Hindawi Publishing Corporation
The Scientific World Journal
Volume 2014, Article ID 950618, 10 pages
http://dx.doi.org/10.1155/2014/950618

Research Article

A Game-Theoretic Response Strategy for Coordinator Attack in Wireless Sensor Networks

Jianhua Liu,[1] Guangxue Yue,[1] Shigen Shen,[1] Huiliang Shang,[2] and Hongjie Li[1]

[1] *College of Mathematics, Physics and Information Engineering, Jiaxing University, Jiaxing 314001, China*
[2] *Department of Electronic Engineering, Fudan University, Shanghai 200433, China*

Correspondence should be addressed to Jianhua Liu; ljh_541@163.com

Received 11 March 2014; Accepted 11 June 2014; Published 1 July 2014

Academic Editor: Fei Yu

The coordinator is a specific node that controls the whole network and has a significant impact on the performance in cooperative multihop ZigBee wireless sensor networks (ZWSNs). However, the malicious node attacks coordinator nodes in an effort to waste the resources and disrupt the operation of the network. Attacking leads to a failure of one round of communication between the source nodes and destination nodes. Coordinator selection is a technique that can considerably defend against attack and reduce the data delivery delay, and increase network performance of cooperative communications. In this paper, we propose an adaptive coordinator selection algorithm using game and fuzzy logic aiming at both minimizing the average number of hops and maximizing network lifetime. The proposed game model consists of two interrelated formulations: a stochastic game for dynamic defense and a best response policy using evolutionary game formulation for coordinator selection. The stable equilibrium best policy to response defense is obtained from this game model. It is shown that the proposed scheme can improve reliability and save energy during the network lifetime with respect to security.

1. Introduction

Both the security and the quality of service (QoS) of ZWSNs are important factors which will affect various services of sensor data delivery, for example, environmental monitoring [1], building monitoring to assess earthquake damage [2], and intelligent home monitoring [3]. On one hand, QoS is one of the key factors for various services that include diverse important parameters, that is, delay, throughput, and dropping probability of packets. Different types of services always need different requirements of QoS. On the other hand, sensor transmission always faces many malicious attacks [4]. In order to get secure network, various security protocols are presented to address security issues [5], including wired equivalent privacy (WEP), 802.1X port access control with extensible authentication protocol (EAP), and IP security protocol (IPsec) [6].

An IEEE 802.15.4 WSN is composed of one coordinator and a set of nodes [7]. The network topology defined in the standard is called cluster tree, where nodes associate with coordinators to establish parent child relationships and form a tree rooted at coordinator. Existing ZWSNs can cooperate with each other to compose sensor service and provide effective and efficient data delivery.

It is evident that sensor services have a certain requirement on both security and QoS to get good performance. Since the requirements might be different in a different circumstance or time, it may be impossible to satisfy requirements from both security and QoS simultaneously due to limited network resources. Considering only the costs of transmission without taking into account the possibility of coordinator attacked is not sufficient for providing secure composition in these environments. To avoid single point of failures owing to attack and increase network lifetime, it is desirable that the service composition based on coordinator selection method executes in a distributed manner.

Wireless sensor data can be proactively received by a coordinator owned by the same network operator. However, when a coordinator node is no longer in the reliable state, the rate of data delivery and QoS will be poor. Therefore, to

improve QoS, multiple sensor nodes can share the reliable coordinator in which case the cost of sensor data transmission for each sensor node will be reduced. In other words, multiple sensor nodes can form a coalition to share the coordinator. When the coordinator nodes in the same coalition are reliable owing to unattack, each of the sensors can fully access the coordinator. However, if one coordinator node from the same coalition is unreliable owing to heavy attack, coordinators failures can occur; therefore, a coordinator selection mechanism would be required for sensor data delivery in the same coalition. In this context, two key questions are (i) how to form coalitions among sensor nodes to share the reliable coordinator to minimize the cost of energy and (ii) how to defend attacker to meet the required QoS requirements. To answer these questions, a joint dynamic defense and coordinator selection scheme are proposed using game theoretical concepts.

Given that the sensors are rational to minimize their own cost, a game-theoretic model is developed to find a solution of the defense attack and coordinator selection problem. This game model consists of two interrelated formulations, that is, a stochastic game for dynamic attack response and evolutionary game for coordinator selecting. The stochastic game formulation utilizes the coalitional structure obtained from the evolutionary game, while the evolutionary game formulation utilizes the cost and QoS performance measures from the stochastic game.

In this paper, our main contributions can be summarized as follows.

(i) We propose a proactive scheme for defending networking coordinators. It enables the defender to proactively select reliable coordinator to minimize the expected network energy loss. To our best knowledge, this is the first work that considers defending and attacking from the perspective of games.

(ii) We formulate the problem of the defending networking coordinators as a 2-player zero-sum game. The payoff of our problem is measured by the maximum sensor service network utility. We propose an evolutionary game-theoretic framework for the defense response policy in which nodes in the network are regarded as players and the local combination of estimation information from different neighbors is regarded as different strategies of coordinator selection.

(iii) We propose a new state estimation algorithm for selecting coordinators using fuzzy logic. We prove that a global Nash equilibrium (NE) exists. We then design a mixed-strategy solution for the defender and attacker that combines the evolutionary game NE strategies and stochastic game NE strategies in order to achieve the maximum payoffs for both players.

The rest of this paper is organized as follows. Section 2 describes related works. Section 3 describes the system model. Section 4 presents the stochastic game for dynamic defense and a best response policy using evolutionary game formulation for coordinator selection. Section 5 performs numerical experiments; the influence of a cost parameter is illustrated. Section 6 concludes the paper.

2. Related Works

ZWSNs security and the quality of service (QoS) combining deployment and management related topics have become an active research area. One of the major constraints of ZWSNs deployment and management is the limited energy. It is crucial for maximizing the lifetime of ZWSNs that data packets are routed to the destination in an energy-efficient manner [8]. ZWSNs are widely studied route metrics for the number of hops [9–11]; hierarchical protocols [12, 13] group nodes into clusters and energy expenditure [14–17]. The relationship between number of hops and network energy for a single packet is investigated in [18]. Most of these approaches do not consider the reliability on the coordinator nodes that suffer attack from malicious nodes. In this paper, we study the possibility of using game theoretical approach to defend malicious nodes. To combat the attack on relay, several lightweight authentication protocols, which are based on computationally efficient hash chain, can be applied in cooperative wireless communication networks. Timed efficient stream loss tolerant authentication (TESLA) is a broadcast authentication protocol based on loose time synchronization [19]. Law et al. [20] showed how the jamming can be used to perform attacks on the network link layer protocols. Xu et al. [21] surveyed issues related to performing a jamming attack against sensor networks by examining both the attack and defense; they presented the following jamming models: constant jammer, deceptive jammer, random jammer, and reactive jammer.

