Cumulative Prospect Theoretic Study of A Cloud Storage Defense Game Against Advanced Persistent Threats

Dongjin Xu*, Liang Xiao*, Narayan B. Mandayam†, H. Vincent Poor‡
* Dept. of Communication Engineering, Xiamen University, China. Email: lxiao@xmu.edu.cn
† WINLAB, Dept. of Electrical and Computer Engineering, Rutgers University, Piscataway, NJ.
Email: narayan@winlab.rutgers.edu
‡ Dept. of Electrical Engineering, Princeton University, Princeton, NJ. Email: poor@princeton.edu

***Abstract*—Cloud storage is vulnerable to advanced persistent threats (APTs), in which an attacker launches stealthy, continuous, well-funded and targeted attacks on storage devices. In this paper, cumulative prospect theory (CPT) is applied to study the interactions between a defender of cloud storage and an APT attacker when each of them makes subjective decisions to choose the scan interval and attack interval, respectively. Both the probability weighting effect and the framing effect are applied to model the deviation of subjective decisions of end-users from the objective decisions governed by expected utility theory, under uncertain attack durations. Cumulative decision weights are used to describe the probability weighting effect and the value distortion functions are used to represent the framing effect of subjective APT attackers and defenders in the CPT-based APT defense game, rather than discrete decision weights, as in earlier prospect theoretic study of APT defense. The Nash equilibria of the CPT-based APT defense game are derived, showing that a subjective attacker becomes risk-seeking if the frame of reference for evaluating the utility is large, and becomes risk-averse if the frame of reference for evaluating the utility is small.**

***Index Terms*—Cloud storage, advanced persistent threat, game theory, cumulative prospect theory.**

I. Introduction

Cloud storage is vulnerable to advanced persistent threats (APTs), in which an attacker launches sophisticated, stealthy, continuous, and targeted attacks to steal information from a target cyber system. The defense against APT attacks is challenging and has attracted significant research attention. For example, the interaction between an APT attacker and a defender was formulated in the seminal work in [1], as a stealthy takeover game. Such game theoretic studies are mostly based on expected utility theory (EUT), in which each player is rational and chooses its strategy to maximize the expected utility. However, as human beings, APT attackers are not always rational as assumed in the traditional game theoretic models. They sometimes make subjective decisions under uncertainty that deviate from the results of EUT, exhibiting behaviors such as risk seeking, loss aversion and the nonlinear weighting of gains and losses, which are modeled by Prospect Theory [2], [3].

This work was supported in part by NSFC under Grant 61671396 and Grant 61271242, in part by the U. S. National Science Foundation under Grant CMMI-1435778, Grant ECCS-1549881, Grant CNS-1421961 and Grant ACI-1541069, and in part by CCF-Venustech Hongyan Research Initiative 2010-2016.

Therefore, prospect theory (PT) was used in [4] to model the decision-making process of subjective APT attackers and successfully explain the deviations of their decisions from the EUT-based results. However, prospect theory does not always provide stochastic dominance and is not readily extended to cases with a large number of outcomes. As a refined variant of prospect theory, cumulative prospect theory (CPT) in [5] introduces cumulative distribution functions for both gains and losses instead of simply transforming each probability as in PT. Being monotone in stochastic dominance and consistent with human preferences, cumulative prospect theory can be applied to uncertain and risky prospects with any number of outcomes while preserving most of the essential features of PT [5].

In this paper, cumulative prospect theory is applied to study cloud storage defense against APTs, and investigate the impact of end-user subjectivity on APT defense under uncertain attack durations with any number of APT defense outcomes. More specifically, CPT is used to improve the PT-based APT defense game model formulated in [4]. In this game, a subjective attacker chooses his or her time interval to launch APT attacks to compromise a storage device and a defender chooses the scan interval to recapture the compromised storage device.

The Prelec probability weighting function [6] is applied to model the probability weighting effect of the subjective decision-making of an attacker and a defender. The value distortion function [5] is used to model the framing effect of subjective decisions of end-users, which has not been considered in the previous work in [4]. For example, a subjective attacker tends to avoid risk if finding a positive frame of reference but be risk-seeking under a negative frame of reference. The Nash equilibria (NEs) of the CPT-based game are derived, showing how the framing effect of attackers impacts the APT defense performance.

The contributions of this work can be summarized as:

- A CPT-based APT defense game is formulated to model the framing effect of subjective attacker and defense decisions to improve the PT-based APT game model as presented in [4].
- The NEs of the game and the conditions under which the equilibria exist are provided to investigate the impact of both the framing effect and probability weighting effect of subjective APT attackers on the APT defense.

