Research Article
Evolutionary Game-Based Secrecy Rate Adaptation in Wireless Sensor Networks

Guanxiong Jiang, 1 Shigen Shen, 1,2 Keli Hu, 1 Longjun Huang, 1,3
Hongjie Li, 2 and Risheng Han 2

1Department of Computer Science and Engineering, Shaoxing University, Shaoxing 312000, China
2College of Mathematics, Physics and Information Engineering, Jiaxing University, Jiaxing 314001, China
3College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou 310014, China

Correspondence should be addressed to Guanxiong Jiang; cnjgx@163.com

Received 22 December 2014; Revised 26 February 2015; Accepted 4 March 2015

Academic Editor: Chuan-Ming Liu

Copyright © 2015 Guanxiong Jiang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Physical layer security, whose aim is to maximize the secrecy rate of a source while keeping eavesdroppers ignorant of data transmitted, is extremely suitable for Wireless Sensor Networks (WSNs). We therefore, by developing the classical wire-tap channel, construct an approach to compute the secrecy rate between a sensor node and its responsible cluster head in the clustered WSNs. A noncooperative secrecy rate game towards WSNs is formulated to solve contradictions between maximizing the secrecy rate of a sensor node and minimizing power consumed for data transmission. Using evolutionary game theory, we set up a selection dynamics upon which a power level can be adaptively selected by a sensor node. Thus, the objective of secrecy rate adaptation for maximizing the fitness of member sensor nodes is achieved. We also prove the game is stable; that is, there exist evolutionarily stable strategies (ESSs) that explain which strategies will be selected by a sensor node in the end. Moreover, a corresponding algorithm of secrecy rate adaptation is given. Numerical experiments show our proposed approach can adaptively adjust the secrecy rate of a sensor node, which provides a novel way to guarantee the confidentiality of WSNs.

1. Introduction

Providing security for Wireless Sensor Networks (WSNs) is challenging, due to the characteristics of wireless communications, limited resources of sensor nodes, dense and enormous networks, as well as the unattended environments where sensor nodes are prone to physical attacks. A large number of security approaches [1] such as cryptography, attack detection, and secure routing have been proposed to defend various threats and vulnerabilities in WSNs. Different to these traditional methods, physical layer (PHY) security [2, 3] using the physical properties of the radio channel to help provide secure wireless communications is currently attracting considerable attention. This approach is extremely suitable for WSNs since it achieves security through taking advantage of the fundamental ability of the physical layer, not adding extra components.

The main idea of PHY security is to maximize the rate of reliable information from a source to a destination, while keeping eavesdroppers ignorant of data transmitted. This rate is referred to as secrecy rate and its maximum reliable value for a channel is known as secrecy capacity. Wyner [4] in his pioneering work introduced a wire-tap channel and showed that perfect secrecy could be attained even without the application of shared secrets. Since its inception, secrecy capacity has been fundamentally developed in other channels including Gaussian wire-tap channel [5], broadcast channel [6], relay channel [7], multiple-access channel [8], interference channel [9], multiple-input single-output (MISO) channel [10], multiple-input multiple-output (MIMO) channel [11], and feedback channel [12].

Along with the foundation of secrecy capacity in various channels, a recent trend of long-standing interest has emerged in how to improve PHY security under the same
surroundings. These include methods such as cooperation relays [13], joint relay and jammer selection [14], channel frequency selectivity [15], and game theory [16–26]. In practice, during the process of transmitting data, the transmission power is a key factor that influences the secrecy rate of a source. From a noncooperative perspective, each sensor node, due to its selfishness, attempts to increase its transmission power for maximizing its secrecy rate in response to actions of the other sensor nodes. In this manner, it will however cause more and more interference to the other nodes and consume its own energy extraordinarily. These interactions among sensor nodes naturally result in applications of game theory.

As an efficient method to solve problems of optimal strategies, game theory provides a rich set of mathematical tools for investigating the multiperson strategic decision-making, which has been broadly employed in WSNs security [27–33]. It is generally assumed that players in the classical game theory have complete information about the game and about behaviors of opponents and must act completely rationally. Distinguishable to these assumptions, evolutionary game theory (EGT) to be borrowed in this paper imagines that conditioned players who are randomly drawn from a large population play the game repeatedly. Moreover, over time players have the opportunity to optimize their individual utilities by reacting to simple observations from their opponents. This nature satisfies the requirement for the current large-scale wireless networks with characteristics of self-organization, self-configuration, and self-optimization. Thus, many researchers are currently engaged in developing EGT based schemes [34, 35]. Typical examples exist in evaluating an incentive protocol [36], adjusting multiple-access control and power control [37], maximizing TCP throughout [38], learning for an optimal strategy [39], coevolving rational strategies [40], implementing network selection [41], sensing the spectrum collaboratively [42], selecting dynamic service [43], enforcing cooperation among network nodes [44], promoting the selfish nodes to cooperate with each other [45], and so forth.

Up to now, there are some papers on combining secrecy capacity with game theory in different environments. The work in [19] formulates a noncooperative game between a source and a relay to achieve the optimal secrecy rate of the source. Also, a noncooperative game between wireless users and a malicious node is introduced in [20], where the wireless users, through choosing a relay station, are to maximize a utility function considering their mutual interference and security of the chosen path whereas the malicious node is to reduce the overall network’s secrecy capacity. From the perspective of information theory, the work in [22] provides a mathematical formulation for the noncooperative zero-sum game existed in the two-user MISO Gaussian interference channel with confidential messages. In [23] the authors model a two-person zero-sum game with the ergodic MIMO secrecy rate as the payoff function, in order to examine the trade-offs for the legitimate transmitter and the adversary. Since cooperation, on the contrary, is capable of improving PHY security, the work in [21] introduces friendly jammers to interfere with the eavesdropper to increase the secrecy rate of a source. A Stackelberg game is investigated to reflect interactions between the source that pays jammers for their interference and jammers who charge the source with a certain price for the jamming. Different from [21], a Stackelberg game [18] between primary users and secondary users in cognitive radio networks is modeled to maximize transmission rates of secondary users. Consequently, primary users’ secrecy rates are improved with the help of trustworthy secondary users. Besides, typical examples of the Stackelberg game exist in analyzing the cooperation between the primary and secondary transmitters in cognitive radio channels [24] and formulating the sources and the friendly jammers in a two-way relay system as a power control scheme to achieve the optimized secrecy rate of the sources [25]. Moreover, a nontransferable coalitional game [17], as one of cooperative games, is applied to achieve secrecy rate gains from cooperation in the presence of a cost for information exchange. The work in [26] formulates the relay selection in a two-stage decode-and-forward cooperative network as a coalitional game with transferable utility, which decreases the computation complexity in solving the distributed relay selection problem. In addition, the cooperative Kalai-Smorodinsky bargaining game [16] is adopted, for transmitters with the MIMO channel, to find an operating point that balances network performance and fairness. This point allows transmitters to adjust their precoders appropriately and thus improves the overall secrecy capacity of the network.

To the best of our knowledge, this paper is the first work to focus on exploring secrecy rate adaptation in WSNs with the idea of EGT. We first extend the classical secrecy rate equation to fit for the WSNs. We are thus able to understand what parameters will influence the secrecy rate in WSNs. Then, we solve the decision-making problem among sensor nodes for maximizing their utilities through a noncooperative secrecy rate game. The replicator dynamics is applied to illustrate the evolution process how sensor nodes select adaptively their power level strategies and achieve their adaptation of secrecy rate.

