2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS): BigSecurity 16: The Fourth International Workshop on Security and Privacy in Big Data

Mobile Offloading Game Against Smart Attacks

Liang Xiao*§, Caixia Xie*, Tianhua Chen*, Huaiyu Dai†, H. Vincent Poor‡

*Dept. CE, Xiamen University, Xiamen, China. Email: lxiao@xmu.edu.cn

§Beijing Key Laboratory of IOT Information Security Technology, Institute of Information Engineering, Chinese Academy of Science, Beijing, China.

†Dept. ECE, North Carolina State University, Raleigh, USA. Email: Huaiyu_Dai@ncsu.edu

‡Dept. EE, Princeton University, Princeton, USA. Email: poor@princeton.edu

***Abstract*—Mobile cloud computing enables mobile devices such as smartphones to offload data to clouds via access points or base stations to reduce energy consumption and improve their user experience. However, mobile offloading is vulnerable to smart attackers that can exploit software defined radios to perform multiple types of attacks, such as spoofing and jamming, based on the status of radio environments and the offloading process. In this paper, a mobile offloading game against smart attacks, in which a mobile device chooses its offloading rate, a smart attacker chooses the type of its attack, and a security agent decides whether to initiate full data protection for the offloading, is investigated. The interactions among a mobile device, a smart attacker and a security agent are formulated as a secure mobile offloading game. The Nash equilibrium (NE) and its existence conditions are provided for the static secure offloading game. A Q-learning based mobile offloading strategy is proposed for dynamic environments to address smart attacks, in which the mobile device is unaware of the system parameters. Simulation results show that the proposed offloading strategy improves both the offloading rate and the security performance.**

***Index Terms*—Mobile offloading, spoofing, jamming, game theory, smart attacks, big data.**

I. Introduction

With the proliferation of cloud-based mobile services, mobile devices such as smartphones and tablets apply data offloading to improve user experience in terms of longer battery lifetime, larger data storage, faster processing speed and more powerful security services. However, data offloading to clouds via access points (APs) or base stations (BSs) makes mobile devices vulnerable to various attacks such as spoofing and jamming [1]. Moreover, based on software defined radio techniques, a smart attacker cannot only choose its attack strength such as jamming power and frequency, but also the type of attacks according to the ongoing offloading status to maximize its illegal gains. For example, a smart attacker can send spoofing signals against a mobile device with a faked MAC address if the spoofing detection is inaccurate, and send jamming signals if the attacker can efficiently block the offloading signals. A security agent at the AP or BS can apply physical-layer and higher-layer security mechanisms to protect the offloading.

Although the detection in the past of attacks such as spoofing and jamming has been investigated [2], [3], mobile devices suffer from time and energy losses due to false alarms and security loss resulting from missed detections. The security agent at the AP or BS can apply security mechanisms at different levels to detect attacks, possibly by processing the data again or changing the session keys, at the cost of processing and transmission overhead. The optimal offloading rate of a mobile device depends on the status of radio environments and attacks [4]–[7]. For example, local data processing is preferred by a mobile device under strong jamming or heavy traffic at the AP.

Most existing game theoretic study of wireless security are focused on the interaction between an attacker and a mobile user [2], [3], [8]. However, the mobile offloading game against smart attacks involves three players, a mobile device, a smart attacker and a security agent. In this paper, we investigate the secure mobile offloading game, in which the smart attacker has multiple types of attacks, the security agent at the AP or BS defends the network at two levels, and the mobile device determines its offloading rate to maximize its gain against smart attacks. The security agent protects the mobile device with a proper security mode at different costs. The Nash equilibrium (NE) of the static secure mobile offloading game is investigated under various conditions. We also propose an offloading strategy based on reinforcement learning for the mobile device that is unaware of system parameters such as attack costs and detection accuracies in dynamic games.

Our main contribution can be summarized as follows:

- We formulate a secure offloading game among three players: a mobile device that sends data to the cloud, a smart attacker that can perform both jamming and spoofing, and a security agent that can apply both physical-layer and higher-layer security mechanism.
- We derive the NE of the static secure offloading game, and provide conditions under which the NE exists.

This work was supported in part by the NSFC (61271242, 61471308), US National Science Foundation under Grants CMMI-1435778, CNS-1016260, ECCS-1307949 and EARS-1444009.

978-1-4673-9955-5/16/$31.00 ©2016 IEEE

- We propose a Q-learning based offloading strategy for dynamic environments to improve the resistance against smart attacks.

