Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2012, Article ID 793194, 9 pages
doi:10.1155/2012/793194

Research Article

On Optimal Antijamming Strategies in Sensor Networks

Yanmin Zhu[1,2] and Yuan Jiang[1,2]

[1] *Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China*
[2] *Shanghai Key Lab of Scalable Computing and Systems, Shanghai Jiao Tong University, Shanghai 200240, China*

Correspondence should be addressed to Yanmin Zhu, yzhu@cs.sjtu.edu.cn

Received 28 October 2011; Accepted 6 February 2012

Academic Editor: Zhen Jiang

Physical layer radio jamming is a serious security threat to a wireless sensor network since the network relies on open wireless radio channels. A radio jammer is typically strategic and chooses its jamming strategy in response to the possible defense strategy taken by the sensor network. In this paper we model the interaction between the sensor network and the attacker as a noncooperative nonzero-sum static game. In such a game, the sensor network has a set of strategies of controlling its probability of wireless channel access and the attacker manipulates its jamming by controlling its jamming probability after sensing a transmission activity. We propose an algorithm for computing the optimal strategies for jamming attack and network defense. A critical issue is that there may exist a number of possible strategy profiles of Nash equilibria. To address this issue, we further propose to choose realistic Nash equilibria by applying the Pareto dominance and risk dominance. Our numerical results demonstrate that the strategies chosen by the Pareto dominance and risk dominance achieve the expected performance. Our results presented in the paper provide valuable defense guidance for wireless sensor networks against jamming attacks.

1. Introduction

Wireless sensor networks are vulnerable to malicious attacks [1, 2]. Several reasons account for this. First, sensor networks are typically deployed in remote regions and remain unattended. On the one hand, sensor nodes may be physically captured, and the program and data inside the node may be analyzed by a counterparty. On the other hand, malicious nodes may be inserted into sensor networks and launch various attacks such as interception, impersonation, and injection of forged data. Second, senor networks rely on wireless communication. The wireless media is open and shared among by radio transmitters and are therefore susceptible to radio interference. This leaves a sensor network more vulnerable to attacks. A number of countermeasures based on cryptography [3, 4] have been proposed for enhancing the security of sensor networks. Nevertheless, such countermeasures are only effective to those attacks which try to access data contents or inject false and misleading data.

Radio jamming is one of effective attacks against wireless sensor networks [1, 5, 6]. To launch a radio jamming attack, the attacker simply transmits high-power radio signals. For a sensor network with a single channel, if the jamming signals are transmitted on the radio channel, all sensor nodes within the interface range of the jammer would suffer degraded performance of data reception. The degree of reduced performance is dependent on the distance between the jammer and the node, and the transmission power of jamming signal. For a receiver to be able to correctly receive data packets, the ratio of signal to noise and interference has to be greater than a given threshold. From the point view of the receiver, the jamming signal is a kind of interference.

Radio jamming is a kind of attack that is easy to launch but difficult to defense [5]. For radio jamming, countermeasures based on cryptography become meaningless since the effect of radio jamming which is that the ability of packet reception is reduced. As long as the jamming signal is present, all the nodes that covered by the jamming signal suffer. Spread spectrum techniques, such as direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS), are effective methods against radio jamming. However, these techniques require complicated radio hardware. It is well known that sensor nodes are resource constrained. Therefore, spread spectrum increases

the hardware complexity of sensor nodes and is unsuitable for wireless sensor networks in most cases.

There are several other countermeasures for defending sensor networks against jamming attacks. Xu et al. have studied the feasibility of detecting jamming attacks in sensor networks [5]. The central idea for jamming detection is that there is likely a jamming attack when the percept signal strength is strong while the delivery ratio is low. In [6], countermeasures including channel surfing and spatial retreat are proposed for defending a sensor network against jamming attacks. It is proposed that when a jamming attack is detected, the sensor nodes can either change to another wireless channel or change their physical positions for the purpose of avoiding the jamming attack. In [1], the authors present good study on the attack and defense strategies in sensor networks.

Although existing methods for jamming attacks may be effective for some situations, they rarely touch the fact that the jammer may be strategic as it may choose an attacking strategy to maximize the gain of attacking. The interaction between the sensor network and the jammer is complicated. A countermeasure against jamming for a sensor network designed without consideration of the strategic nature of the jammer usually is deficient.

In this paper we study the interaction between the sensor network and the attacker and model it as a noncooperative nonzero-sum static game, in which the sum of sensor network payoff and the attacker payoff is not zero. The attacker employs a smart jamming attack technique that it transmits jamming signals after it senses a transmission activity. It manipulates its jamming by controlling its jamming probability. The sensor network employs monitors for detecting jamming attacks by using an optimal sequence hypothesis test. It has a set of strategies of controlling its probability of accessing the wireless channel.

We propose an efficient algorithm for computing the optimal strategies for jamming attack and network defense, respectively. A critical issue is that there may exist a number of possible strategy profiles of Nash equilibria. To address this issue, we further propose to choose realistic Nash equilibria by applying the Pareto dominance and risk dominance. Our numerical results demonstrate that the strategies chosen by the Pareto dominance and risk dominance achieve the expected performance. Our results presented in the paper provide valuable defense guidance for wireless sensor networks against jamming attacks.

In the paper we have made the following contributions:

(i) this is the first work, to the best of our knowledge, that studies the attack-defense interaction between the sensor network and jamming attacks;

(ii) we model the interaction between the sensor network and the jammer as a noncooperative game and design an efficient algorithm for computing the optimal strategies for network defense and jamming attack;

(iii) we deal with the issue of multiple Nash equilibria by applying the Pareto dominance and risk-dominance techniques and derive realistic strategy profiles for sensor networks.