Compared with the related works mentioned herein, there are some distinctions in this paper. We concentrate clearly on the secrecy rate between a sensor node and its responsible cluster head in the clustered WSNs, while many other channels are considered in [4–12, 46–48]. We employ EGT to disclose the dynamics of secrecy rate adaptation for sensor nodes, while EGT is applied to other fields [34, 36–44, 49]. Our eventual objective is to maximize the fitness of sensor nodes while several current works [16–21] make use of various games to improve PHY security for different surroundings. Therefore, our contributions lie mainly in the following aspects:

(1) considering the interference environment, we construct an approach to compute the secrecy rate between a sensor node and its responsible cluster head by developing the classical wire-tap channel [4, 5], which is suitable for the clustered WSNs;

(2) we formulate a noncooperative secrecy rate game towards WSNs, which is able to reflect interactions among sensor nodes and the cost of energy consumed
for transmitting data. Solving the game will help sensor nodes, by maximizing their utilities, to select their power level strategies correctly.

(3) we attain, from the view of EGT, a selection dynamics that promotes sensor nodes to seek a power level strategy with higher fitness, as well as ESSs for the game to describe which power level strategies will be adopted by mutants in the end. The secrecy rate adaptation for sensor nodes is thus achieved.

The rest of this paper is organized as follows. In Section 2, we discuss the network surroundings to be studied and compute the secrecy rate between a sensor node and its responsible cluster head in the clustered WSNs. In Section 3, a noncooperative secrecy rate game towards WSNs is set up. Moreover, secrecy rate dynamics and ESSs for the game are explored. In addition, an algorithm is introduced to describe how to adjust adaptively secrecy rate of sensor nodes. In Section 4, by performing numerical experiments in an example of the secrecy rate game, we illustrate the influence of a cost parameter, as well as the corresponding ESSs. Moreover, the process of secrecy rate adaptation for sensor nodes is disclosed. Finally, a conclusion is provided in Section 5.

2. System Model

2.1. Interference among Sensor Nodes. Multiple-access channels based WSNs are under consideration in this paper. It is well known that multiaccess interference is a significant factor to reduce the performance of such networks. Lack of coordination among sensor nodes will lead to a great number of interfering power from their neighbors, even if each sensor node transmits signals at the lowest required power to its destination.

To attain the number of interferers for a particular sensor node, we use the assumptions as follows. We assume the WSNs are composed of static and identical sensor nodes that are uniformly scattered with node density \( \rho \) on a 2D grid. Each of sensor nodes is equipped with an omnidirectional transmitting and receiving antenna of the same gain and are uniformly scattered with node density \( \rho \). Moreover, the process of secrecy rate adaptation for sensor nodes is disclosed. Finally, a conclusion is provided in Section 5.

Let \( \mathcal{S} \), \( \mathcal{K} \), and \( \mathcal{E} \) be sets of \( M \) member sensor nodes, \( N \) cluster nodes, and \( K \) eavesdroppers, respectively. Thus, \( \mathcal{S} = \{ S_1, S_2, \ldots, S_M \} \), \( \mathcal{K} = \{ H_1, H_2, \ldots, H_N \} \), and \( \mathcal{E} = \{ E_1, E_2, \ldots, E_K \} \). For any member sensor node \( S_m \), \( S_m \in \mathcal{S} \), there exists a uniquely responsible cluster head \( H_n \), \( H_n \in \mathcal{K} \), where \( n \) is in fact determined by \( m \); there also exist several eavesdroppers, each of which is denoted by \( E_k \), \( E_k \in \mathcal{E}_m \), \( \mathcal{E}_m \subseteq \mathcal{E} \), where \( \mathcal{E}_m \) is the set of eavesdroppers capable of listening in on data sensed by \( S_m \). Channel gains from \( S_m \) to \( H_n \) and \( E_k \) are denoted by \( G_{H_n}^{S_m} \) and \( G_{E_k}^{S_m} \), respectively. For simplicity, all thermal noise powers at cluster heads and eavesdroppers are denoted by \( \eta^T \). In addition, each channel bandwidth is \( W \).

\[
I = \rho z_I + 3 \sqrt{\rho \varepsilon_I}.
\]
Due to the broadcast nature of channels, a cluster head endures a collision of signals from some member sensor nodes that are transmitting their data simultaneously. We treat these signals from member sensor nodes other than the target source as additive interference and compute the number of these interferers according to (1). For any member sensor node $S_m$, $S_m \in \mathcal{S}$, let $\delta_m$ be the set of its interferers whose element is denoted by $S_i^m, i \in \{1,2,\ldots, I_m\}$, where $I_m$ denoting the number of interferers of $S_m$ comes from (1). Thus, $\delta_m = \{S_1^m, S_2^m, \ldots, S_{I_m}^m\}$. Following the idea of the classical wire-tap channel [4, 5], the channel capacity from member sensor node $S_m$ to its corresponding cluster head $H_n$, denoted by $C_{H_n}^{S_m}$, can be given by

$$C_{H_n}^{S_m} = W \log_2 \left( 1 + \frac{P_m G_{H_n}^{S_m}}{\sum_{i=1}^{I_m} P_i^m G_{i}^{S_m} + \eta^2} \right),$$

where $P_m$ is the transmission power adopted by $S_m$, $S_m \in \mathcal{S}$, $\overline{P}_i^m$ is the interference power adopted by $S_i^m, S_i^m \in \delta_m$, and $G_{H_n}^{S_m}$ is the channel gain between interferer $S_i^m$ and the interfered cluster head $H_n$.

Similarly, the channel capacity from member sensor node $S_m$ to eavesdropper $E_k$, $E_k \in \mathcal{E}_m$, denoted by $C_{E_k}^{S_m}$, can be given by

$$C_{E_k}^{S_m} = W \log_2 \left( 1 + \frac{P_m G_{E_k}^{S_m}}{\sum_{i=1}^{I_m} P_i^m G_E^{S_m} + \eta^2} \right),$$

where $G_{E_k}^{S_m}$ is the channel gain between interferer $S_i^m$ and eavesdropper $E_k$, $E_k \in \mathcal{E}_m$. The secrecy rate between member sensor node $S_m$ and its responsible cluster head $H_n$, thus, can be defined as (in fact, this scenario can be regarded as $I_m$-user interference channel with $|\mathcal{E}_m|$ external eavesdroppers, where $|\mathcal{E}_m|$ is the number of eavesdroppers who are able to listen in data sensed by $S_m$)

$$C_e(P_m) = \left( C_{H_n}^{S_m} - \max_{E_k \in \mathcal{E}_m} C_{E_k}^{S_m} \right)^+, \quad (4)$$

where $(x)^+ = \max\{x,0\}$.

3. Joint Secrecy Rate and EGT

3.1. A Compendium of EGT. Briefly, EGT is mainly concerned about a dynamic environment where players are continually interacting with others and adapting their strategies based on their expected payoffs they attain. In EGT, the concept of population consisting of a group of individuals (i.e., players) is introduced, and expected payoffs are replaced by fitness of individuals. An individual in an evolutionary game is able to observe the actions of other individuals, learn from these observations, and slowly adjust its strategy to attain the solution in the end. In this manner, we are able to understand the dynamics of interactions among individuals in a population.

