A Survey of Game Theory in Wireless Sensor Networks Security

Shigen Shen[1, 2], Guangxue Yue[2, 3, 4], Qiying Cao[1]
[1]College of Information Science and Technology, Donghua University, Shanghai, China
[2]College of Mathematics and Information Engineering, Jiaxing University, Jiaxing, China
[3]College of Computer and Communication, Hunan University, Changsha, China
[4] Department of Computer Science and Technology, Huaihua University, Huaihua, China
kxsg@21cn.com, guangxueyue@163.com, caoqiying@dhu.edu.cn

Fei Yu
Jiangsu Provincial Key Laboratory for Computer Information Processing Technology, Soochow University, Soochow, China
hunanyufei@126.com

***Abstract*—Wireless Sensor Networks (WSNs) are becoming an integral part of our lives. There are not widespread applications of WSNs without ensuring WSNs security. Due to the limited capabilities of sensor nodes in terms of computation, communication, and energy, providing security to WSNs is challenging. In fact, the process of implementing WSNs security is adaptive and dynamic, which evolves continually. The essence of attack-defend in WSNs security can be expressed by mutual strategies of interdependence while game theory can be used for the purpose of accounting for interactions among strategies of rational decision makers. Therefore, studying WSNs security with game theory has higher scientificity and rationality. This paper presents a survey of security approaches based on game theory in WSNs. According to different applications, a taxonomy is proposed, which divides current existing typical game-theoretic approaches for WSNs security into four categories: preventing Denial of Services (DoS) attacks, intrusion detection, strengthening security, and coexistence with malicious sensor nodes. The main ideas of each approach are overviewed while advantages and disadvantages of various approaches are discussed. Then, this paper overviews related work and highlights the difference from other surveys, and points out some future research areas for ensuring WSNs security based on game theory, including Base Station (BS) credibility, Intrusion Detection System (IDS) efficiency, WSNs mobility, WSNs Quality of Service (QoS), real-world applicability, energy consumption, sensor nodes learning, and expanding game theory applications and different games. Thus, a global view of WSNs security approaches based on game theory is provided. To our best knowledge of knowing, it is the first paper centrally focusing on game theory in WSNs security. It will make the researchers a better understanding of game-theoretic solutions to WSNs security and further research directions.**

***Index Terms*—Wireless Sensor Networks; game theory; Wireless Sensor Networks security; Denial of Services; intrusion detection**

I. INTRODUCTION

With the recent advances in Min-Electro-Mechanical Systems (MEMS) technology, wireless communications, and digital electronics, WSNs have become increasingly one of the most promising and interesting areas in the past years. WSNs may be very large systems, which are comprised of small sized, low power, low-cost sensor nodes that collect information about the physical environment in detail. These sensor nodes are often densely deployed in a sensor field. A sensor node generally consists of four basic parts: a sensing unit, a processing unit, a transceiver unit, and a power unit. It may also have additional application-dependent components such as a location finding system, power generator, and mobilizer [1]. Due to the self-organization and fault- tolerance characteristics, WSNs can be expected to many applications. The authors in [2] have classified the applications of WSNs as military applications, environmental applications, health applications, home applications, and other commercial applications. In the future, this widespread range of application areas will make WSNs an integral part of our lives.

Providing security to small sensor nodes is challenging, due to the limited capabilities of sensor nodes in terms of computation, communication, and energy. However, WSNs security is a primarily important and even critical issue before WSNs are used widely. As a result, it requires desirably various countermeasures for WSNs attacks. According to traditional thinking, these countermeasures mainly include preventing and detection mechanisms such as cryptography, key management, secure routing, secure data fusion, intrusion detection and so on. In practice, a quantitative decision framework for WSNs security is required. Game theory performs scenarios where multiple players with contradictory objectives compete with each other; it can provide a mathematical method for analyzing and modeling WSNs Security problems. Therefore, employing game theory to solve WSNs security issues is very suitable.

This paper surveys the existing typical game-theoretic approaches that are designed to strengthen WSNs Security. With respect to different secure applications, these approaches are divided into four categories: preventing DoS attacks, intrusion detection, strengthening

doi:10.4304/jnw.6.3.521-532

security, and coexistence with malicious sensor nodes. We overview the main ideas and the basic game type of various approaches, as well as discuss their advantages and disadvantages. We are expecting to provide a global view of WSNs security approaches based on game theory. After looking through these disadvantages, we propose some areas for future research. We hope more and more researchers all over the world can devote themselves into this field.

The rest of this paper is organized as follows. Section II discusses the relationship between game theory and WSNs security, as well as the taxonomy of exiting approaches. Section III overviews the current state of research and gives our discussions. Section IV proposes some future research areas. Section V illustrates related work and highlights the difference between this paper and other surveys, and a conclusion is provided in Section VI.

II. GAME THEORY AND WSNS SECURITY

Game theory is a branch of applied mathematics that deals with multi-person decision-making situations. It is devised for the purpose of accounting for interactions among strategies of rational decision makers, and it is essential for determining a preferred strategy where such interactions are in play. A game generally consists of a set of players, a set of strategies for each player, and a set of corresponding utility functions. A strategy for a player is a complete plan of actions in all possible situations throughout the game. In any games, the players try to act selfishly to maximize their consequences according to their preferences. These preferences are expressed by a utility function, which maps every consequence to a real number. Nash equilibrium is a solution concept that describes a steady state condition of the game; no player would like to change his strategy unless there is a better strategy that can result in more utility that is favorable for the player current. The normal form of a game is given by a tuple

$$G= (I, S, U), \tag{1}$$

where G is a particular game, I is a finite set of players,

$$S = \{S_i\}, \tag{2}$$

where S_i is the set of strategies for each player $i \in I$, and

$$U=\{u_i\} \tag{3}$$

is the set of utility functions that the players wish to maximize. For each player i, the utility function u_i, is a function of the particular strategy chosen by player i, s_i, and the particular strategies chosen by all of the other players in the game, s_{-i}. From this model, Nash equilibrium is identified wherein no player will rationally choose to deviate from his chosen strategy otherwise he will diminish his payoff, i.e.,

$$u_i(s_i,s_{-i}) \geqslant u_i(s_i', s_{-i}), \tag{4}$$

for all $s_i' \in S_i$.

WSNs consist of thousands of sensor nodes and may be dispersed over a large area. Typical sensor nodes are of limited communication and computing capabilities, and are powered by batteries. Due to these inherent vulnerabilities, WSNs have to face multiple passive and active attacks. According to [3], the attacks can be categorized into common attacks, DoS attacks, node compromise, side-channel attacks, impersonation attacks, and protocol-specific attacks. Similar to traditional networks, providing confidentiality, integrity, authenticity, and availability of all messages in WSNs are the ultimate security objectives. Every eligible receiver-node should receive all messages intended for it and be able to verify the integrity of every message as well as the identity of the sender-node. Attackers should not be able to deduce the contents of any message. Similar to conventional networks, the primary security goal in WSNs is reliable delivery of data, i.e., protection against DoS attacks. To realize the WSNs security, there usually exit two ways: preventing and detection mechanisms. The objective of preventing mechanism is to prevent attacks, while the detection mechanism is to detect whether there is any invasion events or not, which is performed by the IDS. The IDS can monitor the WSNs running status and provide real-time detection for internal and external attacks.

