2023 IEEE 34th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC) | 978-1-6654-6483-3/23/$31.00 ©2023 IEEE | DOI: 10.1109/PIMRC56721.2023.10293910

Cyber Deception under Strategic and Irrationality Considerations

Satyaki Nan
Department of Computing
Georgia Southwestern State University
Americus, GA, USA
satyaki.nan@gsw.edu

Swastik Brahma
Department of Computer Science
University of Cincinnati
Cincinnati, OH, USA
brahmask@ucmail.uc.edu

***Abstract*— This paper presents a novel cyber deception technique that can employ fake nodes to deceive attackers. To devise such a technique, the paper uses game theory to model strategic interactions between a defender and an attacker, and prospect theory to model their possible cognitive biases, while diligently accounting for cost factors associated with attack-defense strategies. Nash Equilibrium (NE)-based strategies for deploying our devised deception tactics when the defender and the attacker are fully rational in nature as well as when they may exhibit behavioral irrationalities have been analytically characterized in the paper. Among others, our results delineate how vulnerabilities of conventional defense resources can influence adoption of deception-based defenses. Numerous simulation results have been presented that provide important insights into our developed deception-based defense strategies.**

***Index Terms*—Cyber deception, Game theory, Prospect theory, Security.**

I. Introduction

Deception has found use in warfare and politics in the past. Recently, researchers and practitioners have started to investigate the use of deception for designing secure networks. Intuitively, it can become easier to launch a successful attack if the targeted system has no deception-based defense tactics, granting the attacker clear path and access to gain sensitive information as it explores the space of real systems. Without deception, all paths are real and the attacker can relatively easily gain exploitable information. Deception strategies can help to reduce the likelihood of an attacker's success, lessen the cost of defense from deception-less situations, and complement conventional defense measures for enhancing security.

While deception-based defense techniques have been explored by past work to some extent [1]–[7], such works have had a focus on designing deception schemes when such schemes are the ones that are solely used as a defense measure against security threats. In reality, however, it can be expected that a system designer use deception-based tactics to work alongside conventional defense resources (e.g., an anti-malware software) to defend the system. In such a scenario, design of the deception technique would naturally depend on characteristics and capabilities of the conventional defense resource, a perspective which, however, has been overlooked by past work but has been made an important aspect in the design of our proposed deception technique.

This work was supported in part by the NSF under Award Number CCF-2302197 and in part by the University of Cincinnati.

Furthermore, to deploy our devised deception technique in a strategic context, we have not only analytically characterized NE-based attack-defense strategies from a game theoretic perspective [8] considering the system defender and an attacker to be fully rational in nature, but have also characterized such equilibrium strategies considering them to have *cognitive biases* which make them exhibit complex behavioral irrationalities. It should be noted that consideration of behavioral irrationalities, which can greatly impact attack-defense strategies in deceptive environments, largely remain uncharted and is among a novel contribution of our paper. While we initiated some work on the consideration of behavioral irrationalities in [9], the results obtained in our initial work were restricted to special cases with our current work addressing a far more generalized scenario.

Cognitive biases of the defender and the attacker can stem from their subjective perceptions of uncertainties involved in decision making under risk [9]–[11]. To model cognitive biases of the defender and the attacker, in this paper, we have used Prospect Theory [12], which is a Nobel Prize winning work that provides a descriptive model of human decision-making under risk. The defense strategies developed in the paper has applications in various modern adversarial systems, such as to execute a computational task securely in Internet-of-Battlefield-Things (IoBT) [13]. Specifically, the main contributions of the paper are as follows:

- A novel deception technique is presented for executing a computational task securely by deceiving attackers using fake nodes. The presented deception technique accounts for characteristics of conventional defense resources that could be deployed in parts of the system as well as can adapt to costs involved with attack-defense strategies.
- NE-based strategies for deploying our devised deception tactics (from a defender's perspective) and countering them (from an attacker's perspective) have been analytically characterized considering the defender and the attacker to be strategic and fully rational in nature.
- Further, NE-based attack-defense strategies under our devised deception tactics have also been analytically characterized considering the defender and the attacker to be strategic entities who have cognitive biases which make them exhibit behavioral irrationalities.
- Numerous simulation results have been presented which

provide important insights into our devised deception strategies.

