# User-Centric View of Smart Attacks in Wireless Networks

Caixia Xie, Liang Xiao*

Dept. of Communication Engineering, Xiamen University, China. Email: lxiao@xmu.edu.cn

***Abstract*—By applying smart and programmable radio devices, selfish end-users can launch smart attacks and choose multiple types of attacks such as jamming and eavesdropping according to the ongoing transmission of wireless networks. In this paper, we apply prospect theory (PT) to formulate the interaction between a smart attacker as an end-user who makes subjective decision regarding his or her attack mode under uncertain attack detection accuracy and a mobile user who chooses whether or not to apply the higher-layer security mechanism to enhance the physical (PHY)-layer security mechanism as a zero-sum game. The Nash equilibria (NEs) of the static smart attack game are derived and their existence conditions are provided to study the impact of the subjectivity of smart attackers. We also propose a defense strategy based on Q-learning, a model free reinforcement learning technique against subjective smart attacks in the dynamic game. Simulation results show that the proposed defense strategy can exploit the subjective view of smart attackers to suppress the attack motivation of end-users and improve the utility of the mobile user.**

***Index Terms*—Smart attacks, prospect theory, game theory, reinforcement learning.**

## I. Introduction

By using smart and programmable radio devices such as universal software radio peripherals (USRPs) or wireless open-access research platform [1], selfish and autonomous end-users can launch smart attacks by choosing multiple types of attacks and controlling the radio transmission mode such as the transmit power and frequency [2]. For example, a smart attacker can choose to keep silent, perform spoofing attacks or send jamming signals based on the defense strategy and the radio channel state to the target mobile user. Compared with traditional attackers who can perform a single type of attack, a smart attacker is more flexible and powerful, and thus causes more serious damage to wireless networks.

Game theory is a powerful math tool to study wireless security, such as jamming [3] and spoofing [4]. However, based on expected utility theory (EUT), most game theoretic study on wireless security assumes that all the players in the game are rational and choose actions to maximize their expected utilities. However, as illustrated by Alais Paradox [5], subjective decisions made by players under uncertainties sometimes deviate from the EUT results. Therefore, prospect theory (PT), a Nobel prize-winning theory uses the probability weighting function and value function to model the decision making process of subjective players. Prospect theory can explain the probability evaluation distortion, and the facts that people tend to be risk averse regarding gains and risk seeking regarding losses [6].

In this paper, we apply prospect theory to investigate smart attacks launched by subjective and selfish end-users under uncertain defense performance in wireless networks. A zero-sum smart attack game is formulated between an attacker and a mobile user who chooses his or her defense mode, i.e., whether to apply the higher-layer security mechanism for better protection, or only the physical (PHY)-layer security mechanism for less system overhead. The Nash equilibria (NEs) of the subjective game are derived and the existing conditions under which the NEs exist are provided to study how to suppress the motivation of smart attacks and provide a tradeoff between wireless security and system overhead.

We propose a defense strategy based on Q-learning, a model free reinforcement learning technique for each mobile user to derive its optimal defense policy according to the previous attack modes in the dynamic smart attack game.

The main contributions of this work can be summarized as follows:

(1) We apply prospect theory to formulate a subjective smart attack game and provide a user-centric view of smart attacks launched by subjective and selfish end-users with multiple attack modes. We derive the NEs of the static smart attack game to study the impact of the subjective view of the smart attacker on the communication performance.

(2) We propose a Q-learning based defense strategy for a mobile user against smart attacks in the dynamic game.

The remainder of this paper is organized as follows. We review related work in Section II and present the system model in Section III. We study the subjective smart attack game in Section IV, and propose a Q-learning based defense strategy against smart attacks in the dynamic game in Section V. Simulation results are given in Section VI and conclusions are drawn in Section VII.

## II. Related Work

An example of the game theoretic study on smart attacks is the EUT-based mobile offloading game formulated in [2], which provides the NEs of the game between the mobile user and the smart attacker who can perform both jamming and spoofing attacks. A noncooperative game between the users

This work was supported in part by the National Science Foundation of China (61271242, 61471308).