Game theory can be used to capture the nature of conflict in WSNs security. The essence of the attack-defend can be expressed by mutual strategies of interdependence. Thus, WSNs security can be modeled by at least two players interacting in an attempt to maximize their intended objectives. The defender's decision strategies are closely related to those of the attacker and vice versa. Whether defensive strategy is effective will not only depend on the defender's own behavior but also depend on the attacker's strategy. Besides, game theory can be utilized to perform tactical analysis of the options of WSNs threats produced either by a single attacker or by an organized group. It has the ability to examine the huge number of possible threat scenarios in WSNs. Game theory can also provide methods for suggesting several probable actions along with the predicted outcome to control future threats. Therefore, it is very profitable to employ the game theory to study the optimal attack and defense decision-making problems.

There are some papers studying the WSNs security using game theory up to date, after we have looked for keywords *game theory*, *security* and *Wireless Sensor Networks* in ScienceDirect, IEEE Xplore, Springerlink, World Scientific, and ACM digital library. The typical applications include preventing DoS attacks, intrusion detection, strengthening security, and coexistence with malicious modes. The game types for preventing DoS attacks include non-cooperative game [4], cooperative game [6], and repeated game [8, 9]. Those for intrusion detection include non-cooperative game [10-13] and Markov game [15]. Auction theory [5] and coalitional game [16] are for strengthening security while only signaling game [18] is for coexistence with malicious

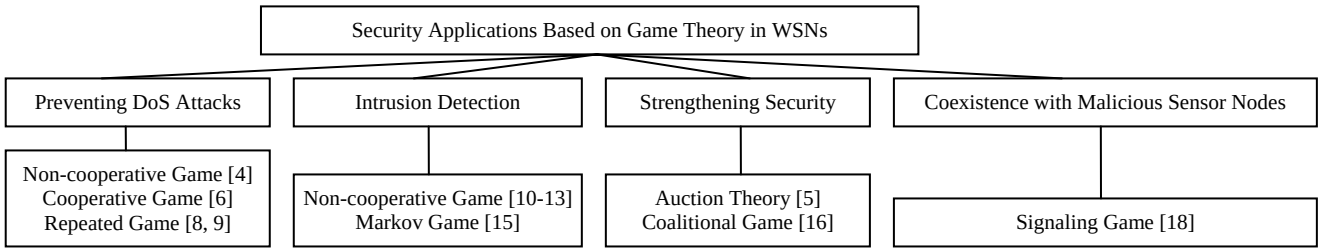

Figure 1. Taxonomy on Current Approaches Based on Game Theory for WSNs Security

sensor nodes. Fig. 1 illustrates the classification of all exiting typical applications to secure WSNs based on game-theoretic approaches. Among these authors, A. Agah *et al.* present the most papers [4-6, 8] that solve the problems of preventing DoS attacks and strengthening security with non-cooperative game [4], cooperative game [6], repeated game [8], and auction theory [5]. From the aspect of affiliations of authors, A. Agah *et al.* [4-6, 8] are in University of Texas, J. M. McCune *et al.* [9] are in Carnegie Mellon University, Y. B. Reddy [10] is in Grambling State University, M. Kodialam *et al.* [12] are in Bell Laboratories, and W. Wang *et al.* [18] are in University of Central Florida, they all are in USA; L. Yang *et al.* [9] are in Northwestern Polytechnical University, Y. Mao *et al.* [13] are in Lanzhou University, and X. Li *et al.* [16] are in The Chinese University of Hong Kong, they all are in China; and T. Alpcan *et al.* [15] are in Technische Universität Berlin, Germany.

III. TAXONOMY ON CURRENT APPROACHES

A. Preventing DoS Attacks

1) Overview

In order to prevent DoS attacks in WSNs and provide a secure routing, the authors in [4] formulate the attack-defense problem as a two-player, nonzero-sum, and non-cooperative game between the attacker and the WSNs. The game is formulated as follows. With respect to one fixed actor sensor node k, the attacker has three strategies: (AS_1) attack sensor node k, (AS_2) does not attack at all, or (AS_3) attack a different actor sensor node. Correspondingly, the WSNs have two strategies: (SS_1) defend sensor node k, or (SS_2) defend a different sensor node. The payoffs of these two players are expressed in the form of 2×3 matrices A and B, which denote the WSNs' and the attacker's payoffs respectively. The authors define $U(t)$ to be the utility of WSNs' ongoing sessions, AL_k to be the average loss of loosing actor sensor node k, C_k to be the average cost of defending actor sensor node k, and N_k to be the number of sensor nodes communicating with actor sensor node k. Then the WSNs' payoff matrix $A=[a_{ij}]$ is defined as

$$\begin{bmatrix} U(t)-C_k & U(t)-C_k & U(t)-C_k-\sum_{i=1}^{N_{k'}} AL_{k'} \\ U(t)-C_{k'}-\sum_{i=1}^{N_k} AL_k & U(t)-C_{k'} & U(t)-C_{k'}-\sum_{i=1}^{N_{k''}} AL_{k''} \end{bmatrix}, \quad (5)$$

where a_{11} represents (AS_1, SS_1) when the attacker and the WSNs choose the same sensor node k, to attack and to defend respectively; a_{12} represents (AS_2, SS_1) when the attacker does not attack at all, but the WSNs defend sensor node k; a_{13} represents (AS_3, SS_1) when the attacker attacks sensor node k', but the WSNs defend sensor node k; a_{21} represents (AS_1, SS_2) when the attacker attacks actor senor node k, but the WSNs defend actor sensor node k'; a_{22} represents (AS_2, SS_2) when the attacker does not attack at all, but the WSNs defend actor sensor node k'; a_{23} represents (AS_3, SS_2) when the attacker attacks actor sensor node k'', but the WSNs defend a different actor sensor node k'. To calculate the attacker payoff matrix, the authors define three parameters: CW to be the cost of waiting and deciding to attack in the future; CI to be the cost of intrusion for attacker; $PI(t)$ to be the average profit of each attack. Then the attacker's payoff matrix $B=[b_{ij}]$ is defined as

$$\begin{bmatrix} PI(t)-CI & CW & PI(t)-CI \\ PI(t)-CI & CW & PI(t)-CI \end{bmatrix}, \quad (6)$$

where b_{11} and b_{21} represent the attacker attacks the sensor node k; b_{12} and b_{22} represent the attacker does not attack any nodes; b_{13} and b_{23} represent the attacker attacks the different sensor nodes rather than sensor node k. The authors prove that the game has Nash equilibrium at strategy pair (AS_1, SS_1). Based on this, they propose two novel schemes for preventing DoS attack. One is called Utility based Dynamic Source Routing (UDSR), which incorporates the total utility of each route in data packets. The other is based on a watch-list, where each sensor node earns a rating from its neighbors, based on its previous cooperation in the network. They compare DSR [28] with UDSR in terms of average number of packets dropped versus pause time and average number of packets dropped per packet received versus *a)* pause time, *b)* percentages of malicious sensor nodes, and *c)* number of sensor nodes. They also compare DSR [28], UDSR with watch-list [4] in terms of average number of packets dropped versus number of sensor nodes and average number of packets dropped per packet sent versus pause time. Experiment results show that the proposed game framework significantly increases the chance of success in defense strategy for WSNs.

