Technical Report

Quality-of-Service in Wireless Sensor Networks: state-of-the-art and future directions

Mário Alves, Nouha Baccour, Anis Koubaa, Ricardo Severino

Gianluca Dini, Nuno Pereira, Rui Sá, Ida Savino, Paulo Grandra de Sousa

HURRAY-TR-091108

Version: 0

Date: 11-11-2009

Quality-of-Service in Wireless Sensor Networks: state-of-the-art and future directions

Mário alves, Nouha Baccour, Anis Koubaa, Ricardo Severino, Gianluca Dini, Nuno Pereira, Rui Sá, Ida Savino, Paulo Grandra de Sousa

IPP-HURRAY!

Polytechnic Institute of Porto (ISEP-IPP)

Rua Dr. António Bernardino de Almeida, 431

4200-072 Porto

Portugal

Tel.: +351.22.8340509, Fax: +351.22.8340509

E-mail:

http://www.hurray.isep.ipp.pt

Abstract

Wireless sensor networks (WSNs) are one of today's most prominent instantiationsof the ubiquituous computing paradigm. In order to achieve highlevels of integration, WSNs need to be conceived considering requirementsbeyond the mere system's functionality. While Quality-of-Service (QoS) istraditionally associated with bit/data rate, network throughput, message delayand bit/packet error rate, we believe that this concept is too strict, inthe sense that these properties alone do not reflect the overall quality-ofserviceprovided to the user/application. Other non-functional propertiessuch as scalability, security or energy sustainability must also be consideredin the system design. This paper identifies the most important non-functionalproperties that affect the overall quality of the service provided to the users,outlining their relevance, state-of-the-art and future research directions.Key words: Wireless Sensor Networks, Quality-of-Service, Non-FunctionalProperties, Cooperating Objects, Scalability, Reliability, Timeliness,Mobility, Heterogeneity, Security, Energy-Sustainability.

Quality-of-Service in Wireless Sensor Networks: state-of-the-art and future directions

Mário Alves*

CISTER/ISEP, Polytechnic Institute of Porto, Portugal

Nouha Baccour[1]

ReDCAD Research Unit, National School of Engineers of Sfax, Tunisia

Anis Koubâa[2]

CISTER/ISEP, Polytechnic Institute of Porto, Portugal

Ricardo Severino

CISTER/ISEP, Polytechnic Institute of Porto, Portugal

Gianluca Dini

University of Pisa, Italy

Nuno Pereira

CISTER/ISEP, Polytechnic Institute of Porto, Portugal

Rui Sá

MSc candidate, ECE Department, ISEP/IPP, Polytechnic Institute of Porto, Portugal

Ida Savino[3]

ELSAG DATAMAT, Italy

Paulo Sousa

*Corresponding author

Email addresses: mjf@isep.ipp.pt (Mário Alves), nabr@isep.ipp.pt (Nouha Baccour), aska@isep.ipp.pt (Anis Koubâa), rars@isep.ipp.pt (Ricardo Severino), gianluca.dini@ing.unipi.it (Gianluca Dini), nap@isep.ipp.pt (Nuno Pereira), 1980168@isep.ipp.pt (Rui Sá), Ida.Savino@elsagdatamat.com (Ida Savino), pag@isep.ipp.pt (Paulo Sousa)

[1]also with CISTER/ISEP, Polytechnic Institute of Porto, Porto, Portugal

[2]also with the Al-Imam Mohamed bin Saud University, Riyadh, Saudi Arabia

[3]formely with the University of Pisa, Italy

Preprint submitted to Computer Networks *November 2, 2009*

CISTER/ISEP, Polytechnic Institute of Porto, Portugal

Abstract

Wireless sensor networks (WSNs) are one of today's most prominent instantiations of the ubiquituous computing paradigm. In order to achieve high levels of integration, WSNs need to be conceived considering requirements beyond the mere system's functionality. While Quality-of-Service (QoS) is traditionally associated with bit/data rate, network throughput, message delay and bit/packet error rate, we believe that this concept is too strict, in the sense that these properties alone do not reflect the overall quality-of-service provided to the user/application. Other non-functional properties such as scalability, security or energy sustainability must also be considered in the system design. This paper identifies the most important non-functional properties that affect the overall quality of the service provided to the users, outlining their relevance, state-of-the-art and future research directions.

Key words: Wireless Sensor Networks, Quality-of-Service, Non-Functional Properties, Cooperating Objects, Scalability, Reliability, Timeliness, Mobility, Heterogeneity, Security, Energy-Sustainability.

1. Introduction

Today, we can find computing capabilities in everyday physical objects as diverse as mobile phones, digital personal assistants, gaming platforms, household appliances or cars, just to name a few examples. From the computational perspective, these devices are often called embedded computing systems, as their computing capabilities are just a component of the whole system. With over 99% of all microprocessors produced today being used in embedded computing systems [1], we can witness the tremendous relevance of these systems.

The computing capability of these embedded devices is usually "hidden" from users, but they are interacting with them and with the physical environment. While today these devices interact with the physical environment at unprecedented levels, an even more dramatic change is yet to come, when these (mostly) isolated islands of computing intelligence will be seamlessly

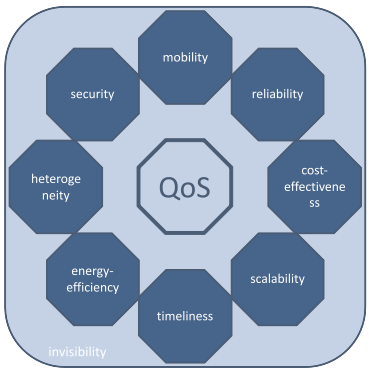

Figure 1: Holistic view of QoS [2]

cooperating for achieving common goals. Road vehicles will interact between them and with fixed infrastructures; humans and machines will coexist in smart computing environments; the Internet will penetrate the physical world via wireless sensor/actuator networks; every single "object" will be electronically and remotely identifiable, monitorable and controllable.