978-1-5090-1316-6/16/$31.00 ©2016 IEEE

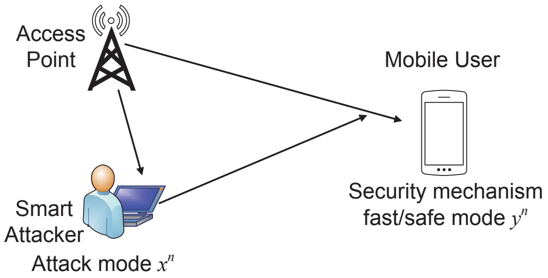


Fig. 1. Illustration of a smart attacker who can choose his or her attack mode, such as jamming and eavesdropping, against a mobile user who applies either the fast mode with the PHY-layer security mechanism or the safe mode with both the PHY-layer and the higher-layer security methods to detect smart attacks.

and the malicious nodes that can eavesdrop, jam, or use a combination of both strategies to reduce the network capacity was formulated in [7], and a fictitious play-based algorithm was proposed to derive a mixed-strategy NE of the game. An adversary that can undermine secret communications by either eavesdropping or jamming was investigated in multiple scenarios using game-theoretic methods [8]. The Bayesian game model was applied to study the defensive effort under uncertain attack type in [9]. A stochastic game was investigated in [10] to provide insights to build the secret and reliable communication against both jamming and eavesdropping.

A PT-based wireless random access game where selfish players adjust their transmission probabilities over a collision channel was formulated in [11], in which the NEs under EUT and PT were compared. Prospect theory was applied in [12] to capture the subjective decision making by end-users in data pricing and channel allocation in cognitive radio networks. The PT-based jamming game presented in [13] discloses the impact of the subjective views of the jammer and end-user under uncertain channel power gains on the signal-to-noise-plus-interference ratio (SINR) in cognitive radio networks.

## III. System Model

As illustrated in Fig. 1, a smart attacker is a selfish and subjective end-user in the wireless network and uses USRPs to choose his or her attack mode at time $n$, denoted by $x^n = 0, 1, ..., K$, where $K$ is the number of attack types. The attacker does not attack if $x^n = 0$, and a larger value of $x^n$ indicates more damages to the mobile user. As a concrete example, the attacker performs eavesdropping if $x^n = 1$, sends jamming signals to reduce the SINR of the mobile user if $x^n = 2$, transmits a signal with a faked media access control (MAC) address of the access point if $x^n = 3$. The target mobile user determines its defense mode denoted by $y^n = 0, 1$. If $y^n = 0$, the mobile user chooses fast mode and uses the basic PHY-layer security mechanism; and if $y^n = 1$, it uses a safe mode with both the PHY-layer and higher-layer security mechanisms for stronger protection with more overhead such as time and energy consumption.

TABLE I
List of Notations

| Symbol | Meaning |
|---|---|
| $K$ | Number of attack types |
| $x = 0, 1, ..., K$ | Attack mode |
| $y = 0, 1$ | Safe/fast defense mode |
| $G_x^y$ | Gain of the user under attack mode $x$ |
| $C_x^y$ | Security loss under attack mode $x$ |
| $z_x^y$ | Miss detection/false alarm rate |
| $\alpha_{D/A}$ | Objective weight of the user/attacker |
| $L$ | Number of non-zero detection error rate quantization levels |
| $P_l^{x,y},\ 0 \le l \le L$ | False alarm/miss detection rate distribution |
| $u_{D/A}$ | Utility of the mobile user/attacker |
| $U_{D/A}^{EUT}$ | Expected utility of the mobile user/smart attacker |
| $U_{D/A}^{PT}$ | PT-based utility of the mobile user/smart attacker |

The gain of the mobile user at defense mode $y$ against attack mode $x$, denoted by $G_x^y$, depends on the transmission benefit plus the gain of successful attack detection minus the detection cost. The security loss of the mobile user denoted by $C_x^y$ represents the cost to detect attacks by mistake, due to either the false alarm or miss detection to detect attack $x$. Let $z_x^y$ be the detection error rate of the mobile user at mode $y$ against attack mode $x$, which is either the miss detection rate or false alarm rate.