Yao et al. [22] proposed a parameterized and localized trust management scheme for WSN security, particularly for secure routing, where each node only maintains highly abstracted parameters to evaluate its neighbors. Aivaloglou and Gritzalis [23] proposed a hybrid trust and reputation management protocol for WSNs by combining certificate-based and behavior-based trust evaluations. Gabrielli et al. [24] analyzed the security vulnerabilities of PEAS, ASCENT, and CCP and represented securing topology maintenance protocols. Bao et al. [25] considered multidimensional trust attributes derived from communication and social networks to evaluate the overall trust of a sensor node. Zonouz et al. [26] employed a game-theoretic response strategy against adversaries modeled as opponents in a two-player Stackelberg stochastic game and proposed fuzzy logic theory to calculate the network-level security metric values. However, [24–26] do not provide response strategy against attackers for coordinators.

Game theory provides a rich set of tools that can be used to model the attack behavior of malicious nodes. Game theory models were applied to solve various issues in wireless networks. In [27], a stochastic game was formulated for network selection problem in cognitive heterogeneous networks. In [28], an evolutionary game model was used to analyze the information diffusion process and the filtering over the adaptive networks. In this paper, we use stochastic and

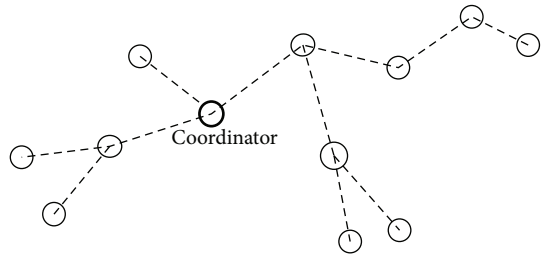


Figure 1: Selecting coordinator coalitional game model.

evolutionary game theory to study the cooperative defense behavior of sensors for coordinator selection under security constraints.

3. System Model

3.1. ZWSN Functionality and QoS. Each node typically provides a basic functionality for operating on the monitored data; sensors provide their functionalities through receiving and forwarding operations. That is, a data packet comes to a sensor, and the sensor receives and forwards to coordinator, while the network of sensor nodes collectively provides a composite service to the end nodes. Unlike the web environment where service provider availability and ample communication bandwidth are typically assured, sensor networks are highly dynamic as nodes often fail or become disconnected and wireless communication capacity is limited. The operation of every ZWSN is associated with two QoS attributes: the average number of hops to the coordinator (hop for minimization) and energy cost (energy for minimization). Energy cost is defined as the fee that a ZWSN consumer has to pay to receiving and forwarding operations. Hop is defined as the total length of path covered between the source of the sensor and the coordinator. Figure 1 illustrates the forwarding and selecting coordinator coalitional game model. Cluster coalition can communicate with other coalitions by coordinators. Not only can a coordinator request or be invited to join a coalition, but also it can leave a coalition. Every coalition has a coordinator and a set of sensors as its members. The coordinator is responsible for receiving and forwarding data and managing the cooperation among these members.

In a coalition, coordinator is the controller of the network and it is responsible for initiating the network set-up; it starts by selecting a suitable communication channel. This selection is performed by the energy detection scan which assesses the level of interference on each channel by measuring the peak energy on each available channel. If a node is available, it selects a node to join coalition; this node starts an exchange of signaling packets with the chosen coordinator to complete formation coalition. A cooperation coalition is managed by the coordinator, which is a sensor composition $S = [s[1], \ldots, s[n]]$ of the coalition members $\{1, \ldots, n\}$; once the coordinator receives a sensor's request, it forwards $s[1]$. If $s[1]$ is available, the coordinator will send data to $s[1]$. Otherwise, it will forward $s[2]$. This process continues until a sensor is available and data is delivered to destination node. Suppose sense i's availability is a_i. Clearly, the resource availability of the coalitions M is given by

$$a_r = 1 - \prod_{i=1}^{n} (1 - a_i). \tag{1}$$

As a coalition can be regarded as a composite sensor, it also possesses other performance metrics as discussed earlier. In particular, its price p_M relies on its availability. Besides, following the widely accepted assumption that the cost of a composite sensor totally depends on the cost of the average number of hops to the coordinator and energy cost, the cost of a coalition M is given by

$$c_M(s) = \sum_{i=1}^{n} \prod_{j=1}^{i-1} \left(1 - a_{s[j]}\right) c_{s[i]}, \tag{2}$$

where $c_{s[i]}$ is the cost of coalition $s[j]$. Let h_i be the average number of hops from the node k to the coordinator. The energy cost for a single packet can be calculated as follows: $c_{s[i]} = (E_r + E_f) \times h_i \times N_i$, where E_r and E_f are energy of the receiving and forwarding, respectively. N_i is the number of nodes in coalition i. The value of a coalition M is a sensor composition S given by $v_M(s) = p_M \times a_M - c_M(s)$.

3.2. Stochastic Game for Coordinator Attack. In this section, we present the game-theoretic formulation of the self-organized network selection problem. We model the coordinator attacked problem as a noncooperative game where the malicious sensors are the attackers, the coordinator sensors are the defenders, and the coordinator run state is considered as the internal state (*NormalState* (NS) or *HackedState* (HS)). The game is represented as

$$G = \left(N, Z, \{A_k\}_{k \in N}, \{u_k\}_{k \in N}\right), \tag{3}$$

where N is the set of players, $N = \{1, 2\} = \{\text{attacker, defender}\}$.

Z is the space of states, $Z_i = \{\text{NS, HS}\}$, and $\{A_i\}_{i \in N}$ is the set of actions (attack and defense) that player i can take. $A_i = \{a_i, r_i, d_i, \emptyset_i\}$; a_i is the attack action bringing the coordinator from state *NormalState* to *HackedState*. r_i is the resignation of the attack in state *NormalState*. d_i represents that the attack action a_i will be detected by the defender. $\emptyset_i$ represents that the attack a_i action will be undetected.