The rest of the paper is organized as follows. Section II presents our proposed deception technique and characterizes NE-based attack-defense strategies in its context considering the defender and the attacker to be strategic and fully rational entities. Section III characterizes NE-based attack-defense strategies under our devised deception tactics considering the defender and the attacker to be strategic entities who exhibit behavioral irrationalities. Section IV presents simulation results that provide important insights into our developed deception tactics. Finally, Section V concludes the paper.

II. Deception under Defender and Attacker Exhibiting Full Rationality

This section introduces our proposed cyber deception technique while adopting a game theoretic perspective to characterize NE-based strategies for deploying our devised deception tactics (from a system defender's viewpoint) and countering them (from an attacker's viewpoint). The defender and the attacker are considered to be strategic and fully rational entities in this section. To illustrate our proposed deception technique, we first consider the availability of two servers which can be used for deception before generalizing our results.

A. Deception using two servers

Consider a system comprised of two servers, labeled Server 1 and Server 2, with Server 1 (without loss of generality) having a conventional defense resource[2] (DR) installed in it. Suppose that the cost of deploying the DR is C and that the probability of successfully compromising it is P_C. Consider an attacker (A) who is aware of which server has the DR installed[3] with the attacker also incurring a cost of C to attack the server having the DR installed.

Suppose now that a defender (D) wants to execute a computational task securely by using one of the two available servers (while using the other one as an unused 'fake' server to deceive A), with A seeking to adopt strategies to prevent D from running the computational task successfully. Consider that the benefit of D from performing the computational task successfully is B^D and that of A from a successful attack is B^A. The dilemma for D is: *Should D run the task on the server having the DR installed (hoping that A is unable to compromise the DR) or on the server without any DR (hoping that A is lured towards attacking the server having the DR installed)?* Likewise, the dilemma for A is: *Should A attack the server having the DR installed (thinking that D would rely on the capabilities of the DR) or on the server without any DR (thinking that D may have tactically wanted to mislead A into attacking the server with the DR installed)?*

Table I shows the notations used. The payoff matrix of the game is shown in Table II, where P_D is the probability of the defender choosing to execute the task on the server having the DR (i.e., Server 1), and P_A is the probability of the attacker choosing to attack the server having the DR (i.e., Server 1). As can be seen from the payoff matrix in Table II, the game has a unique pure strategy Nash Equilibrium (NE) corresponding to D running the task on the server having the DR and A attacking the server without any DR, which, however, exists only when $P_C \leq C/B^A$. In the next lemma, we present the mixed strategy NE of the game.

Lemma 1. *When two servers are available, with one server having a DR installed, at NE, D executes the computational task on the server having the DR with a probability $P_D^* = \left(\frac{1}{1+P_C}\right)\left(1+\frac{C}{B^A}\right)$ and A attacks the server having the DR with a probability $P_A^* = \frac{1}{1+P_C}$.*

Proof. The expected utility of D (say, E_D^{DR}) from executing the task on the server that has the DR is

$$E_D^{DR} = ((1-P_C)*B^D - C)*P_A + (B^D - C)*(1-P_A) \quad (1)$$

Similarly, the expected utility of D (say, $E_D^{\overline{DR}}$) from executing the task on the server that does not have any DR is

$$E_D^{\overline{DR}} = (B^D - C)*P_A + (-C)*(1-P_A) \quad (2)$$

Since D must be indifferent between adopting one of its strategies at the mixed strategy NE, equating (1) and (2), we get

$$P_A^* = \frac{1}{1+P_C} \quad (3)$$

Now, the expected utility of A (say, E_A^{DR}) from attacking the server that has the DR is

$$E_A^{DR} = (P_C * B^A - C)*P_D + (-C)*(1-P_D) \quad (4)$$

Similarly, the expected utility of A (say, $E_A^{\overline{DR}}$) from attacking the server that does not have any DR is

$$E_A^{\overline{DR}} = (0)*P_D + (B^A)*(1-P_D) \quad (5)$$

Since A must be indifferent between adopting one of its strategies at the mixed strategy NE, equating (4) and (5), we get

$$P_D^* = \left(\frac{1}{1+P_C}\right)\left(1+\frac{C}{B^A}\right) \quad (6)$$

This proves the lemma. □

Next, we generalize our results by considering the availability of N servers that can be deployed for cyber deception.