Prospect theory can be used to capture the subjective decision-making process of the smart attacker and the mobile user. According to Prelec probability weighting function [14], the subjective probability viewed by the attacker (or mobile user) denoted by $w_A$ (or $w_D$) is given by

$$w_r(p) = \exp\big(-(-\ln p)^{\alpha_r}\big), \tag{1}$$

where $\alpha_r \in (0, 1]$ is the objective weight of the attacker or user, and $p$ is the objective probability. The probability weighting function in (1) describes how a subjective player under-weighs the high-probability event (i.e., $w_r(p) < p$, if $p$ is close to 1) and over-weighs the low probability event (i.e., $w_r(p) > p$, if $p$ is close to 0). Table I summarizes the notation used in this paper.

## IV. Wireless Security Game Against Smart Attacks

The interaction between a smart attacker and a mobile user can be formulated as a wireless security game, denoted by $\mathcal{G}$, in which the attacker as a selfish and subjective human chooses his or her attack mode $x^n = 0, 1, ..., K$, and the mobile user decides its defense mode $y^n = 0, 1$ at time $n$. In the zero-sum game, the utility of the mobile user (or the attacker) in a time slot denoted by $u_D$ (or $u_A$) depends on the attack mode $x$ and defense mode $y$ given by

$$u_D(x, y) = -u_A(x, y) = G_x^y - z_x^y C_x^y, \tag{2}$$

where $z_x^y \in [0,1]$ is the attack detection error rate, which is assumed to follow the distribution $[P_l^{x,y}]_{0\leq l\leq L}$, where $P_l^{x,y}$ is the probability that $z_x^y = l/L$, and $L$ is the non-zero quantization levels. By definition, we have $P_l^{x,y} \geq 0$ and $\sum_{l=0}^{L} P_l^{x,y} = 1$.

According to (2), the expected utilities of the mobile user and the smart attacker averaged over the attack detection accuracies, denoted by $U_D^{EUT}$ and $U_A^{EUT}$ respectively, are given by

$$U_D^{EUT}(x,y) = -U_A^{EUT}(x,y) = G_x^y - \frac{C_x^y}{L}\sum_{l=0}^{L} lP_l^{x,y}. \quad (3)$$

If the mobile user and the attacker hold subjective views to choose their defense and attack mode under uncertain detection accuracy on the error rate, their decisions may deviate from the EUT-based results. The utilities of the mobile user and the attacker based on prospect theory, denoted by $U_D^{PT}$ and $U_A^{PT}$ respectively, are given by

$$U_D^{PT}(x,y) = G_x^y - \frac{C_x^y}{L}\sum_{l=0}^{L} lw_D(P_l^{x,y}) \quad (4)$$

$$U_A^{PT}(x,y) = -G_x^y + \frac{C_x^y}{L}\sum_{l=0}^{L} lw_A(P_l^{x,y}). \quad (5)$$

The PT-based utility utilizes the subjective probability in (1) to replace the objective probability of the detection error rate probability $P_l^{x,y}$ in (3). A subjective player chooses his or her policy to maximize the PT-based utility instead of the expected utility in (3). The Nash equilibrium of the wireless security game $\mathcal{G}$, denoted by $(x^*, y^*)$, provides the best-response of each player, if the opponent chooses the NE strategy and is given by definition as

$$U_D^{PT}(x^*,y^*) \geq U_D^{PT}(x^*,y), \quad \forall y = 0,1 \quad (6)$$
$$U_A^{PT}(x^*,y^*) \geq U_A^{PT}(x,y^*), \quad \forall 0 \leq x \leq K. \quad (7)$$

We evaluate the NE of the wireless security game $\mathcal{G}$ with $K = 2$, i.e., if $x = 0$, the attacker does not attack, if $x = 1$, the attacker eavesdrops the communication, and $x = 2$ represents jamming against the user.