The rest of this paper is organized as follows. We review related work in Section II, and present the system model in Section III. We formulate the secure offloading game and provide its NE in Section IV and present a dynamic secure offloading game in Section V. We provide simulation results in Section VI. Conclusions are drawn in Section VII.

II. Related Work

A mobile offloading algorithm was developed in [4] for intermittently connected cloudlet systems. In [5], each mobile device judiciously decides whether to offload and which portion of an application to offload. The partition offloading algorithm proposed in [6] divides the computational tasks on handheld devices for offloading. Vehicles equipped with sensors offloaded data to the cloud based on the sensing and transmission costs in [9]. A mobile offloading game was formulated in [7] to derive efficient computation offloading for mobile cloud computing. A non-cooperative mobile offloading game was presented in [10], where the offloading rates of smartphones were determined under the limitations of bandwidth and cloud resources. The distributed mobile offloading algorithm for software defined networks proposed in [11] was applied for big data optimization.

The tradeoff between offloading performance and security was investigated in [12]. The transfer of data and computational tasks to clouds is vulnerable to privacy and security risks, such as denial of services attacks [13], and location privacy issues [1]. In [14], MIMO wiretap channels are investigated in which a wiretapper can choose to passively eavesdrop or actively jam. An attacker that can eavesdrop and jam was investigated in [15] for secret communications.

Game theory has been applied to investigate attacks in wireless communications and the Internet, especially for the cases with attack uncertainties or multiple nodes. For example, the interaction between a transmitter and a dual-threat attacker that can eavesdrop and jam was formulated as a zero-sum game for wireless communications in [2]. Jamming games between a user and a smart jammer were considered in [16]. A Bayesian game was formulated for the allocation of the defensive efforts among nodes in a wireless network in [17]. The joint threats from an advanced persistent threat attacker and insiders were studied in [3] as a two-player differential game.

III. System Model

We consider the offloading of a mobile device against a smart attacker under the protection of a security agent at the serving AP or BS, as illustrated in Fig. 1. The mobile device sends data to the cloud via the AP, which is threatened by the smart attacker that can perform spoofing or jamming. The offloading rate denoted by $x \in [0,1]$ is defined as the proportion of the data under processing that is sent by the mobile device to the cloud. If $x = 0$, the mobile device processes the data locally, while $x = 1$ means a full offloading rate.

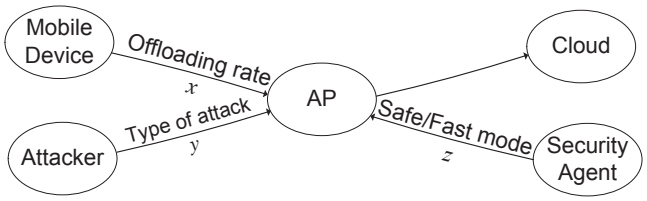


Fig. 1. Illustration of the offloading of a mobile device with offloading rate x against a smart attacker with action y under the protection of a security agent at mode z.

The action of the smart attacker denoted by $y \in \{0,1,2\}$, corresponds to no attack, spoofing and jamming, respectively. The security agent operates in two modes: a safe mode that combines physical-layer and advanced higher-layer security mechanisms to detect attacks ($z = 1$), or a fast mode that applies a basic physical-layer security mechanism ($z = 0$), such as the channel-based spoofing detector in [18]. The cost of the safe mode to the server over that of the fast mode is denoted by β, while the cost of the latter is ignored.

Let C_y^z denote the cost of unit offloading to the mobile device if the smart attacker takes action y against security mode z, which includes the loss of the mobile device due to attack y minus the cost to launch the attack, as well as the penalty of the attacker if being caught by the security agent.

We note that if the attack cost is higher than that of the user loss, C_y^z can be negative. As the attack detection rate depends on the mode of the security agent, the loss of the mobile device C_y^z depends on z. The loss of the mobile device in the fast mode that has weaker protection power is higher than that in the safe mode, i.e., $C_y^0 > C_y^1, \forall y = 1,2$. If there is no attack, we assume zero loss to offloading, i.e., $C_0^z = 0, \forall z = 0,1$.

The gain of the mobile device with unit offloading under attack y and security mode z is denoted by G_y^z. It is clear that $G_0^z = G_1^z = 1$, which is the largest gain for full offloading ($x = 1$), as the transmission of the data is not blocked by the attacker. If the smart attacker sends jamming signals against the transmission with $y = 2$, the gain of the offloading $G_2^z < 1$, as the offloading is blocked. For simplicity, we define a gain matrix $\boldsymbol{G} = [G_y^z]_{y=0,1,2,z=0,1}$ and a cost matrix $\boldsymbol{C} = [C_y^z]_{y=0,1,2,z=0,1}$. Table I summarized the notation used in the paper.

