Understanding adversarial decisions for different probing-action costs in a deception game via cognitive modeling

Harsh Katakwar (katakwarharsh@gmail.com)
Applied Cognitive Science Laboratory, Indian Institute of Technology Mandi
Mandi, India

Palvi Aggarwal (paggarwal@utep.edu)
Department of Computer Science, The University of Texas at El Paso
El Paso, TX, USA

Varun Dutt (varun@iitmandi.ac.in)
Applied Cognitive Science Laboratory, Indian Institute of Technology Mandi
Mandi, India

Abstract

In the cyber world, deception through honeypots has been prominent in response to modern cyberattacks. Prior cybersecurity research has investigated the effect of probing action costs on adversarial decisions in a deception game. However, little is known about the cognitive mechanisms that affect the influence of probing action costs on adversarial decisions. The main objective of this research is to see how an instance-based learning (IBL) model incorporating recency, frequency, and cognitive noise could predict adversarial decisions with different probing action costs. The experimental study had three different probing action costs in the deception game: increasing cost probe (N = 40), no-cost probe (N = 40), and constant cost probe (N = 40). Across the three conditions, the cost for probing the honeypot webserver was varied; however, the cost for probing the regular webserver was kept the same. The results revealed that the cost of probing had no effect on probe and attack actions and that there was a significant interaction between different cost conditions and regular webserver probe actions over the trials. The human decisions obtained in the above experiment were used to calibrate an IBL model. As a baseline, an IBL model with ACT-R default parameters was built. In comparison to the IBL model with ACT-R default parameters, the results showed that the IBL model with calibrated parameters explained adversary decisions more precisely. Results from the model showed higher cognitive noise for cost-associated conditions compared to that of no-cost condition. We highlight the main implications of this research for the community.

Keywords: deception, adversary, honeypots, attacker, Instance-based Learning Theory (IBLT), cognitive modeling, probing cost.

Introduction

Cyberattacks are deliberate attempts by the adversary to intrude into computer systems. Among the various cyberattacks, ransomware attacks increased by 105% in 2021 (Taylor, 2022). Furthermore, attackers have employed phishing as the most common method of luring the public by making lucrative false promises (Taylor, 2022). This rapid increase in attacks drives the scientific community to find adaptable solutions for building secure cyberspace.

Some security solutions, including intrusion detection systems (IDSs), filtering strategies, firewalls, etc. are available to assist in deterring cyberattacks (Aggarwal & Dutt, 2020; Aggarwal et al., 2022; Rowe & Custy, 2007; Scarfone & Mell, 2007; Shang, 2018). When an IDS detects any unusual behaviour, it shoots off a warning (Aggarwal & Dutt, 2020; Scarfone & Mell, 2007). IDSs are robust; however, they can also incur financial losses by generating false warnings (Shang, 2018). Filtering solutions assist in the removal of undesired content while maintaining secure access. This method could lead to bounded non-rational network agents coming to a consensus (Shang, 2018). In general, such an agreement could aid in the detection of intrusions before they become a cybersecurity risk (Shang, 2018). Overall, these available solutions may not be able to assist in combating emerging cyberattacks.

Cyber deception has been a successful method of thwarting cyber-attacks (Rowe & Custy, 2007). In fact, it has been able to reduce the overall cost of data breaches by 30% (BusinessWire, 2021). The main aim of cyber deception is to take human aspects into account in cyber situations while also improving security tools to reduce cyber-attacks (Rowe & Custy, 2007). Cyber deception has been employed via honeypots, which pretend to be real webservers (Almeshekah & Spafford, 2016). This method has been found to be beneficial in monitoring and mitigating cyberattacks. Deception in cybersecurity has been explored using mathematical and canonical games (Carroll & Grosu, 2009; Garg & Grosu, 2007; Kiekintveld et al., 2015). Kiekintveld et al. (2015) examined how a game-theoretical technique could be applied to manipulate information in adversarial environments. Similarly, Garg and Grosu (2007) proposed a mathematical framework for a security game involving deception. Carroll and Grosu (2009) described the interaction between an adversary and a defender as a signalling game.

Recent behavioral cybersecurity research has focused more on technological aspects that influence adversarial decisions in cybersecurity. Some of them include network topology, timing and amount of deception, network size, honeypot proportions, probing action costs, the complexity of cyber-attacks, etc. (Aggarwal et al., 2017; Katakwar et al., 2020). Aggarwal et al. (2017) evaluated the impact of timing and amount of deception on adversarial decisions and revealed that late deception increased the proportion of honeypot attacks when compared to early deception. Similarly, Katakwar et al. (2020) investigated the effect of various network sizes on adversarial decisions in cyberspace. In addition, these researchers have also built computational cognitive models that helped them understand the various cognitive elements that play a vital role in influencing adversarial decisions in cyber scenarios (Katakwar et al., in press).