The remainder of the paper is organized as follows. We review related work in Section II and present the system model in Section III. We present the CPT-based APT defense game with uncertain attack durations in Section IV and provide the NE of the game in Section V. Numerical results are provided in Section VI and conclusions are offered in Section VII.

II. Related Work

Prospect theory has been applied to study wireless communications and network security. For instance, a random access game formulated in [7] applies prospect theory to study the channel access between two subjective end-users in wireless networks. The impact of user subjectivity on both the wireless random access and data pricing games was identified in [8] based on prospect theory. The PT-based pricing and resource allocation scheme proposed in [9] improves the revenue of service providers in the presence of subjective users. A PT-based anti-jamming transmission game formulated in [10] investigates the impact of the subjectivity of end-users and jammers on the throughput in cognitive radio networks.

Cumulative prospect theory has been applied to model the subjective decision-making processes of end-users in social sciences. For instance, a CPT-based routing model formulated in [11] captures the twofold risk attitudes of travelers regarding their travel time losses, i.e., risk seeking under high probability and risk averse under low probability. The CPT-based decision-making model of order allocation in [12] formulates multiple behavioral parameters in order allocation, yielding a parameter adjustment algorithm to increase the CPT-based utility. CPT was first incorporated into a reinforcement learning framework in [13] and a quantile-based scheme was proposed to estimate the CPT-based value. A CPT-based emergency response analysis in [14] determines the ranks of all the response actions according to the prospect value.

Game theory has provided insights into APT defense. For example, in the seminal work of [1], a Flipit game was proposed to formulate the stealthy and continuous attacks of APT. The game between an overt defender and a stealthy attacker investigated in [15] shows that the periodic defense strategy is the best response against a non-adaptive attacker. A cyber-physical signaling game among an APT attacker, a cloud defender and a mobile device was formulated in [16], in which the mobile device decides whether to trust the commands from the cloud against APTs. The APT defense algorithm based on dynamic programming proposed in [17] provides a nearly optimal solution against APT attacks. The two-layer APT defense game formulated in [18] studies the joint threats from an APT attacker and insiders in the cyber system. The PT-based cloud storage defense game formulated in [4] investigates the probability weighting effect of APT attackers under uncertain attack durations, yielding a Q-learning based APT defense scheme to suppress the attack motivation of APT attackers. Compared with our earlier work in [4], we incorporate the framing effect of APT attackers in the game theoretic study on APT defense, and apply CPT to extend to cases with a large number of outcomes.

TABLE I

Summary of Symbols and Notation.

Notation	Definition
$\alpha_{A/D}$	Objective weight of attacker/defender
$\rho_{A/D}$	Risk seeking coefficient of attacker/defender
$\gamma_{A/D}$	Risk aversion coefficient of attacker/defender
$\lambda_{A/D}$	Loss aversion coefficient of attacker/defender
x/y	Defense/attack time interval
z	Duration to complete an attack
G	Defense gain
C	Attack cost
L	Number of non-zero attack duration levels

III. System Model

We consider a cloud storage system consisting of a storage device that is threatened by a subjective APT attacker (A) and is protected by a storage defender (D), as shown in Fig. 1. The defender chooses the time interval to perform the k-th detection at the storage device against APT attacks, denoted by x_k. It is clear that $x_k > 0$, because the defender has to take time to scan the storage device to detect APT attacks. Upon detecting APT attacks, the defender restores the compromised storage device and provides privacy for the data stored on the device. The defender is unaware of whether the storage device is compromised unless the device is monitored.

According to the APT model as given in [17], the APT attacker can apply advanced and sophisticated methods and inject multiple types of malware to estimate the defense strategy of the target system. The attacker can also determine whether the attack successfully controls the target storage device according to the data stolen from the device, and observe the size of the stolen data to determine when the attack is detected and stopped by the defender. The attacker waits y_k time before launching the k-th APT attack against the storage device, once the defender detects attacks and restores that storage device. The duration for the attacker to complete his or her k-th attack at the storage device, denoted by z_k, is in general a positive random variable that is unknown to both players. The defender is assumed to take charge of the storage device at the beginning. Table 1 summarizes the notation used in the paper.

IV. CPT-based APT Defense Game

The interaction between an APT attacker and a storage defender over a storage device is formulated as a CPT-based APT defense game, denoted by $\mathbb{G}$. In this game, the storage defender chooses the scan interval x for the storage device, and the attacker decides his or her attack interval y against the storage device. The defense interval and the attack interval are normalized for simplicity of analysis. According to the maximum scan interval of the defender denoted by T, the attacker and defender compete to take charge of the storage device, with $0 < x \leq 1$ and $0 \leq y \leq 1$.