IV. Secure Offloading Game

A. Game Model

We consider a secure offloading game that consists of three players: the mobile device ($\mathcal{M}$), the smart attacker ($\mathcal{A}$) and the security agent ($\mathcal{D}$) that protects the AP. The mobile device chooses its offloading rate $x \in \mathbf{x} = [0,1]$, the attacker determines the type of its attacks $y \in \mathbf{y} = \{0,1,2\}$, and the security agent selects its mode to defend the offloading $z \in \mathbf{z} = \{0,1\}$. In the zero-sum game denoted by $\mathcal{G}$, the utility of the mobile device as well as that of the security

TABLE I
SUMMARY OF SYMBOLS AND NOTATION

$x \in \mathbf{x} = [0,1]$	Offloading rate
$y \in \mathbf{y} = \{0,1,2\}$	Type of attack
$z \in \mathbf{z} = \{0,1\}$	Mode of the security agent
β	Cost of the safe mode
C_y^z	Cost of the mobile device under attack y and security mode z
G_y^z	Gain of the mobile device under attack y and security mode z
$\boldsymbol{C} = [C_y^z]_{\mathbf{y},\mathbf{z}}$	Cost matrix
$\boldsymbol{G} = [G_y^z]_{\mathbf{y},\mathbf{z}}$	Gain matrix
$u/u_{\mathcal{A}}$	Utility of the mobile device/attacker
(x^*, y^*, z^*)	NE of the static secure offloading game

agent is denoted by u, and the utility of the attacker is defined as $u_{\mathcal{A}} = -u$. If the attacker takes no action with $y = 0$, the utility of the mobile device is given by

$$u(x, 0, z) = x - z\beta, \tag{1}$$

where the second term is the cost of the security agent in the attack detection at mode z.

If the smart attacker sends spoofing signals with $y = 1$, the utility of the mobile device is given by

$$u(x, 1, z) = x - C_1^z - z\beta, \tag{2}$$

where C_1^z represents the impact of the spoofing signals.

If the attacker starts jamming with $y = 2$, we have

$$u(x, 2, z) = xG_2^z - C_2^z - z\beta. \tag{3}$$

Note that G_2^z is introduced in the first term as the channel capacity decrease due to a lower signal-to-noise-plus-interference ratio.

By combining $(1) \sim (3)$, we have

$$u(x, y, z) = -u_{\mathcal{A}}(x, y, z) = xG_y^z - C_y^z - z\beta, \tag{4}$$

where x is the offloading rate of the mobile device, y is the type of attack at this time, z is the mode of the security agent, G_y^z is the gain of full offloading under attack y and security mode z, C_y^z denotes the corresponding cost of the mobile device, and β is the cost of the safe mode to the security agent. In summary, we consider a three-player secure offloading game given by $\mathcal{G} = \langle\{\mathcal{M}, \mathcal{A}, \mathcal{D}\}, \{x, y, z\}, \{u, u_{\mathcal{A}}, u\}\rangle$. In the static game $\mathcal{G}$, the three players choose their actions (x, y and z) at the same time to maximize their individual utilities.

B. Nash Equilibria of the Game

The Nash equilibria of the static offloading game $\mathcal{G}$ denoted by (x^*, y^*, z^*) is given by definition as

$$u(x^*, y^*, z^*) \geq u(x, y^*, z^*), \quad \forall x \in \mathbf{x} \tag{5}$$

$$u(x^*, y, z^*) \geq u(x^*, y^*, z^*), \quad \forall y \in \mathbf{y} \tag{6}$$

$$u(x^*, y^*, z^*) \geq u(x^*, y^*, z), \quad \forall z \in \mathbf{z}. \tag{7}$$

Theorem 1. *If $C_1^0 \leq 0$ and $C_2^0 \leq G_2^0 - 1$, the static offloading game $\mathcal{G}$ has an NE given by $(1, 0, 0)$.*

Proof. By (1), we have $u(1,0,0) = 1$, $u(x,0,0) = x$ and $u(1,0,1) = 1-\beta$. By (2) and (3), we have $u(1,1,0) = 1-C_1^0$, and $u(1,2,0) = G_2^0 - C_2^0$. If $C_1^0 \leq 0$ and $C_2^0 \leq G_2^0 - 1$, we have $u(1,0,0) \leq \min\{u(1,1,0), u(1,2,0)\}$. As $0 \leq x \leq 1$, $u(1,0,0) \geq u(x,0,0)$. As $\beta > 0$, $u(1,0,0) > u(1,0,1)$. Thus $(5) \sim (7)$ hold for $(1,0,0)$, which is an NE of $\mathcal{G}$. □

Remark: If the cost for the smart attacker to successfully launch spoofing (or jamming) is high, C_1^0 (or C_2^0) can be negative. In this case, the attack motivation is suppressed, the mobile device offloads with a full rate, and the security agent applies a fast mode at a low cost.

