SEVENTH FRAMEWORK PROGRAMME
THEME 3
Information and Communication Technologies

Grant agreement for:
Collaborative project, Small and medium-scale focused research project (STREP)

Deliverable D3.2:

Set of Schemes for Adapting to the Dynamic Environment

Project acronym: FRONTS
Project full title: Foundations of Adaptive Networked Societies of Tiny Artefacts
Grant agreement no.: 215270

Responsible Partner: UPB
Report Preparation Date: Friday, 12 February 2010

Contents

1 Introduction

In this workpackage of the FRONTS project we are dealing with societies of tiny artefacts that are deployed to changing environments. Therefore they have to dynamically adapt their structures as well as the tasks and roles assigned to their sensors. All this has to be done in an energy efficient way, and has to be robust against faults and attacks.

In the first year, we have defined research goals and described first results for several tasks in this context as presented in deliverable D3.1. Following this line of research, in the second year we developed a set of schemes for adapting to the dynamic environment, which are presented in this document. We shortly review the motivation for each scheme, state the scheme explicitly, give an overview over relevant work for the schemes within the FRONTS project, and conclude with future work for the third year of FRONTS. For an overview of all papers we refer to the technical report series on the FRONTS web page.

This deliverable is structured according to four major functionalities we have to provide in order to adapt to a dynamically changing environment. For each functionality we contribute schemes. The first functionality we care for is to maintain desirable network properties in a changing environment which might modify the topology of the system of sensors by various influences, e.g., by moving them (wind, currents, active movements of the entities (animals, humans) the sensors are attached to) or by changing their connectivity. We contribute schemes for maintaining clusterings and communication infrastructures in such settings. The second functionality is to guarantee a high degree of robustness against faults and attacks, a severe problem especially in a changing environment. We contribute schemes for coping with sybil attacks and for maintaining reliable communication. The third functionality we address is energy-awareness, a crucial requirement for battery-operated systems. Our contributed schemes consider several aspects like duty-cycling, (i.e., designing strategies that let the system function but letting the sensor be in a sleep mode as often as possible), monitoring objects and disseminating information about them in an energy-efficient way, and energy-aware data transmission. Finally we care for techniques for assigning tasks and roles to sensor nodes. We design schemes that do this in a self-organizing way, a crucial requirement in a changing environment where new situations have to been coped with. Our schemes address scheduling problems and dynamic role assignments.

A good overview of the interaction of the work done in this work package can be found in [BBDC+10]. Here we present a unifying framework where sensors have to perform a task in a changing environment: We consider a scenario where sensors are deployed in order to monitor a population of lizards on a remote island. Especially, we show how the research from Workpackage 3 can be applied in this scenario. Ex-

SCHEMES	TASK
Functionality A: Desirable network properties	
Scheme 1: Maintaining global clusterings	Task 3.1
Scheme 2: Building and maintaining communication infrastructures	Task 3.3
Functionality B: Robustness against faults and attacks	
Scheme 3: Coping with sybil attacks	Task 3.4
Scheme 4: Maintaining reliable communication	Task 3.5
Functionality C: Energy-awareness	
Scheme 5: Self-synchronized duty-cycling and minimum energy multi-casting	Task 3.1
Scheme 6: Monitoring objects and disseminating the gained data	Task 3.2
Scheme 7: Energy-aware transmission policies	Task 3.4
Functionality D: Task- and role-assignment	
Scheme 8: Scheduling selfish distributed computation	Task 3.1
Scheme 9: Assigning roles	Task 3.3

Table 1: Assignment of schemes to WP3 tasks

amples of tasks in this context are tracking the lizards, disseminating information in the network and monitoring eggs.

2 Maintaining global clusterings

2.1 Motivation and problem description

Many applications running on top of a network require that the network is structured in some way. A basic network structure consists of grouping some sensor nodes together and to consider the network as composed of groups of sensors. For instance, an energy aware hierarchical routing strategy, like LEACH, selects a node per group as the leader. The leader is responsible for establishing communication with nodes belonging to others groups. By periodically changing the group leaders, the energy consumption is balanced between the nodes. Generally, in order to build high-level applications, group service communication provides basic building blocks.

The motivation to consider the interacting urn process is to group the nodes of a network together by using a distributed algorithm based on direct communications between the nodes and not requiring global computations. The aim is to group the nodes that can communicate directly or limit the number of hops between the nodes belonging to the same group.

Incidentally, we notice that the interacting urn process collects global information on the network structure, and that it is possible to adapt the process to compute virtual coordinates.

2.2 Scheme description

We give two applications of the interacting urn process to network clustering and sensor localization. With the interacting urn process, the sensors estimate an entry of

the generalized eigenvector. We propose to cluster neighboring sensors that estimate close values. The heuristic that supports the clustering comes from spectral graph drawing theory. Indeed, the values estimated by the sensors are used as a coordinate to draw the graph efficiently. What we propose amounts to cluster neighboring sensors that are drawn closely.

We use the interacting urn process to compute pseudo-coordinates by requiring that the sensors manage two urns and such that anchors manage their urn in a deterministic way. The heuristic comes again from spectral graph drawing theory as well as classical strategies proposed to compute pseudo-coordinates in sensor networks. Indeed, we show that the pseudo-coordinates that we obtain are similar to the one we obtain by computing pseudo-coordinates such that the coordinate of a sensor is the barycentric coordinate of the neighboring sensors.

