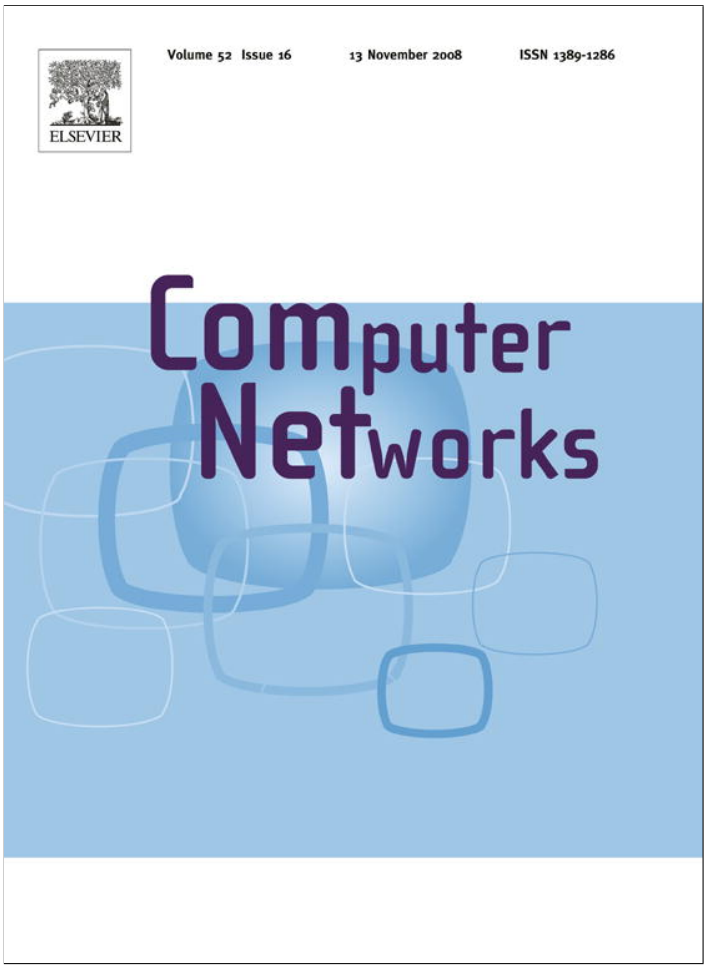

Computer Networks 52 (2008) 3047–3061

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

A survey of game-theoretic approaches in wireless sensor networks

Renita Machado *, Sirin Tekinay

Department of Electrical and Computer Engineering, New Jersey Institute of Technology, Newark, NJ 07029, USA

ARTICLE INFO

Article history:
Received 13 December 2007
Received in revised form 7 June 2008
Accepted 16 July 2008
Available online 7 August 2008

Responsible Editor E. Ekici

Keywords:
Wireless sensor networks
Game theory
Energy efficiency
Security
Pursuit-evasion games

ABSTRACT

Wireless sensor networks (WSNs) comprising of tiny, power-constrained nodes are gaining popularity due to their potential for use in a wide variety of environments like monitoring of environmental attributes, intrusion detection, and various military and civilian applications. While the sensing objectives of these environments are unique and application-dependent, a common performance criteria for wireless sensor networks is prolonging network lifetime while satisfying coverage and connectivity in the deployment region. Security is another important performance parameter in wireless sensor networks, where adverse and remote environments pose various kinds of threats to reliable network operation. In this paper, we look at the problems of security and energy efficiency and different formulations of these problems based on the approach of game theory. The potential applicability of WSNs to intruder detection environments also lends itself to game-theoretic formulation of these environments, where pursuit-evasion games provide a relevant framework to model detection, tracking and surveillance applications.

The suitability of using game theory to study security and energy efficiency problems and pursuit-evasion scenarios using WSNs stems from the nature of strategic interactions between nodes. Approaches from game theory can be used to optimize node-level as well as network-wide performance by exploiting the distributed decision-making capabilities of WSNs. The use of game theory has proliferated, with a wide range of applications in wireless sensor networking. In the wake of this proliferation, we survey the use of game-theoretic approaches to formulate problems related to security and energy efficiency in wireless sensor networks.

1. Introduction

The resource-constrained nature of WSNs in terms of their size, cost, weight and lifetime [1] is a primary area of concern for most potential applications using WSNs. At their best, the constraints of size, weight and cost of individual nodes have propelled their use in a wide variety of military and civilian applications. At their worst, constraint of the power-limited nature of nodes which also constrains their computational, communication and sensing capabilities calls for research into optimizing tradeoffs between reliability and prolonged network operation. Coupled with the inherent unreliability of the wireless channel, possible hostile environment in certain application-specific deployment regions and device unreliability of individual nodes, WSNs are subject to unique challenges for efficient power management to prolong network lifetime in addition to fulfilling sensing objectives of the application.

Energy efficiency and achieving reliability of data collection is a key issue in sensor networks. Energy efficiency has been investigated widely and the various approaches to achieve an energy efficient network include scheduling sensor nodes to alternate between energy-conserving modes of operation, efficient routing algorithms, clustering, incorporating intelligence and use of spatial localization at every sensor node to reduce transmission of redundant data. These approaches draw upon theories from mathematics, game theory, physics and even observation of biological phenomena [2–4]. Another important

* Corresponding author. Tel.: +1 973 392 9289.
E-mail address: renita.machado@gamil.com (R. Machado).

1389-1286/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.gaceta.2008.07.003

problem is security in sensor networks. Since sensor nodes are deployed in diverse geographical environments, they are more prone to failure from hostile environmental conditions in addition to being vulnerable to various kinds of attacks on the network. The unreliability of the wireless channel also poses security challenges in WSNs similar to those encountered in other ad hoc networks. A key application environment for WSNs is for surveillance, detection and tracking. Pursuit-evasion games (PEGs) comprising of a pursuer or group of pursuers searching for evaders have been widely used to model surveillance and detection scenarios. While typical WSNs are made of power-limited nodes that limit computation and communication abilities, PEGs requires the use of mobile, multi-sensor and actuator-equipped devices that are capable of implementing complex search algorithms and are able to communicate among themselves to detect and capture evaders. Another approach that makes use of the advantages offered by low-power nodes of typical WSNs is to use these networks to enhance the visibility and communication capabilities of pursuers, thereby increasing the efficiency of the search process. In this paper, we survey the use of concepts of game theory to solve the problems of energy efficiency, security and pursuit-evasion games in sensor networks. An overview of these approaches is shown in Fig. 1.

2. Game theory and its applications in sensor networks

Game theory is a theory of decision making under conditions of uncertainty and interdependence. We now provide a brief introduction of the basics of game theory with the help of examples modeled on scenarios prevalent in WSNs. A game has three components: a set of players, a set of possible actions for each player and a set of strategies. A player's strategy is a complete plan of actions to be taken when the game is actually played. Players can act selfishly to maximize their gains and hence a distributed strategy for players can provide an optimized solution to the game. In any game, utility represents the motivation of players. A utility function, describing player's preferences for a given player assigns a number for every possible outcome of the game with the property that a higher number implies that the outcome is more preferred. The higher the number of participating nodes, the higher will be the utility. A Nash equilibrium is a set of actions of the players such that, any other action chosen by a player does not result in more favorable utility for the players. Most of the game formulations surveyed in this paper are non-cooperative games, where nodes act selfishly, to minimize their individual utility in a distributed decision-making environment [5]. This is in contrast to cooperative games where nodes agree on pre-mediated strategies to maximize their payoffs.

In WSNs involving non-cooperative energy-efficiency games, nodes can act selfishly to conserve their power by refusing to participate as relays in multi-hop networks. In doing so, a node conserves its power; however the nodes involved in transmission and reception of the message have already used a fraction of their power and decreased their lifetime. The utility function for the nodes is the sav-

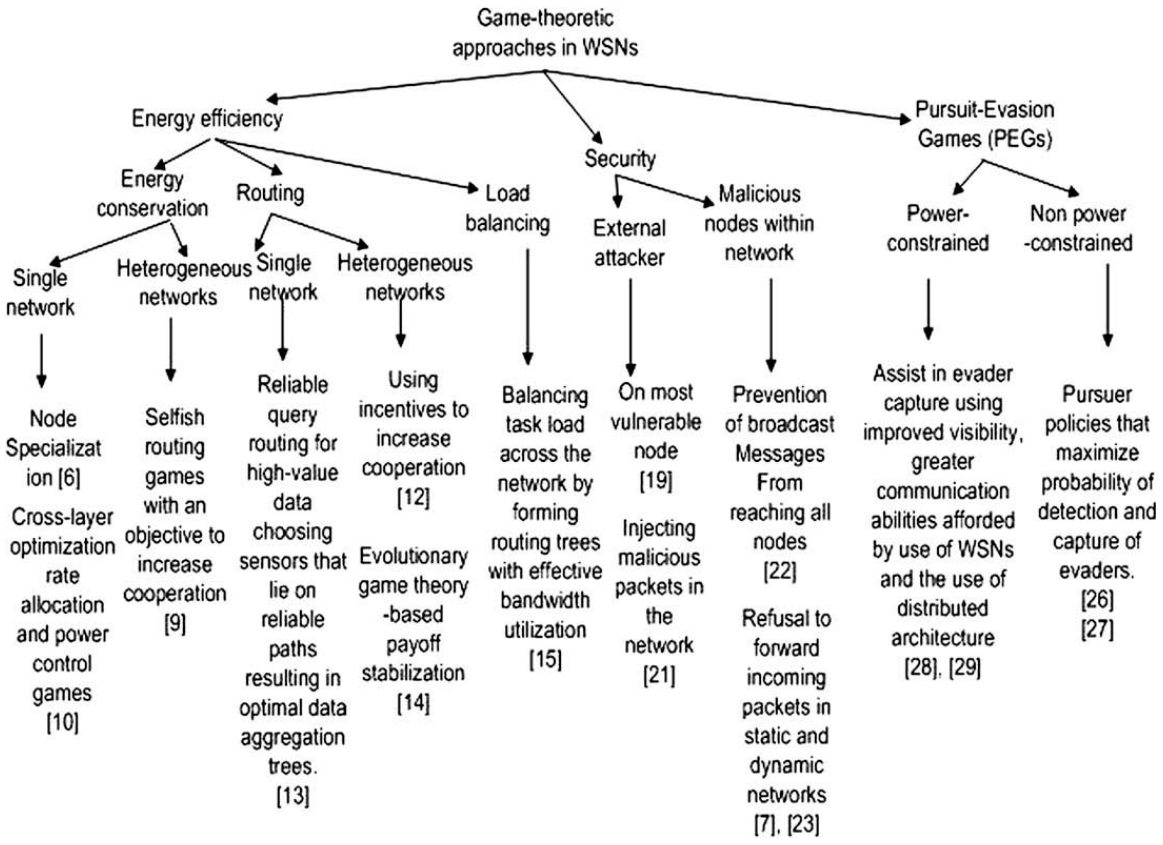

Fig. 1. Overview of game-theoretic approaches in WSNs.