Theorem 2. *If $C_1^z \geq \max\{0, 1 - G_2^z + C_2^z\}$, $\forall z = 0, 1$, the static offloading game $\mathcal{G}$ has two NEs given by*

$$(x^*, y^*, z^*) = \begin{cases} (1,1,0), & C_1^0 - C_1^1 \leq \beta, \\ (1,1,1), & o.w. \end{cases} \tag{8}$$

Proof. By (2), we have $u(1,1,0) = 1 - C_1^0$, $u(x,1,0) = x - C_1^0$ and $u(1,1,1) = 1 - C_1^1 - \beta$. By (1) and (3), we have $u(1,0,0) = 1$ and $u(1,2,0) = G_2^0 - C_2^0$. If $C_1^0 \geq \max\{0, 1 - G_2^0 + C_2^0\}$, we have $u(1,1,0) \leq \min\{u(1,0,0), u(1,2,0)\}$. If $0 \leq x \leq 1$, we have $u(1,1,0) \geq u(x,1,0)$. If $C_1^0 - C_1^1 \leq \beta$, we have $u(1,1,0) \geq u(1,1,1)$. Thus, $(5) \sim (7)$ hold for $(1,1,0)$, which is an NE of $\mathcal{G}$.

Similarly, we can prove that $(1,1,1)$ is an NE, if $C_1^1 \geq \max\{0, 1 - G_2^1 + C_2^1\}$ and $C_1^0 - C_1^1 > \beta$. □

Remark: If spoofing is more harmful to the mobile device than jamming, the smart attacker sends a spoofing signal, the mobile device chooses full offloading, and the security agent applies the mode based on the cost. More specifically, if the safe mode is expensive to carry out compared with the device's potential loss, the security agent chooses a fast mode.

Theorem 3. *If $C_2^z \geq \max\{0, C_1^z, G_2^z - 1, G_2^z - 1 + C_1^z\}$, $\forall z = 0, 1$, the static secure mobile offloading game has six NEs given by*

$$(x^*, y^*, z^*) = \begin{cases} (1,2,0), & I_1 \\ (1,2,1), & I_2 \\ (0,2,0), & I_3 \\ (0,2,1), & I_4 \\ (x_1,2,0), & I_5 \\ (x_2,2,1), & I_6 \end{cases} \tag{9}$$

where

$I_1 : G_2^0 > 0, G_2^1 - C_2^1 - \beta \leq G_2^0 - C_2^0 \leq \min\{1, 1 - C_1^0\}$
$I_2 : G_2^1 > 0, G_2^0 - C_2^0 + \beta < G_2^1 - C_2^1 \leq \min\{1, 1 - C_1^1\}$
$I_3 : G_2^0 < 0, \max\{0, C_1^0\} \leq C_2^0 \leq C_2^1 + \beta$
$I_4 : G_2^1 < 0, \max\{0, C_1^1\} \leq C_2^1 < C_2^0 - \beta$
$I_5 : G_2^0 = 0, \max\{C_1^0 - C_2^0, -C_2^0\} \leq \frac{C_2^1 - C_2^0 + \beta}{G_2^1}$

$I_6: G_2^1 = 0, \max\{C_1^1 - C_2^1, -C_2^1, \frac{C_2^0 - C_2^1 - \beta}{G_2^0}\} \leq 1,$
and

$$\max\left\{C_1^0 - C_2^0, -C_2^0, 0\right\} \leq x_1 \leq \min\left\{\frac{C_2^1 - C_2^0 + \beta}{G_2^1}, 1\right\} \tag{10}$$

$$\max\left\{C_1^1 - C_2^1, -C_2^1, \frac{C_2^0 - C_2^1 - \beta}{G_2^0}, 0\right\} \leq x_2 \leq 1. \tag{11}$$