In fact, the evolutionary process is determined by two noticeable elements: a mutation mechanism to provide mutants and a selection mechanism to promote some mutants with higher fitness over others [52]. While the mutation mechanism is described by evolutionary stable strategy (ESS), the selection mechanism is highlighted by replicator dynamics. The concept of ESS is to require that the final equilibrium must be capable of repelling all invaders; that is, if a strategy is evolutionarily stable, then it must keep such a quality that almost all individuals in the same population follow this strategy and mutants hardly invade successfully. This ESS is in fact a refinement of Nash equilibrium. On the other hand, the replicator dynamics is able to explain and predict the changeable trend towards population shares associated with different pure or mixed strategies. It selects individuals in a fitness proportional fashion. Thus, subpopulations with better fitness than the average will grow, while those with worse fitness than the average will be reduced in their numbers.

3.2. Secrecy Rate Game towards WSNs

Definition 1. The secrecy rate game towards WSNs that is symmetric consists of a 3-tuple $G = (\mathcal{S}, \mathcal{P}, \mathcal{U})$, where

(i) $\mathcal{S} = \{S_1, S_2, \ldots, S_M\}$ is a set of member sensor nodes (individuals) in the same WSNs;

(ii) $\mathcal{P} = \{P_{m} \in \mathcal{P}_m | \ P_{m} \in \mathcal{P}_m, m \in \{1,2,\ldots,M\}\}$ is a set of strategy profiles for all member sensor nodes, where $\mathcal{P}_m = \{P_m \ | \ P_m^m, P_m^2, \ldots, P_m^L\}, m \in \{1,2,\ldots,M\}$. Here $\mathcal{P}_m$ and $L$, respectively, are the set and number of pure power level strategies available to member sensor node $S_m$, $S_m \in \mathcal{S}$;

(iii) $\mathcal{U} = \{\mu(P_m, P_{\bar{m}}) | \ P_{m} \in \mathcal{P}_m, \ P_{\bar{m}} \in \mathcal{P}_{\bar{m}}, m, \bar{m} \in \{1,2,\ldots,M\}\}$ is a set of utility attained by member sensor node $S_m$ adopting power level strategy $P_m$ when its opponent adopting $P_{\bar{m}}$.

In the secrecy rate game towards WSNs, we consider all member sensor nodes form a population and regard them as individuals. These individuals are intelligent agents who, during interactions with others, are able to self-adjust their strategies according to their current fitness. Their objectives are to adapt their secrecy rates by maximizing individual fitness.

Due to the interference among sensor nodes, an optimal power must be allocated to all member sensor nodes. From (4), the secrecy rate of member sensor node $S_m$ may be maximized if $S_m$ transmits its data at its full power. The member sensor node $S_m$ may thus be in more interference to its neighboring sensor nodes and will also conserve its own battery largely. The performance of the WSNs will thus be reduced. Therefore, to meet these interactions, we introduce the utility function for member sensor node $S_m$ as

$$\mu(P_m, P_{\bar{m}}) = C(P_m) - \alpha P_m, \quad (5)$$

where $C(P_m)$ is from (4), and $\alpha$ is a cost parameter that reflects the degree of a member sensor node consuming
energy for data transmission. Note that the member sensor node adopting $p_m$ has been included as one of interferers in the first term of (5). Next, the goal of the secrecy rate game is to help all individuals select their strategies adaptively so that the maximum fitness of member sensor nodes can be attained with the minimum expense of their power. Thus, secrecy rate adaptation of a member sensor node, along with this evolutionary process, is to be achieved.

3.3. Dynamics Analysis on Secrecy Rates of Member Sensor Nodes. We now explore the secrecy rate dynamics of member sensor nodes using the replicator dynamics. To begin with, all member sensor nodes, for transmitting data, select randomly one of available power levels. Each member sensor node, from the view of noncooperative game theory, expects to maximize its own fitness. It therefore adjusts periodically its power level (i.e., its secrecy rate is adjusted) to a new one; otherwise, it keeps its current WSNs. If a higher value is attained, the member sensor node changing its current power level (i.e., its current secrecy rate is changed) to a new one; otherwise, it keeps its current strategy unchanged. Letting $\theta_j(t)$ (note that here, $\forall m, 0 < m \leq M$, we assume $\Psi_m = \Psi_m$, which is rational due to the same characteristic of all member sensor nodes. This assumption means all member sensor nodes have the same set of power level strategies; i.e., $\forall m, 0 < m \leq M$, $j \in \{1, 2, \ldots, M\}$, $P^m_j = P^\ast_j$ is satisfied, where $P^m_j$ and $P^\ast_j$ denote member sensor nodes $S_m$ and $S_\ast$ adopting the same power level strategy $j$ be the fraction of member sensor nodes using power level strategy $j$ at time $t$, we have

$$\sum_{j \in \Psi_m} \theta_j(t) = 1.$$  \(\text{(6)}\)

The state of the WSNs at time $t$, denoted by $\theta(t)$, is then $\theta(t) = [\theta_{m_1}(t), \theta_{m_2}(t), \ldots, \theta_{m_L}(t)]$ that can be considered as a mixed strategy of the WSNs. Let $I$ be the power level strategy adopted by the opponent $S_\ast$. Thus, referring to [53], the fitness of member sensor node $S_m$, adopting power level strategy $j$ at time $t$ is

$$\mu_j(t) = \sum_{l \in \Psi_m} \theta_l(t) \mu_j(l),$$  \(\text{(7)}\)

where $\mu_j(l)$ is from (5). The average fitness of the whole WSNs at time $t$ is

$$\overline{\mu}(t) = \sum_{j \in \Psi_m} \theta_j(t) \mu_j(t).$$  \(\text{(8)}\)

Correspondingly, we define the expected secrecy rate of member sensor node $S_m$ adopting power level strategy $j$ at time $t$ as

$$\zeta_j(t) = \sum_{l \in \Psi_m} \theta_l(t) C_j(l).$$  \(\text{(9)}\)

where $C_j(l)$ is from (4). The average secrecy rate of the whole WSNs at time $t$ is defined as

$$\overline{\zeta}(t) = \sum_{j \in \Psi_m} \theta_j(t) \zeta_j(t).$$  \(\text{(10)}\)

To make use of the replicator dynamics, we require the rate at which member sensor nodes change their strategies. This rate is determined by the performance of current strategies of member sensor nodes and by the population state. Let $\rho_j(t)$ be the average review rate of member sensor nodes using power level strategy $j$. $p^j_q(t)$ (in particular, $p^j_q(t)$ is the probability that the reviewing member sensor nodes adopting power level strategy $j$ do not change their strategy) be the probability that the reviewing member sensor nodes change from power level strategy $j$ to $q$. Thus, in the whole WSNs the fraction of the reviewing member sensor nodes changing from power level strategy $j$ to $q$ is $\theta_j(t) \rho_j(t) p^j_q(t)$. As a result, the outflow from the power level strategy $j$ is

$$\sum_{q \neq j} \theta_j(t) \rho_j(t) p^j_q(t) = \theta_j(t) \rho_j(t) \sum_{q \neq j} p^j_q(t)$$

$$= \theta_j(t) \rho_j(t) \left(1 - p^j_q(t)\right),$$  \(\text{(11)}\)

while the inflow to the power level strategy $j$ is $\sum_{q \neq j} \theta_q(t) \rho_q(t) p^q_j(t)$. Subtracting the outflow from the inflow, we can then attain the differential equation as

$$\dot{\theta}_j(t) = \sum_{q \neq j} \theta_q(t) \rho_q(t) p^q_j(t) - \theta_j(t) \rho_j(t) \left(1 - p^j_q(t)\right)$$

$$= \sum_{q} \theta_q(t) \rho_q(t) p^q_j(t) - \theta_j(t) \rho_j(t),$$  \(\text{(12)}\)

which constructs the replicator dynamics determining which power level strategies will be adaptively selected by a member sensor node.

