Hindawi Publishing Corporation
Journal of Sensors
Volume 2016, Article ID 4254701, 10 pages
http://dx.doi.org/10.1155/2016/4254701

Research Article

Trust Dynamics in WSNs: An Evolutionary Game-Theoretic Approach

Shigen Shen,[1,2] Longjun Huang,[1,3] En Fan,[1] Keli Hu,[1] Jianhua Liu,[2] and Qiying Cao[4]

[1]*Department of Computer Science and Engineering, Shaoxing University, Shaoxing 312000, China*
[2]*College of Mathematics, Physics and Information Engineering, Jiaxing University, Jiaxing 314001, China*
[3]*College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou 310014, China*
[4]*College of Computer Science and Technology, Donghua University, Shanghai 201620, China*

Correspondence should be addressed to Shigen Shen; shigens@126.com

Received 1 October 2015; Revised 31 December 2015; Accepted 10 March 2016

Academic Editor: Eugenio Martinelli

A sensor node (SN) in Wireless Sensor Networks (WSNs) can decide whether to collaborate with others based on a trust management system (TMS) by making a trust decision. In this paper, we study the trust decision and its dynamics that play a key role to stabilize the whole network using evolutionary game theory. When SNs are making their decisions to select action *Trust* or *Mistrust*, a WSNs trust game is created to reflect their utilities. An incentive mechanism bound with one SN's trust degree is incorporated into this trust game and effectively promotes SNs to select action *Trust*. The replicator dynamics of SNs' trust evolution, illustrating the evolutionary process of SNs selecting their actions, are given. We then propose and prove the theorems indicating that evolutionarily stable strategies can be attained under different parameter values, which supply theoretical foundations to devise a TMS for WSNs. Moreover, we can find out the conditions that will lead SNs to choose action *Trust* as their final behavior. In this manner, we can assure WSNs' security and stability by introducing a trust mechanism to satisfy these conditions. Experimental results have confirmed the proposed theorems and the effects of the incentive mechanism.

1. Introduction

Currently, Wireless Sensor Networks (WSNs) have been widely used to a large number of applications that are classified into two categories: monitoring and tracking. Monitoring areas include environment, health, power, factory and process automation, and earthquake. Tracking areas include tracking objects, animals, humans, and vehicles [1]. In order to realize these applications, we must solve the essential problem of how to guarantee WSNs' security and stability. Cryptographic measures, called hard security, usually provide partial solutions by realizing data confidentiality, data integrity, and sensor nodes (SNs) authentication. On the other hand, trust management systems (TMSs) [2–4], called soft security, can efficaciously confront the case in which a normal SN which has gone through the hard security examination behaves fraudulently by giving incorrect or deceitful information to get extra benefits for itself. Therefore, in order to find a solution of the problem that SNs in WSNs often lack tamperproof hardware and are easily compromised, a TMS can be usually employed to decide how much belief should be assigned to a SN during the procedure of making cooperative decision [5].

When a TMS is employed in WSNs, the trust decision of SNs and its dynamics that we will study establish foundations to secure and stabilize the entire network. The misbehaving SNs, according to their reliabilities, will be reduced when they attempt to communicate with others. Generally, trust proofs must be collected and stored in a TMS. The trust degrees of SNs are considered to be computed and actions among SNs are recorded. Based on a TMS, a SN can decide whether to collaborate with others by making a trust decision. This trust decision and its dynamics in fact reveal one SN's interactions with others.

Game theory supplies an abundant group of mathematical approaches and models for exploring the multiplayer strategic decision-making [6], which has been largely employed to the field of WSNs security. Some examples

exist in judging attackers' behaviors [7], obtaining optimal strategies to save IDS agents in WSNs [8], providing optimal strategies for preventing malware propagation [9], and supplying secure and dependable virtual service for SensorCloud [10]. By taking this mathematical tool, we can find the best strategy for each player and the equilibrium state of a system. However, evolutionary game theory supposes that biologically conditioned decision-makers who are stochastically chosen from a massive population play repetitively the game. This theory is proposed to make an analysis of evolutionary choice in such clearly interactive cases [11]. Thus, players have the chance to optimize their individual utilities over time by responding to simple reflections from their opponents. This process is suitable to the requirement for the current large-scale wireless networks with characteristics of self-organization, self-configuration, and self-optimization. Therefore, many researchers are currently responsible for developing evolutionary game-based schemes. Typical examples exist in forwarding control in delay tolerant networks [12], adaptive service selection in small cell networks [13], joint network and user selection in cooperative wireless networks [14], dynamic backhaul resource allocation [15], joint mode selection and spectrum partitioning for D2D communication [16], priority-based time-slot allocation in wireless body area networks [17], and joint cloud and wireless networks operations in mobile cloud computing environments [18].

In this paper, we work on the procedure of trust decision performed by SNs to reveal the basic rule of trust evolution in WSNs, by extending our conference paper [19]. Using evolutionary game theory, we regard SNs as individual players and the entire WSNs as a population. A trust game of WSNs is set up according to the fact that all SNs can choose different strategies. Moreover, we introduce an incentive mechanism integrated into the game in order to investigate its effects of stimulating a SN to choose action *Trust*. We thus can investigate evolutionarily stable strategies (ESSs) of the proposed game with the idea of the replicator dynamics.

Our contributions lie mainly in the following aspects:

(1) We define a WSNs trust game among SNs, which can reveal properly the utilities of SNs when they are making their trust or mistrust decisions.

(2) We find that the incentive mechanism bound with the trust degree of a SN is able to reduce greatly the rate of SNs choosing action *Mistrust* and thus improve effectively the WSNs in its security as well as stability.

(3) We attain the theorems of ESSs related to our game, which provide various conditions to achieve these strategies and can be used to find a theoretical foundation to guide the design of a TMS for WSNs.

The rest of this paper is organized as follows. In Section 2, we illustrate the related work. In Section 3, we overview briefly the evolutionary game theory employed in our work. We then depict our WSNs trust game and investigate its ESSs with the idea of the replicator dynamics. In Section 4, we show our experiments to confirm the ESSs of our WSNs trust game and the effects of the incentive mechanism. Finally, conclusions are provided in Section 5.

