Honeypot Type Selection Games for Smart Grid Networks

Nadia Boumkheld[1], Sakshyam Panda[1][0000−0001−7274−0073], Stefan Rass[2][0000−0003−2821−2489], and Emmanouil Panaousis[1][0000−0001−7306−4062]

[1] Department of Computer Science, University of Surrey, UK
[2] Universität Klagenfurt, Institute of Applied Informatics, Klagenfurt, Austria

Abstract. In this paper, we define a cyber deception game between the Advanced Metering Infrastructure (AMI) network administrator (henceforth, defender) and attacker. The defender decides to install between a low-interaction honeypot, high-interaction honeypot, and a real system with no honeypot. The attacker decides on whether or not to attack the system given her belief about the type of device she is facing. We model this interaction as a Bayesian game with complete but imperfect information. The choice of honeypot type is private information and characterizes the essence and objective of the defender i.e., the degree of deception and amount of threat intelligence. We study the players' equilibrium strategies and provide numerical illustrations. The work presented in this paper has been motivated by the H2020 SPEAR project which investigates the implementation of honeypots in smart grid infrastructures to: (i) contribute towards creating attack data sets for training a SIEM (Security Information and Event Management) and (ii) to support post-incident forensics analysis by having recorded a collection of evidence regarding an attacker's actions.

Keywords: Game theory · Honeypots · Smart Grid · Cyber security

1 Introduction

Smart grid adds information and communication technologies to the traditional grid in order to build a strong electrical grid capable of meeting the growing demand for electricity. A smart grid can be a large system connecting millions of devices and entities using different types of technologies making it complex and attractive target for cyber attackers. Attacks may aim to compromise grid devices with the goal to launch further attacks. For example, a hacked device might abruptly increase the load to cause circuit overflow.

Attacks against the "residential" part of smart grid may also try to insert, change, delete data, or control commands in the network traffic to mislead the smart grid and enforce faulty decisions such as a compromised smart meter causing inaccurate electricity bills [1]. User privacy is also threatened as cyber adversaries who gain access to communication channels used by the smart meters can infer the existence or absence of occupants in a building [2].

A honeypot is a security mechanism set up as a decoy to lure cyber attackers. Few objectives behind using honeypots include protecting real devices from getting attacked, wasting attackers' time, and collecting information about the attack methods used towards improving *threat intelligence* [3]. Honeypots are used to deceive attackers, but they are limited in resources and thus should be deployed smartly to maximize the deception. Game theory has been used to decide strategic deployments of honeypots. Defensive deception cybersecurity and privacy, in general, has been modelled using game theory. Pawlick et al. have published a taxonomy and survey on this topic [4]. A honeypot is a static trap network. Once attackers suspect its existence, they will be able to escape it by turning their effort towards other devices. Thus, it is extremely important, especially when dealing with critical infrastructure, that appropriate type of honeypots are chosen to satisfy specific objectives. To address this, we propose a game-theoretic model that optimizes the defender's choice of a system.

The proposed model, however, is not confined to investigate smart grids but we aim at using this as a basis, in future work - as part of the H2020 SPEAR project, for investigating the optimal use of honeypots in a smart grid testbed. We aim to achieve this by installing different honeypot types (e.g., taking advantage of different configurations of Conpot [5]) in crucial smart grid infrastructure points such as the control center, the Remote Terminal Units (RTUs) and the smart meter gateways. The derived results will be used to assess the performance of game-theoretic strategies in the smart grid testbed.

The aim of this paper is to introduce a game theoretic aid for the defender to optimally decide on the type of honeypot to protect a smart grid. The model aims to maximize threat intelligence while respecting associated costs related to the implementation of different honeypots types. These costs may include (i) network throughput introduced due to adding honeypots to the infrastructure, (ii) hardware cost of these honeypots, and (iii) operational management cost (e.g., system administrators' time spent for operating, auditing, and maintaining honeypots).

In our setting, the attacker decides whether to attack or not given that any unsuccessful attempt can lead to her attribution and disclose her attack methods. More precisely, we model the interactions between the defender and the attacker as a sequential game of complete but imperfect information. We have computed the perfect Bayesian Nash equilibrium as a guidance towards the optimal choice for each player. We assess our game model using numeric simulations to derive the probability of deploying a type of system and the attack probability.

The rest of the paper is organized as follows: Section 3 explains the game model we developed using honeypots. Section 4 presents the analysis for the calculation of the game equilibria, while in section 5 we display the results of our simulations. The next section presents some relevant, to our model, related work in the field and section 6 concludes this paper.