The authors in [6] study the case of malicious sensor nodes refusing to forward incoming packets. They consider WSNs as fully dynamic networks and all communication between clusters is through cluster heads.

They define an optimal payoff function that fulfills the objective for securing a sensor network based on cooperative game. This function consists of three factors: cooperation, reputation, and quality of security. To calculate the payoff between two sensor nodes, the authors consider *a)* sensor nodes' distance, *b)* each sensor node's transmitter signal strength, *c)* how many packets each sensor node receives and forwards at each time slot, and *d)* the trustworthiness of the traffic. The more the transmitter signal strength is, the more the sensor node cooperates with its neighbors. The cooperation between sensor nodes is defined as a function of the minimum signal strength for cooperation, and distance between the sensor nodes and the cost of packet forwarding. The reputation is defined as the ratio of the number of packets forwarded to the total number of received and generated packets between two sensor nodes. It can measure the experienced throughput between every two sensor nodes. The quality of security is defined as the percentage of exposed traffic if security is compromised. Then, the payoff utility function for this game is defined as a weighted function of the cooperation, reputation and the quality of security parameters. If there are enough reputation level, closeness of sensor nodes and good history of joint operation, then the strategy is to cooperate by receiving or forwarding incoming packets; otherwise the strategy is to defect. Because WSNs are dynamic, a sensor node's movement results in changing formation of new clusters and cluster heads. They find that the equilibrium point of the game for any two sensor nodes in same or different clusters is the highest probability of cooperation. In their simulation experiments, they compare the distance-based approach with the utility- based approach in terms of average number of messages passed per sensor node versus time, average number of clusters versus time, average number of message passed for deleting clusters versus time, and average number of message passed for deleting a sensor node from a cluster versus time. They show that the distance-based approach performs worse than the utility-based approach by requiring more number of messages for cluster deletion, more number of clusters, and more number of messages passed per unit time.

A repeated game is a class of dynamic games, in which a game is played numerous times and the players can observe the outcome of the previous game before attending the next repetition [7]. The authors in [8] study the case of preventing passive DoS attacks at routing layer in WSNs. They study a repeated game formulation between malicious sensor nodes and an intrusion detector. Here malicious sensor nodes are those sensor nodes that do not forward incoming packets. The intrusion detector residing at the BS keeps track of sensor nodes' collaboration by monitoring sensor nodes. According to the trigger thresholds, the intrusion detector rates all the sensor nodes in different reputation. It uses the history of sensor node's collaboration to determine paths comprising of malicious sensor nodes. Each sensor node can make one of two decisions: accept a packet and forward it to improve its own reputation *(Normal)*, or do not cooperate and save its own battery life selfishly *(Malicious)*. Correspondingly, the intrusion detector can take one of two actions: miss it, or catch it while being *Malicious*. When a sensor node is *Normal* but the detector catches it as *Malicious*, or when a malicious sensor node is not detected, payoff of one player is the maximum while the other player is the minimum. The least concern is when the detector misses a *Normal* sensor node. According to these four different cases, the intrusion detector has different utility value, which is given by a weighted sum of the product of the payoff function. To ensure the finiteness of the repeated game payoffs, a discounted payoff is introduced, and then the future payoffs are multiplied by a discount payoff related to earlier payoffs. When the intrusion detector and the sensor nodes play the game cooperatively, the Nash equilibrium is reached. The protocol based on repeated game ensures sensor nodes that want to increase their reputation will provide services. In their performance evaluation, they consider average number of hops versus percentage of malicious sensor nodes as well as percentage of successful DoS detection versus number of sensor nodes. They compare 5 hops with 7 hops in terms of throughput versus percentage of malicious sensor nodes, compare a normal sensor node with a malicious sensor node in terms of throughput versus time, and compare 30% malicious sensor nodes with 60% malicious sensor nodes in terms of percentage of detection versus average number of observations. Experiment results show that the throughput drops and the average path length for a received packet diminishes with increasing malicious sensor nodes.

The authors in [9] study the problem of dropping packets attacks in WSNs. Similar to [8], they also model the interactions among sensor nodes as a repeated game. Because misbehavior conducted by malicious sensor nodes will propagate the distrust to entire network, regular sensor nodes will prefer to get the highest payoff by choosing the best strategy. In this fixed-time game, there is a single Nash equilibrium while not all the sensor nodes cooperate. The authors introduce an attack-resistant mechanism to prevent the attacker from the misbehavior when the malicious sensor nodes realize that it is too expensive for attacking and switch to a strategy of cooperation. This mechanism is realized by punishment mainly. When an errant sensor node drops packets and is caught by its neighbors. The errant sensor node will be punished by other sensor nodes, which will drop any packets transmitted to it. It will not be allowed to return to the network until it cooperates for the next timeslot. When the game is repeated infinitely, the malicious sensor nodes will be concerned about the latent compensation for attacking. Since the end of the game is unpredictable, the goal of all sensor nodes is changed to the maximization of their cumulative payoff. The authors deduce that there is Nash equilibrium in the repeated game. They evaluate the influence of the game in terms of throughput versus ratio of malicious sensor nodes. Simulation results show that the throughput decreases rapidly along with the increase of malicious sensor nodes density.

2) Discussion

The proposed approach in [4] keeps the number of dropped packets constant irrespective of the network size. After recognizing and labeling some sensor nodes as malicious ones as bad behavior propagates the throughout of the network, other sensor nodes in the network can ignore these malicious sensor nodes for their future packet forwarding requests. This approach provides an automatic method for the social mechanisms of reputation and cooperation, as well as guarantees a more reliable delivery. However, there is a problem of false labeling, which must be coped with. Besides, defining an acceptable threshold for cooperation and reputation of sensor nodes is very difficult.

Cooperative game used in [6] is a useful method for forming secure clustering, where each cluster is a cooperative environment. Stronger cooperation between two sensor nodes implies more reliable data communication between them. Moreover, the more a sensor node cooperates, the better its reputation is. By choosing this cooperation formula, more power for sensor nodes is conserved and cooperation among heterogeneous sensor nodes is built. Trust and security decisions based on the payoff function are also built while keeping the mobility and volatility transparent. However, how to stable the payoff function with respect to the movement patterns of the sensor node is a problem. The other problem is how to select the optimal parameter setting of cluster formation for reducing the message passed.