B. Deception using N servers

Consider the availability of N servers, with N_{DR} servers having the DR installed and $N_{\overline{DR}} = N - N_{DR}$ servers without any DR. Similar to the model described earlier, consider C to be the cost of deploying/attacking the DR in a server and P_C to be probability with which the DR can be successfully compromised, with A being aware of which servers have the DR installed. Consider, as before, D to obtain a benefit B^D from running the computational task successfully and A to obtain a benefit B^A from launching an attack that successfully cripples the task.

[2]The defense resource, for e.g., can correspond to an anti-malware software.

[3]Attackers typically gather such information via probing techniques [2].

Notation	Description
D	Defender
A	Attacker
P_D	Prob. of the defender using a server having the defense resource
P_A	Prob. of the attacker attacking a server having the defense resource
$1-P_D$	Prob. of the defender using a server without any defense resource
$1-P_A$	Prob. of the attacker attacking a server without any defense resources
B^A	Benefit of the attacker from a successful attack
B^D	Benefit of the defender from performing the computational task successfully
C	Cost of deploying/attacking the defense resource
P_C	Prob. of successfully compromising the defense resource

TABLE I
NOTATIONS USED IN ANALYSIS

D \ A	$DR\ Installed\ (P_A)$	$DR\ not\ Installed\ (1-P_A)$
$DR\ Installed\ (P_D)$	$((1-P_C)*B^D-C),\ P_C*B^A-C$	$B^D-C,\ 0$
$DR\ not\ Installed\ (1-P_D)$	$B^D-C,\ -C$	$-C,\ B^A$

TABLE II
PAYOFF MATRIX OF DEFENDER (D) AND ATTACKER (A). HERE, P_D AND P_A ARE THE PROBABILITIES OF D AND A CHOOSING THE SERVER HAVING THE DR INSTALLED, RESPECTIVELY.

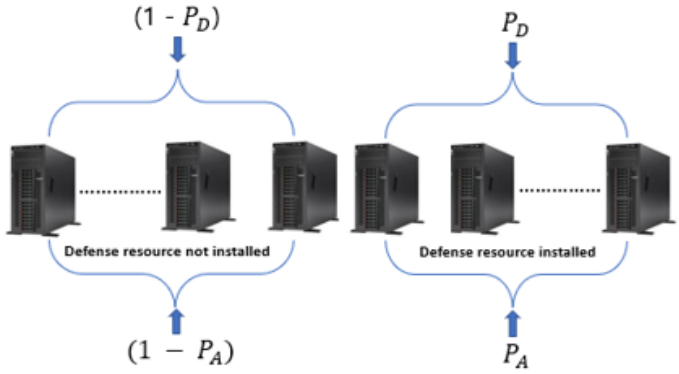


Fig. 1. N available servers depicting attack-defense strategies.

To analyze the mixed strategy NE of the game, as shown in Fig. 1, consider that D chooses to run the task on one of the servers that have the DR with a probability P_D (and chooses to run the task on one of the servers that do have any DR with a probability $1-P_D$). Likewise, suppose that A chooses to attack one of the servers that have the DR with a probability P_A (and chooses to attack one of the servers that do have any DR with a probability $1-P_A$). Consider that D and A both choose a specific server from among their chosen type (i.e., from among the servers that have the DR installed and ones that don't) with a uniform probability. It can be shown that the game has a unique pure strategy NE corresponding to D choosing to run the task on a server that has the DR and A choosing to attack a server that does not have any DR, which, however, holds only when $P_C \leq CN_{DR}/B^A$. In the next theorem, we present the mixed strategy NE of the game, which generalizes the result that was presented in Lemma 1.

