
$f(\cdot), g(\cdot), \tilde{f}(\cdot), \tilde{g}(\cdot)$	functions of $(\cdot)$
$\mathcal{S}$	set of players
$\mathcal{A}_i$	set of actions for player i
y, N_1, N_2	auxiliary variables
$\mathbb{E}[\cdot]$	expected value of $[\cdot]$
$\mathbb{P}[\cdot]$	probability of the event $[\cdot]$
a, b	the two types of attacker
A_j	attacker of type j
$a_{i,j}$	weight's of attacker's payoff when he is of type $j \in \{a, b\}$
d_j	weight's of attacker's payoff when he is of type $j \in \{a, b\}$
μ	belief that the attacker is of type a
ϕ_i	probability of attacking each host for the attacker of type i.
$\phi_{i,\mathrm{m}}$	maximum value of the probability of attacking each host for the attacker of type i
Ω	states of the nature
t	round of the game in a repeated game
G_i	game i
h^t	history of the game after t-th play
$(\cdot)^*$	$(\cdot)$ belongs to the NE
C_i	cost of under or over estimating the demand of the i-th device
$f_{\mathrm{R},i}$	the probability density function of the actual energy consumption
δ_i	the mean energy demand of the i-th device
E_{max}	the maximum energy consumption
p_{uc}	energy price in the unit commitment stage
p_{ed}	energy price in the economic-dispatch stage

According to the aforementioned trade-off for the attacker's side, the attacker's payoff is given by

$$U_{\text{A}}[t] = f\left(a_{i\in\{1,2,3\}}, \sum_{i=1}^{N}\frac{(1+s_{\text{D},i})}{2}s_{\text{a},i}, \sum_{i=1}^{N}\frac{1-s_{\text{D},i}}{2}s_{\text{a},i}, \sum_{i=1}^{N}s_{\text{A},i}\right),\tag{1}$$

where a_1, a_2, a_3 are the non-negative weights that correspond to the impact that the number of attacked real devices; the number of attacked honeypots and the total number of attacks has on its payoff; and f is an increasing function of $\sum_{i=1}^{N}\frac{(1+s_{\text{D},i})}{2}s_{\text{A},i}$, i.e., the number of attacked real devices, and a decreasing function of $\sum_{i=1}^{N}\frac{1-s_{\text{D},i}}{2}s_{\text{A},i}$, i.e., the number of attacked honeypots. Moreover, the total number of attacks, i.e., $\sum_{i=1}^{N}s_{\text{A},i}$, also introduces extra cost to the attacker's payoff due to the implementation cost and the general increase of the probability of the attacker to reveal information about their identity and action. For example, assuming that the aforementioned terms have a linear impact on the attacker's payoff, $U_{\text{A}}[t]$ could be written as

$$U_{\text{A}}[t] = a_1\sum_{i=1}^{N}\frac{(1+s_{\text{D},i})}{2}s_{\text{A},i} - a_2\sum_{i=1}^{N}\frac{1-s_{\text{D},i}}{2}s_{\text{A},i} - a_3\sum_{i=1}^{N}s_{\text{A},i}.\tag{2}$$

On the other hand, the defender's payoff is given by

$$U_{\text{D}}[t] = g\left(d_{i\in\{1,2,3,4\}}, \sum_{i=1}^{N}\frac{(1-s_{\text{D},i})}{2}s_{\text{A},i}, \sum_{i=1}^{N}\frac{(1+s_{\text{D},i})}{2}s_{\text{A},i}, \sum_{i=1}^{N}\frac{(1+s_{\text{D},i})}{2}, N\right),\tag{3}$$

where d_1, d_2, d_3, d_4 are the non-negative weights that correspond to the impact that the number of attacked real devices, the number of attacked honeypots, the number of real devices that are not served, and the total number of used hosts has on its payoff, and g is an increasing function of $\sum_{i=1}^{N}\frac{(1-s_{\text{D},i})}{2}s_{\text{A},i}$ and a decreasing function of the absolute value of $\sum_{i=1}^{N}\frac{(1+s_{\text{D},i})}{2} - N_{\text{r}}$. Moreover, the total number of hosts also introduces an extra cost. Next, it is assumed that the terms coupled with d_1, d_2, and d_4 have a linear impact on the attacker's payoff. Moreover, it is considered that the level of satisfaction of the defender gradually gets saturated as more real devices are served, i.e., the defender's payoff is a concave function, hereinafter modeled by square function, of the number of real devices that are not served. Thus, $U_{\text{D}}[t]$ could be written as

$$U_{\text{D}}[t] = d_1\sum_{i=1}^{N}\frac{(1-s_{\text{D},i})}{2}s_{\text{A},i} - d_2\sum_{i=1}^{N}\frac{(1+s_{\text{D},i})}{2}s_{\text{a},i} - d_3\left(\sum_{i=1}^{N}\frac{(1+s_{\text{D},i})}{2} - N_{\text{r}}\right)^2 - d_4N\tag{4}$$

As it has already been mentioned, if a smart grid device is attacked, this might have several negative consequences, such as the disruption of the normal operation of the electricity grid and financial loss. For example, when the attacks target the dynamic energy management (DEM) system [26], they might lead to the under/overestimation of the energy consumption and, thus, monetary loss in energy trading. This is reflected to the first term of the payoff function of the defender. More specifically, d_1 can be seen as a function of the average cost, $\mathbb{E}[C_i]$, of under- or overestimating the energy demand of the attacked device, assuming that the later corresponds to an energy consumer. Furthermore, assuming that the DEM management operation is implemented over two stages—the unit-commitment and economic-dispatch stages—the utility generates and reserves the energy supply based on the estimated energy demand of the consumers, while if the energy supply was underestimated, the utility needs to buy the energy difference between the actual and the generated energies in the economic dispatch stage to prevent the undersupply situation [27]. In this case, the cost of under- or overestimating the energy demand of the attacked devices is given by [27–29]

$$C_i = p_{\text{uc}}\int_0^{\delta_i}(\delta_i - r)f_{R,i}dr + p_{\text{ed}}\int_{\delta_i}^{E_{\max}}(r - \delta_i)f_{R,i}dr,\tag{5}$$

where $f_{R,i}$ is the probability density function of the actual energy consumption, δ_i is the mean energy demand of the i-th device, E_{max} is the maximum energy consumption, and p_{uc} and p_{ed} are the energy prices in the unit commitment and economic dispatch stages, respectively. On the other hand, the isolated use of some devices could lead to a nonlinear increase of the energy cost, e.g., when a local energy generator is used [30], which is taken into account by the third term of the defender's payoff.

Moreover, it is highlighted that the different terms of the players' payoff do not necessarily correspond to direct monetary loss or gain, but also reflect the potential impact of security risks on the reliable operation of the smart grid, which has an indirect effect on financial loss. Furthermore, it is noted that many of our results could easily be generalized assuming different functions for both U_D and U_A.

3. One-Shot Game

In this section, we focus on an one-shot non-cooperative game between the attacker and the defender, which captures one encounter between them. In general, although game theory is based on optimization, it is the appropriate tool when the optimal decision of one entity (player) depends on the decision of the other player. The rules for predicting how a game will be played defines the solution concepts in terms of which the game is understood [31].

3.1. Game Formulation

It is assumed that both the attacker and the defender have complete information about each other's payoff. The attacker attacks θN hosts, where $0 \leq \theta \leq 1$ denotes the portion of the total number of honeypots hosts. It is further assumed that the IPs are dynamically assigned and that all hosts have the same probability to be a honeypot or to be attacked. It is noted that this assumption leads to the optimal performance for the defender, as it has been shown in [32]. In this case, the attacker's payoff can be directly expressed as a function of a_i, ϕ, θ, and N, i.e.,

$$U_A = \tilde{f}(a_1, a_2, a_3, \phi, \theta, N). \tag{6}$$

The attacker aims at maximizing its payoff, thus the corresponding optimization problem can be written as

$$\begin{aligned} \max_{\phi} \quad & U_A \\ \text{s.t.} \quad & C_1 : 0 \leq \phi \leq \phi_m, \end{aligned} \tag{7}$$

where ϕ_m is the maximum value of ϕ.

Similarly, the payoff of the defender can also be written as a function of ϕ and θ, i.e.,

$$U_D = \tilde{g}(d_1, d_2, d_3, d_4, \phi, \theta, N), \tag{8}$$

while its maximization leads to the following optimization problem.

$$\begin{aligned} \min_{\theta, N} \quad & U_D \\ \text{s.t.} \quad & C_1 : 0 \leq \theta \leq 1 \\ & C_2 : 0 \leq N \leq N_{max} \end{aligned} \tag{9}$$

Based on (2) and (4), the payoff of the attacker and the defender can be written as

$$U_A = a_1(1-\theta)\phi N - a_2\theta\phi N - a_3\phi N \tag{10}$$

and

$$U_D = d_1\theta\phi N - d_2(1-\theta)\phi N - d_3((1-\theta)N - N_r)^2 - d_4 N, \tag{11}$$

respectively.