Wireless sensor networks (WSNs) are one of today's most prominent instantiations of this ubiquituous computing paradigm. In order to achieve these high levels of integration, WSNs need to be conceived considering requirements beyond the mere system's functionality. Properties concerning the quality of the system are also of primary importance.

In this paper, we focus on the most relevant properties of WSNs that, although not affecting their functionality, affect their behavior or performance. These are the so-called Non-Functional Properties (NFP) and include scalability, reliability, robustness, timeliness or security. By employing a broader (than the traditional one) view of Quality-of-Service (QoS), we refer to them as QoS properties.

QoS has been traditionally defined as a set of traffic characteristics for a network service (such as an Internet phone call) [3]. These characteristics may include performance-oriented as well as non-performance-oriented criteria. The ITU-T (International Telecommunication Union) has created two groups of QoS criteria for this purpose [4]. The performance-oriented group includes parameters such as set-up delay, throughput, jitter, or probability of dropping. The non-performance-oriented group defines the parameters cost, priority and level of service. These do not directly affect performance of communications, but are concerned with related matters. Traditional QoS

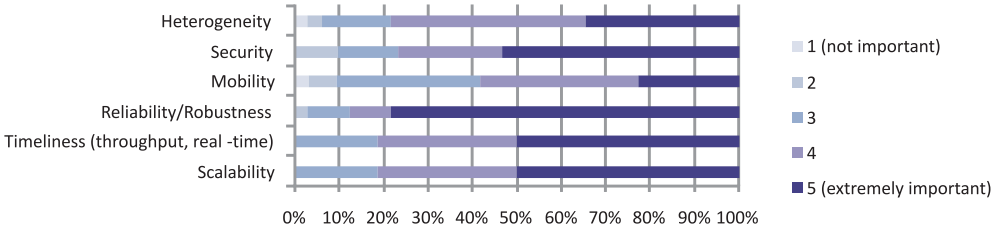

Figure 2: Survey: Non Functional Properties [7]

criteria provide a view of service parameters that is very independent and are thus limited in the way they reflect the *overall* QoS provided to the user/application.

We believe that WSN calls for a broader perspective of QoS. Each WSN application/task (which can be rather diverse [5]) must be correct, secure, produced "on time" and with the smallest energy consumption possible. WSNs are expected to be highly heterogeneous besides being cost-effective, maintainable and scalable. They must also be as much "invisible" to their users/environment as possible, to be seamlessly accepted and used at large-scale [6]. Therefore, QoS should be seen at and addressed in a more extensive and holistic perspective, instantiated in a wider range of properties (as illustrated in Figure 1), namely heterogeneity, energy-sustainability, timeliness, scalability, reliability, mobility, security, cost-effectiveness and invisibility.

The relevance of these NFP can be inferred from the results of a recent survey carried out by the CONET consortium. Figure 2 shows that, with exception to heterogeneity and mobility, all these NFPs were considered of top importance (rank 5) for at least by 50% of the interviewees. Furthermore, around 80% of the answers for every property ranked it as at least 4, except for mobility which had around 60%. One can also note that there is high interest in reliability/robustness issues since that property had 80% of the answers ranking it as 5, featuring its importance for system development. Power efficiency and energy harvesting, which we fit into the context of "Energy Sustainability", have been considered separately (chart not shown here) and both were considered very or extremely important (4 and 5) by over 80% of the interviewees.

This paper attempts to organize the research area and contribute to a more integrated view of QoS. While not providing concrete solutions for

this problem, we selected the most relevant QoS criteria and overview each one. The paper discusses the QoS criteria individually, their relevance and provides an introduction to the research efforts developed up to now.

Invisibility and Cost-Effectiveness are considered to be more subjective and transversal aspects, thus are not explicitly addressed in this paper. The term "Invisibility" is based on Mark Weisers vision [6] - "the best computer is a quiet, invisible servant". In our context, the idea is that if WSN systems/components are to be embedded in the environment in a ubiquitous large-scale fashion, they should be as much invisible and environmentally friendly (e.g. avoiding "buying new is cheaper than maintaining/repairing/recharging", or use recyclable materials and sustainable systems that are ecologically friendly). "Cost-Effectiveness" encompasses issues such as system design/development, hardware (e.g. cost/node), deployment and commissioning, exploration, maintenance and decommissioning.

This paper was written in synergy with the first edition of the CONET Roadmap [7] and also with [2]. The CONET Roadmap includes a complete and comprehensive survey on the current state and future directions of research, practice, technology and applications of Cooperating Objects systems. To the authors' best knowledge, there were no publications specifically addressing this topic so far.

The remainder of this paper elaborates on the previously mentioned QoS properties in WSNs. Section 2 introduces relevant concepts, terminology and relevance of QoS attributes. Section 3 presents the state-of-the-art of research works, practice and technology related to QoS. Section 4 presents gaps, trends and future research directions. In Section 5, we present and analyse the results of a survey regarding the timeline for achieving tangible results on the research challenges presented in Section 4. Some general conclusions are drawn in Section 6.

2. Description and Relevance

2.1. Scalability

Wireless Sensor Network (WSN) systems may involve different entities, such as network nodes (for serving as sensors/actuators, routers/ gateways and/or sinks/controllers), machines (e.g. roller belt, mobile robot, fridge, traffic light) or other agents (e.g. humans, plants, animals, microscopic organisms). Depending on the deployment characteristics such as the application, the environment or the users, a WSN system scale may dynamically

change with time. The term "scale" may refer to the number of nodes in the field (fewer or more nodes in the overall system), spatial density (fewer or more nodes in a restricted area of the system), or the dimension of the geographical region under coverage (smaller or wider, 2D or 3D). The ability of a system to easily/transparently adapt itself to these dynamic changes in scale is named *scalability*.

Scalability might be of a great importance for most WSN applications. For instance, in an environmental monitoring application, the network may need up to thousands of nodes in order to cover the whole area, depending on the required sensing information granularity (more sensor density leads to richer information, but also to more information to transmit and process) and on the transmission range of the sensor nodes. In such a case, the deployed network protocols must scale well with the number of nodes in a region, to continually ensure the correct behavior of the application. In addition, the system should adapt itself to these scale changes in a transparent way, i.e. without requiring (or with a minimum) user intervention.