ings in battery power achieved by not cooperating in packet forwarding of other nodes. Another utility function described in [6] is the mapping of number of sensor nodes participating in a sensory computation to a number. Such selfish nodes can be encouraged to participate in communication by offering incentives. Incentives for the case of wireless sensor networks could be tokens, in the form of reputation or monetary benefits.

The next category of games that we survey is in the area of security in WSNs. The strategies employed in energy-efficiency games differ from security-oriented games in many aspects. For example, malicious nodes within the network might launch an active attack on other nodes in the WSN, where the objective of the malicious nodes is to disrupt network operation without consideration for their own lifetime. Another category of attacks are passive attacks, where malicious nodes prevent broadcast messages and other service-availability related messages from reaching other nodes in the network [7]. In [8], the authors further classify these attacks into one of five categories: data-integrity and confidentiality related, service availability and bandwidth consumption, routing, identity and privacy related attacks. In this paper, we survey models of service availability and bandwidth consumption, routing, energy consumption and security with approaches drawn from game theory. Since game theory offers ways to formulate problems posed by selfish and/or malicious nodes, it can serve as a favorable tool for analyses of WSNs, wherein, optimizing energy consumption in various node activities and enabling secure network operation can be modeled as games with nodes as the players.

Game theory offers models to capture the interaction between players, in this case, nodes, by modeling the players as components of social networks, where players can act in ways that would maximize their own utility, which does not always lead to favorable outcomes for the game. While game theory still lets players choose the best available action, it provides a situation where other players' utilities are also maximized. This work surveys recent contribution to literature and presents some of the problems of wireless sensor networks addressed with the help of game-theoretic models.

3. Energy-efficiency oriented games in WSNs

3.1. Energy conservation

In this section, we present the problem of energy conservation in wireless sensor networks. Since sensors are equipped with non-replenishable energy sources, they should be programmed to achieve energy efficiency in their sensing operations, routing and computational capabilities. In [6], the authors propose node specialization in which sensors adapt to different roles such as idle, sensing, routing and routing/sensing to maximize the utility of nodes and the networks, where the utility is related to the number of nodes participating in a computation. A larger number of participating nodes indicates higher utility, with the constraint of limited battery power for every node.

In [6], the authors present experimental work for wireless sensor networks that are composed of sensor nodes that each have a finite, non-replenishable source of energy, a fixed transmission range R, a unique identifier and that communication among nodes is commutative. All transmissions are assumed to be perfectly scheduled to avoid interference and the transmission from a node reaches the nodes in its neighborhood. The network is presented as an undirected graph $G = (V,E)$, where V is the set of all nodes including the base stations. E is the set of edges in the network defined as follows, where $d(u,v)$ is the distance between nodes u and v, $E = \{(u,v) \| u,v \in V, d(u,v) \in R\}$. The authors propose the node specialization, in which nodes adapt to one of the following roles, idle, routing, sensing and routing/sensing depending on the virtual topology and power levels of the node. Further a node may perform the following operations receiving, transmitting, sensing and aggregation of collected data, each of which is associated with costs c_r, c_s,c_t, c_a, respectively. The utility function maps the number of nodes participating in the sensory computation to a real value which measures the utility derived from output from a subset of sensors of that size. Each sensor domain is associated with a monotonically non-decreasing utility function that maps the number of nodes participating in a sensory computation a real value which measures the utility derived from output from a subset of sensors of that size. In the case of an inelastic utility function, there are three regimes: when very small numbers of nodes participate, the user derives little utility. At a certain threshold, the utility increases dramatically and then beyond a final inflection point, there are diminishing marginal returns and utility increases very slowly. The objective function for this model seeks to ensure that nodes cannot consume more power than they have available, and the data collected from all nodes that get credit for participating in the sensing subset at time t actually gets routed to the base station. The authors propose an objective function of maximizing the total aggregated utility of the network over time, i.e. to maximize the sum over the lifetime of the network, of the utility of computation at intermediate time steps. This long-term strategy can be realized only through a combination of careful power management combined with distributed coordination on the part of the nodes in the sensor network in choosing their roles over time. The authors show that this model motivates nodes to discount current gains in lieu of future rewards, thus optimizing consumption of energy over a long time. As opposed to a best-effort model in which the nodes use their resources without consideration for their future use, the authors have used this model in which economic restraints motivate nodes to adapt to node specialization. The resulting objective function results in better utilization of node resources as compared to a best-effort service model.

Sensors can be deployed in environments where multiple sensing requirements exist. An example of this would be use of varied types of sensors to detect plant growth, wildlife activity and forest fires. Co-location of these sensors belonging to different authorities poses a situation akin to social behavior, wherein the sensors of a particular authority could actively participate in the transmission of packets of other sensors or selfishly refrain from doing so.

The situation when multiple sensor networks are co-located and controlled by different authorities has been studied in [9]. In this paper, the authors analyze the effect of cooperation to achieve increase in the utility of individual network payoff and thereby optimize energy consumption.

Co-existence of multiple sensor networks makes it possible for sensor nodes of a network to save transmission power spent in forwarding packets of nodes belonging to a different authority. The authors assume that all sensors that lie in the transmission range of each other can communicate with each other, even though they belong to different authorities. They further assume that sensed data occupies one message packet. Sensor nodes incur a transmission cost that also includes the processing cost. The reception and processing involve a fixed power R. The routing is assumed to be unselfish, and every node has two routes, one within its own network (non-cooperative) and the other in the common network of all authorities. (cooperative routing). They label a set of networking elements belonging to a single authority i as the domain D_i. If a sensor node runs out of battery power, its domain is called inactive and the routes are recalculated with its route being excluded. They model this situation as a game $G = \{P, S, U\}$ where P is the set of players, i.e. the nodes involved in transmission, S is the set of strategies and U is the set of utility functions. A player i, of domain D_i makes a decision in a given time slot as to whether its sensors/sinks should forward the packets of sensors belonging to a different domain and whether to request other sensors/sinks to forward its packets or to forward the packets only within D_i. Each such decision is called a move and a strategy s_i is a function that defines the move of the player in a slot $t + 1$ given that it was successful in slot t. The payoff for a node is the difference between the benefit received from successful information-sending to the sink and the value of the total (transmission and reception) cost for all sensors belonging to a particular domain for both own and the opponents' packets. In this game, the authors define the utility as the cumulative payoff for the nodes. In order to maximize the utility, the players have to report measurement successfully as many times as possible while minimizing energy consumption. The authors simulate two scenarios: separate sinks where each network has its own sink (Fig. 2) and common sinks (Fig. 3), in which a sink is shared by all networks. For each player, they determined the Nash equilibria that results in the highest utility.

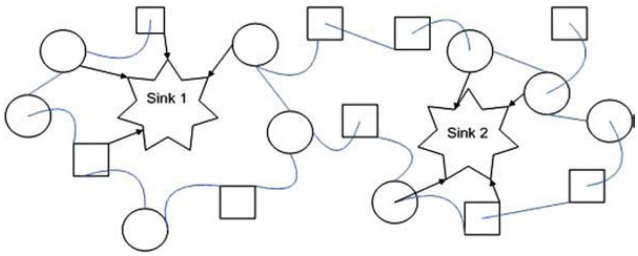

Fig. 2. Two co-located sensor networks with separate sinks. The circles represent the domain D1 of one authority, while the squares represent domain D2 of a different D2. The curved lines between nodes indicate cooperative routing in the common domain of both authorities, while the straight line connectors denote non-cooperative routing paths. The network is shown is that of separate sinks in the deployment region.

They observed the players ended up playing defective equilibria, i.e. do not ask other players to forward and drop all other packets if asked for help or cooperative equilibria, i.e. ask others to forward and forward all packets from others if asked from others. They define a ratio δ, i.e. the ratio of utility achieved by defection to that achieved by cooperation. Simulation results have shown that authorities can have significant benefit by providing service of their sinks for other sensors' networks. If sinks are common resources, then cooperative forwarding is beneficial in sparse networks or in hostile conditions (Fig. 4). The path loss exponent, used to model the hostile conditions of the environment adversely affects the ratio δ. As seen from Fig. 5, with increasing signal attenuation (path loss), δ decreases indicating that cooperation is the preferred strategy to defection.