2.3 Related FRONTS Technical Reports

- FRONTS-TR-2009-62 [LS09]. This technical report contains substantial improvements of [LS08]. We devise a new proof of the convergence of the interacting urn process and we propose a full description of the implementation issues. The aim is to devise a self-stable algorithm to get some knowledge about the global network structure.

2.4 Outlook

We plan to consider the general problem where two sensors desire to exchange data regularly (streaming). In this setting, balancing the energy consumption among all sensors is no longer desirable, but we plan to investigate what is the appropriate criterion in this setting. Another formulation of the problem is that we plan to include energy awareness in multi-paths forwarding protocols.

3 Building and maintaining communication infrastructures

3.1 Motivation and problem description

We want to use mobile sensors to connect stations in the plane by a communication infrastructure consisting of mobile nodes. In order to save energy and mobile nodes, the connecting structure should be as short as possible. In a geometric setting, a natural constraint is that the nodes only have information about their immediate surrounding. Based on this information, the nodes should move in such a way that globally the connection is not lost and the total distance of the communication infrastructure is minimized.

3.2 Scheme description

In a sensor network, it is crucial to have a short communication infrastructure. We consider a setting in a geometric plane with m stations and n memoryless mobile sensor nodes with a bounded view and a connected unit disc graph. In each round, each sensor is allowed to sense its environment, compute a new position and move there. Optionally, sensors can also direct their neighbors to a new position. The goal is to reach a short communication infrastructure between the stations. In [DKMadH10], we consider a simplified version of the problem without stations. The goal is to gather n mobile sensor nodes with a limited viewing radius in one point. We propose an algorithm for the sensors and prove that the expected time to gather them is quadratic in the number of sensors. This problem was considered before in the literature, mostly in settings with global view, but no algorithms with a limited view and runtime bounds were known before.

3.3 Related FRONTS Technical Reports

- FRONTS-TR-2010-8 [DKMadH10]. We introduce a local and distributed algorithm which gathers a group of mobile sensor nodes in one point and we show that it runs in expected time $O(n^2)$, where n is the number of sensors.

Related first year FRONTS Technical Reports

- FRONTS-TR-2008-14 [MS08].
- FRONTS-TR-2009-5 [KM09].

3.4 Outlook

For our communication networks, we want to investigate whether there exist faster algorithms for the general setting. Moreover, some abilities of the sensors might not be necessary. We want to find out which of the abilities are crucial and which can be neglected.

4 Coping with sybil attacks

4.1 Motivation and problem description

One of the key concepts for sensor network security and integrity is a single node's identity. All devices in such a system are assigned an identifier, used for attributing certain datasets, behaviors or commands to a specific entity. Attaching identity information to messages sent through the network has a significant influence on completeness and reliability of the sensor network.

Sybil attacks, i.e., cloning and forging identities, are a common problem arising when dealing with systems and algorithms which use a node's identity. The possibility of cloning honest sensors gives the attacker an opportunity to explore the network and take part in the execution of some algorithms. The leader election in a sensor network is the classical example of an algorithm that is sensitive to node forging. Affecting the output of this algorithm may have a crucial meaning for the security of whole sensor network.

By their nature, sybil attacks are hard to discover, since the malicious nodes physically differ in no way from the legitimate ones. The only distinguishing factor is their behavior, and as such it needs to be carefully examined. This can be easily done if the network is globally supervised and all information (i.e., routing tables of each node, neighborhood lists, etc.) can be compared by a single entity. This however brings the problem of overhead communication and storage and its costs are prohibitive in small sensor scenarios. Another approach is to employ distributed algorithms and use emergent cooperation of nodes. In the two following algorithms we tackle the problem of multiple malicious nodes operating legally in the network using the latter approach: the gain is that inherent resistivity of the network to abuse is achieved at relatively low communication and energetic cost.

4.2 Scheme description

We focus on two concepts of trust. The first concept is presented in the light of robustness to external or internal attack, that is we show that trust may be an inherent property of a network even in the presence of an adversary. The adversary's goal is to use the network, not to block it. Therefore, the generic techniques used by the adversary is to mimic good behavior but cheat other network nodes about existing conditions. In particular, we consider a single hop network model with an adversary who captured a couple of devices, compromised them and is trying to emulate more nodes that he actually captured (Sybil attack). So in fact we explicitly admit that some number of the nodes are under control of the adversary.

Since solving the above mentioned problems is not possible in the purely algorithmic way, we retreat to technical features and capabilities of enforcing trust. Trustful performance must be a consequence of mixed properties of the algorithmic scheme and practical limitations of the malicious party. One of the techniques is blocking some activities entirely, if certain nodes (called allowers) are present and active. This solution is quite opposite to the standard approach in which each device on its own has to determine working conditions and take decisions of its own.

The second concept is that of mutual cooperation of devices in the network to pick out malicious users and spread the knowledge about them in an energy-effective way. In [GKKZ09] we consider an ad-hoc network of users that can connect to information servers to receive some service (e.g., Internet access). The sybil attack in this setting

is an unauthorized access to many of these servers in a short period of time by a network user with the same ID. We assume that there may be potentially many such clones interested in exploiting the information servers; we call them *heavy hitters*.