For a member sensor node, whether or not to switch its power level is based on the corresponding fitness. Among the notations above, we suppose that $j$ and $q$ denote the power level strategies adopted by the original individuals and a small group of mutants, respectively. Then, the reviewing member sensor nodes change to the mutant strategy if and only if the fitness difference observed is positive; that is, $\mu_q(t) - \mu_j(t)$. This difference between random variables $\mu_q(t)$ and $\mu_j(t)$ has a continuously differentiable probability distribution function $\phi : \mathbb{R} \rightarrow [0, 1]$. The conditional probability that member sensor nodes will change to power level strategy $q$, given that its original strategy is $j$, is thus $\phi(\mu_q(t) - \mu_j(t))$. Furthermore, since the probability that member sensor nodes will select power level strategy $q$ at time $t$ is $\theta_q(t)$, we can attain the resulting conditional choice probability as

$$p^j_q(t) = \begin{cases} \theta_q(t) \phi(\mu_q(t) - \mu_j(t)), & \text{if } q \neq j, \\ 1 - \sum_{q \neq j} \theta_q(t) \phi(\mu_q(t) - \mu_j(t)), & \text{if } q = j. \end{cases}$$  \(\text{(13)}\)

In fact, the choice probabilities in (13) result from individual differences in preferences across member sensor nodes and not from observation errors made by member sensor nodes.
nodes with identical preferences. To isolate the effect of choice probabilities, for simplicity, we assume that all review rates are constantly equal to one; that is,
\[ \forall j \in \mathcal{P}_m, \quad r_j (\theta) = 1. \] (14)
Substituting (13) and (14) into (12), we can, for member sensor nodes, get the selection dynamics as
\[ \dot{\theta}_j (t) = \theta_j (t) \sum_{q \neq j} \theta_q (t) \cdot (\phi (\mu_j (t) - \mu_q (t)) - \phi (\mu_q (t) - \mu_j (t))). \] (15)

This selection dynamics, determining the selection probability of a power level strategy, will be used to adapt the decision of a member sensor node and is at the same time affected by decisions of the other member sensor nodes.

3.4. Convergence and Stability Analysis on Secrecy Rate Game towards WSNs

**Lemma 2.** If a power level strategy \( j \) is strictly dominant, then \( \lim_{t \to \infty} \theta_j (t) = 1 \).

**Proof.** The case that a power level strategy is strictly dominant means member sensor nodes with this strategy, irrespective of which strategy any of other member sensor nodes chooses, can gain a strictly higher fitness than with any of other strategies. This will result in increasing the corresponding fraction in the population. Member sensor nodes employing a strictly dominant strategy will then occupy the whole population over time. Lemma 2 therefore follows. \( \square \)

From Lemma 2, we can attain that member sensor nodes whose strategies are strictly dominated will vanish eventually from the population; that is, if a power level strategy \( j \) is strictly dominated, then \( \lim_{t \to \infty} \theta_j (t) = 0 \).

**Theorem 3.** The WSNs population state \( \theta (t) \) converges to equilibrium.

**Proof.** It is obvious that member sensor nodes employing different power level strategies will attain different fitness under the same WSNs surroundings. This fact means only one power level strategy, correspondingly, is endowed with the highest fitness among all strategies. Ranking all fitness values in descending order, we express the relationship of these fitness as \( \mu_1 (t) > \mu_2 (t) > \cdots > \mu_L (t) \), and let \( \lim_{t \to \infty} \theta (t) = [\theta_1 (t), \theta_2 (t), \ldots, \theta_L (t)] \) be the corresponding population state. According to Lemma 2 the WSNs population state, subject to the constraints \( \theta_j (t) \geq 0 \) and \( \sum_{j \in \mathcal{P}_m} \theta_j (t) = 1 \), will ultimately converge to
\[ \lim_{t \to \infty} \theta (t) = [\theta_1 (t), \theta_2 (t), \ldots, \theta_L (t)] = [1, 0, \ldots, 0] \] (16)
as equilibrium. Theorem 3 therefore follows. \( \square \)

**Theorem 4.** The equilibrium of the secrecy rate game towards WSNs is evolutionarily stable.

**Proof.** Following Theorem 3, we can, for the secrecy rate game towards WSNs, attain equilibrium as \([1, 0, \ldots, 0]\) of \( L \)-dimension. At this equilibrium point the set of differential equations denoted in (15), by substituting
\[ \theta_j (t) = 1 - \theta_2 (t) - \cdots - \theta_L (t), \] (17)
can be changed into
\[ \dot{\theta}_j (t) = \theta_j (t) \left( \varphi_{j1} (1 - \theta_j (t)) + \sum_{i=\mathcal{P}_m \setminus \{j\}} \varphi_{ji} \theta_i (t) \right), \] (18)
where \( \varphi_{ji} \) is equal to \( \phi (\mu_j (t) - \mu_i (t)) - \phi (\mu_i (t) - \mu_j (t)) \), and
\[ \vartheta (t) = [\theta_2 (t), \theta_3 (t), \ldots, \theta_L (t)] \] (19)
denotes the corresponding downsized population state, which has equilibrium as \( \vartheta^* (t) = [0, 0, \ldots, 0] \) of \((L - 1)\)-dimension.

We now illustrate, in order to justify the equilibrium is evolutionarily stable, that eigenvalues of the Jacobian matrix of the downsized population state all have negative real part. Here an element of the Jacobian matrix that is (a \((L - 1) \times (L - 1)\) matrix, denoted by \( J_{\vartheta^*} \), is a partial derivative as
\[ J_{\vartheta^*} = \begin{bmatrix} \frac{\partial \vartheta_j (t)}{\partial \vartheta_q (t)} \end{bmatrix}_{\vartheta (t) = \vartheta^* (t)}, \quad j, q = \mathcal{P}_m \ldots, \mathcal{P}_m. \] (20)
The Jacobian matrix denoted by \( J \) is therefore attained by
\[ J = \begin{bmatrix} \varphi_{12} \varphi_{13}^m \cdots & 0 & \cdots & 0 \\ 0 & \varphi_{23} \varphi_{24}^m \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \varphi_{L-1, L} \varphi_{L-1, L}^m \end{bmatrix}. \] (21)
In (21) \( \varphi_{12} \varphi_{13}^m, \varphi_{23} \varphi_{24}^m, \ldots, \varphi_{L-1, L} \varphi_{L-1, L}^m \) are in fact the eigenvalues of Jacobian matrix \( J \). From Lemma 2, for any \( j = 2, \ldots, L \), \( \phi (\mu_j (t) - \mu_q (t)) \) is equal to zero. We can thus attain
\[ \varphi_{j1} = \phi (\mu_j (t) - \mu_1 (t)) - \phi (\mu_1 (t) - \mu_j (t)) \]
\[ = -\phi (\mu_j (t) - \mu_j (t)) < 0. \] (22)
From Theorem 2.7.3 in [54], the equilibrium point \( \vartheta^* (t) \) is evolutionarily stable. Theorem 4 therefore follows. \( \square \)

