Security Games with Incomplete Information

Kien C. Nguyen
Department of Electrical
and Computer Engineering
and the Coordinated Science Laboratory,
University of Illinois
Urbana-Champaign,
Email: knguyen4@illinois.edu

Tansu Alpcan
Deutsche Telekom Laboratories,
Ernst-Reuter-Platz 7,
D-10587 Berlin, Germany
Email: tansu.alpcan@telekom.de

Tamer Başar
Department of Electrical
and Computer Engineering
and the Coordinated Science Laboratory,
University of Illinois
Urbana-Champaign,
Email: basar1@illinois.edu

***Abstract*—We study two-player security games which can be viewed as sequences of nonzero-sum matrix games where at each stage of the iterations the players make imperfect observations of each other's previous actions. The players are the Attacker and the Defense System, who have at their disposal two possible actions each. For the former, the two actions are "attack" and "not to attack", and for the latter they are "defend" and "not to defend". The underlying decision process can be viewed as a fictitious play (FP) game, but what differentiates this class from the standard one is that the communication channels that carry action information from one player to the other, or the sensor systems, are error prone. Two possible scenarios are addressed in the paper: (i) the error probabilities associated with the sensor systems are known to the players, then our analysis provides guidelines for each player to reach the Nash equilibrium (NE), which is related to the NE of the underlying static game; (ii) the error probabilities are unknown to the players, in which case we study the effect of errors in the observations on the convergence to the NE and the final outcome of the game. We discuss both classical FP and stochastic FP, where for the latter the payoff function of each player includes an entropy term to randomize its own strategy, which can be interpreted as a way of concealing its true strategy.**

I. Introduction

Game theoretic approaches have recently been employed widely to solve security problems in computer and communication networks. In a security game between an Attacker and a Defense System, if we assume that the payoff matrices are known to both players, each player can compute the set of Nash equilibria of the game and play one of these strategies to maximize its expected gain (or minimize its expected loss). However, this assumption of knowing each other's payoff matrices is generally not valid in practice, and thus fictitious play can be used for players to learn its opponent's mixed strategy and compute the best response. In a FP game, each player observes all the actions and makes estimates of the mixed strategy of the opponent. At each stage, it updates this estimate and plays the pure strategy that is the best response (or generated based on the best response) to the current estimate of the other's mixed strategy. This is where we have to take into account the accuracy of the observations. Clearly, in practice, the sensor systems that report an attack (or an action of the Defense System, say, whether or not it is deploying security measures against attacks) are not perfect. There always exist a positive *miss probability* (false negative rate) and also a positive *false alarm probability* (false positive rate). It is these scenarios we want to address in this paper. By information incompleteness, we mean to signify both the lack of knowledge about each other's payoff matrix and the uncertainty of the observations on each other's actions.

Specifically, we examine a two-player game, where an Attacker (denoted as player 1 or P_1) and a Defense System (denoted as player 2 or P_2) take part in a discrete-time repeated nonzero-sum matrix game where each one has two possible actions: Attack (A) or not to attack (N) for the Attacker, and defend (D) or not to defend (N) for the Defense System. Players do not have access to each other's payoff function. They adjust their strategies based on each other's actions which they observe. The observations, however, are not accurate due to the imperfectness of the sensor system associated with each player, whose uncertainty is assumed to be independent from stage to stage. The setup of the game is shown in Figure 1. The binary channels that are used to model the sensor systems are asymmetric in general. Also, without much loss of generality, it is assumed that $0 \leq \alpha, \gamma, \epsilon, \mu < 0.5$.

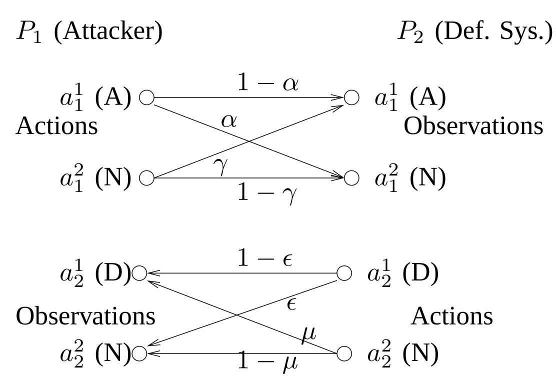

Fig. 1. Player observes the opponent's actions through binary channels with error probabilities α, γ, ϵ, and μ.