Recently, Katakwar et al. (2022) have evaluated the effect of probing action costs on adversarial decisions in a deception-based security game experimentally. They found that cost of probing had no effect on probe and attack actions and that there was a significant interaction between different cost conditions and regular webserver probe actions over the trials. However, they did not look into different cognitive parameters that drive the adversarial decisions in complex cyber circumstances. Building cognitive models based on Instance-based Learning Theory (IBLT) is one approach to comprehending cognitive factors in dynamic situations (Dutt & Gonzalez, 2012; Gonzalez et al., 2003; Gonzalez & Dutt, 2011). Previously, IBLT-based cognitive models were able to explain how adversaries made decisions in different cyber scenarios (Aggarwal et al., 2017; Dutt et al., 2013). Hence, in this research, we address the research gap by building cognitive models based on IBLT that could account for adversarial decisions in cyber situations with different probing costs.

In what follows, we first briefly discuss the working of the Deception Game (DG). Next, we describe the findings of Katakwar et al. (2022). Thereafter, we detail the background of IBLT, and thereafter we present the results and conclusions of the developed cognitive models.

Deception Game

DG is a sequential, single-player, incomplete information game in which an adversary and a network compete against each other (Aggarwal et al., 2016a, 2016b; Garg & Grosu, 2007). The game is formally defined as DG (n, k, γ), where *n* denotes the total number of webservers, *k* denotes the number of honeypots, and *γ* denotes the number of probes after which the adversary makes his final decision to attack the network. The DG has two types of webservers: regular and honeypot. Regular webservers are the real webservers that contain valuable information, whereas honeypots are fake servers that pretend to be real in order to trap opponents and extract meaningful information.

The game is played over multiple rounds. There are two phases in each round of the game: probe stage and attack stage. An adversary could probe webservers several times during the probe stage. Probing implies clicking on the button in the game's UI that represents a webserver. For each probe, the adversary receives a response from the system indicating whether the system is a regular (real) webserver or a honeypot (fake) webserver. Depending on whether or not the deception is present, this feedback may or may not be correct. As a result, the adversary may not be able to learn across multiple rounds in this scenario. Furthermore, the game dynamics may closely resemble those in the real world, in which adversaries may have limited knowledge of the infrastructure they are attempting to attack. Overall, the goal of deception is to deceive the opponent into believing misleading information about the state of the servers. If deception is present in a round, the network response is the total opposite of the webservers' actual state. If there is no deception in a round, the network's response will be identical to the true state of webservers. The adversary also has the option of not probing any webservers during the probe stage. Deception and unreliability in the feedback of the probe stage may increase not-attack activities, as the adversary will likely avoid regular/honeypot attack actions due to the probe stage's response.

We had three different variants of DG in this experiment: increasing-cost, no-cost, and constant-cost. In the increasing-cost condition, the cost of probing the honeypot webserver grew linearly as the round progressed. If the adversary probed the honeypot webserver for the i^{th} time in a given round, the adversary received -5**i* points. In the no-cost condition, there were no penalties for probing the honeypot webservers across all rounds of the DG. In the constant-cost condition, the cost of probing the honeypot webservers was kept constant over the rounds. As a result, the attacker received -5 points for each probe of the honeypot webserver. Across all the conditions, there were constant cost to probe the regular webserver in DG.

Experiment

Experiment Design

Katakwar et al. (2022) randomly allocated participants to one of three between-subjects conditions: no-cost probe (40 participants), constant-cost probe (40 participants), and increasing-cost probe (40 participants). There were four webservers in the network under all conditions, two of which were regular webservers and the other two were honeypots. In addition, there were 29 trials, 14 of which were non-deception rounds, and the rest were deception rounds. The participants were informed about the presence of deception in a DG, but they did not know which round belonged to the deception/non-deception condition. Also, the deception and non-deception rounds in DG did not form a particular sequence or pattern that participants could predict. Across the conditions, the adversary probes multiple times before moving to the attack stage, where he/she makes the decision to attack one of these webservers present in the network. For all the conditions, there were six dependent variables, three for the probe decisions and three for the attack decisions. In addition, we grouped the 29 trials into blocks of 5 trials each to see the effect of varied cost conditions on probe and attack decisions over the trials. As a result, the 29 trials were divided into 6 blocks, with the first block including 5 trials and the last block containing 4 trials. After that, for each block, the proportions of regular webserver probe/attack, honeypot webserver probe/attack, and no webserver probe/attack were determined.