The gain of the defender for a longer scan interval at the storage device is denoted by G, and the attack cost against the device is denoted by C. As shown in Fig. 1, the time interval

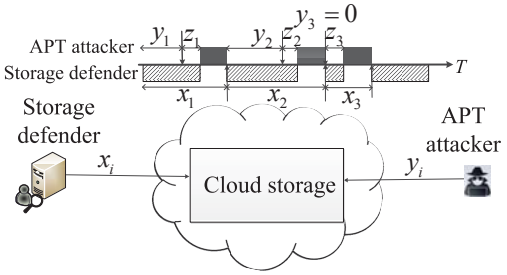


Fig. 1. Illustration of an APT game, in which the defender scans the storage device after interval x_k, the attacker launches APT after interval y_k and the attack duration is z_k, where k is the index of the interaction.

during which the storage device is not compromised and the data is safe is $\min\left((y+z)/x, 1\right)$. Therefore, the data privacy rate denoted by R is defined as the normalized "good" interval and is given by

$$R = \min\left(\frac{y+z}{x}, 1\right). \tag{1}$$

The utility of the defender depends on the data privacy rate and the gain of a longer defense interval. Similar to the game model presented in [17], the utility of the defender denoted by u_D is defined as

$$u_D(x,y) = \min\left(\frac{y+z}{x}, 1\right) + xG. \tag{2}$$

The utility of the attacker denoted by u_A is defined as

$$u_A(x,y) = -\min\left(\frac{y+z}{x}, 1\right) - \mathrm{I}(y<x)C, \tag{3}$$

where the indicator function $\mathrm{I}(\xi) = 1$ if ξ is true and 0 otherwise. The motivation for the attacker to steal information from the storage device is modeled by $-\min\left((y+z)/x, 1\right)$.

The time interval for the attacker to successfully launch an APT attack against the storage device z is difficult to estimate and is quantized into L non-zero levels following the distribution $[P_l]_{0\le l\le L}$, where $P_l = \Pr(z = l/L)$, $\forall 0 \le l \le L$. By definition, we have $P_l \ge 0$ and $\sum_{l=0}^{L} P_l = 1$. The expected utilities of the defender and the attacker over the realizations of attack duration z, denoted by U_D^{EUT} and U_A^{EUT}, respectively, are given by (2) and (3) as

$$U_D^{EUT}(x,y) = \sum_{l=0}^{L} P_l \min\left(\frac{yL+l}{xL}, 1\right) + xG \tag{4}$$

$$U_A^{EUT}(x,y) = -\sum_{l=0}^{L} P_l \min\left(\frac{yL+l}{xL}, 1\right) - \mathrm{I}(y<x)C. \tag{5}$$

Subjective players distort the values of their utilities and the probabilities of events to make decisions. Thus cumulative prospect theory is applied to capture the deviation of the decision-making processes. The value distortion functions are applied to model the framing effect of subjective decisions and the Prelec weighting function is used to represent the probability weighting effect.

Let $\gamma_D \in (0,1]$ (or $\rho_D \in (0,1]$) denote risk aversion over gains (or risk seeking over losses), and U_D^0 be the frame of reference for evaluating the utility of the defender, as a boundary that distinguishes gains from losses. The defender is more sensitive to losses than gains if the loss aversion coefficient $\lambda_D > 1$. The value distortion functions denoted by v_D^+ and v_D^-, model the subjective decision-making of the defender, in term of the frame of reference for evaluating its utility and are given by

$$\begin{cases} v_D^+(u_D) = \left(u_D - U_D^0\right)^{\gamma_D}, & u_D > U_D^0 \quad \text{(6a)} \\ v_D^-(u_D) = -\lambda_D \left(U_D^0 - u_D\right)^{\rho_D}, & \text{o.w.} \quad \text{(6b)} \end{cases}$$

