Book Title: XXXXXXXXXXXXXXXXXXXXXXXXXXXX

Editors

June 20, 2009

Contents

Chapter 1

Game Theory in Wireless Sensor Networks

Pedro O.S. Vaz de Melo, Cesar Fernandes

abstract abstract

1.1 Introduction

1.2 Taxonomy

In this section we show the possibilities of applying game theory in WSNs. Differently from general ad-hoc networks, a WSN is controlled by a single authority, that is responsible to program all its network devices to respond indiscriminately to its commands, without any rational decision making. Thus, in a single WSN, the unique rational agent that can make strategic decisions is the authority that governs the network. This implies that game theory, at first, can only be naturally applied when there is a conflict involving this authority.

One situation where there is a conflict involving the authority that governs the WSN is when one or more WSNs are deployed near each other and interaction between then is possible. In this case, the WSNs may cooperate with each other to improve their operabilities, such as extending its life time by trading routing favors or increasing the data entropy by a common data aggregation. The problem with this cooperation is that the owner of WSNs is only concerned with its network operability, and will only cooperate if this brings clear benefits to the network. He must ensure that its network operability will be higher in a cooperative scenario than in a non-cooperative one.

Other situation where the authority that governs the WSN interact with another rational agent is when its network is under attack of a malicious agent. (CESAR, ESCREVA ESSE PARGRAFO)

Besides the application to scenarios where there is a conflict among rational agents, game theory may be also applied to distributed decision making in WSNs. Since the number of sensor nodes in WSNs can extend to large values such as hundreds of thousands, its decision making should be local, without any assistance of a central authority. Thus, game theory may be used in the design of utility functions that aims to optimize a global network metric from local decisions of the sensor nodes. Figure 1.1 abstracts the possible applications of game theory to WSNs, that will be detailed later in this chapter.

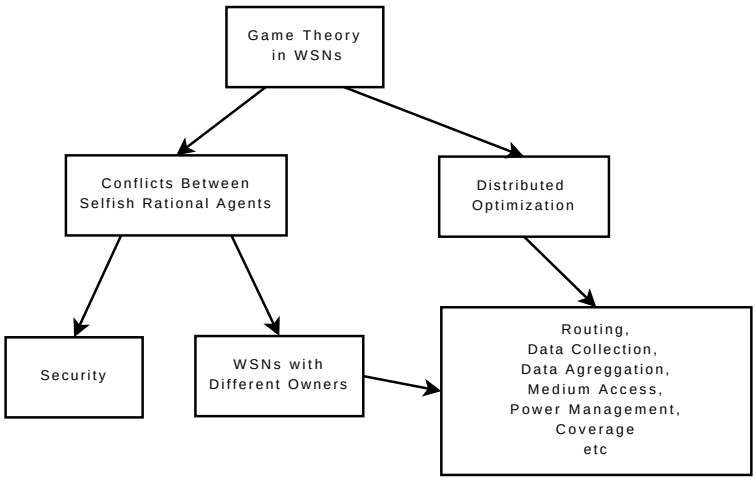


Figure 1.1: Taxonomy of possible applications of game theory to WSNs.

1.3 Conflict Between Selfish Rational Agents

1.3.1 Cooperation Between Different Networks

In a near future, it is expected that the WSNs are deployed on the most different and varied places, like forests, vulcans, seas, cities and deserts. Therefore, the usual scenario for this near future is that distinct WSNs owned by different authorities work at the same place, serving as base for a wide variety of applications. In the Amazon forest, for example, we could have a WSN, owned by the government, deployed for detecting fires and another WSN, owned by a private company, deployed for detecting the movement of specific species of animals.

When two WSNs, installed at the same place, share their sensors nodes in the execution of one or more activities in a intelligent way, both networks may improve their operabilities and perform their activities in a more efficient way. Despite being obvious and simple, this idea brings with it many implications that hinder cooperation between the networks. Whereas a WSN has a rational and selfish character, it will only cooperate with another WSN if this provides services that justify the cooperation. Thus, to model this situation, game theory is used to assess the conflict between the authorities responsible for the networks, which are modeled as the players. Each authority wishes to both maximize the lifetime and the

quality of service of her network, and will only cooperate with another network if it brings her benefits.

In [9], the authors consider that different WSNs may cooperate in the packet forwarding toward the sink node in order to save their energies. They investigate whether cooperation can exist based solely on the self-interest of the authorities that control the networks, without any cooperation enforcement mechanism. In this way, a sensor node that receives a packet from other network may drop it for no particular reason.

It is assumed that time is divided into time slots and, once per time slot, the sensor nodes send their data packets to their sink nodes. In the game theoretic model, the authorities that control the networks are the players of the game and an authority i strategy at time slot t is to define a move $m_i(t)$, characterized by the combination of two actions: let their nodes forward other network packets and/or ask the other network to forward its packets. For each time slot it is also defined a variable $\xi(t) \in \{true, false\}$ that tells if the data collection at time slot t was satisfactory. This is measured by comparing the number of collected data received $\rho_i(t)$ at time slot t with the number of collected data requested SR_i, defined by the application. If $\rho_i(t) \geq SR_i$, then $\xi(t) = true$, otherwise, $\xi(t) = false$. If $\xi(t) = true$, player i receives a gain $g_i(t) = G_i$, otherwise it receives $g_i(t) = 0$. Thus, the payoff $\pi_i(t)$ of player i in time slot t is $\pi_i(t) = g_i(t) - c_i(t)$, where $c_i(t)$ is the total transmission and reception cost of all sensors that belong to i for all packets, considering that $G_i \gg c_i(t)$ for every time slot t[1].

Thus, at every time slot, each player updates its strategy, by altering it move $m_i(t+1)$ in function of $\xi(t)$. To do this, every sensor node receives at each time slot t a bit informing the result of $\xi(t-1)$. The utility U_i of each player i is the cumulative payoff for each time slot t until T, that is the time slot in which the network controlled by i become inactive. The utility function of player i is then defined as $U_i = \sum_{t=0}^{T} \pi_i(t)$ and the objective is to maximize U_i, i.e., report data collections successfully as many times as possible, while minimizing the energy consumption.

[1]This assumption is commonly used when applying game theory to WSNs, since it is rational to think that it is worth to send packets toward the sink when these packets are relevant to the application

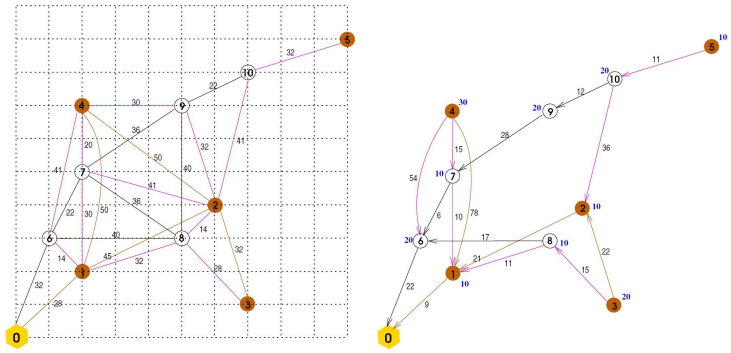
The results of [9] show that the networks converge basically into two states of equilibria, a non-cooperative, which no node provides and asks for services to nodes from another network, and a cooperative, which all nodes provide and ask services to nodes from another network. Moreover, it was found that when the environment is very dense, the cost of receiving dominates the cost of transmission, making the algorithm converge to the non-cooperative equilibria. It was also shown that when the environment is hostile, that is, the value of path loss exponent is high, there are strong incentives for cooperation.