Security games have been examined extensively in a number of papers, see for example, [1], [2], [3], and [4]. A formulation of security games as static games can be found in [1]. In [3], the authors consider security games with imperfect observations and use the finite-state Markov chain framework to analyze the games. The work in [5] employs the framework of Bayesian games to address the intrusion detection problem in wireless ad hoc networks, where a mobile node viewed as a player confronts an opponent whose *type* is unknown. Literature on fictitious play can be found in [6], [7], [8], [9], and [10]. Also, a full version of this paper is available in [14].

Our contributions in this paper are as follows. First, we formulate security games with imperfect observations as fictitious play games. Second, we develop the convergence proof for a version of FP, where the players reverse the effects of observation errors based on their knowledge of error probabilities. We thus provide guidelines for the players to maximize their gain or minimize their loss in such games. Finally, we analyze deviations of their strategies from NE when the players ignore the observation errors, and thereafter provide a means to quantify the potential loss of the players due to the poor comprehension of their sensor systems.

In Section II, we introduce some background and notation adopted from [9], [10]. The analysis for both classical FP and stochastic FP are presented in Section III. In the following section, we state the FP algorithms for both the case where the error probabilities are known to the players and the case where they ignore the errors. After that, simulation results are given in Section V. Finally, some concluding remarks end the paper.

II. BACKGROUND

A. Static games

In this subsection, we present some concepts for static security games. Let a mixed strategy for player P_i be denoted by $p_i \in \Delta(2), i = 1, 2$, where we use $\Delta(2)$ to denote the simplex in $\Re^2$, i.e.,

$$\Delta(2) \equiv \left\{ s \in \Re^2 | s_1, s_2 \geq 0 \text{ and } s_1 + s_2 = 1 \right\}. \tag{1}$$

The utillity function of P_i, $U_i(p_i, p_{-i})$, is given by [1]

$$U_i(p_i, p_{-i}) = p_i^T M_i p_{-i} + \tau_i H(p_i), \tag{2}$$

where M_i is the payoff matrix of $P_i, i = 1, 2$; $H(p_i)$ is the entropy of the probability vector p_i. The weighted entropy $\tau_i H(p_i)$ with $\tau_i \geq 0$ is introduced to boost mixed strategies. In this paper, we do not take $\tau_1 = \tau_2$ as in [9], [10]. In a security game, τ_i represents how much player i wants to randomize its actions to conceal its true mixed strategy, and thus is not necessarily known to the other player. Also, for $\tau_1 = \tau_2 = 0$ (referred to as classical FP), the best response mapping can be set-valued, while it has a unique value when $\tau_i > 0$ (referred to as stochastic FP) [4] [10]. For a static game, each player selects an integer action a_i according to the mixed strategy p_i. The (instant) payoff for player P_i is $v_{a_i}^T M_i v_{a_{-i}} + \tau_i H(p_i)$, where we use $v_j, j = 1, 2$ to indicate the jth vertex of the simplex $\Delta(2)$. For a mixed strategy pair (p_1, p_2), the utility functions are given by the expected payoffs:

$$U_i(p_i, p_{-i}) = E\left[v_{a_i}^T M_i v_{a_{-i}}\right] + \tau_i H(p_i). \tag{3}$$

[1] As normally seen in game theory literature, the index $-i$ is used to indicate those of other players, or the opponent's in this case.

Now, the *best response* mappings $\beta_i : \Delta(2) \to \Delta(2)$ are defined as:

$$\beta_i(p_{-i}) = \arg \max_{p_i \in \Delta(2)} U_i(p_i, p_{-i}). \tag{4}$$

If $\tau_i > 0$, from (4), the best response is unique as mentioned earlier, and is given by the soft-max function:

$$\beta_i(p_{-i}) = \sigma\left(\frac{M_i p_{-i}}{\tau_i}\right), \tag{5}$$

where the soft-max function $\sigma : \Re^2 \to \text{Interior}(\Delta(2))$ is defined as

$$(\sigma(x))_j = \frac{e^{x_j}}{e^{x_1} + e^{x_2}}, j = 1, 2. \tag{6}$$

Note that $(\sigma(x))_j > 0$, thus the range of the soft-max function is just the interior of the simplex.