2 Related work

Configuration and deployment of honeypots have been extensively studied and carries a rich literature [6,7]. However, from a game-theoretic perspective there are relatively fewer studies on the strategic use of honeypots [8]. Píbil et al. categorises the studies based on modelling i) ongoing attack phase which captures the interaction within the honeypots and attackers [9,10] and ii) pre-attack phase where the attacker chooses a target [11]. They further investigated how a honeypot should be designed to optimize the probability that the attacker will attack the honeypot and not the real system [12]. The model also reflects on the *probing capability* of the attacker to determine whether the targeted machine is a honeypot before attacking.

Garg and Grosu studied the strategic use of honeypots for network defense through a signalling game. They investigated the problem of allocating k honeypots out of n possible hosts within a block of IP addresses [13]. In [14], Ceker et al. modelled the interaction between defender and attacker as a signalling game to devise a deception method to mitigate DoS attacks. The defender chooses, for one system, whether to be a honeypot or real system. The attacker can either attack, observe or retreat. La et al. extended the analysis of this work from single-shot game to repetitive game taking into account the deceptive aspects of the players [8]. In [15] the defender deploys honeypots in an AMI network to detect and gather DoS attack information while the attacker has the option to deploy anti-honeypot mechanisms to detect honeypot proxy servers before deciding on whether to attack or not. Similar to our work, the listed work employs honeypots to gather information about the attackers and use deception as a defensive mechanism.

Wagener et al. have trained a high-interaction honeypot to be capable of learning from attackers and dynamically changing its behaviour using reinforced learning [16]. Low interaction honeypots might reveal their true identity while high interaction honeypots may result in adverse conditions, e.g. attacker increases the chance to take control of the real system. Thus, with such adaptive techniques there is a need for finding an *optimal response strategy* for the honeypot to prolong its interaction with malicious entities. Motivated by [16], Hayatle et al. studied the honeypot detection by bootmasters through a Bayesian game of incomplete information [17]. The honeypot decides whether to execute the attack commands received from the botmaster or not; the attacker decides to attack, just test the type of system seen or not interact at all.

Carroll and Grosu defined a signalling in which the type of a system is chosen randomly for a distribution of honeypots and real systems [18]. The defender chooses to be truthful or deceptive regarding the type of each system. Based on the received information, the attacker decides to attack, to withdraw, or condition his attack on testing the type of the system. The detection of a target adds additional cost to the attacker regardless of it being a normal system or a honeypot, but it mitigates the loss of the attacker incurred when attacking a honeypot. In [19], Pawlick and Zhu extended this work by considering the effect of determining the system type to be endogenous on the utility. It analyses two

models: a simple cheap-talk game and a cheap-talk game with evidence where the receiver can detect deception with some probability.

The core structure of our game is motivated from [18,19]. We refine the choices of the defender further i.e, choosing between deploying a high-interaction honeypot or a low-interaction honeypot or normal system, rather than just between honeypot or normal system. Further, we have motivated the parameters of the defender and the attacker from [20]. In [20], Li et al. have presented a simplistic model where the defender decides whether to deploy a honeypot or not and the attacker decides whether to attack or not using a complete imperfect dynamic game. In addition, [21], Li et al. used a Bayesian game to model a distributed honeypot network. Similar to our work, they consider a decoy factor of honeypot which could be conceived as the efficacy of each type of system in our model. Furthermore, we consider types of honeypots (high/low interaction) and propose optimal mix between the choice of a type of honeypot and real system rather than randomly changing the types.

3 Game Model and Assumptions

We model the interaction between the defender $\mathcal{D}$ and the attacker $\mathcal{A}$ as a sequential game with complete but imperfect information called the *Honeypot Type Selection Game* (HTSG), represented in Figure 1. Table 1 presents the list of symbols used in our model.

While deploying a new system, $\mathcal{D}$ has to decide whether it should include a high-interaction honeypot (H), or a low-interaction honeypot (L), or should be a system with no honeypot, i.e., a normal system (R). This choice of the defender is private information and is unknown to the attacker.

A low-interaction honeypot facilitates limited services such as internet protocol, network services and does not provide interaction with the operating system. They are easy to deploy, maintain and minimize the risk by containing the attacker's activities. High-interaction honeypots are more sophisticated, complex to implement and maintain, and they provide interaction with a real/virtual operating system [22].