THEOREM 1. *When N servers are available, with N_{DR} servers having the DR installed and $N_{\overline{DR}}$ servers without any DR, at NE, D chooses to run the task on a server that has the DR with a probability $P_D^* = \left(\frac{1}{1+\frac{N_{\overline{DR}}}{N_{DR}}P_C}\right)\left(1+\frac{CN_{\overline{DR}}}{B^A}\right)$ and A chooses to attack a server that has the DR installed with a probability $P_A^* = \left(\frac{1}{1+\frac{N_{\overline{DR}}}{N_{DR}}P_C}\right)$.*

Proof. The expected utility of D from choosing to run the task on a server that has the DR installed is

$$E_D^{DR} = B^D\left[\left\{\frac{N_{DR}-1}{N_{DR}}+\frac{1-P_C}{N_{DR}}\right\}P_A+(1-P_A)\right]-CN_{DR} \tag{7}$$

Similarly, the expected utility of D from choosing to run the task on a server that does not have any DR installed is

$$E_D^{\overline{DR}} = B^D\left[\left\{\frac{N_{\overline{DR}}-1}{N_{\overline{DR}}}\right\}(1-P_A)+P_A\right]-CN_{DR} \tag{8}$$

Since D must be indifferent between adopting one of its strategies at the mixed strategy NE, equating (7) and (8), and simplifying, yields the equilibrium strategy of A as given in the theorem.

Now, the expected utility of A from attacking a server that has the DR installed is

$$E_A^{DR} = B^A\left\{\binom{N_{DR}}{1}\frac{1}{N_{DR}}\frac{1}{N_{DR}}P_C\right\}P_D-C \tag{9}$$

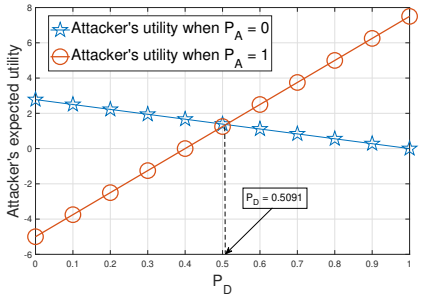
Similarly, the expected utility of A from attacking a server that does not have any DR installed is

$$E_A^{\overline{DR}} = \left[\binom{N_{\overline{DR}}}{1}\frac{1}{N_{\overline{DR}}}\frac{1}{N_{\overline{DR}}}B^A\right](1-P_D) \tag{10}$$

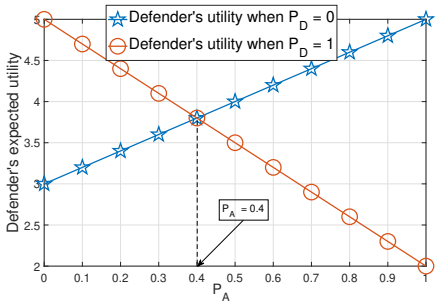
Since A must be indifferent between adopting one of its strategies at the mixed strategy NE, equating (9) and (10), and simplifying, yields the equilibrium strategy of D as given in the theorem. This proves the theorem. □

In Fig. 2, we provide numerical results to corroborate the above results. For the figure, we consider B^A = 50, C = 5, P_C = 0.5, N = 20, N_{DR} = 2, and $N_{\overline{DR}}$ = N - N_{DR} = 18. In Fig. 2(a), we show A's expected utility versus the probability (P_D) of D choosing to run the task on a server that has the DR installed. Against every P_D, the figure plots A's utility from choosing $P_A = 0$ (i.e., from always attacking a server that does not have any DR installed) as well as A's utility

from choosing $P_A = 1$ (i.e., from always attacking a server that has the DR installed). The point where the two utilities intersect makes A's expected utility from attacking a server that has the DR installed to be equal to that of attacking one that does not have any DR (as needed at the mixed strategy NE), which, as can be seen from the figure, occurs at P_D = 0.5091, and which can be shown to tally with D's NE strategy found from Theorem 1.



(a) Attacker's expected utility versus the defender's strategy.



(b) Defender's expected utility versus the attacker's strategy.

Fig. 2. Expected utilities of the defender and the attacker versus their opponent's strategies.