2. Related Work

Many researchers have focused on the approaches of trust establishment, which provide the methods for representing, evaluating, maintaining, and distributing trust within the WSNs. Li et al. [20] proposed a lightweight and dependable trust system for the clustered WSNs, in which the trust decision-making scheme is based on the nodes' identities. They improved system efficiency by canceling feedback between cluster members or between cluster heads. In [21] Anita et al. proposed a collaborative lightweight trust-based (CLT) routing protocol for WSNs with minimal overhead with regard to memory and energy consumption. Confronting the characteristic of long periods of disconnected operation and fixed or irregular intervals between sink visits in unattended WSNs, Ren et al. [22] proposed a trust management scheme to provide efficient and robust trust data storage and trust generation. In [23] Ishmanov et al. presented a novel trust estimation method that is robust against on-off attacks and persistent malicious behavior, in which a modified one-step M-estimator scheme is used to aggregate recommendations securely. They further proposed another robust trust establishment scheme, considering the vulnerability of trust establishment to different attacks and the unique features of SNs [24]. To establish trustworthy relationships among nodes for their cooperation, Zhang et al. [25] set up a multiple-level trust management framework composed of a subjective trust, an objective trust, and the recommended trust. In addition, Jiang et al. [26], considering widespread malicious attacks to calculate SNs' trust value, proposed an efficient distributed trust model in which the direct trust and the recommendation trust are selectively calculated according to the number of packets received by SNs.

Trust in autonomous networks is able to help facilitate security and can be modeled as a strategic interaction. This is because any node's decision to trust or not in the security mechanism influences the decision of others (trust or not) and the result (secure or insecure network). Naturally, trust models combining the idea of game theory are introduced to explain these interactions. Mejia et al. [27] proposed a trust model based on the iterated prisoner's dilemma under the random pairing game. They employed a trust evaluation mechanism in terms of the forwarding rate and the prior observed decision and applied a bacterial-like algorithm to let nodes evolve their cooperation strategies. Yahyaoui [28] proposed a trust game for Web services collaboration. Each of the collaborations is modeled as a game in which the Web service that has the minimal trust-based cost will be the game winner. To ensure trustworthiness and encourage nodes to cooperate, Feng et al. [29] proposed a Bayesian-games-based incentive mechanism which is in pressing demand for trust management schemes. Since the efficiency of the trust evaluation process is largely governed by the trust derivation, Duan et al. [30] proposed an energy-aware trust derivation scheme using the game-theoretic approach, which manages overhead while maintaining adequate security of WSNs. Considering

the selfish nature of network entities, Shen et al. [31] formulated a public-goods-based global-trust-management-system game with a trust-based punishment mechanism that can provide the incentives of behaving cooperatively for network entities. In addition, Li et al. [32] constructed an evolutionary game-based trust strategy model among SNs and further introduced a strategy adjustment mechanism into the process of game evolution.

Evolutionary game has attracted much consideration and has been currently used to various aspects in WSNs. A dynamic incentive mechanism based on the evolutionary game is given in [33], where SNs adjust strategies forwardly and passively to maximize the fitness, making the population in the wireless sensor network converge to a cooperative state ultimately and promoting the selfish SNs cooperating with each other. In [34] Lin et al. proposed an evolutionary game-based data aggregation model that is defined to map the competition and cooperation in aggregation procedure into games and well avoid perfect rationality. The authors in [35] proposed a proactive defense model based on the evolutionary game, in which SNs have a limited ability to learn the evolution of rationality from different attack strategies of the attacker and can dynamically adjust their strategies to achieve the most effective defense. They also employ the evolutionary game to present two routing games, that is, a unicast and a multicast routing game [36]. Liu et al. [37] proposed an evolutionary game-theoretic optimal framework for maximizing the coverage capacity in mobile sensor networks. Their model jointly optimizes both the intracoverage capacity and the intercoverage capacity by considering the control of the power, distance, and interference among SNs. Farzaneh and Yaghmaee [38] applied the evolutionary game to develop a noncooperative game containing large number of SNs as players for alleviating and controlling congestion in WSNs by utilizing the available resource and controlling radio transmission power. Jiang et al. [39] employed the evolutionary game to set up selection dynamics upon which a power level can be adaptively selected by a SN. Thus, the objective of secrecy rate adaptation for maximizing the fitness of SNs is achieved. Moreover, a game-theoretic energy balance routing protocol [40] is proposed to extend the network lifetime by balancing energy consumption in a larger WSN using geographical routing protocols, where the evolutionary game is used to balance the traffic load to available subregions.

Our work is partly motivated by those related works above; however, there are some distinctions compared with them. Many current studies [20–26] have been done for trust establishment, while others [26–31] combine trust with game theory to explain players' interactions. With current works, how to solve the problem of trust evolution of SNs in WSNs still has not been performed, which becomes our aim. We centrally focus on setting up a WSNs trust game concerning on the dynamics of trust evolution during SNs' decision-making. When constructing our WSNs trust game, we consider the factor of trust degree, although they [20, 26, 41–43] have given various computation methods of trust degree. Our WSNs trust game is different from the literatures above, and we believe our game can show the SNs' utilities during their trust interactions. We apply the evolutionary game theory to the area of trust evolution in WSNs while existing literatures employ it to other fields. Moreover, we attain the conditions to reach ESSs of the game, which offer a theoretical basis to devise a TMS for WSNs.

3. Evolutionary Game Theory Based WSNs Trust Game

3.1. Overview of Evolutionary Game Theory. Any game in game theory has three elements: players, strategies, and payoff functions [44]. Strategies generally have two forms which are the pure-strategy and the mixed-strategy. The pure-strategy for a player is a complete plan of actions in all possible situations throughout the game, while the mixed-strategy is a probability distribution over a pure-strategy space. Payoff functions define the gains of each player during their interactions with each other, and the payoff to a profile of mixed-strategy is the expected value of corresponding pure-strategy payoffs. An evolutionary game extends the formulation of a traditional game by containing the concept of population. The number of individuals within a population which consisted of individuals (players) may be finite or infinite. The individuals within a population may select their strategies against individuals in the same population.

Evolutionary game theory concerns mainly a dynamic process, and the replicator dynamics [45] have become the most widely used evolutionary model that can be applied to explain and predict the changeable trend of a population's behavior. Let

$$S = \{a_1, a_2, \ldots, a_n\} \tag{1}$$

be the pure-strategy space of a given population; let $\phi_i(t)$ be the amount of the set of individuals using the pure-strategy a_i at time t; let

$$\theta(t) = \{\theta_1(t), \theta_2(t), \ldots, \theta_n(t)\} \tag{2}$$

be the status of the population at time t, which can be considered a mixed-strategy of the population, where

$$\theta_i(t) = \frac{\phi_i(t)}{\sum_i \phi_i(t)} \tag{3}$$

denotes the rate of individuals using the pure-strategy a_i at time t and $\sum_i \theta_i(t) = 1$ is satisfied. Then the expected payoff of individuals using the pure-strategy a_i at time t is

$$\mu(a_i, \theta(t)) = \sum_j \theta_j(t)\, \mu(a_i, a_j), \tag{4}$$

and the average expected payoff of the population is

$$\overline{\mu}(\theta(t), \theta(t)) = \sum_i \theta_i(t)\, \mu(a_i, \theta(t)). \tag{5}$$

Suppose that the net reproduction rate of each individual is proportional to its score in the stage game [46], which results in

$$\dot{\phi}_i(t) = \phi_i(t)\, \mu(a_i, \theta(t)); \tag{6}$$

Table 1: Payoff matrix.