We further assume that each type of system has an efficacy which we define as the probability of a system to be recognized as a real system by an attacker during reconnaissance. We represent these efficacies as a_L, a_H and p_R for type-L, type-H and type-R, respectively. This efficacy factor induces uncertainty in the attacker's decision. The defender aims at taking advantage of the information asymmetry to gather information about the attacker's behaviour and detecting potential cyber attacks. For example, [23] used honeypots to detect cyber attacks, [24] used honeypots to simulate and learn about Distributed Denial of Service (DDoS) attack on network infrastructure, and [25] used the data collected from honeypots to identify cyber attack trends.

The defender has to bear additional cost for choosing type-L or type-H system compared to the type-R system. This cost may be introduced by network throughput due to honeypot in the infrastructure, cost of implementing, deploy-

Table 1. List of Symbols

Symbol	Condition/Range	Description
a_H	$0 < a_H < 1$	Efficacy of type-H system
a_L	$0 < a_L < a_H$	Efficacy of type-L system
$b^{\mathcal{A}}$	$b^{\mathcal{A}} > 0$	Attacker's benefit on attacking type-R system
$b_H^{\mathcal{D}}$	$b_H^{\mathcal{D}} \geq c_H^{\mathcal{D}}$	Defender's benefit when type-H system is attacked
$b_L^{\mathcal{D}}$	$c_L^{\mathcal{D}} \leq b_L^{\mathcal{D}} < b_H^{\mathcal{D}}$	Defender's benefit when type-L system is attacked
$c_H^{\mathcal{D}}$	$c_H^{\mathcal{D}} > 0$	Cost of running a type-H system
$c_L^{\mathcal{D}}$	$0 < c_L^{\mathcal{D}} < c_H^{\mathcal{D}}$	Cost of running a type-L system
d	$d > b_H^{\mathcal{D}}$	Defender's loss when type-R system is attacked
$l_H^{\mathcal{A}}$	$l_H^{\mathcal{A}} > 0$	Attacker's loss on attacking type-H system
$l_L^{\mathcal{A}}$	$0 < l_L^{\mathcal{A}} < l_H^{\mathcal{A}}$	Attacker's loss on attacking type-L system
p_R	$0 < p_R \leq 1$	Efficacy of type-R system
p_1	$0 \leq p_1 \leq 1$	Attacker's belief about type-R with information set {L,R}
p_2	$0 \leq p_2 \leq 1$	Attacker's belief about type-R with information set {H,R}

ing and maintaining the honeypot and operational management costs. In our model, c_L^D and c_H^D represent the aggregate cost of running a type-L and type-H system. Based on these assumptions, we model HTSG to highlight the strategic aspects of the interaction. The leaf nodes present the payoffs for the action chosen by the players. The payoffs are represented in the form $\binom{x}{y}$, where x and y are the payoffs of $\mathcal{D}$ and $\mathcal{A}$, respectively.

4 Equilibria Analysis

This section analyses the equilibria of the proposed HTSG in Figure 1. We utilize the game-theoretic concept of the perfect Bayesian Nash equilibrium (PBNE) that helps us get an insight into the strategic behaviour of the players. PBNE refines the Bayesian Nash equilibrium to remove (some) implausible equilibria in sequential games [26]. PBNE, in the context of our game, is defined by the four requirements discussed in [27], and met below along our analysis.

From the payoffs in Figure 1, it can be seen that there is no preferred pure strategy for a player. This particular parametric configuration is prescribed to illustrate a network administrator's challenge in deciding which type of system to install in presence of a threat. To analytically determine the optimal choice, represented as a PBNE, we segment our analysis into four sections.

Condition 1: when $\mathcal{U}^D(L, A) > \mathcal{U}^D(H, A)$ and $\mathcal{U}^D(L, NA) \geq \mathcal{U}^D(H, NA)$

Condition 2: when $\mathcal{U}^D(L, A) > \mathcal{U}^D(H, A)$ and $\mathcal{U}^D(L, NA) < \mathcal{U}^D(H, NA)$

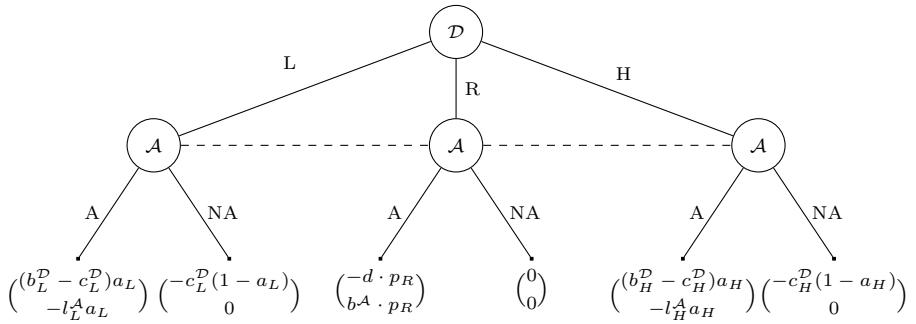

Fig. 1. Extensive form representation of the Honeypot Type Selection Game (HTSG) with the defender ($\mathcal{D}$) choosing between the types of system (type-L, type-H and type-R) and the attacker ($\mathcal{A}$) deciding to attack (A) or not attack (NA).