The probability weighting function proposed by Prelec in [6] is applied to transform the objective probability to subjective probability. Let $\alpha_D \in (0,1]$ be the objective weight of the defender and represent its subjective level to make decisions. The objective weight of the defender decreases with the subjective evaluation distortion, and the defender is objective, if $\alpha_D = 1$ and $w_D(p) = p$. The probability weighting function of the defender, denoted by w_D, is given in [6] by

$$w_D(p) = \exp\Big(-(-\ln p)^{\alpha_D}\Big). \tag{7}$$

The utility of the defender $[u_D(x,y,l/L)]_{0\le l\le L}$ can be sorted in ascending order and labeled as $[u_D^l]_{0\le l\le L}$, where $u_D^i < U_D^0$, if $0 \le i < K$; and $U_D^0 \le u_D^i$, if $K \le i \le L$. The corresponding reordered probability is denoted by $[\tilde{p}_i]_{0\le i\le L}$. Let V_D^- denote the CPT-value of the outcomes designated as losses according to the frame of reference for evaluating the utility of the defender in the framing effect. By [5], we have

$$\begin{aligned} V_D^- =& v_D^-(u_D^0) w_D\left(\tilde{p}_0\right) + \sum_{l=1}^{K} v_D^-\left(u_D^l\right) \\ & \times \left(w_D\left(\sum_{i=0}^{l} \tilde{p}_i\right) - w_D\left(\sum_{i=0}^{l-1} \tilde{p}_i\right)\right). \end{aligned} \tag{8}$$

Similarly, the CPT-value of the outcomes designated as gains according to the frame of reference for evaluating the utility of the defender in the framing effect denoted by V_D^+ is given by

$$\begin{aligned} V_D^+ =& v_D^+\left(u_D^L\right) w_D\left(\tilde{p}_L\right) + \sum_{l=K+1}^{L-1} v_D^+\left(u_D^l\right) \\ & \times \left(w_D\left(\sum_{i=l}^{L} \tilde{p}_i\right) - w_D\left(\sum_{i=l+1}^{L} \tilde{p}_i\right)\right). \end{aligned} \tag{9}$$

Therefore, the CPT-based utility of the defender, denoted by

U_D^{CPT}, is given by

$$\begin{aligned} U_D^{CPT}(x,y) &= V_D^- + V_D^+ \\ &= v_D^-(u_D^0) w_D\left(\tilde{p}_0\right) + v_D^+\left(u_D^L\right) w_D\left(\tilde{p}_L\right) \\ &+ \sum_{l=K+1}^{L-1} v_D^+\left(u_D^l\right)\left(w_D\left(\sum_{i=l}^{L}\tilde{p}_i\right) - w_D\left(\sum_{i=l+1}^{L}\tilde{p}_i\right)\right) \\ &+ \sum_{l=1}^{K} v_D^-\left(u_D^l\right)\left(w_D\left(\sum_{i=0}^{l}\tilde{p}_i\right) - w_D\left(\sum_{i=0}^{l-1}\tilde{p}_i\right)\right). \end{aligned} \quad (10)$$

Similarly, let γ_A (or ρ_A) denote the risk aversion over gains (or risk seeking over losses), U_A^0 be the frame of reference for evaluating the utility, and λ_A be the loss aversion coefficient of the subjective APT attacker. The value distortion functions of the attacker, denoted by v_A^+ and v_A^-, represent the distorted view of the utility according to the attacker, which are given by

$$\begin{cases} v_A^+(u_A) = \left(u_A - U_A^0\right)^{\gamma_A}, & u_A > U_A^0 \quad (11a) \\ v_A^-(u_A) = -\lambda_A\left(U_A^0 - u_A\right)^{\rho_A}, & \text{o.w.} \quad (11b) \end{cases}$$

Let $\alpha_A \in (0,1]$ be the objective weight of the attacker. The probability weighting function of the attacker, denoted by w_A, is given by

$$w_A(p) = \exp\left(-(-\ln p)^{\alpha_A}\right). \quad (12)$$

The utility of the attacker $[u_A(x,y,l/L)]_{0\le l\le L}$ can be sorted in ascending order and labeled as $[u_A^l]_{0\le l\le L}$, where $u_A^i < U_A^0$, if $0 \le i < J$; and $U_A^0 \le u_A^i$, if $J \le i \le L$. The corresponding reordered probability is denoted by $[\tilde{q}_i]_{0\le i\le L}$. Similarly to the framing effect of the defender as in (8) and (9), the CPT-value of the outcomes designated as losses (or gains) according to the frame of reference for evaluating the utility of the attacker, denoted by V_A^- (or V_A^+), is given by

$$\begin{aligned} V_A^- =& v_A^-\left(u_A^0\right) w_A\left(\tilde{q}_0\right) + \sum_{l=1}^{J} v_A^-\left(u_A^l\right) \\ &\times\left(w_A\left(\sum_{i=0}^{l}\tilde{q}_i\right) - w_A\left(\sum_{i=0}^{l-1}\tilde{q}_i\right)\right), \end{aligned} \quad (13)$$

or

$$\begin{aligned} V_A^+ =& v_A^+\left(u_A^L\right) w_A\left(\tilde{q}_L\right) + \sum_{l=J+1}^{L-1} v_A^+\left(u_A^l\right) \\ &\times\left(w_A\left(\sum_{i=l}^{L}\tilde{q}_i\right) - w_A\left(\sum_{i=l+1}^{L}\tilde{q}_i\right)\right). \end{aligned} \quad (14)$$