In contrast to a practical approach, one can understand the theoretical issues of providing strategies that allow cooperation among different networks. Wu et al. [22] propose an *InterSensorNet* scheme which is a federation of multiple sensor networks, that depends on whether a node is willing to cooperate with nodes in a foreign network. In this case, the players of the game are the sensor nodes. Each sensor node has a type t_i, that defines its marginal cost c_i to perform an determined activity. Player i strategy is to reveal a cost a_i to perform its strategy, with a_i not necessarily being equal to c_i. Given the declared costs of every player, a player can decide whether it will contract its services or not. Every player that provides a service receives a payment in the form of credit according to a_i.

Considering this formulation, the authors of [22] propose a mechanism design for data collection in the problem of cooperation among different WSNs. In the data collection, the cooperation should be a choice when a sensor node cannot be reached by its local network and nodes from a foreign network can offer assistance in routing. Moreover, cooperation is beneficial when nodes from a foreign network assist routing traffic via a less expensive path.

Thus, in the mechanism design for the data collection, the authors showed that if the agent reveals its real cost for routing a packet, its benefits will be maximized. In Figure 1.2-a we can observe a sample sensor map in which two WSNs are deployed. The circles with numbers greater than 0 are the sensor nodes, and the circle with number 0 is the sink node. The number on each edge represents the physical distance between the nodes. Network E_1 includes nodes $\{n_1, n_2, n_3, n_4, n_5\}$ and network E_2 includes nodes $\{n_6, n_7, n_8, n_9, n_{10}\}$. The network graph is shown in Figure 1.2-b, where the reception costs are marked next to the nodes and the transmission costs are marked on the edges. Only edges that are used in

communication are shown. We observe that several sensor nodes from a network can use sensor nodes from the other network to reduce its communication costs, e.g., node $n_7 \in E_2$ without cooperation routes its packets through $n_6 \in E_2$ with a path cost of 48 and, with cooperation, it may route its packets using $n_1 \in E_1$ and reduce the path cost to 29.



(a) A sensor network map **(b)** A sensor network graph

Figure 1.2: *InterSensorNet* for data collection. [22]

Another approach to study the problem of cooperation among different WSNs was made by [8], that studied the evolution of cooperation using Evolutionary Game Theory. The authors modeled this problem as a non-cooperative iterated N-player game $g = (P, S, U)$, where P denotes the set of players, S the set of strategies and U is the set of utility functions that define the payoff. The players are, again, the authorities that control the networks, and their strategies are to define if all their sensor nodes will cooperate or not with sensor nodes of a foreign network. The time is divided into time slots and, once per time slot, the sensors of each WSN send packets to be forwarded by a node from a foreign network, that follow the strategy defined to it. This game was assumed to be infinite, since there is a very small probability that the game end in any time slot, i.e., the players are unaware of the ending of the game.

This game, the way it was modeled, is identical to the Iterated Prisoner Dilemma game, which payoff matrix is shown in Figure 1.3. First, the authors consider that the networks expend battery power equivalent to a disincentive in the amount β and gain an incentive for cooperation in the amount γ, following the inequality $\gamma > \beta > 0$.. While the so-called "reward" $R = \gamma - \beta$ represents the payoff for mutual cooperation, the payoff for defection on both sides is the "punishment" $P = 0$. When a network unilaterally defect it gets the

"temptation" payoff $T = \gamma$, while the cooperating network gets the "suckers payoff" $S = -\beta$. Given the inequality $T > R > P > S$ and the assumption $2R > T + S$, mutual cooperation returns the highest collective payoff in repeated encounters.

The authors of [8] demonstrate that cooperation is not evolutionary stable when the networks are playing the iterated N-player prisoners dilemma. Moreover, they showed that in the case of stationary classes there is some possibility for cooperation to emerge without any incentive. For this case, they presented a localized distributed and scalable algorithm called Patient Grim Strategy, that tells a sensor node to cooperate and continue cooperating until the other player defects n times ($n > 0$), then defect forever. This protocol proved that it is a Nash equilibrium of the modeled problem.

In [21], besides routing favors, the authors consider the possibility of different WSNs exchange favors from different nature, such as routing, sensing, processing and data storage. They consider in the formulation of the problem two sponsoring organizations $i \in \{A, B\}$, that are the same authorities that control the networks, each one with K sensors $s_{i1}, ..., s_{iK}$. Each sensor has a probability λ of providing a favor at time slot t, with the payoff of sensor node s_{ik} at time t being given by $u_{ik}(t) = \alpha R_t - \beta P_t - \gamma C_t$, where α,β and γ are positive parameters, R_t is the number of favors received by s_{ik}, P_t is the number of favors provided by s_{ik} and C_t is the number of transmissions made by s_{ik}. Given this, the utility of a network i in the entire game is

$$U_i = \sum_{t=1}^{T} \sum_{k=1}^{K} u_{ik}(t) + \tau_i$$

where τ_i is monetary transfer received by the authority i after the end of period T. The monetary transfers should be bounded above, i.e., $\tau < \infty$, and zero sum, i.e., the transfers τ_A received by authority A should be equal to the transfers τ_B given by authority B. Moreover, the authors assume that $\gamma/\lambda < \alpha - \beta$, so the networks can gain by cooperating. By these constraints, the authors show that a stable solution and beneficial to both systems is only feasible if the owners of the networks sign a financial contract before the network deployment.

It is important to emphasize that the problem of cooperation among different WSNs involves several parameters that can significantly influence the establishment of cooperation. In [26], these parameters are listed and explained, and through simulation, the benefits of cooperation are discussed. This work shows that the configuration of the network impact on the benefits that cooperation can bring, and among the parameters, the path loss exponent, the density, the data collection rate the routing algorithm must be carefully considered when this problem is addressed.

1.3.2 Security

Wireless sensor networks have severe constraints regarding to energy consumption and processing capacity. Due to this issue, most of the well-known techniques to ensure security cannot be applied. Therefore, new strategies need to be devised to achieve good security levels while satisfying these constraints.

Message forwarding

One of the most important problems occurs when one node needs to choose which nodes to trust at forwarding its messages. The paper [1] proposes a game-theoretic technique to deal with this security issue during communications in wireless sensor networks. The approach takes into account reputation, cooperation, quality of security and distance. The distance is taken into account because the nodes expend more energy sending long-ranged signals than sending short-ranged ones. Hence, choosing close hops saves energy.

The game is modeled with the nodes being the players. The utility function is defined for each pair of nodes, and considers the reputation, cooperation and distance between them. The Nash equilibrium is presented, and one pair cooperates with another if the reputation of the other node is sufficient, if there is a good history of joint operations and if they are close enough. Based on this cooperation, clusters of cooperative nodes emerge.

To evaluate the solution a simulator was implemented. The nodes in the simulation can

move, therefore, the distance between two nodes can change, also changing the utility. The scheme proposed is compared to the strategy that only considers proximity. Over time, the average value of the payoff functions and the number of clusters drop. The number of clusters is considerably lower than with the distance-based algorithm. Also, the number of messages passing per node, on average, is lower in the proposed method if compared to the distance-based one.

Message dropping attacks

The previous article helps deciding whether to trust or not another node. The decision of trusting or not is done locally within each node. However, sometimes, it is crucial to flag the untrustworthy nodes, and, ultimately, exclude them from the network. Thus, the network would achieve higher quality.