In [10], the authors use game-theoretic approaches to perform distributed cross layer optimization for power control at the physical layer and rate allocation at the application layer. The power control game at the physical layer addresses transmission interference in nearby sen-

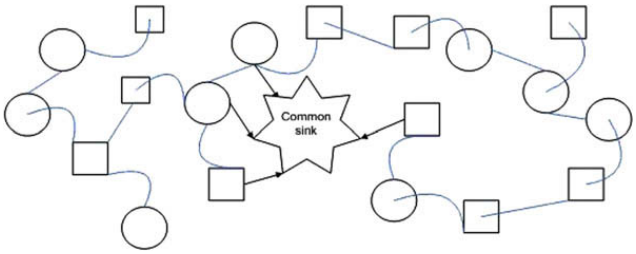

Fig. 3. Common sink scenario for sensor nodes belonging to both authorities.

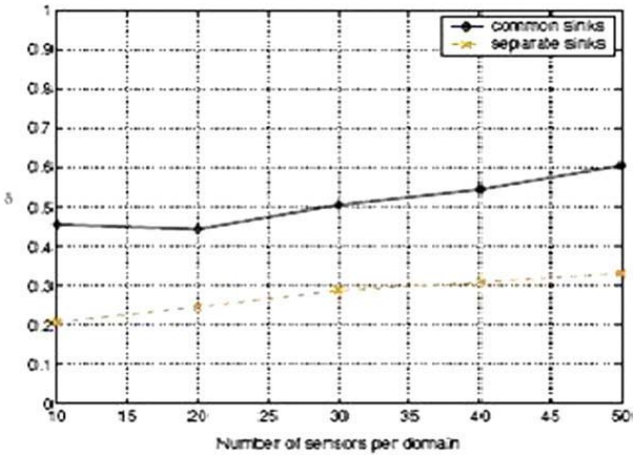

Fig. 4. Plot of network size on the ratio δ. For separate sinks, the incidence of cooperative equilibria is higher than other types of equilibria, as seen by the lower curve of the graph. The higher incidence of cooperative equilibria is attributed to the formation of shorter routes, since sinks of both domains are present. In the case of a common sink, the incidence of defective equilibria is approximately equal to that of cooperative equilibria. With increase in network size, δ decreases, resulting from increased contribution of the reception power to the total power contribution.

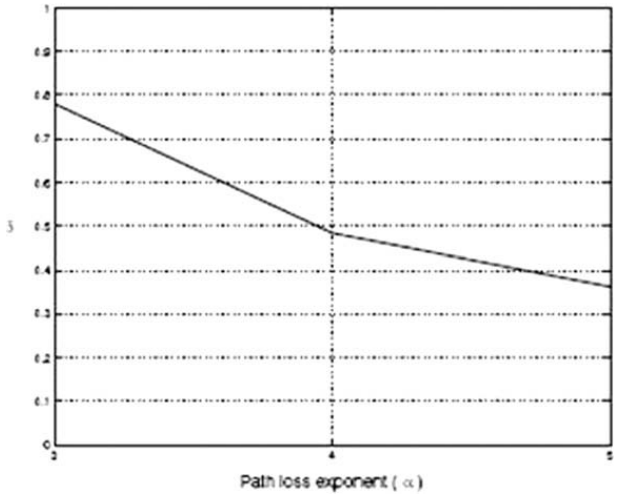

Fig. 5. Plot of the ratio of the utilities achieved by defection to that of cooperation, δ, to the path loss exponent α which indicates the channel variations in the environment. As the path loss (environment hostility) increases, δ decreases, indicating that cooperation strategy is preferred to defection.

sors. They introduce a tax mechanism in this game as an incentive to the nodes (players) to avoid interference. The higher power used by a node results in increased interference to adjacent nodes and hence a higher tax is levied on this node. The tax rate is given by the rate at which other nodes' data rates are decreased with an increase in transmission power. The rate allocation game at the application layer is formulated as a source coding game. The problem here is the estimation of the environment in the deployment region in the presence of observation noise at the sensors. To this end, the objective of the game is to maximize link capacities corresponding to different power levels, while minimizing the distortion at various source rates that are supported by the nodes. The application layer demand of source rates and the physical layer supply of link capacities are linked by shadow variables, which optimize the relationship between source rates and the interference. A quantizer at the node quantizes the noisy observation which is transmitted to the central processing base station along with quantized information from other sensors. Along with the need to minimize the mean-squared error in the estimation process, the authors define another parameter w, called the quantization effort. A higher quantization effort w denotes higher source rates. They introduce a pricing mechanism m into the source coding game, where the tradeoff between source rate and distortion is denoted by the source rate being a linear function of the quantization effort and the pricing mechanism m. They implement the above game with a distributed algorithm that iteratively accounts for the interaction between the source coding and power allocation games at the two layers.

3.2. Routing

An important issue in wireless sensor networks is routing of sensed data. Approaches that deal with choice of efficient routing algorithm in WSNs involve reducing the number of hops, cluster formation, directed diffusion [2] and randomized algorithms [11]. However, there could be a rational interaction between the nodes, where the relay nodes opt to conserve power by refusing to participate in forwarding packets from other nodes, or from nodes belonging to other networks. In this subsection, we continue the discussion of game theory in WSNs by surveying recent work on routing among nodes belonging to single/different authorities using techniques such as provision of incentives to encourage cooperative routing.

Similar to the work in energy-efficiency featuring sensors belonging to different domains, the authors in [12] use game theory to analyze the outcome of a game, in which the deployed sensors belong to different sponsors (authorities) and can receive incentives for cooperative forwarding. The authors use the terms 'favors' for services provided by sensor nodes, typical examples of which are routing, data storage and data aggregation. When sensors request a service from another sensor belonging to a different sponsor, the other sensor may choose to grant the favor depending on its resources or decline the request for a favor. Alternately, it may selfishly decline to grant the favor to conserve its resources. In such a game, where none of the sponsors are obligated to provide favors to the nodes of another sponsor, the Nash equilibria results in non-cooperation of nodes belonging to different sponsors. To avoid this situation, the authors propose the use of tokens as incentives to encourage cooperation between sensors belonging to different sponsors. Two sponsoring organizations $i \in \{A,B\}$ deploy sensors $\{s_{i1},s_{i2},\ldots,s_{ik}\}$, on a rectangular grid consisting of $2K$ nodes. The use of tokens is facilitated by each sponsor signing a contract promising to pay the nodes of the other sponsor at the end of a time period T. When a sensor node a belonging to one sponsor requests a favor from a node b of another sponsor, it sends a request for the favor along with the token. If the favor is granted, the node b receives the token, otherwise node a retains the token. The utility of a sensor node is a function of the number of favors received and provided by a node s_{ik} and the number of communication signals sent out by s_{ik}, which is the total number of requests it made. The utility for a sponsor is the sum of the utilities of all its sensors plus the monetary transfer received by i at the end of T. Using this setting where the sponsors can program their nodes for cooperation and by establishing contracts at the beginning of a time period for the number of tokens that it can provide, the authors state and prove the existence of various Nash equilibria for varying conditions of acceptance/rejection of contract. They show that token equilibria, where sponsors jointly agree on the number of tokens that they can trade for 'favors', exists when the sponsors are able to write contracts. However, under the condition that the sponsor cannot write the contract, the Nash equilibrium is that a sensor cannot request a 'favor', since the sponsor does not have tokens to trade in exchange for the 'favors'. These conditions for Nash equilibria under existence of contracts are summarized in Fig. 6.

A reliable query routing scheme has been proposed by the authors in [13], where they suggest that the number of sensors working simultaneously to collaborate on aggregation of mined data should be chosen such that network-

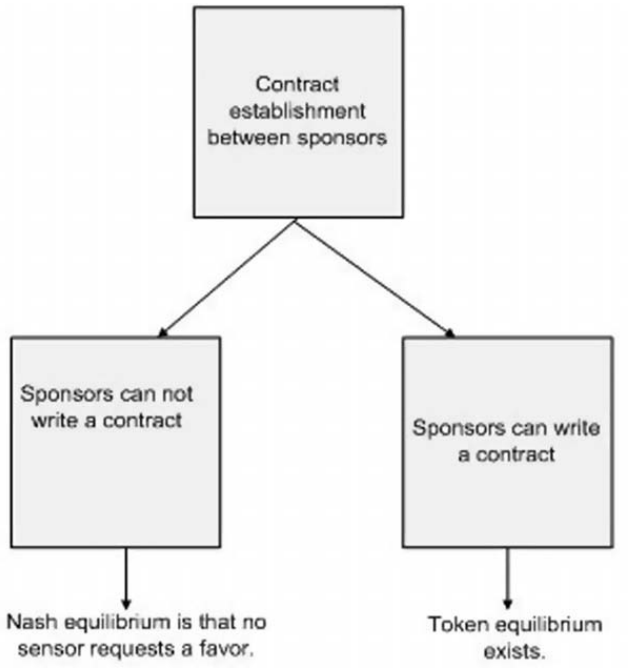

Fig. 6. Existence of Token and Nash equilibria under conditions of contract establishment. If sponsors are unable to write a contract, the Nash equilibria for the routing game involving tokens as incentives is that no sensor requests a favor. However, under the condition that sponsors can write a contract, the token equilibrium exists such that, each sensor requests a favor only if it can provide a token for the favor requested, and each sensor grants a favor if it is possible, whenever it receives a request. This strategy induces cooperation with the introduction of incentive-driven routing games.

wide objectives, namely, increasing information utilization of the network and efficiency of communication resources and energy consumption are achieved. They label this paradigm as sensor-centric and use a game-theoretic approach. In this approach, the sensors are modeled as rational/intelligent agents cooperating to find optimal network architectures that maximize their payoffs in a sensor game, where sensor payoffs are defined as benefits of this sensor's action minus the individual costs.