Finally, a (mixed strategy) Nash equilibrium is defined to be a pair $(p_1^*, p_2^*) \in \Delta(2) \times \Delta(2)$ such that for all $p_i \in \Delta(2)$

$$U_i(p_i, p_{-i}^*) \leq U_i(p_i^*, p_{-i}^*). \tag{7}$$

We can also write a Nash equilibrium (p_1^*, p_2^*) in the form of the best response mappings:

$$p_i^* = \beta_i(p_{-i}^*). \tag{8}$$

B. Discrete-time fictitious play

From the static game described in Subsection II-A, we define discrete-time FP as follows. Suppose that the game is repeated at times $k \in \{0, 1, 2, \ldots\}$. The empirical frequency $q_i(k)$ of player P_i is given by

$$q_i(k+1) = \frac{1}{k+1} \sum_{j=0}^{k} v_{a_i(j)} \tag{9}$$

Using induction, we can prove the following recursive relation:

$$q_i(k+1) = \frac{k}{k+1} q_i(k) + \frac{1}{k+1} v_{a_i(k)}. \tag{10}$$

C. Continuous-time fictitious play

From the equations of discrete-time FP (9), (10), the continuous-time version can be stated as follows ([9], [10], also see [13] for the derivation).

$$\begin{aligned} \dot{p}_1(t) &= \beta_1(p_2(t)) - p_1(t) \\ \dot{p}_2(t) &= \beta_2(p_1(t)) - p_2(t) \end{aligned} \tag{11}$$

III. ANALYSIS

A. Initial setup

Suppose that we are given a two-player two-action static game as in Fig. 1, where the payoff matrices of player 1 and player 2 are

$$M_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad M_2 = \begin{pmatrix} e & g \\ f & h \end{pmatrix}, \tag{12}$$

Based on a realistic security game, we can make the following assumptions:

- $a < c$: When the System defends, the payoff of the Attacker will be decreased if it attacks.

- $b > d$: When the System does not defend, the payoff of the Attacker will be increased if it attacks.
- $e > f$: When the Attacker attacks, the payoff of the System will be decreased if it does not defend.
- $g < h$: When the Attacker does not attack, the payoff of the System will be increased if it does not defend.

B. The case where the error probabilities are known to the players

We present in this subsection some analytical results for the case where the error probabilities associated with the sensor systems are known to the players.

Proposition 1: Consider the discrete-time two-player fictitious play with imperfect observations given in Figure 1. Let $e_\alpha, e_\gamma, e_\epsilon$, and e_μ be the empirical error frequencies of the observations corresponsing to the error probabilities α, γ, ϵ, and μ. It holds that

$$\lim_{k\to\infty} a.s.\ e_\alpha = \alpha; \lim_{k\to\infty} a.s.\ e_\gamma = \gamma;$$
$$\lim_{k\to\infty} a.s.\ e_\epsilon = \epsilon; \lim_{k\to\infty} a.s.\ e_\mu = \mu.$$

where we use *lim a.s.* to denote *almost sure convergence*.

Proof: Given that the binary channels are independent from stage to stage, this proposition can be proved using the strong law of large numbers. ■

Proposition 2: Consider a discrete-time two-player fictitious play with imperfect observations given in Figure 1. Let $\overline{p}_i$ be the observed frequency and p_i be the empirical frequency of player i, it holds that

$$\lim_{k\to\infty} a.s.\ \overline{p}_i = C_i p_i, i = 1, 2. \quad (13)$$

where $C_i, i = 1, 2$ are the channel matrices given by

$$C_1 = \begin{pmatrix} 1-\alpha & \gamma \\ \alpha & 1-\gamma \end{pmatrix}, \quad C_2 = \begin{pmatrix} 1-\epsilon & \mu \\ \epsilon & 1-\mu \end{pmatrix} \quad (14)$$

Proof: Writing the relationship between the observed frequencies and the empirical frequencies for a certain k and taking the limit as $k \to \infty$ yield the above results. For more details, see [14]. ■