The paper [2] addresses the detection of passive DoS at the routing layer. DoS occurs when, in order to save energy, malicious nodes refuse to deliver packets from other nodes. This behavior degrades the quality of the results achieved with a network.

The problem is modeled as a game, where the players are the intrusion detection (IDS) system and the nodes, which this IDS monitors. The game is repeated several times. Each turn, the IDS plays against each node. Based on the behavior of the node on the last turn, the IDS has to decide whether it is malicious or not.

In order to decide this, a utility function was devised to model the payoffs. The table 1.4 depicts these payoffs.

Nodes flagged as malicious will behave maliciously for the rest of the game, regardless if the classification was accurate. Also, catching a bad node has a high payoff. On the other hand, each node has to decide to play cooperatively or not. To promote cooperative actions, a scheme of reputation was created. The impact in the reputation is considered, along with energy consumption, to decide whether to forward a packet. Nodes caught as malicious, will be flagged as malicious for the rest of the game.

After, they propose a technique to define a route to send a packet. This route is defined to be the one with highest payoff, from all possible paths. The payoffs are calculated as the difference between the reputations of each node in the path and the power consumption of these nodes. Since malicious nodes have low reputation, usually, the routes chosen exclude them.

The protocol is tested with simulation to verify the resilience to the increase of malicious nodes and the accuracy of detections of the IDS. The increase on the number of malicious nodes has a high impact on the system. The Figure 1.5 shows this impact.

With 10% of malicious nodes, the throughput dropped to 52%, and with 20% of bad nodes, the throughput dropped to 35%.

Also, as depicted by Figure 1.6 over time, the algorithm gets better at isolating the malicious nodes, preventing them from participating of transmissions.

Another security breach occurs when malicious nodes refuse to forward broadcasts, which is called Denial-of-Message. In the previous articles, the nodes maliciously refused to forward messages from each other, now, messages broadcasted, which may be control messages, are not forwarded.

The paper [20] deals with this issue. It analyzes the problem using a game-theoretic approach and suggests countermeasures.

The most common countermeasure to the attack is for every node to reply to a broadcast with an ACK packet. However, this overloads the network. The article proposes the Secure Implicit Sampling, which reduces the amount of ACKs sent. This protocol chooses a subset of nodes that are required to send an ACK; this subset is unknown to the attacker. Also, since the model takes the possibility of failures on the network into account, ACKs may be lost despite the action of malicious nodes. The system is trained to define the threshold to set apart expected failures from attacks.

The attacker is modeled to maximize its payoff over time. The increase on the number of compromised nodes also increases the probability of detection. Therefore, the utility

		N_q	
		Cooperate	Not Cooperate
N_p	Cooperate	P, P	S, T
	Not Cooperate	T, S	R, R

Figure 1.3: Payoff matrix of the "Prisoner's Dilemma" game.

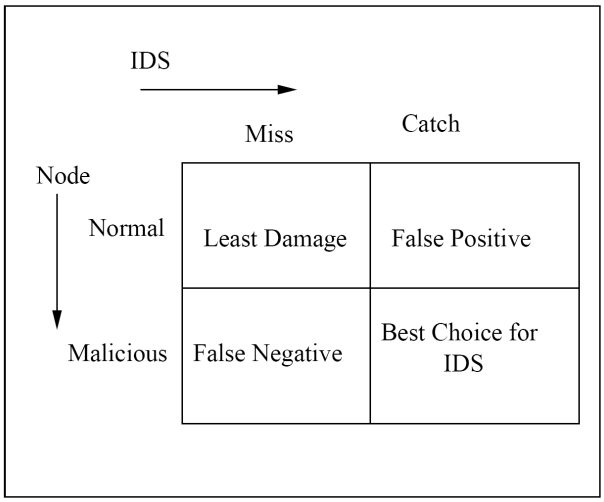


Figure 1.4: Payoff matrix. [2]

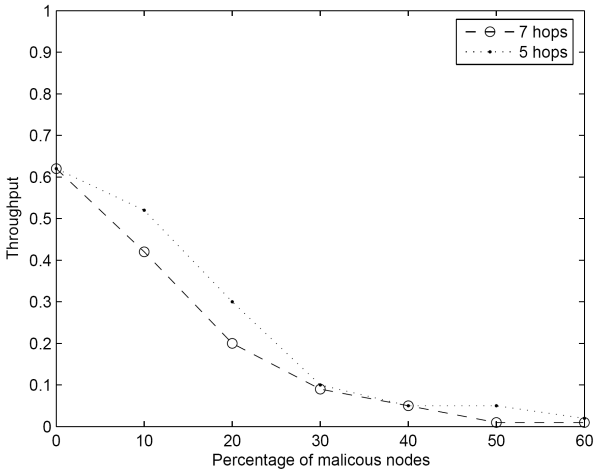


Figure 1.5: Impact of the fraction of malicious nodes. [2]

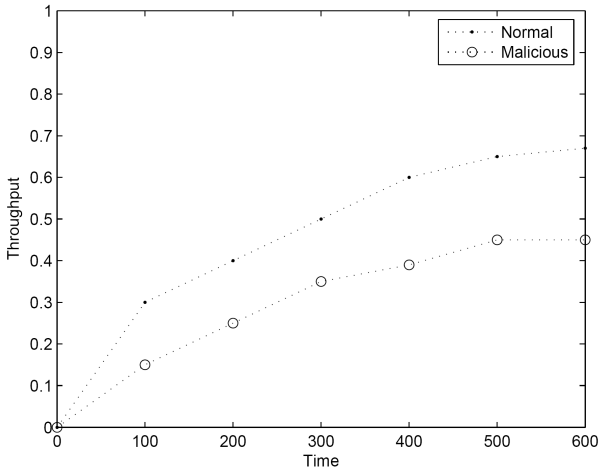


Figure 1.6: Behavior over time. [2]

function of the attacker takes into consideration this probability and models a trade-off between detection probability and nodes prevented from receiving the broadcast. Also, theoretical forecasts about the accuracy of the model are given.

A study is conducted to assess how well the theory predicts the simulation results. The forecasts are shown to be quite close to the simulated results.

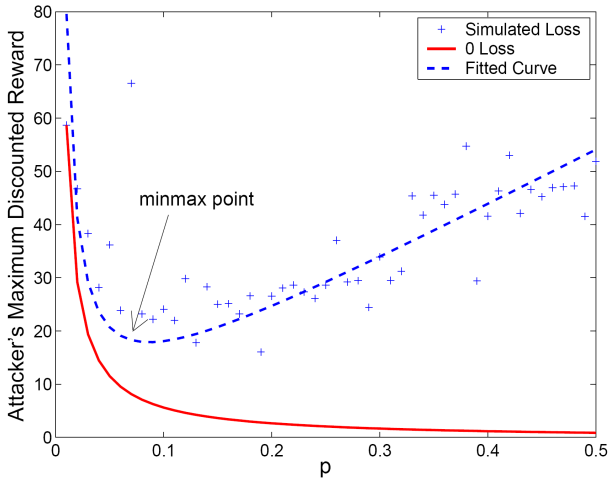


Figure 1.7: Impact of the fraction of ACKs. [20]

They also present the optimum parameters for their strategy on the topology tested. The Figure 1.7 depicts these results. The x-axis shows the fraction of the ACKs and y-axis shows

the payoff of the attacker. In a situation with no natural loss of packets, increasing the number of ACKs also decreases the attacker's payoff. However, surprisingly indeed, when there are losses due to natural causes, increasing the number of ACKs is only helpful till a certain extent. After this minimum point, increasing the number of ACKs decreases the quality of the system, increasing the gain of the attacker.

