Game Theoretic Study of Protecting MIMO Transmissions Against Smart Attacks

Yanda Li*, Liang Xiao*, Huaiyu Dai†, H. Vincent Poor‡
*Dept. Communication Engineering, Xiamen University, Xiamen, China. Email: lxiao@xmu.edu.cn
†Dept. Electrical and Computer Engineering, North Carolina State University, Raleigh, USA.
Email: Huaiyu_Dai@ncsu.edu
‡Dept. Electrical Engineering, Princeton University, Princeton, USA. Email: poor@princeton.edu

***Abstract*—Multiple-input multiple-output (MIMO) systems are threatened by smart attackers, who apply programmable radio devices such as software defined radios to perform multiple types of attacks such as eavesdropping, jamming and spoofing. In this paper, MIMO transmission in the presence of smart attacks is formulated as a noncooperative game, in which a MIMO transmitter chooses its transmit power level and a smart attacker determines its attack type accordingly. A Nash equilibrium of this secure MIMO transmission game is derived and conditions assuring its existence are provided to reveal the impact of the number of antennas and the costs of the attacker to launch each type of attack. A power control strategy based on Q-learning is proposed for the MIMO transmitter to suppress the attack motivation of smart attackers in a dynamic version of MIMO transmission game without being aware of the attack and the radio channel model. Simulation results show that our proposed scheme can reduce the attack rate of smart attackers and improve the secrecy capacity compared with the benchmark strategy.**

***Index Terms*—MIMO, smart attacks, power control, game theory, learning**

I. Introduction

Multiple-input multiple-output (MIMO) techniques that can improve the capacity and reliability of wireless communications [1] are still threatened by smart attackers, who use smart and programmable radio devices such as software defined radios (SDRs) to flexibly choose their attack methods or even the types of attacks, such as eavesdropping [2], jamming [3] and spoofing [4], [5], according to the ongoing transmission status and the radio channel states. For example, the multiuser MIMO system is vulnerable to active sniffing attacks, in which eavesdroppers report faked channel state information to access points to improve their own capacities [2]. Another example is the eavesdropper who sends spoofing signals and pretends to be an amplify-and-forward relaying node [6]. A smart attacker can also combine passive eavesdropping with active jamming to attack massive MIMO systems [7]. However, most MIMO power allocation strategies [8] have been designed for attack-free radio environments.

Game theory can be used to analyze wireless security under uncertain types of attacks [9]–[13], and the secrecy capacity of wireless communications against both active and passive attacks [14]. Reinforcement learning based attacker type identification developed in [10] improves the transmission capacity under an uncertain type of attacks in time-varying radio channels. The intrusion detection system investigated in [14] helps legitimate users resist smart eavesdroppers by switching the transmission mode. The relay architecture presented in [15] applies fictitious play to improve secrecy capacity against both eavesdropping and jamming. The interactions between a transmitter and an eavesdropper are formulated in [16] as a zero-sum game, yielding a power allocation strategy to improve the secrecy capacity.

In this paper, we investigate a secure transmission game for multiple-antenna systems against smart attackers who choose their attack methods and perform eavesdropping, jamming or spoofing according to the status of the MIMO transmitter and the radio channel states. The Nash equilibrium (NE) of the static secure MIMO transmission game is derived and an existence condition is analyzed to investigate the impact of the number of antennas and the attack costs on the resistance against smart attacks.

As a model-free reinforcement learning technique, the Q-learning algorithm can derive the optimal strategy with probability one if all the feasible actions are repeatedly sampled over all the states in the Markov decision process [17]. A Q-learning based power control scheme is proposed for the MIMO transmitter to resist smart attacks without being aware of the attack and channel models in the dynamic secure MIMO transmission game, in which the transmit power level is chosen based on the quality function of each action-state pair that is updated via the anti-attack communication history. Simulation results show that our proposed scheme can improve the secrecy capacity and reduce the attack rate of smart attackers in the MIMO transmission game.

The contributions of this work can be summarized as follows:

(1) We formulate a secure MIMO transmission game against smart attacks, and derive the NE of the static MIMO game.

(2) We propose a Q-learning based power control scheme for the MIMO transmitter to improve the secrecy capacity against smart attacks in the dynamic game.

The remainder of the paper is organized as follows: We present the system model in Section II, and investigate a secure

This research was supported in part by National Natural Science Foundation of China under Grant 61671396 and the CCF-Venustech Hongyan Research Initiative (2016-010), and in part by the U.S. National Science Foundation under Grants ECCS-1307949, EARS-1444009, CMMI-1435778 and ECCS-1647198.