In Fig. 2(b), we show D's expected utility versus the probability (P_A) of A choosing to attack a server that has the DR installed. Against every P_A, the figure plots D's utility from choosing $P_D = 0$ (i.e., from always running the task on a server that does not have any DR installed) as well as D's utility from choosing $P_D = 1$ (i.e., from always running the task on a server that has the DR installed). The point where the two utilities intersect makes D's expected utility from always running the task on a server that has the DR installed to be equal to that of running the task on a server that does not have any DR (as needed at the mixed strategy NE), which, as can be seen from the figure, occurs at P_A = 0.40, and which can be shown to tally with A's NE strategy found from Theorem 1. This corroborates Theorem 1.

In the next section, we consider D and A to be strategic entities who exhibit behavioral irrationalities.

III. Deception under Defender and Attacker Exhibiting Behavioral Irrationalities

In this section, we characterize NE-based strategies for deploying our devised deception tactics (from D's perspective) and countering them (from A's perspective) considering them to be strategic entities who have cognitive biases which make them exhibit behavioral irrationalities. Our analysis in this section employs game theory to model strategic interactions between D and A, and prospect theory [12] to model their cognitive biases. We first provide a brief introduction to prospect theory before presenting our results.

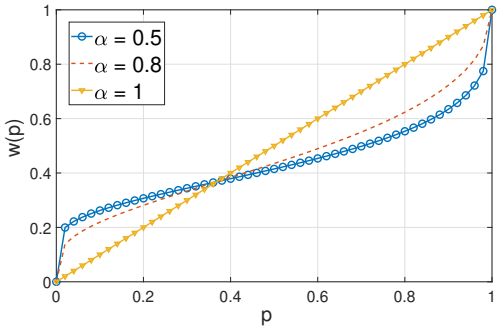


Fig. 3. Behavior of the Prelec function

A. Prospect Theory

Prospect theory provides a descriptive model of human decision-making behavior and says that humans, due to their cognitive biases, perceive probabilities in a subjective manner which makes them deviate from expected utility theoretic norms. In particular, the theory says that humans overweigh smaller probabilities but underweigh larger probabilities, a well accepted function for modeling which is the Prelec function [14], which is defined as

$$w(p) = exp(-(-\ln p)^{\alpha}),\ 0 < \alpha \leq 1 \qquad (11)$$

where p is the probability of an event and α is the probability distortion coefficient which models the degree of subjectivity (irrationality) of a human. A smaller value of α results in a more curved Prelec function, signifying a more cognitively biased human, as shown in Fig. 3.

Based on such subjective perception of probabilities, a cognitively biased human agent's *prospect theoretic* utility from a gamble that can lead to outcomes having valuations $x_1, x_2, \cdots, x_N$ with probabilities $p_1, p_2, \cdots, p_N$, respectively, is $\sum_{i=1}^{N} x_i w(p_i)$, which clearly deviates from norms followed by the conventional expected utility theoretic regime. In the following, we account for such deviations in the design and analysis of our proposed cyber deception tactics.

B. Deception using N servers under behavioral irrationalities

Consider a model similar to the one described in Section II-B, where there are N available servers, with N_{DR} servers having the DR installed and $N_{\overline{DR}} = N - N_{DR}$ servers without any DR. Consider C to be the cost of deploying/attacking the DR in a server, P_C to be the probability with which the DR can be successfully compromised, and A to be aware of which servers have the DR installed. Consider, as before, D to obtain a benefit B^D from running the computational task successfully and A to obtain a benefit B^A from launching an attack that successfully cripples the task, with D and A acting strategically against each other.

To analyze the mixed strategy NE of the game, consider D and A to choose a server that has the DR installed with

the probabilities P_D and P_A, respectively, with D and A choosing a specific server from among their chosen type with a uniform probability. Further, consider D and A to be cognitively biased in nature who perceive various probabilistic structures involved in the attack-defense process in a subjective manner (following (11)). In the next theorem, we characterize the mixed strategy NE of the game.