$\{u_i\}_{i \in N}$ is the utility function of player i. The defenders aim at maximizing the network lifetime with carefully-designed coordinator selecting schedules, while the malicious attackers want to decrease the network lifetime by strategic jamming. Therefore, they have opposite objectives and their dynamic interactions can be well modeled as a noncooperative (zero-sum) game. The coordinators as defenders are cooperative and rational players with the objective of maximizing their network throughput and decreasing the average number of hops and energy cost to itself. Thus, we define the utility function as defender's expected payoff for a choice of action as

$$u_i(a_i, a_{-i}) = E\left[v_i(s) \mid (a_i, a_{-i})\right] = \sum_{a \in A} p(a)\, v_k(a). \tag{4}$$

The choice of defender i that maximize defender i's expected payoff over its action space A_k is called the player's best response action. The decision making of defender i in a game then becomes

$$(G): \max_{a_i \in A_k} u_i\left(a_i, a_{-i}\right), \quad \forall i \in N. \tag{5}$$

3.3. Best Response Policy Using Evolutionary Game Formulation. Given a network topology denoted as a directed graph $G = (N, E)$, N is the set of nodes and E is the set of arcs. Each node $i \in N$ has the initial resource availability a_i. Let r_i be the self-resistance of node i to attacks. Let x_i and y_i be the defending and attacking resource allocated to defenders and attackers, respectively. We adopt the contest model proposed in [29] where the resource availability loss ratio of node i is given by

$$\tau_{ij}\left(x_i\right) = \frac{\left(y_i\right)^m}{\alpha_i\left(r_i + x_i\right)^m + \left(y_i\right)^m}, \tag{6}$$

where $m \in (0, 1]$ reflects the nonlinearity or linearity of the loss ratio on node i, and α_i is a parameter reflecting the relative difficulties for the defender to protect in a particular node compared with the attacker. When $\alpha_i \in (0, 1)$, the defender has to allocate more resources than the attacker in order to mitigate the effect of the attack, while $\alpha_i > 1$ means that the defender can easily detect and mitigate the effect of the attack. The payoff of a coalition M is a sensor composition S rewritten as

$$v_M^a(s) = p_M \times a_M - c_M(s) - \tau_M(s). \tag{7}$$

Let A_0 be the original sensor composition S resource availability without suffering from any attack. For the defender, its goal is to maximize the payoff $v_M^a(s)$ over x to protect the maximum network QoS by selecting coordinator as much as possible. On the other hand, the attacker aims to minimize $v_M^a(s)$ by attacking key coordinator nodes or, equivalently, maximize $A_0 - v_M^a(s)$ over y. Equation (7) suggests that $v_M^a(s)$ can be increased if $c_M^a(s)$ can be reduced. It is to be noticed that $c_M(s)$ depends on h_i, E_r, and E_f; a reduction of h_i, E_r, and E_f also reduces $c_M(s)$. This can be obtained by evolutionarily selecting the coordinator position and deciding its reliability state. For coordinator node i with degree d_i (not including node itself) and coalition set $\{i_1, \ldots, i_{d_i}\}$, the general parameter updating rule can be written as

$$\begin{aligned} h_{i,t+1} &= B_{i,t+1}\left(\Phi\left(h_{i1,t}\right), \Phi\left(h_{i2,t}\right), \ldots, \Phi\left(h_{id_i,t}\right)\right) \\ &= \sum_{l \in w} \sum_{j \in N} B_{i,t+1}(j,l)\, \Phi\left(h_{j,l,t}\right), \end{aligned} \tag{8}$$

where $\Phi(\cdot)$ can be any adaptive role configuration function. $B_{i,t+1}$ represents some specific linear combination rules, w represents the number of coalitions, and N denotes the number of coalitions members.

Evolutionary game theory (EGT) is originated from the study of ecological biology [30], which differs from the classical game theory by emphasizing more on the dynamics and stability of the whole population's strategies, instead of only the property of the equilibrium. Such an equilibrium strategy is defined as the evolutionarily stable strategy (ESS).

Let us consider an evolutionary game with k strategies $\theta = \{1, 2, \ldots, k\}$. The utility matrix U is a matrix $k \times k$, whose entries γ_{ij} denote the payoff for strategy i versus strategy j. The population fraction of strategy i is given by p_i, where $0 < p_i < 1$, $i \in \{1, \ldots, k\}$. The fitness of strategy is given by $f_i = \sum_{j=1}^{k} p_j \gamma_{ij}$. For the average fitness of the whole population, we have $\eta = \sum_{i=1}^{k} p_i f_i$. The Wright-Fisher model has been widely adopted to let a group of players converge to the ESS [27], where the strategy updating equation for each player can be written as

$$p_i(t+1) = \frac{p_i(t)\, f_i(t)}{\eta(t)}. \tag{9}$$

From (8), it can be seen that the strategy updating process in the evolutionary game is similar to the position parameter updating process in adaptive selecting of the coordinator problem. It is intuitive that we can use evolutionary game to formulate the distributed adaptive selecting of the coordinator position problem. Given the definition of the players, strategy space, and payoffs, the maximum network QoS of evolutionary game Ω can be defined as

(i) players: defender, attacker,

(ii) strategy: θ_{ij},

(iii) payoffs: $v_M^a(s)$, $A_0 - v_M^a(s)$.

Each coordinator node represents a defense player; θ_{ij} denotes the probability that the strategy of node i will replace that of node j from its neighbor. We first discuss how players' strategies are updated in EGT, which is then applied to the position parameter updating in distributed adaptive coordinator selection. In EGT, the fitness of a player is locally determined from interactions with all adjacent players, which is defined as

$$f = (1 - \lambda) \cdot v_m(s) + \lambda \cdot v_M^a(s), \tag{10}$$

where λ parameter represents the selection of new coordinator node intensity, that is, the relative contribution of the game to fitness. The case $\lambda \to 0$ represents the limit of weak selection of new coordinator node owing to jam weak attack, while $\lambda = 1$ denotes strong selection, where fitness equals payoff. There are two different strategy updating rules for the evolution dynamics called AC, TC.

(i) AC (alternative coordinator) update rule: a coordinator player is chosen to abandon his/her current coordinator role. Then, the chosen player selects one of its neighbors as coordinator with the probability of being proportional to their fitness; its neighbor copies its strategy and configuration, as shown in Figure 2(a).

(ii) TC (temporary coordinator) update rule: a neighbor player adopts the strategy and configuration of one coordinator as a temporary coordinator node and

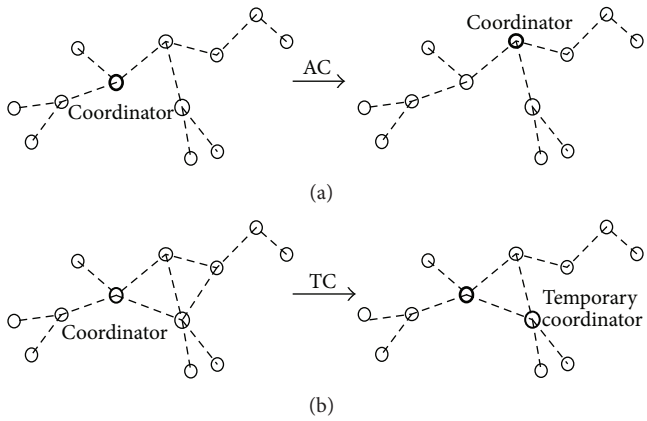


Figure 2: (a) Alternative coordinator. (b) Temporary coordinator.

remains with its current strategy; old coordinator configures as a temporary ordinary (TO) node, with the probability of being proportional to fitness. Moreover, the neighbor player keeps the strategy and configuration until the jamming attack weakens and old coordinator node recovers its role, as shown in Figure 2(b).