**Theorem 1.** *The wireless security game $\mathcal{G}$ with $K = 2$ has an NE $(0,0)$, if (8) and (9) hold.*

*Proof:* According to (4), if (8) holds, we have

$$U_D^{PT}(0,0) = G_0^0 - \frac{C_0^0}{L}\sum_{l=0}^{L} lw_D(P_l^{0,0})$$
$$\geq G_0^1 - \frac{C_0^1}{L}\sum_{l=0}^{L} lw_D(P_l^{0,1}) = U_D^{PT}(0,1). \quad (10)$$

By (5), if (9) holds, we have

$$U_A^{PT}(0,0) = \frac{C_0^0}{L}\sum_{l=0}^{L} lw_A(P_l^{0,0}) - G_0^0$$
$$\geq \max\left\{\frac{C_1^0}{L}\sum_{l=0}^{L} lw_A(P_l^{1,0}) - G_1^0, \frac{C_2^0}{L}\sum_{l=0}^{L} lw_A(P_l^{2,0}) - G_2^0\right\}$$
$$= \max\left\{U_A^{PT}(1,0), U_A^{PT}(2,0)\right\}. \quad (11)$$

Thus, both (6) and (7) hold for $(0,0)$, which is an NE of the game. ■

**Theorem 2.** *The wireless security game $\mathcal{G}$ with $K = 2$ has an NE $(0,1)$, if (12) and (13) hold.*

*Proof:* Similar to that of Theorem 1. ■

**Theorem 3.** *The wireless security game $\mathcal{G}$ with $K = 2$ has an NE $(2,0)$, if (14) and (15) hold.*

*Proof:* Similar to that of Theorem 1. ■

**Theorem 4.** *The wireless security game $\mathcal{G}$ with $K = 2$ has an NE $(2,0)$, if (16) and (17) hold.*

*Proof:* Similar to that of Theorem 1. ■

**Remark:** If the defender holds the view that the utility of a fast mode is larger than a safe mode, possibly due to a high transmitting gain, a fast mode is preferred. If the smart attacker believes that the defender is able to detect attacks accurately, i.e., the smart attacker is afraid of being detected even it is a small probability event, the smart attacker chooses to keep silent.

As shown in Fig. 2, the attack motivation is suppressed if the attacker is subjective with $\alpha_A < 0.8551$, while a more objective attacker launches jamming attacks if $\alpha_A > 0.8551$, with $\alpha_D = 1$. The same tendency occurs, and the turning point of $\alpha_A$ is 0.9 instead, if $\alpha_D = 0.8$. Therefore, the utility of the mobile user takes a sudden decrease from 0.824 to 0.7725 at $\alpha_A = 0.8551$, if $\alpha_D = 1$.

## V. Dynamic Subjective Wireless Security Game

In the dynamic subjective wireless security game, a smart attacker and a mobile user repeat their interactions without being aware of the environment model. More specifically, the mobile user can apply the Q-learning [15] based defense strategy to derive the optimal defense policy based on the system state denoted by $s^n$, which consists of the attack mode in the last time slot.