978-1-4673-8999-0/17/$31.00 ©2017 IEEE

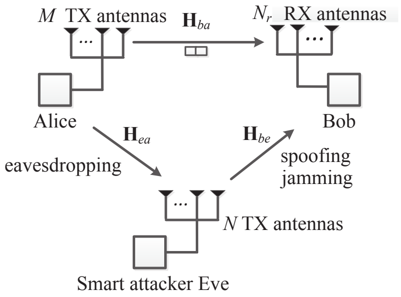


Fig. 1. Illustration of the secure MIMO transmission between Alice and Bob against Eve.

TABLE I
SUMMARY OF SYMBOLS AND NOTATION.

Notation	Definition
M	Number of antennas at Alice
N_r	Number of antennas at Bob
N	Number of antennas at Eve
P_{max}	Maximal transmit power of Alice
$\mathbf{H}_{ba/be/ea}$	Channel matrix
$\lambda_i^{ba/be/ea}$	i-th eigenvalue of the channel matrix
$\mathbf{y}_{J/S}$	Signal received by Bob under jamming/spoofing attacks
$\mathbf{n}_{b/e}$	Receiver noise vector at Bob/Eve
$\mathbf{x}_a$	Transmit signal of Alice
$\mathbf{y}_E$	Signal received by Eve
$\mathbf{z}_{J/S}$	Transmit signal of Eve
$\mathbf{\Theta} = [0, \theta_E, \theta_J, \theta_S]$	Attack costs
$\mathbf{G} = [R\ R_E\ R_J\ R_S]$	Gain vector
C_a	Transmission cost of Alice
L	Maximal quantized power level

MIMO game in Section III. We present a dynamic MIMO game in Section IV, and provide simulation results in Section V. We draw the conclusions in Section VI.

II. System Model

As shown in Fig. 1, we consider a MIMO system consisting of Alice who uses M antennas to communicate with Bob with N_r antennas, against a smart attacker Eve who applies programmable radio devices with N antennas to eavesdrop, jam, spoof or keep silent in each time slot. More specifically, Eve uses N antennas to eavesdrop on Alice's signals if she can derive enough information; sends jamming signals if she can efficiently block Alice's signal at Bob; or spoofs Alice if the spoofing detection rate is low. The action of Eve is denoted by $q \in \{0, 1, 2, \cdots, K\}$, where K is the number of attack types. In this work, we set $K = 3$ and assume that Eve keeps silent, eavesdrops, jams or sends spoofing signals, respectively, if $q = 0,\ 1,\ 2$ or 3.

Alice sends an M-dimensional signal vector denoted by $\mathbf{x}_a$ with transmit power $P = \mathcal{E}\left[\mathbf{x}_a^T\mathbf{x}_a\right]$, following power constraint P_{max}, i.e., $0 \le P \le P_{max}$. The $N_r \times M$ channel matrix $\mathbf{H}_{ba}$ consists of the channel power gains from the transmit (TX) antennas at Alice to the receive (RX) antennas at Bob. The i-th largest eigenvalue of $\mathbf{H}_{ba}\mathbf{H}_{ba}^T$ is denoted by λ_i^{ba}. Similarly, the channel matrix between Alice and Eve (or between Eve and Bob) is denoted by $\mathbf{H}_{ea}$ $\left(\text{or } \mathbf{H}_{be}\right)$, and the corresponding largest eigenvalue is denoted by λ_i^{ea} $\left(\text{or } \lambda_i^{be}\right)$.

Each channel matrix is assumed to have independent and identically distributed (i.i.d) complex Gaussian elements, i.e., $\mathbf{H}_\mu \sim \mathcal{CN}(\mathbf{0}, \sigma_\mu^2\mathbf{I})$, with $\mu = ba, be$ and ea. Bob can estimate the Alice-Bob channel matrix $\mathbf{H}_{ba}$, which is not known by Alice who has to allocate power uniformly over M transmit antennas. For simplicity, the N_r-dimensional receiver noise vector at Bob, denoted by $\mathbf{n}_b$, is assumed to be normalized complex Gaussian, i.e., $\mathbf{n}_b \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$. By using the singular value decomposition of $\mathbf{H}_{ba}$ and assuming Gaussian distributed signals, by [8], we can write the capacity of the MIMO transmission denoted by R as

$$R = \log_2 \det\left(\mathbf{I} + \frac{P}{M}\mathbf{H}_{ba}\mathbf{H}_{ba}^T\right) = \sum_{i=1}^{N_r} \log_2\left(1 + \frac{P\lambda_i^{ba}}{M}\right). \tag{1}$$