Although a very large number of processors and sensors can operate in parallel and hence the processing and sensing capabilities increase linearly with the number of WSN nodes, the communication capability unfortunately does not. Due to unreliability of the radio link quality, message collisions and to the multihop nature of communications, QoS can be severely affected by the increase in the network scale. Therefore, WSN communication protocols and mechanisms must encompass scalability. Medium Access Control (MAC) and routing mechanisms must be scalable, otherwise problems such as uncontrolled routing and medium access delays as well as overflow of routing tables may occur. Scalability must also be taken into consideration for achieving efficient data processing, aggregation, storage and querying in WSNs, especially when large amounts of data are involved.

2.2. Timeliness

The timing behaviour in WSNs is becoming increasingly important, mainly due to the growing tendency for a very tight integration and interaction between embedded computing devices and the physical environment, via sensing and actuating actions [8]. Such "cyber-physical" systems require a rethinking in the usual computing and networking concepts [9], and given that the computing entities closely interact with their environment, timeliness is of increasing importance [10]. *Timeliness* represents the timing behaviour of

a system, both in terms of computations and communications, encompassing issues such as message transmission delay (how long does it take for a message to be transmitted from source to destination, task execution time, task and message priority, network bandwidth/throughput, etc.

Some WSN applications, or some specific tasks within an application, might impose to be finished within a certain time limit (deadline). These are usually referred to as "real-time" applications/tasks and require real-time computation (requiring real-time operating systems and programming languages) and real-time communications (requiring real-time communication protocols). For instance, in a WSN application there might be a task that is to detect a certain event (e.g. gas leak) in a certain region and transmit that information to a remote sink within at most 10 seconds. Note that the timing behaviour of WSN hardware, such as sensors/actuators devices, signal conditioning circuits and analogue-to-digital converters, must also be considered due to its impact in monitoring/control loops.

A fundamental difficulty in designing WSN systems with real-time requirements results from design principles that are usually antagonist to "traditional" real-time systems. "Traditional" real-time systems rely on the overallocation of resources (due to the pessimism of the analysis, e.g. Worst-Case Execution Time), usually reducing their ability to tackle the dynamic behaviour of the physical phenomena. On the other hand, WSN systems based on unattended resource-constrained nodes, must optimize resource utilization and heavily depend on the dynamic nature of their environment. An example is tracking the motion and evolution of a fluid (e.g. gas leak), where the computational and communication demands change in time and space, according to the propagation of that fluid.

2.3. Reliability/Robustness

Robustness refers to the fact that a component or a system performs well not only under ordinary conditions, but also under abnormal conditions that violate its designers' assumptions. Both hardware and software system components must be robust to be resistant and adaptive to sudden and/or long-term changes. An algorithm/protocol (e.g. for routing, localization, mobility) is robust if it continues operating correctly despite abnormalities (e.g. in inputs, calculations) or despite the change of its operational conditions or its network/system structure.

On the other hand, *Reliability* is the ability of a system or component to perform its required functions under predefined conditions for a speci-

fied period of time. This is especially important in WSNs, since it may be extremely difficult or even impossible to access them again once they are deployed. In such applications, nodes are expected to live as long as possible. To achieve these high levels of reliability, WSNs must be robust and support fault-tolerance mechanisms.

In addition, depending on the application and environment characteristics and requirements, WSN hardware (e.g. sensors, actuators) must be resistant to potentially harsh environmental conditions [11] [12] [13] [14] such as vibration/mechanical impacts, high and/or low temperature, water/humidity/moisture, dust or Radio-Frequency (RF) and Electromagnetic Interference (EMI) sources. Moreoever, WSN nodes resource limitations and the multi-hop nature of the communication worsen the situation. As a consequence, considering robustness and reliability becomes a must in the design process of WSNs to overcome the impact of these harsh operational conditions, thus mitigating maintenance actions and maximizing system lifetime.

2.4. Mobility

Mobility will be a key issue in WSNs as at least some nodes/agents are likely to be physically or logically moving relatively to each other. Physical mobility mainly refers to the changes of the entity's geographical locations during time, such as the movement of vehicles, animals, humans. Logical mobility refers to the dynamic changes in the network topology such as adding or removing new entities to/from the system.

Mobility can be classified according to the type of mobile entity into three classes: (1) *Node mobility:* (mobile nodes, node clusters, routers and gateways), (2) *Sink Mobility:* (data sinks may be moving, either on purpose (e.g. data mules) or due to the application requirements), (3) *Event Mobility:* (which means that the events physically move from one location to another, such as in event detection/tracking). Mobility can also be classified according to other aspects (e.g. mobility speed, intra/inter-cell, etc.; please refer to [7] (Section 3.3.5) for further details).

Mobility support significantly increases the capabilities of a WSN system, namely: to repair or extend the network connectivity [15] [16], to balance energy consumption, such as rotating routers closer to the sink, to adapt to dynamic stimulus changes, such as collecting information when a sudden incident occurs, or to improve the lifetime of WSNs with mobile data collectors ("data mules"). However, in many application scenarios it is not enough that the WSN protocol supports joining and leaving of nodes, since this process

might lead to inadmissible network inaccessibility times (unbounded message delays or message losses). Mobility support in WSNs is therefore a rather heterogeneous and challenging topic.

2.5. Security

Given the interactive and pervasive nature of WSNs, security is one of the key points for their acceptance outside the research community. In fact, a security breach in such systems can result in severe privacy violations and physical side effects, including property damage, injury and even death.

Security in WSNs is a more difficult long-term problem than is today in desktop and enterprise computing. In fact, such objects that are in spatial proximity cooperate among themselves in order to jointly execute a given task. It follows that there is no central, trusted authority that mediates interaction among them. Furthermore, WSNs use wireless communication in order to simplify deployment and increase reconfigurability. So, unlike a traditional network, an adversary with a simple radio receiver/transmitter can easily eavesdrop as well as inject/modify packets in a wireless network.