The Q-learning algorithm, as a model-free reinforcement learning algorithm, depends on the quality function or Q-function denoted by $Q(x,y)$, which is the expected discount long-term utility if taking defense mode $y$ in state $s$ at time $n$. The value function denoted by $V(s)$ represents the maximum value of the Q-function in state $s$. According to the iterative Bellman equation, the mobile user updates its Q-function at

$$G_0^0 - \frac{C_0^0}{L}\sum_{l=0}^{L} l \exp\left(-\left(-\ln P_l^{0,0}\right)^{\alpha_D}\right) \geq G_0^1 - \frac{C_0^1}{L}\sum_{l=0}^{L} l \exp\left(-\left(-\ln P_l^{0,1}\right)^{\alpha_D}\right) \tag{8}$$

$$\begin{aligned} & G_0^0 - \frac{C_0^0}{L}\sum_{l=0}^{L} l \exp\left(-\left(-\ln P_l^{0,0}\right)^{\alpha_A}\right) \\ & < \min\left\{G_1^0 - \frac{C_1^0}{L}\sum_{l=0}^{L} l \exp\left(-\left(-\ln P_l^{1,0}\right)^{\alpha_A}\right), G_2^0 - \frac{C_2^0}{L}\sum_{l=0}^{L} l \exp\left(-\left(-\ln P_l^{2,0}\right)^{\alpha_A}\right)\right\} \end{aligned} \tag{9}$$

$$G_0^1 - \frac{C_0^0}{L}\sum_{l=0}^{L} l \exp\left(-\left(-\ln P_l^{0,1}\right)^{\alpha_D}\right) \geq G_0^0 - \frac{C_0^0}{L}\sum_{l=0}^{L} l \exp\left(-\left(-\ln P_l^{0,0}\right)^{\alpha_D}\right) \tag{12}$$

$$\begin{aligned} & G_0^1 - \frac{C_0^1}{L}\sum_{l=0}^{L} l \exp\left(-\left(-\ln P_l^{0,1}\right)^{\alpha_A}\right) \\ & \leq \min\left\{G_1^1 - \frac{C_1^1}{L}\sum_{l=0}^{L} l \exp\left(-\left(-\ln P_l^{1,1}\right)^{\alpha_A}\right), G_2^1 - \frac{C_2^1}{L}\sum_{l=0}^{L} l \exp\left(-\left(-\ln P_l^{2,1}\right)^{\alpha_A}\right)\right\} \end{aligned} \tag{13}$$

$$G_2^0 - \frac{C_2^0}{L}\sum_{l=0}^{L} l \exp\left(-\left(-\ln P_l^{2,0}\right)^{\alpha_D}\right) \geq G_2^1 - \frac{C_2^1}{L}\sum_{l=0}^{L} l \exp\left(-\left(-\ln P_l^{2,1}\right)^{\alpha_D}\right) \tag{14}$$

$$\begin{aligned} & G_2^0 - \frac{C_2^0}{L}\sum_{l=0}^{L} l \exp\left(-\left(-\ln P_l^{2,0}\right)^{\alpha_A}\right) \\ & \leq \min\left\{G_0^0 - \frac{C_0^0}{L}\sum_{l=0}^{L} l \exp\left(-\left(-\ln P_l^{0,0}\right)^{\alpha_A}\right), G_1^0 - \frac{C_1^0}{L}\sum_{l=0}^{L} l \exp\left(-\left(-\ln P_l^{1,0}\right)^{\alpha_A}\right)\right\} \end{aligned} \tag{15}$$

$$G_2^1 - \frac{C_2^1}{L}\sum_{l=0}^{L} l \exp\left(-\left(-\ln P_l^{2,1}\right)^{\alpha_D}\right) \geq G_2^0 - \frac{C_2^0}{L}\sum_{l=0}^{L} l \exp\left(-\left(-\ln P_l^{2,0}\right)^{\alpha_D}\right) \tag{16}$$

$$\begin{aligned} & G_2^1 - \frac{C_2^1}{L}\sum_{l=0}^{L} l \exp\left(-\left(-\ln P_l^{2,1}\right)^{\alpha_A}\right) \\ & \leq \min\left\{G_0^1 - \frac{C_0^1}{L}\sum_{l=0}^{L} l \exp\left(-\left(-\ln P_l^{0,1}\right)^{\alpha_A}\right), G_1^1 - \frac{C_1^1}{L}\sum_{l=0}^{L} l \exp\left(-\left(-\ln P_l^{1,1}\right)^{\alpha_A}\right)\right\} \end{aligned} \tag{17}$$

time $n$ as follows:

$$Q\left(s^n, y^n\right) \leftarrow (1-\gamma) Q\left(s^n, y^n\right) \tag{18}$$

$$+ \gamma\left(u_D\left(s^n, y^n\right) + \delta V\left(s^{n+1}\right)\right) \tag{19}$$