The problem is modeled to be that of reliable energy-constrained routing, in which a set of sensors are the players of the routing game. When a sink node sends a query to the nodes in this set, it is checked for a match with the attributes of the data sensed by the node. They abstract this idea of information retrieval by a value v_i that represents the closeness of the match. If $v_i = 0$, it implies that the query does not match any attributes. This ensures that high-value data are routed over reliable paths even at higher costs. Information is routed to the sink node through an optimally chosen set of sensors. They call this game as the reliable query routing (RQR) game. Each sensor node is modeled as relaying a received data packet to only one neighbor and hence forms only one link between any pair of source and destination nodes. A sensor node's strategy is modeled to be pure in the form of a binary vector, $\{l_{i1}, l_{i2}, \ldots, l_{in}\}$, where $l_{i\ i} = 1/0$ represents a sensor node s_i's choice to send/not send a packet to sensor node s_j. Since every sensor that receives data has an incentive in reaching the sink node, its payoff is a function of the path reliability and the expected value of information at that node. This results in a data aggregation tree that is optimal, since if a sensor node decides to choose a different neighbor on another tree, it results in suboptimal behavior, i.e. reduced payoffs to/from other nodes. Hence, this also forms the Nash equilibrium for the reliable query routing game. Since the network is unreliable and the sensors maximize their own payoff subject to overall network objectives, they use a path metric called the 'path weakness' to evaluate various suboptimal paths. The path weakness determines how much the node would have gained by deviating from its current path to an optimal one. A negative deviation suggests that a node s_i is benefiting more from its given strategy/profile path (perhaps at the expense of some other sensor). A positive deviation indicates that the sensor node could have performed better. They also present a team version of this game called team RQR (TRQR), in which all nodes on the path share the payoff of the worst node on that path. Rather than selecting a neighbor to maximize their individual payoffs in the original game, nodes in the TRQR model compromise by maximizing their least possible payoff. As in RQR, each node's strategy is to select at most one neighbor. The TRQR routing algorithm was compared to the following routing algorithms:

Cheapest neighbor path (CNP): The cheapest neighbor path between two nodes i and j is defined as the path obtained by each node choosing the next-hop node via the cheapest link, where the cost is the expense incurred by a node for link formation. The CNP usually has longer path-lengths, and is less reliable than the most reliable path (MRP) algorithm.

Overall least cost (cheapest) path (MCP): The overall least cost path is the path with the least link costs, and can be evaluated from Djikstra's shortest path algorithm.

Most reliable path (MRP): The most reliable path can be similarly obtained from Djikstra's shortest path algorithm, where node success probabilities (i.e. the probability of staying 'awake') are taken to be the same for all nodes.

The simulation results of TRQR compared with CNP, MCP, MRP and genetic algorithm based heuristic showed that the TRQR performed quite well in cases of varying success probabilities of a node and maximum edge (path) costs. A key observation was that in the event of node success probabilities $p \in (0,1]$ and the cost of a path between nodes i and j $c_{ij} = c$ for all i and j, the most reliable path is the equilibrium path of the RQR game. For uniform p, the equilibrium path also becomes the overall cheapest path (MCP). In the scenario of rational nodes wanting to maximize their own payoffs with respect to the network objectives, simulation results shown in Fig. 7 also found that TRQR has low path weakness as it inherits the characteristics of MRP in unreliable networks and that of the cost-optimizing algorithm in highly reliable networks.

In contrast to the above approaches which use classical game theory to study energy efficiency in WSNs, in [14], the authors consider the problem of packet forwarding in multi-class WSNs using evolutionary game theory. In classical game theory, players choose a particular strategy in

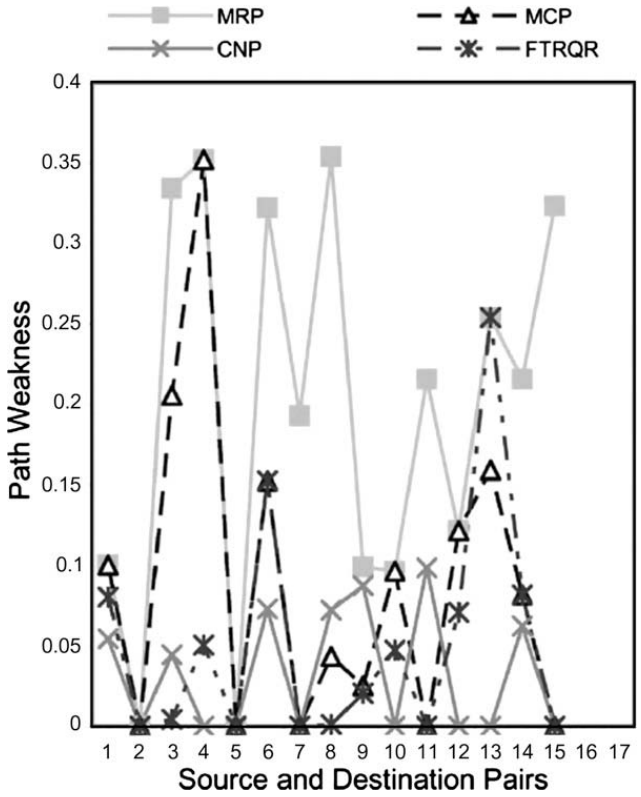

Fig. 7. Plot of the path weakness as a function of the number of source–destination pairs for node success probability $p = 0.998$, and cost $c = 0.058$. The TRQR algorithm performs better than the MRP, MCP, CNP and the genetic algorithm (GA) by having the least path weakness for any given number of source destination pairs. The path weakness determines the quality of the routing path in terms of the weakness of individual nodes on the routing path. This metric determines the payoff for nodes, i.e. the amount a node gains by deviating from a current path and participating in another path.

response to other players' strategies and this strategy does not change over time. However, in evolutionary game theory, the frequency with which a player chooses a given strategy varies over time in response to the strategies adopted by other players. Thus, while in classical game theory, players are assumed to possess decision-taking abilities for obtaining payoff-maximizing strategies, evolutionary game theory derives from the study of population dynamics, where players (as in individuals of a species) adopt strategies that maximize payoff by increasing the frequency of strategies that increase the fitness of future generations of the species. The use of evolutionary game theory allows for players being able to choose from pre-programmed set of actions and strategies and the use of only local information. This does not require processing at nodes to determine the strategy for a set of player actions, thus conserving power and avoiding the use of memory space for computing and storing action profiles and strategies. They assume a multi-class (heterogeneous) WSN, where any two non-neighboring class communicate via multi-hop routing. Nodes can be selfish and act strategically to optimize throughput over its active connections. They consider inter-class relaying, when a class can cooperate and forward packets or defect. They assume noiseless bidirectional links between nodes, and hence loss of a packet is solely due to defection by a selfish class of nodes. They model the game as that of non-cooperative repeated N-player game between classes of nodes, where nodes participate repeatedly in games with other nodes. In repeated games, a node's action in a given round is influenced by the actions of other nodes and corresponding playoffs in previous rounds. Thus a repeated game offers ways to punish nodes that do not cooperate by decreasing their payoffs at the end of the game. This can be done by tarnished reputation or decrease in incentives resulting in reduced payoffs at the end of the game. Cooperation is similarly rewarded, by examining the payoffs after repeated rounds of the game. Nodes with higher history of collaborative efforts have higher reputation, accumulate incentives faster and are included in reliable routes. Authorities of each class decide whether or not to forward packets. The game ends when only two classes remain active, where a class is considered inactive on depletion of its first node. In order to develop the payoff matrix for cooperation/defection, they introduce incentive for cooperation. In transmitting or forwarding a packet, classes spend battery energy β and gain an incentive γ. If classes refuse to retransmit, they gain ϕ and there is no cost to them. The nodes in all classes are assumed to be pre-programmed with two strategies: cooperate and defect. The benefit for non-cooperating players is a value α multiplied by the number of cooperating nodes. They consider two scenarios: packet forwarding between mobile classes and packet forwarding between spatially dispersed stationary classes. They introduce a strategy, the Patient Grim strategy described as follows: 'Cooperate and continue to cooperate until the other player defects n ($n \geqslant 0$) times, and then defect forever. The payoff of this strategy is given as the weighted sum of payoffs overall periods weighted by δ, where $0 < \delta < 1$. They show that for packet forwarding between stationary classes, Nash equilibrium is achieved if each player plays the Patient Grim strategy and the discount factor δ is approximately close to unity. For stationary classes, cooperation stabilizes the payoff by forming clusters and reducing exploitation by defection. This is in contrast to mobile classes, where defection has been shown to be the only strategy for stable payoff based on the theory of evolutionary dynamics. For packet forwarding in mobile classes, they assume that the benefit of cooperation increases with the number of cooperating players. It should be noted, however, that the strategy cooperation for payoff stabilization in stationary classes is dependent on α. A higher value of α results in cooperation being unstable even for stationary classes. These results are summarized in Fig. 8.