The algorithm we propose assumes that each server stores a list of users that have recently accessed it in a given period of time. Since the lists can be long, we devise a three-phase fully distributed algorithm for finding the most frequent entries among all the servers. We show that, with high probability, the resulting intersection of lists contains all heavy hitters. This is achieved with communication overhead of order $\mathcal{O}(m)$, where m is the length of the access lists stored in information servers.

4.3 Related FRONTS Technical Reports

- FRONTS-TR-2009-6 [BGKM09]. We provide a security mechanism for passive devices guarding their activation in non-trustful environments. Since passive devices are unable to determine the working conditions, this task is shifted to more powerful nodes called *allowers*. We propose an algorithmic scheme in which the simple devices can respond only in the presence of allowers.

- FRONTS-TR-2009-7 [GKKK09a]. The paper addresses the question of technical details of conflict resolution for wireless communication in ad hoc setting. A leader election scheme which is usually executed consists of a number of trials; each of them fails with a constant probability. In order to control the energy usage by each station, it has been proposed before to use a kind of dependent trial. Asymptotically this does not change the behavior of the algorithm. For practical values, however, this is not true. The paper examines these effects closely and yields some engineering rules.

- FRONTS-TR-2009-38 [GKKK09b] We address the question of unfair competition for a radio channel in ad hoc systems. Since the capacity of the wireless channel is limited, it is inevitable that some "smart" artefacts may try to gain more transmission time by unfair behavior in the conflict resolution protocols. The easiest way is to emulate many units. The paper, considering leader election algorithm as an example, shows how to deal with this problem in an algorithmic way using some physical limitations of the communication equipment – it is shown that if a device cannot listen and transmit at the same time it is possible to construct a scheme that leads to detection of frauds and elimination of single compromised station that use multiple identities (Sybil attack) to gain some advantage.

- FRONTS-TR-2009-39 [GKKZ09]. We propose an efficient method for detecting unfair use of resources in a distributed network. In particular, it offers detection of large scale cloning of artefacts without building a global database, thus pre-

venting privacy violation. The core of the algorithm is a scheme for determining intersection of two sets held by two nodes without revealing the sets.

4.4 Outlook

The scheme presented in [GKKK09b] – a countermeasure against multiple identities attack – will be extended to the case where certain nodes cooperate against the rest of the network. The goal is to develop mechanisms that eliminate these nodes as untrusted. As the scheme solving this problem has to trade off the probability of exposing duplicated nodes for complexity of the procedure, careful design decisions are necessary.

The results regarding access to the shared radio channel are to be extended to fine optimization for the case of a small number of nodes and sophisticated strategies that admit an arbitrary probability distribution over deterministic strategies. So far the fault model assumed that the faults have global character: either all stations in the range can receive a signal or none of them. In practice, the situation might be different and non careful design of network algorithms may lead to a lack of common view of the protocol participants and malfunction of the system. Protocols immune to this kind of faults are to be developed. Similar considerations have to be applied for the case of broadcast services.

The scheme for heavy hitters discovery can be further extended to include geographic localization of information servers into the process of selecting malicious users. In fact, if two relatively distant servers discover that the same ID has accessed them within the same time period, no further confirmation from other intermediate servers is needed to classify this ID as heavy hitter. This quick decision making can save communication overhead as well as increase global network's resistance to sybil attacks at distant regions.

5 Maintaining reliable communication

5.1 Motivation and problem description

One of the main issues in emerging pervasive systems is assuring robust mechanisms of communication as this lays foundations for any other cooperation protocols. The network can be corrupted by unfair or adversarial activities or simply technical problems. Therefore, building trust between communicating parties and introducing security-oriented techniques remains a serious aspect.

There is a growing awareness of the problem of unreliability of communication. This concerns technical problems as well as malicious or selfish behavior. A good example of a such recent work is [DMP09]. Even though many solutions for security and trust building have been proposed, it is a challenging problem to review and re-

design these proposals with network unreliability in mind as key factor influencing its standard operation.

5.2 Scheme description

In the previous years we investigated an *alarm problem* and robust and secure message passing on a multi-hop path. These two ideas smoothly merge into one scheme wherein an event is sensed by a number of sensors and a notification (alarm) of this event is propagated through the network to a base station. The problem we need to face is that the number of nodes that sense the event (e.g., a fire) is unknown, and yet can be large enough that when the nodes start transmitting their report, it will get jammed due to mutual radio interference. On the other hand, we want to assure that paths along which the report propagates are secured against an adversary who can capture nodes en route hence breaking the chain of information.

For alarm reporting ([CZ09]) we assume that in a network of n stations, m of them sense the event, and we split the time into m slots. Each station can decide to send its message in any of the m timeslots. In a standard approach, the station chooses each slot independently of others. However, we have investigated more general strategies where a station chooses with some probability $k < m$ slots in which to transfer. Noticeably, for $k = 2$ the optimal probability is uniform $= \frac{1}{2}$, but it changes for k greater than 2. We have also shown that there is a strategy wherein a given station *does not* send its report and it still raises the probability of informing the base station. These analyses were done numerically, but increasing k, m, n drastically increases complexity, so it becomes unfeasible with bigger k to identify the optimal strategy.