3.5. Secrecy Rate Adaptation Algorithm. The algorithm of secrecy rate adaptation for WSNs is in fact to describe the process how member sensor nodes select adaptively their power level strategies. During this iterative process, periodically, a member sensor node observes its fitness in an entirely distributed mode and evaluates its current fitness with the average fitness of the whole WSNs. If the difference is larger than a predefined maximum bound, then the member
sensor node selects a new power level strategy according to the selection dynamics from (15). This interactive process goes on until the ESS of the secrecy rate game towards WSNs is achieved. All member sensor nodes thus find a satisfactory solution to secrecy rate adaptation, and no member sensor nodes can benefit by switching their current power level strategies while the other ones keep their strategies unchanged. From now on, we can show the algorithm as follows.

Algorithm 1.

(1) Initialize all coefficients including $W$, $I$, $\eta^2$ and all channel gains;
(2) $t \leftarrow 0$;
(3) select a power level strategy $j$ with the selection probability $\theta(t) = [1/L, 1/L, \ldots, 1/L]$. This probability assures each member sensor node has the same fitness at the beginning of the game;
(4) compute the fitness $\mu_j(t)$ and the average fitness $\bar{\mu}(t)$ according to (7) and (8), respectively;
(5) compute the expected secrecy rate $\xi_j(t)$ and the average secrecy rate $\bar{\xi}(t)$ according to (9) and (10), respectively;
(6) DO WHILE .T.

// $\tau$ means a predefined minimum bound;

(7) IF $|\bar{\mu}(t) - \mu_j(t)| < \tau$;

(8) EXIT;

(9) ENDDIF

// $\overline{\tau}$ means a predefined maximum bound;

(10) IF $|\bar{\xi}(t) - \mu_j(t)| > \overline{\tau}$;

(11) get $\theta(t + 1)$ by solving (15) with the standard numerical solver;

(12) select a new power level strategy $j$ with the new selection probability $\theta(t + 1)$;

(13) compute the fitness $\mu_j(t + 1)$ and the average fitness $\bar{\mu}(t + 1)$ according to (7) and (8), respectively;

(14) compute the expected secrecy rate $\xi_j(t + 1)$ and the average secrecy rate $\bar{\xi}(t + 1)$ according to (9) and (10), respectively;

(15) ENDDIF;

(16) $t \leftarrow t + 1$;

(17) ENDDO;

(18) RETURN the array of $\xi_j$ and $\bar{\xi}$.

4. Experiments

Since member sensor nodes are generally constrained in limited computation, memory, and battery life, we simplify the number of power level strategies to introduce an example of the secrecy rate game towards WSNs. We consider that a member sensor node $S_m$, when transmitting data, has to select a strategy in $\mathcal{S}_m = \{P_{H}, P_{L}\}$, where $P_{H}$ and $P_{L}$ denote the high and low power levels, respectively. That is, for any $m \in \{1, 2, \ldots, M\}$, $\mathcal{S}_m = \{P_{H}, P_{L}\}$. The utility of a member sensor node, from (5), can thus be rewritten as

$$
\mu(P_m, P_m) = W \left( \log_2 \left( 1 + \frac{P_m G_{H}}{\sum_{i=1}^{\hat{m}} P_i G_{H_i} + \eta^2} \right) \right) - \max_{E_k \in \mathcal{E}_m} \left( \frac{P_m G_{E_k}}{P_m G_{E_k} + \sum_{i=1}^{\hat{m}} P_i G_{E_i} + \eta^2} \right)^{\alpha} - \alpha P_m
$$

where $P_m, P_{\hat{m}} \in \mathcal{S}_m, S_m, \mathcal{S}_m \in \mathcal{S}$. For simple description, let $\mu_{HL}, \mu_{HL}, \mu_{LL}$, and $\mu_{HH}$ be $\mu(P_{H}, P_{H}), \mu(P_{H}, P_{L}), \mu(P_{L}, P_{L})$, and $\mu(P_{L}, P_{H})$, respectively.

Obviously, for the example of the secrecy rate game towards WSNs, we can get (a) $P_{H}$ is an ESS if and only if $\mu_{HH} > \mu_{HL}$ and $\mu_{HL} > \mu_{LL}$, (b) $P_{L}$ is an ESS if and only if $\mu_{HH} < \mu_{HL}$ and $\mu_{HL} < \mu_{LL}$, and (c) $(\mu_{HH} - \mu_{HL})/(\mu_{HH} - \mu_{LL}) = (\mu_{HH} - \mu_{HL})/(\mu_{HH} - \mu_{LL})$ is an ESS if and only if $\mu_{HH} < \mu_{HL}$ and $\mu_{HL} > \mu_{LL}$.

Next, we initialize all coefficients required in the example of the secrecy rate game towards WSNs for performing numerical experiments. According to IEEE 802.15.4 physical layer specifications, we let $\rho = 0.01$, $W = 2$ MHz, $P_{H} = 30$ mW, $P_{L} = 10$ mW, and $\sigma^2 = -112$ dBm, respectively. We also let the channel gain between a member sensor node and its responsible cluster head be 1, and we let the channel gain between a member sensor node and an eavesdropper be 0.6. Since different power levels will lead to different interference zones, we let $r_{H} = 50$ m and $r_{L} = 10$ m, where $r_{H}$ and $r_{L}$ denote the interference distance of a member sensor node adopting $P_{H}$ and $P_{L}$, respectively. In addition, we assume the working probability of interferers is 0.01 based on the empirical value. The number of interferers adopting the high (resp., low) power level strategy $P_{H}$ (resp., $P_{L}$), therefore, is $0.01 \times (\rho \pi r_{H}^2 + 3 \sqrt{\rho \pi r_{L}^2})$ (resp., $0.01 \times (\rho \pi r_{L}^2 + 3 \sqrt{\rho \pi r_{L}^2})$).

4.1 Effect of $\alpha$. The ESSs of the secrecy rate game towards WSNs are dependent on the cost parameter $\alpha$. As depicted in Figure 2, utilities of all strategy profiles are decreasing linearly with different speeds while $\alpha$ is increasing gradually. This fact means the influence of a power level strategy becomes larger than that of secrecy rate on the utility of a member sensor node. We can see lines of $\mu_{HH}$ and $\mu_{HL}$ intersect when $\alpha \approx 4.2267$, which implies $\mu_{HH} > \mu_{HL}$ if $\alpha < 4.2267$. 

\[ \text{International Journal of Distributed Sensor Networks} \]
Figure 2: Effect of $\alpha$ on ESSs of the example of the secrecy game towards WSNs.

otherwise $\mu_{HH} < \mu_{HL}$. Similarly, if $\alpha < 5.0919$ then $\mu_{HH} > \mu_{LL}$; otherwise $\mu_{HL} < \mu_{LL}$. Therefore, $P_H$ is an ESS if and only if $\alpha < 4.2267$; $P_L$ is an ESS if and only if $\alpha > 5.0919$; $(\mu_{LL} - \mu_{HL})/\mu_{HH} > (\mu_{HH} - \mu_{HL})/\mu_{HH} - (\mu_{LL})/\mu_{HH}$ is a mixed ESS if and only if $4.2267 < \alpha < 5.0919$.