These two kinds of strategy updating rules can be matched to two different kinds of position parameter updating algorithms in distributed adaptive coordinator selection. The degree of coordinator node i is d_i. We use N to denote the set of all nodes in a coalition.

For the AC update rule, the probability that the coordinator player selects and configures one of its neighbors j as coordinator is

$$P_j = \frac{f_j}{\sum_{q\in N} f_q}\frac{1}{\Gamma_j}, \tag{11}$$

where the $f_j/\sum_{q\in N} f_q$ is the probability that the neighboring node j is chosen to act as coordinator, and $1/\Gamma_j$ is the probability that node j is chosen for copying coordinator's strategy and updating configuration. The equivalent parameter updating rule for ZWSN can be written as

$$\begin{aligned} h_{i,t+1} = {} & \left(\frac{f_j}{\sum_{q\in N} f_q}\frac{1}{\Gamma_j}\right)\Phi_{\mathrm{AC}}\left(h_{j,t}\right) \\ & + \left(1 - \frac{f_j}{\sum_{q\in N} f_q}\frac{1}{\Gamma_j}\right)\sum_{i\in w\cup N\setminus\{j\}}\Phi\left(h_{i,t}\right), \end{aligned} \tag{12}$$

where the first term is that the neighboring node is chosen for configuration as an alternative coordinator, and the second term is that all nodes are configured as a new average hop from source node to new coordinator.

For the TC update rule, the equivalent parameter updating rule for ZWSN can be written as

$$\begin{aligned} h_{z,t+1} = {} & \left(\frac{f_j}{\sum_{q\in N} f_p}\frac{1}{\Gamma_j}\right)\Phi_{\mathrm{TC}}\left(h_{j,t}\right) \\ & + \left(\frac{f_j}{\sum_{q\in N} f_p}\frac{1}{\Gamma_j}\right)\Phi_{\mathrm{TO}}\left(h_{i,t}\right) \\ & + \left(1 - \frac{f_j}{\sum_{q\in N} f_p}\frac{1}{\Gamma_j}\right)\sum_{z\in w\cup N\setminus\{j,i\}}\Phi\left(h_{z,t}\right), \end{aligned} \tag{13}$$

where the first term is that the neighboring node is chosen for configuration as a temporary coordinator, the second term is that it itself is configured as a temporary ordinary node, and the third term is that all nodes are configured as a new average hop from source node to new temporary coordinator. The payoff of a coalition M is a sensor composition S rewritten by

$$v_M^a(s) = p_M \times a_M - c_M(s) - \tau_M(s) - c_\Phi(s), \tag{14}$$

where $c_\Phi(s)$ is the cost of configuration. Its immediate reward for a cluster sensor with n coordinators is defined as a weighted sum of the performance of a cluster sensor:

$$r_\Phi = \sum_{i=1}^{n}\left(w_i \cdot c_\Phi^{\mathrm{AC}}(i) + (1-w_i)\cdot\left(c_\Phi^{\mathrm{TC}}(i) + c_\Phi^{\mathrm{TO}}(i)\right)\right), \tag{15}$$

where $w_i < 1$. The "goodness" of a configuration action in a given evolutionary state is measured by a value function $Q(Z, a)$; we employ temporal-difference (TD) method for configuration function update:

$$\begin{aligned} Q\left(Z_t, a_t\right) \longleftarrow {} & Q\left(Z_t, a_t\right) \\ & + \omega\cdot\left[r_{\Phi,t+1} + \xi\cdot Q\left(Z_{t+1}, a_{t+1}\right) - Q\left(Z_t, a_t\right)\right], \end{aligned} \tag{16}$$

where ω is a learning rate parameter that facilitates convergence in the presence of stochastic transitions.

4. FQL Based Reinforcement Learning for Coordinator Selection

4.1. Fuzzy Logic. Fuzzy logic is a mathematical approach to emulate human way of thinking and learning. Fuzzy systems have been used as function approximating to facilitate generalization in state space for generating continuous actions. We propose fuzzy Q learning (FQL) [10] to a fuzzy evolutionary game decision (FEGD) setting. The proposed FEGD takes into account the channel occupied information with respect to the coordinator (C_o) and the amount of remaining battery energy of that coordinator (E_b). Their degree of relevance is expressed as a function $\chi = f(C_o, E_b)$, where χ denotes "selection level" or "quality" of the coordinator. In FEGD system, the input linguistic parameters are the amount of channel occupied with coordinator (C_o) and the amount of remaining battery energy of that coordinator (E_b). The

term sets for each input linguistic parameter are defined, respectively, as

$$T(C_0) = \{\text{Low (LO)}, \text{High (HG)}\},$$
$$T(E_0) = \{\text{Low (LO)}, \text{Moderate (ME)}, \text{High (HG)}\}. \quad (17)$$

The output linguistic parameter that is the possibility of coordinator selection is defined as

$$O(\chi) = \{\text{Low (LO)}, \text{Moderate (ME)}, \text{High (HG)}\}. \quad (18)$$

The fuzzy rules matrix is also summarized in Table 1. Following FQL, we define fuzzy inference system for fuzzy evolutionary game as consisting of 4 rules of the following form.

(1) IF C_0 is HG AND E_0 is HG THEN χ is HG.

(2) IF C_0 is HG AND E_0 is ME THEN χ is ME.

(3) IF C_0 is LO AND E_0 is ME THEN χ is ME.

(4) IF C_0 is LO AND E_0 is HG THEN χ is ME.