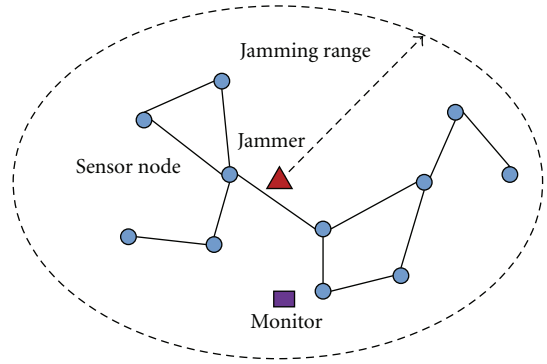

Figure 1: Illustration of the sensor network and the jammer. There is a jammer node that interferes the sensor nodes. The monitor node is a special node that detects jamming attacks.

The remainder of the paper is organized as follows. In Section 2, we present the system model describing the network model, the attacker model, and the defense model. In Section 3, the nonoperative nonzero-sum game played by the sensor network and the attacker is explained, and the problem for attack and defense is defined. In Section 4, we prose algorithm and techniques for computing the optimal strategies of jamming attack and network defense. Performance results and analysis are presented in Section 5. Section 6 presents related work on antijamming in sensor networks. Finally, the paper is concluded in Section 7 that also discusses the directions of future work.

2. Network Model and Problem Statement

We present the network model and the model for jamming and defense and a similar system model that has been utilized in [1].

2.1. Network Model. We consider a wireless sensor network with sensor nodes being uniformly distributed in a region with spatial density ρ (nodes per unit area), as shown in Figure 1. The sensor nodes are static. All sensor nodes always have packets to transmit. The packets can be originated locally or received from neighbors and should be further be forwarded.

The sensor nodes operate with a single wireless channel and adopt an Aloha-like access control protocol. Time is slotted and the slot size equals to the time for transmission of a data packet. All nodes are assumed to be synchronized with respect to slot boundaries. A node j within the transmission range R of node i can correctly receive packets from node i. A node j within the interference range R_s of node i is aware of the transmission activity of node i. However, it cannot receive packets from the node if it is outside of the transmission range of the node. All nodes falling in the transmission range of node i defines the neighborhood of node i (denoted by $\mathcal{N}_i$). Let $n_i = |\mathcal{N}_i|$. Each node has an initial amount of energy E.

Each node accesses the radio channel with probability γ in a time slot. For analysis simplification, we let the accessing

probability be selected from a set of all possible probabilities, $\Upsilon = \{\gamma_0, \gamma_1, \ldots, \gamma_{n-1}\}$, $0 < \gamma_i \leq 1$, $0 \leq i \leq n-1$. Each node uses unicast routing and chooses the destination equally likely from its neighborhood. Thus, the probability is that node i sends a packet to $j \in \mathcal{N}_i$ is γ/n_i.

2.2. Attacker Model. We consider the advisory inserts attackers into the wireless sensor network. The goal of the advisory is to cause maximal damage to the sensor network. For simplicity of analysis, we assume that only one attacker is inserted. Note that it is possible that there exist many attackers in the sensor network. However, the attackers can be considered together and be modeled by a virtual attacker.

The attacker operates in the same channel as the sensor network. The attacker is also called the jammer. The initial energy of the attackers is E_m. It is equipped with omni-directional antenna with adjustable transmission range R_m. and interference range R_{ms}. The jammer employs a smart jamming techniques that it sends a short high-power jamming signal when it senses a transmission activity in the channel. The jammer controls its aggressiveness with probability of jamming q in each time slot. Existing study [7] shows that by using such a technique the energy for transmitting jamming signals is negligible. However, the energy for activity sensing is nonnegligible. For analysis simplification, we let the jamming probability be selected from a set of all possible probabilities, $Q = \{q_0, q_1, \ldots, q_{n-1}\}$, $0 < q_i \leq 1$, $0 \leq i \leq n-1$.

2.3. Defense Model. The sensor network uses a mechanism for detecting jamming attacks. A set of nodes are employed as monitors that try to detect jamming. For each monitor node, it watches its collisions and detects a jamming attack by checking if the collisions happened to be abnormal. We focus on the situation of one monitor. The monitor observes the probability of collision it has experienced. When the monitor is jammed by an attacker, the probability of collision it experiences would be different from what it experiences under normal situations. An increased probability of collision usually results from a jamming attack. The monitor takes observations for each time slot (collided or not collided) and decides whether there has appeared jamming. The monitor prefers to use a short-time window of observation so that a jamming attack can be detected as quickly as possible. Meanwhile, it takes long enough time so as to minimize the false alarm rate.

The specific algorithm for jamming detection is Wald's Sequential Probability Ratio Test (SPRT) [8]. The algorithm minimizes the average number of required observations while the false alarm and detection of missing rate do not exceed the given thresholds above.

Let H_0 and H_1 denote the two hypotheses, meaning absence and presence of jamming, respectively. According to the algorithm, the mean number of time slots for jamming detection is given by

$$E[N \mid H_1] = \frac{C}{\theta_1 \log(\theta_1/\theta_0) + (1-\theta_1)\log((1-\theta_1)/(1-\theta_0))}, \tag{1}$$

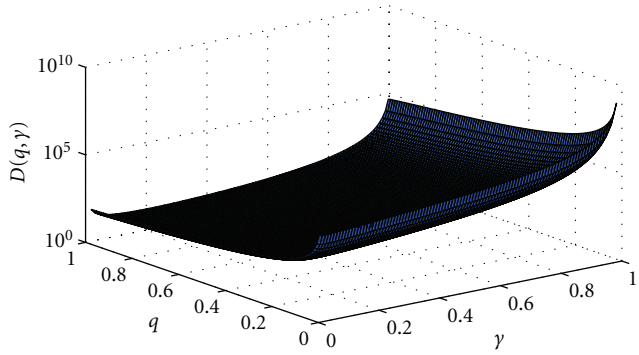

Figure 2: The expected delay of jamming detection as a function of q and γ.