4.2. ESSs for the Example of the Secrecy Rate Game towards WSNs. To illustrate the evolution of member sensor nodes selecting different power level strategies, the probability distribution function $\phi$ in (15) should be first defined. According to the idea [52] through linearizing the function $\phi$, we suppose

$$\phi(x) = \beta + \gamma x,$$

where $\beta, \gamma \in \mathbb{R}$, such that $0 \leq \beta + \gamma x \leq 1$. Substituting (24) into (15), we can attain the selection dynamics of member sensor nodes as

$$\dot{\theta}_j(t) = 2\gamma \theta_j(t) \sum_{q \neq j} \theta_q(t) \left( \mu_j(t) - \mu_q(t) \right),$$

where $\gamma$ is in fact a parameter that will influence the convergence speed of ESS. Let $\gamma$ be 0.5 (in practice, $\gamma$ may be an arbitrary real number); we attain different ESSs of the example of the secrecy game under different cost parameter values 3, 4.5, and 6, which are illustrated in Figures 3, 4, and 5, respectively. Note that these cost parameter values determine three different ESSs. As illustrated in Section 4.1, $\alpha = 3$ specifies that $P_H$ is an ESS, $\alpha = 4.5$ specifies that $P_L$ is an ESS, and $\alpha = 6$ specifies that there is a mixed ESS.

In Figure 3, when the initial value of (25) is 0.005, that is, if only 0.5% member sensor nodes select the high power level strategy $P_H$ in the beginning, the fraction of member sensor nodes selecting $P_H$, after about 51 times of playing the game, will be stable at 1; that is, all member sensor nodes select $P_H$ as their optimal strategy. We can also see that the higher initial fraction of member sensor nodes selecting $P_H$ is, the faster convergence speed of achieving ESS $P_H$ can be attained. These results reflect the fact that $P_H$ is an ESS when $\alpha = 3$.

In Figure 4, even if 99.5% member sensor nodes select $P_H$ in the beginning, we can find that, after about 37 times of playing the game, the fraction of member sensor nodes selecting $P_H$ will be stable at 0; that is, all member sensor nodes select the low power level strategy $P_L$ in the end. In addition, the convergence speed of achieving ESS $P_L$ becomes faster and faster as decreasing the initial fraction of member sensor nodes selecting $P_H$. The fact that $P_L$ is an ESS when $\alpha = 6$ is thus reflected.

In Figure 5, all curves of member sensor nodes selecting $P_H$, irrespective of different initial value of (25), converge to a limit 0.6841 or so. At this equilibrium point, about

Figure 3: $P_H$ is an ESS when $\alpha = 3$.  

Figure 4: $P_L$ is an ESS when $\alpha = 6$.  

Figure 5: All curves of member sensor nodes selecting $P_H$, irrespective of different initial value of (25), converge to a limit 0.6841 or so. At this equilibrium point, about
68.41% member sensor nodes select $P_H$ while about 31.59% member sensor nodes selecting $P_L$, as their respective optimal strategies. The other interpretation is that member sensor nodes switch their strategies between strategies $P_H$ and $P_L$, that is, playing $P_H$ for 68.41% of the time and $P_L$ for the remainder of the time. In fact, under this situation the case that all member sensor nodes select $P_H$ (resp. $P_L$) cannot be evolutionarily stable. This is because the utility of a member sensor node adopting $P_H$ (resp., $P_L$), when encountering one adopting $P_H$ (resp., $P_L$), is better than that of a member sensor node adopting $P_H$ (resp., $P_L$). These results lead to the fact that there is a mixed ESS $(0.6841, 0.3159)$ when $\alpha = 4.5$.

4.3. Secrecy Rate Adaptation. Our mechanism of secrecy rate adaptation in WSNs is realized when member sensor nodes select adaptively their power level strategies for maximizing their fitness. For convenience, let $\theta_H(t)$ be the fraction of member sensor nodes adopting $P_H$ at time $t$; then the fraction of nodes adopting $P_L$ at time $t$ is $1 - \theta_H(t)$. We denote the fitness of member sensor nodes adopting $P_H$ and $P_L$ at time $t$ by $\mu_H(t)$ and $\mu_L(t)$, respectively, where $\mu_H(t)$ and $\mu_L(t)$, from (7), are given by

\begin{align*}
\mu_H(t) &= \theta_H(t) \mu_{HH} + (1 - \theta_H(t)) \mu_{HL}, \\
\mu_L(t) &= \theta_H(t) \mu_{HL} + (1 - \theta_H(t)) \mu_{LL}.
\end{align*}

From (8), we can attain that the average fitness of the whole WSNs is

\begin{equation}
\overline{\mu}(t) = \theta_H(t) \mu_H(t) + (1 - \theta_H(t)) \mu_L(t).
\end{equation}

Similarly, we denote the expected secrecy rate of a member sensor node adopting $P_H$ and $P_L$ at time $t$ by $\zeta_H(t)$ and $\zeta_L(t)$, respectively, where $\zeta_H(t)$ and $\zeta_L(t)$, from (9), are given by

\begin{align*}
\zeta_H(t) &= \theta_H(t) \zeta_{HH} + (1 - \theta_H(t)) \zeta_{HL}, \\
\zeta_L(t) &= \theta_H(t) \zeta_{HL} + (1 - \theta_H(t)) \zeta_{LL},
\end{align*}

and the average secrecy rate of the whole WSNs, $\zeta(t)$, from (10), is given by

\begin{equation}
\zeta(t) = \theta_H(t) \zeta_H(t) + (1 - \theta_H(t)) \zeta_L(t). \tag{31}
\end{equation}

Here $\zeta_{uv}$, $u, v \in \{H, L\}$, denotes the secrecy rate of a member sensor node adopting $P_u$ when encountering one adopting $P_v$, which can be computed by the first term in (23).

We are now able to, under different cost values 3, 4.5, and 6, show changeable trends of fitness depicted in Figures 6, 7, and 8, as well as expected secrecy rates in Figures 9, 10, and 11, respectively. In Figures 6 and 9 where $P_H$ is an ESS, the fitness (resp., expected secrecy rate) of a member sensor node adopting $P_H$ is always higher than that of one adopting $P_L$. As member sensor nodes play the game continuously, both fitness values (resp., expected secrecy rates) decrease gradually while the average fitness (resp., secrecy rate) of the whole WSNs increases. After about 51 times of playing the game, the curves of both $\mu_H(t)$ (resp., $\zeta_H(t)$) and $\overline{\mu}(t)$ (resp., $\zeta(t)$) converge to a limit 42.9739 (resp., 132.9091) or so. Arriving at this equilibrium point implies all member sensor nodes, through switching their power level strategies adaptively, select $P_H$ in the end due to its higher fitness. The secrecy rate attained by a member sensor node is also adjusted adaptively. In Figures 7 and 10 where $P_L$ is an ESS, we can see some converse phenomena. The fitness of a member sensor node adopting $P_L$ is higher than that of a member sensor node adopting $P_H$, whereas the expected secrecy rate of a member sensor node adopting $P_L$ is lower. Moreover, the average fitness of the whole WSNs is increasing while the average secrecy rate is decreasing. In the end, when
all member sensor nodes select $P_L$ as their optimal power level strategy, the curves of both $\mu_L(t)$ and $\overline{\mu}(t)$, after about 37 times of playing the game, converge to a limit $-1.0675$ or so. Correspondingly, the expected secrecy rate attained by a member sensor node is adjusted adaptively to a limit 59.9593 or so. In Figures 8 and 11 where a mixed ESS exists at $(0.6841, 0.3159)$ or so, there is a similar trend among curves of $\mu_H(t)$, $\mu_L(t)$, and $\overline{\mu}(t)$. After about 36 times of playing the game, all curves in Figure 8 converge to a limit 6.8323 or so. That is, after achieving the mixed equilibrium point, both strategies $P_H$ and $P_L$ coexist permanently and all member sensor nodes have the same fitness regardless of their different strategies. On the other hand, in Figure 11 we can see expected secrecy rates of member sensor nodes adopting $P_H$ or $P_L$ are decreasing slowly. The average secrecy rate of the whole WSNs, however, is increasing little by little. This adaptation of average secrecy rate results in equilibrium point $113.3959$ or so in the end.