Generic intrusion detection

So far, only the problem of messages maliciously dropped was investigated. However, there are several other possible attacks in sensor networks. Therefore, some works created generic frameworks to address the intrusion detection issue without focusing on a specific attack.

The paper [3] divides the nodes within clusters, and the objective is to choose which cluster to protect at each period of time. Due to limitations, the intrusion detection system (IDS) is modeled as being able to protect only one node at a time. To meet this requirement, each cluster has a cluster head, which is the node that would be protected if the cluster is chosen to be kept safe. In order to decide the cluster to be protected, three techniques are presented and evaluated.

The first technique is based on game theory. The game modeled is a two-player non-cooperative, where the players are the IDS and the attacker. The network is divided within clusters, each containing a node that would be protected. Recall that the IDS is capable of protecting only one node. Therefore, the attacker has three options, attack a cluster k, attack a different cluster, or not attack at all. The IDS has two options, defend cluster k, or defend another cluster. The article assumes that the choice of the node to be protected is perfect; hence, whenever an attack occurs to cluster k, the IDS is capable of detecting it by monitoring the chosen node from this cluster. The Nash equilibrium is given, and the IDS needs to protect the cluster k, while the attacker would always attack cluster k. The cluster k to be defended is chosen to be the cluster with the highest utility of all available clusters.

The second strategy is based on Markov decision process. It is designed to, through a learning process, assess the cluster which will be attacked, and, therefore, needs to be

protected. The third strategy protects the cluster with the highest traffic.

The schemes are tested with simulation, even though the attacking algorithm was not clear. The game theory strategy of protecting only the most valuable cluster achieved the highest overall quality of all three strategies.

In paper [4] there are several virtual nodes that correspond to software monitoring agents. They are responsible for monitoring the system and signaling whenever they detect a suspicious behavior. These nodes report to the Intrusion Detection System (IDS), which decides if an attack is occurring. Therefore, differently from [3] where the IDS actively protected a node, in this article, there are several monitoring nodes that report suspect behavior to the IDS. Although the paper does not address wireless sensor networks, the problem studied has straightforward applications in WSN.

The game is modeled involving the IDS and the attackers. The attacker can choose the type of the attack, and the IDS can choose, based on the information received, the response to the signals of the monitoring nodes. The network of nodes is modeled as a third player, which, according to a specific attack, has a probability of correctly alerting the IDS. The game with only one possible attack and only one possible countermeasure to an attack is depicted in the Figure 1.8.

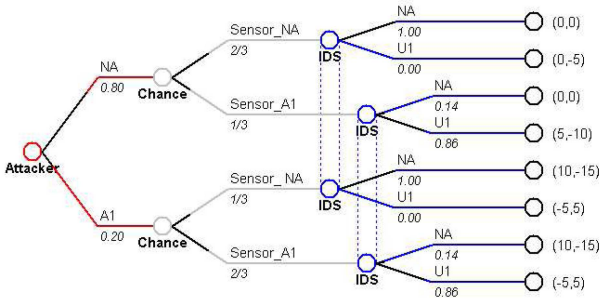


Figure 1.8: Example of a game. [4]

It concludes that using a pure strategy is not adequate for neither of the players. Therefore, each player needs to randomize its action. Also, it presents the Nash equilibrium for the intrusion detection problem.

Jamming attack

One of the possible attacks of an intruder is the jamming attack. Jamming attack occurs when malicious nodes prevent other nodes from communicating. Jamming can be done by interfering on the transmission frequency or by corrupting packets. Also, jamming can occur naturally, since packets may be lost or corrupted without the action of an attacker. The paper [18] addresses the issue of jamming attacks. The article, in particular, deals with attacks based on packet collision.

The attacker is modeled as having a probability of attacking. The attack consists of sending a packet with the intention of causing a collision. The success of the attack depends on the probability of attacking and the probability of a packet being sent during the attack. Also, the attacker faces the tradeoff; attacking more frequently increases the short-term payoff and the probability of being caught, and attacking less frequently increases the payoff on the long run.

The defense mechanism is composed by a fixed number of nodes. These nodes have been trained to assess the probability of random and natural collisions. Therefore, they signal an attack whenever the perceived rate of collisions is above the expected.

The first scenario analyzed is the jamming with constant power and one monitor node. Initially, both sides have full-knowledge about the probability of an access (probability of a transmission from a legitimate node) and the probability of jamming. Therefore, the game is modeled as a zero-sum game where the attacker tries to maximize the time before being caught while still damaging the network, by choosing its probability of jamming, and the network tries to minimize this time, by choosing its access probability. It is concluded that the attacker needs to choose the minimum probability of jamming that does enough damage to the network, in order to stay undetected for longer. The concept of enough corresponds to positive values for the utility function of the attacker, that takes into account the damage and the energy consumed. For the network it is shown that there is an optimum value of access probability. However, the solution needs to be the closest to the optimum that satisfies the energy constraints. Still on the first scenario, both sides are analyzed, now without the

knowledge about the probability of the adversary. Thus, the game is analyzed as a minimax; where each party defines the best response possible considering that the other party has chosen the probability that achieves the highest payoff for itself.

The second scenario is the constant jamming power and several monitors. Now the attacker needs to remain undetected by all monitors, while damaging the network. The solution presented assess that the attacker needs to choose the lower probability of attacking while still doing some damage.

The last scenario is the controllable jamming power and several monitors. In this sense, the attacker can choose how far its jamming signal can reach. Therefore it needs to choose the correct power that maximizes its payoff. The article presents an algorithm for the attacker. The strategy for the attacker is to calculate the payoffs for shortest jamming and for longest jamming. After, it needs to calculate and decide if increasing the power also increases the payoff.

1.4 Distributed Optimization

In WSNs, because the cost of data communication is a major constraint [25], it must be avoided always as possible and transmissions must be performed whether their utility compensate their cost. Consequently, an interesting challenge in WSNs is to develop solutions that are able to judge which sensor activities are essential and which are not given a determined scenario. However, because of the distributed nature and large scale of WSNs, the main challenge in the design of such solutions is to make the decision making of sensor nodes local, that is, without the assistance of a central control. Decentralized and/or distributed control systems can be viewed in mathematical terms as games of identical interests in which player status is attributed to systems components with decision-making or control authority [7].

Given this challengeable scenario, game theory comes with interesting concepts that can aid in the design of distributed solutions for WSNs. To support this, two main ideas serve

as base. The first one is the "sensor-centric" paradigm [14], which states that to maximize network utilization and information viability in a WSN, sensors should cooperate to achieve network wide objectives while maximizing their individual lifetime, since longer a node survives, better it is for the network. The other is the idea of treating the sensor nodes as "selfish", using appropriate utility functions, enables the design of distributed algorithms for optimizing the network performance as a "whole" [23].