There are a number of shapes that can be used for the membership function of each input such as trapezoidal and Gaussian shapes. We have chosen the Gaussian shape, since it is common in engineering applications and easy to use. A Gaussian fuzzy set membership degree in name is defined as follows:

$$\mu_A(x) = \exp\left(-\frac{(x-\varepsilon)^2}{2\sigma^2}\right), \quad (19)$$

where ε and σ are the fuzzy number mean and standard deviation and are assigned initially, $\mu_A : U \rightarrow [0,1]$, for instance, to quantify the rule shown in Table 1 for the input $f(0.4, 0.5)$, using (19) to calculate the $\mu_A(0.4) = 0.14$, $\mu_A(0.5) = 0.01$, $\varepsilon = 0.2$, and $\sigma = 0.1$. The main remaining part is how to quantify the logical "and" operation that combines the meaning of two linguistic terms into a single premise. Consider

$$f_A = (0.4, 0.7) = \mu_A(0.4 \wedge 0.5) = \min\{0.14, 0.01\} = 0.01. \quad (20)$$

Finally, the numerical result of this fuzzy operation, defuzzification, is the last step in the operating procedure of the fuzzy inference mechanism; we use the most common method called a center of gravity. This method converts the fuzzy set into the value for which the area under the graph of the membership function, $\chi = f(C_o, E_b)$, is given by computing the center of gravity (CoG) of the area at the center:

$$\mu_A^* = \frac{\sum_{i=1}^{n} \mu_A(x_i) \times x_i}{\sum_{i=1}^{n} \mu(x_i)}. \quad (21)$$

4.2. Stochastic Learning Procedure. Here, we discuss obtaining the NE via stochastic evolutionary learning. As the attacker strategy is time-varying and the defense action is selected by each player simultaneously. We propose a decentralized algorithm based on stochastic evolutionary learning (SEL), by which the coordinator learn toward the equilibrium strategy from their individual action-reward history.

Table 1: The fuzzy rule matrix.

E_0/C_0	LO	HG
LO	LO	LO
ME	ME	ME
HG	ME	HG

To facilitate the development of the SEL-based algorithm, let the mixed strategy $P_i(t) = [p_{i,1}(t), \ldots, p_{i,M}(t)]$ the coordinator selection probability vector for player i, where $p_{i,a_i}(t)$ is the probability that player i selects strategy $a_i \in A_i$ at time t. The proposed self-organized defense algorithm by selecting coordinator is described in Algorithm 1.

Algorithm 1. Self-organized defense by selecting coordinator (SoDSC):

(1) Initially, set $t = 0$ and the coordinator selection probability vector as $p_{i,a_i}(t) = 1/\Gamma_j$.

(2) At every time t, each player selects an action $a_i(t)$ as the outcome of a probabilistic strategy based on $P_i(t)$.

(3) The coalitions receive the instantaneous reward $v_i(t)$ specified.

(4) Each coordinator in coalitions updates its selection probability vectors according to the following rules:

CID = getcurrent_node (ID)

CRS = Get_CoordinatorResourceState (CID) using FQL coordinator selection.

REPEAT

IF CRS = HG

$$h_{i,t+1} \longleftarrow h_{i,t} \text{ according to (12)}$$
$$p_{i,a_i}(t+1) \longleftarrow p_{i,a_i}(t) + \bar{\omega} \cdot h_{i,t+1}(1_{\{a_i = d_i\}} - p_{i,a_i}(t))$$

$$Q(Z_{t+1}, a_{t+1}) \longleftarrow Q(Z_t, a_t) + \omega \cdot \left(\sum_{i=1}^{n} \left(w_i \cdot c_{\Phi}^{\text{AC}}(i)\right) + \xi \cdot Q(Z_{t+1}, a_{t+1}) \cdot 1_{\{a_i = \Phi_{\text{AC}}\}} - Q(Z_t, a_t)\right). \quad (22)$$

ELSE, IF CRS = ME

$$h_{z,t+1} \longleftarrow h_{z,t} \text{ according to (13)}$$

$$p_{i,a_i}(t+1) \longleftarrow p_{i,a_i}(t) + \varpi \cdot h_{z,t+1}(1_{\{a_i=d_i\}} - p_{i,a_i}(t))$$

$$Q(Z_{t+1}, a_{t+1}) \longleftarrow Q(Z_t, a_t) + \omega \cdot \left(\sum_{i=1}^{n} \left((1-w_i) \cdot \left(c_{\Phi}^{\mathrm{TC}}(i) + c_{\Phi}^{\mathrm{TO}}(i) \right) \right) + \xi \cdot Q(Z_{t+1}, a_{t+1}) \cdot 1_{\{a_i=\Phi_{\mathrm{TC}\wedge\mathrm{TO}}\}} - Q(Z_t, a_t) \right). \tag{23}$$

(5) *UNTIL* value function converges,

where $0 < \varpi < 1$ is the learning rate. $1_{\{\cdot\}}$ is the indicator function. $h_{i,t+1}$ or $h_{z,t+1}$ is the normalized reward.

The instantaneous reward serves as a reinforcement signal so that a high reward brings a high probability in the next strategy update (Step 4). Also note that coordinator selection based on a probabilistic experiment (Step 2) might result in reconfiguration between different evolutionary rules in the beginning of the learning procedure. However, a stable long-term best response strategy for defending will be yielded after the learning period and the time required for convergence is a small fraction of the total operation time.

Algorithm 2. Get_CoordinatorResourceState (CID):

(1) Initialization: C_o, E_b.

(2) Use (19) to calculate $\mu_A(C_o)$'s and $\mu_A(E_b)$'s for $T(C_0)$ and $T(E_0)$, respectively, given by (17) and (18).

(3) Combine $T(C_0)$ and $T(E_0)$ using Table 1 to form $O(\chi)$.

(4) Calculate the $\mu_A(C_o \wedge E_b)$'s $O(\chi)$ resulting from step 3 as $\mu_A(O(\chi)) = \min\{\mu_A(C_o), \mu_A(E_b)\}$.

(5) Calculate the output of defuzzification $\chi = f(C_o, E_b) = \mu_A^*$ according to (21).

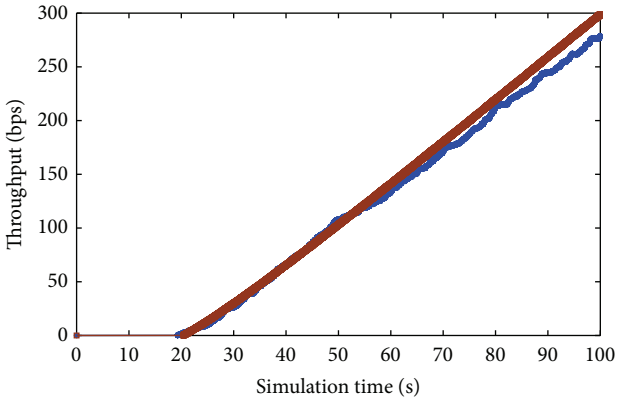
(6) Return $O(\chi)$.