	Trust	*Mistrust*
Trust	$\omega_T + \omega_C + \alpha T - 2\beta$	$\omega_T + \alpha T - \beta - \gamma$
Mistrust	$\omega_M + \omega_C - \beta$	ω_M

thus the replicator dynamics formula [46] is

$$\begin{aligned}\dot{\theta}_i(t) &= \frac{\dot{\phi}_i(t)\sum_i \phi_i(t) - \phi_i(t)\sum_i \dot{\phi}_i(t)}{\left(\sum_i \phi_i(t)\right)^2} \\ &= \frac{\left(\dot{\phi}_i(t)/\phi_i(t)\right)\sum_i \phi_i(t) - \sum_i \dot{\phi}_i(t)}{\sum_i \phi_i(t)} \cdot \frac{\phi_i(t)}{\sum_i \phi_i(t)} \\ &= \theta_i(t)\left(\mu\left(a_i, \theta(t)\right) - \overline{\mu}\left(\theta(t), \theta(t)\right)\right).\end{aligned} \tag{7}$$

Moreover, the ESS has become one core concept in evolutionary game theory, which is the strategy that reaches an equilibrium point during the evolutionary process. It reflects actually the mutation mechanism that provides variety, while the replicator dynamics face the selection mechanism that favors some varieties over others. The idea of ESS is to demand that the equilibrium should be able to repel invaders; that is, if a strategy is evolutionarily stable, then it must maintain such a characteristic that almost each individual of the population follows this strategy and mutants hardly invade successfully. This ESS in fact is a refinement of Nash equilibrium.

3.2. WSNs Trust Game. For the convenience, we introduce some notations illustrated in Notations.

Definition 1. A population $\mathcal{G}$ consists of a vast amount of individuals responding to SNs in WSNs.

Definition 2. The WSNs trust game, which is symmetric, is formulated by a 3-tuple $\mathbb{G} = (\mathcal{I}, \mathcal{A}, \mathbf{M})$, where

(i) $\mathcal{I}$ is a set of SNs (individuals) in WSNs (population $\mathcal{G}$);

(ii) $\mathcal{A}$ is a set of actions, and $\mathcal{A} = \{a_1, a_2\} = \{Trust, Mistrust\}$;

(iii) $\mathbf{M}$ is a payoff matrix that is represented in Table 1.

In general, a trust degree is managed to assess trust levels of SNs. Many authors [20, 22, 25, 26, 41, 47] have proposed various computation approaches to a trust degree. We do not consider in this paper how to calculate a trust degree for a SN, which is in fact not the focus of the current work. Nevertheless, we assume that any SN has been assigned a trust degree by a TMS.

In our WSNs trust game, action *Trust* or *Mistrust* may be chosen by a SN in different cases. Choosing action *Trust* indicates that a SN will collaborate with its opponent; on the other hand, choosing action *Mistrust* indicates noncooperation. We next discuss various payoffs in different cases:

(1) Two senor nodes both choose action *Trust*. This case means that either of two SNs collaborates with the other and assists its opponent to forward sensed data. Therefore, their trust degrees are improved and both of them receive gain ω_T. Either of them also receives gain ω_C due to its opponent's trust which leads to assisting itself to forward its own sensed data. In order to encourage SNs to choose action *Trust*, we consider an incentive mechanism based on the trust degree; that is, one obtains gain αT when it chooses action *Trust*. Simultaneously, one must compensate cost β caused by the computation and power consumption because one transmits its own sensed data or forwards its opponent's. In a sum, the entire payoff for either of them is $\omega_T + \omega_C + \alpha T - 2\beta$.

(2) A SN chooses action *Trust*, whereas its opponent chooses action *Mistrust*. For the SN choosing action *Trust*, it receives gain ω_T because of an improvement in its trust degree received by forwarding its opponent's sensed data and the incentive gain αT. Simultaneously, it must compensate cost β caused by the computation and power consumption because it forwards its opponent's sensed data. On the other hand, because its opponent choosing action *Mistrust* will lead to noncooperation between two SNs, it suffers from loss γ since its own sensed data cannot be transmitted to the expected SN. Therefore, the entire payoff for one choosing action *Trust* is $\omega_T + \alpha T - \beta - \gamma$. For one choosing action *Mistrust*, it does not need to forward its opponent's sensed data, so it receives gain ω_M since it does not require to consume its power and its lifetime is extended. It also receives gain ω_C since its opponent chooses action *Trust*. Simultaneously, it must compensate cost β for transmitting its own sensed data with success. Therefore, its entire payoff is $\omega_M + \omega_C - \beta$.

(3) Both of two SNs choose action *Mistrust*. This case results in the consequence of noncooperation between each other. From the similar analysis above, either of them receives gain ω_M.

3.3. ESSs of Our WSNs Trust Game. Because our WSNs trust game has two actions, we denote $\theta(t) = (\delta, 1-\delta)$ as the mixed-strategy for the population $\mathcal{G}$ at time t, where δ is the rate of SNs choosing action *Trust* (i.e., a_1), and $1 - \delta$ is the rate of SNs choosing action *Mistrust* (i.e., a_2). From (4), we get the expected payoff of SNs choosing action *Trust* as

$$\begin{aligned}\mu\left(a_1, \theta(t)\right) = {} & \delta\left(\omega_T + \omega_C + \alpha T - 2\beta\right) \\ & + (1-\delta)\left(\omega_T + \alpha T - \beta - \gamma\right)\end{aligned} \tag{8}$$

and the expected payoff of SNs choosing action *Mistrust* as

$$\mu\left(a_2, \theta(t)\right) = \delta\left(\omega_M + \omega_C - \beta\right) + (1-\delta)\,\omega_M. \tag{9}$$

From (5), we get the mean payoff of the entire population $\mathcal{G}$ as

$$\overline{\mu}\left(\theta(t), \theta(t)\right) = \delta\mu\left(a_1, \theta(t)\right) + (1-\delta)\,\mu\left(a_2, \theta(t)\right). \tag{10}$$

Therefore, from (7), we get the replicator dynamics formula of trust evolution in WSNs as

$$R(\delta) = \dot{\theta}(t) = \delta\left(\mu\left(a_1, \theta(t)\right) - \overline{\mu}\left(\theta(t), \theta(t)\right)\right) = \delta(1 - \delta)\left[\delta\left(\omega_T + \alpha T - \omega_M - \beta\right) + (1-\delta)\left(\omega_T + \alpha T - \omega_M - \beta - \gamma\right)\right]. \tag{11}$$

Let $R(\delta) = 0$; we can get three fixed states at most from (11), which are

$$\delta_1^* = 0, \quad \delta_2^* = 1, \quad \delta_3^* = \frac{\left(\omega_M + \beta + \gamma - \omega_T - \alpha T\right)}{\gamma}. \tag{12}$$

As determined by the features of ESS, a fixed state in an evolutionary game must be resistant to a small interference, which in fact corresponded to the necessary conditions of the fixed theorem of differential formulas. In other words, $R'(\delta^*) < 0$ must be assured once δ^* is a fixed state. If the phase diagram of the replicator dynamics formula is used, then the ESSs of our WSNs trust game are the intersections with the x-axis where the slope of the tangent line is negative.