Cost reasons cause devices to have limitations in terms of energy consumption, computation, storage, and communication capabilities. This leads to constraints on the types of security solutions that can be applied. To further worsen this scenario, devices often lack adequate physical/hardware support to protection and tamper-resistance. This, together with the fact that WSNs can be deployed over a large, unattended, possibly hostile area, implies that each device can be tampered with by a malicious subject.

Finally, the drive to provide richer functionalities, increased customizability and flexible reconfigurability of WSNs requires the ability to dynamically download software on them [17] [18]. In fact, traditional systems have been designed to perform a fixed set of predefined functionalities in a well-known operating environment. Hence, their functionality is not expected to change during the system lifetime. This design approach can no longer be pursued in the vast majority of applications. In order to be cost-effective and operational over time, WSNs must be reconfigurable for becoming customizable to different operating environments and adaptable to changing operating conditions. However, the need for reconfigurability acts against security as it introduces new sources of vulnerability. Downloading malicious software (including viruses, worms, and Trojan horses) is by far the instrument of choice in launching security logical attacks. The magnitude of this problem will

only worsen with the rapid increase in the software content of embedded systems.

2.6. Heterogeneity

WSN systems will inherently be composed of heterogeneous components, therefore heterogeneity must be appropriately considered both pre-run-time (at design time) and during system operation (e.g. for system management and maintenance). In the context of this paper, heterogeneity is considered in a broad perspective and at different levels, namely:

- *heterogeneity in networking hardware/software*: sensor/actuator-level nodes (different motes, RFID, MEMS) and communication protocols, higher-level nodes (e.g. gateways) and communication protocols, system and network planning/management;
- *heterogeneity in embedded system nodes hardware/software architecture* : sensors and sensor boards, design diversity, calibration, operating systems and programming languages for resource-constrained networked embedded systems, middleware;
- *heterogeneity in cyber/pervasive/host computing devices*: HMIs (in general), wearable computers, mobile phones, PDAs, HMDs, mobile robots, transportation vehicles and other industrial (or other) machinery;
- *heterogeneity in applications/services/user-perspective*: many applications/services may be provided by the same networking infrastructure, different human users, eventually with different roles.

The integration of heterogeneous Cooperating Objects featuring different embedded information processing and communication capabilities has a huge number of application possibilities. Furthermore, WSNs featuring heterogeneous hardware offer the additional advantage of exploiting the complementarities and specialisation of each object. Nevertheless, it must be highlighted that system design/management complexity grows (even more than linearly) with heterogeneity.

2.7. Energy Sustainability

Particularly in larger-scale WSNs, most of the nodes must be energetically self-sustainable, as maintenance actions such as battery recharge/replacement may not be feasible or at least not convenient. Current WSN nodes rely on small batteries with a very restricted energy budget. Moreover, batteries with reasonable form factor and cost do not yield the lifetime required by most applications, despite recent technological advances [19].

Energy-efficiency has been a major focus of research since the dawn of the WSN paradigm and witnessed significant advancements over the last decade. Energy efficiency can be defined as the ratio of the amount of work done to the amount of energy consumed. Thus, using less energy to perform the same amount of work or performing more work from the same energy input can be defined as an *efficiency gain*. However, efficiency alone is not enough to reduce energy consumption. This is why several techniques have been proposed to maximize the lifetime of battery-powered WSN nodes. These techniques aim at energy conservation, which can be defined as reducing energy consumption through a reduction in the amount of work done. Conservation schemes leave the ratio of the amount of work done to energy consumption unchanged and so do not affect efficiency.

Efficiency and conservation, even in combination, prolong the lifetime of a WSN system, but cannot turn it "perpetual". Therefore, energy must be collected from the surrounding environment in order to supplement or even replace batteries [20][21]. The process of extracting energy from the ambient environment and converting it into consumable electrical energy is generally known as energy harvesting (or energy scavenging). Energy harvesting, along with energy efficiency and energy conservation, are the available means to enable nodes self-sustainability and to prolong system lifetime, and can all be framed within the broader concept of "Energetic Sustainability".

3. State of the art

3.1. Scalability

Although the new paradigm of WSNs was coined over one decade ago and lots of research has been done in this area, real-world WSNs applications are still of insignificant number and particularly of insignificant scale. To our best knowledge, real (academic-driven and temporary) WSN deployments were only up to a few hundred (e.g. VigilNet, [22]) to one thousand

nodes (ExScal, [23]). Reasons for the non-existence of large-scale applications include the lack of standards and mature and cost-effective technologies for WSNs. Some considerations about the current state of research in scalability-related aspects are presented next.

A typical strategy for supporting WSN scalability relies on the use of hierarchical (or tiered) network architectures, e.g. cluster-based (e.g. [24], [25] or [26]), hexagonal ([27]) or heterogenous-protocols (e.g. [28], [29]). The underlying philosophy in these communication architectures is to have a more powerful (e.g. higher energy capacity, radio coverage and bit rate) network technologies working as a backbone for less powerful (sub)networks at the sensor/actuator level.

In [30], the authors proposed the use of a two-tiered WSN architecture for structural health monitoring. This is a GSM-like architecture that divides the monitored area into several clusters. Each cluster is managed by a local master that handles the communication using a TDMA-like protocol inside the cluster. This approach lacks scalability inside each cluster due to the TDMA inherent limitations. Also, this architecture is entirely dependent on the presence of a local master to ensure communications, which is not suitable for WSNs. In fact, for a large-scale network, this architecture is unpractical since the number of local master's increases linearly with the number of deployed nodes, resulting in a significant increase of the overall cost.

In [29], the authors proposed using a gateway as a portal where every WSN node is identified by an IP address, allowing direct and individual access. However, there is no mobility support and the handling of very large networks may become a difficult task. In [31], the authors proposed a multiple-tiered architecture relying on a IEEE 802.11/WiFi-based backbone and a IEEE 802.15.4/ZigBee-based sensor/actuator network. Though there is a concern on supporting QoS in IEEE 802.15.4/ZigBee-based WSNs, especially on supporting both best-effort and real-time traffic, there are still many open issues, specially on the interoperability with the backbone network.