Proof. By (3), we have $u(1,2,0) = G_2^0 - C_2^0$, $u(x,2,0) = xG_2^0 - C_2^0$ and $u(1,2,1) = G_2^1 - C_2^1 - \beta$. By (1) and (2), we have $u(1,0,0) = 1$ and $u(1,1,0) = 1 - C_1^0$. If $G_2^0 - C_1^0 \leq \min\{1, 1 - C_1^0\}$, we have $u(1,2,0) \leq \min\{u(1,0,0), u(1,1,0)\}$. If $G_2^0 > 0$, we have $u(1,2,0) \geq u(x,2,0)$. If $G_2^0 - C_2^0 \geq G_2^1 - C_2^1 - \beta$, we have $u(1,2,0) \geq u(1,2,1)$. Thus, (5) $\sim$ (7) hold for $(1,2,0)$, which is an NE of $\mathcal{G}$.

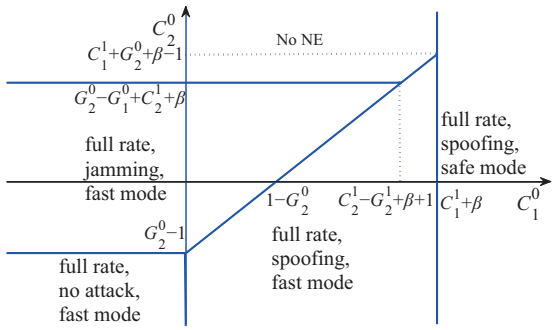
Similarly, we have the NE $(1,2,1)$, $(0,2,0)$ and $(0,2,1)$ under condition I_2, I_3 and I_4, respectively.

Now we consider the case with $G_2^0 = 0$. By (3), we have $u(x,2,0) = -C_2^0$. By (1) and (2), we have $u(x,0,0) = x$ and $u(x,1,0) = x - C_1^0$. If $x \geq \max\{C_1^0 - C_2^0, -C_2^0\}$, we have $u(x,2,0) \leq \min\{u(x,0,0), u(x,1,0)\}$. By (3), we have $u(x,2,0) = -C_2^0$, and $u(x,2,1) = xG_2^1 - C_2^1 - \beta$. If $x \leq \frac{C_2^1 - C_2^0 + \beta}{G_2^1}$, we have $u(x,2,0) \geq u(x,2,1)$. Thus, if $\max\{C_1^0 - C_2^0, -C_2^0\} \leq \frac{C_2^1 - C_2^0 + \beta}{G_2^1}$, (5) $\sim$ (7) hold for $(x_1,2,0)$, which is an NE of $\mathcal{G}$, if $\max\left\{C_1^0 - C_2^0, -C_2^0, 0\right\} \leq x_1 \leq \min\left\{\frac{C_2^1 - C_2^0 + \beta}{G_2^1}, 1\right\}$.

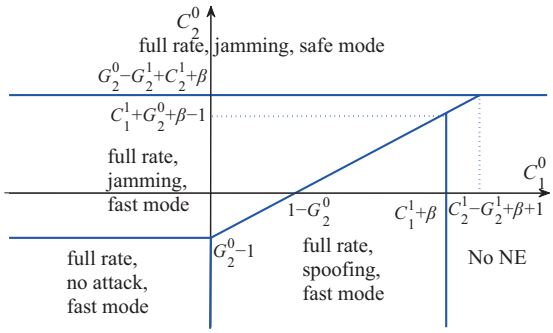
Similarly, we can prove that $(x_2,2,1)$ is an NE if I_6 holds. □

Remark: If the jamming strength is high with $\min\{G_2^0, G_2^1\} < 0$, the mobile data is processed locally at the mobile device. The security mode depends on the cost to the security agent of the safe mode relative to the fast mode.

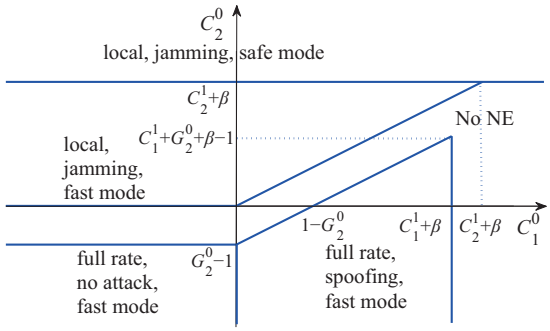
As shown in Fig. 2, the mobile device applies full offloading if $G_2^0 > 0$. The attack motivation is suppressed if the attack cost is too high, possibly due to an accurate attack detection by the security agent. The smart attacker chooses to jam under a high C_2^0, and to spoof if C_1^0 is larger. If the user loss is small, the security agent applies a fast mode, while a safe mode is taken only under large $C_{1/2}^0$.