3.3. Load balancing in wireless sensor networks from point of view of bandwidth allocation

The distributed nature of sensor networks can lead to high workload for sensor nodes in the network. With the resource constraint of battery power and thereby network lifetime, distributing the workload of query flooding, processing query replies and control overhead across the network helps in balancing energy consumption and increasing network lifetime [15–17]. The authors in [15] model the load balancing problem by using techniques

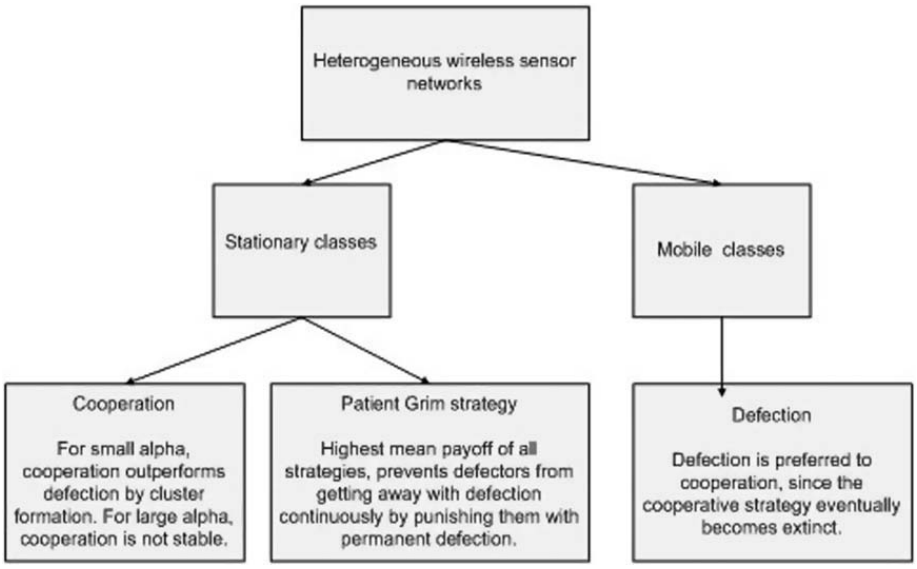

Fig. 8. Payoff stabilization criteria in mobile and stationary classes of WSNs using evolutionary game theory.

from mechanism design and game theory to design a decentralized sensor network. Unlike the above two approaches in which we strive to increase the utility of sensor nodes and the network in general, where the utility function is known a priori, the authors design the utility functions of individual nodes such that the network objectives are met when the sensors maximize their individual utility functions. The problem here is to organize data gathering from large multi-hop sensor networks to distribute the query processing and reply load. This is done by constructing a tree rooted at the base station/ sink. Every node has a level in the network which is the number of hops from the sink node. A node must find and attach to a parent with fewer children than the current one. The decisions taken by a node at every level are independent of the decisions taken by nodes at all other levels. In the load balancing problem for sensor networks, the authors describe a distributed algorithm to design the utility functions of individual nodes, such that when these utility functions are optimized by the sensor nodes, the overall objective of the network is met. They do so from a bandwidth allocation point of view and compare their results with that of a centralized algorithm [18].

The problem they look into is that of the load balanced data gathering tree, which is essentially finding an optimally semi-matching in a bipartite graph. They describe a distributed iterative algorithm for sensor networks for load balanced data gathering. In multi-hop sensor networks, when a base station sends a query to the network, it may do so by flooding the network. The individual nodes then organize themselves into levels and select a neighboring node at the previous level to be their parent. The problem here for a sensor node is to find a parent that has fewer children and attach to it. Since the decision to attaching to a particular parent node is independently taken by sensors, the overall data gathering tree will be load balanced. The game is played on the edges of a bipartite graph, where the graph $G = (M \cup N, E)$, where M is set of all parents, N is the set of all children. An edge (i, j) belongs to E, if j belongs to M and i belongs to N and vice versa. The algorithm is designed as an iterative game being played by selfish sensors. The players in the game are the child nodes, with the utility being the bandwidth guarantee C provided by a parent to the child, i.e. the parent is committed to provide a bandwidth of at least C to child i for all iterations after k as long as i is child of p. At every iteration, a parent gives equal bandwidth guarantees to its children. They define a parent to be saturated if the total bandwidth guaranteed by parent p at iteration k is equal to 1. The algorithm followed by the child node is as follows. At an iteration k, a child tries to connect to an unsaturated parent that provides the best possible bandwidth guarantees. If there are multiple such parents, the child expresses a willingness to connect to all of them. After the child has been accepted by one parent, it notifies the other parents of its inability to join them (Fig. 9). The algorithm for the parent node is as

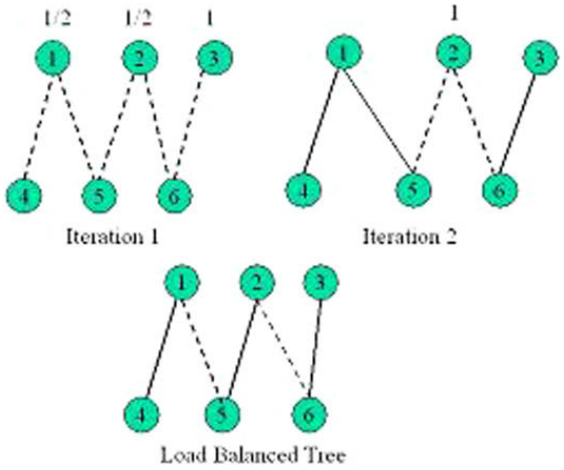

Fig. 9. The set of parents $M = \{1,2,3\}$ and the set of children $N = \{4,5,6\}$ with the bandwidth guarantees indicated on top of each parent. At each iteration, the child chooses a parent that offers the best bandwidth guarantee. The solid lines indicate matched parent–children sets (M,N) given by $\{1,4\}$, $\{2,5\}$ and $\{3,6\}$.

follows. The bandwidth guarantee provided by a parent is initially of the form $1/\deg(p)$, where the $\deg(p)$ is the degree of a node in the bipartite graph. Until a parent is saturated, it increases the bandwidth guarantee by $1/\deg(p) - 1$, $1/\deg(p) - 2$ until it becomes 1. While it is not saturated, it finds the upper bound on the number of children it can take and provides bandwidth guarantees depending on its level of saturation. However, if a child leaves or a child joins, the bandwidth guarantee is not increased. The algorithm terminates at the following iteration at which the parents are saturated. They prove that the total number of iterations required to terminate the algorithm is $O(N\gamma)$, where γ is the degree of the parent node n the graph. At termination, Nash equilibrium results, this is the condition when all parents are saturated. The simulation results performed for the algorithms showed that the number of parents of degree x produced by their distributed algorithm and that produced by the centralized algorithm employing optimal semi-matching algorithms described in [18] are same.

4. Security

The large number of nodes in WSNs coupled with the unreliability if nodes and wireless channels along with the fundamental constraints in memory, battery power and computational capacity introduce significant security issues in WSNs. While the set of security issues in WSNs are diverse, we focus on two main security challenges: attacks by malicious nodes in the WSN and attacks by an outside intruder on the WSN. In this section, we look at three different scenarios, detection of intrusion to the most vulnerable node in a network, intrusion by injecting a malicious packet on a link in the network and malicious nodes in the network that prevent the broadcast message from the base station from reaching the nodes in the network.

In [19], the authors deal with the issue of detecting attacks by an intruder on the most vulnerable node in a sensor network. The authors propose a non-cooperative, zero-sum game-theoretic model to analyze the situation where an intruder attacks the sensor network. They propose an Intrusion Detection System (IDS), whose task is to detect the most vulnerable node in the network and protect it from the intruder's attack. These nodes are divided into clusters and one node in the cluster is chosen as the clusterhead. The choice of clusterhead is done with the help of a clustering mechanism called weight clustering approach (WCA) [20], where clusters are adaptively formed depending on the mobility of nodes, cluster size, transmission power and battery energy of nodes to achieve connectivity between nodes and load balancing across the network with low latency. The game is formulated as follows. With respect to one cluster k, the attacker has three strategies, attack cluster k ($AS1$), do not attack at all ($AS2$), and attack a different cluster ($AS3$). At every time slot, IDS is protecting a cluster. The strategy for IDS would be to defend a cluster k ($SS1$), and to defend another cluster ($SS2$). The payoffs of these two players are expressed in the form of 2×3 matrices A_{ij} and B_{ij} which denote the payoffs of IDS and the attacker respectively. They define $U(t)$ to be the utility of the sensor network's ongoing sessions, AL_k to be the average loss of losing cluster k, C_k to be the average cost of defending cluster k, and N_k the number of nodes in cluster k. To calculate the IDS payoff matrix, for e.g. $a_{11} = (AS1, SS1)$ which is when both attacker chooses to attack the same cluster that IDS is defending. So, for IDS, the payoff will be the original value of utility minus the cost of defending cluster k. a_{21} represents $(AS1, SS2)$ when the attacker attacks a cluster different from the one that IDS is defending. In this case, the payoff will be utility minus the average of defending a cluster as well as deducting the average cost of loss the other cluster. Similar arguments are applied to find the values of other elements in the IDS payoff matrix. To calculate the attacker payoff matrix B_{ij}, the authors define three parameters, the cost of waiting and deciding to attack in the future (CW), the cost of intrusion for the attacker (CI), average profit for each attack (PI). b_{12} and b_{22} are the non-attack mode CW, b_{11} and b_{21} are representing attacks to cluster k, and b_{13} and b_{23} represent attacks to cluster other than k.

The authors prove that the equilibrium solution for this game is the state $(AS1, SS1)$. They compare this game-theoretic model of defending a sensor network with two other approaches, a Markov Decision Approach (MDP) to predict the most vulnerable sensor node, and another scheme in which they use an intuitive metric, traffic metric and protect the node with highest value of this metric. Simulation results show that IDS performs almost twice better than MDP.