Some commercial solutions are available (e.g. from Digi, ScatterWeb, SensiNode and CrossBow) to interface WSNs to IP/Internet, therefore fostering scalability. However, QoS properties (such as timeliness) are basically neglected. The IETF 6loWPAN group is driving IPv6 over IEEE 802.15.4, aiming at scaling up Internet into the "smart objects" level. This solution might be interesting for WSN applications with scalability and interoperability requirements, provided that 6loWPAN supports the required levels of

QoS.

Recent findings on wireless dominance-based MAC protocols (like the one used in the Controller Area Network [32]) provide unprecedented advantages for WSNs, since aggregate computations can be performed with a complexity that is independent of the number of sensing nodes [33].

3.2. Timeliness

Real-time issues have only recently drawn attention from the "wireless sensor networks" scientific community [10]. However, the timing behaviour of WSNs will be of increasing importance for many applications: real world processes and phenomena often require real-time data acquisition and processing [8]. Some examples include mission critical applications, such as early warning systems for natural disasters or contamination (forest fires, earthquakes, tsunamis, radiation, etc.), critical infrastructures monitoring (e.g. bridges, tunnels, energy grid) or support for emergency interventions (firemen, doctors at a hospital etc.).

In this context, it is crucial that WSN resources are predicted in advance, to support the prospective applications with a pre-defined timeliness. Thus, it is mandatory to have adequate methodologies to dimension network resources in such a way that the system behaves as expected [10]. However, the provision of timeliness guarantees has always been considered as very challenging due to the usually severe limitations of WSN nodes, such as the ones related to their energy, computational and communication capabilities, in addition to the large-scale nature of WSNs. So, adequate mechanisms must be devised for dimensioning WSN resources in order to guarantee a minimum timeliness performance. Actually, the evaluation of the performance limits of WSNs is a crucial task, particularly when the network is expected to operate under worst-case conditions [34].

Real-time communications over sensor networks are mostly achieved through deterministic routing and MAC (Medium Access Control) protocols. Most of the MAC protocols developed to support deadline requirement in the context of WSN are designed around some TDMA-based scheme. Indeed, TDMA protocols have very appealing characteristics for this context, such as being inherently collision-free, having the possibility of scheduling transmit/receive times, and consequently being very power efficient.

Common to all TDMA-based protocols is the requirement that nodes have the same time reference. This is a notably difficult problem, that has been addressed in a number of ways. The simplest approach is to use some type of

global clock. This can be achieved, for example, using GPS. However, GPS requires power hungry receivers, and does not perform well indoors. The synchronization problem was also tackled using distributed algorithms that distribute/exchange clock information. There are several such time synchronization schemes in the research literature, where some of the most salient of these, providing good accuracy, are RBS [35], TPSN [36] or FTSP [37]. Notably, the work in [38] is the only practical synchronization strategy that does not require nodes to construct a hierarchical organization, but it can take an unbounded number of broadcasts to achieve synchronization.

Some examples of TDMA-baed MAC protocols are TRAMA [39], RT-Link [40], PEDAMACS [41], or I-EDF [42]. This last work ([42]) is interesting in that it implements the EDF algorithm when accessing the medium. It is based on the assumption that all nodes know the traffic on the other nodes that compete for the medium and all these nodes execute the EDF scheduling algorithm. Unfortunately, this algorithm is based on the assumption that a node knows the arrival time of messages on other nodes, thus nodes be placed in static cells, and channel assignment needs to be carefully handled to avoid interference between neighbor cells. The Dual-mode real-time MAC protocol [43] is similar to I-EDF in the respect that it is also based on a cellular structure, where each cell has a different channel. This MAC protocol ([43]) has two modes: protected and unprotected. The unprotected mode is used while no collisions are detected, after which the protected mode is started. The protected mode is a typical TDMA scheme.

The MAC layer in IEEE 802.15.4 [44] has several operating modes. For the purpose of this section (supporting messages with deadline requirements in wireless ad-hoc networks) the most interesting mode is the beacon-enabled mode, where nodes organize themselves in a Personal Area Network (PAN), and a coordinator (called the PAN coordinator) organizes channel access and data transmissions in a structure called the superframe.A thorough review of IEEE 802.15.4 in the context of supporting messages with deadline requirements in WSN can be found in [45]. The GTS allocation mechanism was also subject of several studies that address the throughput and delay guarantees provided by this mechanism [46], and energy/delay trade-offs [47]. To overcome the maximum limit of seven GTS allowed, in [48] the authors propose i-Game, an implicit GTS allocation mechanism that enables the use of a GTS by several nodes.

At the routing layer, timeliness has been address by several works (e.g. [49, 50, 51, 52]). Other works have also employed hierarchical network/topological

models such as hexagonal, grid or cluster-tree (e.g. [53], [54], [27], [28], [55]).

3.3. Reliability/Robustness

There are different fault-management techniques for "traditional" distributed systems [56]: 1) *fault prevention*, to avoid or prevent faults; 2) *fault detection*, to use different metrics to collect symptoms of possible faults; 3) *fault isolation*, to correlate different types of fault indications received from the network, and propose various fault hypotheses; 4) *fault identification*, to test each of the proposed hypotheses in order to precisely localize and identify faults; 5) *fault recovery*, to treat faults, i.e., reverse their adverse effects.

Most fault avoidance techniques in WSNs operate in the network layer by adding redundancy in routing paths and sometimes enabling load balancing and congestion control. Some proposals are GRAB [57], Node-Disjoint Multipath [58], and Braided Multipath [58]. Fault prevention techniques prevent faults from happening by (1) ensuring full network coverage and connectivity at the design and deployment stages as proposed in [59] [60] [61], (2) constantly monitoring network status and triggering reactive actions if deemed necessary, or (3) enforcing redundancy in the data delivery path, hoping that at least one of the paths will survive.