Condition 3: when $\mathcal{U}^D(L, A) \leq \mathcal{U}^D(H, A)$ and $\mathcal{U}^D(L, NA) < \mathcal{U}^D(H, NA)$

Condition 4: when $\mathcal{U}^D(L, A) \leq \mathcal{U}^D(H, A)$ and $\mathcal{U}^D(L, NA) \geq \mathcal{U}^D(H, NA)$

Having defined the necessary concepts, next, we determine the possible PBNEs of the game for the defined situations, where the PBNEs are strategy profiles and beliefs that satisfies all the four requirements described earlier.

Condition 1: This case refers to the situation when L is dominating H i.e., $\mathcal{U}^{\mathcal{D}}(L, A) > \mathcal{U}^{\mathcal{D}}(H, A)$ and $\mathcal{U}^{\mathcal{D}}(L, NA) \geq \mathcal{U}^{\mathcal{D}}(H, NA)$ implying that H can be removed form the strategy set of the defender reducing the 3×2 payoff matrix to 2×2 payoff matrix. From the payoff matrix, it can observed that none of the players have preferred strategy. Following the requirements for a PBNE, we have

a) *Belief consistency*: Requirement 1 states that if the play of the game reaches a player's non-singleton information set then the player with the move must have a belief about which node has been reached. Let the attacker believes that the defender has chosen R with probability p_1.
b) *Attacker's sequentially rational condition given updated beliefs*: Given the attacker's belief p_1, we calculate the payoffs for playing A and NA and choose the strategy that maximizes his payoff. For strategy A to be sequentially rational $\mathcal{U}^A(NA) < \mathcal{U}^A(A)$ which gives

$$p_1 > \frac{a_L \cdot l_L^A}{p_R \cdot b^A + a_L \cdot l_L^A} \tag{1}$$

c) *Defender's sequentially rational condition given attacker's best response*: Knowing the best responses of the attacker i.e. A for $p_1 > \frac{a_L \cdot l_L^A}{p_R \cdot b^A + a_L \cdot l_L^A}$ and NA for $p_1 < \frac{a_L \cdot l_L^A}{p_R \cdot b^A + a_L \cdot l_L^A}$, we determine the best response of the defender. When the attacker prefers to attack, defender's best response is play L and for NA

the defender's best response in R. Thus, the PBNEs of the game are

$$\begin{cases} (L, A;\ p_1), & \text{where } p_1 > \frac{a_L \cdot l_L^A}{p_R \cdot b^A + a_L \cdot l_L^A} \\ (R, NA;\ p_1), & \text{where } p_1 < \frac{a_L \cdot l_L^A}{p_R \cdot b^A + a_L \cdot l_L^A} \end{cases}$$

Note that the PBNEs include the updated beliefs of the attacker satisfying the last two requirements.

Condition 2: This section presents the analysis when $\mathcal{U}^{\mathcal{D}}(L, A) > \mathcal{U}^{\mathcal{D}}(H, A)$ and $\mathcal{U}^{\mathcal{D}}(L, NA) < \mathcal{U}^{\mathcal{D}}(H, NA)$. We solve the 3×2 matrix game with graphical solution approach. Let the attacker chooses A with probability α and NA with probability $1 - \alpha$. The attacker's average payoff when the defender plays

$$\begin{cases} L, & \mathcal{U}^A = \alpha \cdot a_L \cdot (-l_L^A) \\ R, & \mathcal{U}^A = \alpha \cdot p_R \cdot b^A \\ H, & \mathcal{U}^A = \alpha \cdot a_H \cdot (-l_H^A) \end{cases}$$

We plot these linear functions for $0 \leq \alpha \leq 1$. For a fixed value of α, the attacker aims at maximizing his average payoff. This is obtained by finding α that achieves the maximum in the lower envelop of these functions. From figure 2, this should be at the intersection of the three lines at $\alpha = 0$.