In the transmission model ([KKK09]), we organize the network into layers and messages are routed on layer-to-layer basis. We assume that messages are transmitted not along one path, but we devised an algorithm where each message is split in two independent parts at each relaying node. These parts are sent along their own routes. Therefore, in order to capture a message, the adversary would have to identify two transmitting nodes in a given layer. The problem of establishing routes in such a setting can be nicely reduced to a balls-and-bins problem with one condition, that two balls are thrown at the same time to two different bins. Numerical analysis showed that for a random selection of bins (transmitting nodes in a single layer) it is difficult to identify a node that is likely to transmit with probability greater than $1/t$, where t is the number of nodes in the layer. It means that, by analyzing radio traffic, the adversary gains no advantage in breaking into datastream.

5.3 Related FRONTS Technical Reports

- FRONTS-TR-2009-68 [CZ09]. We develop algorithms for propagation of alarm messages in a sensor network for the situations with a high rate of faults. Im-

munity against faults is the main requirement for many applications where the essential issue is to maintain network operation during heavy conditions.

- FRONTS-TR-2009-67 [KKK09]. We propose a routing architecture that is immune against an adversary that may break into single nodes in an uncontrolled environment. The scheme is based on double paths and dynamic, autonomous rebuilding of the paths. So the path can be trusted to some degree even if an adversary can capture a certain number of devices and control them.

Related first year FRONTS Technical Reports

- FRONTS-TR-2008-29 [CKZ08].

5.4 Outlook

To provide a concise description of the scheme and the protocols it is using, we need to establish mathematical models and present proofs for their applicability. In the alarm problem case, the numerical experiments have revealed some very interesting properties of the probability distributions, that, if proven to be universal, can limit the searchspace logarithmically. Further research in the area of multi-path routing will focus on getting some real-world data to be contrasted with experimental ones. Based on this we need to specify the most efficient (in terms of energy and security) algorithm for switching the transmission load between nodes in the same layer.

As a result, we should be able to provide a full description of solutions to be utilized in the event sensing scheme. We foresee it to be robust to single node capture and transmission efficient in terms of reporting alarms.

6 Self-synchronized duty-cycling and minimum energy multi-casting

6.1 Motivation and problem description

The nodes in mobile sensor networks are generally equipped with batteries. This makes energy a scarce resource, and different means of distributed cooperation can be employed for energy saving. One of them is known as *duty-cycling*. Hereby, sensor nodes alternate between (at least) two states: being awake and being asleep. When being awake they can perform their normal duties such as, for example, monitoring the environment, processing and sending data, etc. When sleeping, sensors spend their time in a state that is characterized by low energy consumption. It is generally important that the sensor nodes synchronize their activity periods. Another aspect concerns the harvesting of energy from the environment. Increasingly many sensor network deployments use harvested environmental energy to extend the system lifetime. However, energy sources such as the sun are quite variable due to changing weather conditions.

A related fundamental problem in sensor networks arises when one node is required to transmit data to a subset of the other network nodes. This scenario is known as multi-casting. Again, an important requirement when realizing a multicast request is spending as little energy as possible. This problem is known as the minimum energy multi-cast (MEM) problem. Solving this problem can be seen as a form of distributed cooperation between the sensor nodes.

6.2 Scheme description

Concerning the self-synchronized duty-cycling, we consider a setting in the Euclidean plane with static or mobile sensor nodes. Sensor nodes are equipped with omni-directional antennas. In the case of mobile networks we use the random way point model as the mobility model. Finally, we consider sensor nodes which are equipped with tools for harvesting energy in the form of sun light. The focus is on the development of mechanisms that allow sensor networks to function in a self-organized way. In this framework we proposed a protocol for static network topologies, analyzing it in two different network topologies: in the first topology the sensor nodes form a grid, in the second they are distributed randomly in the same area. In addition, we considered networks with different numbers of sensors. We then simulated an adapted protocol in the scenario with mobile sensors. This protocol is also able to deal with asynchronized clocks: instead of exchanging information at the same time, sensor nodes wake up periodically based on their own internal clock and perform an update of their internal state based on the information received by their neighbors. Finally, it includes a mechanism to deal with varying weather conditions.

The framework for the minimum energy multi-casting problem is similar to the one for duty-cycling. A difference is that we consider directional instead of omni-directional antennas here (note that omni-directional antennas are a special case of directional antennas). Again, the focus is to develop mechanisms which let the sensor networks function in a self-organized way.

6.3 Related FRONTS Technical Reports

- FRONTS-TR-2009-53 [HB09c]. We investigated the self-synchronized duty-cycling mechanism initially proposed in [HBM$^+$09] for static networks. We studied two different static network topologies: a grid and randomly distributed sensors. In order to study the statistical validity of the results, we employed 10 runs of the proposed system for each different scenario.

- FRONTS-TR-2009-54 [HB09b]. In our first two publications on self-synchronized duty-cycling we neglected many technical aspects that will have to be respected if this technique were to be used in physical sensor networks. In this paper, we adopt our protocol to deal with asychronized clocks and mobile sensor

nodes. We show that the system is able to adapt to varying weather conditions that may be present at different locations of the deployment area at the same time.

- FRONTS-TR-2009-70 [HB09a]. We present improved versions of the algorithms presented in [HBF08, HB08] for the minimum energy multi-cast problem. The extensive collection of experimental results shows that the presented algorithms are currently state of the art for the considered problem.

Related first year FRONTS Technical Reports

- FRONTS-TR-2008-54 [HBF08].
- FRONTS-TR-2008-34 [HBM$^+$09].