If Eve listens to Alice's signal $\mathbf{x}_a$, she receives a signal $\mathbf{y}_E$ given by

$$\mathbf{y}_E = \mathbf{H}_{ea}\mathbf{x}_a + \mathbf{n}_e, \tag{2}$$

where $\mathbf{n}_e$ is an N-dimensional additive normalized zero-mean complex Gaussian noise vector, i.e., $\mathbf{n}_e \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$. In this case, the maximum achievable MIMO secrecy rate, denoted by R_E, is given by [18] by

$$\begin{aligned} R_E &= \log_2 \det\left(\mathbf{I} + \frac{P}{M}\mathbf{H}_{ba}\mathbf{H}_{ba}^T\right) - \log_2 \det\left(\mathbf{I} + \frac{P}{M}\mathbf{H}_{ea}\mathbf{H}_{ea}^T\right) \\ &= \sum_{i=1}^{N_r} \log_2\left(1 + \frac{P\lambda_i^{ba}}{M}\right) - \sum_{i=1}^{N} \log_2\left(1 + \frac{P\lambda_i^{ea}}{M}\right). \end{aligned} \tag{3}$$

If Eve sends a jamming signal, denoted by $\mathbf{z}_J$, with the power constraint $P_J = \mathcal{E}\left[\mathbf{z}_J^T\mathbf{z}_J\right]$ to interrupt Alice's transmission, Bob receives a signal denoted by $\mathbf{y}_J$, and given by

$$\mathbf{y}_J = \mathbf{H}_{ba}\mathbf{x}_a + \mathbf{H}_{be}\mathbf{z}_J + \mathbf{n}_b. \tag{4}$$

Not knowing $\mathbf{H}_{be}$, Eve has to allocate the transmit power uniformly over N antennas, i.e., $\mathcal{E}\left[\mathbf{z}_J\mathbf{z}_J^T\right] = P_J\mathbf{I}/N$. Based on the signal-to-noise-plus-interference-ratio (SINR) of the signal received at Bob, the capacity under jamming denoted by R_J is given by [18] as

$$\begin{aligned} R_J &= \log_2 \det\left(\mathbf{I} + \frac{P}{M}\mathbf{H}_{ba}\mathbf{H}_{ba}^T\left(\mathbf{I} + \frac{P_J}{N}\mathbf{H}_{be}\mathbf{H}_{be}^T\right)^{-1}\right) \\ &= \sum_{i=1}^{N_r} \log_2\left(1 + \frac{P\lambda_i^{ba}N}{M(N + \lambda_i^{be}P_J)}\right). \end{aligned} \tag{5}$$

If Eve uses N antennas to send a spoofing signal $\mathbf{z}_S$ with $\mathcal{E}\left[\mathbf{z}_S\mathbf{z}_S^T\right] = P_S\mathbf{I}/N$, Bob obtains a signal denoted by $\mathbf{y}_S$ from N_r antennas, which is given by

$$\mathbf{y}_S = \mathbf{H}_{be}\mathbf{z}_S + \mathbf{n}_b. \tag{6}$$

The "secrecy capacity" under spoofing attacks, denoted by R_S, is defined as the difference between the MIMO capacity and the capacity between Eve and Bob, because the loss increases with the number of the spoofing messages received by Bob, which is modeled as a linear function of the capacity between Eve and Bob for simplicity. Note that a spoofer aims to send spoofing information to Bob instead of blocking the transmission of Alice. Therefore, if choosing to perform spoofing attacks, Eve sends signals only when Alice is silent. By applying singular value decomposition on channel matrices $\mathbf{H}_{ba}$ and $\mathbf{H}_{be}$ and assuming equal power allocation, we can rewrite the capacity of Alice under spoofing as

$$R_S = \log_2 \det\left(\mathbf{I} + \frac{P}{M}\mathbf{H}_{ba}\mathbf{H}_{ba}^T\right) - \gamma \log_2 \det\left(\mathbf{I} + \frac{P_S}{N}\mathbf{H}_{be}\mathbf{H}_{be}^T\right)$$
$$= \sum_{i=1}^{N_r} \log_2\left(1 + \frac{P\lambda_i^{ba}}{M}\right) - \gamma \sum_{i=1}^{N_r} \log_2\left(1 + \frac{P_S\lambda_i^{be}}{N}\right), \qquad (7)$$

where γ quantifies the impact of each spoofing message of unit size. For ease of reference, the commonly used notation is summarized in TABLE 1.

III. Secure MIMO Transmission Game

The interactions between Alice and Eve in the MIMO transmissions are formulated as a static secure MIMO game denoted by $\mathbb{G}$, in which Alice chooses her transmit power $0 \le P \le P_{max}$ and Eve chooses her attack mode $q \in \{0, 1, 2, 3\}$, corresponding to no-attack, eavesdropping, jamming and spoofing, respectively. In each time shot, Eve chooses her action to decrease the "secrecy capacity" of Alice, i.e., R_E, R_J or R_S, and to reduce her attack cost and the resulting penalty if detected.