(a) $G_2^0 > 0$, and $C_1^1 \geq \max\{0, 1 - G_2^1 + C_2^1\}$



(b) $G_2^0 > 0$, and $C_2^1 \geq \max\{G_2^1 - 1, G_2^1 - 1 + C_1^1\}$



(c) $G_2^1 < 0$, and $C_2^1 \geq \max\{0, C_1^1\}$

Fig. 2. Illustration of the NEs and their regions in the static secure offloading game $\mathcal{G}$, where the mobile device applies full rate offloading ($x^* = 1$) or processes the data locally ($x^* = 0$), the smart attacker chooses to spoof ($y^* = 1$), jam ($y^* = 2$) or keep silent ($y^* = 0$), and the security agent enters the fast mode security check ($z^* = 0$) or safe mode ($z^* = 1$).

V. Dynamic Mobile Offloading Game

If the mobile offloading repeats in dynamic environments, we formulate a dynamic mobile offloading game, in which the mobile device, smart attacker, and security agent are unaware of the system parameters such as the cost of attack ($\boldsymbol{C}$) and the gain of offloading ($\boldsymbol{G}$). We consider a Q-learning based offloading strategy, in which the mobile device observes the actions of its two opponents and forms its system state denoted by $\mathbf{s}$. The system state that the mobile device obtains at the n-th time slot is given by $\mathbf{s}^n = [y^{n-1}, z^{n-1}]$. In the dynamic game, the offloading rate is quantified into L levels and is selected based on the state, i.e., $x^n \in \{\frac{i}{L-1} : 0 \leq i \leq L-1\}$ for simplicity.

Let $Q(\mathbf{s}, x)$ denote the quality function of the mobile device with offloading rate x in state $\mathbf{s}$. The value function denoted by $V(\mathbf{s})$ represents the maximum Q value in state $\mathbf{s}$. The mobile device updates its Q-function based on the observed instant

Algorithm 1 Secure offloading strategy with Q-learning.

Initialize α, δ, ϵ, Q, $V(\mathbf{s})$, y, z.
For $n = 1, 2, 3, ...$
  Update the state $\mathbf{s}^n = [y^{n-1}, z^{n-1}]$;
  Choose the offloading rate x^n via (14);
  Send x^n of the data to the cloud;
  Observe y^n and z^n;
  Obtain utility u;
  Update $Q(\mathbf{s}^n, x^n)$ via (12);
  Update $V(\mathbf{s}^n)$ via (13).
End for

utility u and the value function as follows:

$$Q\left(\mathbf{s}^n, x^n\right) \leftarrow (1-\alpha) Q\left(\mathbf{s}^n, x^n\right) + \alpha\left(u\left(\mathbf{s}^n, x^n\right) + \delta V\left(\mathbf{s}^{n+1}\right)\right) \quad (12)$$

$$V\left(\mathbf{s}^n\right) = \max_{\mathbf{x}} Q\left(\mathbf{s}^n, x^n\right), \quad (13)$$

where $\alpha \in (0, 1]$ is a learning factor indicating the weight of the current estimate $Q(\mathbf{s}^n, x^n)$ in the update of the quality function, and the discount factor δ represents the uncertainty of the mobile device about the future rewards.

According to the ϵ-greedy policy [19], the offloading rate that maximizes the current quality function is chosen with a high probability $1-\epsilon$, while the other $L-1$ rates are taken with equal probability $\frac{\epsilon}{L-1}$, i.e.,

$$\Pr\left(x^n\right) = \begin{cases} 1-\epsilon, & x^n = \arg\max_{\mathbf{x}} Q\left(\mathbf{s}^n, x\right) \\ \frac{\epsilon}{L-1}, & o.w. \end{cases} \quad (14)$$

The secure offloading process of the mobile device is summarized in Algorithm 1.

VI. Simulation Results

Simulations have been performed to evaluate the performance of the dynamic secure offloading game with $L = 11$, $\boldsymbol{C} = [0, 0; -0.1, -0.3; -0.5, -0.8]$, $\boldsymbol{G} = [1, 1; 1, 1; 0.6, 0.9]$, $\beta = 0.2$, $\alpha = 0.9$, $\delta = 0.7$ and $\epsilon = 0.95$.