6.4 Outlook

Concerning duty-cycling, we studied the interplay of system parameters in a more profound way. Moreover, the study presented in [HB09b] already took some technical constraints of physical sensor networks into consideration. However, most probably we still neglect other technical constraints of real sensor networks. Therefore, an important research target concerns the implementation of our system within a sensor network simulator such as Shawn. We also envisage the implementation of our system for hardware such as SunSpots and/or iSense sensors.

Furthermore, we are currently working on an algorithm for the minimum energy multi-casting problem for a slightly more realistic problem version where antennas have a fixed set of transmission levels in contrast to a transmission power that can be set to any positive real value. Moreover, even though the artificial ants employed by our algorithms work in a distributed way, the algorithm still requires some amount of global control. Therefore, it will be mandatory to develop a real distributed algorithm that changes and adapts initial multi-cast solutions during the operation time of the network in order to maximize its lifetime.

7 Monitoring objects and disseminating the gained data

7.1 Motivation and problem description

When sensors discover resources in their vicinity that they are designed to track and monitor, they have to be assigned to them in a proper way. It is necessary to assign more than one sensor to an object in order to monitor it properly, on the other hand the sensor can only be assigned to an object in its vicinity. When assigned to the objects, the sensors can monitor them. Now the task is to disseminate the gathered data in the network. A particularly important resource in sensor networks is the energy, and the

efficient energy management is crucial to ensure the operability of the network over a long period. The energy aware routing of the data into the network must therefore favor paths (sets of sensors) such that the sensors relaying the data have the capacity to support the energy consumption of transmitting data. From that point of view, the energy aware routing of data consists in tracking sensors with high-energy capacity. Since energy is not a renewable resource, overusing sensors with high-energy capacity is not sufficient to implement a sustainable strategy. The collaborative routing scheme that we consider consists in balancing the energy consumption among the sensors.

7.2 Scheme description

We consider a set of sensors in the Euclidean plane. The sensors are able to monitor one object iff it is in a ball with constant radius. Within the same radius they are able to communicate with other sensors. The sensors have to choose one of the objects in their vicinity which they want to monitor. An object is monitored properly iff enough sensors decide to monitor it. The objective is to properly monitor as many sensors as possible. In [BDKP09] we describe a cluster-based constant factor approximation algorithm with resource augmentation. The runtime of the algorithm is $O(\log^* n)$.

After collecting the data, it has to be disseminated. We consider an energy-aware routing protocol applied to the data-gathering problem. In this particular setting, all the sensors generate data according to events sensed in the neighboring environment. The data packets are conveyed towards a particular base station (sink) in a multi-hops fashion. We provide an algebraic characterization of the set of paths such that the energy-balance routing of data maximizes the total flow of data. We use this characterization to define two optimal communication topologies. In both configurations, the nodes choose to transmit between two levels of power. In the first configuration, the sensors choose between forwarding a packet of data to one of the neighboring nodes or transmit directly to the sink. The successive choices are done by considering the remaining energy level of the neighboring sensors. This topology is optimal, and we use the characterization provided in the report to show that augmenting the number of links does not improve the capacity of the network. In the second characterization, the sensors choose between forwarding a packet of data to a neighboring node (the minimal level of energy transmission) or to a sensor located two-hops away (the maximal level of energy transmission). Energy-balance routing maximizes the total flow of data in this topology. We propose a distributed implementation of an energy-balance routing protocol for both configurations, and we validate the performance numerically.

7.3 Related FRONTS Technical Reports

- FRONTS-TR-2009-42 [BDKP09]. We analyze the complexity of the problem of monitoring objects and provide a constant factor approximation using constant factor resource augmentation.
- FRONTS-TR-2009-61 [LSR09]. In this technical report, we consider the characterization of paths for routing data, which are optimal from the point of view of energy. Given a network with a fixed topology, we algebraically characterize the paths such that an energy balance routing strategy, which uses only these paths, is optimal in the sense that it maximizes the functioning time of the network. Moreover, we also give an algebraic characterization of the optimal sub-networks. These sub-networks use only a subset of the communication links and are such that using more communication links does not improve the total flow of data. We consider distributed strategies for routing data and balancing the energy consumption. We validate the different strategies numerically and consider different optimal topologies.

7.4 Outlook

We believe that the algorithm for monitoring objects can be improved by reducing the constant approximation factor. A further goal is to get rid of the resource augmentation and to generalize our results to more general objective functions. The results proved in the framework of data-dissemination about energy-balance protocols are worth to be extended to different applications. Indeed, we prove that energy-balance routing of data maximizes the total flow of data if the network structure satisfies some algebraic constraints. This is relevant for distributed implementation since energy-balance is a local criterion, i.e., balancing the energy consumption between neighboring sensors is sufficient to balance the energy consumption in the complete network.

8 Energy-aware transmission policies

8.1 Motivation and problem description

The emergence of trust in sensor networks can be a result of many mechanisms. From a single node's perspective, this can be achieved by means of a game played between sensors, but also from a data-centric point of view this may be seen as an adherence of sensor's readings to some previously agreed model. We consider trust crucial as a mean to reach a good usage of resources in settings in which small devices must cooperate to efficiently share resources. In the settings of interest to the project, we cannot postulate the existence of an authority that can impose and make sure that an efficient and fair algorithm for sharing resources is in place. Thus we must find other

ways. In the first year of the project we have explored a game theoretic approach to trust and shown that if players (in our cases, tiny artefacts) can keep memory of the past and are perfectly synchronized, then there exist equilibria states that correspond to fair and cooperative usage of resources. The synchronization requirement is quite difficult to satisfy and thus, in the second year, we have considered alternative ways to achieve trust for tiny artefacts.