Now suppose that the play order is P_1-P_2 and P_2 observes P_1's actions (with errors). In Table I, we have the expected payoffs of P_2 for pure strategies D and N, given the true empirical frequency of P_1, (p_1^1, p_1^2). In classical FP, P_2 just picks from this table the pure strategy that yields the better payoff (or randomize over two pure strategies with probability 0.5 each if they yield the same payoff). We call this the best response based on the empirical frequency. Now we look at the P_1-P_2 extensive form with imperfect observations plotted in Figure 2. In this graph, we model the imperfect observations as the *Nature play* [11]. Here the information sets [11] are the very observations of the System. While the System knows which information set it is in, it cannot distinguish between the two nodes in each information set: Given an observation, it cannot tell deterministically if there is an attack or not. Table II shows the payoffs of P_2 given a particular information set. Each entry of this table is the weighted average of the payoff

$P_2 \backslash P_1$	A w.p. p_1^1 and N w.p. p_1^2 $(p_1^1 + p_1^2 = 1)$
D	$ep_1^1 + gp_1^2$
N	$fp_1^1 + hp_1^2$

TABLE I
EXPECTED PAYOFFS OF P_2 FOR PURE STRATEGIES D AND N, GIVEN THE TRUE EMPIRICAL FREQUENCY OF P_1, (p_1^1, p_1^2).

$P_2 \backslash P_1$	$I(q_1^1)$	$II(q_1^2)$
D	$\frac{ep_1^1(1-\alpha)+gp_1^2\gamma}{p_1^1(1-\alpha)+p_1^2\gamma}$	$\frac{ep_1^1\alpha+gp_1^2(1-\gamma)}{p_1^1\alpha+p_1^2(1-\gamma)}$
N	$\frac{fp_1^1(1-\alpha)+hp_1^2\gamma}{p_1^1(1-\alpha)+p_1^2\gamma}$	$\frac{fp_1^1\alpha+hp_1^2(1-\gamma)}{p_1^1\alpha+p_1^2(1-\gamma)}$

TABLE II
PAYOFFS OF P_2 AT A GIVEN INFORMATION SET.

of P_2 given an information set and a pure strategy of this player. If at each step, the players use the distribution of the observations (instead of the true actions) of the opponent to pick its own pure strategy (action), this response will be called the best response based on the distribution of the information sets. We now state the following proposition.

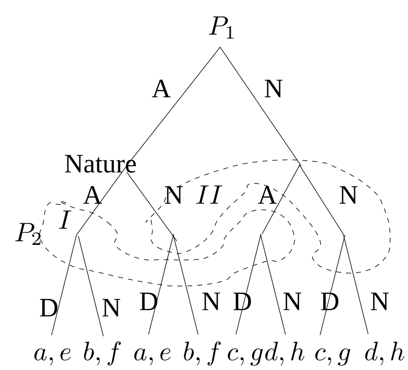

Fig. 2. P_1-P_2 extensive form with imperfect observation.

Proposition 3: If the error probabilities are known to the players, in each stage, the best response based on the distribution of the information sets is also the best response based on the empirical frequency.

Proof: See [14]. ■

Remark 1: Although the result given in this proposition is not surprising, it does pave the way for us to propose two FP algorithms, which will be presented in the next section, where the players simply compensate for the effects of the observation errors before playing the regular FPs.

Theorem 1: A classical non-zero-sum 2×2 fictitious play game where each player uses Algorithm IV-C converges to the Nash Equilibrium of the underlying static game.

Proof: Proposition 1 and the convergence proof for classical non-zero-sum 2×2 fictitious play [7] imply this theorem. Note that with the assumption $0 \le \alpha, \gamma, \epsilon,\ \mu < 0.5$, C_1 and C_2 are always invertible. ■

Remark 2: Although we have Algorithms IV-C and IV-D respectively for classical and stochastic discrete-time FP (which will be presented later in Section IV), Theorem 1 only states the convergence of the classical version. A convergence proof for the stochastic discrete-time FP, however, is as yet not available.