Let $f(q)$ denote the cost for Eve to perform attack q. For simplicity, we set $f(q) = 0$, θ_E, θ_J and θ_S, respectively, for $q = 0$, 1, 2 and 3, where θ_E, θ_J and θ_S are the costs of Eve to launch eavesdropping, jamming and spoofing attacks, respectively, which consist of the transmission or receive costs and the risks of being detected. For compactness, we define the attack cost vector as $\mathbf{\Theta} = [0, \theta_E, \theta_J, \theta_S]$.

The utility of Alice in the static game, denoted by u_a, depends on the MIMO secrecy capacity and the transmit power consumption, and is defined as

$$u_a(P, q) = \ln 2 \sum_{k=0}^{K} G_k \mathrm{I}(k = q) - C_a P, \qquad (8)$$

where C_a is the cost of unit transmit power for Alice, G_k is the k-th element of the transmission gain vector $\mathbf{G} = [R\ R_E\ R_J\ R_S]$, and $\mathrm{I}(\cdot)$ is the indicator function, which equals 1 if its argument is true and 0 otherwise. The coefficient $\ln 2$ is introduced to simplify the analysis of the NE of the game. Similarly, the utility of Eve in the static game, denoted by u_e, depends on the secrecy capacity and the attack cost, i.e.,

$$u_e(P, q) = -\ln 2 \sum_{k=0}^{K} G_k \mathrm{I}(k = q) - f(q). \qquad (9)$$

In summary, we consider a secure MIMO game given by $\mathbb{G} = \langle\{\mathbb{A}, \mathbb{E}\}, \{P, q\}, \{u_a, u_e\}\rangle$, in which Alice chooses her total transmit power P over M antennas to maximize her utility u_a, while Eve chooses her attack strategy q to maximize u_e. The NE strategy of the game $\mathbb{G}$ denoted by (P^*, q^*) is given by definition as

$$u_a(P^*, q^*) \ge u_a(P, q^*), \qquad \forall 0 \le P \le P_{max} \qquad (10)$$
$$u_e(P^*, q^*) \ge u_e(P^*, q), \qquad \forall q = 0, 1, 2, 3. \qquad (11)$$

Lemma 1. *The static secure MIMO game* $\mathbb{G}$ *has an NE* $(x^*, 0)$ *given by*

$$\begin{cases} \displaystyle\sum_{i=1}^{N_r} \frac{1}{M/\lambda_i^{ba} + x^*} = C_a & (12a) \\ 0 \le x^* \le P_{max}, & (12b) \end{cases}$$

if

$$\begin{cases} \displaystyle\theta_E \ge \sum_{i=1}^{N} \ln\left(1 + \frac{x^*\lambda_i^{ea}}{M}\right) & (13a) \\ \displaystyle\theta_J \ge \sum_{i=1}^{N_r} \ln\left(1 + \frac{x^* P_J \lambda_i^{ba}\lambda_i^{be}}{M(N + P_J\lambda_i^{be}) + x^* N\lambda_i^{ba}}\right) & (13b) \\ \displaystyle\theta_S \ge \gamma \sum_{i=1}^{N_r} \ln\left(1 + \frac{P_S\lambda_i^{be}}{N}\right) & (13c) \\ \displaystyle\sum_{i=1}^{N_r} \frac{1}{M/\lambda_i^{ba} + P_{max}} < C_a < \sum_{i=1}^{N_r} \lambda_i^{ba}/M. & (13d) \end{cases}$$

Proof: If Eqs. (13a)-(13c) hold, by (9), we have

$$u_e(x^*, 0) - u_e(x^*, 1) = \theta_E - \sum_{i=1}^{N} \ln\left(1 + \frac{x^*\lambda_i^{ea}}{M}\right) \ge 0$$
$$u_e(x^*, 0) - u_e(x^*, 2) = \theta_J - \sum_{i=1}^{N_r} \ln\left(1 + \frac{x^* P_J \lambda_i^{ba}\lambda_i^{be}}{M(N + P_J\lambda_i^{be}) + x^* N\lambda_i^{ba}}\right) \ge 0$$
$$u_e(x^*, 0) - u_e(x^*, 3) = \theta_S - \gamma \sum_{i=1}^{N_r} \ln\left(1 + \frac{P_S\lambda_i^{be}}{N}\right) \ge 0.$$

Thus, (11) holds for $(x^*, 0)$.