8.2 Scheme description

From our second year research, we have identified a possible scheme for enforcing and guaranteeing that players reach a cooperative configuration in the case of communication between sensors that belong to two different (and possibly conflicting) entities. Specifically, we look at the case in which two players with limited batteries compete to make their transmission heard. It is clear that if both players transmit at the same time, then the one with higher transmission power has a better chance of success. This motivates each of the two players to increase the transmission power until they both transmit at the highest possible power. This results in a very short sensor life since transmitting at higher power drains batteries much faster. It would be much better for the battery life if the two players would take turns in transmitting at the lowest possible power but this can be achieved only if the two players trust each other. In the previous year we have seen that cooperation can be achieved if sensors are synchronized and have a history. This scheme is unsatisfactory, since synchronization is hard to achieve and sensors have limited memory to store history. In this situation, we propose to artificially reduce the payoff of some of the strategies so to create new (and possibly efficient) equilibrium points. More precisely, we propose to artificially lower the payoff associated with the underlying strategic game so that the resulting game is more efficient in terms of resources used. In general, it is not always possible to obtain this in a meaningful and realistic way.

8.3 Related FRONTS Technical Reports

- In [Per09] we apply our scheme to the case of sensors with limited battery competing for access to a shared communication medium. We implement the scheme by reducing the probability of success of higher power transmission by means of a third party that, with a fixed probability $Q > 0$, jams all communication. We show that it is always possible to choose Q in such a way that the two players reach an equilibrium in which they only use the lowest transmission power which in turn greatly increases the system life-time. This is unlike the results obtained in the previous year regarding Interference games (see [AMPP08]) which did not admit any Nash equilibria.

8.4 Outlook

In the next year we will give a new instantiation of the scheme proposed to other scenarios involving tiny artefacts in which it is possible to reduce the payoff in a realistic way. We will also explore other ways (that is, not necessarily by reducing payoffs) by which a third party can enforce efficient equilibria in games that have no equilibria or in which all equilibria are extremely inefficient. In addition we will also study the time of convergence to equilibria in these new games, as it is likely that devices will not have the equilibria wired in but rather will have to adapt to the strategy of the third part.

9 Scheduling selfish distributed computation

9.1 Motivation and problem description

Distributed cooperation also arises when someone wants to use n sensors in order to process in parallel a set of m independent tasks, as soon as possible, i.e, when the goal is to minimize the *makespan*. Depending on their type and location, different sensors may have different processing times for the same task, and the only way to persuade selfish sensors to participate and report their true processing times, is to pay them back (in energy). In such a setting, the objective of each sensor/machine is to *selfishly* minimize the time to process its own tasks minus the payment. A central question in the area of Algorithmic Mechanism Design is to determine which is the algorithm that achieves the best approximation of this goal. Thanks to a classical result in mechanism design, the Revelation Principle, we can concentrate on *truthful* mechanisms, i.e., mechanisms where no player (sensor) has an incentive to lie about its true processing times, whatever the other players' declarations may be. The motivation behind this model is one of the most basic principles when designing a sensor network: while single devices should make a careful and efficient use of their resources, at the same time they should cooperate, so as to collectively perform one or more tasks. The sensors refuse to cooperate to process the set of tasks, unless they make sure that they are compensated for the energy they spend in processing it, which guarantees their viability.

9.2 Scheme description

Our scheduling problem is treated as a classic game-theoretic scheduling problem. Our results apply for all kinds of networks, no specific considerations are made concerning the distribution or communication of the nodes. In this framework we study the geometric shape of the partitions of the input space created by the allocation rule of a truthful mechanism for multi-unit auctions with multidimensional types and additive quasilinear utilities. We introduce a new method for describing the allocation

graph and the geometry of truthful mechanisms for an arbitrary number of items (or tasks). By pplying this method, we characterize all possible mechanisms for the case of three items. Previous work shows that monotonicity is a necessary and sufficient condition for truthfulness in convex domains. If there is only one item, monotonicity is the most practical description of truthfulness we could hope for, however for the case of more than two items and additive valuations (like in the scheduling domain) we would need a global and more intuitive description, hopefully also practical for proving lower bounds. We replace monotonicity by a geometrical and global characterization of truthfulness. Our results apply directly to the scheduling unrelated machines problem. Until now such a characterization was only known for the case of two tasks. It was one of the tools used for proving a lower bound of $1 + \sqrt{2}$ for the case of 3 players. This makes our work potentially useful for obtaining improved lower bounds for this very important problem. Finally we show lower bounds of $1 + \sqrt{n}$ and n respectively for two special classes of scheduling mechanisms, defined in terms of their geometry, demonstrating how geometrical considerations can lead to lower bound proofs.

9.3 Related FRONTS Technical Reports

- FRONTS-TR-2009-23 [Vid09]. We show lower bounds of $1 + \sqrt{n}$ and n respectively for two special classes of scheduling mechanisms, defined in terms of their geometry, demonstrating how geometrical considerations can lead to lower bound proofs.