Participants

Katakwar et al. (2022) recruited 120 participants anonymously recruited from the crowd-sourcing platform called Amazon Mechanical Turk (Mason & Suri, 2012). Sixty-six percent of participants were male, whereas the remaining thirty-four percent were female. More than ninety-four percent of the participants had a college degree. Seventy-four percent of the participants were from the fields of Science, Technology, Engineering, and Management (STEM) background. Once the study was over, participants were thanked and compensated INR 50 (USD 0.72) for their participation in the study. In addition, the top-three scorers were randomly chosen for the lucky draw contest, with one of them winning a gift card.

Procedure

Participants in the study were provided information about their roles and goals in the DG. Participants were also given information about their tasks and the associated payoffs. Over the course of numerous rounds of DG, participants were asked to maximize their payoff. The presence of deception and non-deception rounds in DG was communicated to participants by text instructions, but they were unaware of which rounds involved deception or non-deception. In addition, the configuration of regular and honeypot webservers was randomized in each round so that the percentage of regular and honeypot webservers remained consistent with the conditions. There were two phases to each round of DG: probe and attack. During the probe phase, the adversary may or may not probe a few webservers present in the network. Similarly, during the attack phase, the adversary had the option of attacking one of the webservers or none of them. Participants were thanked and compensated for their participation once the study was completed.

Results

Influence of different probe costs on adversarial decisions during probe and attack stages

Katakwar et al. (2022) investigated the impact of the different probing action costs on adversarial decisions during the probe stage. They found that proportion of different probe decisions were insignificant across different cost conditions. The proportion of regular webserver probe decisions in the increasing-cost condition, no-cost condition, and constant-cost condition were 0.44, 0.47, and 0.45, respectively (*F* (2, 117) = 0.919, *p* = .402, η^2 = 0.015). Similarly, the proportion of honeypot webserver probe decisions in increasing-cost condition, no-cost condition, and constant-cost condition were 0.43, 0.47, and 0.43, respectively (*F* (2, 117) = 1.454, *p* = .238, η^2 = 0.020). The proportion of no webserver probe decisions in increasing-cost condition, no-cost condition, and constant-cost condition were 0.13, 0.06, and 0.12, respectively (*F* (2, 117) = 1.359, *p* = .261, η^2 = 0.024).

Similarly, they also investigated the effect of the different probing action costs on adversarial decisions during the attack stage. The proportion of different attack decisions were insignificant across different cost conditions. The proportion of regular webserver attack decisions in increasing-cost condition, no-cost condition, and constant-cost condition were 0.42, 0.45, and 0.42, respectively (*F* (2, 117) = 0.606, *p* = .547, η^2 = 0.010). The proportion of honeypot webserver attack decisions in increasing-cost condition, no-cost condition, and constant-cost condition were 0.40, 0.44, and 0.43, respectively (*F* (2, 117) = 1.454, *p* = .238, η^2 = 0.024). The proportion of no webserver attack decisions in increasing-cost condition, no-cost condition, and constant-cost condition were 0.18, 0.11, and 0.14, respectively (*F* (2, 117) = 1.359, *p* = .261, η^2 = 0.023).

Influence of different cost conditions over the trials on adversarial decisions during probe stage

Katakwar et al. (2022) investigated the effect of probe decisions over the trials as a within-subject factor and different probing cost conditions as a between-subject factor. Figure 1 shows the proportion of regular probes over blocks of trials in different cost conditions. As shown in Figure 1, they also found that there was a significant interaction between different cost conditions and blocks (*F* (10, 585) = 2.052, *p* < .05, η^2 = 0.034). Also, averaged over all conditions, the proportions of regular probe decisions over the blocks were significant and decreasing (*F* (5, 585) = 2.529, *p* < .05, η^2 = 0.021).

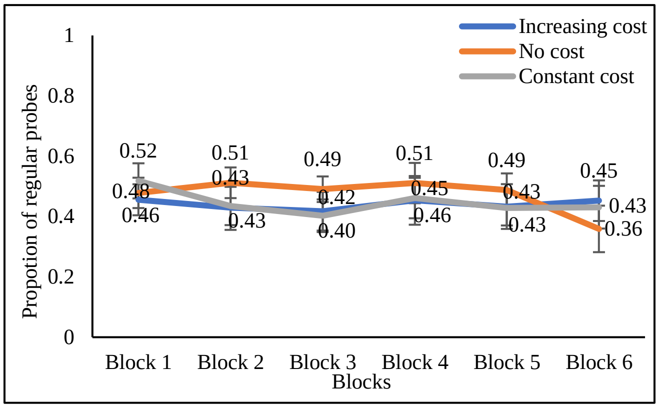


Figure 1. Proportion of regular webserver probes over the blocks of trials across different cost conditions.