Theorem 3. *If $\omega_T + \alpha T - \omega_M - \beta > 0$, $\omega_M + \beta + \gamma - \omega_T - \alpha T > 0$, and $2\omega_T + 2\alpha T - 2\omega_M - 2\beta - \gamma > 0$, then both $\delta_1^* = 0$ and $\delta_2^* = 1$ are the ESSs of our WSNs trust game, and they satisfy $\rho(\delta_1^* = 0) < \rho(\delta_2^* = 1)$, where $\rho(\delta_1^* = 0)$ and $\rho(\delta_2^* = 1)$ indicate the probability of SNs choosing action Mistrust and that of ones choosing action Trust, respectively.*

Proof. Computing the derivative of (11), we attain

$$R'(\delta) = -3\gamma\delta^2 + \left(2\omega_M + 2\beta + 4\gamma - 2\omega_T - 2\alpha T\right)\delta + \omega_T + \alpha T - \omega_M - \beta - \gamma. \tag{13}$$

We set $\delta = 0$ and $\delta = 1$, respectively, and attain

$$R'(0) = \omega_T + \alpha T - \omega_M - \beta - \gamma < 0, \quad R'(1) = \omega_M + \beta - \omega_T - \alpha T < 0. \tag{14}$$

Since $2\omega_T + 2\alpha T - 2\omega_M - 2\beta - \gamma > 0$, we attain $\omega_T + \alpha T - \omega_M - \beta > \omega_M + \beta + \gamma - \omega_T - \alpha T$. Therefore, we attain

$$0 < \frac{\left(\omega_M + \beta + \gamma - \omega_T - \alpha T\right)}{\gamma} = \frac{\omega_M + \beta + \gamma - \omega_T - \alpha T}{\omega_T + \alpha T - \omega_M - \beta + \omega_M + \beta + \gamma - \omega_T - \alpha T} < \frac{\omega_M + \beta + \gamma - \omega_T - \alpha T}{2\left(\omega_M + \beta + \gamma - \omega_T - \alpha T\right)} = \frac{1}{2}. \tag{15}$$

From (14) and (15), the phase diagram of the replicator dynamics Equation (11) is illustrated in Figure 1.

In Figure 1, both $\delta_1^* = 0$ and $\delta_2^* = 1$ are the ESSs because both the slopes of the tangent lines at $\delta_1^* = 0$ and $\delta_2^* = 1$ are less than zero. Moreover, from (15), the probability of SNs choosing action *Mistrust* is less than that of ones choosing action *Trust*, that is, $\rho(\delta_1^* = 0) < \rho(\delta_2^* = 1)$. □

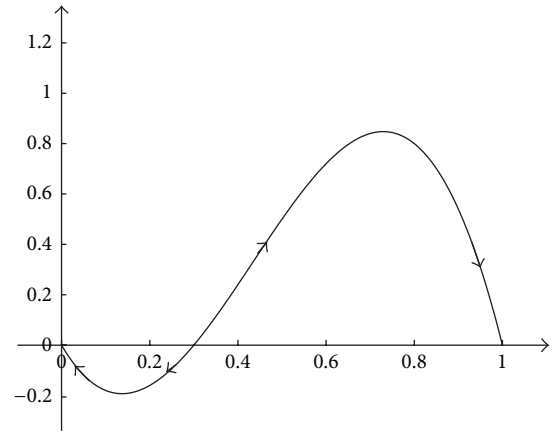

Figure 1: The phase diagram of the replicator dynamics (1).

The meaning of Theorem 3 is discussed as follows. When a SN chooses action *Trust*, its opponent receives more utilities from choosing action *Trust* than action *Mistrust* due to $\omega_T + \omega_C + \alpha T - 2\beta - (\omega_M + \omega_C - \beta) = \omega_T + \alpha T - \omega_M - \beta > 0$. On the other hand, when one chooses action *Mistrust*, its opponent receives more utilities from choosing action *Mistrust* than action *Trust* due to $\omega_T + \alpha T - \beta - \gamma - \omega_M < 0$. Moreover, the case that both $\delta_1^* = 0$ and $\delta_2^* = 1$ are the ESSs means that action *Trust* or *Mistrust* is probably chosen by SNs during the trust evolution in WSNs.

Theorem 4. *If $\omega_T + \alpha T - \omega_M - \beta > 0$, $\omega_M + \beta + \gamma - \omega_T - \alpha T > 0$, and $2\omega_T + 2\alpha T - 2\omega_M - 2\beta - \gamma < 0$, then both $\delta_1^* = 0$ and $\delta_2^* = 1$ are the ESSs of our WSNs trust game, and they satisfy $\rho(\delta_1^* = 0) > \rho(\delta_2^* = 1)$.*

Proof. From the proof procedure of Theorem 3, we attain

$$R'(0) = \omega_T + \alpha T - \omega_M - \beta - \gamma < 0, \tag{16}$$

$$R'(1) = \omega_M + \beta - \omega_T - \alpha T < 0, \tag{17}$$

$$\frac{1}{2} < \frac{\left(\omega_M + \beta + \gamma - \omega_T - \alpha T\right)}{\gamma} < 1. \tag{18}$$

From (16), (17), and (18), the phase diagram of the replicator dynamics Equation (11) is illustrated in Figure 2.