The method in [8] based on repeated game achieves the truthfulness by recognizing the presence of sensor nodes that agree to forward packets but fail to do so. This approach can distinguish different sensor nodes with respect to their dynamical measured behavior. Using the repeated game, the BS has a history of the previous games and when a sensor node is malicious it gets a negative reputation while the total reputation is computed, thus a path including less number of malicious sensor nodes is chosen to be the wining path. This results in isolation of malicious sensor nodes. In fact, infinite repetition is the key for obtaining behavior in the stage games, whereas it is not realistic. The authors propose a discount payoff to ensure the finiteness, but how to select a rational value is a problem. Also, the BS credibility should be considered.

The attack-resistant mechanism in [9] based on repeated game prevents dropping packets attack effectively. The introduced punishment mechanism impels sensor nodes to reach a collaborative Nash equilibrium. This cooperation stimulation mechanism does not require any tamper-proof hardware or central banking services. It can compensate the low misbehavior detection efficiency by choosing reasonable configuration parameters. However, how to balance the price of misbehavior punishment and the gain of cooperation of all sensor nodes in WSNs is a problem.

B. Intrusion Detection

1) Overview

The authors in [10] consider sensor network broadcast environment, where malicious sensor nodes can deprive other sensor nodes from receiving a broadcast message, which is called a Denial of Message (DOM) attack. A simple approach avoiding this attack is for every broadcast recipient sending an authenticated acknowledgment for each broadcast message. However, this approach results in ACK implosion problem so they propose a Secure Implicit Sampling (SIS) protocol that works by eliciting authenticated acknowledgements from a subset of sensor nodes per broadcast, where the subset is unpredictable and tunable to the DOM attack so as to mitigate ACK implosion on the BS. The SIS requests message acknowledgments by controlled probabilistic checking. Based on cryptographic techniques, the SIS constrains an attacker such that he is unable to guess ahead of time which subset of sensor nodes is sampled. They consider the attacker and SIS as two players in a zero-sum game. An attacker's best strategy is to compromise all neighbor sensor nodes of the BS, in this way, he achieves maximum payoff. Once the attacker is detected, his payoff goes to zero. Thus a clever attacker will try to remain undetected with high probability while still doing damage to the network. In practice, the attacker's optimal strategy depends on the attack's countermeasures we perform upon detection of malicious behavior. The equilibrium of the game is given by a minimax construction on the payoff. The authors test SIS performance with blind flooding as the broadcast algorithm by extending GloMoSim. They configure GloMoSim to use a Bellman-Ford routing protocol to route acknowledgements back to the BS. Their analysis of SIS is based on the number of deprived sensor nodes, rather than the number of attacking sensor nodes. As the number of victim sensor nodes increases, the attackers' impacts on the network become detectable by SIS. They compare simulation results with theoretical expected performance in terms of probability of detection versus number of deprived sensor nodes. Simulation results show that the transmission resulting in a greater natural loss probability of acknowledgements increase as the number of sensor nodes sampled increases.

The author in [11] studies intrusion detection technique when the data are transferred from sensor nodes to the BS. During transferring data between sensor nodes and the BS, the attacker always tries to control the routing layer of the sensor nodes so that the data flow will be disrupted. When the sensor nodes are formed into clusters, the attacker targets the routing layer at cluster head to jam the data flow or drop the packers. The author considers that the IDS at the cluster head monitors the data transfer from sensor nodes to cluster head and tries to maintain the normal functionality of the network while the attacker may attack any sensor nodes in the cluster and try to disturb the network. This case is modeled by a two-player, zero-sum, and non-cooperative game. The attacker maximizes its benefit by destroying the functionality of the system while the IDS tries to protect the facility. The author proves that the game is not Pareto optimal and has no pure Nash equilibrium. Finally, the author selects several intermediate sensor nodes along the forwarding path to detect the malicious sensor nodes using the game.

The authors in [12] consider that intrusion detection is accomplished by sampling a portion of the packets that are

transmitted through selected network links or router interfaces. Because sampling incurs network costs, it is necessary to develop a sampling strategy that does not exceed a given total sampling budget, which is considered in a game-theoretic framework. They model a game between the intruder and the service provider. When the intruder injects a malicious packet from some malicious sensor nodes to attack a target sensor node, the service provider samples packets on the links in the network to detect and prevent the intrusion. Since sampling is expensive to perform in real time, the authors set a bound on the sampling rate. This bound represents the maximum rate at which the sensor node for intrusion detection can process packets in real time. The intruder minimizes the probability to be detected while the service provider maximizes the detection number of malicious sensor nodes. Obviously, this is a two-player and zero-sum game, where the payoffs of the intruder and the service provider add up to zero. It is well known that there exists a minmax optimal solution to the game, which is Nash equilibrium for a zero-sum game. According to the minmax optimal solution, along any paths the intruder chooses, the malicious packets will be sampled at most on a link. If the bound is equal to or greater than the maximum flow from a source sensor node to a target sensor node, the malicious packets will always be detected; otherwise, there is non-null probability that the malicious packets will be detected. The authors perform three cases of experiments: *a)* single attack sensor node and single target sensor node, *b)* multiple attack sensor nodes and single target sensor node, and *c)* multiple attack sensor nodes and multiple target sensor nodes. For each of the cases, they run three different algorithms: minimization of maximum link utilization algorithm [12], flow flushing algorithm [12], and cut saturation algorithm [12]. Experiment results show that the maximum flow value can be changed significantly by changing the routing in the network, as well as the performance of the flow flushing algorithm and the cut saturation algorithm are quite similar, and better than the simple minimization of maximum link utilization algorithm.

The authors in [13] study the intrusion detection in cluster-based WSNs. They select the HYENAS [14] algorithm for choosing a cluster head sensor node. The IDS is placed on each cluster head sensor node. A non-cooperative game-theoretic framework is used to help each cluster head sensor node decide the probability of starting up IDS service. The game is played between an attacker and a cluster head sensor node. The set of strategies of the head sensor node is {*monitor, attacked*}, which means respectively the IDS being started, or the cluster head sensor node being attacked. The set of strategies of the attacker is {*attacking, waiting*}, which means respectively attacking the cluster head sensor node, or doing nothing but waiting for. Then, the net utility can be computed. For example, for the action profile (*monitor, attacking*), the cluster head sensor node gain is equal to the payoff of not being attacked minus the cost of starting IDS; the attacker losses the cost of attacking the cluster head sensor node. The authors prove that there is not pure strategy of Nash equilibrium in the game. Theoretical analysis of network performance based on the proposed game model concludes that the proposed game can greatly reduce the resource consumption that is caused by the cluster head sensor node starting IDS to monitor attacks. At the same time, the authors perform simulations in GloMoSim. For achieving the resource consumption situation of the sensor network, they compare all monitor model [13] with game theory model in terms of number of invalid sensor nodes versus time. They also give different probability of succeeding in detecting several attacks that include Jamming, Exhaustion, Misdirection, and Flooding. Simulation results show that the intrusion detection based on their proposed game can reduce the resources consumption caused by monitoring sensor nodes.