The authors in [21] model a game between the intruder and service provider of the network. The objective of the intruder is to inject a malicious packet in the network at some node a with node t as the target. The intrusion is successful when the packet reaches the target and unsuccessful when it does not. To protect the nodes from the attack, the service provider is allowed to sample the packets flowing through the links on the network. Since sampling the packets introduces additional computational costs, there is a bound on the sampling rate. This bound B, represents the maximum number of packets that can be sampled per second and the sampling effort is distributed arbitrarily overall the links in the networks. If a link e has a traffic f_e and it is sampled at a rate s_e, then the probability of detecting a malicious packet is $p_e = f_e/s_e$. The objective of the intruder is to minimize the probability that the malicious packet is detected by the service provider, while the objective of the service provider is to maximize the number of times a malicious packet is detected. This is the classical two-person, zero-sum game, where the payoffs of the intruder and service provider add up to zero, in other words, the intruder's win amounts to the service provider's loss and vice versa. The optimal solution for this game is the minmax optimal solution, which is the Nash equilibrium for a zero-sum game. The minimax solution for this game is that along any path the intruder will choose, the packets will be sampled once along the link. If the sampling bound B is greater than the maximum flow from a to t, the malicious packet will always be detected. If B is less than the maximum flow, there is a non-null probability that the packet will be detected.

In [22], the authors consider the environment where malicious sensor nodes prevent the broadcast message from the base station from reaching other nodes in a network. A simple method to avoid this is for every sensor node to acknowledge the receipt of the broadcast message. However, this results in a large number of acknowledgements reaching the base station causing an implosion at the base station. Hence the authors consider a framework where a subset of the total number of nodes sends an acknowledgement to the base station. The attacker should have no means of knowing the identity of this subset of nodes to secure the broadcast message. This method, called secure implicit sampling (SIS) assumes the existence of a base station that is computationally and energy-wise powerful than the sensor nodes. The strategy of an optimal attacker is to deprive nodes of the broadcast message from the base station. In the absence of SIS, the payoff of the attacker would be the number of legitimate nodes deprived of the broadcast message. However, in the presence of SIS, once the attacker is detected his payoff goes to zero. In a particular round, the attacker's payoff is the total number of nodes x that he deprived of the broadcast message. However, nodes may be deprived of the broadcast message due to probabilistic packet loss and channel conditions. Also, the base station may fail to receive an acknowledgement for the same reasons. The authors introduce a factor called the discount factor γ. When γ less than 1, the attacker is always attaches less importance to a future reward. When γ is equal to zero, the attacker is concerned only about maximizing his immediate reward and when it is equal to one, he attaches equal importance to his immediate and future reward. The total reward of an attacker is a function of the total number of nodes x that he succeeds in denying the broadcast message. As the probability of sampling a node increases, the probability of detecting the attacker increases. However, increased sampling also increases the transmissions in the network which may cause a loss of the broadcast message. They analyze this tradeoff with the help of a zero-sum game-theoretic model, with the equilibrium given by a minmax condition on the reward. The reward function J now is a function of both p and x. They define p_i as the probability that the base station receive an acknowledgement from the node that is sampled. $p_{r_0} = \frac{1}{n}\sum_{i=1}^{n} p_i$

The authors use flooding as the broadcast algorithm and study the performance of the network where sufficient number of nodes compromised. As the number of attacked nodes increases, the attacker's impact on the network becomes detectable by SIS. The optimal value of p for which the attacker's payoff was minimized was found to be between 0.1 and 0.15. Simulation results performed show that as the number of nodes sampled increases, there is an increase in transmission resulting in a greater natural loss probability of acknowledgements.

In [7], the authors study another scenario of detecting passive DoS attacks by malicious nodes in the network. However, unlike the game formulation in [22] where an attacker turns nodes malicious and prevents them from letting broadcast messages reach other nodes in the network, in [7] the authors study a game formulation at the routing layer between malicious nodes that do not forward incoming packets and an intrusion detector residing at the base station. Malicious nodes in this work are those nodes that selfishly do not forward incoming packets. The intrusion detector monitors WSN of N nodes and detects attacks by malicious nodes by keeping track of collaboration of nodes which accumulates into reputation ratings for a node over time. They model this scenario as a repeated game, where the IDS uses the history of nodes' collaboration to determine paths comprising of malicious nodes. The game is played as a non-cooperative N-player game between N nodes in the WSN and an IDS residing at the BS. Each node can take one of two actions- accept a packet and forward it to improve its reputation (normal) or selfishly decide not to forward the packet (malicious). The IDS can detect an intrusion by malicious nodes by taking one of two actions: 'catching' it while being malicious or 'miss' it. These action profiles for the IDS and the nodes give rise to the following four cases, each with different payoff functions: A false positive occurs when a node is 'normal' but the IDS 'catches' it as malicious. A false negative occurs when a malicious node is not detected. The most rewarding situation for the IDS is when the IDS catches a malicious node. The case of least concern for network security is when a normal node is 'missed' by the IDS. The utility for the IDS is given by a weighted sum of the product of the payoff function in a given case and the number of occurrences of that case over the case of the repeated game. This weighted utility function has a corrective benefit, since by taking into account the number of occurrences of a case, it accounts for past behavior of the IDS and accordingly wither rewards it for detecting malicious nodes accurately or punishes it for false positives and false negatives. In order to ensure finiteness of the repeated game payoffs, the authors introduce 'discounted' payoffs, where future payoffs are multiplied by a discount factor delta relative to earlier payoffs. The authors consider the following retaliation strategy for the nodes and the IDs. Initially, a node cooperated to forward messages, so IDS does not catch any node. In later periods, if the node has always cooperated, the IDS does not 'catch' it. However, if the IDS catches a nodes being malicious, the node acts malicious for the rest of the game. The retaliation strategy for the node in the initial stage of the game is similar. In later periods, a node does not act maliciously if the IDS has missed it. However, if the IDS catches a node, it acts maliciously for the rest of the game. The authors show that the best response for the IDS is to cooperate and not deviate from the above strategy. The Nash equilibrium of the game results when the IDS and the nodes in the WSN play the game cooperatively by following their respective strategies. The proposed protocol for the repeated game shows a correlation between network size and successful intrusion detection, where detection success increases with higher percentage of malicious nodes. An increase in the number of malicious nodes has also been shown to reduce the throughput of the WSN.

In [23], the authors study the case of malicious packets refusing to forward incoming packets. Here the authors consider a dynamic WSN of mobile nodes and address security with three key parameters, cooperation, reputation and quality of security. They consider a wireless sen-

sor network, where any node can be malicious by refusing to cooperate with other nodes by not forwarding incoming packets. The WSN is made up of clusters of mobile nodes, and communication between clusters is facilitated by clusterheads. They study the performance of the WSN in terms of cluster formation and messages per node with the help of a utility-based approach which considers network security in the payoff function. The payoff between two nodes as a function of the three parameters of cooperation, reputation and quality of security is defined as follows: The cooperation between nodes is described as a function of the minimum signal strength for cooperation, distance between the nodes and the cost of packet forwarding. The reputation is defined as the ratio of packets forwarded to the total number of packets received and generated packets between two nodes. The quality of security for each cluster is defined as the percentage of exposed traffic if security is compromised. This is calculated as the difference between the total number of packets generated between two nodes and the total number of packets dropped between them. The payoff utility function for this game and the node strategy is given as a weighted function of the cooperation, reputation and the quality of security parameters. If there is sufficient reputation, cooperation and known history of trusted collaboration between nodes, node cooperates. Since the WSN is assumed to be dynamic, node movement causes formation of new clusters and clusterheads as nodes move out of communication range. They show that the equilibrium strategy for the game for any two nodes i and j in same or different clusters is for the highest probability of cooperation. They compare the utility-based approach or cluster formation with the distance-based approach in terms of the number of average number of messages passed per node per unit time, average number of clusters and average number of messaged required to delete cluster or nodes from a cluster. They show the utility-based approach performs better than the distance-based approach by requiring lesser number of messages for cluster/node deletion, lesser number of clusters and hence lesser number of messages passed per unit time. An overview of all the above security-related game-theoretic approaches is given in Table 1.

5. Pursuit-evasion games

The final area of game theory research in WSNs that we survey is in the field of detection, tracking and surveillance applications for WSNs. While most of the literature in sensor networks for surveillance applications studies the use of power-constrained sensor nodes that also have constraints on processing and computation ability, in this section, we survey the use of sensor networks with computationally intensive, mobile nodes that are not limited by power constraints. The nature of games played by such networks differs from the games surveyed so far in that, while we still have a set of players (pursuers and evaders), their strategies are solely oriented towards maximizing probability of locating and detecting capture for pursuers and evading capture for pursuers. This is in contrast to the strategies of energy-efficiency games, where nodes adopt strategies that optimize the tradeoff between energy expenditure and social incentives such as reputation or monetary benefits derived from cooperation. Likewise, in security-oriented games, if security attacks are perpetrated by nodes in the network wishing to conserve energy by denying other nodes of broadcast messages, or not participating in routing, the strategies used to achieve efficient network operation range from introducing reputation-based incentives to enlisting the help of intrusion detection systems (IDS) to protect the most vulnerable node from attack by external attackers. However, the strategies for PEGs involve developing efficient algorithms to locate the evader with the help of information obtained from sensor networks using distributed control, multi-sensor coordination. Such efficient control mechanisms can combine information from various levels of heterogeneous sensors to build maps that reflect the highest probability of evader presence in a certain region of the environment [24].