C. The case where players ignore the observation errors

Let $N = (1,1)^T$, we restate the following theorem from [9] for the general case where the coefficients of the entropy terms for the players (τ_1 and τ_2) are not necessarily equal (Cf. Equation (2)). This theorem in [9] is stated for $\tau_1 = \tau_2$, however, one can always scale the payoff matrices to get the general case.

Theorem 2: (A variant of Theorem 3.2 [9] for general $\tau_1, \tau_2 > 0$) Consider a two-player two-action fictitious play game with $(N^T \tilde{M}_1 N)(N^T \tilde{M}_2 N) \neq 0$, where $\tilde{M}_i$ are the payoff matrices of $P_i,\ i = 1, 2$. The solutions of continuous-time FP (11) satisfy

$$\lim_{t\to\infty} (p_1(t) - \beta_1(p_2(t))) = 0 \quad (15)$$

$$\lim_{t\to\infty} (p_2(t) - \beta_2(p_1(t))) = 0, \quad (16)$$

where $\beta_i(p_{-i}),\ i = 1, 2$, are given in (5).

Theorem 3: Consider a two-player two-action fictitious play game with imperfect observations where the binary channels are given in Figure 1 and Equation (14). Suppose that the players ignore the errors and play the stochastic FP given in II-C. If $(N^T M_1 C_2 N)(N^T M_2 C_1 N) \neq 0$, the solutions of continuous-time FP with imperfect observations (11) will satisfy

$$\lim_{t\to\infty} p_1(t) = \sigma\left(\frac{M_1 C_2 \lim_{t\to\infty} p_2(t)}{\tau_1}\right), \quad (17)$$

$$\lim_{t\to\infty} p_2(t) = \sigma\left(\frac{M_2 C_1 \lim_{t\to\infty} p_1(t)}{\tau_2}\right). \quad (18)$$

where $\beta_i(p_{-i}),\ i = 1, 2$, are given in (5), and $\sigma(.)$ is the soft-max function defined in (6).

Proof: Using the same procedure as in [13] to approximate the discrete-time FP with the continuous-time version. Consider a version of stochastic discrete-time FP where the recursive equations to update the empirical frequencies are given as

$$q_i(k+1) = \frac{k}{k+1} q_i(k) + \frac{1}{k+1} \beta_i(C_{-i} q_{-i}(k)), \quad (19)$$

where C_i are the channel matrices given in (14). Letting $\Delta = 1/k$, we can write (19) as

$$q_i(k+\Delta k) = \frac{k}{k+\Delta k} q_i(k) + \frac{\Delta k}{k+\Delta k} \beta_i(C_{-i} q_{-i}(k)). \quad (20)$$

Let $t = \log(k)$ and $\tilde{q}_i(t) = q_i(e^t)$, we then have, as $\Delta \to 0$,

$$q_i(k+\Delta k) \to q_i(e^{\log(k)+\Delta}) = \tilde{q}_i(t+\Delta).$$

Also, as $\Delta \to 0$, we have $\frac{k}{k+\Delta k} \to 1 - \Delta$ and $\frac{\Delta k}{k+\Delta k} \to \Delta$. Thus (20) can be rearranged to become

$$(\tilde{q}_i(t+\Delta) - \tilde{q}_i(t))/\Delta = \beta_i(C_{-i}\tilde{q}_{-i}(t)) - \tilde{q}_i(t). \quad (21)$$

Again, letting $\Delta \to 0$, and using q_i for $\tilde{q}_i$ to simplify the notation, we have that

$$\dot{q}_1(t) = \beta_1(C_2 q_2(t)) - q_1(t), \quad (22)$$

$$\dot{q}_2(t) = \beta_2(C_1 q_1(t)) - q_2(t). \quad (23)$$

Now, using Theorem 2 with $\tilde{M}_1 = M_1 C_2$ and $\tilde{M}_2 = M_2 C_1$, we have that

$$\lim_{t\to\infty} \left(p_1(t) - \sigma\left(\frac{M_1 C_2 p_2(t)}{\tau_1}\right)\right) = 0, \quad (24)$$

$$\lim_{t\to\infty} \left(p_2(t) - \sigma\left(\frac{M_2 C_1 p_1(t)}{\tau_2}\right)\right) = 0, \quad (25)$$

and thus Theorem 3 is proved. ■

Remark 3: Although the convergence of the continuous-time fictitious play with imperfect observations does not guarantee that of the discrete-time counterpart, this theorem does provide the necessary limit results for the discrete-time version. Comparing Equations (17) and (18) with Equations (5) and (8), we see that that the distorted observations (due to the channel matrices) will form a new NE, which in turn changes the payoffs of the players, which are still computed by (2).