Thus, the game, hereinafter termed as Game 1, that captures this situation consists of the following.

Game 1:

1. The set of players $\mathcal{S}$, which includes the attacker and the defender, i.e., $\mathcal{S} = \{A, D\}$
2. The set of actions for each player, i.e, $\mathcal{A}_D = \{\theta \in [0, 1], N \in [0, N_{\max}]\}$ for the defender and $\mathcal{A}_A = \phi \in [0, \phi_{\mathrm{m}}]$ for the attacker.
3. The payoff functions for each player, i.e., U_A and U_D.

Then, the game can be described by the set G_1:

$$G_1 : \{\mathcal{S}, A_D, A_A, U_A, U_D\}. \tag{12}$$

Based on the definitions of the payoffs and strategies in G_1, the defender tries to select the total number of hosts and honeypots in order to mitigate the impact of attacks by maximizing its payoff, while the attacker aims at maximizing its payoff by properly selecting the number of hosts that will attack. Moreover, this game can be classified as a sequential one of imperfect information, as the defender first decides the number of hosts (N) and the portion of them that corresponds to honeypots (θ), while the attacker has partial knowledge of the defender's strategy, as the attacker can observe the total number of hosts, but does not know which of them are honeypots [33]. Thus, it is assumed that the two players choose θ and ϕ simultaneously at the beginning of the game, assuming common knowledge about the game (payoffs). As it has already been mentioned, the objective of both players is to maximize their payoffs, which implies that both players are rational [33].

3.2. Solution of Game 1

In order to solve the game that has been described in the previous subsection, the concept of Nash Equilibrium (NE) will be used. From the practical point of view, the NE is the optimal decision for a player, e.g., the defender, given that the strategy of the other player, i.e., the attacker, is also optimized. Moreover, if a player decides to optimize their payoff ignoring the payoff of the other player and alleviate from the NE, then they will achieve a worst payoff if the other player sticks to the NE. In conclusion, in the considered framework, a defender's strategy belongs to the NE if it is is the best reply to the attacker's strategy, and vice versa. In a NE, "unilateral deviations", which refer to the case that one player changes its own decision while the others stick to their current choices, do not benefit any of the players [31].

Definition 1. *The action profile (θ^*, ϕ^*, N^*) is a NE if by deviating from it none of the players can gain anything, i.e.,*

$$\begin{aligned} U_D(\theta^*, N^*, \phi^*) &\geq U_D(\theta, N, \phi^*), \\ U_A(\theta^*, N^*, \phi^*) &\geq U_A(\theta^*, N^*, \phi). \end{aligned} \tag{13}$$

Thus, a strategy of each player belongs to the NE if this is a best reply to the strategy of the other player [31].

To derive the NE, first, the following lemma is provided which reduces the set of the candidate best strategies for the attacker.

Lemma 1. *In the NE—if it exists—$\phi^* \in \{0, \phi_{\mathrm{m}}\}$.*

Proof. Let us assume that the set ($\theta^*, N^* \neq 0, \phi'$) is is a NE and that $\phi' \in (0, \phi_{\mathrm{m}})$. Then, it holds that

$$(a_1(1 - \theta)N - a_2\theta N - a_3 N)\phi' \geq (a_1(1 - \theta) - a_2\theta - a_3)\phi_{\mathrm{m}}, \tag{14}$$

i.e., $\phi' \geq \phi_{\mathrm{m}}$, which contradicts the assumption. □

Theorem 1. *The NE is given by*

$$(\theta^*, N^*, \phi^*) = \begin{cases} (0, \frac{2d_3 N_r - d_4}{2d_3}, 0), \text{ if} \\ \quad 0 \leq \frac{2d_3 N_r - d_4}{2d_3} \leq N_{\max} \text{ and } a_1 \leq a_3, \\ (0, N_{\max}, 0), \text{ if} \\ \quad \frac{2d_3 N_r - d_4}{2d_3} > N_{\max} \text{ and } a_1 \leq a_3, \\ (0, 0, 0), \text{ if} \\ \quad \frac{2d_3 N_r - d_4}{2d_3} < 0 \text{ and } a_1 \leq a_3, \\ (\frac{(d_1 + d_2)\phi_m + 2d_3 N_{\max} - 2d_3 N_r}{2d_3 N_{\max}}, N_{\max}, \phi_m), \text{ if} \\ \quad 0 \leq \frac{(d_1 + d_2)\phi_m + 2d_3 N_{\max} - 2d_3 N_r}{2d_3} \leq N_{\max} \text{ and } d_1 \phi_m \geq d_4 \\ \quad \text{and } (a_1 + a_2) N_r \geq (a_2 + a_3) N_{\max} + \frac{(a_1 + a_2)(d_1 + d_2)}{2d_3}, \\ (0, N_r - \frac{d_2 \phi_m + d_4}{2d_3}, \phi_m), \text{ if} \\ \quad d_1 \phi_m < d_4 \text{ and } a_1 > a_3 \text{ and } 0 < N_r - \frac{d_2 \phi_m + d_4}{2d_3} \leq N_{\max}, \\ (0, N_{\max}, \phi_m), \text{ if} \\ \quad (d_1 + d_2)\phi_m + 2d_3 N_{\max} - 2d_3 N_r < 0 \text{ and} \\ \quad a_1 > a_3 \text{ and } N_r - \frac{d_2 \phi_m + d_4}{2d_3} > N_{\max}, \\ (0, 0, \phi_m), \text{ if} \\ \quad (d_1 + d_2)\phi_m + 2d_3 N_{\max} - 2d_3 N_r < 0 \text{ and} \\ \quad a_1 > a_3 \text{ and } N_r - \frac{d_2 \phi_m + d_4}{2d_3} < 0, \\ \sharp, \text{ elsewhere.} \end{cases} \quad (15)$$

Proof. By using Lemma 1, the values of ϕ that can potentially belong to the NE are $\phi = 0$ and $\phi = \phi_m$. First, let us assume that $\phi^* = 0$. This can be valid only if

$$\phi_m(a_1(1 - \theta) - a_2\theta - a_3) \leq 0. \quad (16)$$

when $\phi^* = 0$ then $\theta^* = 0$. Thus, $\phi = 0$ can be belong to the equilibrium if $a_1 \leq a_3$. By setting $\frac{\partial U_D}{\partial N} = 0$, $\theta = 0$, and $\phi = 0$, it holds that

$$N^* = \left[\frac{2d_3 N_r - d_4}{2d_3} \right]_0^{N_{\max}} \quad (17)$$

where $[\cdot]_0^{N_{max}} = \min\{\max\{\cdot, 0\}, N_{\max}\}$.

Next, let us assume that $\phi^* = \phi_m$. By setting $\frac{\partial U_D}{\partial \theta} = 0$, it holds that

$$\theta = \frac{(d_1 + d_2)\phi_m + 2d_3 N - 2d_3 N_r}{2d_3 N}, \quad (18)$$

while

$$\frac{\partial^2 U_D}{\partial \theta^2} = -2d_3 N^2 \leq 0, \quad (19)$$

i.e., U_D is concave with respect to θ.

By assuming that $0 < \frac{(d_1 + d_2)\phi_m + 2d_3 N - 2d_3 N_r}{2d_3 N} < 1$, it holds that $\frac{\partial U_D}{\partial N} \geq 0$ if $d_1 \phi_m \geq d_4$. In this case, the value of θ that maximizes U_D is given by (18) and $N = N_{\max}$, as U_D is concave with respect to θ and, given the solution of (18), an increasing function of N. Furthermore, $\phi = \phi_m$ belongs to the equilibrium if

$$U_{A, \phi = \phi_m} \geq U_{A, \phi = 0}, \quad (20)$$

which can be written as

$$(a_1 + a_2)N_r \geq (a_2 + a_3)N_{max} + \frac{(a_1 + a_2)(d_1 + d_2)}{2d_3}. \tag{21}$$

Finally, if $\frac{(d_1+d_2)\phi_m + 2d_3 N - 2d_3 N_r}{2d_3 N} < 0$ (i.e., U_D is not maximized for $\theta > 0$), from $\frac{\partial U_D}{\partial N} = 0$ and considering that $\frac{\partial^2 U_D}{\partial N^2} \leq 0$, for $\theta = 0$ it holds that

$$N^* = \left[N_r - \frac{d_2\phi_m + d_4}{2d_3} \right]_0^{N_{max}}. \tag{22}$$

Apparently, in this case, $\phi = \phi_m$ belongs to the equilibrium if $a_1 > a_3$, as then $U_{A,\phi=max} \geq U_{A,\phi=0}$. Finally, it is noted that $\theta = 1$ cannot belong to an equilibrium, as in this case $\phi^* = 0$. □

Theorem 2. *The Nash equilibrium of Game 1—if it exists—is unique.*

Proof. This can easily be proved by observing that all sets of conditions for each branch of (15) are mutually exclusive, as can also be verified by the proof of Theorem 1. □