Algorithm 2 describes the proposed fuzzy logic-based coordinator resource state decision algorithm from the point of view of a single coordinator node C_i. Moreover, we also assume that the relay C_i is able to read its battery level $E_{b,i}$ and estimate $C_{o,i}$ using the ACK message from the coordinator.

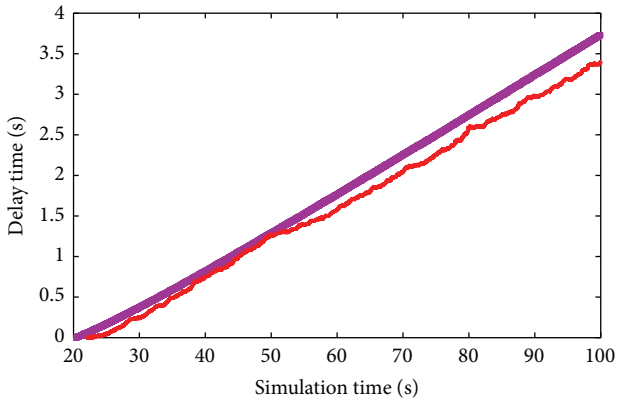
Proposition 3. *The SoDSC Algorithm converges to NE when the learning rate ϖ, ω is sufficiently small.*

Proof. Let limit P of the interpolated process satisfies the ODE [31] and consists of N probability vectors.

Let $P^d = (P_1^d, \ldots, P_N^d)$ be the mixed strategy of all players, which are denoted by P_{ij}^d. Let $\Theta(P_i^d) = E[u_i^e]$ and $\Upsilon(P_j^d) = E[\Phi_j^c]$ be the expected response reward function of player i and the expected configuration function, respectively, over the mixed strategy P^d. Ψ also has the same number of mixed strategy which will be denoted as Ψ_{ij}. The component equations of (12)–(17) are



(a)



(b)

Figure 3: (a) The throughput related to the new topology for coordinator attacks. (b) The delay related to the new topology for coordinator attack.

$$\frac{dp_{i,a_i}(t)}{dt} = p_{i,a_i}(t) \sum_{a_i'} p_{i,a_i'}(t) \left[\Theta_i(\pi_i, P_{-i}) - \Theta_i(\pi_{i'}, P_{-i}) \right]$$

$$\frac{dQ_{z,a_j}(t)}{dt} = Q_{z,a_j}(t) \sum_{a_j'} q_{z,a_j'}(t) \left[\Upsilon_j(\pi_j, P_{-j}) - \Upsilon_i(\pi_{j'}, P_{-j}) \right]$$

$$\frac{d\Psi_{ij}(P^d)}{dt} = \sum_i \sum_j \frac{\partial \Psi_{ij}(P^d)}{\partial p_{i,j}} \frac{dp_{i,a_i}(t)}{dt} \frac{dQ_{z,a_j}(t)}{dt} = p_{i,a_i}(t) \cdot p_{i,a_i'}(t) \cdot \Theta(\pi, P) \cdot Q_{z,a_j}(t) \cdot q_{z,a_j'}(t) \cdot \Upsilon(\pi, P) \geq 0, \tag{24}$$

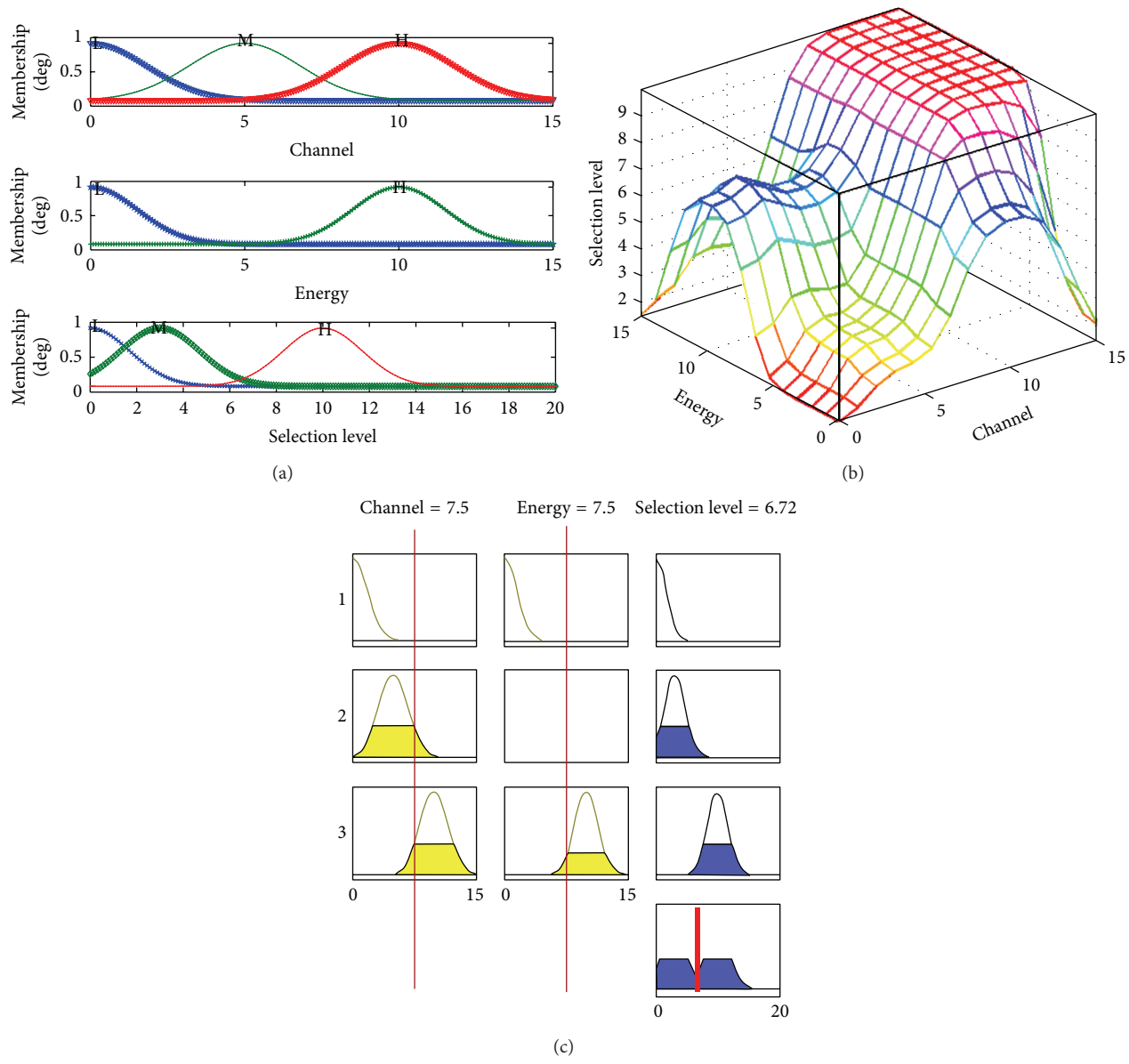


FIGURE 4: (a) Membership function for selection of coordinator. (b) The fuzzy inference for selection of coordinator. (c) The fuzzy inference process for selection of coordinator.