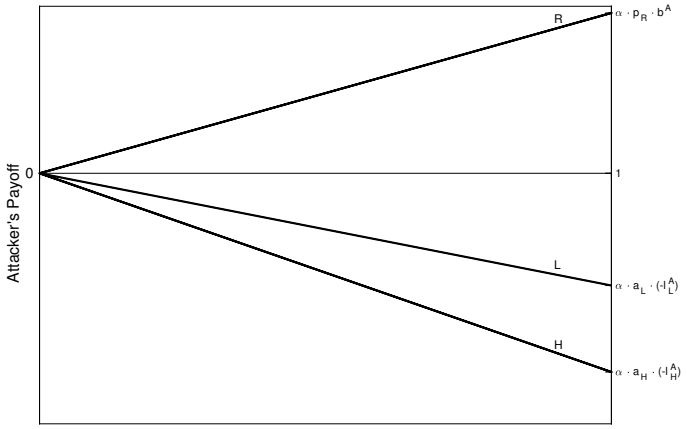

Fig. 2. Attacker's expected payoffs for attacking against defender's strategy.

As more than two lines passes through the intersection point, we choose sets of two lines with opposite slopes. Applying the methodology as in Case A with lines L, R and attacker's belief on defender playing R with probability p_2, we obtain the same PBNEs as in Case A. With lines R and H, PBNEs are

$$\begin{cases} (H, A;\ p_2), & \text{where } p_2 > \frac{a_H \cdot l_H^A}{p_R \cdot b^A + a_H \cdot l_H^A} \\ (R, NA;\ p_2), & \text{where } p_2 < \frac{a_H \cdot l_H^A}{p_R \cdot b^A + a_H \cdot l_H^A} \end{cases}$$

Table 2. Overview of Equilibria of the HTSG

	$\mathcal{U}^D(L,NA) < \mathcal{U}^D(H,NA)$	$\mathcal{U}^D(L,NA) \geq \mathcal{U}^D(H,NA)$
$\mathcal{U}^D(L,A) \leq \mathcal{U}^D(H,A)$		(L,A; p_1) $p_1 \geq \frac{a_L \cdot l_L^A}{p_R \cdot b^A + a_L \cdot l_L^A}$
	(H,A; p_2) $p_2 \geq \frac{a_H \cdot l_H^A}{p_R \cdot b^A + a_H \cdot l_H^A}$	(R,NA; p_1) $p_1 < \frac{a_L \cdot l_L^A}{p_R \cdot b^A + a_L \cdot l_L^A}$
	(R,NA; p_2) $p_2 < \frac{a_H \cdot l_H^A}{p_R \cdot b^A + a_H \cdot l_H^A}$	(H,A; p_2) $p_2 \geq \frac{a_H \cdot l_H^A}{p_R \cdot b^A + a_H \cdot l_H^A}$
		(R,NA; p_2) $p_2 < \frac{a_H \cdot l_H^A}{p_R \cdot b^A + a_H \cdot l_H^A}$
$\mathcal{U}^D(L,A) > \mathcal{U}^D(H,A)$	(L,A; p_1) $p_1 \geq \frac{a_L \cdot l_L^A}{p_R \cdot b^A + a_L \cdot l_L^A}$	
	(R,NA; p_1) $p_1 < \frac{a_L \cdot l_L^A}{p_R \cdot b^A + a_L \cdot l_L^A}$	(L,A; p_1) $p_1 \geq \frac{a_L \cdot l_L^A}{p_R \cdot b^A + a_L \cdot l_L^A}$
	(H,A; p_2) $p_2 \geq \frac{a_H \cdot l_H^A}{p_R \cdot b^A + a_H \cdot l_H^A}$	(R,NA; p_1) $p_1 < \frac{a_L \cdot l_L^A}{p_R \cdot b^A + a_L \cdot l_L^A}$
	(R,NA; p_2) $p_2 < \frac{a_H \cdot l_H^A}{p_R \cdot b^A + a_H \cdot l_H^A}$	

We determine all the possible PBNEs for HTSG by exhaustively applying this methodology over the *Condition 3* and *Condition 4*, described earlier. Table 2 illustrates the solution space of HTSG.

5 Simulation Results

In this section, we present the results of our simulations which were established by comparing our game-theoretic (HTSG) approach with a non-game-theoretic (No GT) approach where the defender randomly chooses the type of the systems to deploy. We present the players' utility by varying the probability p_R of the attacker detecting a real system, and second by varying the number of honeypots in the network. Furthermore, we represent the players' utility in HTSG with different values of beliefs p_1 and p_2.