3.3. Strategy Selection When NE Does Not Exist

As it can be observed in the previous subsection, the NE does not always exist. Thus, to meet the requirements of practical scenarios, a different framework is required when the NE does not exist. In this case, the strategy of the defender can be chosen by using "maxmin" analysis, which, instead of relying on predictions about choices of other player, it is concerned with maximizing the lowest value the other player can force the player to receive when they know the player's action [34]. The maxmin value for the defender is defined as

$$\max_{0 \leq \theta \leq 1, 0 \leq N \leq N_{max}} \min_{0 \leq \phi \leq \phi_m} U_D \tag{23}$$

To solve (23), it needs to be observed that U_D is either an increasing or a decreasing value of ϕ, for specific values of θ and N. Thus, the attacker can force the defender to receive the lowest value by either choosing ϕ_m or 0. When $\phi = \phi_m$,

$$U_D = d_1 \theta \phi_m N - d_2(1-\theta)\phi_m N - d_3((1-\theta)N - N_r)^2 - d_4 N, \tag{24}$$

while when $\phi = 0$,

$$U_D = -d_3((1-\theta)N - N_r)^2 - d_4 N. \tag{25}$$

Thus, (23) can be rewritten as

$$
\begin{aligned}
\max_{\theta, N} \quad & y \\
\text{s.t.} \quad & C_1 : 0 \leq \theta \leq 1, \\
& C_2 : 0 \leq N \leq N_{max}, \\
& C_3 : d_1 \theta \phi_m N - d_2(1-\theta)\phi_m N - d_3((1-\theta)N - N_r)^2 - d_4 N \geq y, \\
& C_4 : -d_3((1-\theta)N - N_r)^2 - d_4 N \geq y.
\end{aligned} \tag{26}
$$

The aforementioned problem is non-convex and thus difficult to solve this in its current format. To this end, by setting $\theta N = N_1$ and $(1-\theta)N = N_2$, it can be written as

$$
\begin{aligned}
\max_{N_1, N_2} \quad & y \\
\text{s.t.} \quad & C_1 : N_1 + N_2 \leq N_{max}, \\
& C_2 : d_1 \phi_m N_1 - d_2 \phi_m N_2 - d_3(N_2 - N_r)^2 - d_4(N_1 + N_2) \geq y, \\
& C_3 : -d_3(N_2 - N_r)^2 - d_4(N_1 + N_2) \geq y, \\
& C_4 : N_1, N_2 \geq 0.
\end{aligned} \tag{27}
$$

The optimization problem in (27) is a convex one and can be solved by standard convex optimization methods.

4. Repeated Game with Uncertainty about the Type of Attacker

In this section, based on the results for the one-shot game, we focus on a more realistic scenario according to which a repeated game is assumed, i.e., the attacker and the defender play the same game more than once.

4.1. Game Formulation

Players observe the outcome of the first round before the start of the second round. Payoffs for the entire game are defined as the sum of the payoffs from the previous stages. It is noted that repeated games have a more complex strategic structure than their their one-shot counterparts, as the players' strategic choices in the following stages are influenced by the outcome of the choices they make in an earlier stage [31].

Furthermore, it is assumed that the defender does not have complete knowledge of the weights of the attacker's payoff, i.e., a_i. Among others, this corresponds to the existence of multiple attackers with different preferences or the change of the same attacker's payoff over time. Then, a multi-stage game which belongs to the class of games known as "multi-stage games with observed actions and incomplete information" is considered. More specifically, it is assumed that there are two types of attackers, namely, a and b, each of which has different weights. Moreover, the impact of attacks from each type at the defender might be different, which is reflected by the use of wights $d_{i,a}$ and $d_{i,b}$, when the attacks come from the attacker a and b, respectively. It is assumed that in each time slot, solely all attacks are from the same type of attacker. Similarly to G_1, the attacker does not have perfect information of the last value of *theta* selected by the defender, but perfectly knows all former actions. A mixed strategy is assumed for the attacker where the attacker plays according to a probability distribution over the available strategies. Such a randomized behavior can potentially mislead the defender and lead them to reduced performance in terms of achieved average payoff. Thus, to model the interaction between the attacker and the defender, the concept of Bayesian games will be used [31]. In general, in Bayesian games, the term "type" is used to capture the incomplete information. In addition to the actual players in the game, there is a special player called "Nature". Nature randomly chooses a type for the attacker. It is further assumed that the distribution of Nature's moves is also unknown.

More specifically, let us assume that the attacker performs an attack to each host with probability $\phi_i < \phi_m$ with $i \in \{a, b\}$. Then, the expected payoff of the attacker is

$$\mathbb{E}[U_{A_i}] = a_{1,i}(1 - \theta)\phi_i N - a_{2,i}\theta\phi_i N - a_{3,i}\phi_i N, \tag{28}$$

where $\mathbb{E}[\cdot]$ denotes expectation. We assume that $0 \leq \phi_i \leq \phi_{i,m}$, where $\phi_{i,m}$ is the maximum value of ϕ_i. It is noted that for practical reasons $\phi_{i,m} < 1$, as attacking all defender's hosts would lead to extreme measures from the defender. It is highlighted that hereinafter when ϕ is used will denote the portion of hosts that are attacked (without specifying who is the attacker), while when ϕ_i is used will denote the probability that the attacker of type i attacks each host. Moreover, to avoid redundancy, it is further assumed that $a_{1,a} > a_{3,a}$ and $a_{1,b} > a_{3,b}$, as otherwise if one of the inequalities does not hold true, the attack cannot come from the corresponding type of attacker.

Based on the described attacker's behavior, the defender's strategy depends on his belief about the attacker's type. More specifically, the defender's belief is defined as a probability distribution over the nodes within his/her information set, conditioned on the fact that this information set has been reached. In other words, it represents how likely this player believes that a certain number of attacks comes from a certain type of the opponent. A system of beliefs is assembled from all individual information sets. For the current game, we only need to define belief for the attacker, i.e., their type. Let $0 \leq \mu \leq 1$ denote the belief of the defender that the attacker is of type a.

Considering the above, the expected value for the defender is

$$\mathbb{E}[U_D] = \mu \times (d_{1,a}\theta\phi_a N - d_{2,a}(1-\theta)\phi_a N - d_3((1-\theta)N - N_r)^2 - d_4 N)$$
$$+ (1-\mu) \times (d_{1,b}\theta\phi_b N - d_{2,b}(1-\theta)\phi_b N - d_3((1-\theta)N - N_r)^2 - d_4 N). \tag{29}$$

It is assumed that both players aim at maximizing their expected payoffs. Thus, the game, hereinafter termed as Game 2, that captures this situation consists of the following.

Game 2:

(i)   The set of players $\mathcal{S}$ that includes the attacker and the defender, i.e., $\mathcal{S} = \{A, D\}$.
(ii)   The set of states of nature, denoted by Ω.
(iii)   The types of the attacker, i.e., the set (a, b).
(iv)   The set of actions for each player, i.e, $\mathcal{A}_D = \{\theta, N\}$ for the defender and $(\mathcal{A}_{A_a}, \mathcal{A}_{A_a}) = (\phi_a, \phi_b)$ for the attacker of type a and b, respectively.
(v)   The expected payoff functions for each player, i.e., $\mathbb{E}[U_A]$ and $\mathbb{E}[U_A]$.
(vi)   The belief μ about the type of the attacker.
(vii)   The history h^t of the game at the t-th round.

The game can be described by the set G_2:

$$G_2 : \{\mathcal{S}, \Omega, (a, b), \mathcal{A}_D, (\mathcal{A}_{A_a}, \mathcal{A}_{A_b}), \mathbb{E}[U_A], \mathbb{E}[U_D], \mu, h^t\} \tag{30}$$

4.2. Solution of Game 2 Given Updated Beliefs

To solve the situation described in the previous subsection, the Bayesian Nash Equilibrium (BNE) will be used.

Lemma 2. *In the BNE—if it exists—$\phi_a^* \in \{0, \phi_{a,m}\}$ and $\phi_b^* \in \{0, \phi_{b,m}\}$.*

Proof. The proof is similar to the one of Lemma 1. $\square$

In the following, we analyze BNE based on the assumption that μ is a common prior, i.e., the attacker knows the defender' belief of μ [35].