where

$$\Theta(\pi, P) = \Theta_i(\pi_i, P_{-i}) - \Theta_i(\pi_{i'}, P_{-i}),$$
$$\Upsilon(\pi, P) = \Upsilon_j(\pi_j, P_{-j}) - \Upsilon_i(\pi_{j'}, P_{-j}). \quad (25)$$

$\Theta(\pi, P)$ and $\Upsilon(\pi, P)$ always have the same sign and are greater than zero. While the convergence to an NE is guaranteed as $\varpi \to 0, \omega \to 0$. A smaller value of ϖ, ω leads to a slower convergence rate. A proper value of ϖ, ω can be numerically determined to strike the desired tradeoff between the accuracy and the rate of convergence for practical operations of the algorithm. □

5. Simulation

An extensive simulation evaluation of dynamic defense and response strategy is reported in this section. We carry out our experiments using the Network Simulator 2 version 2.34 tool, which is a simulator implementing physical and MAC layers of the IEEE 802.15.4 standard. We first show that dynamic defense and response strategy increases average throughput by selecting unattacked coordinator to form a new network topology, hence a new coordinator, starting from the initial IEEE 802.15.4/ZigBee cluster trees. We also show the network lifetime increase over the basic IEEE 802.15.4/ZigBee configuration when fuzzy logic and evolutionary game for the defense response policy are applied to a network with coordinators failures owing to heavy attacks.

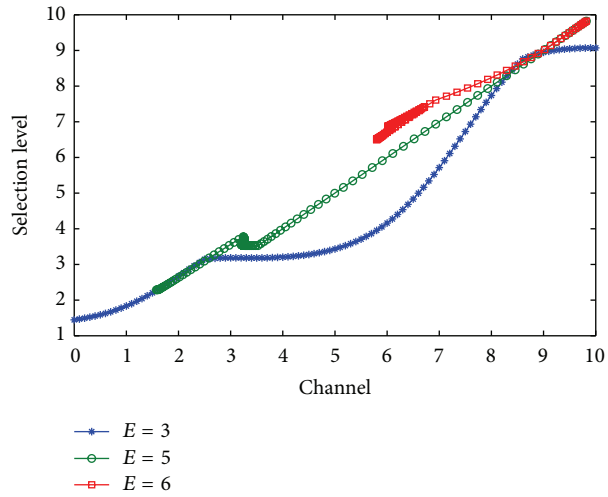


Figure 5: Effect of $E = 3$, $E = 5$, and $E = 6$ on the selection level for coordinator in face of jam attack.

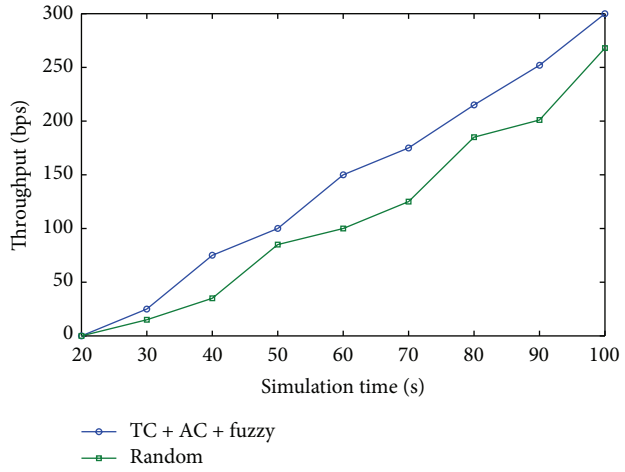


Figure 6: End-to-end throughput with $K = 20$ nodes.

Table 2: Simulation scenarios.

Parameters	Value
Protocols	AODV, Mac/802.15.4
Number of nodes	20
Simulation area	50 × 50
Traffic type	cbr, Poisson
Packet size	70 Bytes
Packets rate	250 k
Distance	5 m, 9 m, 10 m, 11 m, and 12 m
Simulation time	100 s

This section shows a comparison, in terms of jamming attack for cluster trees; network topology is formed with fuzzy logic and evolutionary game. We consider a network scenario consisting of N nodes, randomly deployed in a square area. The nodes' transmission range is reported in Table 2. At the beginning of each experiment the initial coordinator is randomly selected.

As for the physical layer Network Simulator-2 implements all primitives described in the IEEE 802.15.4 Standard and uses the two-ray ground propagation model. Each packet received at the physical layer should be above the receive threshold value, that is assumed to be equal to 3.24×10^{-10} W to be correctly received. By varying the position of coordinator node and jamming attack on the field, we repeat the IEEE 802.15.4 association procedure for N times. At the end of the procedure we record the throughput related to the new topology for coordinator attack. Figures 3(a) and 3(b) show throughput and delay of defense for coordinator attack, respectively, and the results for IEEE 802.15.4 and selection of coordinator using Algorithm 1. When a network has a high jam attack, coordinator improves the topology configuration for defending jam attack by game selection; game selection has the same throughput and delay as IEEE 802.15.4 that is not selection of coordinator in face of jam attack. This is because the game selection Algorithm 1 uses TC and AC rules to select coordinator and keep higher throughput to approximate to IEEE 802.15.4 that does not face jam attack. Moreover, shorter routing paths can be established between any node and the coordinator, which saves node's energy and reduces data delivery delay.

Figures 4(a), 4(b), and 4(c) show the fuzzy inference for selection coordinator in face of jam attack. Figure 5 shows energy effect of $E = 3$, $E = 5$, and $E = 6$ on the selection level for coordinator in face of jam attack. Figure 6 shows that, by selecting coordinator, the throughput of networks is increased, for different selection coordinator methods for defending jam attack. Performance of the proposed algorithm shows that, by game selection and fuzzy inference, the throughput of networks is increased up to 300 bps (for a Zigbee network with 20 nodes) with TC + AC + Fuzzy rules, while the throughput of networks is increased up to 275 bps with random selection coordinator.

6. Conclusion

We have presented a coordinator selection scheme for ZWSNs to defend action from malicious nodes and minimize the cost of wireless transmission energy. By exploiting coordinator selection among multiple sensor nodes, the path security and reliability can be improved and the cost of data transmission can be reduced by selecting rules. We have formulated a game-theoretic model for joint dynamic defense and response strategy, taking into account the fact that each sensor node is rational to maximize its own payoff. The proposed game model is composed of two formulations, that is, a stochastic game for dynamic attack response and evolutionary game for coordinator selecting. The solutions of these games can achieve Nash equilibrium for the attack response strategy game.