THEOREM 2. *When D and A are cognitively biased, at NE, D chooses to run the computational task on a server that has the DR installed with a probability P_D^* that corresponds to the root of the equation*

$$w\left(\binom{N_{DR}}{1}\frac{1}{N_{DR}}\frac{P_C P_D}{N_{DR}}\right) - w\left(\frac{1-P_D}{N_{\overline{DR}}}\right) - \frac{C}{B^A} = 0 \quad (12)$$

and A attacks a server that has the DR installed with a probability $P_A^* = \frac{1}{1+\frac{N_{\overline{DR}}}{N_{DR}}P_C}$.

Proof. The prospect theoretic utility (say, PT_D^{DR}) of D from choosing to run the computational task on one of the N_{DR} servers that have the DR installed is

$$PT_D^{DR} = B^D w\left(\left(\frac{N_{DR}-1}{N_{DR}} + \frac{1-P_C}{N_{DR}}\right)P_A + (1-P_A)\right) \quad (13)$$

Similarly, the prospect theoretic utility (say, $PT_D^{\overline{DR}}$) of D from choosing to run the computational task on one of the $N_{\overline{DR}}$ servers that do not have any DR is

$$PT_D^{\overline{DR}} = B^D w\left(\left(\frac{N_{\overline{DR}}-1}{N_{\overline{DR}}}\right)(1-P_A) + P_A\right) \quad (14)$$

Since D must be indifferent between adopting one of its strategies at the mixed strategy NE, equating (13) and (14), and simplifying, yields the equilibrium strategy of A as given in the theorem.

Now, the prospect theoretic utility (say, PT_A^{DR}) of A from choosing to attack one of the N_{DR} servers that have the DR installed is

$$PT_A^{DR} = B^A w\left(\binom{N_{DR}}{1}\frac{1}{N_{DR}}\frac{P_C P_D}{N_{DR}}\right) - C \quad (15)$$

Similarly, the prospect theoretic utility (say, $PT_A^{\overline{DR}}$) of A from choosing to attack one of the $N_{\overline{DR}}$ servers that do not have any DR is

$$PT_A^{\overline{DR}} = B^A w\left(\frac{1-P_D}{N_{\overline{DR}}}\right) \quad (16)$$

Since A must be indifferent between adopting one of its strategies at the mixed strategy NE, equating (15) and (16), and simplifying, yields (12), which characterizes D's strategy at equilibrium. This proves the theorem. □

1) Existence of Nash Equilibrium: Theorem 2 uses Equation (12) to characterize the NE strategy of D under behavioral irrationalities. We next prove that D's NE strategy exists by showing that (12) has a solution in [0,1] (note that P_D, i.e., the variable characterizing D's strategy in (12), is a probability).

LEMMA 2. *The equilibrium strategy of D that was characterized in Theorem 2 exists.*

Proof. Let us denote the L.H.S of (12) as

$$f(P_D) = w\left(\binom{N_{DR}}{1}\frac{1}{N_{DR}}\frac{P_C P_D}{N_{DR}}\right) - w\left(\frac{1-P_D}{N_{\overline{DR}}}\right) - \frac{C}{B^A} \quad (17)$$

It can be shown that $df(P_D)/dP_D \geq 0$, which implies that $f(P_D)$ is a monotonically increasing function of P_D. Further, it can be shown that $\lim_{P_D \to 0} f(P_D) < 0$ and $\lim_{P_D \to 1} f(P_D) > 0$. Thus, we can conclude that there exists a value of $P_D \in [0, 1]$ at which $f(P_D) = 0$. This proves the lemma. □

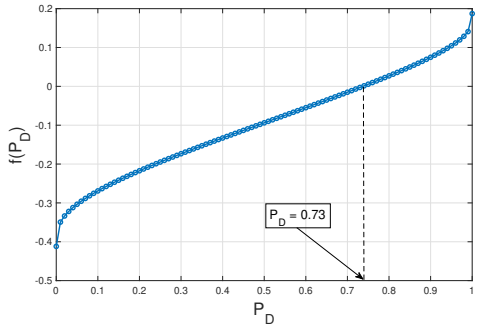


Fig. 4. Nature of the function $f(P_D)$ (17). In the figure, $f(P_D) = 0$ at $P_D = 0.73$.