Network monitoring, as in traditional distributed systems, provides a fundamental support for efficient fault detection and identification, either in passive (observing the traffic already present in the network to infer network condition) or active (probes injected into the network or relying on reports from the nodes) modes. Monitored network parameters include: (1) Node Status, concerning node's energy level, e.g. eScan [62] or energy map [63]; (2) Link Quality, enabling higher level protocols to adapt by changing routing structures as in [12]; (3) Congestion Level, by observing the buffer length as proposed in [64] and in CODA [65]; (4) Packet Loss, to be used as an indicator of faults, e.g. PSFQ [66] and GARUDA [67].

Upon detecting abnormal situations, fault isolation and identification will diagnose the causes. For instance, when a sink does not hear from a particular part of the routing tree, it is unknown whether it is due to failure of a key routing node, or failure of all nodes in a region. Sympathy [68] determines whether the cause of failure is in node health, bad connectivity/connection, or at the sink by, using an empirical decision tree.

Faults can be recovered independently of applications, like CODA [65]. However, this type of application-independent recovery does not differentiate between important (e.g., a new report) and unimportant packets (e.g.,

redundant reports, control packets). On the other hand, application aware fault tolerant protocols try to achieve application specified metrics (e.g., the percentage of distinct packets delivered), which requires the nodes to analyze packets and take different actions based on packet types.

There are different proposals for ensuring reliability in data collection in upstream communications, according to the data collection mode (raw or aggregated data). ESRT [64], PERG [69] and TAG [70]are some examples. Also, for downstream communications, other techniques were already proposed in the literature. PSFQ [66], GARUDA [67], and ReACT [71] are among the most popular.

In order to provide a higher level solution for fault-tolerance, fault-management frameworks with complete management infrastructures and information models have been also proposed (e.g. Digest [72], SNMS [73], AgletBus [74], MANNA [75]), which can be complemented with previous discussed approaches to achieve better performance.

3.4. Mobility

Mobility management has long been addressed for different types of computer networks, such as IP-based [76, 77], MANETs [78] or cellular [79] networks. Nevertheless, WSN characteristics such as scale (number of nodes and coverage area), node resource constraints and the fact that WSNs are usually supposed to detect/track physical phenomena, impose a rethinking of the mobility management paradigm.

In most WSNs literature, topology dynamics results mainly from nodes failure rather than from the mobility of nodes (sensors or sinks), i.e. WSN nodes (and the physical topology) are assumed to be static during runtime. Most WSN architectures/protocols support joining and leaving of nodes (e.g. ZigBee). Nevertheless, they react to topological changes by dropping the broken paths and computing new ones, thus resulting in network inaccessibility times that lead to message delay/loss. Although several WSN architectures have explored the use of mobility for data collection (e.g. [80]), target tracking (e.g. [81]) or repairing network connectivity (e.g. [82, 16]), no guarantees are given on timely data delivery. Some other works on mobility in WSNs (e.g. [83, 84]) reflect incomplete results.

Mobility scenario generation models enable to test mobility in WSNs. They are often based on stochastic models [85], taking into account mobility parameters such as speed, movement direction, radio propagation models

and presence of obstacles. BonnMotion [86] is an example of a tool to create and analyze mobility scenarios that can feed several network simulators.

Mobility support greatly impacts WSN lower protocol layers design and particularly MAC and routing mechanisms, for two main reasons: first, mobility involves topological changes that may affect algorithms that need to tune some parameters according to the density of nodes in the contention area. Second, MAC algorithms based on medium reservation may fail in case of mobility, since the reservation procedures usually assume static nodes. For instance, algorithms based on the Request-To-Send/Clear-To-Send (RTS/CTS) handshake for medium reservation may fail because either the corresponding nodes move outside the mutual coverage range after the handshake or external nodes get into the contention area and start transmitting without being aware of the medium reservation. Nevertheless, some MAC algorithms can self-adapt to topological changes resulting from nodes mobility (e.g. [87, 88]), but at the expense of higher energy consumption and medium access delay.

Generally speaking, many routing algorithms are able to cope with topology dynamics resulting from nodes mobility. However, most of them react to topology variations by dropping the broken paths and computing new ones from scratch, thus incurring in performance degradation. In particular, mobility may strongly affect cluster-based algorithms, due to the high cost of maintaining the cluster-architecture over a set of mobile nodes. Some routing algorithms specifically designed for networks with slow mobile nodes (e.g. GAF [89], TTDD [90]) attempt to estimate the nodes trajectories. The SPIN [91] family of protocols seems well-suited for environments where the sensors are mobile, since forwarding decisions are based on local neighbourhood information.

Another relevant issue is how well WSN nodes are able to estimate radio link quality, since usually handoff is performed when the current radio link quality is over passed by the link quality of an adjacent cell or cluster. The problem is that radio links cannot be identified just as "good" or "bad". There is a "transitional region" that leads to very variable quality and symmetry properties and is not adequately characterized by current link quality estimators [92].

3.5. Security

On the communication side, low power and low bit rate wireless networks suitable for WSN systems are the focus of an industrial consortium [93], IEEE

standard [94], and research community [95]. These proposals address multiple embedded devices and control of them from authenticated principals. They also propose solutions for preventing usage of the WSN by external principals. While ZigBee and IEEE 802.15.4 took the stance that cryptographic hardware support is needed (e.g. CC2420), TinySec has shown that with sufficient engineering effort, it is possible to encrypt and authenticate all communications entirely in software, without special hardware, at a cost of $5 - 10\%$ performance loss [95]. TinySec has also proven that the advantages introduced by cryptographic hardware support are limited with respect to its costs both financial and in terms of increased power consumption.

In all these secure communication proposals a crucial problem is how devices can establish a shared secret cryptographic key. This is the classical *key agreement problem* that has been extensively investigated in general networks. This problem becomes non trivial in WSNs for the following reasons. The public-key agreement schemes used in general networks (e.g., Diffie-Hellman) are not suitable for wireless sensor networks due to the limited computational abilities ofsensor nodes. Furthermore, pre-distribution of secret keys for all pairs of nodes is not viable due to the large amount of memory this requires when the network size is large. Finally, resorting to centralized trusted third-party (e.g., Kerberos) is not suitable for WSN due to the communication overhead it would cause.