where θ_0 is the probability of collision at the monitor,

$$\theta_0 = 1 - (1-\gamma)^n - n\gamma(1-\gamma)^{n-1}, \tag{2}$$

and θ_1 is the probability of collision at the monitor if in the time slot the jammer sends jamming signals,

$$\theta_1 = 1 - (1-\gamma)^n - (1-q)n\gamma(1-\gamma)^{n-1}. \tag{3}$$

In (2) and (3), n is the neighborhood size of the monitor. In the following, let $D(q,\gamma)$ denote $E[N \mid H_1]$, which is the expected delay for jamming detection. In Figure 2, the mean delay as a function of q and γ is plotted. Note that the system parameters are detailed in Section 6, and the same configuration is used for the following figures. For the detail of analysis, refer to [1].

3. Game Theoretic Formulation

The performance gain for the attack is dependent on the action that is taken by the senor network, and the performance gain of the sensor network is related to the jamming action of the attacker. This interaction between the senor network and the attacker is a noncooperative game.

3.1. Attacker Payoff. The payoff for the jammer (denoted by U_{mC}) is quantified by the number of incurred corrupted links. Note that this number does not include those caused by legitimate contention. Let U_{mI} be the payoff of the jammer in a time slot. Thus we have

$$U_{mC} = U_{mI} \times (D(q,\gamma) + W(q,\gamma)), \tag{4}$$

where $W(q,\gamma)$ is the time for the monitor sending a notification message out of the jammed area.

In order to obtain U_{mI}, we first derive the mean number of successful transmissions in a time slot. Let X and Y denote the number of attempted transmissions and the number of successful transmission links, respectively. It is not difficult to find success the probability of an attempted transmission, p_s, as follows:

$$p_s = \rho\gamma A\left(e^{-\rho\gamma A} - e^{-\rho A}\right), \tag{5}$$

where A is the area covered by the transmission range of a sensor node.

By conditioning on X, we can derive the mean number of successful transmission links,

$$\begin{aligned} E[Y] &= E_X[E_Y[Y \mid X = x]] \\ &= A_m\left(A(\rho\gamma)^2\left(e^{-\rho\gamma A} - e^{-\rho A}\right)\right), \end{aligned} \tag{6}$$

where A_m is the area covered by the transmission range of the jammer. The instantaneous payoff for the attacker that jams with probability q after sensing a transmission is

$$\begin{aligned} U_{mI}(q,\gamma) &= q \times E[Y] \\ &= qA_m\left(A(\rho\gamma)^2\left(e^{-\rho\gamma A} - e^{-\rho A}\right)\right). \end{aligned} \tag{7}$$

The average time for sending the notification message out of the jammed area is dependent on q and γ. The mean time (T_a) for a sensor node successfully accessing the channel where a jamming is present is

$$T_a = \sum_{j=1}^{\infty} j(1-a)^{j-1} p_a = \frac{1}{p_a}, \tag{8}$$

where p_a is probability of successful channel access,

$$p_a = (1-q)\gamma(1-\gamma)^{n-1}. \tag{9}$$

The message is sent hop-by-hop. The mean number of hops that the message needs to be forwarded is $H = R_m/2R$. Therefore, the average time needed for notification broadcast is

$$W(q,\gamma) = \frac{H}{p_a} = \frac{R_m}{2R(1-q)\gamma(1-\gamma)^{n-1}}. \tag{10}$$

Thus, the overall accumulated payoff of the jamming until it is detected is

$$\begin{aligned} U_{mC} &= U_{mI} \times (D(q,\gamma) + W(q,\gamma)) \\ &= qA_m\left(A(\rho\gamma)^2\left(e^{-\rho\gamma A} - e^{-\rho A}\right)\right) \\ &\quad \times \left(\frac{C}{\theta_1 \log(\theta_1/\theta_0) + (1-\theta_1)\log((1-\theta_1)/(1-\theta_0))} \right. \\ &\quad \left. + \frac{R_m}{2R(1-q)\gamma(1-\gamma)^{n-1}}\right). \end{aligned} \tag{11}$$

3.2. Network Payoff. Let U_I be the payoff of the sensor network in a time slot. It is the number of successful transmission links in the presence of jamming,

$$\begin{aligned} U_I(q,\gamma) &= (1-q)E[Y] \\ &= (1-q)A_m\left(A(\rho\gamma)^2\left(e^{-\rho\gamma A} - e^{-\rho A}\right)\right). \end{aligned} \tag{12}$$

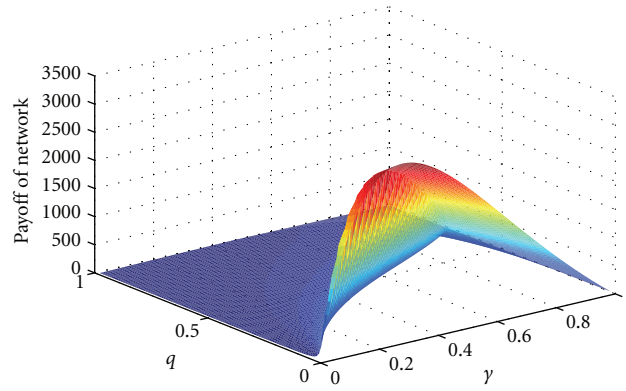

Figure 3: The payoff of the sensor network as a function of q and γ.