In Figure 2, both $\delta_1^* = 0$ and $\delta_2^* = 1$ are the ESSs because both the slopes of the tangent lines at $\delta_1^* = 0$ and $\delta_2^* = 1$ are less than zero. Moreover, from (18), the probability of SNs choosing action *Mistrust* is larger than that of ones choosing action *Trust*, that is, $\rho(\delta_1^* = 0) > \rho(\delta_2^* = 1)$. □

Theorem 5. *If $\omega_T + \alpha T - \omega_M - \beta < 0$, then $\delta_1^* = 0$ is the only ESS of our WSNs trust game.*

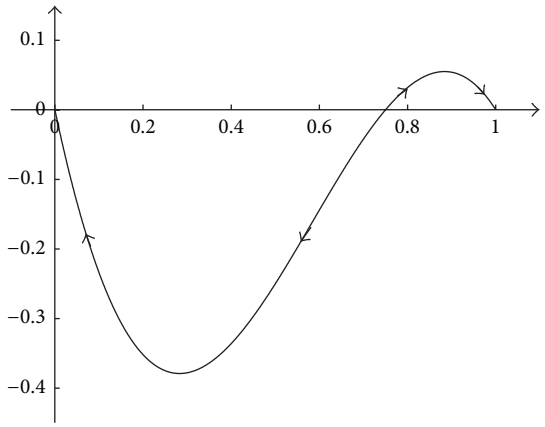

Figure 2: The phase diagram of the replicator dynamics (2).

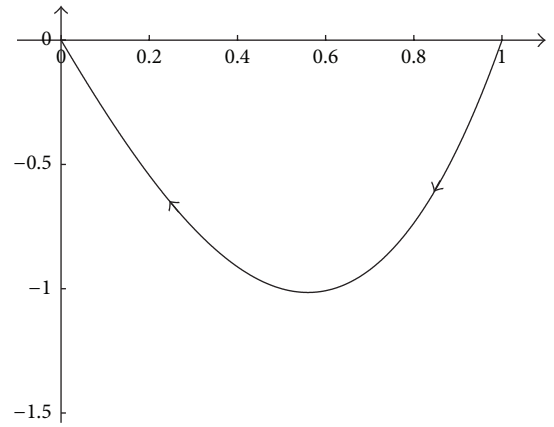

Figure 3: The phase diagram of the replicator dynamics (3).

Proof. From the proof procedure of Theorem 3, we attain

$$R'(0) = \omega_T + \alpha T - \omega_M - \beta - \gamma < 0,$$
$$R'(1) = \omega_M + \beta - \omega_T - \alpha T > 0. \quad (19)$$

From (19), the phase diagram of the replicator dynamics (see (11)) is illustrated in Figure 3.

In Figure 3, the slope of the tangent line at $\delta_1^* = 0$ is less than zero; $\delta_1^* = 0$ therefore is the ESS. □

Theorem 5 indicates that when a SN chooses action *Trust* or *Mistrust*, its opponent receives more utilities from choosing action *Mistrust* than from choosing action *Trust*. Therefore, the rate of SNs choosing action *Trust* will be fixed at 0% eventually; that is, all SNs will choose action *Mistrust*.

Theorem 6. *If $\omega_T + \alpha T - \omega_M - \beta - \gamma > 0$, then $\delta_2^* = 1$ is the only ESS of our WSNs trust game.*

Proof. From the proof procedure of Theorem 3, we attain

$$R'(0) = \omega_T + \alpha T - \omega_M - \beta - \gamma > 0,$$
$$R'(1) = \omega_M + \beta - \omega_T - \alpha T < \omega_M + \beta + \gamma - \omega_T - \alpha T < 0. \quad (20)$$

According to (20), the phase diagram of the replicator dynamics (see (11)) is illustrated in Figure 4.

In Figure 4, $\delta_2^* = 1$ is the ESS because the slope of the tangent line at $\delta_2^* = 1$ is less than zero. □

Theorem 6 indicates that when a SN chooses action *Trust* or *Mistrust*, its opponent receives more utilities from choosing action *Trust* than from choosing action *Mistrust*. Therefore, the rate of SNs choosing action *Trust* will be fixed at 100% eventually; that is, all SNs will choose action *Trust*. In fact, action *Trust* is the strictly dominant one when the condition of Theorem 6 is satisfied.

From Theorems 3–6, we should make a TMS satisfy the cases of Theorems 3 and 6 because they can promote SNs to choose action *Trust*. In this manner, we can realize WSNs' security and stability. Moreover, the introduced gain αT adds an incentive mechanism for SNs choosing action *Trust*. When the conditions of Theorem 3 are satisfied and the value of αT is increasing continuously, then $\delta_3^* = (\omega_M + \beta + \gamma - \omega_T - \alpha T)/\gamma \to 0$ which means the rate of SNs choosing action *Mistrust* is decreasing continuously and reaches a low fixed level eventually. As the value of αT increases until the condition of Theorem 6 is satisfied, the WSNs will be in a realistically fixed state at that time whenever SNs choose action *Trust* or *Mistrust* in the beginning; all of them will finally choose action *Trust*. Obviously, the cases of Theorems 4 and 5 must be avoided when we devise a TMS. If not, the probability of SNs choosing action *Mistrust* is larger than that of ones choosing action *Trust* or all SNs eventually choose action *Mistrust* as their fixed state. Consequently, either will cause the WSNs to be unstable.

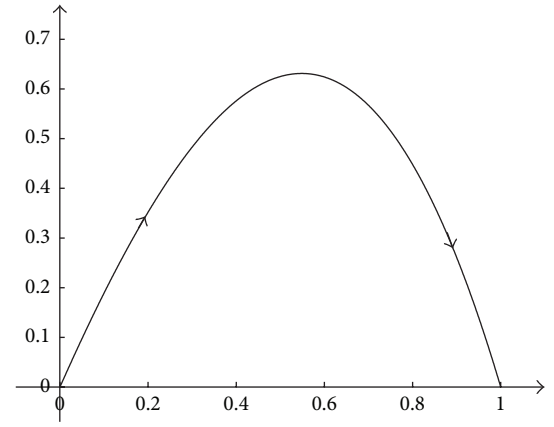

Figure 4: The phase diagram of the replicator dynamics (4).

4. Numerical Experiments

Using MATLAB R2009a, we confirm the ESSs of our WSNs trust game and the effects of the incentive mechanism with varied parameter values of ω_T, ω_M, β, γ, and αT. The experiments are categorized into two groups. In the first

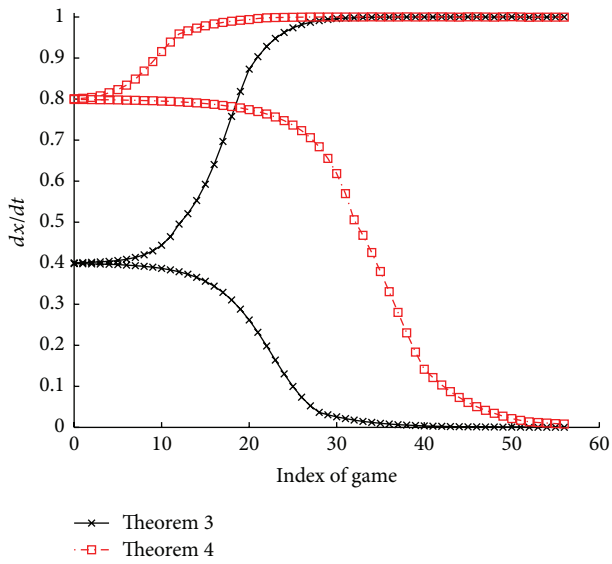

Figure 5: Curves of the WSNs trust evolution (1).