However, the proportion of honeypot webserver probes were not significant over blocks (*F* (5, 585) = 1.662, *p* = .142, η^2 = 0.014). Also, the interaction between honeypot webserver probes and different cost conditions was not significant (*F* (10, 585) = 1.667, *p* = .085, η^2 = 0.028). Similarly, the proportion of no webserver probe decisions were not significant over blocks (*F* (5, 585) = 1.348, *p* = .243, η^2 = 0.011). Also, the interaction between different cost conditions and the no webserver probe decisions were found to be insignificant (*F* (10, 585) = 1.171, *p* = .307, η^2 = 0.020).

Influence of different cost conditions over the trials on adversarial decisions during attack stage

Katakwar et al. (2022) investigated the effect of different cost conditions over the trials on adversarial decisions in the attack stage. They found that there was not any significant interaction between different cost conditions and the following proportions of attack decisions over blocks: regular webserver attack (F (10, 585) = 0.579, p = .832, η^2 = 0.010), honeypot webserver attack (F (10, 585) = 0.664, p = .758, η^2 = 0.011) and no webserver attack (F (10, 585) = 1.422, p = .166, η^2 = 0.024). Also, the proportion of decisions over blocks was not significant for these decisions: regular webserver attack (F (5, 585) = 0.111, p = .990, η^2 = 0.001), honeypot webserver attack (F (5, 585) = 0.936, p = .457, η^2 = 0.008), and no webserver attack (F (5, 585) = 1.854, p = .100, η^2 = 0.016).

IBL Model

IBLT is a decision-making theory for complicated circumstances based on experience (Dutt & Gonzalez, 2012; Gonzalez et al., 2003; Gonzalez & Dutt, 2011). Prior research in computational modeling using cognitive theories such as IBLT has shown to be effective in forecasting human behaviour in complex situations. The instances are built in the memory for each occurrence of an outcome on choice options in an IBL model. In the model, an instance has the triplet frame situation-decision-utility. The circumstance in the instance represents the current situation, the decision represents the decision made in the current situation (option of one of the alternatives), and utility represents the outcome achieved from the decision made in the current situation. When a decision must be made, the instances of each alternative are retrieved from memory. These occurrences are then blended together for each choice. The activation of occurrences, as well as their likelihood of being recalled from memory, are used thereafter for calculating the blended value of an option.

$$V_{j,t} = \sum_{i=1}^{n} p_{i,j,t}\, x_{i,j,t}$$

where $p_{i,j,t}$ is the likelihood of recalling an instance i for an option j in the t^{th} trial of the experiment, and $x_{i,j,t}$ is the utility value of an instance i for an option j in the trial t. In each trial, the model chooses the option with the highest blended value. The blended value for each option is generated using the above equation, which is the summation of all observed outcomes weighted by the retrieval probability. The retrieval probability of the instances is described as follows:

$$p_{i,j} = \frac{e^{\frac{A_{i,j,t}}{\tau}}}{\sum_{i=1}^{n} e^{\frac{A_{i,j,t}}{\tau}}}$$

where $A_{i,j,t}$ is the activation value of an instance i corresponding to the memory choice j; τ is the random noise parameter, which is specified as $\tau = \sigma * 2$; and σ is the free cognitive noise parameter to represent the uncertainty of recalling prior experiences from the memory. In a given trial, the activation value of an instance is determined by the frequency with which its outcome happens and the time difference between the current time and the previous time when the instance's outcome occurred in the task. The activation value of a given instance i is defined for each trial t as follows:

$$A_i = \ln\Big(\sum_{t_{p,i} \in \{1,\ldots,t-1\}} (t - t_{p,i})^{-d} \Big) + \sigma * \ln\Big(\frac{1-\gamma_{i,t}}{\gamma_{i,t}}\Big)$$

where, d and σ are the hyperparameters known as memory decay and cognitive noise respectively; t is the current trial; $t_{p,i}$ are the prior trials in which outcome with instance i occurred in the task; and $\gamma_{i,t}$ is the random number chosen from the uniform distribution between 0 and 1. So, the frequency of occurrence of outcomes in the task and the recency of those outcome observations increase the activation of an instance corresponding to the observed outcome. The decay parameter d takes into consideration reliance on current information. The greater the reliance on recency and the faster memory decay, the higher the value of the d parameter. The σ parameter compensates for variation in instance activation from sample to sample. The greater the value, the higher variability in instance activations and trial-to-trial decisions.