As shown in Fig. 4(a), the mobile device with the proposed offloading scheme applies a higher offloading rate until reaching a value as high as 0.93, which is 86% higher than that of a random strategy.

The jamming rate and spoofing rate as shown in Fig. 4(b) decrease from 0.33 to 0.05 and 0.07, respectively, which is consistent with the results of Theorems $1\sim3$. The proposed strategy has a higher security rate than the random counterpart. For example, the spoofing rate of the random strategy is 0.13 and that of the proposed scheme achieves 0.07. The safe mode rate in Fig. 4(c) shows that as the no-attack rate increases, the security agent tends to choose the fast mode with probability 80%.

The proposed offloading strategy increases the utility of the mobile device as shown in Fig. 4(d), e.g, the original utility is 0.65, and it reaches 0.9 finally. In contrast, the utility of the random strategy decreases under smart attacks, as the latter adjusts its attack type to maximize its illegal gains.

VII. Conclusions

In this paper, we have investigated the offloading game of a mobile device against a smart attacker that can perform jamming and spoofing with a security agent that protects the AP with a fast mode or safe mode. We have derived the NE of the static secure offloading game and provided conditions for various attack scenarios. We have also proposed a Q-learning based offloading game for dynamic environments. Simulation results show that both the utility of the mobile device and the security performance are improved by the proposed scheme. For example, compared with random offloading, the proposed scheme reduces the jamming rate by 6%. The utility of the mobile device is increased by 97%.

References

[1] K. Kumar and Y. Lu, "Cloud computing for mobile users: Can offloading computation save energy?," *IEEE Trans. Computers*, vol. 43, pp. 51–56, Apr. 2010.

[2] A. Mukherjee and A. L. Swindlehurst, "Optimal strategies for countering dual-threat jamming/eavesdropping-capable adversaries in MIMO channels," in *Proc. IEEE Military Commun. Conf.*, pp. 1695–1700, Oct. 2010.

[3] P. Hu, H. Li, H. Fu, D. Cansever, and P. Mohapatra, "Dynamic defense strategy against advanced persistent threat with insiders," in *Proc. IEEE Int'l Conf. on Computer Commun. (INFOCOM)*, 2015.

[4] Z. Yang, D. Niyato, and P. Wang, "Offloading in mobile cloudlet systems with intermittent connectivity," *IEEE Trans. Mobile Computing*, vol. 14, pp. 2516–2529, Dec. 2015.

[5] Y. Wang, X. Lin, and M. Pedram, "A nested two stage game-based optimization framework in mobile cloud computing system," in *Proc. IEEE Int'l Symposium on Service Oriented System Engineering (SOSE)*, pp. 494–502, Mar. 2013.

[6] Z. Li, C. Wang, and R. Xu, "Computation offloading to save energy on handheld devices: A partition scheme," in *Proc. ACM int'l conf. on Compilers, Architecture, and Synthesis for Embedded Systems*, pp. 238–246, 2001.

[7] X. Chen, "Decentralized computation offloading game for mobile cloud computing," *IEEE Trans. Parallel and Distributed Systems*, vol. 26, pp. 974–983, Apr. 2015.

[8] H. Sun, S. Hsu, and C. Chen, "Mobile jamming attack and its countermeasure in wireless sensor networks," in *Proc. IEEE Int'l Conf. on Advanced Information Networking and Applications Workshops*, vol. 1, pp. 457–462, May 2007.

[9] L. Xiao, T. Chen, C. Xie, and J. Liu, "Mobile crowdsensing game in vehicular networks," in *Proc. IEEE Region 10 Conference (TENCON), invited talk*, pp. 1–6, Nov. 2015.

[10] Y. Li, J. Liu, Q. Li, and L. Xiao, "Mobile cloud offloading for malware detections with learning," in *Proc. IEEE Int'l Conf. on Computer Communications (INFOCOM), -BigSecurity Workshop*, pp. 197–201, Apr. 2015.

[11] L. Liu, X. Chen, M. Bennis, G. Xue, and Z. Han, "A distributed ADMM approach for mobile data offloading in software defined network," in *Proc. IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1748–1752, Mar. 2015.

[12] T. Meng, K. Wolter, and Q. Wang, "Security and performance tradeoff analysis of mobile offloading systems under timing attacks," in *Computer Performance Engineering*, vol. 9272, pp. 32–46, Springer, Aug. 2015.

[13] J. Park, K. Yi, and J. Park, "SSP-MCloud: A study on security service protocol for smartphone centric mobile cloud computing," in *IT Convergence and Services*, vol. 107, pp. 165–172, Springer, Nov. 2011.