The main approaches to pair-wise key establishment in WSNs are based on pre-deployment. All these approaches move from the observation that, in the most general case, WSN deployment is a random process and thus deterministically predicting the set of neighbors is not possible. In order to solve this problem Eschenauer and Gligor propose a random key pre-distribution scheme and show that, by adjusting the parameters of the scheme, key-establishment probability can be sufficiently great, nodes can set up keys with sufficiently many nodes, and the network becomes fully connected [96]. The main weakness of this approach is that an attacker who compromises a sufficiently number of nodes could reconstruct the key set and break the scheme. In LEAP+, Zhu *et al.* assume that a sensor node is able to resist an attack for a short period of time (say several seconds) when captured by an adversary and propose a scheme in which a shared secret is pre-deployed in every node [97]. The disadvantage of this scheme is that newly deployed nodes cannot establish a secure channel with those already deployed.

Recently, Malan *et al.* have shown that a purely software implementation of the Diffie-Hellman key establishment based on Elliptic Curve Cryptogra-

phy (ECC) over $\mathbb{F}_{2^p}$ for sensor nodes on 8-bit, 7.3828 MHz MICA2 mote is indeed feasible [98].

In-network processing is a fundamental technique for elaborating the wealth of data provided by WSNs in an efficient and scalable way. In order to efficiently support this technique while guaranteeing security, pair-wise security is not adequate because it would ensue too many pair-wise encryptions and decryptions. Thus, it is more convenient to organize sensor nodes in a *group* and distribute a *group key* to all group members which use it to encrypt and decrypt messages. The challenge here consists in securely and efficiently revoking and distributing group keys upon joining and leaving of nodes [99]. Several group key management systems have been proposed so far aimed at reducing the overhead of group key management [97, 100, 101]. Younis *et al.* suggest a dynamic combinatorial grouping strategy [101]. Zhu *et al.* group neighbouring sensor nodes and iteratively merge groups up to establish network-wide shared key [97]. S2RP provides a dynamic, scalable and efficient group rekeying by integrating in a novel way two basic mechanisms, namely Logical Key Hierarchy [102] and Lamport's one time passwords [103].

A related problem is *authenticated broadcast*, a fundamental security service that enables a sender to broadcast critical data and/or commands to sensor nodes in an authenticated way. Due to the resource constraints on WSN nodes, traditional broadcast authentication techniques based on digital signatures are not viable. Perrig *et al.* developed μTESLA for broadcast authentication in WSNs based on symmetric cryptography, which removes the dependence on public key cryptography [104]. Several multi-level μTESLA schemes have been later proposed to extend the capability of the original μTESLA protocol. A relevant example is reported in [105].

3.6. Heterogeneity

Almost no work has been tackling heterogeneity in WSNs. In our perspective, one of the most important reasons is that the number of WSN deployments so far is almost insignificant, particularly concerning real-world applications.

WSN nodes currently span over a large range of types, from MEMS (MicroElectroMEchanical Systems, e.g. for accelerometers), passive RFIDs (Radio-Frequecy Identifiers, e.g. for inventory), active RFIDs (e.g. for toll charge), "general-purpose" motes (e.g. Mica, Telos, FireFly) to more powerful nodes for routing/gateway or processing/control (e.g. iMote, SunSPOT, Stargate). The integration of Radio-frequency Identifier (RFID) technology

with Wireless Sensor Networks has been accepted to provide a symbiotic solution that leads to improved system performance. The growing convergence between WSN and RFID nodes technology (particularly active RFIDs, whose computation and communications modules are battery-powered) has been turning the frontier between these heterogeneous technologies increasingly undefined.

Also, different types of sensors and sensor boards may be used for measuring different physical parameters, adding complexity to the WSN system (e.g. calibration). "Design diversity", i.e. using heterogeneous components to perform the same task (e.g. measuring the same physical parameter with two different types of sensors or performing the same computation using two different processors), is usually required in critical applications. Different operating systems and programming languages (particularly for resource-constrained networked embedded systems) might also be required. Also middleware (e.g. for security or fault tolerance) might be quite heterogeneous. Solutions for supporting these different levels of heterogeneity have not been achieved yet, particularly for large-scale systems.

Communication protocols might also be heterogeneous, both in horizontal and vertical perspectives. Some solutions are available for achieving interoperability between sensor/actuator-level network protocols in process control and automation industry (e.g. PROFIBUS, ASi, FF, HART, DeviceNet, ModBus), in automotive systems (e.g. CAN, FlexRay, TTP, LIN, MOST) or in building automation (e.g. EIB/KNX, LonWorks, HomePlug). The interoperability between these and higher-level networks, such as the Internet has also been achieved through adequate gateway-like devices. However, the large-scale nature of emerging networked embedded systems impose new networking architectures based on wireless communications, both at the sensor/actuator-level (e.g. IEEE 802.15.4, ZigBee, IEEE 802.15.6 (Body Sensor Networks), 6loWPAN, Bluetooth Low Power, ISA SP100 or WirelessHART) and at backbone levels (e.g. WiFi/WiGig, WiMAX). Tangible results on this interoperability between wireless protocols are not available yet.

3.7. Energy sustainability

Several techniques regarding sensor networks have been proposed to maximize the lifetime of battery-powered wireless sensor nodes. In [106] the authors identify three main enabling techniques used for energy conservation

in wireless sensor networks: duty cycling, data driven, and mobility. The design principles behind them and their features are presented in the referred survey, however for a complete set of networking protocols the reader is referred to [107]. While all these techniques optimize and adapt energy usage to maximize the lifetime of energy reservoirs, the lifetime remains bounded and finite. Thus, further enhancements have to be done, especially regarding energy harvesting, to accomplish perpetual operation [108][109].