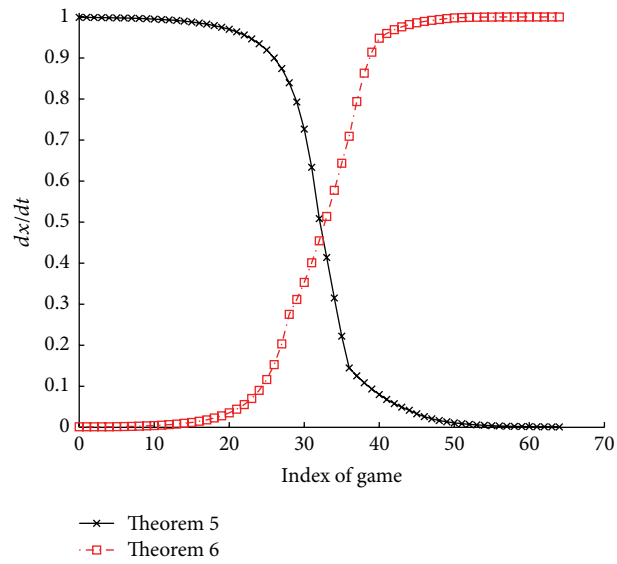

Figure 6: Curves of the WSNs trust evolution (2).

group, after initializing the parameter values to satisfy the conditions of Theorems 3–6, respectively, we observe the changeable trends of trust evolution curves of SNs in WSNs. In the other group, we understand the effects of the incentive mechanism during the trust evolution by changing the value of αT. Note that how to decide α is an open issue; however, it is not the focus of our current work but it should be considered during devising a TMS in WSNs.

In Figure 5, the conditions of Theorem 3 are satisfied by setting the parameter values related to curve ×. Once the value of (11) is initialized by 0.401 indicating that 40.1% SNs choose action *Trust* at first, it is shown that SNs adaptively change their actions continuously and the rate of SNs choosing action *Trust*, after ~38 rounds of playing the game, will be fixed at $\delta_2^* = 1$. This case means that all participated SNs will choose action *Trust* eventually, if only the rate of ones choosing action *Trust* is more than 40.1% at first. Once the value of (11) is initialized by 0.399 indicating that 39.9% SNs choose action *Trust* at first, the rate of ones choosing action *Trust* will be fixed at $\delta_1^* = 0$ after ~44 rounds of playing the game. This case means that all participated SNs will choose action *Mistrust* eventually, if the rate of ones choosing action *Trust* is only less than 39.9% at first. Experimental results confirm that both $\delta_1^* = 0$ and $\delta_2^* = 1$ are the ESSs of our WSNs trust game and that $\rho(\delta_1^* = 0) < \rho(\delta_2^* = 1)$ is sure when we satisfy the conditions of Theorem 3.

In Figure 5, the conditions of Theorem 4 are satisfied by setting the parameter values related to curve □. Once the value of (11) is initialized by 0.801 indicating that 80.1% SNs choose action *Trust* at first, the rate of ones choosing action *Trust* will be fixed at $\delta_2^* = 1$ after ~30 rounds of playing the game. Once the value of (11) is initialized by 0.799 indicating that 79.9% SNs choose action *Trust* at first, the rate of ones choosing action *Trust* will be fixed at $\delta_1^* = 0$ after ~56 rounds of playing the game. This case means that all participated SNs will choose action *Trust* eventually, only if the rate of ones choosing action *Trust* is more than 79.9% at first. Experimental results confirm that both $\delta_1^* = 0$ and $\delta_2^* = 1$ are the ESSs of our WSNs trust game and that $\rho(\delta_1^* = 0) > \rho(\delta_2^* = 1)$ is sure when we satisfy the conditions of Theorem 4.

In Figure 6, the condition of Theorem 5 is satisfied by setting the parameter values related to curve ×. We can see the rate of SNs choosing action *Trust* will be fixed at $\delta_1^* = 0$ after ~58 rounds of playing the game, even if 99.9% SNs choose action *Trust* at first. The experimental result shows that $\delta_1^* = 0$ is the ESS of our WSNs trust game when we satisfy the condition of Theorem 5.

In Figure 6, the condition of Theorem 6 is satisfied by setting the parameter values related to curve □. The rate of SNs choosing action *Trust* will be fixed at $\delta_2^* = 1$ eventually after ~53 rounds of playing the game, if only 0.1% SNs choose action *Trust* at first. The experimental result indicates that $\delta_2^* = 1$ is the ESS of our WSNs trust game when we satisfy the condition of Theorem 6.

Next, we illustrate the effects of the incentive mechanism. Figure 7 shows the curves of WSNs trust evolution under different initial values of (11), while Figure 8 shows the changeable trends of curves that converge to $\delta_2^* = 1$ under the same initial value of (11).

In Figure 7, we can see that the critical initial value of trust evolution of SNs is 0.401 if $\alpha T = 3$, while it is 0.301 if $\alpha T = 3.5$. This means that though the rate of SNs choosing action *Trust* decreases from 40.1% to 30.1%, $\delta_2^* = 1$, as the value of αT increasing from 3 to 3.5, will still be the ESS of our WSNs trust game. In Figure 8, it takes ~38 rounds of playing the game if $\alpha T = 3$ but only ~20 if $\alpha T = 3.5$ to reach the fixed point $\delta_2^* = 1$. Apparently, the speed of the curve $\alpha T = 3.5$ converging to the fixed state is obviously faster than that of the curve $\alpha T = 3$. These results in Figures 7 and 8 reflect the significant effects of the incentive mechanism. That is, through binding the trust degree to the incentive mechanism and rewarding the trust degree, it is profitable to the WSNs evolution to a fixed state

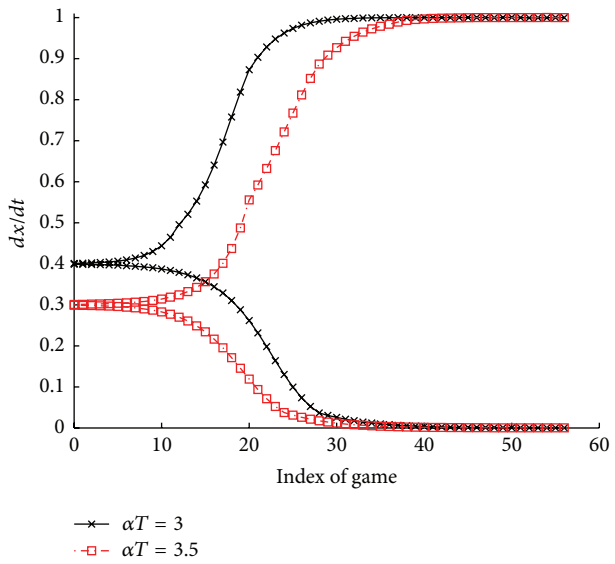

Figure 7: Curves of the WSNs trust evolution (3).