Parameter Calibration

We built two different variants of the IBL model. The first variant of the IBL model had calibrated parameters of d and σ, which was referred to as IBL-calibrated model. However, the second variant of the model had default ACT-R parameters of d and σ as 0.50 and 0.25 respectively, referred as IBL-ACT-R model. Using experimental data of different cost conditions, we found the optimal values of d and σ for IBL-calibrated model. For both the variants of IBL-based model, 120 model agents were used across different trials. Across the 29 trials, we tried to minimize the average of Mean Squared Deviations (MSD) on the proportion of attack and not-attack decisions made by humans and models.

$$MSD = \frac{1}{29}\sum_{t=1}^{29}(model_t - human_t)$$

where, t depicts trial from 1 to 29; $model_t$ and $human_t$ refers to the attack decisions in the trial t from model and human participants, respectively. So, if the MSD value is minimal, the model's fit to human data is better. To maximize the values of d and σ parameters for both model participants, the Genetic Algorithm (GA), an optimization algorithm, was utilized. In the genetic algorithm, the utility value for the regular webserver, honeypot webserver, and no probe/attack varied from -100 to 100, whereas the d and σ parameters varied from 0 to 10.

The IBL-ACT-R model is based upon ACT-R framework, a cognitive theory that has been used to explain a variety of cognitive science findings (Anderson et al., 1997). ACT-R is a cognitive architecture designed to account for the various complex operations of the human mind. In the IBL-ACT-R model, we have d and σ parameters, which were set based on the ACT-R default values of 0.50 and 0.25, respectively. Smaller values of d suggest that information is less reliant on frequency and recency, and smaller values of σ indicate that trial-to-trial decisions are less variable. We compared the performance of IBL-ACT-R and IBL-calibrated models.

Model Results

Table 1 shows the values of model parameters and MSD between human and model for different conditions of both models. The d and σ are the free parameters of the models where d parameter denotes the memory decay and σ denotes the variability in trial-to-trial decisions. In the IBL-calibrated model, d value was smaller for cost-associated conditions i.e., constant cost (d = 1.21) and increasing cost (d = 1.56) and higher for no-cost condition (d = 8.50). Similarly, σ value was higher for the cost-associated conditions i.e., constant cost (σ = 8.89) and increasing cost (σ = 7.67), and lower for no cost (σ = 0.56). The MSD value for the attack and not attack actions of the IBL-ACT-R model across all the conditions were higher compared to the total MSD value of the calibrated model. Figure 2 shows the proportion of different attack and not attack decisions over the blocks of trials in increasing cost conditions in human data, IBL-calibrated model, and IBL-ACT-R model. Figure 3 shows the proportion of different attack and not attack decisions over the blocks of trials in constant cost condition in human data, IBL-calibrated model, and IBL-ACT-R model. Figure 4 shows the proportion of different attack and not attack decisions over the trials in no cost condition in human data, IBL-calibrated model, and IBL-ACT-R model.

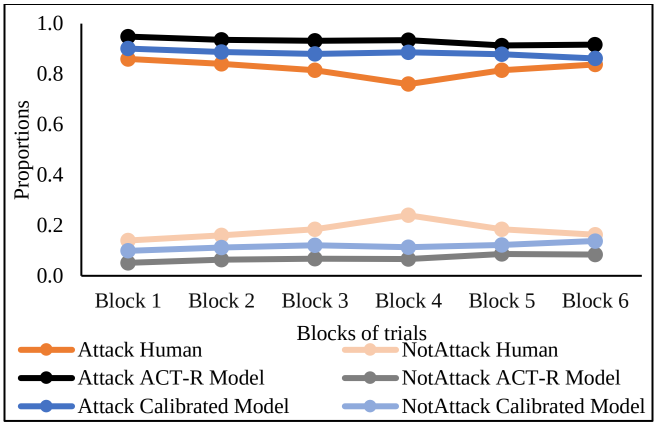


Figure 2. Proportion of different attack and not attack decisions over the blocks of trials in increasing cost conditions in human, IBL-calibrated model, and IBL-ACT-R model.