Theorem 3. *The BNE is given by*

$$(\theta^*, N^*, \phi_a^*, \phi_b^*) =$$

$$\begin{cases}
(\tilde{\theta}_1, N_{\max}, \phi_{a,\mathrm{m}}, \phi_{b,\mathrm{m}}), \text{if} \\
\quad 0 \leq \tilde{\theta}_1 \leq 1 \text{ and } \mu d_{1,a}\phi_{a,\mathrm{m}} + d_{1,b}\phi_{b,\mathrm{m}}(1-\mu) \geq d_4 \\
\quad \text{and} -\mu\left(d_{1,a}+d_{2,a}\right)\phi_{a,\mathrm{m}} + (\mu-1)\left(d_{1,b}+d_{2,b}\right)\phi_{b,\mathrm{m}} + 2d_3 N_r \geq \frac{2d_3(a_{2,a}+a_{3,a})N_{\max}}{a_{1,a}+a_{2,a}} \\
\quad \text{and} -\mu\left(d_{1,a}+d_{2,a}\right)\phi_{a,\mathrm{m}} + (\mu-1)\left(d_{1,b}+d_{2,b}\right)\phi_{b,\mathrm{m}} + 2d_3 N_r \geq \frac{2d_3\left(a_{2,b}+a_{3,b}\right)N_{\max}}{a_{1,b}+a_{2,b}}, \\
\left(0, N_r - \frac{d_4+d_{2,b}\phi_{b,\mathrm{m}}+d_{2,a}\mu\phi_{a,\mathrm{m}}-d_{2,b}\mu\phi_{b,\mathrm{m}}}{2d_3}, \phi_{a,\mathrm{m}}, \phi_{b,\mathrm{m}}\right), \text{if} \\
\quad \tilde{\theta}_1 < 0 \text{ and } 0 \leq N_r - \frac{d_4+d_{2,b}\phi_{b,\mathrm{m}}+d_{2,a}\mu\phi_{a,\mathrm{m}}-d_{2,b}\mu\phi_{b,\mathrm{m}}}{2d_3} \leq N_{\max}, \\
(0, N_{\max}, \phi_{a,\mathrm{m}}, \phi_{b,\mathrm{m}}), \text{if} \\
\quad \tilde{\theta}_1 < 0 \text{ and and} N_r - \frac{d_4+d_{2,b}\phi_{b,\mathrm{m}}+d_{2,a}\mu\phi_{a,\mathrm{m}}-d_{2,b}\mu\phi_{b,\mathrm{m}}}{2d_3} > N_{\max}, \\
(0, 0, \phi_{a,\mathrm{m}}, \phi_{b,\mathrm{m}}), \text{if} \\
\quad \tilde{\theta}_1 < 0 \text{ and and} N_r - \frac{d_4+d_{2,b}\phi_{b,\mathrm{m}}+d_{2,a}\mu\phi_{a,\mathrm{m}}-d_{2,b}\mu\phi_{b,\mathrm{m}}}{2d_3} < 0, \\
(\tilde{\theta}_2, N_{\max}, \phi_{a,\mathrm{m}}, 0), \text{if} \\
\quad 0 \leq \tilde{\theta}_2 \leq 1 \text{ and } \mu\phi_{a,\mathrm{m}}d_{1,a} \geq d_4 \text{ and } \frac{(a_{1,a}+a_{2,a})(2d_3 N_r - \mu\phi_{a,\mathrm{m}}(d_{1,a}+d_{2,a}))}{d_3(a_{2,a}+a_{3,a})} \geq N_{\max} \\
\quad \text{and} \frac{(a_{1,b}+a_{2,b})(2d_3 N_r - \mu\phi_{a,\mathrm{m}}(d_{1,a}+d_{2,a}))}{d_3(a_{2,a}+a_{3,a})} \leq N_{\max}, \\
(0, 0, \phi_{a,\mathrm{m}}, 0), \text{if} \\
\quad \tilde{\theta}_2 < 0 \text{ and } N_r - \frac{d_4+\mu d_{2,a}\phi_{a,\mathrm{m}}}{2d_3} < 0, \\
(\tilde{\theta}_3, N_{\max}, 0, \phi_{b,\mathrm{m}}), \text{if} \\
\quad 0 \leq \tilde{\theta}_3 \leq 1 \text{ and } (\mu-1)\phi_{b,\mathrm{m}}d_{1,b} \geq d_4 \text{ and } \frac{(a_{1,a}+a_{2,a})(2d_3 N_r - \mu\phi_{a,\mathrm{m}}(d_{1,a}+d_{2,a}))}{d_3(a_{2,a}+a_{3,a})} \leq N_{\max} \\
\quad \text{and} \frac{(a_{1,b}+a_{2,b})(2d_3 N_r - \mu\phi_{a,\mathrm{m}}(d_{1,a}+d_{2,a}))}{d_3(a_{2,a}+a_{3,a})} \geq N_{\max}, \\
(0, 0, 0, \phi_{b,\mathrm{m}}), \text{if} \\
\quad \tilde{\theta}_3 < 0 \text{ and } N_r - \frac{(1-\mu)\phi_{b,\mathrm{m}}d_{2,b}+d_4}{2d_3} < 0, \\
\nexists, \text{elsewhere},
\end{cases} \quad (31)$$

where

$$\tilde{\theta}_1 = \frac{(d_{1,a}+d_{2,a})\mu\phi_{a,\mathrm{m}}}{2N^* d_3} + \frac{(d_{1,b}+d_{2,b}-\mu d_{1,b}-\mu d_{2,b})\phi_{b,\mathrm{m}}+2d_3(N^*-N_r)}{2N^* d_3}, \quad (32)$$

$$\tilde{\theta}_2 = \frac{\mu\phi_{a,\mathrm{m}}d_{1,a}+\mu\phi_{a,\mathrm{m}}d_{2,a}+2d_3 N^* - 2d_3 N_r}{2N^* d_3}, \quad (33)$$

$$\tilde{\theta}_3 = \frac{(1-\mu)\phi_{b,\mathrm{m}}d_{1,b}+(1-\mu)\phi_{b,\mathrm{m}}d_{2,b}+2d_3 N^* - 2d_3 N_r}{2N^* d_3}, \quad (34)$$

with the value of N^* in (32)–(34) being determined by the branch that they appear.

Proof. Three different cases will be considered, namely, $\phi_a^* = \phi_{a,\mathrm{m}}$ and $\phi_b^* = \phi_{b,\mathrm{m}}$, $\phi_1^* = \phi_{a,\mathrm{m}}$ and $\phi_b^* = 0$, and $\phi_a^* = 0$ and $\phi_b^* = \phi_{b,\mathrm{m}}$.

First, let us assume that $\phi_1^* = \phi_{1,m}$ and $\phi_2^* = \phi_{2,m}$. By setting $\frac{\partial U_D}{\partial \theta} = 0$, it holds that

$$\theta = \frac{(d_{1,a}+d_{2,a})\mu\phi_{a,\mathrm{m}}}{2N d_3} + \frac{(d_{1,b}+d_{2,b}-\mu d_{1,b}-\mu d_{2,b})\phi_{b,\mathrm{m}}+2d_3(N-N_r)}{2N d_3} \quad (35)$$

and also it is noted that $\frac{\partial^2 U_D}{\partial \theta^2} \leq 0$. By assuming that

$$0 < \frac{(d_{1,a}+d_{2,a})\mu\phi_{a,\mathrm{m}}}{2N d_3} + \frac{(d_{1,b}+d_{2,b}-\mu d_{1,b}-\mu d_{2,b})\phi_{b,\mathrm{m}}+2d_3(N-N_r)}{2N d_3} < 1, \quad (36)$$

it is given that $\frac{\partial U_D}{\partial N} \geq 0$ if $\mu d_{1,a}\phi_{a,m} + d_{1,b}\phi_{b,m}(1-\mu) \geq d_4$. In this case, the value of θ that maximizes U_D is given by (36) and $N = N_{max}$. Moreover, $\phi_a = \phi_{a,m}$ and $\phi_b = \phi_{b,m}$ belong to the equilibrium if

$$U_{A_a,\phi_a=\phi_{a,m}} \geq U_{A,\phi_a=0} \tag{37}$$

and

$$U_{A_b,\phi_b=\phi_{b,m}} \geq U_{A,\phi_b=0}, \tag{38}$$

respectively, which can be written as

$$-\mu\left(d_{1,a}+d_{2,a}\right)\phi_{a,m} + (\mu-1)\left(d_{1,b}+d_{2,b}\right)\phi_{b,m} + 2d_3 N_r \geq \frac{2d_3\left(a_{2,a}+a_{3,a}\right)N_{max}}{a_{1,a}+a_{2,a}} \tag{39}$$

and

$$-\mu\left(d_{1,a}+d_{2,a}\right)\phi_{a,m} + (\mu-1)\left(d_{1,b}+d_{2,b}\right)\phi_{b,m} + 2d_3 N_r \geq \frac{2d_3\left(a_{2,b}+a_{3,b}\right)N_{max}}{a_{1,b}+a_{2,b}}, \tag{40}$$

respectively.