IV. ALGORITHMS

We present in this subsection four algorithms for classical FP and stochastic FP. Algorithms IV-A and IV-B, which are derived from [6], [7], [9], and [10], are for the perfect observation case. Players also use these algorithms when they have no estimates of the error probabilities of their sensor systems and thus ignore the errors. Algorithms IV-C and IV-D, developped based on the analysis in Section III, are used for players who have estimates of the error probabilities and want to compensate for these.

A. Classical FP with perfect observations

In classical FP, at time k, player $i, i = 1, 2$, carries out the following steps:

1) Update the empirical frequency of the opponent using (10).
2) Pick the optimal pure strategy using Table I. If there are multiple optimal strategies, randomize over the optimal strategies with equal probabilities.

B. Stochastic FP with perfect observations

In stochastic FP, at time k, player $i, i = 1, 2$, carries out the following steps:

1) Update the empirical frequency of the opponent using (10).
2) Compute the best response using (5). (Note that the result is always a completely mixed strategy.)
3) Generate an action using the mixed strategy from step 2.

C. Classical FP with imperfect observations

At time k, player $i, i = 1, 2$, carries out the following steps:

1) Update the observed frequency of the opponent using (10).
2) Compute the estimated frequency using

$$p_{-i} = C_{-i}^{-1}\overline{p}_{-i}, i = 1, 2, \tag{26}$$

where $C_i, i = 1, 2$ are given by (14).
3) Pick the optimal strategy using Table I. If there are multiple optimal strategies, randomize over the optimal strategies with equal probabilities.

D. Stochastic FP with imperfect observations

At time k, player $i, i = 1, 2$, carries out the following steps:

1) Update the observed frequency of the opponent using (10).
2) Compute the estimated frequency using (26) and (14).
3) Compute the best response using (5). (Note that the result is always a completely mixed strategy.)
4) Generate an action using the mixed strategy from step 3.

V. SIMULATION RESULTS

We present in this section some simulation results for both classical and stochastic discrete-time FP (For more detailed simulation results, see [14]). The payoff matrices of player 1 and player 2 are chosen to be

$$M_1 = \begin{pmatrix} 1 & 5 \\ 3 & 2 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 4 & 1 \\ 3 & 5 \end{pmatrix}, \tag{27}$$

which satisfy the assumptions in III-A. The static game with simultaneous moves do not have a pure strategy NE. The mixed strategy NE is $(0.8,\ 0.2)$ and $(0.6,\ 0.4)$. The error probabilities of the binary channels are $\alpha = 0.1, \gamma = 0.05, \epsilon = 0.2$, and $\mu = 0.15$. The number of stages for the simulations of classical FP is $10,000$, while that of stochastic FP is $20,000$. We use $\tau_1 = 0.5$ and $\tau_2 = 0.3$ for the simulations of stochastic FP. The empirical frequencies of the players in classical FP are plotted in Figures 3, 4, and 5, and those in stochastic FP in Figures 6, 7, and 8. As can be seen from the graphs of classical FP, when the observations are perfect, the empirical frequencies converge to the mixed strategy NE (Figure 3).

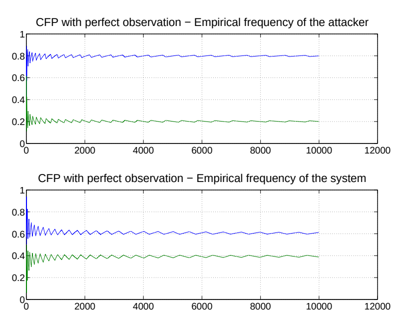

Fig. 3. Classical FP with perfect observations.