By (8), we have

$$\frac{\partial u_a(P, 0)}{\partial P} = \sum_{i=1}^{N_r} \frac{1}{M/\lambda_i^{ba} + P} - C_a \qquad (14)$$
$$\frac{\partial^2 u_a(P, 0)}{\partial P^2} = -\sum_{i=1}^{N_r} \left(\frac{1}{M/\lambda_i^{ba} + P}\right)^2 \le 0, \qquad (15)$$

indicating that $\partial u_a(P, 0)/\partial P$ monotonically decreases with P. Thus if (13d) holds, by (14), we have

$$\frac{\partial u_a(P, 0)}{\partial P}|_{P=0} = \sum_{i=1}^{N_r} \frac{\lambda_i^{ba}}{M} - C_a > 0 \qquad (16)$$
$$\frac{\partial u_a(P, 0)}{\partial P}|_{P=P_{max}} = \sum_{i=1}^{N_r} \frac{1}{M/\lambda_i^{ba} + P_{max}} - C_a < 0, \qquad (17)$$

showing that $\partial u_a(P, 0)/\partial P = 0$ has a unique solution given by (12a). By (15)-(17), we see that $u_a(P, 0)$ increases with P, if $P \leq x^*$, and it decreases with P if $P > x^*$. Thus (10) also holds and $(x^*, 0)$ is an NE of the game. ■

As shown in Lemma 1, the attack motivation is suppressed if the attack costs are higher than the transmission cost of Alice $\big($i.e., Eqs. (13a)-(13c)$\big)$. Otherwise, under serious radio channel degradation and serious potential information leakage, $\big($i.e., Eqs. (13d)$\big)$, Alice stops transmission.

Lemma 2. *The NE of the static secure MIMO game* $\mathbb{G}$ *is* $(P_{max}, 0)$ *if*

$$\begin{cases} \theta_E \geq \displaystyle\sum_{i=1}^{N} \ln\left(1 + \frac{P_{max}\lambda_i^{ea}}{M}\right) & \text{(18a)} \\ \theta_J \geq \displaystyle\sum_{i=1}^{N_r} \ln\left(1 + \frac{P_{max}P_J\lambda_i^{ba}\lambda_i^{be}}{M(N + P_J\lambda_i^{be}) + P_{max}N\lambda_i^{ba}}\right) & \text{(18b)} \\ \theta_S \geq \gamma \displaystyle\sum_{i=1}^{N_r} \ln\left(1 + \frac{P_S\lambda_i^{be}}{N}\right) & \text{(18c)} \\ \displaystyle\sum_{i=1}^{N_r} \frac{1}{M/\lambda_i^{ba} + P_{max}} \geq C_a. & \text{(18d)} \end{cases}$$

Proof: Similarly to the proof of Lemma 1, if Eqs. (18a)-(18c) hold, by (9), we have

$$\begin{aligned} & u_e(P_{max}, 0) - u_e(P_{max}, 1) \\ =& \theta_E - \sum_{i=1}^{N} \ln\left(1 + \frac{P_{max}\lambda_i^{ea}}{M}\right) \geq 0. \end{aligned} \tag{19}$$

Similarly, $u_e(P_{max}, 0) \geq u_e(P_{max}, 2)$ and $u_e(P_{max}, 0) \geq u_e(P_{max}, 3)$, indicating that (11) holds. By (15) and (18d), we see that $\partial u_a(P, 0)/\partial P$ monotonically decreases with P, and thus

$$\frac{\partial u_a(P,0)}{\partial P} \geq \frac{\partial u_a(P,0)}{\partial P}|_{P=P_{max}} \geq 0, \ \forall 0 \leq P \leq P_{max}, \tag{20}$$

indicating that (10) holds for $(P_{max}, 0)$, which is an NE of the game. ■

As shown in Lemma 2, under low transmission costs $\big($i.e., (18d)$\big)$, or high attack costs $\big($i.e., (18a)-(18c)$\big)$, Alice chooses the maximum transmit power.

IV. MIMO Power Control in Dynamic Game

In dynamic radio environments Alice will have difficulty in accurately estimating the attack model and the radio channel information in a timely manner. As a widely-used reinforcement learning technique without assuming any probability model, Q-learning as reviewed in [19] can be used by Alice to derive the optimal power allocation strategy via trial-and-error in the dynamic secure MIMO transmission game, which consists of the repeated interactions between Alice and Eve.

As summarized in Algorithm 1, the Q-learning based power allocation is based on the system state which represents the state of the environment and the opponent. More specifically, at time n, Alice observes Eve's attack mode in the last slot q^{n-1} and uses it as the system state denoted by $s^n = q^{n-1}$, which serves as the basis of the decision making process. For simplicity, Alice quantizes the transmit power into $L+1$ levels and chooses the transmit power level $P \in \{lP_{max}/L\}_{0 \leq l \leq L}$.