The authors in [15] model the interactions between malicious attackers and the IDS with Markov game, which is a two-player and zero-sum game. This game is extended to a stochastic and dynamic one. They consider the sensor nodes observing and reporting the attacks to the IDS as a finite-state Markov chain. According to the degree of knowing the WSNs characteristics and the opponents' actions, they discuss three different information structures: *a)* full information, *b)* no information about sensor network characteristics, and *c)* having only information about own costs, past actions, and past states. In the case of full information, each player knows everything about the WSNs, so, he can use well-known Markov Decision Process (MDP) method to compute his own optimal mixed strategy solution to the game. In the case of no information, the attacker can calculate its optimal strategy using minmax-Q, which is a variation of the standard Q-learning technique [15]. In the third case, the players use a single agent naïve Q-learning scheme [26] to optimize their strategies, which ignores the other players' actions. The authors numerically analyze the payoffs of malicious attackers and the IDS as well as evolution of mutual cost values under different information structures and various game parameters.

2) Discussion

In the presence of message loss, detecting a stealthy attacker is a challenge. The proposed SIS in [10] can detect an adversary and reduce the number of acknowledgements sent to the BS. Even if the attacker can ascertain that an uncompromised sensor node acknowledges a broadcast only by observing the acknowledgements produced by the other sensor nodes, it is too late for him to disrupt the other sensor nodes from receiving this broadcast. However, their model is assumed in the environment where the WSNs operate under stable conditions, that is, sensor nodes are immobile and do not fail over time.

Because total number of acknowledgements expected to receive at the source equals to the sum of the acknowledgements received and dropped, the approach in [11] using zero-sum game may find malicious sensor nodes in the forwarding path. However, there are not enough simulations to evaluate this approach. Only a simple example, the total energy spent by both the IDS

and the attacker equates zero or the total energy must not change, is done.

The idea of modeling intrusion detection in [12] using sampling in WSNs based on a game-theoretic framework is a very early attempt. In fact, this approach leads to a routing problem because the service provider needs to maximize the chances of detecting malicious packets. The solution to the game is a maximum flow problem, and the routing problem can be formulated as a multi-commodity flow problem. Due to the sampling way, the game-theoretic results are much more natural than the discrete allocation models. However, more experiments should be performed for ensuring the effectiveness of this method.

The proposed method in [13] not only improves the security of WSNs, but also reduces the cost caused by monitoring sensor nodes and prolongs the lifecycle of each sensor node. However, the method does not consider the effects of the selfishness of the sensor nodes, which can discard normal packets or not transfer normal packets in WSNs.

The stochastic and dynamic Markov game in [15] can capture the complexities of the underlying system further. By deploying dynamic learning methods, the players can consider future costs for optimizing their strategies. They can refine their own strategies offline or online by learning more about the system and their adversaries continuously. Thus, a more realistic depiction of the interactions between the attacker and the IDS can be obtained. However, simulation experiments should be performed for validating the effectiveness of intrusion detection based on Markov game, although there is a numerical analysis process.

C. Strengthening Security

1) Overview

An auction is a method for allocating scarce foods based on competition. A seller wants to make more money possibly while a buyer wishes to pay less. Generally, there are four major auction formats: English, Dutch, First-Price and Second-Price sealed auctions [5]. The authors in [5] propose a Secure Auction based Routing (SAR) protocol using the First-Price auction format. In their First-Price sealed auction, the bidder with the highest bid wins the auction and reaches equilibrium, and thereafter the truth bidding is a dominant strategy for sensor nodes. Both malicious and truthful sensor nodes compete against each other in order to forward incoming packets and, by doing so, each sensor node improves its reputation among other sensor nodes. If a sensor node does not have enough battery power, then it does not participate in bidding; the winner of the bid loses a percentage of its battery power. The sensor nodes decide by themselves to whether to participate in an auction, whereas a malicious sensor node tries its best to win the bid, drop the packets, and corrupt the network. In the proposed protocol, a Route-request message is sent out from a source sensor node. If all other sensor nodes receiving this message have not received the same request yet, then they put themselves into the route and forward it to their neighbors. If a receiving sensor node is the destination, then it does not forward the request but send a Reply-message containing the full source route and the bid price that it is willing to pay. After receiving several routes, the source sensor node selects the highest bid one, stores it and sends messages along it. The auction on routes ensures a view on which sensor nodes will provide possible service. This sealed-bid auction is a typical static game with incomplete information. A sensor node knows its own valuation of other bidders. There is a Nash equilibrium to solve the sealed-bid auction, which is a point that no sensor nodes want to deviate. The payoff of each sensor node is calculated based on battery power and reputation. The authors consider communication and computation of sensor nodes when computing the required power for each sensor node. If a sensor node saves its power by not forwarding incoming packets or dropping them for its selfishness, then it will be isolated from the network and get a bad reputation; otherwise, it will get a good reputation. As a result, sensor nodes prefer to participate in forwarding incoming packets and gaining reputation. The competition of sensor nodes is based on First-Price sealed auction above. The amount of a bid that each sensor node offers is equal to its utility value; the price that a winner of a bid pays is a reduction in its battery power. The sensor node's truthful bidding is a dominant strategy. As time passes, more sensor nodes select route paths through sensor nodes with good reputation. They simulate the SAR protocol in NS2, considering three different types of attacks: IP spoofing attack, the black holes attack, and a falsify route error message attack. They compare no secure routing, CONFIDANT [29] with SAR in terms of average number of packets dropped versus *a)* pause time, *b)* percentage of malicious sensor nodes, and *c)* numbers of sensor nodes, as well as the reputation of a malicious sensor node versus pause time. They compare no secure routing, INSENS [30] with SAR in terms of routing overhead versus number of sensor nodes. Experiment results show that the SAR protocol can guarantee more reliable delivery as well as it can observe the behavior of sensor nodes and isolate suspicious sensor nodes by defining an acceptable threshold for reputation of sensor nodes.

The authors in [16] study how to strengthen security in WSNs using coalitional game. They propose a throughput characteristic function that describes the total expected gain of a coalition from the cooperation. For finding a reliable routing path, they formulate a coalition to a weighted and directed graph, where vertexes represent sensor nodes in the coalition, edges represent routing directions between sensor nodes, and weights represent probabilities that a sensor node wants to communicate with another. From the graph, a possible routing path can be discovered by a routing discovery procedure. The number of routing paths is related to the size of the coalition. When the coalition size increases, more reliable routes can be obtained. In order to fairly distribute the gains among all sensor nodes, they consider Shapley value method and prove that it is applicable to the payoff allocation inside coalitions given their proposed throughput characteristic function. The set of strategies of each sensor node is *{join, notjoin}*, which means the

sensor node either joins or does not join into a coalition respectively. Some game rules are defined as follows: *a)* A sensor node will join into a coalition only if it can get more payoff than being alone; *b)* A sensor node will deviate from the current coalition and join into another coalition only if it can get more payoff in the future than current; *c)* A coalition will refuse a sensor node if the sensor node can not increase the total payoff of the coalition; *d)* A coalition will exclude a sensor node if the sensor node can not benefit the coalition; *e)* Sensor nodes failing to join into any coalitions will be denied from the WSNs. These rules form a threatening mechanism for sensor nodes in WSNs. Under the game rules above, the selfish sensor nodes that do not forward others' data packets will hardly be admitted into coalitions because of their poor reputation. The coalitional game model can be integrated with all kinds of routing protocols. The authors take AODV [17] routing protocol for example. Theoretical analysis is performed by two aspects. One is the speed of convergence and the size of coalition. The other is the non-emptiness of core. They show that the convergence time of formation is short and the size will keep growing until a grand coalition is reached. They also show that the core in WSNs is difficult to achieve and easy to be destroyed.