Therefore, the cumulative payoff for the network is

$$\begin{aligned} U_C(q,\gamma) &= (1-q)A_m A(\rho\gamma)^2\left(e^{-\rho\gamma A} - e^{-\rho A}\right) \\ &\quad \times \left(\frac{C}{\theta_1 \log(\theta_1/\theta_0) + (1-\theta_1)\log((1-\theta_1)/(1-\theta_0))} \right. \\ &\quad \left. + \frac{R_m}{2R(1-q)\gamma(1-\gamma)^{n-1}}\right). \end{aligned} \tag{13}$$

3.3. Problem Formulation. For the sensor network, it is difficult to find the optimal strategy for accessing the radio channel and defense against jamming. The achievable performance of the sensor network heavily depends on the action taken by the jammer. When the sensor nodes access the channel frequently while the jammer sends extensive jamming signals, the performance gain is poor. This effect is shown in Figure 3.

Similarly, there is no obvious dominant strategy for the attacker. If the attack sends a lot of jamming signals while the sensor network rarely accesses the channel, the jamming attack is inefficient. In addition, a more aggressive jamming expanses itself more to the monitor and therefore results in a short time to be detected. This effect is shown in Figure 4.

In this paper, we model the interaction between the attacker and the sensor network as a noncooperative game model. We assume that the jammer knows the set of possible actions and the payoff of the network. On the other hand, the network observes the set of actions and the payoff of the jammer. Either side is strategic and tries to maximize its own payoff.

For the jammer, its action is the selection of jamming probability, and thus the set of all possible strategies is $Q = \{q_0, q_1, \ldots, q_{n-1}\}$, $0 < q_i \leq 1$, $0 \leq i \leq n-1$. For the network, its action is the selection of accessing probability and thus the set of strategies is $\Upsilon = \{\gamma_0, \gamma_1, \ldots, \gamma_{n-1}\}$, $0 < \gamma_i \leq 1$, $0 \leq i \leq n-1$.

Then, the jamming-defense game problem is as follows.

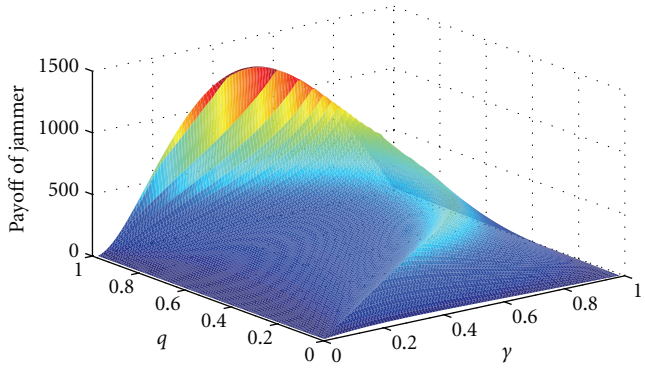

Figure 4: The payoff of the jammer as a function of q and γ.

Definition 1 (jamming-defense game). Given the system model and payoff forms for both sides, what is the optimal jamming strategy for the attacker? And what is the optimal defense strategy for the sensor network?

4. Optimal Strategies of Jamming and Defense

In this section we derive the optimal jamming strategy for the attacker and the optimal defense strategy for the sensor network.

4.1. Computing Optimal Strategies. We are interested in the question if there exist dominant strategies for the attack and the sensor network. According to game theory, a strategy is dominant if it provides the player with a larger payoff than any other regardless what strategies the other players take. If such a strategy exists, then there is a strong desire for the player to stick to this strategy. However, after analysis, we find that there do not exist dominant strategies for both sides, as shown in the following theorem.

Theorem 2. *In the jamming-defense game, there are no dominant strategies for either the attacker or the network.*

Proof. We first prove that there is no dominant strategy for network defense. It can be proved in a similar way that there is no dominant strategy for the attacker. We prove it by contradiction. Suppose that there is a dominant strategy for network defense and denote the defense strategy with γ^*. Then it follows that we have that the proposition γ^* must be unique. We select two different jamming probabilities, q_1 and q_2. When the jamming probability is given, the payoff of the network $U_C(q, \gamma)$ then become a function of only one variable, that is, accessing probability γ. It is not difficult to find γ_1^* and γ_2^* that maximizes the network payoff when the jamming probability takes q_1 and q_2, respectively. By supposing a configuration instance of the network and the attacker, we compute γ_1^* and γ_2^* and find that they are not the same. This is contradictory to the previous proposition that γ^* must be unique. This concludes our proof. □

Since there are no dominant strategies, a rational player should select an optimal strategy, taking into account the possible strategy of the opponent player. This leads to the concept of Nash equilibrium which is a situation where each player's strategy is optimal given the strategies of all other players. That is, when in a Nash equilibrium, the player is unwilling to change its strategy unilaterally if other players do not change their strategies; otherwise, its payoff will be reduced. A Nash equilibrium defines a strategy profile which defines the optimal strategies for the players. For the sensor network, the strategy of the Nash equilibrium should be the best defending strategy in the presence of a strategic jamming attacker.

input:
$Q = \{q_0, q_1, \ldots, q_{n-1}\}$: Jammer's strategy set
$M_{\text{jam}} = (U_{mC}(q_i, \gamma_j))_{n\times n}$: Jammer payoff matrix
$\Upsilon = \{\gamma_0, \gamma_1, \ldots, \gamma_{n-1}\}$: Network's strategy set
$M_{\text{network}} = (U_C(q_i, \gamma_j))_{n\times n}$: Network payoff matrix
output:
(q_*, γ_*): Nash equilibria
main procedure:
for each $q_i \in Q$
for each $\gamma_j \in \Upsilon$
$U_{mC}(q_i, \gamma_j) = \max(M_{\text{jam}}(q_i, \gamma_j))$;
$S_1 \leftarrow (q_i, \gamma_j)$;
end for
end for
for each $\gamma_j \in \Upsilon$
for each $q_i \in Q$
$U_C(q_i, \gamma_j) = \max(M_{\text{net}}(q_i, \gamma_j))$;
$S_2 \leftarrow (q_i, \gamma_j)$;
end for
end for
if $(q_*, \gamma_*) \in S_1$ && $(q_*, \gamma_*) \in S_2$
return (q_*, γ_*);
end if

Algorithm 1: Optimal strategy algorithm.