The game formulations in PEGs follow one of the following three approaches: *worst-case* approach, where the

Table 1
Summary of various security-related game-theoretic approaches

Type of attack	Defense strategy	Ideal strategy	Payoff function
External intruder: Attacks most vulnerable node in the network	IDS protects clusters of nodes from the intruder	IDS protects the same cluster which the intruder attacks	Function of utility, cost of defending/protecting a cluster
External intruder: Injects malicious packet in the network	Service provider tries to detect malicious packets by sampling network flows at various links	Sampling strategy should be greater than the maximum flow of packets	Function of the probability of detecting a malicious packet
External attacker: Causes nodes to turn malicious by causing them to prevent broadcast messages from reaching other nodes	A certain subset of nodes, unknown to attackers sends acknowledgement to the base station for the broadcast messages	Detect attacked nodes so that attacker payoff goes to zero	Attacker payoff is proportional to the number of nodes deprived of the broadcast messages
Internal: Malicious nodes do not forward incoming packets	Introduce reputation ratings for collaboration between nodes	Catch nodes in the process of being malicious, i.e. while dropping packets	Function of a discount factor times the previous payoff
Internal: Malicious nodes in mobile WSNs do not forward incoming packets	Maintain good cooperation, reputation and quality of security ratings at each node	Nodes cooperate only if there has been a good history of cooperation, reputation and quality of security, otherwise they defect	Function of the distance between nodes, number of packets forwarded and received, quality of service of traffic as a % of exposed traffic when security is compromised

pursuers search for the evader in unknown environments [25]. To overcome the complexity of searching for evaders in an unknown environment, another approach is to obtain maps of the environment beforehand and use this information to develop PEGs for evader capture [26]. The third approach is the *probabilistic* approach, where the pursuers search for evaders by simultaneously building maps of the environment and utilizing pursuit algorithms to detect and capture evaders [24]. We now look at a probabilistic formulation of a PEG between pursuers and evaders in an obstacle-filled environment.

In [24], the authors model a probabilistic PEG between a group of pursuers and evaders in a 2-dimensional environment. The environment consists of square cells and an unknown number of obstacles. Pursuers comprise of two groups of agents – unmanned aerial vehicles (UAVs) and unmanned ground vehicle (UGVs), where UAVs can locate and share information about evaders' location, but not capture them. An evader is said to be captured when the distance between the pursuer and the evader is lesser than a pre-specified capture distance. Evaders move independently of each other and pursuers can locate each evader uniquely. Both pursuers and evaders gather information about the environment as a set of following three measurements: pursuer, evader and obstacle locations. At each time instant, pursuers estimate the locations of evaders and obstacles from this information and recursively find the conditional probability of the evader being in a given cell at that instant and compute an evader map. The game ends when all evaders are captured. The authors assume a simple binary model to determine the presence of an evader/obstacle, i.e. [0,1] to indicate false positives and false negatives. Using the probability of calculating false positives and false negatives and also the information about the pursuer and evader locations, the authors calculate another map for the obstacles in the environment. To determine the position of the evader(s) at the next time instant, pursuers assume a Markov model that calculates the probability of the evader moving to one of the eight cells adjacent to its current cell location. They define two greedy policies for the pursuers: local-max and greedy-max. In local-max, the pursuer searches and moves to that location in the one-step reachable set that has the highest probability of containing an evader. This probability can be executed by each pursuer locally, and hence is a scalable and computationally-efficient strategy. In global-max, the pursuers search over the entire map to determine the location closest to the evader. While this strategy is more computationally intensive than local-max, it has been shown to outperform local-max policy by requiring lesser capture time for evader capture. The strategies outline so far assumed the instance of randomly-moving evaders. The authors then introduce the case of intelligent evaders that build maps of the pursuer and obstacle locations and intelligently evade the pursuer. Their simulation results show that it takes longer to capture an intelligent evader than a randomly-moving evader.

In [27], the authors introduce additional strategies for improvement of PEGs. The performance of the local-max and global-max strategies discussed above can be further improved by avoiding overlap between the sensing regions of pursuers. The authors thus define 'local max with no overlap', where a pursuer that moves to a region that overlaps with the sensing region of another pursuer is heavily penalized. This reduction in incentives forces pursuers to choose strategies to move to unsensed locations to detect the evaders, thereby improving efficiency of the local-max algorithm. In order to reduce overlap in the global-max policy, the authors introduce a modified 'global max with no overlap' policy where instead of the pursuer moving directly from its current position to the next position to detect the evader, it can take one of three routes: move along the principal direction, or move along one of two 45° lines to the principal direction. The pursuers then use the 'local max with no overlap' policy along the chosen route to move to call location closest to the evader. They further improve the global max policy, by implementing it over sub-regions of the map instead of the entire map. The area of a sub-region is equal to the sensing region of a pursuer. A pursuer is assigned to a given location for the next time instant in a sub-region, such that the pursuer's distance to the evader is the least. This process is adopted for all pursuers in their respective sub-regions. They then move to these computed locations using the 'global max with no overlap' policy. This policy ensures that pursuers are not over-assigned to certain locations. A summary of the player-motion algorithms is shown in Fig. 10.

Simulation results show that the reduction in sensing-overlap and avoiding over-assignment of pursuers resulted in lower median capture time for the local-max and global-max strategies with no overlap and the global sub-regional policies. The features of these strategies for pursuers and evaders are given in Tables 2 and 3.

We now present the application of a traditional sensor network of power-constrained nodes that can be used to aid in PEGs. In [28], the authors describe one such scenario where, sensor networks have been shown to improve the detection ability of pursuers. Since pursuers usually have limited visibility over the surveillance region, the use of sensor networks can improve visibility for pursuers by enabling search over the entire region. Sensor networks can also improve communication between pursuers, since their large scale deployment over the entire surveillance region can function as relays to pursuers and can result in faster dissemination of sensed data between pursuers. The authors propose sample hardware and software architectures to address localization, synchronization and scalability and distributed control between pursuers. They present a hierarchical control structure to implement distributed control applications for PEGs with the help of sensor networks. They extend the idea of hierarchical control structures for PEGs using sensor networks to a specific implementation of space monitoring and debris detection [29]. They use a PEG framework with sensor networks to detect and capture debris (evaders) with the help of space vehicles (detectors), both of which are orbiting around the earth. Sensor nodes deployed over the surveillance region are used to provide location estimates of nearby objects in their sensing region using signal strength measurements and then communicate this information to supernodes over the shortest paths. The measurement process is as fol-

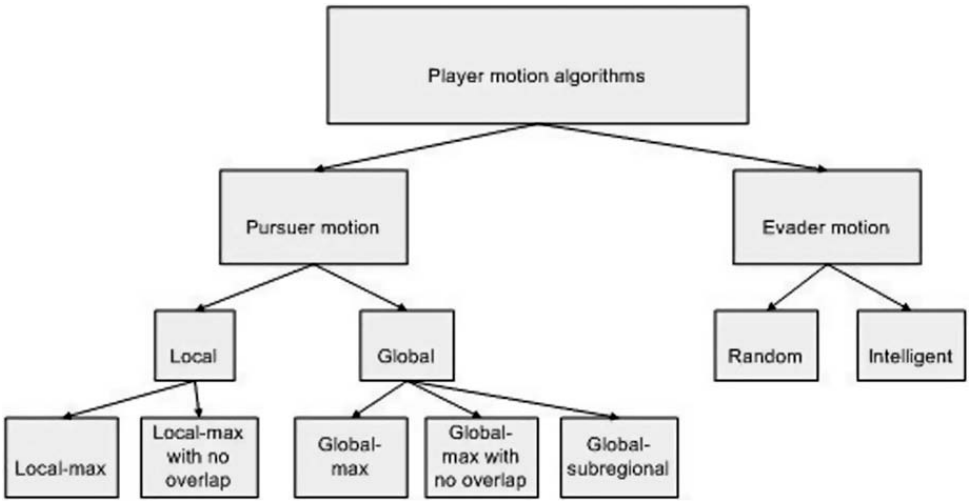

Fig. 10. Overview of motion algorithms for pursuers and evaders in pursuit-evasion games.

Table 2
Features of various pursuit-evasion algorithms for pursuers in PEGs

Algorithm	Features	Advantages/Disadvantages
Local-max	• Search and move to that local in the one-step reachable set with highest probability of evader presence	*Advantages*: Uses local information, Computationally less intensive, scalable
Local-max with no overlap	• Pursuers are penalized for moving to cells that overlap with sensing regions of other pursuers	*Advantages*: No overlap
Global-max	• Pursuers search over entire map and move toward cells with maximum distance-discounted probability of evader presence along the direct line joining the pursuer's current location to evader's current location. (Principal direction)	*Advantages*: Lesser time for evader capture
Global-max with no overlap	• Pursuers can move towards target cell along one of three paths: principal direction or one of two 45° lines to right and left of principal direction. The choice of the preferred path is made using local max with no overlap policy.	Disadvantages: Assigns all pursuers to one specific target area, underutilize network resources
Global sub-regional	• The grid is divided into sub-regions, and the sub-region with maximum reward value is selected. Further, the single cell within this sub-region with maximum reward is chosen. The pursuer closest to this cell is instructed to move toward this cell according to global-max with no overlap policy. This cells is removed from further iterations, where this step is iterated for all sub-regions and pursuers	*Advantages*: Best policy in terms of lesser capture time, utilization of network resources

Table 3
Features of various pursuit-evasion algorithms for evaders in PEGs

Algorithm	Features	Advantages/Disadvantages
Random evader motion	Evaders move randomly across the grid	Advantages: Lesser time to capture
Intelligent evader motion	Perfect knowledge of pursuer and obstacle locations	Disadvantages: Longer time to capture

lows: A sensor detects the presence of an object from the signal strength as z_i. It also listens for measurements of z_i from nearby sensors. If an incoming z_i is larger than all incoming messages, then the position of the object is estimated from the value of the largest z_i and communicated to the nearest supernode. The estimation accuracy increases with the number of nodes participating in the sensing operation. The authors incorporate communication delay and transmission failure in the sensing model and propose a multi-layer control architecture for this scenario. With the help of a mathematical formulation for the vehicle dynamics, efficient tracking algorithms and the hierarchical control architecture, they show that the inclusion of sensor networks in the PEG framework can greatly benefit in developing efficient pursuit strategies for pursuers in a distributed surveillance environments.