In Fig. 4, we show the nature of the function $f(P_D)$ (17) with varying P_D. In the figure, we consider P_C = 0.8, B^A = 10, α = 0.6, C = 2, N_{DR} = 2, and $N_{\overline{DR}}$ = 8. The figure illustrates the monotonically increasing nature of $f(P_D)$ and that there exists a P_D such that $f(P_D) = 0$. This corroborates Lemma 2.

IV. SIMULATION RESULTS

In this section, we provide simulation results to gain important insights into our proposed deception technique and the characterized equilibrium strategies.

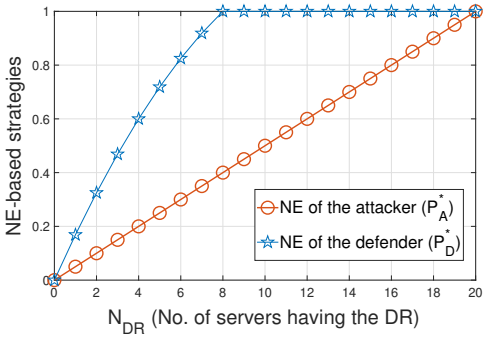


Fig. 5. NE-based strategies versus the number of servers (N_{DR}) having the DR.

Fig. 5 plots NE-based strategies of D and A versus N_{DR}, i.e., the number of servers that has the DR installed, considering D and A to be strategic and rational in nature. In the figure, we consider B^A = 40, C = 5, P_C = 0.5, and N = 20. The equilibrium strategies were computed using Theorem 1. As can be seen from the figure, with increasing N_{DR}, D monotonically increases the probability of running the task

on a server that has the DR installed to take advantage of the capabilities of the DR while aiming to deceive A into attacking a server being unused by D. Accordingly, A, with increasing N_{DR}, also increases the probability of attacking a server that has the DR installed as a best response to D's strategy.

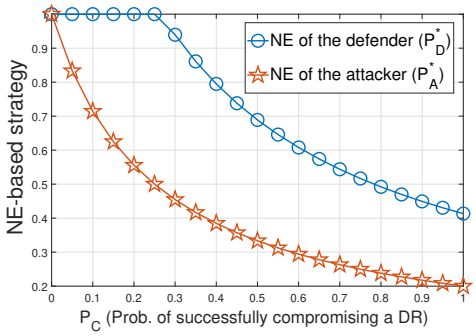


Fig. 6. NE-based strategies versus probability of successfully compromising a DR (P_C).

Fig. 6 plots NE-based strategies of D and A versus P_C, i.e., the probability of A successfully compromising a DR, considering D and A to be strategic and rational in nature. In the figure, we consider B^A = 30, C = 2, N = 20, and N_{DR} = 4. The equilibrium strategies were computed using Theorem 1. As can be seen from the figure, and as is intuitive, the probability with which D runs the task on a server that has the DR monotonically decreases with P_C (since the quality of the DR degrades with increasing P_C). Accordingly, with increasing P_C, A decreases its probability of attacking a server that has the DR installed as a best response to D's strategy. It can also be noted that, after P_C exceeds a certain threshold (corresponding to $P_C = 0.25$ in the figure), the nature of decrease of P_D^* makes D to rely more on the employment of deception-based strategies to run the computational task securely (rather than always relying on the capabilities of the DR), which emphasizes how our proposed deception strategy can complement capabilities of conventional defense resources.