The tradeoff during the learning process between exploitation and exploration has an important impact on the convergence of the algorithm. Therefore, the ε-greedy policy [17] is applied for Alice to choose the transmit power P^n based on the system state. Let $Q(s, P)$ denote the quality or Q function of Alice for system state s and action P, which is the expected discounted long-term reward of Alice. The value function $V(s)$ is the maximum of $Q(s, P)$ over Alice's possible actions. In each time slot, Alice updates both the Q function and the value function, as shown in Algorithm 1, in which the learning rate $\alpha \in (0, 1]$ represents the weight of the current experience in the learning process and $\delta \in [0, 1]$ is the discount factor indicating the uncertainty of Alice about the future gains. During the trials, Alice learns Eve's attack mode and chooses the transmit power to improve her long-term reward.

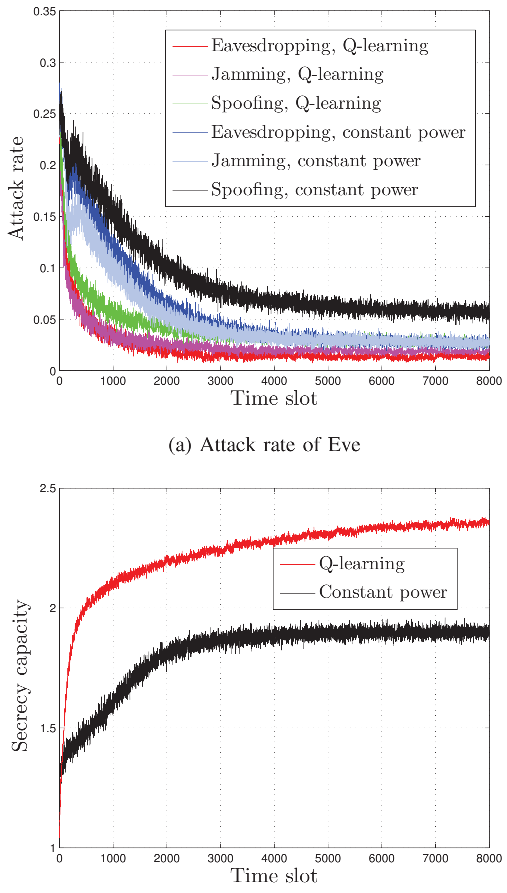
Algorithm 1 MIMO power allocation with Q-learning.

```
Initialize $q^0 = 0$, $Q(s, P) = 0$, $V(s) = 0$, $\forall s, P$.
for $n = 1, 2, 3, ...$ do
    Update the state $s^n = q^{n-1}$
    Choose $P^n$ using the $\varepsilon$-greedy policy
    Transmit with power $P^n$ over $M$ antennas
    Observe the attack type $q^n$ and $u_a$
    Update the Q function and value function:
    $Q(s^n, P^n) = (1 - \alpha)Q(s^n, P^n) + \alpha(u_a(s^n, P^n) + \delta V(s^{n+1}))$
    $V(s^n) = \max_{0 \leq P \leq P_{max}} Q(s^n, P)$
end for
```

V. Simulation Results

The performance of the secure MIMO transmission game algorithm was evaluated via simulations with $M = 5$, $N = N_r = 3$, $\sigma_{ba}^2 = 1.2$, $\sigma_{be}^2 = 2$, $\sigma_{ea}^2 = 0.5$, $\mathbf{\Theta} = [2.2, 3, 3.2]$, $P_J = 3$, $P_S = 3.2$, $C_a = 0.1$ and $\gamma = 0.5$. A constant transmit power system is used as a benchmark, in which Alice randomly chooses a transmit power level at the beginning of each game and sticks to it afterwards.

As shown in Fig. 2, the proposed power control scheme rapidly reduces the attack frequency of the smart attacker. For instance, as shown in Fig. 2 (a), the proposed scheme decreases the eavesdropping rate from 25% at the beginning of the game to 1.2% after 3000 time slots. The attack rate of a smart attacker can be suppressed faster by our proposed scheme compared with the benchmark strategy having constant transmit power. For example, the eavesdropping rate of the proposed scheme decreases to 5% over 500 time slots, while that of the benchmark strategy reaches 5% after 2500 time slots. Similarly, the jamming rate and spoofing rate decrease from 25% to 2% and 4%, respectively over 3000 time slots.



(a) Attack rate of Eve

(b) Secrecy capacity

Fig. 2. Performance in the dynamic secure transmission game for a 5 × 3 MIMO system with $\mathbf{\Theta} = [2.2, 3, 3.2]$, $C_a = 0.1$, and $N = 3$.