6. Conclusion

This article discussed problems dealing with energy efficiency, security and detection/tracking in WSNs with the help of concepts from game theory. Modeled to imitate social behavior, approaches from game theory are feasible for wireless sensor nodes, in which nodes strive to achieve

conservation of battery power by selfish behavior. We discussed energy efficiency in networks where nodes specialize to different roles for power saving, while satisfying the objective function of maximizing the number of nodes involved in a sensory computation. Thus, while every node works on power saving as well as maximizing the network utility which is directly proportional to the number of sensors involved, the network achieves optimization of energy over a long time. We have also discussed multiple sensor networks, where nodes belonging to different authorities behave selfishly and refuse to forward packets of sensors from another network. This problem has been modeled to involve two authorities with different action profiles, one of which is cooperative equilibrium. Cooperative packet forwarding has been found beneficial when the two authorities have common or individual sinks per authority. The existence of networks of multiple authorities has been discussed in the context of routing, where incentives in the form of tokens are given to a network for participating in cooperative forwarding. Reliable query routing has been discussed in which replies to a query from the sink are classified according to their importance and the high-value data are routed over reliable paths. We also present the problem of load balancing from a bandwidth allocation perspective in sensor networks, where the sensor nodes are classified into levels. The levels are determined by the number of hops they are away from the sink. The goal is to find nodes on the previous level, parents that have fewer children and attach to it. The utility here is the bandwidth guarantee that the parent provides to the child. Various security-oriented formulations have been detailed, involving attacks by malicious nodes and external attackers where the objectives of the attack range from denial of service, selfish routing and introducing malicious packets for specific nodes as targets. We also summarized recent research on pursuit-evasion games in WSNs used to model detection, tracking and surveillance applications. These formulations have provided insight into the ways of applying game theory to sensor networks. As the applications of wireless sensor networks increase, it will be useful to apply models from theories that model the behavior of sensor networks from a rational point of view. Increased interaction between nodes requires the use of distributed algorithms to achieve increase in network lifetime and reliable network operation. This paper presented an overview of the applications of game theory to wireless sensor networks in recent literature and emphasizes the need for modeling sensor networks with problem formulations based on the nature of interaction between nodes in wireless sensor networks.

References

[1] M. Cardei, J. Wu, Energy-efficient coverage problems in wireless ad-hoc sensor networks, Journal of Computer Communications 29 (2006) 413–420.

[2] W.R. Heinzelman, A. Chandrakasan, H. Balakrishnan, Energy-efficient communication protocol for wireless microsensor networks, in: Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, vol. 2, 2000.

[3] M. Dorigo, V. Maniezzo, A. Colorni, Ant system: optimization by a colony of cooperating agents, IEEE Transactions on Systems, Man and Cybernetics 26 (2) (1996) 29–41.

[4] M. Zhu, R. Brooks, M. Piretti, S.S. Iyengar, Physics and Chemistry, in: R. Brooks, S.S. Iyengar (Eds.), Distributed Sensor Networks, Chapman and Hall/CRC Press, 2005, pp. 879–894.

[5] A.B. MacKenzie, L.A. DaSilva, Game Theory for Wireless Engineers (Synthesis Lectures on Communications), Morgan & Claypool Publishers, 2006.

[6] J. Byers, G. Nasser, Utility-based decision-making in wireless sensor networks, in: Proceedings of the First ACM International Symposium on Mobile ad hoc networking and Computing, Poster Session, 2000, pp. 143–144.

[7] A. Agah, M. Asadi, S.K. Das, Prevention of DoS attacks in sensor networks using repeated game theory, in: Proceedings of the International Conference on Wireless Networks, 2006.

[8] P. Sakarindr, N. Ansari, Security services in group communication over wireless infrastructure, mobile ad hoc and wireless sensor networks, IEEE Wireless Communications Magazine (2007) 8–20.

[9] M. Felegyhazi, J.-P. Hubaux, L. Buttyan, Cooperative packet forwarding in multi-domain sensor networks, in: Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications Workshops, 2005, pp. 345–349.

[10] J. Yuan, W. Yu, Distributed cross-layer optimization of wireless sensor networks: a game theoretic approach, in: Proceedings of IEEE Global Telecommunications Conference, 2006.

[11] S.D. Servetto, G. Barrenechea, Constrained random walks on random graphs: routing algorithms for large wireless sensor networks, in: Proceedings of the First International ACM Workshop on Wireless Sensor Networks and Applications, 2002, pp. 12–23.

[12] D. Miller, S. Tilak,T. Fountain, "Token" equilibria in sensor networks with multiple sponsors, in: Proceedings of the Workshop on Stochasticity in Distributed Systems, 2005.

[13] R. Kannan, S.S. Iyengar, Game-theoretic models for reliable path-length and energy-constrained routing with data aggregation in wireless sensor networks, IEEE Journal of Selected Areas in Communications (2004) 1141–1150.

[14] G.V. Crosby, N. Pissinou, Evolution of cooperation in multi-class wireless sensor networks, in: Proceedings of the 32nd IEEE Conference on Local Computer Networks, 2007, pp. 489–495.

[15] N. Sadagopan, M. Singh, B. Krishnamachari, Decentralized utility based sensor network design, Journal of ACM Mobile Networks and Applications 3 (2006) 341–350.

[16] H. Dai, R. Han, A node-centric load balancing algorithm for wireless sensor networks, in: Proceedings of the IEEE Global Communications Conference – Wireless Communications, vol. 1, 2003, pp. 548–552.

[17] I. Raicu, Local load balancing for globally efficient routing in wireless sensor networks, International Journal of Distributed Sensor Networks 1 (2005) 163–185.

[18] N.J. Harvey, R.E. Ladner, L. Lovasz, T. Tamir, Semi-matchings for bipartite graphs and load balancing, in: Proceedings of Workshop of Algorithms and Data Structures, 2003.

[19] A. Agah, K. Basu, S.K. Das, Preventing DoS attack in sensor networks: a game theoretic approach, in: Proceedings of IEEE International Conference on Communications, vol. 5, 2005, pp. 3218–3222.

[20] M. Chatterjee, S.K. Das, D. Turgut, WCA: A weighted clustering algorithm for mobile ad hoc networks, Journal of Cluster Computing (Special Issue on Mobile Ad hoc Networks) 5 (2002) 193–204.

[21] M. Kodialam, T.V. Lakshman, Detecting network intrusions via sampling: a game theoretic approach, in: Proceedings of Twenty Second IEEE INFOCOMM, 2003.

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

[23] A. Agah, K. Basu, S.K. Das, A game theory based approach for security in sensor networks, in: Proceedings of the International Performance Computing and Communications Conference, 2004.

[24] R. Vidal, O. Shakernia, H. Kim, D. Shim, S. Sastry, Probabilistic pursuit-evasion games: theory, implementation, and experimental evaluation, IEEE Transactions on Robotics and Automation 18 (5) (2002) 662–669.

[25] I. Suzuki, M. Yamashita, Searching for a mobile intruder in a polygonal region, SIAM Journal of Computing 21 (5) (1992) 863–888.

[26] S. Thrun, W. Burgard, D. Fox, A probabilistic approach to concurrent mapping and localization for mobile robots, Machine Learning and Autonomous Robots 31 (5) (1998) 1–25.

[27] A. Antoniades, H.J. Kim, S. Sastry, Pursuit-evasion strategies for teams of multiple agents with incomplete information, in: Proceedings of Forty Second IEEE Conference on Decision and Control, vol. 1, 2003, pp. 756–761.

[28] B. Sinopoli, C. Sharp, L. Schenato, S. Schaffert, S.S. Sastry, Distributed control applications within sensor networks, Proceedings of the IEEE 91 (8) (2003) 1235–1246.

[29] L. Schenato, O. Songhwai, S. Sastry, P. Bose, Swarm coordination for pursuit evasion games using sensor networks, in: Proceedings of the IEEE International Conference on Robotics and Automation, 2005, pp. 2493–2498.

Renita Machado received her B.E. degree in Electronics and Communications Engineering with distinction from Manipal Institute of Technology, Manipal, India in 2004. She received her M.S. degree in electrical engineering from New Jersey Institute of Technology, NJ in 2005. She is currently pursuing her Ph.D. in Electrical Engineering while conducting research at the New Jersey Center for Wireless Networking and Internet Security (NJWINS lab) at New Jersey Institute of Technology. Her research interests are in mobile ad hoc networks, wireless sensor networks, pervasive computing and cognitive modeling for wireless networks.

Sirin Tekinay received her Ph.D. degree in Electrical and Computer Engineering from George Mason University in 1994. She holds MS (1991) and BS (1989) degrees in Electrical Engineering from Bogazici University, Istanbul, Turkey. She joined the Division of Computing and Communications Foundations (CCF), National Science Foundation as the Program Director for Theoretical Foundations in Communications Research in September 2005. She recently received the NSF Director's Award for "Excellence in Program Management." She has been on faculty at Electrical and Computer Engineering Department, New Jersey Institute of Technology since 1997, where she is currently an associate professor. She was the recipient of NJIT's "Excellence in Graduate Teaching Award" in 2003. Before joining the academia, she worked at Bell Labs, Lucent Technologies, and NORTEL. Her current research interests include cross layer wireless communication and network system design and analysis, traffic modeling, mobility and location problems, ad hoc and sensor networks. She holds eight patents. She has authored numerous publications, developed and offered courses. She is on the Board of Governors of the IEEE Communications Society, and the editorial board of the IEEE Communications Surveys and Tutorials.