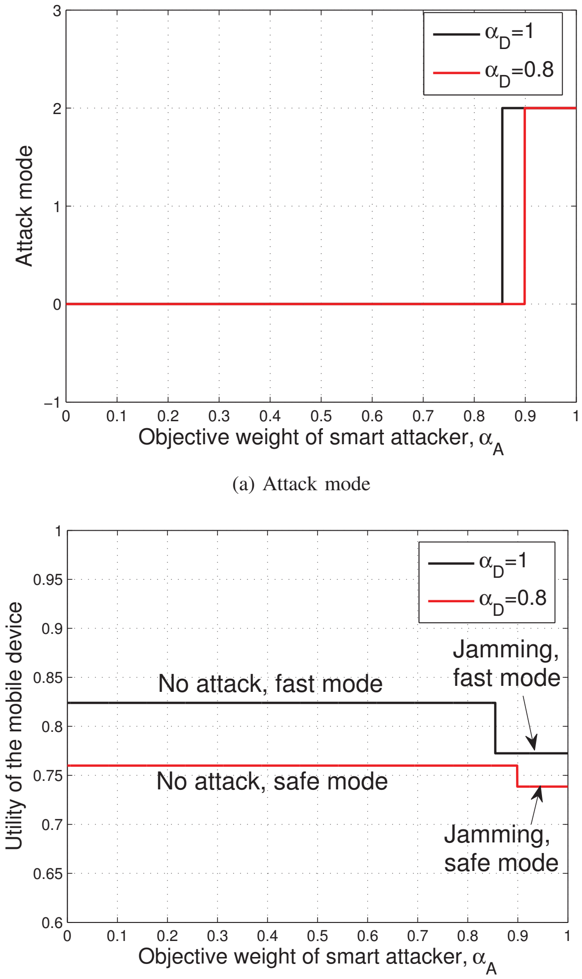
$$V\left(s^n\right) = \max_{y \in \{0,1\}} Q\left(s^n, y^n\right), \tag{20}$$

where the learning factor $\gamma \in (0, 1]$ represents the learning rate of the mobile user, and the discount factor $\delta \in [0, 1]$ represents how the mobile user views the importance of future rewards.

According to the $\epsilon$-greedy strategy, the mobile user chooses the action that maximizes its Q-function with a high probability $1-\epsilon$, and chooses each of the other actions with a small probability, where $\epsilon \in (0, 1)$ is a small positive value. The Q-learning based defense strategy against smart attacks is summarized in Algorithm 1.