We design the optimal strategy algorithm for computing the strategy profiles of the Nash equilibrium. The central idea of this algorithm is as follows. All possible strategy profiles define a payoff matrix. For each player, it finds the maximum payoff for each of this strategy and marks the strategy profile. If a strategy profile has been marked twice, then it corresponds to a Nash equilibrium. The detailed pseudocode of the optimal strategy algorithm is shown in Algorithm 1.

This algorithm contains two double-loops. The time complexity of each double-loop is $\mathcal{O}(n^2)$. As the time complexity of the other part of the algorithm is $\mathcal{O}(n \log_2 n)$, the total time complexity of the algorithm is $\mathcal{O}(n^2)$. We have to store the elements of S_1 and S_2. The number of the elements in S_1 or S_2 is less than n. Thus, the total space complexity of the algorithm is $\mathcal{O}(n)$.

4.2. Dealing with Multiple Nash Equilibria. The optimal strategy algorithm outputs a number of Nash equilibria. The existence of multiple equilibria creates difficulty in understanding the jamming-defense game in wireless sensor network. It is apparent that for each computed equilibrium,

when the other player fixes its strategy, the player's best strategy is to follow the one defined by the strategy profile of the Nash equilibrium.

However, in the real world, only one equilibrium takes place. Will these equilibria happen with equal probability? Or will only one of the equilibria is better than the rest? Actually, it is not uncommon that many games have several Nash equilibria. For different application scenarios, different Nash equilibria may not preferred.

In the following, we present two possible equilibria that may be applied in the jamming-defense game of wireless sensor networks.

4.2.1. Pareto-Dominated Equilibrium. Although there are multiple Nash equilibria, we find that the equilibria are associated with different payoffs for the network and the attacker. It is highly desirable in the real situation that each player achieves the maximum payoff among all Nash equilibria at the same time. In other words, this equilibrium earns larger payoffs for all players simultaneously than any other equilibria. It is highly probable that all players will have unanimous tendency to this equilibrium. That is, all players in this game will choose the strategy defined by this equilibrium and also predict that other players will do the same.

The approach to selecting a Nash equilibrium is based on the Pareto efficiency. The equilibrium selected by Pareto efficiency is called Pareto-dominated equilibrium. We develop the Pareto algorithm, as shown in Algorithm 2, for computing the Pareto-dominated equilibrium and the corresponding optimal strategy profile for the attacker and the network. Note that it is unnecessary that a game always has a Pareto-dominated equilibrium.

4.2.2. Risk-Dominated Equilibrium. In practice, the strategies defined by the Pareto-dominated equilibrium are not the best choice, because there is uncertainity with how the opponent player chooses its strategy. The possible reasons are the incompleteness of information or the limited rational degree of the opponent player. In addition, Pareto-dominated equilibrium may not exist.

With this in mind, it is useful to consider the risk-dominated equilibrium. A Nash equilibrium is risk-dominated if it has the largest basin of attraction, which means that the more uncertainty players have about the actions of the other player(s), the more likely they will choose the strategy corresponding to it. A risk-dominated equilibrium defines the optimal strategy for a player in the sense that the strategy results in the best expected payoff on the condition that the opponent player may choose its strategy with certain randomness. We develop the risk algorithm, as shown in Algorithm 3, for computing the optimal risk-dominated strategies for jamming attack and network defense.

input:
$\{(q_i, \gamma_i) \mid 0 \le i \le k-1\}$: k Nash equilibriums
$M_{\text{jam}} = (U_{mC}(q_i, \gamma_j))_{n\times n}$: Jammer payoff matrix
$M_{\text{net}} = (U_C(q_i, \gamma_j))_{n\times n}$: Network payoff matrix
output:
(q_*, γ_*): Risk-dominated equilibrium
main procedure:
for $i = 0$ to $k-1$
$t_i = \left(\frac{1}{n} \times \sum_{j=1}^{n} M_{jam}(q_i, \gamma_j)\right)$;
end for
$t_m = \max(t_0, t_1, \ldots, t_{k-1})$;
$q_* \leftarrow q_m$;
for $j = 0$ to $k-1$
$s_j = \left(\frac{1}{n} \times \sum_{i=1}^{n} M_{jam}(q_i, \gamma_j)\right)$;
end for
$s_l = \max(s_0, s_1, \ldots, s_{k-1})$;
$\gamma_* \leftarrow \gamma_l$;
return (q_*, γ_*);

Algorithm 2: Risk algorithm.

input:
$\{(q_i, \gamma_i) \mid 0 \le i \le k-1\}$: k Nash equilibriums
$M_{\text{jam}} = (U_{mC}(q_i, \gamma_j))_{n\times n}$: Jammer payoff matrix
$M_{\text{net}} = (U_C(q_i, \gamma_j))_{n\times n}$: Network payoff matrix
output:
(q_*, γ_*): Pareto-dominated equilibrium
main procedure:
$(q_*, \gamma_*) = (q_0, \gamma_0)$;
for $i = 1$ to $k-1$
if $M_{\text{jam}}(q_i, \gamma_i) > M_{\text{jam}}(q_*, \gamma_*)$ &&
$M_{\text{net}}(q_i, \gamma_i) > M_{\text{net}}(q_*, \gamma_*)$
$(q_*, \gamma_*) \leftarrow (q_i, \gamma_i)$;
end if
end for
return (q_*, γ_*);

Algorithm 3: The Pareto algorithm.

5. Performance Results

In this section, we conduct numerical experiments to verify our previous theoretical analysis and show the performance of the Pareto-dominated optimal strategies and risk-dominated strategies.