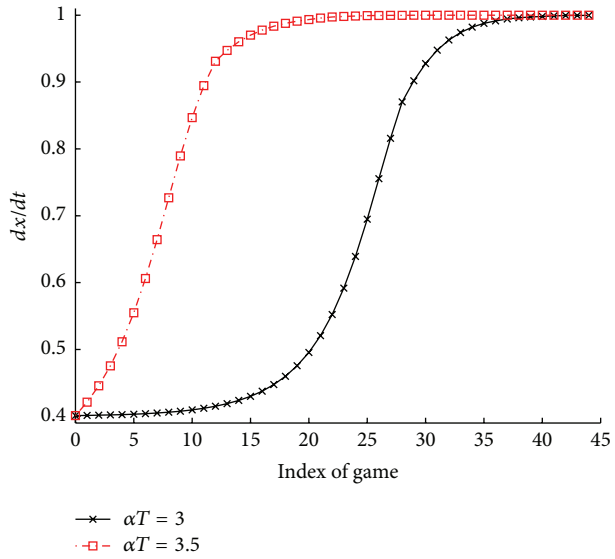

Figure 8: Curves of the WSNs trust evolution (4).

of trust among SNs for ensuring the security and stability of the network.

5. Conclusions

The trust-based mechanism in WSNs is one of important security technologies, which is able to make SNs construct their belief and lower the risk of collaboration. We have formulated a WSNs trust game, which can reveal SNs' payoffs when they make a decision of choosing action *Trust* or *Mistrust*. We have attained the replicator dynamics formula of trust evolution, which sets up an approach to illustrate various ESSs under different cases. The proven ESSs show how the fixed points of the dynamic trust evolution in WSNs can be eventually reached after SNs adaptively change their actions continuously. These ESSs also provide theoretical foundations for devising a TMS. Experimental results have confirmed the ESSs of our WSNs trust game and the effects of the incentive mechanism. From these ESSs, a TMS must accord the conditions of theorems that will lead SNs to choose action *Trust* as their final behavior, when it is devised to realize WSNs' security and stability. In addition, the incentive mechanism bound with the trust degree of a SN has effectively reduced the rate requirement of the initial value of SNs choosing action *Trust* and improved the convergence speed of the dynamic system evolving to the fixed state at which all SNs will choose action *Trust*.

Notations

T: Trust degree of a SN
α: Adjustment factor to T
ω_T: Gain received by a SN choosing action *Trust*
ω_M: Gain received by a SN choosing action *Mistrust*
ω_C: Cooperative gain received by a SN because of its opponent choosing action *Trust*
β: Cost caused by a SN transmitting its own or its opponents' sensed data
γ: Uncooperative loss taken by a SN because of its opponent choosing action *Mistrust*.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This work was supported by National Natural Science Foundation of China under Grants nos. 61272034 and 61572014 and by Science Foundation of Shaoxing University under Grant no. 20145021.

References

[1] L. M. Borges, F. J. Velez, and A. S. Lebres, "Survey on the characterization and classification of wireless sensor network applications," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 4, pp. 1860–1890, 2014.

[2] Y. Wu, Y. Zhao, M. Riguidel, G. Wang, and P. Yi, "Security and trust management in opportunistic networks: a survey," *Security and Communication Networks*, vol. 8, no. 9, pp. 1812–1827, 2015.

[3] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," *Journal of Network and Computer Applications*, vol. 42, pp. 120–134, 2014.

[4] G. Han, J. Jiang, L. Shu, J. Niu, and H.-C. Chao, "Management and applications of trust in Wireless Sensor Networks: a survey," *Journal of Computer and System Sciences*, vol. 80, no. 3, pp. 602–617, 2014.

[5] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A survey of trust and reputation management systems in wireless communications," *Proceedings of the IEEE*, vol. 98, no. 10, pp. 1755–1772, 2010.

[6] T. Alpcan and T. Başar, *Network Security: A Decision and Game-Theoretic Approach*, Cambridge University Press, Cambridge, UK, 2010.

[7] 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*, vol. 12, no. 5, pp. 1467–1476, 2012.

[8] S. Shen, K. Hu, L. Huang, H. Li, R. Han, and Q. Cao, "Quantal response equilibrium-based strategies for intrusion detection in WSNs," *Mobile Information Systems*, vol. 2015, Article ID 179839, 10 pages, 2015.

[9] 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. 11, pp. 1962–1973, 2014.

[10] J. Liu, S. Shen, G. Yue, R. Han, and H. Li, "A stochastic evolutionary coalition game model of secure and dependable virtual service in Sensor-Cloud," *Applied Soft Computing*, vol. 30, pp. 123–135, 2015.

[11] J. W. Weibull, *Evolutionary Game Theory*, MIT Press, Cambridge, UK, 1995.

[12] R. El-Azouzi, F. De Pellegrini, H. B. A. Sidi, and V. Kamble, "Evolutionary forwarding games in delay tolerant networks: equilibria, mechanism design and stochastic approximation," *Computer Networks*, vol. 57, no. 4, pp. 1003–1018, 2013.

[13] K. Zhu, E. Hossain, and D. Niyato, "Pricing, spectrum sharing, and service selection in two-tier small cell networks: a hierarchical dynamic game approach," *IEEE Transactions on Mobile Computing*, vol. 13, no. 8, pp. 1843–1856, 2014.

[14] H. Pervaiz, Q. Ni, and C. C. Zarakovitis, "User adaptive QoS aware selection method for cooperative heterogeneous wireless systems: a dynamic contextual approach," *Future Generation Computer Systems*, vol. 39, pp. 75–87, 2014.

[15] I. V. Loumiotis, E. F. Adamopoulou, K. P. Demestichas, T. A. Stamatiadi, and M. E. Theologou, "Dynamic backhaul resource allocation: an evolutionary game theoretic approach," *IEEE Transactions on Communications*, vol. 62, no. 2, pp. 691–698, 2014.

[16] K. Zhu and E. Hossain, "Joint mode selection and spectrum partitioning for device-to-device communication: a dynamic stackelberg game," *IEEE Transactions on Wireless Communications*, vol. 14, no. 3, pp. 1406–1420, 2015.