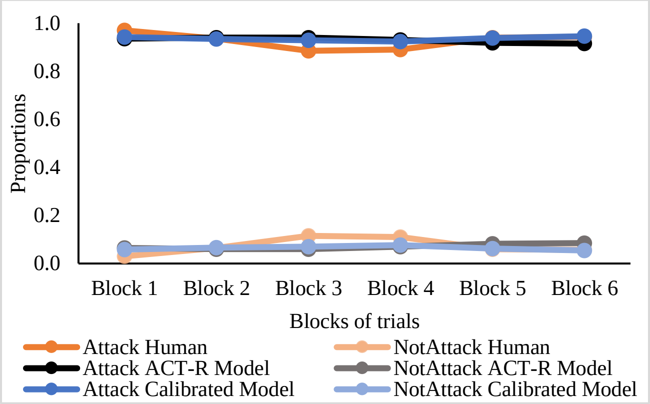
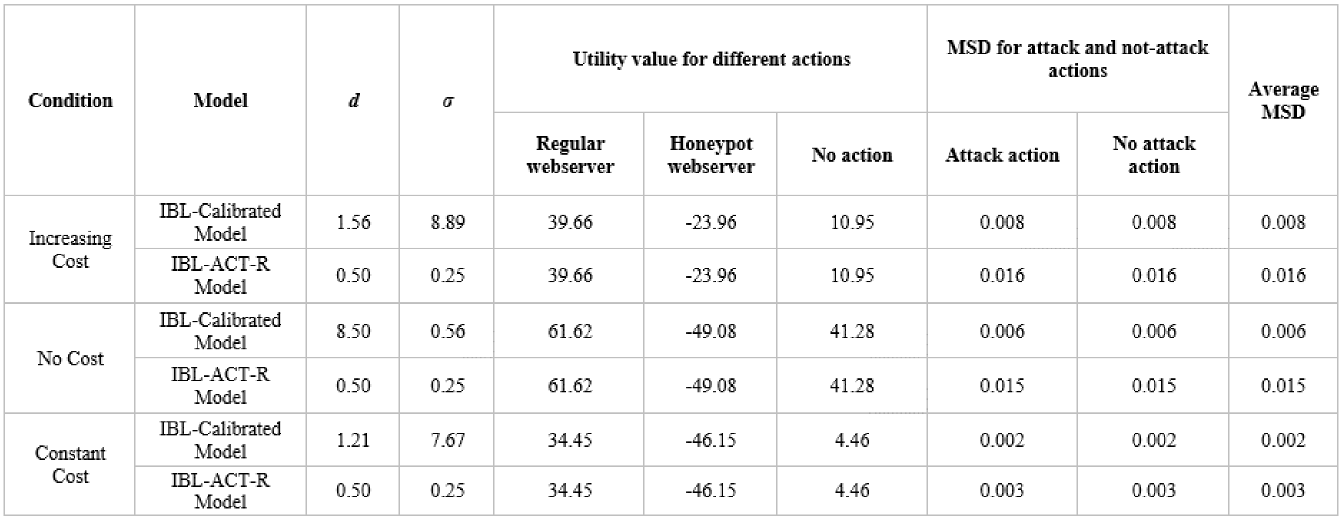


Figure 3. Proportion of different attack and not attack decisions over the blocks of trials in constant cost condition in human data, IBL-calibrated model, and IBL-ACT-R model.

Table 1. Model parameters, MSD across different conditions for the IBL-calibrated model and the IBL-ACT-R model, and utility value of the pre-populated instances of regular webserver, honeypot webserver, and no actions



Condition	Model	*d*	*σ*	Utility value for different actions			MSD for attack and not-attack actions		Average MSD
				Regular webserver	Honeypot webserver	No action	Attack action	No attack action	
Increasing Cost	IBL-Calibrated Model	1.56	8.89	39.66	-23.96	10.95	0.008	0.008	0.008
	IBL-ACT-R Model	0.50	0.25	39.66	-23.96	10.95	0.016	0.016	0.016
No Cost	IBL-Calibrated Model	8.50	0.56	61.62	-49.08	41.28	0.006	0.006	0.006
	IBL-ACT-R Model	0.50	0.25	61.62	-49.08	41.28	0.015	0.015	0.015
Constant Cost	IBL-Calibrated Model	1.21	7.67	34.45	-46.15	4.46	0.002	0.002	0.002
	IBL-ACT-R Model	0.50	0.25	34.45	-46.15	4.46	0.003	0.003	0.003

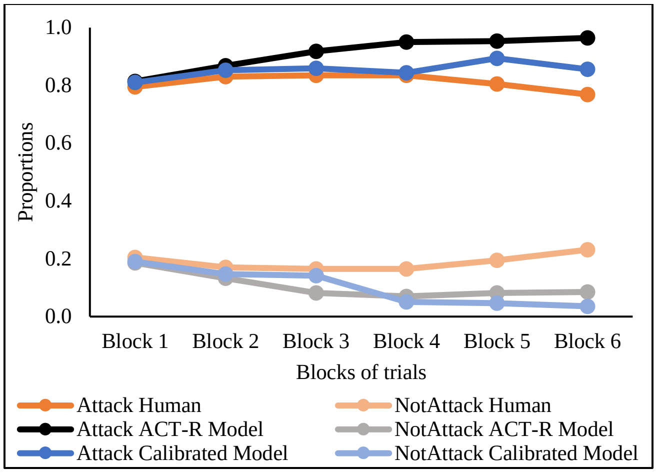


Figure 4. Proportion of different attack and not attack decisions over the trials in no cost condition in human data, IBL-calibrated model, and IBL-ACT-R model.