Therefore, the CPT-based utility of the APT attacker in the game, denoted by U_A^{CPT}, is given by

$$\begin{aligned} U_A^{CPT}(x,y) &= V_A^- + V_A^+ \\ &= v_A^-\left(u_A^0\right) w_A\left(\tilde{q}_0\right) + v_A^+\left(u_A^L\right) w_A\left(\tilde{q}_L\right) \\ &+ \sum_{l=J+1}^{L-1} v_A^+\left(u_A^l\right)\left(w_A\left(\sum_{i=l}^{L}\tilde{q}_i\right) - w_A\left(\sum_{i=l+1}^{L}\tilde{q}_i\right)\right) \\ &+ \sum_{l=1}^{J} v_A^-\left(u_A^l\right)\left(w_A\left(\sum_{i=0}^{l}\tilde{q}_i\right) - w_A\left(\sum_{i=0}^{l-1}\tilde{q}_i\right)\right). \end{aligned} \quad (15)$$

V. NE OF THE CPT-BASED GAME

An NE of the CPT-based APT defense game $\mathbb{G}$, denoted by (x^*, y^*), consists of the best response of each player in terms of the CPT-based utility, if the opponent uses the NE strategy. By definition, we have

$$x^* = \arg\max_{\mathbf{x}} U_D^{CPT}(x, y^*) \quad (16)$$

$$y^* = \arg\max_{\mathbf{y}} U_A^{CPT}(x^*, y). \quad (17)$$

Theorem 1. *The CPT-based APT defense game $\mathbb{G}$ with $U_D^0 = U_A^0 = 0$ has an NE $(x^*, y^*) = (1, 1)$, if*

$$\begin{aligned} &\sum_{l=0}^{L-1}\left(\frac{l}{L} + C\right)^{\rho_A}\left(w_A\left(\sum_{i=l}^{L} P_i\right) - w_A\left(\sum_{i=l+1}^{L} P_i\right)\right) \\ &\ge 1 - (1+C)^{\rho_A} w_A\left(P_L\right). \end{aligned} \quad (18)$$

Proof: By (3), we have

$$\frac{\partial u_A}{\partial z} = \begin{cases} -\frac{1}{x}, & z \le x - y \\ 0, & z > x - y \end{cases} \le 0, \quad (19)$$

and thus we have $\tilde{q}_i = P_{L-i}, \forall 0 \le i \le L$.

If (18) holds, by (15), $\forall 0 \le y < 1$ we have

$$\begin{aligned} U_A^{CPT}(1,1) &= -\lambda^A \ge -\lambda^A (1+C)^{\rho_A} w_A\left(P_L\right) \\ &- \sum_{l=0}^{L-1}\lambda^A\left(\min\left(y + \frac{l}{L}, 1\right) + C\right)^{\rho_A}\left(w_A\left(\sum_{i=l}^{L} P_i\right)\right. \\ &\left. - w_A\left(\sum_{i=l+1}^{L} P_i\right)\right) = U_A^{CPT}(1,y). \end{aligned} \quad (20)$$

Thus, (17) holds for $(x^*, y^*) = (1, 1)$.

Similarly, we have $\partial u_D/\partial z \ge 0$, and thus $\tilde{p}_i = P_i, \forall 0 \le i \le L$. By (10), $\forall 0 < x \le 1$ we have

$$U_D^{CPT}(1,1) = (1+G)^{\gamma_D} \ge (1+xG)^{\gamma_D} = U_D^{CPT}(x,1).$$

Thus, (16) holds for $(x^*, y^*) = (1, 1)$, indicating that $(1, 1)$ is an NE of the game. ■

As shown in (18), a subjective attacker has no motivation to launch APT attacks against the cloud storage if the attack cost is high, and the defender maximizes its scan interval to save energy.