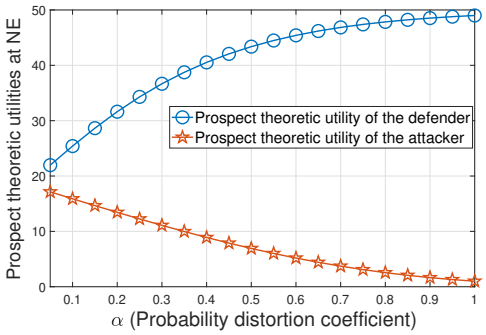


Fig. 7. Prospect theoretic utility of the defender and attacker versus α

Fig. 7 plots prospect theoretic utilities of D and A at NE versus α, i.e., the probability distortion coefficient (which models the degree of irrationality of a human in the Prelec function (11)). In the figure, we consider B^A = 50, C = 50, B^D = 50, P_C = 0.5, N_{DR} = 5, and $N_{\overline{DR}}$ = 15. The NE strategies of D and A were calculated using Theorem 2. The figure shows that increase of α (i.e., increase of the degree of rationality) positively impacts D's prospect theoretic utility at NE while negatively impacting that of A, implying that a higher degree of rationality enables D to better employ the proposed deception tactics in a strategic context.

V. Conclusion

This paper presented a novel technique that can enable a defender to run a computational task securely by using 'fake' unused servers to deceive an attacker. Under use of our proposed deception technique, the paper characterized NE-based attack-defense strategies considering the defender and the attacker to be fully rational in nature as well as considering them to exhibit behavioral irrationalities due their cognitive biases. Our developed model accounts for cost factors associated with attack-defense strategies and our results have provided understanding of how cyber deception strategies can complement capabilities of conventional defense resources. Numerous simulations results were presented in the paper that provided important insights into our developed cyber deception strategies.

References

[1] S. Nan, S. Brahma, C. A. Kamhoua, and L. L. Njilla, "On development of a game-theoretic model for deception-based security," *Modeling and Design of Secure Internet of Things*, pp. 123–140, 2020.

[2] A. Schlenker, O. Thakoor, H. Xu, M. Tambe, P. Vayanos, F. Fang, L. Tran-Thanh, and Y. Vorobeychik, "Deceiving cyber adversaries: A game theoretic approach," in *International Conference on Autonomous Agents and Multiagent Systems*, 2018.

[3] A. L. Davis, "Deception in game theory: A survey and multiobjective model," Air Force Institute Of Technology Wright-Patterson AFB OH Wright-Patterson, Tech. Rep., 2016.

[4] T. E. Carroll and D. Grosu, "A game theoretic investigation of deception in network security," *Security and Communication Networks*, vol. 4, no. 10, pp. 1162–1172, 2011.

[5] R. M. Campbell, K. Padayachee, and T. Masombuka, "A survey of honeypot research: Trends and opportunities," in *2015 10th international conference for internet technology and secured transactions (ICITST)*. IEEE, 2015, pp. 208–212.

[6] C. Wang and Z. Lu, "Cyber deception: Overview and the road ahead," *IEEE Security & Privacy*, vol. 16, no. 2, pp. 80–85, 2018.

[7] M. Zhu, A. H. Anwar, Z. Wan, J.-H. Cho, C. A. Kamhoua, and M. P. Singh, "A survey of defensive deception: Approaches using game theory and machine learning," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2460–2493, 2021.

[8] D. Fudenberg and J. Tirole, *Game Theory*. Cambridge, MA: MIT Press, 1991.

[9] S. Nan, S. Brahma, C. A. Kamhoua, and N. O. Leslie, "Behavioral cyber deception: A game and prospect theoretic approach," in *IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2019, pp. 1–6.

[10] V. S. S. Nadendla, S. Brahma, and P. K. Varshney, "Towards the design of prospect-theory based human decision rules for hypothesis testing," in *2016 54th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. IEEE, 2016, pp. 766–773.

[11] B. Geng, X. Cheng, S. Brahma, D. Kellen, and P. K. Varshney, "Collaborative human decision making with heterogeneous agents," *IEEE Transactions on Computational Social Systems*, vol. 9, no. 2, pp. 469–479, 2022.

[12] D. Kahneman and A. Tversky, "Prospect theory: An analysis of decision under risk," in *Handbook of the fundamentals of financial decision making: Part I*. World Scientific, 2013, pp. 99–127.

[13] L. Zhu, S. Majumdar, and C. Ekenna, "An invisible warfare with the internet of battlefield things: a literature review," *Human behavior and emerging technologies*, vol. 3, no. 2, pp. 255–260, 2021.

[14] D. Prelec, "The probability weighting function," *Econometrica*, pp. 497–527, 1998.