Discussion

Deception using honeypot has been demonstrated to be an important approach for combating modern cyber-attacks (Almeshekah & Spafford, 2016). Researchers in the field of adversarial cybersecurity have created and deployed canonical games to investigate the effectiveness of deception in various cybersecurity scenarios (Aggarwal et al., 2016a; 2016b). In addition, researchers have examined the many human factors that influence the adversary's decision in deception-based security games (Aggarwal et al., 2016a; Katakwar et al., 2020). Recently, Katakwar et al. (2022) has evaluated the effects of probing action costs in a deception-based game. However, they did not try to understand different cognitive factors involved in adversarial decisions in this cyber situation.

The findings of Katakwar et al. (2022) revealed that the varying costs of probing actions had no effect on adversarial decisions made during the attack phase in DG. However, there was a significant effect of regular probe decisions over the blocks of trials in DG. The results also indicated that both constant-cost and increasing-cost conditions, the proportion of regular probing decisions followed a consistent pattern over rounds. Furthermore, the proportion of regular probe decisions decreased across the blocks of trials. According to IBL theory, humans choose the alternatives that maximize their overall values. When there is a cost connected for probing honeypot webserver, the adversary suffers negative consequences. This negative experience reduces the combined value of the honeypot probe/attack decision. In contrast, the attacker suffers no negative consequences when probing/attacking a webserver in the no-cost probe. As a result, we see a significant effect of different cost conditions on regular probe decisions in DG over the trials. Also, there was no influence of different cost conditions on the adversarial decision-making during the attack phase. As the attack phase followed the probe phase and the cost was associated with probing. Thus, the proportion of actions during the attack phase across different cost conditions were similar.

The cognitive models' results revealed that the no-cost condition had a higher memory decay value (d = 8.50) than the cost-associated conditions. As in the no-cost condition, the adversaries had no negative experience, which made them more reliant on the DG's feedback. As a result, the memory decay value for the no cost condition is much higher than that for the cost-associated situations. Furthermore, the model revealed a high cognitive noise value for cost-associated conditions (σ = 8.89 for constant cost and σ = 7.67 for increasing cost). One explanation for this result is that increasing the cost of probing the honeypot webserver increases the adversary's negative experience. This negative experience along with the presence of deception baffled the adversary, prompting the adversary to probe fewer regular webservers.

We also found pre-populated utility values for regular webserver action, honeypot webserver action, and no webserver action for the various cost conditions via calibration. The pre-populated utility value for regular webserver action and no action for the no-cost condition was quite high in comparison to cost-associated conditions. Furthermore, the pre-populated utility value for honeypot webserver action for cost-associated conditions was negative as compared to the no-cost condition. The reasons behind both outcomes can be understood with the aid of IBLT. In the no-cost condition, the adversary does not receive any negative feedback, making instances of gains more active than instances of losses. As a result, adversaries have a positive opinion about the honeypot webserver. Furthermore, in the no-cost condition, the adversary only received positive rewards for probing/attacking webservers, resulting in a positive opinion about webservers. Thus, the utility values for regular webserver action and no webserver action in the no-cost condition were higher than in cost-associated conditions. However, in cost-associated conditions, as the adversaries have some negative experiences, this leads to a negative perception of honeypot webservers among the adversaries.

One drawback of this study is that the results are based on a lab-based study. As a result, some of the findings might not be applicable in the real-world settings. In addition, the adversaries in this investigation were unaware of deception rounds and the actual identities of webservers, which could have influenced their decisions during the probe and attack stages. One practical implication of this research in the real-world is that the cognitive models derived from this research could be used to build decision support system for organizations, which may assist inexperienced defenders and analysts to make decisions in cyber environments. Also, the models can be utilized for performing penetration testing in different cyber settings to determine exploitable vulnerabilities.

In the future, we intend to investigate how various deception and non-deception patterns might be used to deceive the enemy from the genuine target in a cyber environment. Furthermore, because of the complicated cyber environment, it is quite expected that adversaries will exhibit various cognitive biases; hence, we plan to investigate the presence of cognitive biases in cyber settings. These are some ideas that we intend to study in our future research.

References

Aggarwal, P., & Dutt, V. (2020). The role of information about opponent's actions and intrusion-detection alerts on cyber decisions in cyber security games. *Cyber Security: A Peer-Reviewed Journal*, *3*(4), 363–378.