Conflict of Interests

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

Acknowledgments

This work was partly supported by the National Natural Science Foundation of China under Grant no. 61272034; Zhejiang Provincial Natural Science Foundation of China under Grant nos. LY12F02019 and LY13F030012; Research Start-up Foundation of Jiaxing University under Grant no. 70512020; and Scientific Research Foundation of Zhejiang Provincial Education Department of China under Grant no. Y201431192.

References

[1] H. Yang, Y. Qin, G. Feng, and H. Ci, "Online monitoring of geological CO_2 storage and leakage based on wireless sensor networks," *IEEE Sensors Journal*, vol. 13, no. 2, pp. 556–562, 2013.

[2] T. Torfs, T. Sterken, S. Brebels et al., "Low power wireless sensor network for building monitoring," *IEEE Sensors Journal*, vol. 13, no. 3, pp. 909–915, 2013.

[3] N. K. Suryadevara and S. C. Mukhopadhyay, "Wireless sensor network based home monitoring system for wellness determination of elderly," *IEEE Sensors Journal*, vol. 12, no. 6, pp. 1965–1972, 2012.

[4] D. E. Tiliute, "Security of mobile ad hoc wireless networks: a brief survey," *Advances in Electrical and Computer Engineering*, vol. 7, no. 2, pp. 37–40, 2007.

[5] N. L. S. Da Fonseca, "Second quarter 2009 IEEE communications surveys and tutorials," *IEEE Communications Surveys and Tutorials*, vol. 11, no. 2, pp. 1–2, 2009.

[6] C. Tang and D. O. Wu, "An efficient mobile authentication scheme for wireless networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 4, pp. 1408–1416, 2008.

[7] Zigbee specification, 2006, http://www.zigbee.org/.

[8] C. Chong and S. P. Kumar, "Sensor networks: evolution, opportunities, and challenges," *Proceedings of the IEEE*, vol. 91, no. 8, pp. 1247–1256, 2003.

[9] C. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," in *Proceedings of the Conference on Communications Architectures, Protocols and Applications (SIGCOMM '94)*, pp. 234–244, London, UK, 1994.

[10] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in *Mobile Computing*, T. Imielinski and H. F. Korth, Eds., pp. 153–181, Kluwer Academic Publishers, 1996.

[11] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '99)*, pp. 90–100, New Orleans, La, USA, February 1999.

[12] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless sensor networks," in *Proceedings of the Hawaii International Conference System Sciences*, vol. 8, pp. 1–10, 2000.

[13] S. Lindsey and C. S. Raghavendra, "PEGASIS: power-efficient gathering in sensor information systems," in *Proceedings of the IEEE Aerospace Conference*, vol. 3, pp. 1125–1130, Big Sky, Mont, USA, March 2002.

[14] J. Chang and L. Tassiulas, "Maximum lifetime routing in wireless sensor networks," *IEEE/ACM Transactions on Networking*, vol. 12, no. 4, pp. 609–619, 2004.

[15] M. Zimmerling, W. Dargie, and J. M. Reason, "Energy-efficient routing in linear wireless sensor networks," in *Proceedings of the IEEE Internatonal Conference on Mobile Adhoc and Sensor Systems (MASS '07)*, pp. 1–3, Pisa, Italy, October 2007.

[16] F. Shao, X. Shen, and L. Cai, "Energy efficient reliable routing in wireless sensor networks," in *Proceedings of the 1st International Conference on Communications and Networking in China (ChinaCom '06)*, pp. 1–5, Beijing, China, October 2006.

[17] H. Chang and L. Tassiulas, "Energy conserving routing in wireless ad hoc networks," in *Proceedings of the IEEE INFOCOM*, pp. 22–31, Tel-Aviv, Israel, 2000.

[18] F. Cuomo, A. Abbagnale, and E. Cipollone, "Cross-layer network formation for energy-efficient IEEE 802.15.4/ZigBee Wireless Sensor Networks," *Ad Hoc Networks*, vol. 11, no. 2, pp. 672–686, 2013.

[19] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 56–73, May 2000.

[20] Y. W. Law, L. van Hoesel, J. Doumen, P. Hartel, and P. Havinga, "Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols," in *Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '05)*, pp. 76–88, November 2005.

[21] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: attack and defense strategies," *IEEE Network*, vol. 20, no. 3, pp. 41–47, 2006.

[22] Z. Yao, D. Kim, and Y. Doh, "PLUS: parameterized and localized trust management scheme for sensor networks security," in *Proceedings of the IEEE International Conference on Mobile Ad Hoc and Sensor Sysetems (MASS '06)*, pp. 437–446, October 2006.

[23] E. Aivaloglou and S. Gritzalis, "Hybrid trust and reputation management for sensor networks," *Wireless Networks*, vol. 16, no. 5, pp. 1493–1510, 2010.

[24] A. Gabrielli, L. V. Mancini, S. Setia, and S. Jajodia, "Securing topology maintenance protocols for sensor networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 3, pp. 450–465, 2011.

[25] F. Bao, I. Chen, M. Chang, and J. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," *IEEE Transactions on Network and Service Management*, vol. 9, no. 2, pp. 169–183, 2012.

[26] S. A. Zonouz, H. Khurana, W. Sanders, and T. Yardley, "RRE: a game-theoretic intrusion response and recovery engine," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 395–406, 2013.

[27] L.-C. Tseng, F.-T. Chien, D. Zhang, R. Y. Chang, W.-H. Chung, and C. Y. Huang, "Network selection in cognitive heterogeneous networks using stochastic learning," *IEEE Communications Letters*, vol. 17, no. 12, pp. 2304–2307, 2013.

[28] C. X. Jiang, Y. Chen, and K. J. R. Liu, "Distributed adaptive networks: a graphical evolutionary game-theoretic view," *IEEE Transactions on Signal Processing*, vol. 61, no. 22, pp. 5675–5688, 2013.

[29] S. Skaperdas, "Contest success functions," *Economic Theory*, vol. 7, no. 2, pp. 283–290, 1996.

[30] J. M. Smith, *Evolution and The Theory of Games*, Cambridege University Press, Cambridge, UK, 1982.

[31] P. S. Sastry, V. V. Phansalkar, and M. A. L. Thathachar, "Decentralized learning of Nash equilibria in multi-person stochastic games with incomplete information," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 24, no. 5, pp. 769–777, 1994.