### 5. Conclusion

We have demonstrated the evolution process of secrecy rate adaptation for sensor nodes in the clustered WSNs. For this aim, the classical wiretap channel has been extended to fit for the clustered WSNs and the corresponding equation to compute secrecy rate has been attained. The secrecy rate game we have constructed is able to reflect the interactions among member sensor nodes. With EGT, we have attained a selection dynamics to determine how member sensor nodes
for maximizing their fitness will select their power level strategies. We have also proved the stability of the secrecy rate game to illustrate which power level strategy will be adopted in the end. The results from experiments for an example of the secrecy rate game towards WSNs have verified all ESSs and have revealed the process of expected secrecy rate adaptation for member sensor nodes. As a result, this disclosure of secrecy rate adaptation will be beneficial to employ PHY security to guarantee the secrecy of transmission in WSNs.

**Notations**

\( \rho \): Node density \\
\( r_H \): Receiving distance \\
\( r_I \): Interfering distance \\
\( \sqrt{\sigma} \): Standard deviation \\
\( z_I \): Maximum number of interferers to a sensor node \\
\( S, H, \text{ and } E \): Sets of \( M \) member sensor nodes, \( N \) cluster nodes, and \( K \) eavesdroppers, respectively \\
\( E_m \): Set of eavesdroppers capable of listening in data sensed by member sensor node \( S_m \) \\
\( G_H \): Channel gain between member sensor node \( S_m \) and its responsible cluster head \( H \) \\
\( G_{E_k} \): Channel gain between member sensor node \( S_m \) and eavesdropper \( E_k \), \( E_k \in E_m \) \\
\( \eta^2 \): Thermal noise power at cluster heads and eavesdroppers, respectively \\
\( W \): Channel bandwidth \\
\( \bar{S}_i \): An interferer to member sensor node \( S_m \), \( i \in \{1, 2, \ldots, I_m\} \) \\
\( S_m \): Set of interferers to member sensor node \( S_m \) \\
\( C_{S_m} \): Channel capacity from member sensor node \( S_m \) to its responsible cluster head \( H \) \\
\( P_m \): Transmission power adopted by member sensor node \( S_m \) \\
\( \rho_i_m \): Interference power adopted by interferer \( S_m \) \\
\( C_{E_k} \): Channel gain between interferer \( S_m \) and the interfered cluster head \( H \) \\
\( C_{E_k} \): Channel capacity from member sensor node \( S_m \) to eavesdropper \( E_k \), \( E_k \in E_m \) \\
\( C(P_m) \): Secrecy rate between member sensor node \( S_m \) adopting a power level \( P_m \) and its responsible \\
\( G = (S, F, U) \): Our secrecy rate game towards WSNs \\
\( F \): Set of strategy profiles for all member sensor nodes \\
\( F_m \): Set of pure power level strategies available to member sensor node \( S_m \) \\
\( U \): Set of utilities \\
\( \mu(P_m, P_m) \): Utility function for member sensor node \( S_m \) adopting power level \( P_m \) when its opponent \\
\( \alpha \): Cost parameter reflecting the degree of a member sensor node consuming energy for transmission \\
\( \theta_j(t) \): Fraction of member sensor nodes using power level strategy \( j \) at time \( t \) \\
\( \theta(t) \): State of the whole WSNs at time \( t \) \\
\( \mu_j \): Fitness of member sensor nodes adopting power level strategy \( j \) at time \( t \) \\
\( \bar{\mu}(t) \): Average fitness of the whole WSNs at time \( t \) \\
\( \xi_j(t) \): Expected secrecy rate of member sensor nodes adopting power level strategy \( j \) at time \( t \) \\
\( \bar{\xi}(t) \): Average secrecy rate of the whole WSNs at time \( t \) \\
\( r_j(\theta) \): Average review rate of member sensor nodes using power level strategy \( j \) \\
\( p_j^L(\theta) \): Probability of a reviewing member sensor node changing from power level strategy \( j \) to \( q \) \\
\( \phi \): Probability distribution function \\
\( \theta_j(t) \): Fraction of member sensor nodes in the downsized population using power level strategy \( j \) at time \( t \) \\
\( \theta(t) \): State of the downsized population at time \( t \) \\
\( \Psi_{y_j} \): Notation simple to denote equation \\
\( f_j(t) \): Element of Jacobian matrix \( f \)
\( P_H \) and \( P_L \): High and low power levels in the example of the secrecy rate game, respectively.

\( \mu_{HH}, \mu_{HL}, \mu_{LH}, \) and \( \mu_{LL} \): Notations simple to denote \( \mu(P_{H1}, P_{L1}), \mu(P_{H2}, P_{L2}), \mu(P_{L}, P_{L}), \) and \( \mu(P_{L}, P_{L}) \), respectively.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work was supported by National Natural Science Foundation of China under Grant no. 61272034, by Zhejiang Provincial Natural Science Foundation of China under Grants LY13F030012 and LY13F020035, and by Science Foundation of Shaoxing University under Grant no. 20145021.

References

[1] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: a survey," IEEE Communications Surveys and Tutorials, vol. 11, no. 2, pp. 52–73, 2009.

[2] H. V. Poor, "Information and inference in the wireless physical layer," IEEE Wireless Communications, vol. 19, no. 1, pp. 40–47, 2012.

[3] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multilayer wireless networks: a survey," IEEE Communications Surveys and Tutorials, vol. 16, no. 3, pp. 1550–1573, 2014.

[4] A. D. Wyner, "The wire-tap channel," The Bell System Technical Journal, vol. 54, no. 8, pp. 1355–1387, 1975.

[5] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," IEEE Transactions on Information Theory, vol. 24, no. 4, pp. 451–456, 1978.

[6] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," IEEE Transactions on Information Theory, vol. 24, no. 3, pp. 339–348, 1978.

[7] Z. H. Awan, A. Zaidi, and L. Vandendorpe, "Secure communication over parallel relay channel," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 359–371, 2012.

[8] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," IEEE Transactions on Information Theory, vol. 54, no. 3, pp. 976–1002, 2008.