On the other hand, assuming that

$$\frac{\left(d_{1,a}+d_{2,a}\right)\mu\phi_{a,m}}{2N_{max}d_3} + \frac{\left(d_{1,b}+d_{2,b}-\mu d_{1,b}-\mu d_{2,b}\right)\phi_{b,m}+2d_3(N-N_r)}{2Nd_3} < 0, \tag{41}$$

from $\frac{\partial U_D}{\partial N} = 0$ it holds that

$$N = N_r - \frac{d_4 + d_{2,b}\phi_{b,m} + d_{2,a}\mu\phi_{a,m} - d_{2,b}\mu\phi_{b,m}}{2d_3}. \tag{42}$$

Apparently, $\phi_a^* = \phi_{a,m}$ and $\phi_b^* = \phi_{b,m}$ belong to the equilibrium if $a_{1,a} > a_{3,a}$ and $a_{1,b} > a_{3,b}$, as then $U_{A_a,\phi_a=\phi_{a,m}} \geq U_{A_a,\phi_a=0}$ and $U_{A_b,\phi_b=\phi_{b,m}} \geq U_{A_b,\phi_a=0}$, respectively.

Next, it is assumed that $\phi_a^* = \phi_{a,m}$ and $\phi_b^* = 0$. By setting $\frac{\partial U_D}{\partial \theta} = 0$ and making similar observations for the second derivative of U_D with respect to θ as with the previous case, it holds that

$$\theta = \frac{\mu\phi_{a,m}d_{1,a} + \mu\phi_{a,m}d_{2,a} + 2d_3 N - 2d_3 N_r}{2Nd_3}. \tag{43}$$

By assuming that

$$0 < \frac{\mu\phi_{a,m}d_{1,a} + \mu\phi_{a,m}d_{2,a} + 2d_3 N - 2d_3 N_r}{2Nd_3} < 1, \tag{44}$$

it can be shown that $\frac{\partial U_D}{\partial N} \geq 0$ if $\mu\phi_{a,m}d_{1,a} \geq d_4$. In this case, the value of θ that maximizes U_D is given by (43) and $N = N_{max}$. Moreover, $\phi_a = \phi_{a,m}$ and $\phi_b = 0$ belong to the equilibrium if

$$U_{A_a,\phi_a=\phi_{a,m}} \geq U_{A,\phi_a=0}, \tag{45}$$

and

$$U_{A_b,\phi_b=\phi_{b,m}} \leq U_{A,\phi_b=0}, \tag{46}$$

respectively, which can be written as

$$\frac{\left(a_{1,a}+a_{2,a}\right)\left(2d_3 N_r - \mu\phi_{a,m}\left(d_{1,a}+d_{2,a}\right)\right)}{d_3\left(a_{2,a}+a_{3,a}\right)} \geq N_{max} \tag{47}$$

and

$$\frac{\left(a_{1,b}+a_{2,b}\right)\left(2d_3 N_r - \mu\phi_{a,m}\left(d_{1,a}+d_{2,a}\right)\right)}{d_3\left(a_{2,a}+a_{3,a}\right)} \leq N_{max}, \tag{48}$$

respectively. If

$$\frac{\mu\phi_{a,\mathrm{m}}d_{1,a} + \mu\phi_{a,\mathrm{m}}d_{2,a} + 2d_3 N - 2d_3 N_r}{2Nd_3} < 0,$$

(49)

from $\frac{\partial U_D}{\partial N}$ it holds that

$$N = \left[N_r - \frac{d_4 + \mu d_{2,a}\phi_{a,\mathrm{m}}}{2d_3} \right]_0^{N_{\max}}$$

(50)

Apparently, if

$$N_r - \frac{d_4 + \mu d_{2,a}\phi_{a,\mathrm{m}}}{2d_3} > 0,$$

(51)

$\phi_b^* = 0$ cannot belong to the equilibrium, as having assumed that $a_{1,b} > a_{3,b}$, it leads to $U_{\mathrm{A_b},\phi_b = \phi_{b,\mathrm{m}}} > U_{\mathrm{A_b},\phi_a = 0}$.

Finally, assuming that $\phi_a^* = 0$ and $\phi_b^* = \phi_{b,\mathrm{m}}$, similar steps can be followed to find the equilibrium, which result in (43), (47), and (48) being replaced by

$$\theta = \frac{(1 - \mu)\phi_{b,\mathrm{m}}d_{1,b} + (1 - \mu)\phi_{b,\mathrm{m}}d_{2,b} + 2d_3 N^* - 2d_3 N_r}{N^* 2d_3}$$

(52)

$$\frac{(a_{1,a} + a_{2,a})(2d_3 N_r - \mu\phi_{a,\mathrm{m}}(d_{1,a} + d_{2,a}))}{d_3(a_{2,a} + a_{3,a})} \le N_{\max}$$

(53)

and

$$\frac{(a_{1,b} + a_{2,b})(2d_3 N_r - \mu\phi_{a,\mathrm{m}}(d_{1,a} + d_{2,a}))}{d_3(a_{2,a} + a_{3,a})} \ge N_{\max},$$

(54)

□

respectively.

Theorem 4. *The BNE of Game 2—if it exists—is unique.*

Proof. This can easily be proved by observing that all sets of conditions for each branch are mutually exclusive, as it can also be verified by the proof of Theorem 3. □

4.3. Update of Belief

As the game has only two players and only the defender needs to maintain its belief at any point in time, the defender's belief at stage t is defined as [33,35]

$$\mu^t = \mathbb{P}(A_a | h^t)$$

(55)

and

$$1 - \mu^t = \mathbb{P}(A_b | h^t),$$

(56)

where $\mathbb{P}(A_i | \phi)$ is the probability that when the portion of attacked hosts is ϕ, the type of attacker is i. Moreover, h^t is the history profile of the attacker, defined as a vector that contains the actions of the attacker, i.e.,

$$h^t = (\phi^1, ..., \phi^{t-1}).$$

(57)

The belief can be determined by using the Bayes' rule, i.e.,

$$\mu^{t+1} = \frac{\mathbb{P}(\phi^t | A_a, h^t)\mathbb{P}(A_a)}{\mathbb{P}(\phi^t | h^t)},$$

(58)

which can be written as

$$\mu^{t+1} = \frac{\mathbb{P}(\phi^t|A_a,h^t)\mathbb{P}(A_a)}{\mathbb{P}(\phi^t|A_a,h^t)\mathbb{P}(A_a) + \mathbb{P}(\phi^t|A_b,h^t)\mathbb{P}(A_b)}. \tag{59}$$

Observing new actions ϕ^t, the posterior belief μ^{t+1} via Bayesian updates can be estimated as

$$\mu^{t+1} = \frac{\mu^t\mathbb{P}(\phi^t|A_a,h^t)}{\mu^t\mathbb{P}(\phi^t|A_a,h^t) + (1-\mu^t)\mathbb{P}(\phi^t|A_b,h^t)}. \tag{60}$$

It is further assumed that each player believes that their opponent is playing according to the BNE. Thus, $\mathbb{P}(\phi^t|A_a,h^t)$ and $\mathbb{P}(\phi^t|A_b,h^t)$ can be calculated using the binomial distribution formula by

$$\mathbb{P}(\phi^t|A_a,h^t) = \binom{N}{\phi^t N}(\phi_a^{t*})^{\phi^t N}(1-\phi_a^{t*})^{N(1-\phi^t)} \tag{61}$$

and

$$\mathbb{P}(\phi^t|A_b,h^t) = \binom{N}{\phi^t N}(\phi_b^{t*})^{\phi^t N}(1-\phi_b^{t*})^{(1-\phi^t)N}, \tag{62}$$

where $\binom{n}{k} = \frac{n!}{k!(n-k)!}$. Considering the above, and as the term $\binom{N}{\phi^t N}$ appears in both $\mathbb{P}(\phi|A_a,h^t)$ and $\mathbb{P}(\phi^t|A_b,h^t)$, (60) can be rewritten as

$$\mu^{t+1} = \frac{\mu^t(\phi_a^{t*})^{\phi^t N}(1-\phi_a^{t*})^{N(1-\phi^t)}}{\mu^t(\phi_a^{t*})^{\phi^t N}(1-\phi_a^{t*})^{N(1-\phi^t)} + (1-\mu^t)(\phi_b^{t*})^{\phi^t N}(1-\phi_b^{t*})^{(1-\phi^t)N}}. \tag{63}$$

5. Simulation Results & Discussion

To study the behavior of our model, a simulation environment was implemented in Python. Three experiments have been carried out to study the player's strategies and the overall system behavior for the one-shot game and for the repeated game as well as in the case that NE does not exist.

5.1. One-Shot Game

The parameters that were used for the one-shot game are provided in Table 2. It should be noted that the simulation results do not depend on the exact values of the weights (a_i and d_i) but on the ratio among them; thus, the utilized values of weights are normalized to a common value. In this experiment, we compare the optimal strategy for the attacker and the defender with 2000 random solutions in order to verify that the equilibrium indeed yields the maximum payoff, considering that the opponent always chooses the best strategy.

Table 2. Simulation parameters for the one-shot game.