The jamming rate and spoofing rate of the proposed scheme decrease to 5% after 500 and 1300 time slots, respectively, which are 75% and 74% faster than the constant power strategy. The secrecy capacity increases by 110% over 500 time slots, which is 35% higher than the constant power strategy, as shown in Fig. 2 (b).

The average performance of the dynamic secure MIMO transmission game is presented in Fig. 3 with $\sigma_{ba}^2 = 9.5$, $\sigma_{be}^2 = 3.5$, $\sigma_{ea}^2 = 4$, $\mathbf{\Theta} = [7, 7.4, 7.2]$, $P_J = 7.4$, $P_S = 7.2$, and $N = 1$. The average secrecy capacity increases with the number of receive antennas, as shown in Fig. 3 (a). For instance, if Alice sends signals with equal power over 5 antennas, the average secrecy capacity increases about 6 times to 23 as the number of receive antennas changes from 1 to 5, which is 28% higher than that of the benchmark constant power allocation strategy. However, if Alice equally allocates transmit power over 7 antennas, the secrecy capacity slightly decreases to 22, because the average transmit power allocated at each antenna decreases with the number of receive antennas. As shown in Fig. 3 (b), the average eavesdropping rate decreases with the number of receive antennas at Bob, e.g., it decreases from 11.8% to 9%, as the number of receive antennas N_r changes from 1 to 5, if Alice sends signals over 5 antennas. Similarly, the average jamming and spoofing rates also decrease with the number of receive antennas, as shown in Fig. 3 (c) and (d). For instance, the jamming rate decreases from 12% to 8.8% and the spoofing rate decreases from 8.7% to 5%, as N_r changes from 1 to 5. Moreover, the eavesdropping and jamming rates decrease with the number of transmit antennas, e.g., as shown in Fig. 3 (b) and (c), it decreases to 8.6% and 8.5%, respectively, if Alice sends signals using 7 antennas.

VI. Conclusion

In this paper, we have formulated a secure MIMO transmission game, in which the transmitter chooses the transmit power over multiple antennas to improve the secrecy capacity and security gain, while the smart attacker selects its attack mode among eavesdropping, jamming, spoofing and no-attack. We have derived the NE of the secure MIMO transmission game, and shown that the attack motivation decreases with the number of transmit antennas. We have proposed a Q-learning based power control algorithm for MIMO transmission, which can improve the secrecy capacity and address smart attacks. Simulation results show that the eavesdropping, jamming and spoofing rates of the smart attacker against 5 × 3 MIMO transmission decrease from 25% to 1.2%, 2% and 4%, respectively after 3000 time slots in a dynamic game, which are 30%, 54% and 51% of that of the benchmark power allocation strategy.

References

[1] G. Foschini and M. Gans, “On limits of wireless communications in a fading environment when using multiple antennas,” *Wireless Personal Communications*, vol. 6, no. 3, pp. 311–335, 1998.

[2] Y. Tung, S. Han, D. Chen, and K. Shin, “Vulnerability and protection of channel state information in multiuser MIMO networks,” in *Proc. ACM SIGSAC Conf. Computer and Commun. Security*, Scottsdale, AZ, Nov. 2014, pp. 775–786.

[3] 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, no. 12, pp. 2578–2590, Dec. 2015.

[4] P. Baracca, N. Laurenti, and S. Tomasin, “Physical layer authentication over MIMO fading wiretap channels,” *IEEE Trans. Wireless Communications*, vol. 11, no. 7, pp. 2564–2573, May 2012.

[5] L. Xiao, T. Chen, G. Han, W. Zhuang, and L. Sun, “Game theoretic study on channel-based authentication in MIMO systems,” *IEEE Trans. Vehicular Technology*, Jan. 2017.

[6] Y. Zeng and R. Zhang, “Active eavesdropping via spoofing relay attack,” in *Proc. IEEE Int'l Conf. Acoustics, Speech and Signal Processing (ICASSP)*, Shanghai, Mar. 2016, pp. 2159–2163.