First, we consider the case when no game theory approach is used. We work with ten systems for this simulation and the defender randomly decides the type of system to install. We first assume that the defender installs five High-interaction honeypots with different values of efficacy $a_H = 0.69$, $a_H = 0.71$, $a_H = 0.73$, $a_H = 0.75$, $a_H = 0.79$; four low-interaction honeypots with efficacy values $a_L = 0.45$, $a_L = 0.49$, $a_L = 0.51$ and $a_L = 0.53$; and one real system. We consider different p_R values. Figure 3 illustrates both players' utilities. We observe that the defender's utility decreases by 16% and the attacker's utility increases by approximately 10% when p_R increases. This is expected because with increasing p_R attacker becomes more capable of detecting the presence of real systems in the network and attacking them.

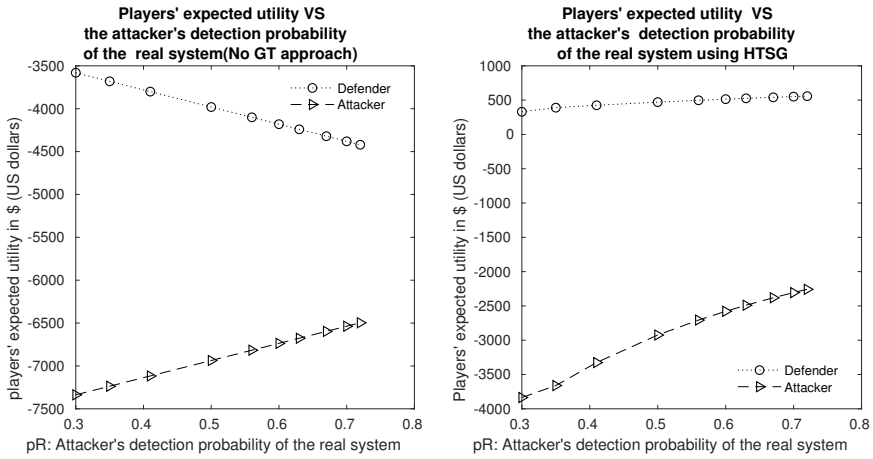

Fig. 3. Players' expected utilities for different attacker's detection capabilities.

Second, the defender plays the equilibrium strategy of HTSG which gives an advice to the defender about what configuration to choose among (L,R,H). We also vary p_R and set $p_1 = 0.4$ and $p_2 = 0.77$. Figure 3 shows that the defender's expected utility improves by 112.62% compared to the No GT case for $p_R = 0.72$.

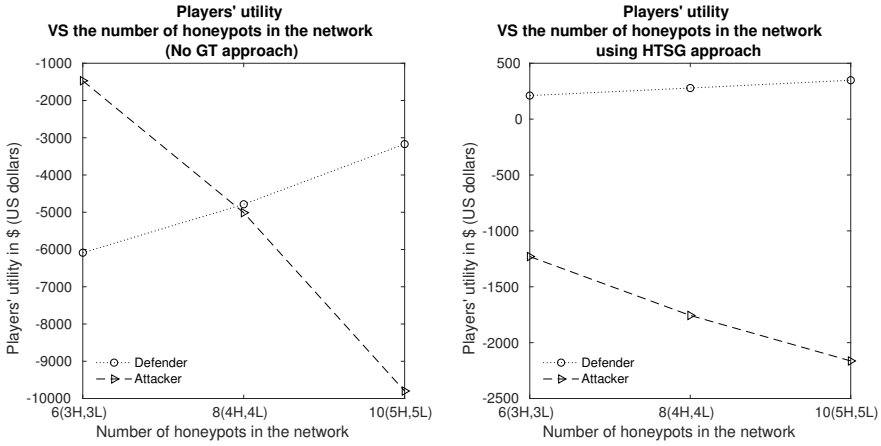

Fig. 4. Players' expected utilities VS the number of honeypots in the network.

Similarly, we consider the case of No GT, but this time we vary the number of High-interaction and Low-interaction honeypots the defender installs each time, by keeping the attacker's probability of detecting the real system fixed $p_R = 0.5$. We plot the players' utilities in Figure 4. The figure shows that the defender's utility increases with the number of honeypots; getting improved by 100% when increasing the number of honeypots by 2/3. For the same increase

in the number of honeypots, the attacker's utility decreases by 33% when the number of honeypots goes up.