Parameter	Value
N_r	3
N_{max}	10
ϕ_{max}	1
$a_{\{1,2,3\}}$	$[0.76, 0.01, 0.10]$
$d_{\{1,2,3,4\}}$	$[0.03, 0.40, 0.45, 0.01]$
Random solutions for θ	2000
Random solutions for ϕ	2000

The provided Figures 2 and 3 verify that the payoffs of both players are optimal when the game reaches its equilibrium state. The red bullet in each graph points to the payoff in the equilibrium state. In more detail, Figure 2 shows that the payoff achieved in the equilibrium state (red bullet) is higher compared to 2000 random strategies ϕ, assuming that $N\theta$ remains at the optimal state. Similarly, the

payoff achieved for the defender in Figure 3 is higher compared to $2000N_{max}$ random combinations of $N\theta$, assuming that the opponent always chooses the best possible strategy. Moreover, it is notable that the payoffs follow a specific pattern when N remains constant and θ varies.
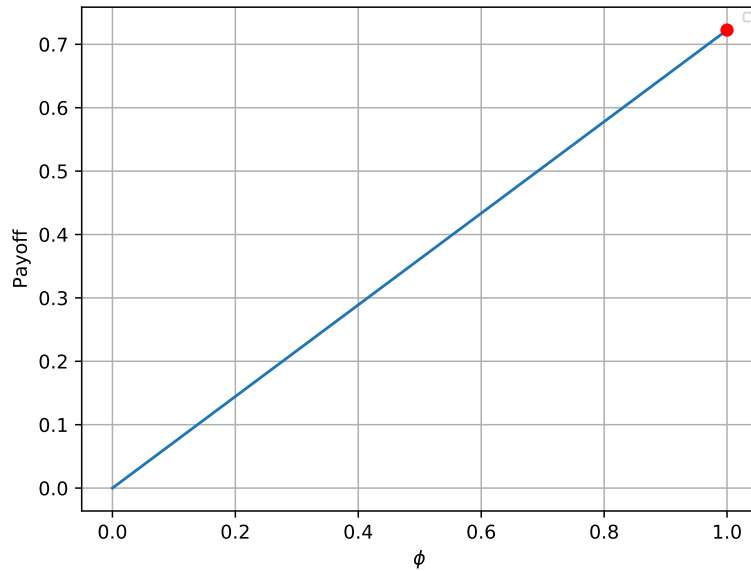

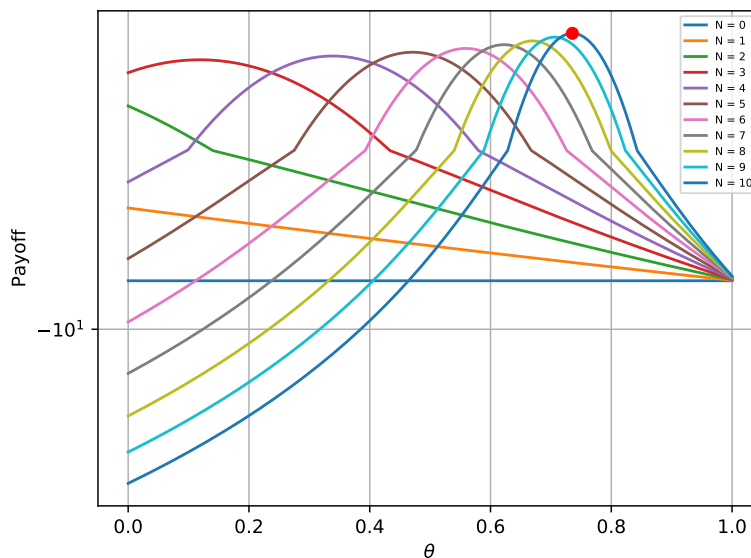**Figure 2.** Attacker's payoff for different strategies in the one-shot game.

**Figure 3.** Defender's payoff for different strategies in the one-shot game.

5.2. Max-Min Solution in the One-Shot Game

The second experiment examines the situation in which the game parameters do not result in an equilibrium, thus the defender applies a max-min analysis to maximize the worst-case scenario as described in Equation (27). The parameters of this experiment are provided in Table 3. The convex optimization problem of Equation (27) was solved by employing the CVXPY Python library [36,37].

Table 3. Simulation parameters for the one-shot game when equilibrium does not exist.

Parameter	Value
N_r	3
N_{max}	10
ϕ_{max}	1
$a_{\{1,2,3\}}$	$[0.81, 0.01, 0.06]$
$d_{\{1,2,3,4\}}$	$[0.31, 0.24, 0.81, 0.14]$
Random solutions for θ	2000

Figure 4 depicts the maximum worst-case payoff that corresponds to the solution received by Equation (27). This solution is compared to the worst-case payoffs that are received for different values of $N\theta$. The results prove that the defender successfully chooses the best possible strategy that yields the maximum payoff, assuming that the attacker always chooses the best strategy. Similar trends for various values of N are noticed, as with the first experiment.
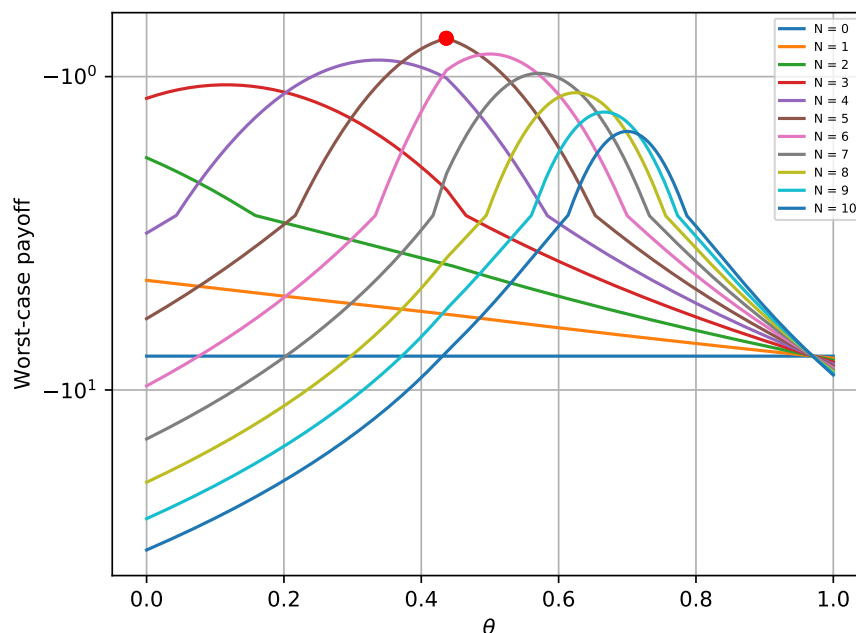
Figure 4. Defender's worst-case payoff when equilibrium does not exist.

5.3. Repeated Game

Finally, a third experiment was carried out in order to evaluate and study the repeated game. The main characteristic of this game is that the defender has imperfect information about the attacker's strategy, i.e., the identity of the actual kind of attacker that is hidden behind each attack. The simulation parameters are provided in Table 4.

The experiment realizes two type of defenders that correspond to deployment strategies and preferences of defenders deploying production or research honeypots. In our example, type *a* corresponds to a defender that deploys production honeypots and type *b* corresponds to a defender that deploys research honeypots. This is justified as the defender that deploys production honeypots cares more about the impact on the production equipment, meaning that the damage that an attack would cause against real devices would be greater than the benefit that the defender would enjoy if this attack would be against a honeypot, i.e., $d_{a,1} > d_{a,2}$. On the contrary, a defender that deploys research honeypots cares more about attracting attackers, meaning that the benefit for each attack against honeypots would be greater than the damage against a real device would cause, i.e., $d_{b,1} < d_{b,2}$.

Table 4. Simulation parameters for the repeated game.

Parameter	Value
Number of rounds	50
N_r	6
N_{max}	8
$\phi_{a,max}$	0.6
$\phi_{b,max}$	0.2
$a_{a\{1,2,3\}}$	$[0.48, 0.46, 0.10]$
$a_{b\{1,2,3\}}$	$[0.39, 0.48, 0.02]$
$d_{a\{1,2\}}$	$[0.70, 0.04]$
$d_{b\{1,2\}}$	$[0.04, 0.68]$
d_3, d_4	$0.77, 0.006$