[9] R. Liu, I. Marić, P. Spasojević, and R. D. Yates, "Discrete memoryless inference and broadcast channels with confidential messages: secrecy rate regions," IEEE Transactions on Information Theory, vol. 54, no. 6, pp. 2493–2507, 2008.

[10] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy outage in MISO systems with partial channel information," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 704–716, 2012.

[11] S. Shaee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the gaussian MIMO wire-tap channel: the 2-2-1 channel," IEEE Transactions on Information Theory, vol. 55, no. 9, pp. 4033–4039, 2009.

[12] L. Lai, H. El Gamal, and H. V. Poor, "The wiretap channel with feedback: encryption over the channel," IEEE Transactions on Information Theory, vol. 54, no. 11, pp. 5059–5067, 2008.

[13] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," IEEE Transactions on Signal Processing, vol. 58, no. 3, pp. 1875–1888, 2010.

[14] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," IEEE Transactions on Information Forensics and Security, vol. 7, no. 1, pp. 310–320, 2012.

[15] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Physical layer security of MIMO-OFDM systems by beamforming and artificial noise generation," Physical Communication, vol. 4, no. 4, pp. 313–321, 2011.

[16] S. A. A. Fakoorian and A. L. Swindlehurst, "MIMO interference channel with confidential messages: achievable secrecy rates and precoder design," IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 640–649, 2011.

[17] W. Saad, Z. Han, T. Başar, M. Debbah, and A. Hjorungnes, "Distributed coalition formation games for secure wireless transmission," Mobile Networks and Applications, vol. 16, no. 2, pp. 231–245, 2011.

[18] Y. Wu and K. J. R. Liu, "An information secrecy game in cognitive radio networks," IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 831–842, 2011.

[19] M. Yuksel, X. Liu, and E. Erkip, "A secure communication game with a relay helping the eavesdropper," IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 818–830, 2011.

[20] 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 Proceedings of the Military Communications Conference (MILCOM ’11), pp. 119–124, November 2011.

[21] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, "Physical layer security game: interaction between source, eavesdropper, and friendly jammer," EURASIP Journal on Wireless Communications and Networking, vol. 2009, Article ID 452907, 10 pages, 2009.

[22] S. A. A. Fakoorian and A. L. Swindlehurst, "Competing for secrecy in the MISO interference channel," IEEE Transactions on Signal Processing, vol. 61, no. 1, pp. 170–181, 2013.

[23] A. Mukherjee and A. L. Swindlehurst, "Jamming games in the MIMO wiretap channel with an active eavesdropper," IEEE Transactions on Signal Processing, vol. 61, no. 1, pp. 82–91, 2013.

[24] F. Gabry, N. Li, N. Schrammar, M. Girnyk, L. K. Rasmussen, and M. Skoglund, "On the optimization of the secondary transmitter’s strategy in cognitive radio channels with secrecy," IEEE Journal on Selected Areas in Communications, vol. 32, no. 3, pp. 451–463, 2014.

[25] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," IEEE Transactions on Vehicular Technology, vol. 61, no. 8, pp. 3693–3704, 2012.

[26] Z. Liu, Y. Shang, R. Zhang, and H. Xiang, "Relay selection based on coalition game for secure wireless networks," IET Communications, vol. 8, no. 8, pp. 1355–1363, 2014.

[27] L. Chen and J. Leneutre, "Fighting jamming with jamming—a game theoretic analysis of jamming attack in wireless networks and defense strategy," Computer Networks, vol. 55, no. 9, pp. 2259–2270, 2011.
[28] R. Machado and S. Tekinay, “A survey of game-theoretic approaches in wireless sensor networks,” Computer Networks, vol. 52, no. 16, pp. 3047–3061, 2008.

[29] H.-Y. Shi, W.-L. Wang, N.-M. Kwok, and S.-Y. Chen, “Game theory for wireless sensor networks: a survey,” Sensors, vol. 12, no. 7, pp. 9055–9097, 2012.

[30] S. Shen, G. Yue, Q. Cao, and F. Yu, “A survey of game theory in wireless sensor networks security,” Journal of Networks, vol. 6, no. 3, pp. 521–532, 2011.

[31] S. Shen, Y. Li, H. Xu, and Q. Cao, “Signaling game based strategy of intrusion detection in wireless sensor networks,” Computers and Mathematics with Applications, vol. 62, no. 6, pp. 2404–2416, 2011.

[32] S. Shen, R. Han, L. Guo, W. Li, and Q. Cao, “Survivability evaluation towards attacked WSNs based on stochastic game and continuous-time Markov chain,” Applied Soft Computing Journal, vol. 12, no. 5, pp. 1467–1476, 2012.

[33] S. Shen, H. Li, R. Han, A. V. Vasilakos, Y. Wang, and Q. Cao, “Differential game-based strategies for preventing malware propagation in wireless sensor networks,” IEEE Transactions on Information Forensics and Security, vol. 9, no. II, pp. 1962–1973, 2014.

[34] M. A. Khan, H. Tembine, and A. V. Vasilakos, “Evolutionary coalitional games: design and challenges in wireless networks,” IEEE Wireless Communications, vol. 19, no. 2, pp. 50–56, 2012.

[35] S. Moretti and A. V. Vasilakos, “An overview of recent applications of game theory to bioinformatics,” Information Sciences, vol. 180, no. 22, pp. 4312–4322, 2010.

[36] B. Q. Zhao, J. C. S. Lui, and D.-M. Chiu, “A mathematical framework for analyzing adaptive incentive protocols in P2P networks,” IEEE/ACM Transactions on Networking, vol. 20, no. 2, pp. 367–380, 2012.

[37] H. Tembine, E. Altman, R. El-Azouzi, and Y. Hayel, “Evolutionary games in wireless networks,” IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics, vol. 40, no. 3, pp. 634–646, 2010.

[38] M. P. Anastasopoulos, D. K. Petraki, R. Kannan, and A. V. Vasilakos, “TCP Throughput adaptation in wimax networks using replicator dynamics,” IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics, vol. 40, no. 3, pp. 647–655, 2010.

[39] M. A. Khan, H. Tembine, and A. V. Vasilakos, “Game dynamics and cost of learning in heterogeneous 4G networks,” IEEE Journal on Selected Areas in Communications, vol. 30, no. 1, pp. 198–213, 2012.

[40] Y. Wang, A. Nakao, and A. V. Vasilakos, “On modeling of coevolution of strategies and structure in autonomous overlay networks,” ACM Transactions on Autonomous and Adaptive Systems, vol. 7, no. 2, article 17, 25 pages, 2012.

[41] D. Niyato and E. Hossain, “Dynamics of network selection in heterogeneous wireless networks: an evolutionary game approach,” IEEE Transactions on Vehicular Technology, vol. 58, no. 4, pp. 2008–2017, 2009.

[42] B. Wang, K. J. R. Liu, and T. C. Clancy, “Evolutionary cooperative spectrum sensing game: how to collaborate?” IEEE Transactions on Communications, vol. 58, no. 3, pp. 890–900, 2010.

[43] K. Zhu, D. Niyato, P. Wang, and Z. Han, “Dynamic spectrum leasing and service selection in spectrum secondary market of cognitive radio networks,” IEEE Transactions on Wireless Communications, vol. 11, no. 3, pp. 1136–1145, 2012.
Submit your manuscripts at http://www.hindawi.com