Aggarwal, P., Gonzalez, C., & Dutt, V. (2016a). Cyber-security: Role of deception in cyber-attack detection. *Advances in Intelligent Systems and Computing*, *501*, 85–96. https://doi.org/10.1007/978-3-319-41932-9_8

Aggarwal, P., Gonzalez, C., & Dutt, V. (2016b). Looking from the hacker's perspective: Role of deceptive strategies in cyber security. *2016 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2016*. https://doi.org/10.1109/CYBERSA.2016.7503288

Aggarwal, P., Gonzalez, C., & Dutt, V. (2017). Modeling the effects of amount and timing of deception in simulated network scenarios. *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA)*,1–7, https://doi.org/10.1109/CyberSA.2017.8073405

Aggarwal, P., Moisan, F., Gonzalez, C., & Dutt, V. (2022). Learning About the Effects of Alert Uncertainty in Attack and Defend Decisions via Cognitive Modeling. *Human Factors*, 64(2), 343–358. https://doi.org/10.1177/0018720820945425

Almeshekah, M. H., & Spafford, E. H. (2016). Cyber security deception. *Cyber Deception: Building the Scientific Foundation*, 23–50. https://doi.org/10.1007/978-3-319-32699-3_2

Anderson, J. R., Matessa, M., & Lebiere, C. (1997). ACT-R: A theory of higher level cognition and its relation to visual attention. *Human-Computer Interaction*, *12*(4), 439–462. https://doi.org/10.1207/s15327051hci1204_5

Carroll, T. E., & Grosu, D. (2009). A game theoretic investigation of deception in network security. *Proceedings - International Conference on Computer Communications and Networks, ICCCN*. https://doi.org/10.1109/ICCCN.2009.5235344

BusinessWire (2021). Cyber Deception Reduces Data Breach Costs by Over 51% and SOC Inefficiencies by 32%. https://www.businesswire.com/news/home/20200914005165/en/Cyber-Deception-Reduces-Data-Breach-Costs-by-Over-51-and-SOC-Inefficiencies-by-32

Dutt, V., & Gonzalez, C. (2012). Making Instance-based Learning Theory usable and understandable: The Instance-based Learning Tool. *Computers in Human Behavior*, *28*(4), 1227–1240. https://doi.org/10.1016/j.chb.2012.02.006

Dutt, V., Ahn, Y. S., & Gonzalez, C. (2013). Cyber situation awareness: Modeling detection of cyber attacks with instance-based learning theory. *Human Factors*, *55*(3), 605–618. https://doi.org/10.1177/0018720812464045

Garg, N., & Grosu, D. (2007). Deception in honeynets: A game-theoretic analysis. *Proceedings of the 2007 IEEE Workshop on Information Assurance, IAW*, 107–113. https://doi.org/10.1109/IAW.2007.381921

Gonzalez, C., & Dutt, V. (2011). Instance-Based Learning: Integrating Sampling and Repeated Decisions From Experience. *Psychological Review*, *118*(4), 523–551. https://doi.org/10.1037/a0024558

Gonzalez, C., Lerch, J. F., & Lebiere, C. (2003). Instance-based learning in dynamic decision making. *Cognitive Science*, *27*(4), 591–635. https://doi.org/10.1016/S0364-0213(03)00031-4

Katakwar, H., Aggarwal, P., Maqbool, Z., Dutt, V. (2020). Influence of network size on adversarial decisions in a deception game involving honeypots. *Frontiers in Psychology*, *11*, 2385.

Katakwar, H., Aggarwal, P., Maqbool, Z., & Dutt, V. (2022). Influence of Probing Action Costs on Adversarial Decision-Making in a Deception Game. In S. Fong, N. Dey, & A. Joshi (Eds.), *ICT Analysis and Applications* (pp. 649–658). Springer Singapore.

Katakwar, H., Uttrani, S., Aggarwal, P., & Dutt, V. (in press). Modeling the effects of network size in a deception game involving honeypots. In A. A. Moustafa (Ed.), *Cybersecurity and Cognitive Science*. Elsevier.

Kiekintveld, C., Lisý, V., & Píbil, R. (2015). Game-theoretic foundations for the strategic use of honeypots in network security. *Advances in Information Security*, *56*, 81–101. https://doi.org/10.1007/978-3-319-14039-1_5

Mason, W., & Suri, S. (2012). Conducting behavioral research on Amazon's Mechanical Turk. *Behavior Research Methods*, *44*(1), 1–23. https://doi.org/10.3758/S13428-011-0124-6

Rowe, N. C., & Custy, E. J. (2007). Deception in cyber attacks. *Cyber Warfare and Cyber Terrorism*, 91–96. https://doi.org/10.4018/978-1-59140-991-5.CH012

Scarfone, K., & Mell, P. (2007). Guide to intrusion detection and prevention systems (idps). *NIST Special Publication*, *800*(2007), 94.

Shang, Y. (2018). Hybrid consensus for averager–copier–voter networks with non-rational agents. *Chaos, Solitons and Fractals*, *110*, 244–251.

Taylor, A. (2022). *Ransomware cyberattacks surged in 2021 according to a new report*. Fortune. https://fortune.com/2022/02/17/ransomware-attacks-surge-2021-report/