5.1. Simulation Setup. The transmission range $R = 20$ m, energy constraint $E/P = 500$, jammer transmission range $R_m = 200$ m, energy constraint $E_m/P_m = 1000$, $P_D = 1 - P_M = 0.98$, $P_{FA} = 0.02$. Probabilities q and γ are discretized from (0, 1) into 100 unites, that is, $n = 100$. The default node density $\rho = 0.0025$.

Considering the power constrains of the sensor nodes and the jammer, we assume that if the total time used for jamming detection and sending out an alarm message exceeds the time that the sensor nodes and jammer can survive, the jammer and the network will gain no more payoffs.

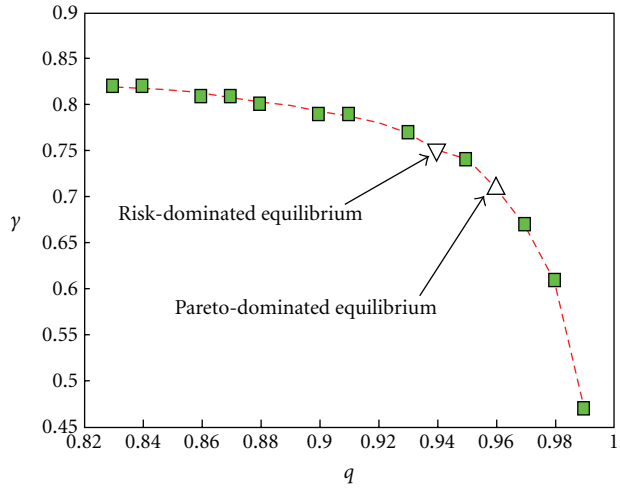

Figure 5: All Nash equilibriums, along with Pareto-dominated equilibrium and risk-dominated equilibrium.

We also vary the node density ρ in order to study the performance under different configurations of node density.

5.2. Multiple Nash Equilibria. We compute all Nash equilibria by running the optimal strategy algorithm. In Figure 5, all optimal strategy profiles corresponding to the Nash equilibria are shown. We can find that there are in total 16 Nash equilibria. This verifies the previous claim that the jamming-defense game may have multiple Nash equilibria.

To study the payoff of each of the strategy profile, we further plot the payoffs of the attacker and the network for each of the strategy profile. Figure 6 shows the payoff of the attacker and Figure 7 shows the payoff of the network. We can find that different strategy profiles produce very different payoffs. By only observing the payoffs, we are unable to tell which strategy profile would take place in a real combating sensor network against the jammer.

5.3. Pareto-Dominated and Risk-Dominated Strategies. By running the Pareto algorithm and the risk algorithm, we compute the Pareto-dominated and the risk-dominated strategy profiles. The corresponding Pareto-dominated and the risk-dominated equilibria are shown in Figure 5 along with the rest of Nash equilibria.

To study the performance of the Pareto-dominated strategy, we compare the payoffs of both the attacker and the network with three other Nash equilibria' strategies. The comparison is shown in Figures 8 and 9. We can find that the network payoff is larger than those of the three other Nash equilibria defined strategies under different node densities. And this is also true for the attacker payoff. This verifies that the Pareto-dominated strategy profile achieves the best payoffs among all Nash equilibria defined strategy profiles.

To study the performance of the risk-dominated strategy, we compare the payoff losses of both the attacker and the network with other strategies defined by other Nash equilibria. We let one player randomly selects a strategy and compare the player's payoff loss. Figure 10 shows the

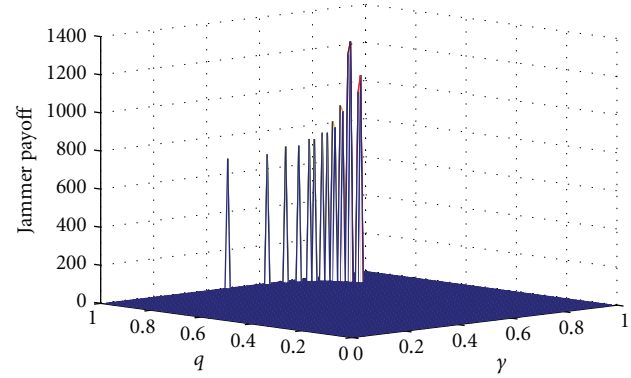

Figure 6: Payoffs of the attacker for all optimal strategy profiles.

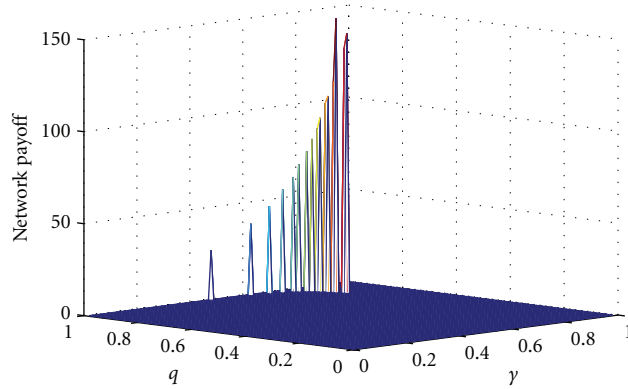

Figure 7: Payoffs of the network for all optimal strategy profiles.

comparison. We can find that the risk-dominated strategy profile produces less payoff loss than the other method. This verifies that the risk-dominated strategy profile can effectively offset risks.

6. Related Work

Radio jamming has been recognized as a serious threat to wireless sensor networks [1, 5–7, 9]. A sensor network is susceptible to jamming attacks since it consists of miniature energy-constrained sensor nodes.