As with the one-shot experiment, Figures 5 and 6 illustrate the achieved payoff of player's equilibrium, in respect to 2000 random solutions for the attacker and $2000N_{max}$ random solutions for the defender. Once again, the red bullet on each of these graphs depicts the equilibrium state. It is validated from Figure 5 that the attacker payoff drops if the attacker deviates from the optimal solution derived from the equilibrium. The same behavior is also noticed in Figure 6 for the defender.
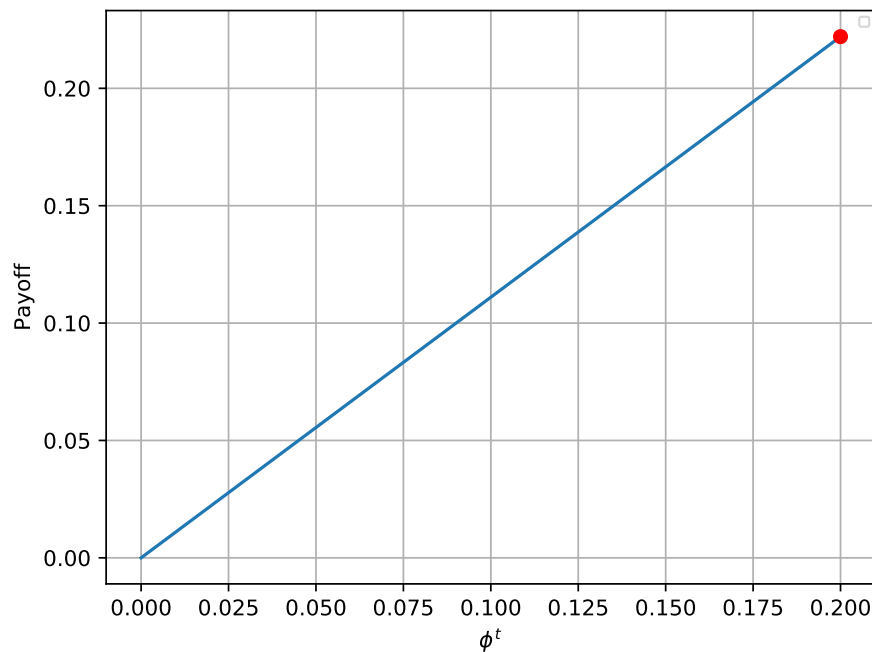
Figure 5. Attacker's payoff for different strategies in a single turn of the repeated game.
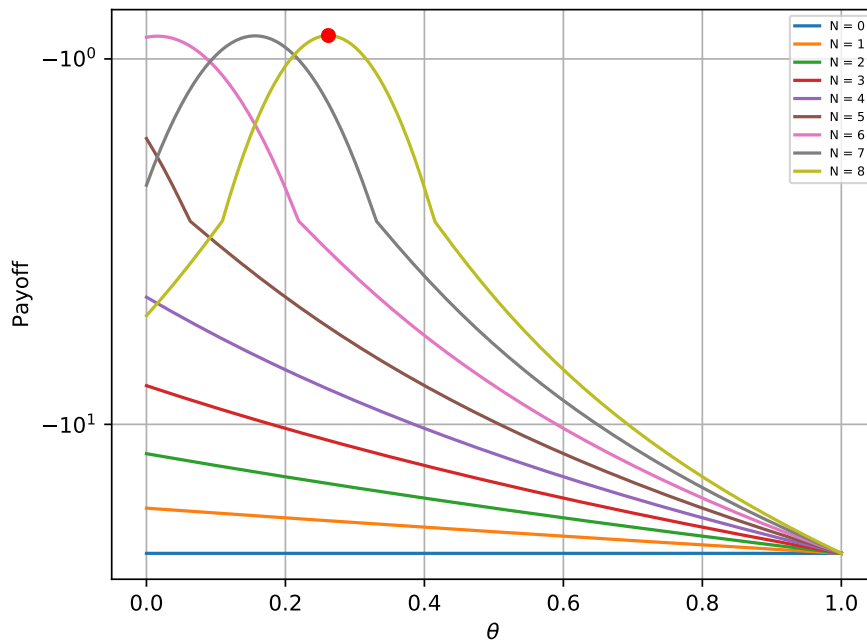
Figure 6. Players' payoff for different strategies in a single turn of the repeated game.

Finally, Figures 7 and 8 study the defender's belief about the actual type of the attacker. In particular, Figure 7 compares the belief of the defender about the attacker's type with the actual type of the attacker. It is assumed that 1 represents type *a* and 0 represents type *b*. It is shown that the defender successfully identifies the attacker's type in round 4 and does not change their belief, as the attacker's behavior remains the same throughout the game
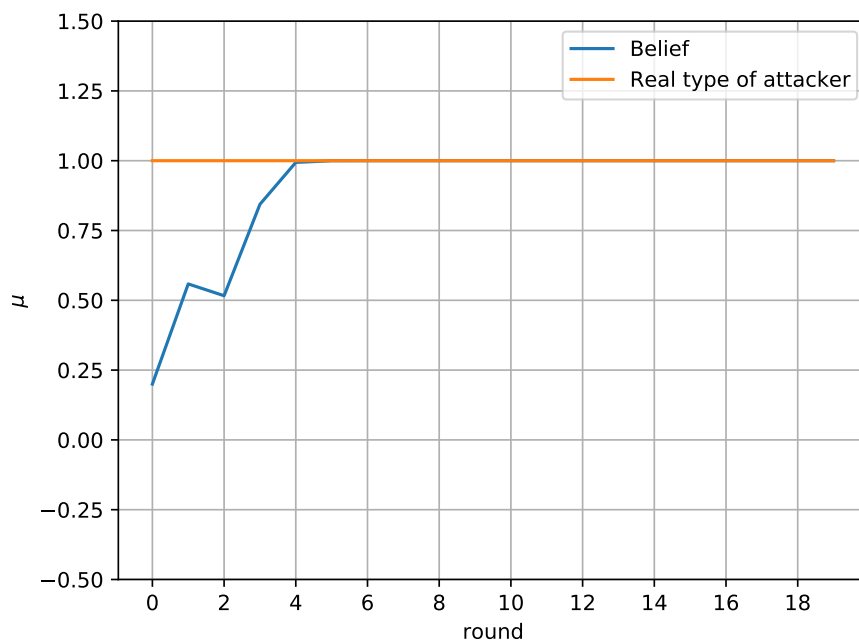
Figure 7. Defender's belief in the repeated game.

Figure 8 depicts the players' payoff through time. It is evident that the defender's payoff increases as they approach the actual type of the attacker. The defender's payoff exceeds the payoff of its opponent and gets maximized after round 4, when the defender is confident enough about the real type of the attacker.
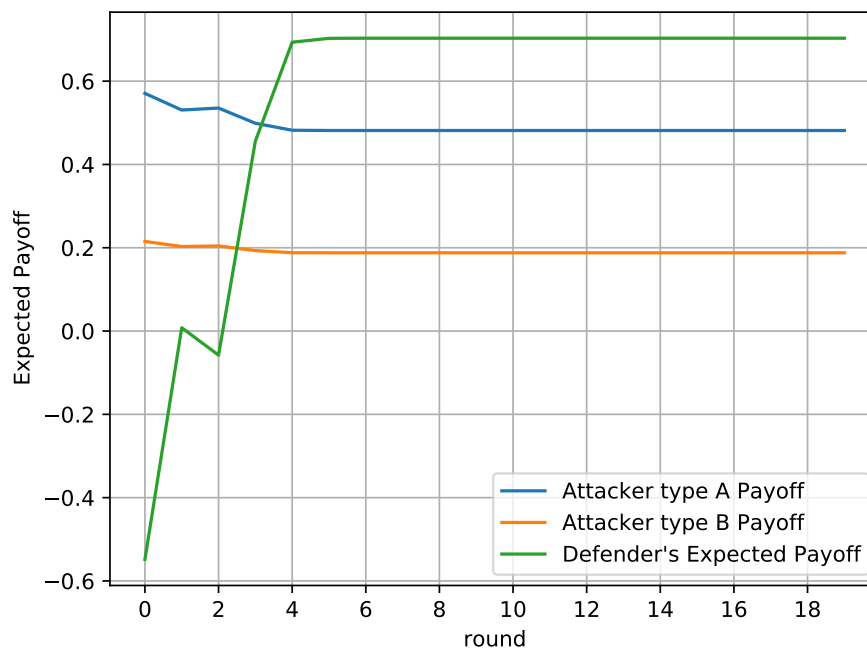
Figure 8. Defender's payoff in the repeated game.

6. Conclusions

In this paper, the efficient use of honeypots has been considered with the aim of mitigating the impact of attacks to smart grid infrastructure. More specifically, the interaction of an attacker and a defender has been investigated, who both aim at maximizing their payoffs by optimizing the deployment of attacks and honeypots, respectively. Two different games have been considered, namely, a one-shot one with perfect knowledge of the players' payoff and a repeated one with uncertainty about the payoff of the attacker. The Nash Equilibrium and the Bayesian Nash Equilibrium have been derived for the first and the second game, respectively, as well as the corresponding conditions, while the Equilibria uniqueness has been proved. Moreover, an alternative framework has also been provided for the case that an Equilibrium does not exist, which can be seen as the optimization of the worst-case scenario, as it is based on the maximization of the lowest value the attacker can force the defender to receive when they know the defender's action. Simulation results validated the analytical results of the equilibrium for both the attacker and the defender, for both games. Furthermore, the derived solution for case that the equilibrium does not exist has also also been evaluated. Finally, concerning the repeated game, it has been shown that the defender successfully identifies the attacker's type, thus maximizing its payoff throughout the game.