Related first year FRONTS Technical Reports

- FRONTS-TR-2008-31 [CKV08].

9.4 Outlook

Having already done a significant progress concerning the game-theoretic scheduling problem [CKV07, CKK07, KV07, CKV08, Vid09] we intend to continue the study of this problem. We will try not only to determine which is the best approximation an algorithm can achieve, but also to give a characterization of all possible mechanisms and to close this very important problem of Algorithmic Game Theory.

10 Assigning roles

10.1 Motivation and problem description

In a dynamically changing environment, the positions of the sensors change. If roles, such as providing services to other sensors, are depending on the position, these roles

have to change as well. This problem is known as facility location problem. Due to the mobility of the sensor nodes, we investigate it in a dynamic setting. Moreover, each sensor should again use only information from its local environment. Thus, each sensor has to decide its role with knowledge of its current local neighborhood only.

10.2 Scheme description

Our scheme consists of a metric dynamic environment, in which sensors are moved externally. Some of the sensors (facilities) must provide a service to the remaining sensors (clients), where this choice of facilities and clients can be changed over time. Each sensor is able to choose whether it wants to fulfill the role of a facility or of a client. The goal is, at each point of time, to minimize the overall costs, which consist of fixed costs for each facility and costs for each client depending linearly on the distance to the nearest facility. At the same time, the nodes should not have to change from facility to client and vice versa often. Especially, the movement of a node should not have impact on the role of a node far apart. After introducing a constant factor approximation algorithm for a global and central setting last year in [DGL08], this year we modified this algorithm to work in a local and distributed fashion [DKP10].

10.3 Related FRONTS Technical Reports

- FRONTS-TR-2010-9 [DKP10]. We show a distributed algorithm that yields a constant factor approximation for the facility location problem in a dynamic setting using only knowledge from a constant neighborhood.

Related first year FRONTS Technical Reports

- FRONTS-TR-2008-57 [DGL08].

10.4 Outlook

We want to adapt our algorithm to be more robust: It should be possible to add or remove sensor nodes. Furthermore we want to find out whether it is possible to trade the approximation factor with runtime.

References

[AMPP08] Vincenzo Auletta, Luca Moscardelli, Paolo Penna, and Giuseppe Persiano. Interference games in wireless networks. In *Internet and Network Economics, 4th International Workshop (WINE 2008)*, volume 5385 of *Lecture Notes in Computer Science*, pages 278–285, September 2008. FRONTS-TR-2008-19.

* [BDKP09] Olaf Bonorden, Bastian Degener, Barbara Kempkes and Peter Pietrzyk. Complexity and approximation of a geometric local robot assignment problem. In *Algorithmic Aspects of Wireless Sensor Networks (ALGOSENSORS 09*, pages 252 – 262. Springer Verlag, July 2009. FRONTS-TR-2009-14.

* [BGKM09] Przemyslaw Blaskiewicz, Zbigniew Golebiewski, Marek Klonowski and Krzysztof Majcher. RFID system with allowers. In *Seventh Annual IEEE International Conference on Pervasive Computing and Communications - Workshops (PerCom Workshops)*, pages 1–6. IEEE Computer Society, March 2009. FRONTS-TR-2009-6.

[CKK07] George Christodoulou, Elias Koutsoupias, and Annamária Kovács. Mechanism design for fractional scheduling on unrelated machines. In *ICALP*, pages 40–52, 2007.

[CKV07] George Christodoulou, Elias Koutsoupias, and Angelina Vidali. A lower bound for scheduling mechanisms. In *SODA*, pages 1163–1169, 2007.

[CKV08] George Christodoulou, Elias Koutsoupias, and Angelina Vidali. A characterization of 2-player mechanisms for scheduling. In *16th annual European symposium on Algorithms (ESA 2008)*, volume 5193/2008 of *Lecture Notes in Computer Science*, pages 297–307. Springer Berlin / Heidelberg, September 2008. FRONTS-TR-2008-31.

[CKZ08] Jacek Cichon, Miroslaw Kutylowski, and Marcin Zawada. Power of discrete nonuniformity – optimizing access to shared radio channel in ad hoc networks. In *Mobile Ad-hoc and Sensor Networks (MSN 2008)*, pages 9 – 15. IEEE Press, 2008. FRONTS-TR-2008-29.

* [CZ09] Jacek Cichoń and Marcin Zawada Fault-tolerant alarm protocol for ad-hoc radio networks. Technical report, Wroclaw University of Technology, 2009. FRONTS-TR-2009-68.

[DGL08] Bastian Degener, Joachim Gehweiler, and Christiane Lammersen. Kinetic facility location. *Algorithmica*, 2008. FRONTS-TR-2008-57.

* [DKMadH10] Bastian Degener, Barbara Kempkes and Friedhelm Meyer auf der Heide. A local $O(n^2)$ gathering algorithm, 2010. submitted. FRONTS-TR-2010-8.

* [DKP10] Bastian Degener, Barbara Kempkes and Peter Pietrzyk. A local, distributed constant-factor approximation algorithm for the dynamic facility location problem. In *Proc. of the 2010 IEEE International Parallel and Distributed Processing Symposium*, 2010. to appear. FRONTS-TR-2010-9.

[DMP09] Stefan Dziembowski, Alessandro Mei, and Alessandro Panconesi. On active attacks on sensor network key distribution schemes. In *Algosensors*, pages 52–63, 2009.