Jamming is a kind of attack in the physical layer and usually realized by transmission of high power radio signals. All communication links falling in the corrupted area of the jamming attack result in degraded performance of wireless communication. Wood and Stankovic [10] provide a taxonomy of denial of service (DoS) attacks for sensor networks from the physical up to the transport layer. According to the jamming pattern in the time dimension, jamming attacks can be classified into constant, random, perceptive, and reactive jamming [5]. According the spectrum pattern, jamming has three classes, that is, singletone, multitone, and partially jam. Traditional defense techniques against jamming in the physical layer use the spread spectrum technology. However, such technology is so energy consuming that it can hardly be used in sensor networks with severe resource constraints.

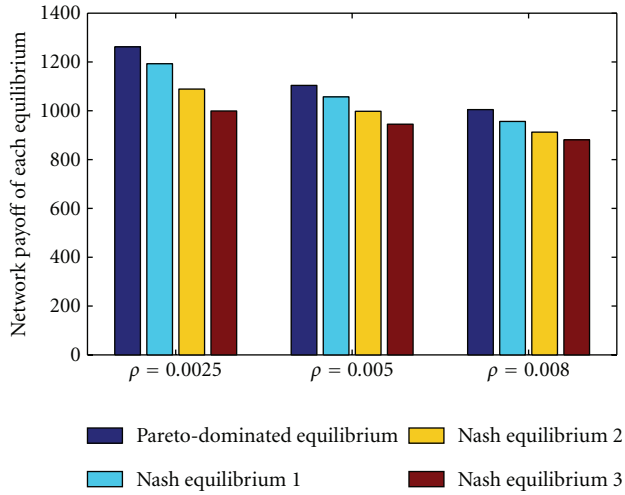

Figure 8: Network payoff comparison between Pareto-dominated strategies and other strategies.

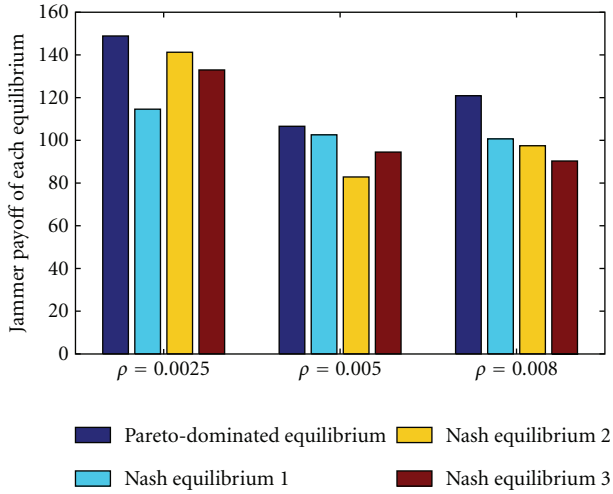

Figure 9: Attacker payoff comparison between Pareto-dominated strategies and other strategies.

Jamming attacks can also be implemented in the data link layer. An attacker can corrupt control packets, such as RTS/CTS or ACK. When control packets are corrupted by the jamming, normal nodes may be prevented from accessing the wireless channel or caused for repeated retransmissions. In addition, the attacker can also reserve the wireless channel for the maximum allowable number of slots. In this case, other nodes experience long delay and low link throughput [2]. In [11], the problem of a sensor node and a jammer transmitting to a common receiver in an on-off mode is studied with in a game-theoretic framework.

Jamming is also implemented in the network and higher layers. Jamming attacks on the network layer inject malicious packets along certain routes. On the transport layer, control segments such as SYN may be corrupted. It should be noticed that in sensor networks they rarely use the transport layer protocol like TCP/UDP since such protocols may introduce heavy cost. Thus, traditional methods [12] for computer

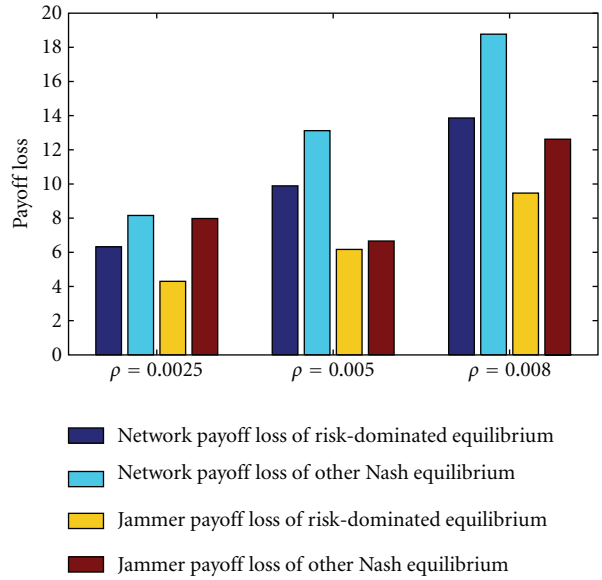

Figure 10: Payoff loss comparison between risk-dominated strategies and other strategies.

networks can hardly be used. The method [13] proposes the use of controlled authentication for detecting spam messages, which includes a distributed scheme for the trade-off between attack resilience and computational cost.

Effective jamming attacks of various kinds have been studied. In [7], low-energy attacks corrupt a packet by corrupting only a few bits. Low Density Parity Check (LDPC) codes are proposed as a method to defend against these attacks. In [14], attacks by learning sensor network protocols are proposed, which are based on semantics such as temporal packet arrangement, slot size or preamble size. In [15], the authors study the problem of sending notification messages out of a jammed region.

Various countermeasures against radio jamming have been proposed. In [5], the authors use empirical methods based on signal strength and packet delivery ratio measurements to detect jamming attacks. In [6], different countermeasures against jamming are assessed. Channel surfing involves on-demand frequency hopping in case of an jamming attack and spatial retreat refers to moving away from jamming region. The case of an attacker that corrupts broadcasts from a base station to a sensor network is considered in [9]. The interaction between the attacker and the base station is modeled as a zero-sum game in which the attacker selects the number of sensors to jam and the base station chooses the sample rate of sensor status.