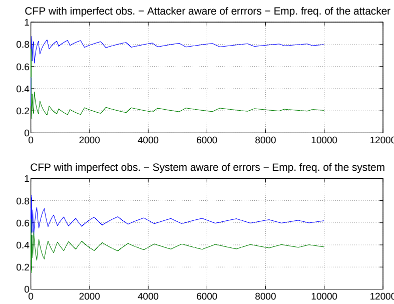

Fig. 4. Classical FP with imperfect observations where players are aware of the error probabilities.

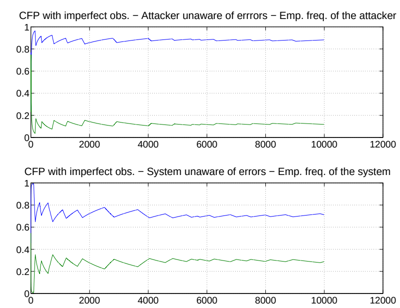

Fig. 5. Classical FP with imperfect observations where players are unaware of errors.

When the observations are erroneous and the players use Algorithm IV-C to fix the errors, the empirical frequencies exhibit larger fluctuations but still converge to the NE (Figure 4). Finally, if the observations are erroneous, but the error probabilities are unknown to the players, and they still use Algorithm IV-A, Figure 5 shows the deviation of the empirical frequencies from the original NE.

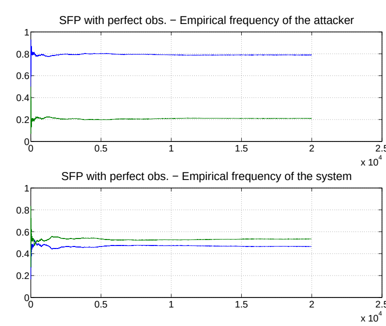

Fig. 6. Stochastic FP with perfect observation.

Regarding stochastic FP, Figure 6 shows the empirical frequencies of the players when the observations are perfect. The empirical frequencies approximately converge to $(0.79,\ 0.21)$ and $(0.47,\ 0.53)$. These are also the solutions of the best response mapping equations in (8). It can be noticed that the NE of the stochastic game is slightly more uniform than that of the classical version ($(0.79,\ 0.21)$ and $(0.47,\ 0.53)$

versus $(0.8,\ 0.2)$ and $(0.6,\ 0.4)$), due to the entropy terms in the payoff functions. When there are observation errors and the players use Algorithm IV-D to compensate for the errors, the empirical frequencies also approximately converge to $(0.79,\ 0.21)$ and $(0.47,\ 0.53)$ (Figure 7), which is the NE of the static game. Finally, if the players ignore the observation errors, their empirical frequencies approximately converge to $(0.86,\ 0.14)$ and $(0.42,\ 0.58)$, which is also the solutions of Equations (17) and (18). The simulations thus confirm the theoretical results derived in Section III and show that the counter-error algorithms presented in Section IV work properly.

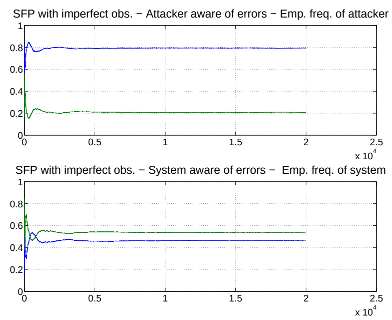

Fig. 7. Stochastic FP with imperfect observation where players are aware of the error probabilities.

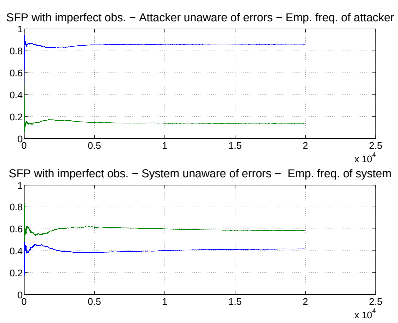

Fig. 8. Stochastic FP with imperfect observation where players are unaware of errors.

VI. Conclusion

In this paper, we have proposed some security game models that take into account each player's lack of knowledge of the opponent's motivations and the imperfectness of the observations reported by sensor systems. If each player has a good estimate of the error probabilities of its own sensor system, we provide the analysis and algorithms for it to reach the NE of the game, which is the point where it maximizes its gain or minimizes its loss against all possible strategies of the opponent. Otherwise, if each player does not know exactly the error rates and chooses to ignore the errors, our analysis allows one to estimate the deviation of the player's strategies from the NE, and thus examine its potential loss due to the poor grasp of its own sensor system. Our simulations have confirmed the analytical results and shown that the algorithms work properly.