1.4.1 Data Collection

In this direction, the work of [6] propose a model in which the sensor nodes adapt themselves locally to improve an utility of the user, that is the consumer of the output of the WSN. The utility is measured by a real value, that is mapped by a monotone utility function $U : S \rightarrow [0 : 1]$ which, for a network graph $G = (V, E)$, defines the real value from the sensing subset $S \subset V$, that is the set of all nodes in the graph that are sensing. The strategy of a sensor node is to define locally which type of activity it will perform, in a way that it increase the function U but also save its energy. The authors call this strategy change as *node specialization*, which defines four types of modes for a sensor node: idle, routing, sensing, or routing/sensing. There are costs c_s, c_t, c_r, c_a associated to the four operations a node may perform: sensing, transmitting and receiving a fixed size message, and aggregating sensory data, respectively.

The authors consider two scenarios: the all-or-nothing case, where the output of the network is totally useful or is useless, and a more forgiving scenario, where the utility of the output varies inelastically. The utility function for both scenarios is illustrated in Figure 1.9. In the first scenario the utility function is the one on the left hand side of Figure 1.9, and useful data fusion is only possible when and only when the number of nodes participating in the sensing operation is at least as large as the threshold set by the function. This scenario characterizes applications where the user needs, for instance, the complete information of the environment where the WSN is deployed. If the user can not have the complete information, all the information is useless. In the second scenario the utility function is illustrated on the right hand side of Figure 1.9, where there is some freedom in tuning the number of

participating nodes in the sensing activity. The authors of [6] modeled the utility function of the second scenario as the one illustrated in the right hand side of Figure 1.9, but it may be modeled using other types of curves, since it will depend on the application in which the WSN works for.

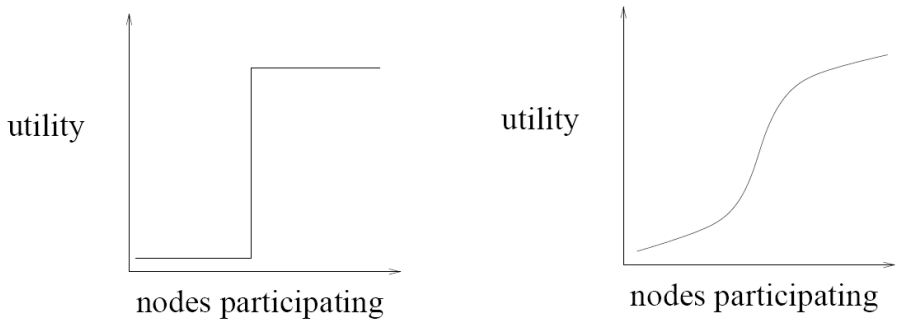


Figure 1.9: Utility functions described in [6].

Modeled the utility function, the authors propose an objective function that reflects a natural goal for the WSN, which is the maximization of the total aggregated utility of the network over time. The proposed objective function takes into account the costs incurred by each possible activity of the sensor nodes that were modeled, and has two constraints. First, the nodes can not consume more power than they have available and, second, the data collected from all nodes who get credit for participating in the sensing subset S at time t have to be routed to the sink node. This is only possible 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.

1.4.2 Data Communication

The use of utility functions was also used to design solutions for the routing problem in WSNs, particularly in the construction of a data collecting tree. When routing is done using a data collecting tree, an important issue is the construction of that tree. Each sensor node must decide locally which node will be its ancestor and the nodes that will be its descendants nodes in the tree. Different criteria can be used such as reliability, energy, and delay.

In [23], the authors apply techniques from Mechanism Design and Game Theory to facilitate the design of decentralized algorithms for constructing a data collecting tree that aims to optimize data gathering in sensor networks. They investigate the problem we are discuting in this section, proposing the design of suitable local utility functions such that each sensor node while "selfishly" optimizing its own local utility function leads to optimizing the desired global objective. They consider the problem of constructing a load balanced spanning tree rooted at the data sink in the network for continuous data gathering applications.

Basically, the algorithm is initiated with a flooding at the sink node. Each sensor node is marked then with a level, defined by its distance to the sink node. After this, a load balanced tree is built choosing an ancestor node of level i by its descendants of level $i+1$. For the solution of this problem, the authors consider an iterative game, in which an iteration is defined as a round in which parents in the collecting tree announce their bandwidth guarantees and the children decide on the parent they want to attach. The utility function of each sensor node dictates that at each iteration, a sensor node prefers to connect to a parent that gives it the maximum bandwidth guarantee, being selfish about the bandwidth guarantee it receives. The bandwidth offered by the ancestors varies as the descendants are being chosen. A descendant node may disconnect itself from an ancestor node in case it considers that the association to another ancestor is more beneficial to it. The process finishes when no descendant has the intention to connect to another ancestor node.

Besides distributing the data collection fairly among the sensor nodes, it is also crucial to the operability of a WSN that the routing solutions consider an even energy consumption among the nodes. When a group of sensor nodes run out of energy, the network will be led to partition, what reduces its lifetime and compromise its functioning. Thus, besides the load balanced data collecting tree, the authors of [23] also propose an algorithm to construct an energy balanced data collecting tree. They use the same strategy, which considers that each sensor node is selfish and has a local utility function that determines which is its parent in the tree. For the construction of this tree, the utility function considers the residual energy e_i of the sensor node and of the sensor nodes i in the subtree rooted at the sink node. Thus, the sensor nodes tends to route its data to the sink over the shortest path using $1/e_i$ as the edge lengthmetric, resulting in the desired energy balanced data aggregation tree.

In the same direction, the work of [28] propose a game theoretic energy balance routing algorithm to even the energy consumption among the sensor nodes. The players are the sensor nodes and their strategies are to relay or not an event packet toward the sink node. Every relay course is considered as a game and the payoff matrix of the nodes is illustrated in Figure 1.10. In this game, a node is playing against its neighbors, in a way that if it relay the message and some other neighbor also relay it, the ones that relayed the message receive a benefit of a, proportional to the number of nodes that relayed the message, and the ones that have not receive a benefit of $c = 0$. If the node relay the message and the other nodes do not, that is, be in silent, it receive a benefit of $b > a$ and other nodes receive a benefit of c. If all nodes did not relay the message, they receive a benefit of $d < 0$.

		other nodes relay	other nodes silent
node i	relay	$a, *$	b, c
	silent	$c, *$	d, d

Figure 1.10: Payoff matrix of the routing game described in [28].

To support the decision making of the sensor nodes, the authors of [28] define probabilities of a node relaying a message and be in silent. Also, they define a probability that all nodes be silent in a determined time. All of these probabilities are in function of the residual energy of the nodes, what is done to fairly distribute the energy consumption in relaying the messages among the sensor nodes. Moreover, in simulation results, it was shown that the proposed algorithm has desirable convergence and good performance.

The above solutions considers that energy management is the unique and primary objective in the construction of a data collecting routing algorithm. On the other side, we should consider that WSNs are being design to be deployed in hazardous and hostile environments in which they can fail to operate or be destroyed. In such scenarios it may exist applications for monitoring environmentally toxic situations, seismic activities in earthquakes or rubble zones, tsunamis and hurricanes or even enemy movement in military battlegrounds. To operate efficiently, such networks should consider other QoS metrics rather than long-term survability, that is guaranteed through energy economy. They should consider that the information they are routing is somewhat essential and/or time-critical and the sensor nodes should route them via the most reliable paths available.

This scenario was considered by [16], which the authors add another constraint to sensor nodes, beside the ones that imply that they have unreplenishable and limited energy resources and should make decisions without the assistance of a central authority. The authors also propose that a sensor node s_i can fail with a probability p_i, given the inhospitality of the environment it is inserted on.