2) Discussion

The security enforcement in [5] using auction theory can detect non-cooperative sensor nodes. This secure mechanism does not need to establish key and store long sized keys. It also does not require a monitor and rating system at each individual sensor node, which saves the memory and battery power of sensor nodes. The SAR protocol in [5] can seize the dynamics of a large group of players, and the strategy chosen by a player not only depends on a self-interested perception of the game but also takes into account a group of policies for all the players. However, when a subset of bidders gather together and do not agree to outbid each other, which has the overall effect of lowering the winning bid, the functionality of the SAR should be confirmed. Different bidders have not the same motivations. When these bidders agree to reduce competition by no competition against each other, the impaction of the cooperation between sensor nodes should be researched furthermore.

Cooperation is the inherent nature of WSNs. Formulating the sensor network as cooperative game will not destroy this nature but make full use of it. The coalitional game used in [16] can strengthen security in WSNs. A coalition can achieve the maximal throughout and the most reliable traffic. The presented game rules establish effectively a threatening mechanism. In such rules, sensor nodes are enforced to participate in a coalition and those that cannot join into any coalitions are under very high suspicion of being malicious. The theoretical analysis justifies the correctness of the formulation. However, it is lack of simulation experiments for validating the performance of coalitional game integrated with the routing protocol, such as AODV, DSR [27], and so on.

D. Coexistence with Malicious Sensor Nodes

1) Overview

The authors in [18] study the interactions between a malicious sensor node and a regular sensor node in WSNs. Even if a malicious sensor node is detected, it does not know whether it has been identified or not, and it still disguises itself like a regular sensor node. Therefore, there might be situations where malicious sensor nodes can be kept and used. This coexistence gives both the malicious and regular sensor nodes different benefits. In this situation, the authors formalize the interactions into two games. The first game, namely malicious sensor node detection game, is a signaling game that is a special category of Bayesian game with imperfect information. The second game, called post-detection game, is played when the regular sensor node knows confidently that its opponent is a malicious sensor node. The authors apply signaling game, which is played between a sender and a receiver, to model the process of detecting the malicious sensor nodes in the network. The set of strategies of the sender is *{Attack, Forward}*. *Attack* means the sender is malicious while *Forward* means the sender is regular or a malicious sensor node disguises itself. The set of strategies of the receiver is *{Monitor, Idle}*, which means the receiver monitors the sender or not respectively. Then, the net utility can be computed. For example, for the action profile *(Attack, Monitor)*, the attacking malicious sensor node (sender) losses the sum of the payoff of a malicious sensor node to attack successfully and the associated cost; the receiver gain is equal to the payoff of a malicious sensor node to attack successfully minus the monitoring cost. The authors prove that there is a mixed strategy Bayesian Nash equilibrium. They apply dynamic Bayesian game theory to solve the problem of updating the belief dynamically. If a sensor node monitors continuously, its belief can be calculated with the belief it holds at the immediate previous stage and the actions it observed. Under this belief system, the game is played in a sequential manner. The best response strategies of sensor nodes are dependent on the current beliefs held by the sensor nodes. Thus, Perfect Bayesian Equilibrium (PBE) can be applied to characterize the aforementioned dependency. Then, the authors prove that the dynamic malicious sensor node detection game has a PBE. Compared to the malicious sensor node detection game, the sender and the receiver in the post-detection game have the same strategies. However, a coexistence index is introduced if the coexistence index for the sender falls under a certain threshold, then the receiver will isolate the sender and terminate the post-detection game because keeping the sender is no longer beneficial; otherwise, the game will be played in a repeated manner. The authors also state the post-detection game has a mixed strategy Nash equilibrium. Finally, the authors study the properties of the perfect Bayesian Nash equilibrium in the malicious sensor node detection game and the post-detection sub-game perfect Nash equilibrium through simulations. Simulation results show that the malicious sensor node decreases its attack rate and does more packet forwarding as a regular sensor node for a larger attack gain. Thus,

malicious and regular sensor nodes can coexist, and coexistence equilibrium improves the throughput of the network.

2) Discussion

Coexistence with malicious sensor nodes in [18] based on game theory improves the network throughput and extends the network lifetime. Malicious sensor nodes and regular sensor nodes can coexist as long as the destruction they bring is less than the contribution they make. Especially when the network resources are limited, every regular sensor node has to forward packets economically in order to prolong the lifetime of the network, if a malicious sensor node can be used to handle some traffic, it is beneficial. Be different to traditional method, this idea takes the WSNs security a novel approach. However, simulations should be depicted further. The authors do not mention where their simulations are done and how to configure the simulation environment.

IV. DIRECTIONS FOR FUTURE RESEARCH

In order to realize the broad applications of WSNs, security in WSNs is an emerging area with many remaining issues. WSNs security system is a complex giant system in which mutual profit-actors are interdependent to form players of WSNs security game. The process of implementing WSNs security is an adaptive and dynamic process that evolves continually. The players interact with another for decision-making, forming the basic pattern of WSNs security game. Therefore, studying WSNs security with game theory has higher scientificity and rationality, which is a very promising future direction of development. We consider areas for future research as follows.