The proposed theoretical framework in the considered analysis facilitates the investigation of the potential benefits of using honeypots to enhance security in smart grids and creates opportunities for future research on this topic. For example, the use of more complicated payoffs can be explored, taking into account the particularities of different case studies. Moreover, further research is also needed in order to specify the long-term monetary gain of capturing attacks of a certain type by the utilized honeypots. Finally, the results can be extended to the case of more than two attackers types, while also considering uncertainty for the type of the defender.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

1. Cisco Annual Internet Report (2018–2023). White Paper. Available online: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html (accessed on 13 June 2020)
2. Littlefield, M. *Putting Industrial Cyber Security at the Top of the CEO Agenda*; LNS Research Library: Cambridge, MA, USA, 2017.
3. *Global Risks 2018: Insight Report*; World Economic Forum: Geneva, Switzerland, 2018.
4. The SPEAR Project. Available online: https://www.spear2020.eu/ (accessed on 13 June 2020).
5. Spitzner, L. The Honeynet Project: trapping the hackers. *IEEE Secur. Priv.* **2003**, *1*, 15–23. [CrossRef]
6. Spitzner, L. The Value of Honeypots, Part One: Definitions and Values of Honeypots. Available online: http://www.symantec.com/connect/articles/value-honeypots-part-one-definitions-and-values-honeypots (accessed on 13 June 2020).
7. Scott, C.; Carbone, R. *Designing and Implementing A Honeypot for a SCADA Network*; SANS Institute Reading Room: Singapore, 2014; p. 39.
8. Wei, L.; Sarwat, A.I.; Saad, W.; Biswas, S. Stochastic Games for Power Grid Protection Against Coordinated Cyber-Physical Attacks. *IEEE Trans. Smart Grid* **2018**, *9*, 684–694. [CrossRef]
9. Pawlick, J.; Colbert, E.; Zhu, Q. A Game-theoretic Taxonomy and Survey of Defensive Deception for Cybersecurity and Privacy. *ACM Comput. Surv.* **2019**, *52*, 1–28. [CrossRef]
10. Tian, W.; Ji, X.; Liu, W.; Liu, G.; Zhai, J.; Dai, Y.; Huang, S. Prospect Theoretic Study of Honeypot Defense Against Advanced Persistent Threats in Power Grid. *IEEE Access* **2020**, *8*, 64075–64085. [CrossRef]
11. Kumar, B.; Bhuyan, B. Using game theory to model DoS attack and defence. *Sādhanā* **2019**, *44*, 245. [CrossRef]
12. Çeker, H.; Zhuang, J.; Upadhyaya, S.; La, Q.D.; Soong, B.H. Deception-Based Game Theoretical Approach to Mitigate DoS Attacks. In *Lecture Notes in Computer Science*; Springer International Publishing: Berlin/Heidelberg, Germany, 2016; pp. 18–38.
13. Wang, K.; Du, M.; Maharjan, S.; Sun, Y. Strategic Honeypot Game Model for Distributed Denial of Service Attacks in the Smart Grid. *IEEE Trans. Smart Grid* **2017**, *8*, 2474–2482. [CrossRef]
14. Du, M.; Wang, K. An SDN-Enabled Pseudo-Honeypot Strategy for Distributed Denial of Service Attacks in Industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2020**, *16*, 648–657. [CrossRef]
15. Cho, J.H.; Zhu, M.; Singh, M. Modeling and Analysis of Deception Games Based on Hypergame Theory. In *Auton. Cyber Decept.* ; Springer International Publishing: Berlin/Heidelberg, Germany, 2019; pp. 49–74.
16. Horák, K.; Bošanský, B.; Tomášek, P.; Kiekintveld, C.; Kamhoua, C. Optimizing honeypot strategies against dynamic lateral movement using partially observable stochastic games. *Comput. Secur.* **2019**, *87*, 101579. [CrossRef]
17. Tian, W.; Ji, X.; Liu, W.; Liu, G.; Lin, R.; Zhai, J.; Dai, Y. Defense Strategies Against Network Attacks in Cyber-Physical Systems with Analysis Cost Constraint Based on Honeypot Game Model. *Comput. Mater. Contin.* **2019**, *60*, 193–211. [CrossRef]
18. Tian, W.; Ji, X.P.; Liu, W.; Zhai, J.; Liu, G.; Dai, Y.; Huang, S. Honeypot game-theoretical model for defending against APT attacks with limited resources in cyber-physical systems. *ETRI J.* **2019**, *41*, 585–598. [CrossRef]
19. La, Q.D.; Quek, T.Q.S.; Lee, J.; Jin, S.; Zhu, H. Deceptive Attack and Defense Game in Honeypot-Enabled Networks for the Internet of Things. *IEEE Internet Things J.* **2016**, *3*, 1025–1035. [CrossRef]
20. La, Q.D.; Quek, T.Q.S.; Lee, J. A game theoretic model for enabling honeypots in IoT networks. In Proceedings of the 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, 22–27 May 2016; pp. 1–6.
21. Bilinski, M.; Gabrys, R.; Mauger, J. Optimal Placement of Honeypots for Network Defense. In *Lecture Notes in Computer Science*; Springer International Publishing: Berlin/Heidelberg, Germany, 2018; pp. 115–126.
22. Fraunholz, D.; Schotten, H.D. Strategic defense and attack in deception based network security. In Proceedings of the 2018 International Conference on Information Networking (ICOIN), Chiang Mai, Thailand, 10–12 January 2018; pp. 156–161.

23.   Jicha, A.; Patton, M.; Chen, H. SCADA honeypots: An in-depth analysis of Conpot. In Proceedings of the 2016 IEEE Conference on Intelligence and Security Informatics (ISI), Tucson, AZ, USA, 28–30 September 2016.

24.   Dalamagkas, C.; Sarigiannidis, P.; Ioannidis, D.; Iturbe, E.; Nikolis, O.; Ramos, F.; Rios, E.; Sarigiannidis, A.; Tzovaras, D. A Survey On Honeypots, Honeynets and Their Applications On Smart Grid. In Proceedings of the 2019 IEEE Conference on Network Softwarization (NetSoft), Paris, France, 24–28 June 2019.

25.   Islam, S.N.; Mahmud, M.; Oo, A. Impact of optimal false data injection attacks on local energy trading in a residential microgrid. *ICT Express* **2018**, *4*, 30–34. [CrossRef]

26.   Diamantoulakis, P.D.; Kapinas, V.M.; Karagiannidis, G.K. Big data analytics for dynamic energy management in smart grids. *Big Data Res.* **2015**, *2*, 94–101. [CrossRef]

27.   Shafie, A.E.; Chihaoui, H.; Hamila, R.; Al-Dhahir, N.; Gastli, A.; Ben-Brahim, L. Impact of Passive and Active Security Attacks on MIMO Smart Grid Communications. *IEEE Syst. J.* **2019**, *13*, 2873–2876. [CrossRef]

28.   El Shafie, A.; Niyato, D.; Hamila, R.; Al-Dhahir, N. Impact of the Wireless Network's PHY Security and Reliability on Demand-Side Management Cost in the Smart Grid. *IEEE Access* **2017**, *5*, 5678–5689. [CrossRef]

29.   Niyato, D.; Wang, P.; Hossain, E. Reliability analysis and redundancy design of smart grid wireless communications system for demand side management. *IEEE Wirel. Commun.* **2012**, *19*, 38–46. [CrossRef]

30.   Mohsenian-Rad, A.; Wong, V.W.S.; Jatskevich, J.; Schober, R.; Leon-Garcia, A. Autonomous Demand-Side Management Based on Game-Theoretic Energy Consumption Scheduling for the Future Smart Grid. *IEEE Trans. Smart Grid* **2010**, *1*, 320–331. [CrossRef]

31.   Iqbal, A.; Gunn, L.J.; Guo, M.; Ali Babar, M.; Abbott, D. Game Theoretical Modelling of Network/Cybersecurity. *IEEE Access* **2019**, *7*, 154167–154179. [CrossRef]

32.   Garg, N.; Grosu, D. Deception in Honeynets: A Game-Theoretic Analysis. In Proceedings of the 2007 IEEE SMC Information Assurance and Security Workshop, West Point, NY, USA, 20–22 June 2007; pp. 107–113.

33.   Liang, X.; Xiao, Y. Game Theory for Network Security. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 472–486. [CrossRef]

34.   Chamberlain, G. Econometric applications of maxmin expected utility. *J. Appl. Econom.* **2000**, *15*, 625–644. [CrossRef]

35.   Liu, Y.; Comaniciu, C.; Man, H. A Bayesian game approach for intrusion detection in wireless ad hoc networks. In *Proceedings of the 2006 Workshop on Game Theory for Communications and Networks*; Association for Computing Machinery: New York, NY, USA, 2006. [CrossRef]

36.   Diamond, S.; Boyd, S. CVXPY: A Python-embedded modeling language for convex optimization. *J. Mach. Learn. Res.* **2016**, *17*, 1–5.

37.   Agrawal, A.; Verschueren, R.; Diamond, S.; Boyd, S. A rewriting system for convex optimization problems. *J. Control Decis.* **2018**, *5*, 42–60. [CrossRef]