Thus, in this scenario, the sensor nodes should route over the most reliable paths while minimizing their own energy consumption rather than some aggregate energy criterion. The authors claimed that this model of reliable energy-constrained routing has the advantage of allowing the nodes to choose their next hop in the path using only its local information, also choosing the hop that is cheap to it, saving its energy and prolonging its lifetime.

The game theoretic formulation was made in a way that the players of the routing game are the sensor nodes $S = \{s_1, ..., s_n\}$ and each sensor s_i has a information with value $v_i \in \Re^+$, that represents an abstract quantification of the value of the event sensed at node s_i, being 0 for nodes whose sensed information does not satisfy the specified attributes of the query. The data is routed to sink node s_q through an optimally chosen set $S' \subseteq S$ of intermediate nodes by forming neighbor communication links. The formation of links between node s_i and s_j is made rationally by each node, taking into account the reliability of the path from s_j and the cost in terms of energy $c_{i,j}$ of link i, j. Thus, the strategy of each node s_i is to choose locally to which node it will connect to propagate its message The payoff $\Pi_i(l)$ of sensor node s_i is a function of the strategy profile l, that is, the routing tree T formed in the network, and is given by:

$$\Pi_i(l) = \begin{cases} V_i R_i - c_{i,j} & \text{if } s_i \in T \\ 0 & \text{otherwise} \end{cases}$$

where R_i denotes the path reliability from s_i onwards to s_q and V_i denote the expected value of the data at node s_i given the set of its parents F_i, where $V_i = v_i + \sum_{j \in F_i} p_j V_j$. Thus, s_i gets information from its parents only if they survive with the given probabilities.

In Figure 1.11, take from [16], the payoff of node s_5 is $\Pi_5 = R_5(v_5 + p_1 v_1 + p_2 v_2) - c_{5,6}$.

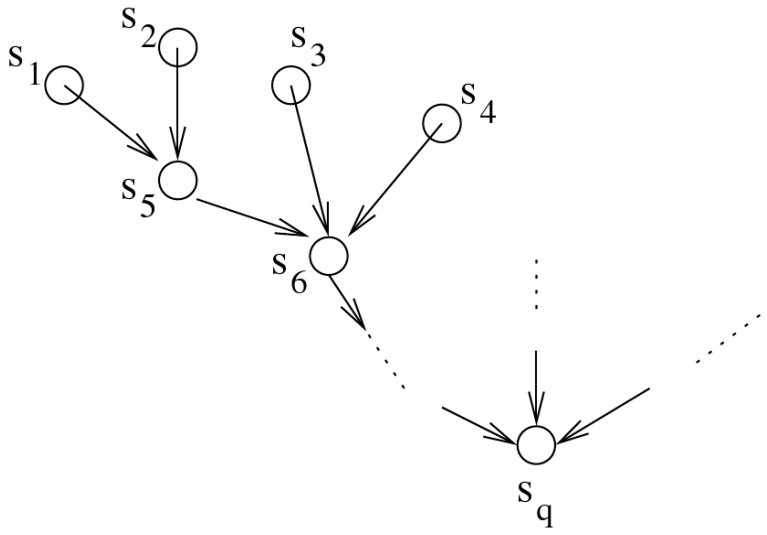


Figure 1.11: Abstract View of a Vehicular Area Network

Finally, the authors show that the Nash Equilibrium for this game is the tree generated when all nodes are playing its best response to the other nodes strategies, that is, every node is receiving its optimal payoff. However, finding the strategy that leads to the optimal payoff requires each node to determine the optimal tree formed by each of its possible successors on receiving its data, what the authors show to be NP-Hard. Thus, the authors propose a distributed algorithm in which the nodes compromise to maximize their least possible payoff rather than selecting a neighbor to maximize their individual payoffs. This solution was compared to other centralized solutions and given the proposed scenario it found reasonable good paths. Other results for this problem can be found in later similar work of these authors[12, 13, 15].

In routing game theory can also be used to define the cluster heads of hierarchical routing algorithms. Since the number of sensor nodes in WSNs can extend to large values such as hundreds of thousands, clustering is a grouping technique that pose as an efficient method to reduce the energy consumption. In this technique, a group of sensor nodes are grouped and among them a cluster head is selected. The cluster head is responsible to gather the information of all sensor nodes in its group and to forward the data in the direction of the sink node. One of the main challenges is to efficiently distribute the energy consumption

among the nodes in a group, since the energy expenditure at the cluster head is significantly higher. Thus, game theory is used to solve the conflict of selecting the cluster head, since no node, if selfish, would naturally declare itself as the one.

In [17], the authors refer to the problem of choosing a single clusterhead among the population of N nodes from a game theoretic point of view. A clustering game $CG =< I, S, U >$ is defined, where I is the set of players, $S = \{S_i\}$ is the set of the available strategies and $U = \{U_i\}$ is the set of utility functions for each node. The players are the sensor nodes and they have two possible pure strategies $\{D, ND\}$: to declare (D) itself as clusterhead or not (ND).

The payoff of the players is again modeled considering the abstract value v of the data that should be transmitted to the sink and the costs involved in this transmission. Thus, if a player declares itself as clusterhead its payoff is $c - v$, where v is the abstract value for successfully delivering the data with value v and c is the cost of becoming a clusterhead, that involves all the energy consumption incurred to this role, such as the reception of all the data collected by the sensor nodes of its group and the transmission of this data to the sink, for instance. If a player does not declare itself a clusterhead and no other node becomes a clusterhead either, its payoff will be 0, as the player will be unable to sent its data toward the sink. On the other hand, if at least one node from its group declares itself as clusterhead, then its payoff will be solely v, that is the highest possible for this game.

For the two-player clustering game, the payoff matrix is illustrated in Figure 1.12. In this two-player symmetric game, the symmetrical strategies (D, D) and (ND, ND) are not Nash Equilibrium strategies, since, in the first one, a player can improve its payoff by changing its strategy to ND and, in the second one, a player does it by changing its strategy to D. Thus, the Nash Equilibrium strategies of this game are all assymetrical, the (D, ND) and (ND, D) strategies.

		s_2	
		D	ND
s_1	D	$v - c, v - c$	$v - c, v$
	ND	$v, v - c$	$0, 0$

Figure 1.12: Payoff matrix of the two-player clustering game.

In the N player clustering game, the results are basically the same, where no symmetric pure strategies Nash Equilibria exist. The unique Nash Equilibrium is the assymetrical strategy profile which all players play ND and only one plays D. Because there is no symmetrical equilibrium in this game, the payoff of the nodes is unbalanced, what causes an unfairly energy consumption among the nodes and, consequently, an early depletion of the network operability. In order to solve this problem, the authors of [17] allow the players to play mixed strategies, i.e., players chose their strategies randomly following a probability distribution. In this case, every player plays D with probability p and plays ND with probability $1 - p$. In this game, the authors show that exists a mixed strategies Nash Equilibrium if the players play:

$$p = 1 - \frac{c}{v}^{1/(N-1)}$$

From the above described games and results, the authors of [17] develop a more realistic energy consumption model and, by it, propose and evaluate an algorithm to select the clusterhead of a group of sensor nodes. They compare the proposed algorithm with the well known LEACH protocol [10] and the proposed method achieves higher network lifetime values for most of the evaluated cases.