- BS credibility: Current secure approaches based on game theory for WSNs assume that the BS is trustworthy or do not consider the security of BS. In fact, there are many situations, for example the battlefield, where the BS is easy to destroyed or attacked. Therefore, when new schemes or approaches based on game theory are designed to secure WSNs, how to realize mutual trust between the BS and sensor nodes for preventing from disguising data should be considered.
- IDS efficiency: Current IDSs based on game theory monitor all sensor nodes in WSNs without emphasis, which makes the IDS less efficient. Due to the hard work, the IDS performance may descent sharply, and may even make itself unpractical. If an IDS is designed to centralize its resources on the sensor nodes that have larger malicious probabilities, then it is more efficient. However, how to realize this intelligent IDS need to be studied further.
- WSNs mobility: Current proposed detection mechanisms and secure routing protocols based on game theory focus on static WSNs, ignoring mobility. This mobility may be at the BS, sensor nodes, or both. In fact, the WSNs topology changes frequently due to sensor nodes' energy consumption or mobility. However, secure routing protocols now cannot be applied to mobile WSNs environment directly. Designing novel detection mechanisms and secure routing protocols for mobile WSNs need to be developed.
- WSNs QoS: Current WSNs security research based on game theory only focus on individual topics. However, introducing game theory to WSNs security will decline WSNs performance significantly. In order to achieve more benefits, how to balance the contradictory between security and QoS need to be studied.
- Real-world applicability: Current WSNs security studies are evaluated by simulations or controlled laboratory experiments, even not evaluated by any methods. However, WSNs are applied in noisy, unpredictable real-world environment. Thus, it is necessary to evaluate the applicability of WSNs security based on game theory in a real-world setting for practical applications, although which is very difficult.
- Energy consumption: Energy consumption is one of important evaluating value of WSNs. Current preventing or detecting mechanisms based on game theory devote to their accuracy rates but do not consider the energy consumption issues. How to decrease energy consumption of methods based on game theory decides whether these methods become practical or not.
- Sensor nodes learning: As soon as intelligence is considered as decision-making part, each player will employ a learning mechanism to predict the behavior of other players in addition to access to the history of game. Limited memory of sensor nodes will become the most influent actor. Therefore, efficient learning mechanisms based on game theory need to be developed.
- Expanding game theory applications and different games: The WSNs protocol stack consists of application layer, transport layer, network layer, data link layer, and physical layer. The game-theoretic approaches used clearly to prevent DoS attacks include non-cooperative game [4], cooperative game [6], and repeated game [8, 9]. In fact, there are many other various attacks in different layers. The data link layer attacks include collision, abuse of MAC priority schemes, and exhaustion of battery resources. The network layer attacks include *a)* Spoofed, altered or replaying information, *b)* Selective forwarding, *c)* Sinkhole attacks, *d)* Sybil attack, *e)* Wormholes, *f)* Hello flood attacks, and *g)* Acknowledgement spoofing. The transport layer can be attacked via flooding or de-synchronization. How to apply game theory to all attacks above is worth studying further. At the same time, some other different games, e.g., evolutionary game may be considered to solve the security problems in WSNs.

V. Related Work

The works related to this paper, which are for WSNs, mainly include surveys on intrusion detection system, security, and game theory.

The authors in [19] present a detailed discussion and an analysis of the existing intrusion detection systems for WSNs. They classify these systems' approaches into three categories: purely distributed, purely centralized and distributed-centralized, according to the place of installing an IDS agent. The authors in [1, 3, 20-23] all survey the security in WSNs. In [1], the authors outline the constraints, security requirements, and attacks with their corresponding countermeasures in WSNs. They classify these security issues into five categories: cryptography, key management, secure routing, secure data aggregation, and intrusion detection. They also highlight the advantages and disadvantages of various WSNs security protocols in each category and conclude some possible future research directions on security in WSNs. In [3], the authors analyze the relationship between different security threats, requirements, applications, and security technologies. In [20], the authors identify the threats and vulnerabilities to WSNs and summarize the defense methods based on the network protocol layer's analysis. They divide these secure issues into seven categories: cryptography, key management, attack detections and preventions, secure routing, secure location security, secure data fusion, and other security issues. They also point out open research issues and directions in each category. In [21], the authors discuss security challenges and vulnerabilities in WSNs. They survey representative security mechanisms designed to address known vulnerabilities and highlight key research issues that remain to be tackled. In [22] the authors classify the main aspects of WSNs security into four categories: the obstacles to sensor network security, the requirements of a secure wireless sensor network, attacks, and defensive measures. They provide an overview of the rather broad areas of WSNs security. In [23], the authors describe the security challenges, threats and attacks that WSNs suffer from, along with security techniques proposed to address them. They stress and point out the main drawbacks of the existing solutions of key management for WSNs. The authors in [24] survey the existing game-theoretic solutions that are designed to enhance network security and present the taxonomy for classifying the proposed solutions. According to the situations of network security, they divide game theory into non-cooperative game and cooperative game. Then, non-cooperative game is divided into static game and dynamic game. Furthermore, static game is divided into *a)* complete and imperfect information game, and *b)* incomplete and imperfect information game while dynamic game is divided into *a)* complete and perfect information game, *b)* complete and imperfect information, *c)* incomplete and perfect information game, and *d)* incomplete and imperfect information game. The authors in [25] survey the use of concepts of game theory to solve the problems of energy efficiency, security, and detection and tracking in WSNs. They discuss the game-theoretic approaches in WSNs for energy efficiency in three aspects: energy conservation, routing, and load balancing. They consider three different security scenarios: intrusion detection, intrusion by injecting a malicious packet, and preventing the broadcast message by malicious sensor nodes. They also summarize recent research on pursuit-evasion game used to model detection, tracking and surveillance applications in WSNs.

Compared to the related works above, our work centrally focuses on game theory in WSNs security. To our best knowledge of knowing, there is no paper centrally concerned about this focus in ScienceDirect, IEEE Xplore, Springerlink, World scientific, and ACM digital library. Compared to [25], our work is more detailed and comprehensive. With respect to different attack-defense scenarios, we classify these game-theoretic approaches into different applications in Fig. 1. We also propose some areas for future research in WSNs security based on game theory.

VI. Conclusion

The field of WSNs security is a very important research area. Due to the limited capabilities of sensor nodes, providing security to sensor networks is a challenging task, however, there are not popular applications of WSNs without considering WSNs security. Game theory has the capability to exam a larger amount of possible scenarios before performing the action. It can sophisticate a decision process as a modeling tool. The direction of applying game theory to WSNs security is prospective. Some researchers have already explored the game-theoretic approaches to address WSNs security problems and have proposed some competing solutions. In this paper, we have given the taxonomy of exiting approaches in order to provide a global view of game theory for WSNs security. We have categorized existing security application based on game theory into preventing DoS attacks, intrusion detection, strengthening security, and coexistence with malicious sensor nodes. We have found that *a)* there are non-cooperative game [4], cooperative game [6], repeated game [8, 9] for preventing DoS attacks, *b)* there are non-cooperative game [10-13], and Markov game [15] for intrusion detection, *c)* there are auction theory [5] and coalitional game [16] for strengthening security, and *d)* there is only signaling game [18] for coexistence with malicious sensor nodes. We have illustrated the main ideas of each game type applied to WSNs security while we have discussed their advantages and disadvantages. Thus, researchers can efficiently employ these advantages, such as the idea of coexistence with malicious sensor nodes, to form new ideas of WSNs security based on game theory. After looking through these disadvantages, we have proposed some future research areas, which include BS credibility, IDS efficiency, WSNs mobility, WSNs QoS, real-world applicability, energy consumption, sensor nodes learning, and expanding game theory applications and different games. Considering these areas, researchers may propose some novel security mechanisms based on game theory for WSNs security in the future.

ACKNOWLEDGMENT

This work is based on research supported by Hunan Provincial Natural Science Foundation of China under grant No. 07JJ6140, 07JJ6109, 05FJ3018, Zhejiang Provincial Natural Science Foundation of China under grant No. Y1080901, the Key Project of Chinese Ministry of Education under grant No. 104086, and the Project of Chinese Ministry of Education under grant No. CNGI2008-092.