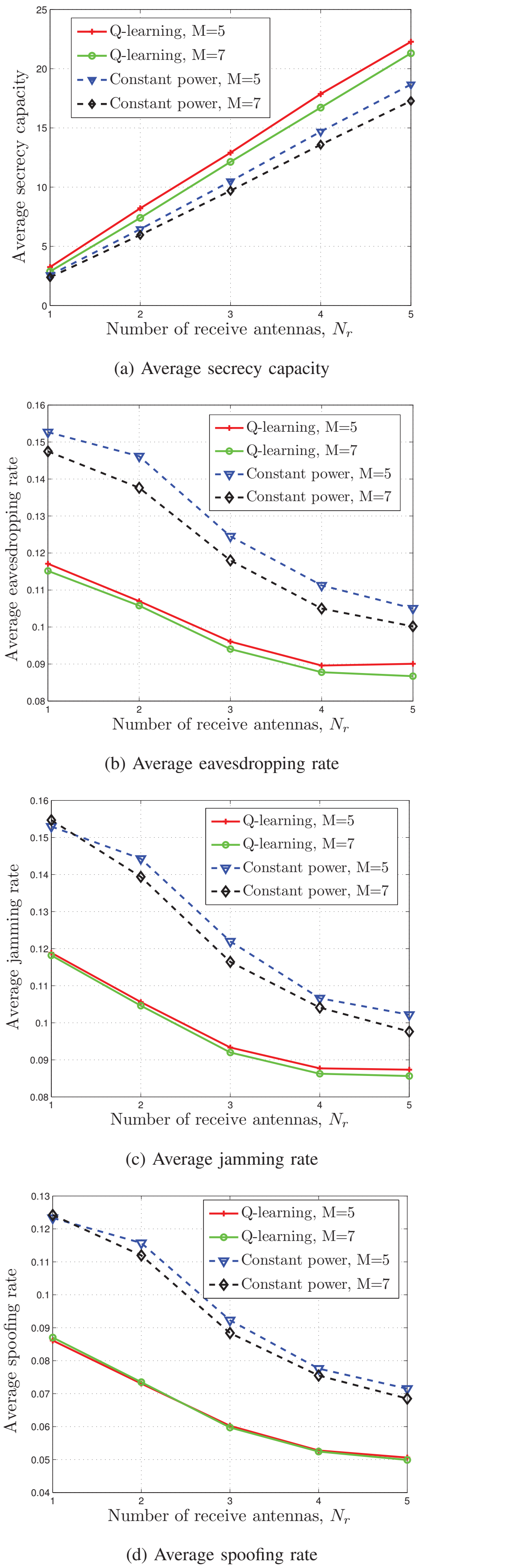
[7] D. Kapetanovic, G. Zheng, and F. Rusek, “Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks,” *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.

[8] A. Goldsmith, *Wireless Communications*, Cambridge Univ. Press, 2005.

[9] 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.*, San Jose, CA, Nov. 2010, pp. 1695–1700.

[10] X. He, H. Dai, P. Ning, and R. Dutta, “A stochastic multi-channel spectrum access game with incomplete information,” in *Proc. IEEE Int'l Conf. Commun.*, London, Jun. 2015, pp. 4799–4804.

[11] A. Garnaev, M. Baykal-Gursoy, and H. V. Poor, “Incorporating attack-type uncertainty into network protection,” *IEEE Trans. Information Forensics and Security*, vol. 9, no. 8, pp. 1278–1287, Aug. 2014.



(a) Average secrecy capacity

(b) Average eavesdropping rate

(c) Average jamming rate

(d) Average spoofing rate

Fig. 3. Average performance in the dynamic secure MIMO transmission game with $\mathbf{\Theta} = [7, 7.4, 7.2]$, $N = 1$ over 4000 time slots.

[12] L. Xiao, C. Xie, T. Chen, H. Dai, and H. V. Poor, “A mobile offloading game against smart attacks,” *IEEE Access*, vol. 4, pp. 2281–2291, May 2016.

[13] C. Xie and L. Xiao, “User-centric view of smart attacks in wireless networks,” in *Proc. IEEE Int’l Conf. Ubiquitous Wireless Broadband (ICUWB)*, Nanjing, Oct. 2016.

[14] 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. Wireless Communications*, vol. 15, no. 3, pp. 2155–2163, Mar. 2016.

[15] 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.*, Baltimore, MD, Nov. 2011, pp. 119–124.

[16] A. Mukherjee and A. L. Swindlehurst, “Jamming games in the MIMO wiretap channel with an active eavesdropper,” *IEEE Trans. Signal Process.*, vol. 61, no. 1, pp. 82–91, Jan. 2013.

[17] E. R. Gomes and R. Kowalczyk, “Dynamic analysis of multiagent Q-learning with ε-greedy exploration,” in *Proc. ACM Annual Int’l Conf. Machine Learning*, Montreal, Jun. 2009, pp. 369–376.

[18] A. Garnaev and W. Trappe, “The eavesdropping and jamming dilemma in multi-channel communications,” in *Proc. IEEE Int’l Conf. Commun.*, Budapest, Jun. 2013, pp. 2160–2164.

[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, no. 2, pp. 156–172, Mar. 2008.