1.4.3 Cross-Layer Optimization

While general-purpose networks are designed to support a wide variety of applications, WSNs are particular ad hoc networks that are designed for specific applications with specific constraints. Because of this, in WSNs is it possible to escape from the strict boundaries concept of network layers from the OSI model and, therefore, to allow communication between layers to optimize a network functionality, a method that is called Cross-Layer Design. Moreover, a Cross-Layer Design is particularly important for any network using wireless technologies, since the state of the physical medium can significantly change over time [5, 19].

In WSNs, the application layer is responsible to estimate the underlying physical phenomenon as accurately as possible while the other layers operate under the network resource limitation. Thus, in [27], the authors formulate a network optimization problem, in which the objective is to the minimize the overall distortion at the application layer considering the resource constraints of WSNs. The authors formulate a source coding game at the application layer and a power control game at the physical layer, both implemented in a distributed fashion.

In the power control game, the players are the communication links formed by the sensor nodes and their strategies are to increase or decrease their powers. The main problem of the power control game is the transmission interference among nearby sensors. In order to intelligently avoid interference, the authors introduce a tax mechanism in which the higher the power a link uses, more interference it will produce to others and more tax it has to pay. With this it was modeled a payoff function for each link player maximize and it was proved that at a certain defined condition, the game is ensured to converge to a unique and stable Nash equilibrium.

On the application layer, the source coding game characterizes the interaction among sensor rates and estimation distortion. The underlying physical phenomenon is denoted as θ, which is a vector of M independent random variables. Then, each sensor node i deployed in the field make a local observation θ_j of θ, being corrupted by independent observation noise n_i. The observation channel is characterized by a matrix H. At each sensor i, the noisy observation y_i, that is a result of n_i over θ_j, is quantized into a codeword u_i. The quantized information from all sensors is transmitted through the network to the sink node (in [27], the authors refer to the remote central office - CEO) with source rates $(s_1, ..., s_N)$. At the sink node, the decoder first jointly decodes the codewords u, then estimates the source $\hat{\theta}$. Thus, the performance criterion is to minimize the mean squared error $D(\hat{\theta}, \theta) = \left\|\hat{\theta} - \theta\right\|^2$ considering that smaller distortions came from higher source rates, which implies higher energy consumptions. In order to control this, the authors introduce a payoff function with a price mechanism such that it is easy for nodes to make a good tradeoff between energy consumption and distortion in a distributed manner, reaching, at a defined condition, an unique and stable Nash equilibrium.

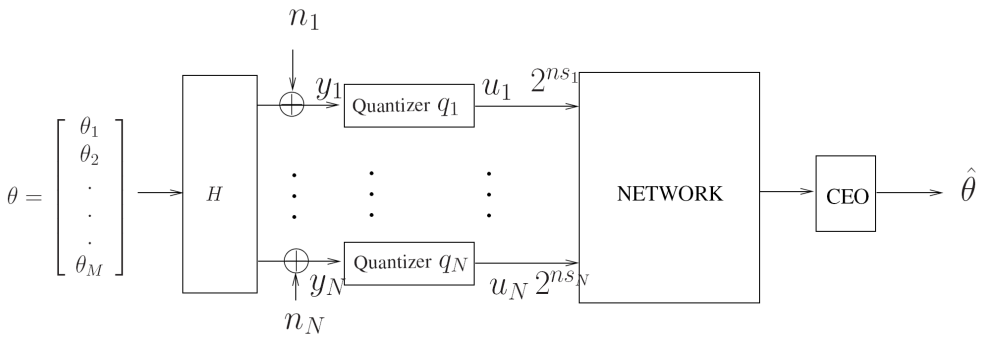


Figure 1.13: Distributed source coding [27]

For both power control game and source coding game the authors propose distributed algorithms. Then, they present a distributed primal-dual algorithm which iteratively executes these algorithms and updates shadow prices. This cross-layer design, incorporated with game theoretic concepts, allowed the overall network optimization problem to be solved approximately and in a distributed manner, which is fundamental for WSNs.

1.4.4 Power Management

In WSNs, due to the severe energy constraints of the sensor nodes, they are encouraged to turn off their parts that are not needed. They can turn of their radio transmitter and receiver, and also their sensor devices. In [11], Hill et al. state that a WSN should embrace the philosophy of getting the work done as quick as possible and going to sleep, in order to save the network energy and extend its lifetime. The problem is the trade-off that exists between the energy saving and the operability of the network. An efficient power management design for WSNs should save the energy resources of the sensor nodes without compromising the network operability.

In this direction, in [24], Niyato et al. proposed a game-theoretic approach to optimal energy management in WSNs. Basically, while the sensor nodes radio is turned on, the data is relayed more efficiently but the energy consumption is higher. On the other hand, if the sensor nodes spend too much time in sleep mode, they will probably miss several and important data communication that is essential to the network and end-user, but will save

their energies. They define three states of node operation: *active*, *listen*, and *sleep*. In active mode, the sensor node can receive and transmit packets. In listen mode, the transmitter circuitry is turned off, making the node not able to transmit packets. In sleep mode, both the receiver and transmitter are turned off.

The authors of [24] propose a bargaining game to obtain the equilibrium strategy for the energy saving mechanism at a tagged sensor node and the other nodes that are relaying packets to this tagged node, in a way that all be satisfied with the perceived QoS performance. The players of this game are two, the first one is the *entity* that governs arrival of packets at the queue of the sensor node and the second one is the sensor node itself. The arrival of packets at the sensor nodes comes from other sensor nodes that are relaying their packets and from the sensor device within the tagged node. The strategy for the first player is to select the wake up probability $P_{active,sleep}$ when the sensor node is in sleep mode. The strategy for the second player is to select the wake up probability $P_{active,listen}$ when the sensor node is in listen mode. The time a sensor node is in sleep mode defines a packet blocking probability P_{block} that an incoming packet is blocked and the time a sensor node is in listen mode defines a packet dropping probability P_drop that a received/generated packet is dropped due to lack of buffer space, making the energy used in receiving/generating this packet to be wasted. These probabilities define the payoff of both players, in a way that the payoff of the first player $U_1 = 1 - P_{block}$ and the payoff of the second player $U_2 = 1 - P_{drop}$.

In this two-person bargaining game, the players try to come to an agreement on trading/sharing a limited amount of resource, cooperating to gain a higher benefit than that they could have obtained by playing the game without cooperation. While the first player wants that the second player to be active and to receive the incoming packets, the second player wants to save its energy and be in a sleep state. On the other hand, the second player wants the first player to transmit its packets that are in the buffer, but the first player wants to transmit only when the second player is in the listen mode. Then, both players change their strategies in the direction of making an agreement. If an agreement between both players cannot be reached, the utility they receive is 0. Based on the Nash equilibrium, the optimal values of the $P_{active,sleep}$ and $P_{active,listen}$ probabilities can be obtained so that the throughput of a sensor node is maximized while the power supply constraint is met.

Another important concern in an efficient power management in WSNs is whether the sensor nodes should keep their sensor devices on or off. Considering that they have a radius of sensor coverage, if a large region is being covered by several sensor nodes, probably one or more of them should turn of their sensor devices in order to save their energies.