In [1], it studies the optimal jamming and defense policies for wireless sensor network. It proposes a framework for jamming attack and network defense against jamming. It presents the optimal jamming policies when the defense policy of the network is given, and the optimal defense policies when the jamming policies is given. In contrast, we study the jamming and defense in sensor network from a different perspective by applying a game-theoretic approach, which is more realistic to the real-world situations and

provides more constructive guidance to sensor network defense against jamming attacks.

In summary, jamming in sensor networks has received significant attention and a number of countermeasures have been proposed. However, the majority of the existing methods do not take into account the strategic characteristic of jamming attackers. As a result, existing methods are deficient in many environments. The preliminary result of the research of this paper was presented in [16].

7. Conclusion

As sensor networks rely on wireless communications, they are vulnerable to radio jamming attacks. A sensor network under jamming attacks suffer reduced ability of data communication. In this paper, we have studied the interaction between strategic attackers and the sensor network. We study the optimal strategies for attacking and defense in the framework of noncooperative nonzero-sum game. The attacker strategically manipulates its jamming probability and the network controls its access probability. For this game, we first prove that there does not exist a dominant strategy for either side of the attacker or the sensor network. We then turn to the find the optimal strategies in the sense of the Nash equilibrium. To solve the issue of multiple equilibriums, we propose techniques of the Pareto-dominance and risk-dominance to find optimal strategies that are useful in real-world situations. We conduct numerical analysis and results have verified our theoretical analysis. Results also demonstrate that the resultant Pareto-dominated strategies provide better payoffs that the strategies defined by other equilibria, and the risk-dominated strategies have better ability of offsetting risks.

This paper studies the complicated game between strategic attackers and sensor networks. To reduce unnecessary complication, we have assumed a relatively simplified system model. It is worthwhile to extend the current model and make it closer to the real situations. First, it is necessary to study the jamming conducted by multiple attackers. The difficulty will be in the fact that sensor nodes and monitors will be interfered by different set of attackers. Second, we will study more realistic media access control protocols than the one assumed in the paper. For example, CSMA/CA-like protocols will be more meaningful. Finally, we should study other more sophisticated jamming techniques.

Acknowledgments

This research is supported by Shanghai Pu Jiang Talents Program (10PJ1405800), Shanghai Chen Guang Program (10CG11), NSFC (no. 61170238, 60903190, 61027009, 60970106, 61170237), 973 Program (2005CB321901), MIIT of China (2009ZX03006-001-01), Doctoral Fund of Ministry of Education of China (20100073120021), 863 Program (2009AA012201 and 2011AA010500), and HP IRP (CW267311). In addition, it is partially supported by the Open Fund of the State Key Laboratory of Software Development Environment (Grant no. SKLSDE-2010KF-04), Beijing University of Aeronautics and Astronautics.

References

[1] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attacks and network defense policies in wireless sensor networks," in *Proceedings of the 26th IEEE International Conference on Computer Communications (INFOCOM'07)*, pp. 1307–1315, Anchorage, Alaska, USA, May 2007.

[2] R. Negi and A. Perrig, "Jamming Analysis of MAC protocols," Carnegie Mellon Technical Memo, 2003.

[3] S. A. Çamtepe and B. Yener, "Combinatorial design of key distribution mechanisms for wireless sensor networks," *IEEE/ACM Transactions on Networking*, vol. 15, no. 2, pp. 346–358, 2007.

[4] D. Liu and P. Ning, "Improving key predistribution with deployment knowledge in static sensor networks," *ACM Transactions on Sensor Networks*, vol. 1, no. 2, 2005.

[5] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC'05)*, pp. 46–57, May 2005.

[6] W. Xu, T. Wood, W. Trappe, and Y. Zhang, "Channel surfing and spatial retreats: defenses against wireless denial of service," in *Proceedings of the ACM Workshop on Wireless Security (WiSe'04)*, pp. 80–89, October 2004.

[7] G. Lin and G. Noubir, "On link layer denial of service in data wireless LANs," *Wireless Communications and Mobile Computing*, vol. 5, no. 3, pp. 273–284, 2005.

[8] V. P. Dragalin, A. G. Tartakovsky, and V. V. Veeravalli, "Multihypothesis sequential probability ratio tests—part I: asymptotic optimality," *IEEE Transactions on Information Theory*, vol. 45, no. 7, pp. 2448–2461, 1999.

[9] J. M. McCune, E. Shi, A. Perrig, and M. K. Reiter, "Detection of denial-of-message attacks on sensor network broadcasts," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 64–78, May 2005.

[10] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *IEEE Computer*, vol. 35, no. 10, pp. 54–62, 2002.

[11] R. K. Mallik, R. A. Scholtz, and G. P. Papavassilopoulos, "Analysis of an on—off jamming situation as a dynamic game," *IEEE Transactions on Communications*, vol. 48, no. 8, pp. 1360–1373, 2000.

[12] J. Jung, V. Paxson, A. W. Berger, and H. Balakrishnan, "Fast portscan detection using sequential hypothesis testing," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 211–225, May 2004.

[13] V. Coskun, E. Cayirci, A. Levi, and S. Sancak, "Quarantine region scheme to mitigate spam attacks in wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 5, no. 8, pp. 1074–1086, 2006.

[14] 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, New York, NY, USA, November 2005.

[15] M. Cagalj, S. Capkun, and J.-P. Hubaux, "Wormhole-based anti-jamming techniques in sensor networks," *IEEE Transactions on Mobile Computing*, vol. 6, no. 1, pp. 100–114, 2007.

[16] Y. Zhu and Y. Jian, "A game-theoretic approach to anti-jamming in sensor networks," in *Proceedings of the IEEE 16th International Conference on Parallel and Distributed Systems (ICPADS '10)*, pp. 617–624, Shanghai, China, December 2010.