## VI. Simulation Results

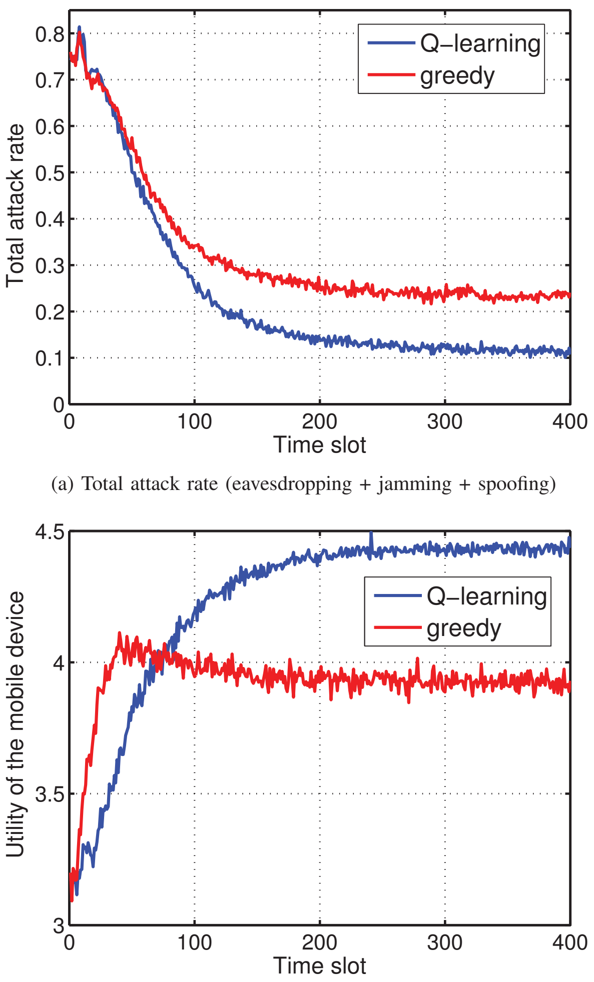
Simulations have been implemented to evaluate the performance of the Q-learning based defense strategy against a smart attacker with Q-learning based attack strategy to choose from eavesdropping, jamming, spoofing and no attack, with $K = 3$, $\boldsymbol{C} = [0.2\ 0.1;\ 0.3\ 0.2;\ 0.6\ 0.3;\ 0.9\ 0.4]$, $\boldsymbol{G} = [1.7\ 4.5;\ 1.5\ 5.7;\ 1.6\ 5.6;\ 1.1\ 5.5]$, $L = 10$, $\alpha_D = 1$, $\alpha_A = 0.8$, $\gamma = 0.95$, $\delta = 0.7$ and $\epsilon = 0.9$, if not specified otherwise. As a benchmark, we evaluate a greedy defense strategy, in which the mobile user chooses the defense mode



(a) Attack mode

(b) Utility of the mobile user

Fig. 2. Performance of the static subjective wireless security game under uncertain detection error rate at the NEs, with $K = 2$, $\boldsymbol{G} = [0.89\ 0.81;\ 1.8\ 1.7;\ 2.19\ 1.4]$, $\boldsymbol{C} = [1.2\ 0.5;\ 0.5\ 0.3;\ 1.5\ 0.7]$, $L = 10$, and the attacker launches eavesdropping attacks if $x = 1$, jamming attacks if $x = 2$, and does not attack if $x = 0$.



(a) Total attack rate (eavesdropping + jamming + spoofing)

(b) Utility of the mobile user

Fig. 3. Performance of the Q-learning based defense strategy against smart attacks in the dynamic game with $K = 3$, $\boldsymbol{C} = [0.2\ 0.1;\ 0.3\ 0.2;\ 0.6\ 0.3;\ 0.9\ 0.4]$, $\boldsymbol{G} = [1.7\ 4.5;\ 1.5\ 5.7;\ 1.6\ 5.6;\ 1.1\ 5.5]$, $L = 10$, $\alpha_D = 1$ and $\alpha_A = 0.8$.

**Algorithm 1** Q-learning based defense strategy

```
Initialize $\gamma$, $\delta$, $\epsilon$, $x^0$, $Q(s, y) = 0$, $V(s) = 0$.
For $n = 1, 2, 3, ...$
    $s^n = x^{n-1}$;
    Choose a defense mode $y^n$ with $\epsilon$-greedy strategy;
    Observe $x^n$;
    Obtain $u_D$;
    Update $Q(s^n, y^n)$ via (19);
    Update $V(s^n)$ via (20);
End for
```

to maximize its immediate utility.

As shown in Fig. 3 (a), the total attack rate of the smart attacker decreases with time from 0.75 at the beginning to 0.12 at time 300. The proposed defense strategy exceeds the benchmark with a lower attack rate, e.g., the attack rate decreases by 54% after 300 time slots. Therefore, as shown in Fig. 3 (b), the utility of the mobile user increases with time slot, and the proposed scheme exceeds the benchmark with a 16% higher utility at time 300 after convergence, because the Q-learning based defense strategy can make a tradeoff between the immediate reward and future reward to achieve the optimal policy by trial.