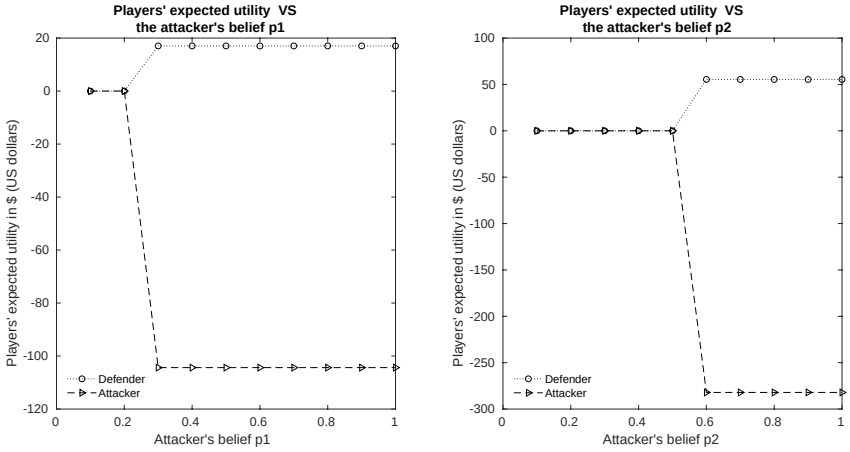

Fig. 5. Players' expected utilities VS the attacker's beliefs p_1 and p_2 for the HTSG approach.

We also simulated the case when the HTSG equilibrium strategy is played and the number of honeypots varies and the probability of the attacker detecting the real system equals 0.5 ($p_R = 0.5$) with $p_1 = 0.4$ and $p_2 = 0.6$. Figure 4 shows that the defender's utility improves by 110.98% compared to the No GT case for 10 honeypots.

Last, Figure 5 shows that the utility changes at the belief value $p_1 = 0.3$ for both players, because at this point the equilibrium changes from (R,NA,p_1) to (L,A,p_1). The utility also changes at $p_2 = 0.6$, because for this value, the equilibrium changes from (R,NA,p_2) to (H,A,p_2).

6 Conclusions

In this work, we developed a game-theoretic model to analyze the challenge of the network administrator/defender in selecting among the following types of systems: a low-interaction honeypot, a high-interaction honeypot and a system with no honeypot with each having its own set of costs and benefits. If the defender chooses to deploy a honeypot, her aim is to lure the attacker to this honeypot to gain threat intelligence. On the other hand, the attacker has to decide whether to attack or not given the different costs and benefits of both choices. This interaction between the players is modeled as a dynamic game of complete but imperfect information. We derived its PBNE solutions and have presented numerical results with the optimal probability of deploying a type of system for the defender and the optimal attack probability for the attacker under different parametric conditions.

This paper is a first step towards implementing game-theoretic strategies in actual smart grid networks as part of the H2020 SPEAR project. To this end, we are planning to collect data from these networks to instantiate the game parameters and derive the corresponding equilibria. We will then apply the assess how these equilibria improve threat intelligence and defence of the smart grid network as opposed to existing strategies used by the project end users. In terms of theoretic extensions of this paper, future work may allow to consider a more complex model capturing a number of different costs (e.g., deployment, configuration, maintenance), related to honeypots, rather than congregated values. Secondly, future work may allow repeated version of the game with belief update schemes and dynamic choice of the type of system to deploy based on the updated belief. In this case, we shall investigate the trade-offs between playing instantiated (single-shot) version and iterative version of the game.

In addition, in contrast to the current work, future work could investigate the situation where the defender has multiple honeypots in the network. Finally, we could consider a more sophisticated attacker who is able to detect the presence of honeypots in the network using anti-honeypots techniques [15] and assess how the difference in efficacies of the honeypot types affect the players' decision.

Acknowledgement

We thank the anonymous reviewers for their comments.
Nadia Boumkheld and Emmanouil Panaousis are supported by the H2020 SPEAR grant agreement, no 787011.