In this direction, Campos-Nañes et al. [7] proposed a game theoretic distributed scheme to efficiently manage the sensory coverage in WSNs. It was modeled a game in which the players are the n sensor nodes of the network and a player i strategy $a_i \in \{0, 1\}$ is to define whether its sensor device is on ($a_i = 1$) or off ($a_i = 0$). The authors also define a coverage function based on the network operational configuration $a = a_1, ..., a_n$:

$$K(a) = \sum i = 1^n 1_i a$$

where

$$1_i a \quad = \quad \begin{cases} 1 & \text{if sensor } i \text{ is covered under action profile } a \\ 0 & \text{otherwise} \end{cases}$$

and a sensor is considered covered if all points within its sensing radius are covered by the sensor itself or by other active sensors. In order to quantify the trade-off between energy usage and sensing coverage of the network, the authors modeled a payoff function that is common to all sensor nodes:

$$U(a) = K(a) - c \sum i = 1^n a_i$$

where c is the cost of maintaining a sensor device on. This payoff function measures how

effective is being the management of the sensory coverage of the network and an optimal sensor coverage configuration is given by the solution of

$$\max_{a \in A}\{U(a)\}, A = \{0,1\}^n$$

The solution of this problem can be solved in a centralized and off-line mode for reasonable sized instances of n, but since scalability is a major concern in WSNs, the authors of [7] propose a distributed online algorithm that finds suboptimal solutions and converges to a Nash equilibrium state. The authors also showed good experimental performance results on a *MicaZ* testbed and on large-scale topologies.

1.5 Open Issues

References

[1] A. Agah, S.K. Das, and K. Basu. A game theory based approach for security in wireless sensor networks. pages 259–263, 2004.

[2] Afrand Agah, Mehran Asadi, and Sajal K. Das. Prevention of dos attack in sensor networks using repeated game theory. In Hamid R. Arabnia, editor, *ICWN*, pages 29–36. CSREA Press, 2006.

[3] Afrand Agah, Sajal K. Das, Kalyan Basu, and Mehran Asadi. Intrusion detection in sensor networks: A non-cooperative game approach. In *NCA*, pages 343–346. IEEE Computer Society, 2004.

[4] T. Alpcan and T. Basar. A game theoretic analysis of intrusion detection in access control systems. volume 2, pages 1568–1573 Vol.2, Dec. 2004.

[5] Frank Aune. Cross-layer design tutorial. Published under Creative Commons License., November 2004.

[6] John Byers and Gabriel Nasser. Utility-based decision-making in wireless sensor networks. In *MobiHoc '00: Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing*, pages 143–144, Piscataway, NJ, USA, 2000. IEEE Press.

[7] Enrique Campos-Naòez, Alfredo Garcia, and Chenyang Li. A game-theoretic approach to efficient power management in sensor networks. *Oper. Res.*, 56(3):552–561, 2008.

[8] Garth V. Crosby and Niki Pissinou. Evolution of cooperation in multi-class wireless sensor networks. *Local Computer Networks, Annual IEEE Conference on*, 0:489–495, 2007.

[9] M. Felegyhazi, L. Buttyan, and J. P. Hubaux. Cooperative packet forwarding in multi-domain sensor networks. In *Proceedings of IEEE PerSeNS 2005*, Hawaii, USA, March 2005.

[10] Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan. Energy-efficient communication protocol for wireless microsensor networks. In *HICSS '00: Proceedings of the 33rd Hawaii International Conference on System Sciences-Volume 8*, page 8020, Washington, DC, USA, 2000. IEEE Computer Society.

[11] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister. System architecture directions for networked sensors. In *Proceedings of the 9th International Conference on Architectural Support for Programming Languages and Operating Systems*, November

2000.

[12] R. Kannan and S. S. Iyengar. Game-theoretic models for reliable path-length and energy-constrained routing with data aggregation in wireless sensor networks. *IEEE Journal on Selected Areas in Communications*, 22(6):1141–1150, 2004.

[13] Rajgopal Kannan, Lydia Ray, Ram Kalidindi, and S. S. Iyengar. Max-min length-energy-constrained routing in wireless sensor networks. In *in Proc. 1st European Workshop Wireless Sensor Networks*, 2004.

[14] Rajgopal Kannan, Sudipta Sarangi, and S. Sitharama Iyengar. Sensor-centric energy-constrained reliable query routing for wireless sensor networks. *J. Parallel Distrib. Comput.*, 64(7):839–852, 2004.

[15] Rajgopal Kannan, Sudipta Sarangi, and S. Sitharama Iyengar. Sensor-centric energy-constrained reliable query routing for wireless sensor networks. *J. Parallel Distrib. Comput.*, 64(7):839–852, 2004.

[16] Rajgopal Kannan, Sudipta Sarangi, S.S. Iyengar, and Lydia Ray. Sensor-centric quality of routing in sensor networks. *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE*, 1:692–701 vol.1, March-3 April 2003.

[17] Georgios Koltsidas and Fotini-Niovi Pavlidou. Towards a game theoretic formulation of clustering routing in wireless sensor networks. In *ValueTools '08: Proceedings of the 3rd International Conference on Performance Evaluation Methodologies and Tools*, pages 1–9, ICST, Brussels, Belgium, Belgium, 2008. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[18] M. Li, I. Koutsopoulos, and R. Poovendran. Optimal jamming attacks and network defense policies in wireless sensor networks. In *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, pages 1307–1315, 2007.

[19] X. Lin, N. B. Shroff, and R. Srikant. A tutorial on cross-layer optimization in wireless networks. *Selected Areas in Communications, IEEE Journal on*, 24(8):1452–1463, 2006.

[20] Jonathan M. McCune, Elaine Shi, Adrian Perrig, and Michael K. Reiter. Detection of denial-of-message attacks on sensor network broadcasts. In *SP '05: Proceedings of the 2005 IEEE Symposium on Security and Privacy*, pages 64–78, Washington, DC, USA, 2005. IEEE Computer Society.

[21] David A. Miller, Sameer Tilak, and Tony Fountain. "token" equilibria in sensor networks with multiple sponsors. In *CollaborateCom*. IEEE, 2005.

[22] Wei Shu Min-You Wu. Intersensornet: strategic routing and aggregation. In *IEEE Global Telecommunications Conference - GLOBECOM '05*, 2005.

[23] M. Singh N. Sadagopan and B. Krishnamachari. Decentralized utility based sensor network design. In *Mobile Networks and Applications Journal (MONET), to appear*. ACM/Kluwer, 2005.

[24] D. Niyato, E. Hossain, M.M. Rashid, and V.K. Bhargava. Wireless sensor networks with energy harvesting technologies: a game-theoretic approach to optimal energy management. volume 14, pages 90–96, August 2007.

[25] G.J. Pottie and W.J. Kaiser. Embedding the internet wireless integrated network sensors. In *Communications of the ACM*, volume 43, pages 51–58, may 2000.

[26] Pedro O.S. Vaz de Melo, Felipe D. da Cunha, Jussara M. Almeida, Antonio A.F. Loureiro, and Raquel A.F. Mini. The problem of cooperation among different wireless sensor networks. In *MSWiM '08: Proceedings of the 11th international symposium on Modeling, analysis and simulation of wireless and mobile systems*, pages 86–91, New York, NY, USA, 2008. ACM.

[27] Jun Yuan and Wei Yu. Wsn11-1: Distributed cross-layer optimization of wireless sensor networks: A game theoretic approach. pages 1–5, 27 2006-Dec. 1 2006.

[28] Jia Zeng, Chundi Mu, and Min Jiang. Game theoretic distributed energy control in sensor networks. In *CIT '07: Proceedings of the 7th IEEE International Conference on Computer and Information Technology*, pages 1015–1019, Washington, DC, USA, 2007. IEEE Computer Society.