## VII. Conclusion

In this paper, we have investigated the PT-based wireless security game between a subjective smart attacker who uses smart and programmable radio devices to choose his or her attack mode and a mobile user who can choose the defense mode as a tradeoff between the security level and system overhead. The NEs of the subjective security game have been derived to show the impacts of the subjectivity of the smart attacker and the mobile user on the attack rate and the utility of the mobile user. A Q-learning based defense strategy was proposed for a mobile user to address smart attacks without knowing the attack model and detection accuracy. Simulation results show that the proposed defense strategy improves the utility of the mobile user by 16%, and suppresses the attack rate by 54%, compared with the benchmark defense strategy.

## References

[1] P. Murphy, A. Sabharwal, and B. Aazhang, "Design of WARP: A wireless open-access research platform," in *Proc. Eur. Signal Process. Conf.*, pp. 1–5, Florence, Sep. 2006.

[2] L. Xiao, C. Xie, T. Chen, H. Dai, and H. V. Poor, "Mobile offloading game against smart attacks," in *Proc. IEEE Int'l Conf. on Computer Commun. (INFOCOM), BigSecurity Workshop*, pp. 249–254, San Francisco, CA, Apr. 2016.

[3] L. Xiao, T. Chen, J. Liu, and H. Dai, "Anti-jamming transmission Stackelberg game with observation errors," *IEEE Commun. Letters*, vol. 19, pp. 949–952, Jun. 2015.

[4] R. W. Thomas, B. J. Borghetti, R. S. Komali, and P. Mahonen, "Understanding conditions that lead to emulation attacks in dynamic spectrum access," *IEEE Commun. Magazine*, vol. 49, pp. 32–37, Mar. 2011.

[5] A. Tversky and D. Kahneman, "Advances in prospect theory: Cumulative representation of uncertainty," *J. Risk and Uncertainty*, vol. 5, pp. 297–323, Oct. 1992.

[6] D. Kahneman and A. Tversky, "Prospect theory: An analysis of decision under risk," *Econometrica*, vol. 47, pp. 263–291, Mar. 1979.

[7] Q. Zhu, W. Saad, Z. Han, H. V. Poor, and T. Basar, "Eavesdropping and jamming in next-generation wireless networks: A game-theoretic approach," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, pp. 119–124, Baltimore, MD, Nov. 2011.

[8] A. Garnaev and W. Trappe, "To eavesdrop or jam, that is the question," in *Proc. Int. Conf. on Ad Hoc Networks*, pp. 146–161, Barcelona, Oct. 2013.

[9] A. Garnaev, M. Baykal-Gursoy, and H. V. Poor, "Incorporating attack-type uncertainty into network protection," *IEEE Trans. Info. Forensics and Security*, vol. 9, pp. 1278–1287, Aug. 2014.

[10] A. Garnaev, M. Baykal-Gursoy, and H. V. Poor, "A game theoretic analysis of secret and reliable communication with active and passive adversarial modes," *IEEE Trans. on Wireless Commun.*, vol. 15, pp. 2155–2163, Mar. 2016.

[11] T. Li and N. B. Mandayam, "Prospects in a wireless random access game," in *Proc. Annual Conf. on Info. Sci. and Syst. (CISS)*, pp. 1–6, Princeton, NJ, Mar. 2012.

[12] 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. and Networking*, vol. 1, pp. 56–70, Mar. 2015.

[13] 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. Info. Forensics and Security*, vol. 10, pp. 2578–2590, Dec. 2015.

[14] D. Prelec, "The probability weighting function," *Econometrica*, vol. 66, pp. 497–527, May 1998.

[15] C. J. Watkins and P. Dayan, "Q-learning," *Machine learning*, vol. 8, pp. 279–292, May 1992.