Theorem 2. *The CPT-based APT defense game* $\mathbb{G}$ *with* $U_D^0 = U_A^0 = 0$ *and* $\gamma_D = 1$*, has an NE* $(x^*, y^*) = (1, 0)$*, if*

$$\begin{cases} G + \dfrac{1}{L}\displaystyle\sum_{l=1}^{L} w_D \left(\sum_{i=l}^{L} P_i\right) \\ \geq \max\limits_{1\leq j\leq L} \dfrac{jG}{L} + \dfrac{1}{j}\displaystyle\sum_{l=1}^{j} w_D \left(\sum_{i=l}^{L} P_i\right) & \text{(21a)} \\ \displaystyle\sum_{l=0}^{L-1} \left(\frac{l}{L} + C\right)^{\rho_A} \left(w_A\left(\sum_{i=l}^{L} P_i\right) - w_A\left(\sum_{i=l+1}^{L} P_i\right)\right) \\ \leq 1 - (1+C)^{\rho_A} w_A\left(P_L\right). & \text{(21b)} \end{cases}$$

Proof: The proof is similar to that of Theorem 1. ■

As shown in (21), an attacker maximizes the attack frequency if the attack cost is low, and the defender maximizes its scan interval to save energy if the scan cost is high.

Theorem 3. *The CPT-based APT defense game* $\mathbb{G}$ *with* $U_D^0 = U_A^0 = 0$ *and* $\rho_D = 1$*, has an NE* $(x, y^*) = (k^*/L, 0), 1 \leq k^* \leq L$ *if*

$$\begin{cases} k^* = \arg\max\limits_{1\leq k\leq L} \dfrac{kG}{L} + \dfrac{1}{k}\displaystyle\sum_{l=1}^{k} w_D \left(\sum_{i=l}^{L} P_i\right) & \text{(22a)} \\ \displaystyle\sum_{l=1}^{k^*-1} \left(\frac{l}{k^*} + C\right)^{\rho_A} \left(w_A\left(\sum_{i=l}^{L} P_i\right) - w_A\left(\sum_{i=l+1}^{L} P_i\right)\right) \\ + (1+C)^{\rho_A} w_A\left(\displaystyle\sum_{i=k^*}^{L} P_i\right) \leq 1. & \text{(22b)} \end{cases}$$

Proof: The proof is similar to that of Theorem 1. ■

As shown in (22), an attacker maximizes his or her attack frequency if the attack cost is low, and the defender chooses the scan interval according to the distribution of attack duration.

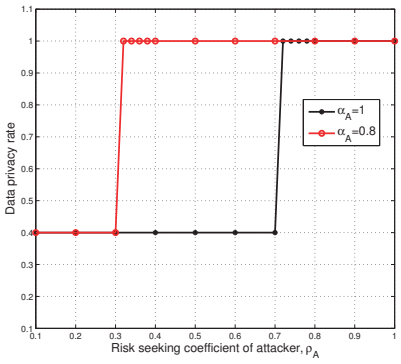
Theorem 4. *The CPT-based APT defense game* $\mathbb{G}$ *with* $U_D^0 = 0$ *and* $U_A^0 = -A \leq -1 - C$*, has an NE* $(x^*, y^*) = (1, 1)$*, if*

$$\sum_{l=1}^{L} \left(A - \frac{l}{L} - C\right)^{\gamma_A} \left(w_A\left(\sum_{i=0}^{l} P_i\right) - w_A\left(\sum_{i=0}^{l-1} P_i\right)\right) \leq (A-1)^{\gamma_A} - (A-C)^{\gamma_A} w_A\left(P_0\right). \quad \text{(23)}$$

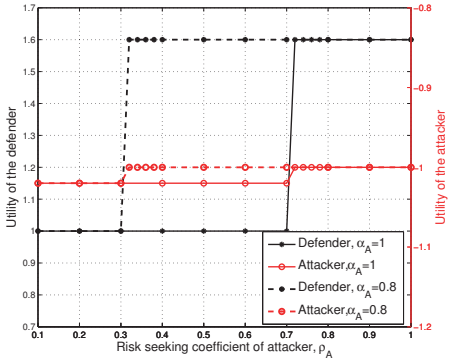
Proof: The proof is similar to that of Theorem 1. ■

As shown in (23), a subjective attacker has no motivation to launch APT attacks against the cloud storage if the attack cost is high, and the defender maximizes the scan interval to save energy.

Theorem 5. *The CPT-based APT defense game* $\mathbb{G}$ *with* $U_D^0 = 0$*,* $U_A^0 = -A \leq -1 - C$ *and* $\gamma_D = 1$*, has an NE* $(x^*, y^*) = (1, 0)$*, if*



(a) Data privacy rate



(b) Utility

Fig. 2. Performance of the CPT-based APT defense game at the NEs, with $C = 0.62$, $G = 0.6$, $P_0 = 0.4$, $P_1 = 0.4$, $\alpha_D = 1$, $U_A^0 = 0$ and $L = 2$.