[14] A. Mukherjee and A. Swindlehurst, "Jamming games in the MIMO wiretap channel with an active eavesdropper," *IEEE Trans. Signal Processing*, vol. 61, pp. 82–91, Jan. 2013.

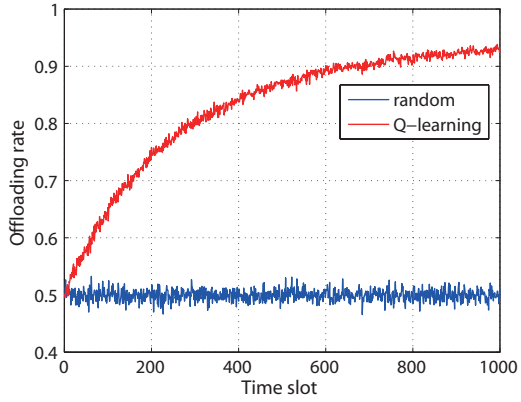
[15] A. Garnaev and W. Trappe, "To eavesdrop or jam, that is the question," in *Ad Hoc Networks*, pp. 146–161, Springer, Jan. 2014.

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

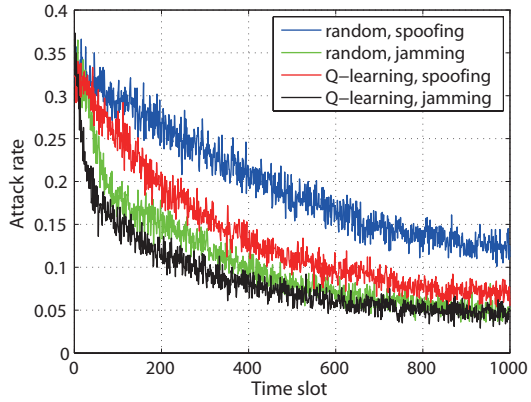
[17] A. Garnaev, M. Baykal-Gursoy, and H. V. Poor, "Incorporating attack-type uncertainty into network protection," *IEEE Trans. Information Forensics and Security*, vol. 9, pp. 1278–1287, Aug. 2014.

[18] L. Xiao, L. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based spoofing detection in frequency-selective rayleigh channels," *IEEE Trans. Wireless Communications*, vol. 8, pp. 5948–5956, Dec. 2009.

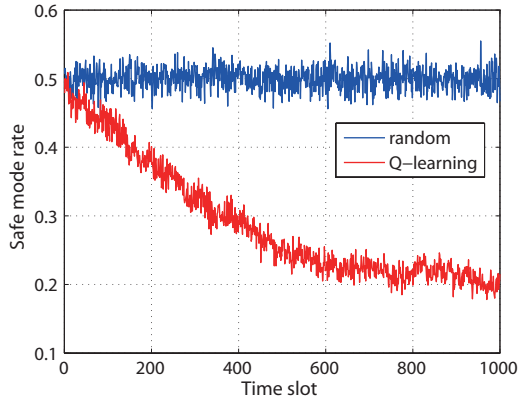
[19] L. Busoniu, R. Babuska, and B. De Schutter, "A comprehensive survey of multiagent reinforcement learning," *IEEE Trans. Systems, Man, and Cybernetics, Part C: Applications and Reviews*, vol. 38, pp. 156–172, Mar. 2008.



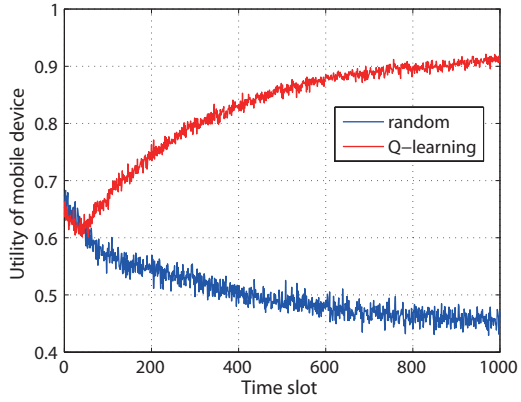
(a) Average offloading rate



(b) Attack rate



(c) Safe mode rate



(d) Average utility of the mobile device

Fig. 3. Performance of the dynamic offloading game with $\boldsymbol{C} = [0, 0; -0.1, -0.3; -0.5, -0.8]$, $\boldsymbol{G} = [1, 1; 1, 1; 0.6, 0.9]$, and $\beta = 0.2$.