* [GKKK09a] Zbigniew Gołębiewski, Michał Koza, Marek Klonowski and Mirosław Kutyłowski. Leader election for multi-channel radio networks - dependent versus independent trials. In Ngoc Thanh Nguyen, Huynh Phan Nguyen, and Adam Grzech, editors, *ACIIDS*, pages 477–482. IEEE Computer Society, 2009. FRONTS-TR-2009-7.

* [GKKK09b] Zbigniew Golebiewski, Marek Klonowski, Michal Koza and Miroslaw Kutylowski. Towards fair leader election in wireless networks. In *ADHOC-NOW '09: Proceedings of the 8th International Conference on Ad-Hoc, Mobile and Wireless Networks*, volume 5793 of *LNCS*, pages 166–179. Springer-Verlag, September 2009. FRONTS-TR-2009-38.

* [GKKZ09] Zbigniew Gołębiewski, Jarosław Kutyłowski, Mirosław Kutyłowski and Filip Zagórski. Detecting heavy-hitters in a P2P network. In *IFIP 1st International Conference on Network and Service Security*, 2009. FRONTS-TR-2009-39.

[HB08] H. Hernández and C. Blum. Energy-efficient multicasting in wireless ad-hoc networks: An ant colony optimization approach. In *Proceedings of ISWCS 2008 – International Symposium on Wireless Communication Systems*, pages 667–671. IEEE Press, Piscataway, NJ, 2008. FRONTS-TR-2008-59.

* [HB09a] H Hernández and C. Blum. Ant colony optimization for multicasting in static wireless ad-hoc networks. *Swarm Intelligence*, 3(2):125–148, 2009. FRONTS-TR-2009-70.

* [HB09b] H Hernández and C. Blum. Asynchronous simulation of a self-synchronized duty-cycling mechanism for mobile sensor networks. In *Proceedings of BADS 2009 – Workshop on Bio-inspired Algorithms for Distributed Systems*, pages 61–68. ACM press, New York, NY, 2009. FRONTS-TR-2009-54.

* [HB09c] H Hernández and C. Blum. Self-synchronized duty-cycling in sensor networks with energy harvesting capabilities: the static network case. In F. Rothlauf et al., editor, *Proceedings of GECCO 2009 – Genetic and Evolutionary Computation Conference*, pages 33–40. ACM press, New York, NY, 2009. FRONTS-TR-2009-53.

[HBF08] H. Hernández, C. Blum, and G. Frances. Ant colony optimization for energy-efficient broadcasting in ad-hoc networks. In M. Dorigo et al., editor, *Proceedings of ANTS 2008 – 6th International Conference on Ant Colony Optimization and Swarm Intelligence*, volume 5217 of *Lecture Notes in Computer Science*, pages 25–36. Springer-Verlag, Berlin, Germany, 2008. FRONTS-TR-2008-54.

[HBM+09] H. Hernández, C. Blum, M. Middendorf, K. Ramsch, and A. Scheidler. Self-synchronized duty-cycling for mobile sensor networks with energy harvesting capabilities: A swarm intelligence study. In *Proceedings of SIS 2009 – IEEE Swarm Intelligence Symposium*, pages 153–159. IEEE press, Piscataway, NJ, 2009. FRONTS-TR-2008-34.

* [KKK09] Marek Klonowski, Michal Koza and Miroslaw Kutylowski. Security challenges for wireless sensor networks. Dynamic routing as a security paradigm. *ERCIM News*, 76:29, 2009. FRONTS-TR-2009-67.

[KM09] J. Kutylowski and F. Meyer auf der Heide. Optimal strategies for maintaining a chain of relays between an explorer and a base camp. *Theoretical Computer Science*, 2009. FRONTS-TR-2009-5.

[KV07] Elias Koutsoupias and Angelina Vidali. A lower bound of 1+ϕ for truthful scheduling mechanisms. In *MFCS*, pages 454–464, 2007.

[LS08] P. Leone and E.M. Schiller. Interacting urns process: for clustering of large-scale networks of tiny artifacts. In *Proceedings of the 2008 ACM symposium on Applied computing*, pages 2046–2051, Fortaleza, Ceara, Brazil, 2008.

* [LS09] Pierre Leone and Elad Michael Schiller Interacting urns processes 2 for clustering of large-scale networks of tiny artifacts. Technical report, 2009. submitted: FRONTS-TR-2009-62.

* [LSR09] Pierre Leone, Nikoletseas Sotiris and Jose Rolim. Optimal data gathering paths and energy balance mechanisms in wireless networks. Technical report, 2009. FRONTS-TR-2009-61.

[MS08] F. Meyer auf der Heide and B. Schneider. Local strategies for connecting stations by small robotic networks. In *IFIP International Federation for Information Processing*, volume 268, Biologically-Inspired Collaborative Computing, pages 95–104. Springer Boston, 2008. FRONTS-TR-2008-14.

* [Per09] Giuseppe Persiano Technology games with applications to wireless communications. Technical report, 2009. FRONTS-TR-2009-71.

* [Vid09] Angelina Vidali The geometry of truthfulness. In *5th Workshop on Internet and Network Economics (WINE 2009)*, volume 5929/2009 of *Lecture Notes in Computer Science*, pages 340 – 350. Springer Berlin/Heidelberg, December 2009. FRONTS-TR-2009-23.