[17] S. Misra and S. Sarkar, "Priority-based time-slot allocation in wireless body area networks during medical emergency situations: an evolutionary game-theoretic perspective," *IEEE Journal of Biomedical and Health Informatics*, vol. 19, no. 2, pp. 541–548, 2014.

[18] Z. Yin, F. R. Yu, S. Bu, and Z. Han, "Joint cloud and wireless networks operations in mobile cloud computing environments with telecom operator cloud," *IEEE Transactions on Wireless Communications*, vol. 14, no. 7, pp. 4020–4033, 2015.

[19] S. Shen, C. Jiang, H. Jiang, L. Guo, and Q. Cao, "Evolutionary game based dynamics of trust decision in WSNs," in *Proceedings of the International Conference on Sensor Network Security Technology and Privacy Communication System*, pp. 1–4, Harbin, China, March 2013.

[20] X. Li, F. Zhou, and J. Du, "LDTS: a lightweight and dependable trust system for clustered wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 6, pp. 924–935, 2013.

[21] X. Anita, M. A. Bhagyaveni, and J. Martin Leo Manickam, "Collaborative lightweight trust management scheme for wireless sensor networks," *Wireless Personal Communications*, vol. 80, no. 1, pp. 117–140, 2015.

[22] Y. Ren, V. I. Zadorozhny, V. A. Oleshchuk, and F. Y. Li, "A novel approach to trust management in unattended wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 13, no. 7, pp. 1409–1423, 2014.

[23] F. Ishmanov, S. W. Kim, and S. Y. Nam, "A secure trust establishment scheme for wireless sensor networks," *Sensors*, vol. 14, no. 1, pp. 1877–1897, 2014.

[24] F. Ishmanov, S. W. Kim, and S. Y. Nam, "A robust trust establishment scheme for wireless sensor networks," *Sensors*, vol. 15, no. 3, pp. 7040–7061, 2015.

[25] B. Zhang, Z. Huang, and Y. Xiang, "A novel multiple-level trust management framework for wireless sensor networks," *Computer Networks*, vol. 72, pp. 45–61, 2014.

[26] J. Jiang, G. Han, F. Wang, L. Shu, and M. Guizani, "An efficient distributed trust model for wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 5, pp. 1228–1237, 2015.

[27] M. Mejia, N. Peña, J. L. Muñoz, O. Esparza, and M. A. Alzate, "A game theoretic trust model for on-line distributed evolution of cooperation inMANETs," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 39–51, 2011.

[28] H. Yahyaoui, "A trust-based game theoretical model for Web services collaboration," *Knowledge-Based Systems*, vol. 27, pp. 162–169, 2012.

[29] R. Feng, S. Che, X. Wang, and J. Wan, "An incentive mechanism based on game theory for trust management," *Security and Communication Networks*, vol. 7, no. 12, pp. 2318–2325, 2014.

[30] J. Duan, D. Gao, D. Yang, C. H. Foh, and H.-H. Chen, "An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 58–69, 2014.

[31] Y. Shen, Z. Yan, and R. Kantola, "Analysis on the acceptance of Global Trust Management for unwanted traffic control based on game theory," *Computers and Security*, vol. 47, pp. 3–25, 2015.

[32] Y. Li, H. Xu, Q. Cao, Z. Li, and S. Shen, "Evolutionary game-based trust strategy adjustment among nodes in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2015, Article ID 818903, 12 pages, 2015.

[33] Z. Chen, Y. Qiu, J. Liu, and L. Xu, "Incentive mechanism for selfish nodes in wireless sensor networks based on evolutionary game," *Computers and Mathematics with Applications*, vol. 62, no. 9, pp. 3378–3388, 2011.

[34] J. Lin, N. Xiong, A. V. Vasilakos, G. Chen, and W. Guo, "Evolutionary game-based data aggregation model for wireless sensor networks," *IET Communications*, vol. 5, no. 12, pp. 1691–1697, 2011.

[35] Z. Chen, C. Qiao, Y. Qiu, L. Xu, and W. Wu, "Dynamics stability in wireless sensor networks active defense model," *Journal of Computer and System Sciences*, vol. 80, no. 8, pp. 1534–1548, 2014.

[36] Z. Chen, C. Qiao, L. Xu, and W. Wu, "Optimizing wireless unicast and multicast sensor networks on the basis of evolutionary game theory," *Concurrency Computation Practice and Experience*, vol. 26, no. 5, pp. 1130–1141, 2014.

[37] J. Liu, G. Yue, S. Shen, H. Shang, and H. Li, "Coverage capacity optimization for mobile sensor networks based on evolutionary games," *International Journal of Distributed Sensor Networks*, vol. 2014, Article ID 264307, 12 pages, 2014.

[38] N. Farzaneh and M. H. Yaghmaee, "An adaptive competitive resource control protocol for alleviating congestion in wireless sensor networks: an evolutionary game theory approach," *Wireless Personal Communications*, vol. 82, no. 1, pp. 123–142, 2015.

[39] G. Jiang, S. Shen, K. Hu, L. Huang, H. Li, and R. Han, "Evolutionary game-based secrecy rate adaptation in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2015, Article ID 975454, 13 pages, 2015.

[40] M. A. Abd, S. F. M. Al-Rubeaai, B. K. Singh, K. E. Tepe, and R. Benlamri, "Extending wireless sensor network lifetime with global energy balance," *IEEE Sensors Journal*, vol. 15, no. 9, pp. 5053–5063, 2015.

[41] C. Zhu, H. Nicanfar, V. C. M. Leung, and L. T. Yang, "An authenticated trust and reputation calculation and management system for cloud and sensor networks integration," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 1, pp. 118–131, 2015.

[42] H. Zhu, S. Du, Z. Gao, M. Dong, and Z. Cao, "A probabilistic misbehavior detection scheme toward efficient trust establishment in delay-tolerant networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 1, pp. 22–32, 2014.

[43] H. Zhao, X. Yang, and X. Li, "CTrust: trust management in cyclic mobile Ad Hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 6, pp. 2792–2806, 2013.

[44] D. Fudenberg and J. Tirole, *Game Theory*, The MIT Press, London, UK, 1991.

[45] P. D. Taylor and L. B. Jonker, "Evolutionarily stable strategies and game dynamics," *Mathematical Biosciences*, vol. 40, no. 1-2, pp. 145–156, 1978.

[46] D. Fudenberg and D. K. Levine, *The Theory of Learning in Games*, The MIT Press, Cambridge, UK, 1998.

[47] G. Zhan, W. Shi, and J. Deng, "SensorTrust: a resilient trust model for wireless sensing systems," *Pervasive and Mobile Computing*, vol. 7, no. 4, pp. 509–522, 2011.