Several more complex scenarios can be addressed. First, one can consider the case where one player knows the error probabilities of its sensor system and the other one does not. Second, players may have incorrect estimates of the error probabilities. In another direction, one might be interested in extending the action spaces of the players. For two-player zero-sum classical FP, the convergence proof was obtained for arbitrary numbers of actions for each player $(m \times n)$ [6], and therefore the analysis in this paper can be extended accordingly. For nonzero-sum games, the proofs for two-player FP have been found for the case where one player is restricted to 2 actions (See [8] for classical FP and [9] for stochastic FP). It is worth noting that there are counter examples (e.g., for 3×3 games) where FP does not converge to the mixed strategy NE [13]. Lastly, convergence of discrete-time stochastic fictitious play can also be examined.

Acknowledgement

This work was supported by Deutsche Telekom Laboratories and in part by the Vietnam Education Foundation (VEF). We are grateful to the anonymous reviewers for their valuable comments.

References

[1] T. Alpcan and T. Başar, "A Game Theoretic Approach to Decision and Analysis in Network Intrusion Detection", *Proceedings of the 42nd IEEE Conference on Decision and Control*, Hawaii, USA, 2003, pp. 2595–2600.
[2] T. Alpcan and T. Başar, "A game theoretic analysis of intrusion detection in access control systems," *Proceedings of the 43rd IEEE Conference on Decision and Control*, Paradise Island, Bahamas, 2004, pp. 1568–1573.
[3] T. Alpcan and T. Başar, "An intrusion detection game with limited observations," *Proceedings of the 12th Int. Symp. on Dynamic Games and Applications*, Sophia Antipolis, France, 2006.
[4] Z. Yin, "*Trust-based game-theoretic intrusion detection*," M.S. thesis, University of Illinois at Urbana-Champaign, 2006.
[5] Y. Liu, C. Comaniciu, and H. Man, "A Bayesian game approach for intrusion detection in wireless ad hoc networks," *Proceedings of the Workshop on Game Theory for Networks (GameNets)*, Pisa, Italy, 2006.
[6] J. Robinson, "An iterative method of solving a game," *Ann. Math.*, vol. 54, pp. 296-301, 1951.
[7] K. Miyasawa, "On the convergence of learning processes in a 2×2 nonzero-sum two person game," *Economic Research Program*, Princeton University, Princeton, NJ, Tech. Rep. 33, 1961.
[8] U. Berger, "Fictitious play in $2 \times n$ games," *Economics Working Paper Archive at WUSTL*. Available at: http://econpapers.repec.org/paper/wpawuwpga/0303009.htm
[9] J. S. Shamma and G. Arslan, "Unified convergence proofs of continuous-time fictitious play," *IEEE Transactions on Automatic Control*, Vol. 49, No.7, July 2004.
[10] J. S. Shamma and G. Arslan, "Dynamic fictitious play, dynamic gradient play, and distributed convergence to Nash equilibria," *IEEE Transactions on Automatic Control*, Vol. 50, No.3, March 2005.
[11] T. Başar and G. J. Olsder, *Dynamic Noncooperative Game Theory*, 2nd ed. Philadelphia, PA: SIAM, 1999.
[12] R. D. McKelvey, A. M. McLennan, and T. L. Turocy, *Gambit: Software Tools for Game Theory, Version 0.2007.01.30*, 2007. Available at http://gambit.sourceforge.net.
[13] A. Ozdaglar, "Lecture 11: Fictitious Play and Extensions," *Game Theory and Mechanism Design, MIT OpenCourseWare*. Available at http://ocw.mit.edu/OcwWeb/Electrical-Engineering-and-Computer-Science/6-972Spring-2005/CourseHome/index.htm.
[14] K. C. Nguyen, T. Alpcan, and T. Başar, "Security Games with Incomplete Information," *Technical Report*, UIUC, Sep. 2008. Available at http://decision.csl.uiuc.edu/˜knguyen4/research/research.html