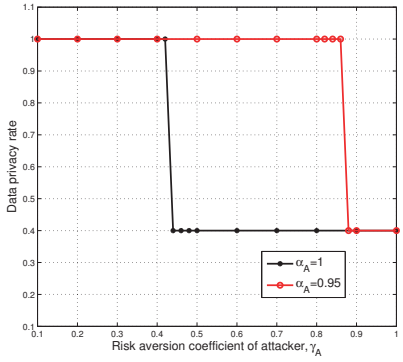
$$\begin{cases} G + \dfrac{1}{L}\displaystyle\sum_{l=1}^{L} w_D \left(\sum_{i=l}^{L} P_i\right) \\ \geq \max\limits_{1\leq j\leq L} \dfrac{jG}{L} + \dfrac{1}{j}\displaystyle\sum_{l=1}^{j} w_D \left(\sum_{i=l}^{L} P_i\right) & \text{(24a)} \\ \displaystyle\sum_{l=1}^{L} (A - \frac{l}{L} - C)^{\gamma_A} \left(w_A\left(\sum_{i=0}^{l} P_i\right) - w_A\left(\sum_{i=0}^{l-1} P_i\right)\right) \\ \leq (A-1)^{\gamma_A} - (A-C)^{\gamma_A} w_A(P_0). & \text{(24b)} \end{cases}$$

Proof: The proof is similar to that of Theorem 1. ■

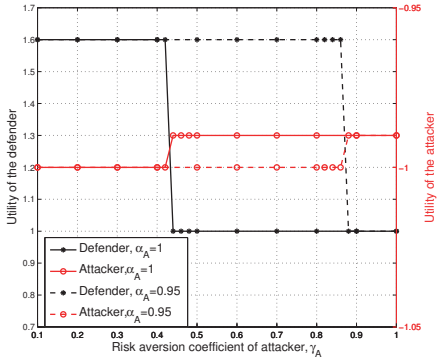
As shown in (24), an attacker launches APT frequently if the attack cost is low, and the defender maximizes the scan interval to save energy if the gain for a longer interval is high.

VI. Numerical Results

Numerical results illustrating Theorems 1 through 5 are provided to illustrate the performance of the CPT-based APT defense game, with $G = 0.6$, $P_0 = 0.4$, $P_1 = 0.4$, $\alpha_D = 1$, $\gamma_D = 1$ and $L = 2$, if not specified otherwise. As shown in Fig. 2, the data privacy rate of the cloud storage, with $C = 0.62$ and $U_A^0 = 0$, increases sharply from 0.4 to 1, as the risk seeking coefficient of the attacker ρ_A changes at around



(a) Data privacy rate



(b) Utility

Fig. 3. Performance of the CPT-based APT defense game at the NEs, with $C = 0.59$, $G = 0.6$, $P_0 = 0.4$, $P_1 = 0.4$, $\alpha_D = 1$, $U_A^0 = -3$ and $L = 2$.

0.72 with objective weight $\alpha_A = 1$, because an APT attacker with smaller ρ_A becomes risk-seeking. The turning point of the risk seeking coefficient $\rho_A = 0.72$ is given by Eq. $(21b)$ and (18). In this case, the utility of the defender increases sharply from 1 to 1.6. The data privacy rate increases to 1, as ρ_A changes at around 0.3 with $\alpha_A = 0.8$, because an attacker with a smaller α_A tends to overweigh his or her attack cost and has less attack motivation.

As shown in Fig. 3, the data privacy rate of the game, with $C = 0.59$ and $U_A^0 = -3$, decreases abruptly from 1 to 0.4, as the risk aversion coefficient of the attacker γ_A changes at 0.42 with objective weight $\alpha_A = 1$, because an APT attacker with smaller γ_A becomes risk-averse. The risk aversion coefficient of attacker $\gamma_A = 0.72$ corresponds to the turning point from Eq. (23) to $(24a)$, i.e., the utility of the defender decreases sharply from 1.6 to 1. The data privacy rate decreases to 0.4, as γ_A changes at around 0.86 with $\alpha_A = 0.95$, because a attacker with smaller α_A tends to overweigh his or her attack cost and reduce the attack frequency.

VII. Conclusion

In this work, we have formulated a CPT-based cloud storage defense game to investigate the impact of both the probability weighting effect and the framing effect of subjective attackers and cloud storage defender under uncertain APT attack durations. The NEs of the CPT-based game and the conditions under which the equilibria exist have been provided, showing that a subjective APT attacker becomes risk-seeking if his or her frame of reference for evaluating the utility is large, and becomes risk-averse if the frame of reference is small. In addition, a subjective attacker under the probability weighting effect tends to overweigh the attack cost, and thus attacks less frequently in the CPT-based defense game.