REFERENCES

[1] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," IEEE Communications Surveys & Tutorials, vol. 8, 2006, pp. 2-23.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Communications Magazine, vol. 40, 2002 , pp. 102-114.

[3] J. Lopez, R. Roman, and C. Alcaraz, "Analysis of security threats, requirements, technologies and standards in wireless sensor networks," Lecture Notes in Computer Science, vol. 5705, 2009, pp. 289–338.

[4] A. Agah, K. Basu, and S. K. Das, "Preventing DoS attack in sensor networks: a game theoretic approach," Proc. IEEE International Conference on Communications (ICC 2005), vol. 5, 2005, pp. 3218-3222.

[5] A. Agah, K. Basu, and S. K. Das, "Security enforcement in Wireless Sensor Networks: A framework based on non-cooperative games," Pervasive and Mobile Computing, vol. 2, Apr. 2006, pp. 137-158.

[6] A. Agah, S. K. Das, and K. Basu, "A game theory based approach for security in wireless sensor networks," Proc. IEEE International Conference on Performance, Computing, and Communications, 2004, pp. 259-263.

[7] G. Owen, Game Theory. New York: Academic Press, 2001.

[8] A. Agah and S. K. Das, "Preventing DoS attacks in wireless sensor networks: A repeated game theory approach," International Journal of Network Security, vol.5, Sept. 2007, pp. 145–153.

[9] L. Yang, D. Mu, and X. Cai, "Preventing dropping packets attack in sensor networks: A game theory approach," Wuhan University Journal of Natural Sciences, vol. 13, 2008, pp. 631-635.

[10] J. M. McCune, E. Shi, A. Perrig, and M. K. Reiter, "Detection of denial-of-message attacks on sensor network broadcasts," Proc. IEEE Symposium on Security and Privacy, 2005, pp. 64-78.

[11] Y. B. Reddy, "A game theory approach to detect malicious nodes in wireless sensor networks," Proc. Third International Conference on Sensor Technologies and Applications (SENSORCOMM '09), 2009, pp. 462-468.

[12] M. Kodialam and T. V. Lakshman, "Detecting network intrusions via sampling: A game theoretic approach," Proc. Annual Joint Conference of the IEEE Computer and Communications (INFOCOM 2003), vol. 3, 2003, pp. 1880-1889.

[13] Y. Ma, H. Cao, and J. Ma, "The intrusion detection method based on game theory in wireless sensor network," Proc. IEEE International Conference on Ubi-Media Computing, 2008, pp. 326-331.

[14] P. Tillapart, T. Thumthawatworn, P. Pakdeepinit, T. Yeophantong, S. Charoenvikrom, and J. Daengdej, "Method for cluster heads selection in wireless sensor networks," Proc. IEEE Aerospace Conference, vol. 6, 2004, pp. 3615-3623.

[15] T. Alpcan and T. Basar, "An intrusion detection game with limited observations," http://www.tansu.alpcan.org/papers/isdg06.pdf, Jul. 2006.

[16] X. Li and M. R. Lyu, "A novel coalitional game model for security issues in wireless networks," Proc. IEEE Global Telecommunications Conference (GLOBECOM 2008), 2008, pp. 1-6.

[17] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," RFC 3561, Jul. 2003.

[18] W. Wang, M. Chatterjee, and K. Kwiat, "Coexistence with malicious nodes: A game theoretic approach," Proc. International Conference on Game Theory for Networks (GameNets '09), 2009, pp. 277-286.

[19] A. H. Farooqi and F. A. Khan, "Intrusion Detection Systems for wireless sensor networks: A survey," Proc. Communications in Computer and Information Science, vol. 56, 2009, pp. 234–241.

[20] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: a survey," IEEE Communications Surveys & Tutorials, vol. 11, 2009, pp. 52-73.

[21] E. Sabbah and K. Kang, "Security in wireless sensor networks," in Guide to Wireless Sensor Networks, S. C. Misra, I. Woungang, and S. Misra, Eds. Springer London, 2009, pp. 491-512.

[22] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor networks security: A survey," in Security in Distributed, Grid, and Pervasive Computing, Y. Xiao, Eds. Auerbach Publications, Apr. 2007, pp. 367-410.

[23] K. Kifayat, M. Merabti, Q. Shi, and D. Llewellyn-Jones, "Security in wireless sensor networks," in Handbook of Information and Communication Security, P. Stavroulakis and M. Stamp, Eds. Springer Berlin Heidelberg, 2010, pp. 513-552.

[24] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," Proc. 43rd Hawaii International Conference on System Sciences, 2010, pp. 1-10.

[25] R. Machado and S. Tekinay, "A survey of game-theoretic approaches in wireless sensor networks," Computer Networks, vol. 52, Nov. 2008, pp. 3047-3061.

[26] D. P. Bertsekas, Dynamic Programming and Optimal Control, 2nd edition. Nashua: Athena Scientific, 2001.

[27] D. Johnson, Y. Hu, and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4," RFC 4728, Feb. 2007.

[28] J. Broch, D. B. Johnson, and D. A. Maltz, "The Dynamic Source Routing protocol for mobile Ad Hoc Networks," Internet Draft, http://tools.ietf.org/id/draft-ietf-manet-dsr-03.txt, Oct. 1999.

[29] S. Buchegger and J. L. Boudec, "Performance analysis of the CONFIDANT protocol," Proc. the 3rd ACM international symposium on Mobile ad hoc networking & computing, 2002, pp. 226–236.

[30] J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion-tolerant routing for wireless sensor networks," Computer Communications, Vol. 29, Jan. 2006, pp. 216-230.

Shigen Shen received his B.S. degree in mathematics education from Zhejiang Normal University, Jinhua, China in 1995, his M.S. degree in computer science and technology from Zhejiang University, Hangzhou, China in 2005. He is currently pursuing his Ph.D. in pattern recognition and intelligent system at the College

of Information Science and Technology, Donghua University, Shanghai, China. Also, he is an associate professor at the College of Mathematics and Information Engineering, Jiaxing University, Jiaxing, China. His current research interests include *Wireless Sensor Networks security* and *Game Theory*.

Guangxue Yue is a Ph.D. candidate at the College of Computer and Communication, Hunan University, Changsha, China. Also, he is a professor at the College of Mathematics and Information Engineering, Jiaxing University, Jiaxing, China. His current research interests include *Distributed Computing & Network*, *Network Security*, *Biological Information*, and *Hybrid & Embedded Systems*.

Qiying Cao received his B.S. degree from Harbin Engineering University, Harbin, China in 1982, both his M.S. and Ph.D. degree from Jiangsu University, Zhenjiang, China in 1993 and 1998, respectively. From 1999 to 2001, he was a Post-doctorate at Chunlan Postdoctoral Research Center, Taizhou, China. Currently, he is a professor of computer applications at the School of Computer Science & Technology, Donghua University, Shanghai, China. His current research interests include *Pervasive Computing*, *Ubiquitous Computing* and *Intelligent Information Processing*.