References

1. Li, X., Liang, X., Lu, R., Shen, X., Lin, X., Zhu., H.: Securing smart grid: cyber attacks, countermeasures, and challenges. IEEE Communications Magazine **50**(8) (2012)
2. Petrovic, T., Echigo, K., Morikawa, H.: Detecting Presence From a WiFi Router's Electric Power Consumption by Machine Learning. IEEE Access **6** (2018) 9679–9689
3. Barnum, S.: Standardizing cyber threat intelligence information with the structured threat information expression (stix). Mitre Corporation **11** (2012) 1–22
4. Pawlick, J., Colbert, E., Zhu, Q.: A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy. arXiv preprint arXiv:1712.05441 (2017)
5. Jicha, A., Patton, M., Chen, H.: Scada honeypots: An in-depth analysis of conpot. In: 2016 IEEE conference on intelligence and security informatics (ISI), IEEE (2016) 196–198
6. Mairh, A., Barik, D., Verma, K., Jena, D.: Honeypot in network security: a survey. In: Proceedings of the 2011 international conference on communication, computing & security, ACM (2011) 600–605
7. Nawrocki, M., Wählisch, M., Schmidt, T.C., Keil, C., Schönfelder, J.: A survey on honeypot software and data analysis. arXiv preprint arXiv:1608.06249 (2016)

8. La, Q.D., Quek, T.Q., Lee, J., Jin, S., Zhu, H.: Deceptive attack and defense game in honeypot-enabled networks for the internet of things. IEEE Internet of Things Journal **3**(6) (2016) 1025–1035
9. Williamson, S.A., Varakantham, P., Hui, O.C., Gao, D.: Active malware analysis using stochastic games. In: Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems-Volume 1, International Foundation for Autonomous Agents and Multiagent Systems (2012) 29–36
10. Wagener, G., Dulaunoy, A., Engel, T., et al.: Self adaptive high interaction honeypots driven by game theory. In: Symposium on Self-Stabilizing Systems, Springer (2009) 741–755
11. Rowe, N.C., Custy, E.J., Duong, B.T.: Defending cyberspace with fake honeypots. JCP **2**(2) (2007) 25–36
12. Píbil, R., Lisý, V., Kiekintveld, C., Bosansky, B., Pechouc, M.: Game theoretic model of strategic honeypot selection in computer networks. International Conference on Decision and Game Theory for Security(GameSec) (2012)
13. Garg, N., Grosu, D.: Deception in honeynets: A game-theoretic analysis. In: 2007 IEEE SMC Information Assurance and Security Workshop, IEEE (2007) 107–113
14. Çeker, H., Zhuang, J., Upadhyaya, S., La, Q.D., Soong, B.H.: Deception-based game theoretical approach to mitigate dos attacks. In: International Conference on Decision and Game Theory for Security, Springer (2016) 18–38
15. Wang, K., Du, M., Maharjan, S., Sun, Y.: Strategic honeypot game model for distributed denial of service attacks in the smart grid. IEEE Transactions on Smart Grid **8**(5) (2017) 2474–2482
16. Wagener, G., State, R., Engel, T., Dulaunoy, A.: Adaptive and self-configurable honeypots. In: 12th IFIP/IEEE international symposium on integrated network management (IM 2011) and workshops, IEEE (2011) 345–352
17. Hayatle, O., Otrok, H., Youssef, A.: A game theoretic investigation for high interaction honeypots. In: 2012 IEEE International Conference on Communications (ICC), IEEE (2012) 6662–6667
18. Carroll, T.E., Grosu, D.: A game theoretic investigation of deception in network security. Security and Communication Networks **4**(10) (2011) 1162–1172
19. Pawlick, J., Zhu, Q.: Deception by design: evidence-based signaling games for network defense. arXiv preprint arXiv:1503.05458 (2015)
20. Li, H., Yang, X., Qu, L.: On the offense and defense game in the network honeypot. In: Advances in Automation and Robotics, Vol. 2. Springer (2011) 239–246
21. Li, Y., Shi, L., Feng, H.: A game-theoretic analysis for distributed honeypots. Future Internet **11**(3) (2019) 65
22. Mokube, I., Adams, M.: Honeypots: concepts, approaches, and challenges. In: Proceedings of the 45th annual southeast regional conference, ACM (2007) 321–326
23. Jasek, R., Kolarik, M., Vymola, T.: Apt detection system using honeypots. In: Proceedings of the 13th International Conference on Applied Informatics and Communications (AIC'13), WSEAS Press. (2013) 25–29
24. Weiler, N.: Honeypots for distributed denial-of-service attacks. In: Proceedings. Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, IEEE (2002) 109–114
25. Kelly, G., Gan, D.: Analysis of attacks using a honeypot. In: International Cybercrime, Security and Digital Forensics Conference. (2011)
26. Fudenberg, D., Tirole, J.: Perfect bayesian equilibrium and sequential equilibrium. journal of Economic Theory **53**(2) (1991) 236–260
27. Gibbons, R.: A primer in game theory. Harvester Wheatsheaf (1992)