References

[1] M. van Dijk, A. Juels, A. Oprea, and R. L. Rivest, "Flipit: The game of stealthy takeover," *J. Cryptology*, vol. 26, no. 4, pp. 655–713, Oct. 2013.

[2] D. Kahneman and A. Tversky, "Prospect theory: An analysis of decision under risk," *Econometrica*, vol. 47, no. 2, pp. 263–291, Mar. 1979.

[3] L. Xiao, N. B. Mandayam, and H. V. Poor, "Prospect theoretic analysis of energy exchange among microgrids," *IEEE Trans. Smart Grid*, vol. 6, no. 1, pp. 63–72, Jan. 2015.

[4] L. Xiao, D. Xu, C. Xie, N. B. Mandayam, and H. V. Poor, "Cloud storage defense against advanced persistent threats: A prospect theoretic study," *IEEE J. Selected Areas Commun.*, in press.

[5] A. Tversky and D. Kahneman, "Advances in prospect theory: Cumulative representation of uncertainty," *J. Risk Uncertainty*, vol. 5, no. 4, pp. 297–323, Oct. 1992.

[6] D. Prelec, "The probability weighting function," *Econometrica*, vol. 66, no. 3, pp. 497–527, May 1998.

[7] T. Li and N. B. Mandayam, "Prospects in a wireless random access game," in *Proc. Annu. Conf. Inf. Sci. Syst.*, pp. 1–6, Princeton, NJ, Mar. 2012.

[8] T. Li and N. B. Mandayam, "When users interfere with protocols: Prospect theory in wireless networks using random access and data pricing as an example," *IEEE Trans. Wireless Commun.*, vol. 13, no. 4, pp. 1888–1907, Apr. 2014.

[9] Y. Yang, L. T. Park, N. B. Mandayam, I. Seskar, A. L. Glass, and N. Sinha, "Prospect pricing in cognitive radio networks," *IEEE Trans. Cognitive Commun. Netw.*, vol. 1, no. 1, pp. 56–70, Mar. 2015.

[10] L. Xiao, J. Liu, Q. Li, N. B. Mandayam, and H. V. Poor, "User-centric view of jamming games in cognitive radio networks," *IEEE Trans. Inf. Forensics and Security*, vol. 10, no. 12, pp. 2578–2590, Dec. 2015.

[11] S. Gao, E. Frejinger, and M. Ben-Akiva, "Adaptive route choices in risky traffic networks: A prospect theory approach," *Transp. Res. C Emerg. Technol.*, vol. 18, no. 5, pp. 727–740, Oct. 2010.

[12] W. Liu, C. Liu, and M. Ge, "An order allocation model for the two-echelon logistics service supply chain based on cumulative prospect theory," *J. Purchasing Supply Management*, vol. 19, no. 1, pp. 39–48, Mar. 2013.

[13] L. A. Prashanth, J. Cheng, F. Michael, M. Steve, and S. Csaba, "Cumulative prospect theory meets reinforcement learning: Prediction and control," in *Proc. ACM Int. Conf. Machine Learning*, pp. 1406–1415, New York, NY, 2016.

[14] Y. Liu, Z. P. Fan, and Y. Zhang, "Risk decision analysis in emergency response: A method based on cumulative prospect theory," *Comput. Oper. Res.*, vol. 42, pp. 75–82, Feb. 2014.

[15] M. Zhang, Z. Zheng, and N. B. Shroff, "Stealthy attacks and observable defenses: A game theoretic model under strict resource constraints," in *Proc. IEEE Global Conf. Signal Inf. Process (GlobalSIP)*, pp. 813–817, Atlanta, GA, Dec. 2014.

[16] J. Pawlick, S. Farhang, and Q. Zhu, "Flip the cloud: Cyber-physical signaling games in the presence of advanced persistent threats," in *Proc. Int. Conf. Decision and Game Theory for Security*, pp. 289–308, Springer, London, UK, Nov. 2015.

[17] M. Zhang, Z. Zheng, and N. B. Shroff, "A game theoretic model for defending against stealthy attacks with limited resources," in *Proc. Int. Conf. Decision and Game Theory for Security*, pp. 93–112, London, UK, Nov. 2015.

[18] P. Hu, H. Li, H. Fu, D. Cansever, and P. Mohapatra, "Dynamic defense strategy against advanced persistent threat with insiders," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, pp. 747–755, HK, May 2015.