A comprehensive review of the many possible sources of energy that could potentially be harnessed is given in [110]. Among the currently most feasible are photonic, mechanical and thermal differentials. Solar-energy harvesting is based on the well-known principle of photovoltaic conversion, which provides high power densities, making it the best-suited choice to power wireless outdoor applications (e.g. ZebraNet, Trio, SHiMmer, etc.). A solution to power indoor routers was proposed in [111]. This approach revealed several weaknesses that enhance the need for further research on this area. In [112] several motes are reviewed and AmbiMax is presented as a new solution that uses both a solar panel and a wind generator to charge a supercapacitor based energy storage system. The need for multiple power sources is mentioned in [113] and a well successful approach is exploited in the multi-powered platform for precision agriculture proposed in [114]. In the cited example, besides a solar panel and a wind turbine, a small size hydrogenerator has been introduced as a way to harvest the energy of water-flow in irrigation pipes.

Mechanical energy from vibrations or movements is present almost everywhere and it can be transformed into useful electrical power by any kind of electromechanical transduction. Piezoelectric, electrostatic, and electromagnetic devices habe been widely investigated and several companies now offer commercially miniature mechanical harvesters delivering sufficient power for sensor operating in an industrial environment [115]. However, researchers have not yet overcome difficulties encountered for body-powered applications [116], which require MEMS devices.

Temperature differences between various objects (natural and industrial) are also freely available within the environment. Manufacturing applications, where heat is a by-product of the manufacturing process, are typically ideal applications for thermal energy harvesting. Several companies (e.g. Micropelt, Nextreme and Thermolife) are already commercializing thermoelectric generators that can exploit those scenarios. Despite their high cost and low efficiency, due to their reliability and absence of moving parts, there has been

a growing interest in the generation of power from body heat [117], as a means to power wearable devices. Further research is needed on nanostructured materials and multilayers, in order to optimize thermoelectric properties [118], as well as on miniaturization using micromachining [119].

4. Roadmap

4.1. Scalability

From the very beginning of WSN research, the scientific community has been aware of the importance of building scalable systems. Although there were some research efforts where WSNs of a few hundreds (e.g. [22]) to one thousand nodes ([23]) were deployed, WSN with tens or hundreds of thousands of nodes are still a vision.

Hierarchical (multiple-tiered, clustered) architectures are a well-known and proven principle to make computer networks scale, bringing advantages such as: the communication latency increases very slowly with distance (timeliness), the cost per node is approximately the same as the one of the cheapest nodes (cost-efficiency) and it is easy to manage "sleep schedules" for nodes (energy-efficiency). Though eventually leading to more complex network architectures, the multiple-tiered architectural solution that we dubbed "heterogenous-protocols" seems the most promising for supporting scalability without compromising other QoS metrics (e.g. throughput, delay, reliability). In this case, the communication architecture is composed of a more powerful (e.g. higher energy capacity, radio coverage and bit rate) network technologies serving as a backbone to less powerful (sub)networks at the sensor/actuator level. Communication technologies such as the ones referred in Section 3.6 must be explored as potential candidates for these architectures.

Algorithms such as MAC, routing, data processing/aggregation and congestion control have been developed to operate as far as possible at different network scales, especially envisaging large scale systems. However, existing approaches are still far away from the desired scalability, so requiring further investigation. New algorithms might be either designed from scratch or based on (adapting) already available ones. Just as an example, dominance-based MAC protocols for WSNs may be explored in a way that the time complexity in the computation of aggregate quantities becomes independent of the number of nodes [33].

Larger scale may also mean more information sinks, depending on the application. While this can lead to a more complex design and system

architecture (e.g. concerning routing), it might also be beneficial in some other perspectives. The existence of multiple geographically distributed sinks might ease the load balancing task, reducing the amount of "bottlenecks" in the WSN. A multiple-tiered architecture may be seen as a particular case of "multiple sinks", since data converges to separate "sink" nodes that may act as gateways to a higher level network.

4.2. Timeliness

As already referred the "big" challenge in large-scale WSN systems is to optimize all QoS properties simultaneously, knowing a priori that some (most) of them are contradictory. In what concerns "Timeliness", we point to the following research directions:

- *explore hierarchical network architectures and models*, particularly trying to merge interesting features from more "mesh-like" (probabilistic MAC/routing, but more flexible, scalable and redundant) and more "clustered-like" approaches (deterministic MAC/routing, but less flexible and redundant, synchronization is complex), to grab the "best of both worlds";

- *design protocols and algorithms in an optimized cross-layered approach*; analyse trade-offs in terms of flexibility and interoperability, since the software structure becomes more difficult to update and maintain; for example, explore how prioritized MAC schemes can be used to compute aggregated computations, in a way that time-complexity becomes independent of the number of nodes;

- *consider timeliness (and real-time) both at the node level (hardware and software) and at the network level*; the timing performance of a WSN depends on node hardware design, on the operating system (if any), programming language and style, as well as on the network protocol; in this line, investigate existing operating systems (OSs) for resource-constrained embedded systems, specially the most widely used (e.g. TinyOS and Contiki) in a way to support real-time features (preemption, priority inheritance mechanism) existing in other OSs (e.g. nano-RK and ERIKA);

- *investigate whether the classical approaches of embedded real-time systems still apply* (such as formal WCET analysis, synchronous lan-

guages), despite their strong resource limitations, or if more probabilistic-oriented approaches must be followed; these probabilistic models must consider the peculiarities of resource-constrained devices, particularly considering the probability of transmission errors (e.g. radio link quality must be correctly estimated) and thus of message retransmissions; one approach is to associate a confidence level with each guaranteed delay bound to *quantify the uncertainty* on the guaranteed delay bound;

- *design innovative MAC mechanisms for improving timeliness, reliability and energy-efficiency* (e.g. for mitigating the hidden-node problem, to avoid "idle/waste" times during nodes power on; using scheduling techniques for nodes efficiently sharing TDMA slots), guaranteeing an optimal trade-off between flexibility and complexity;

- *investigate on distributed and dynamic resource allocation schemes* for synchronized WSNs, where resources (e.g. bandwidth and memory) must be adequately allocated depending of the physical/logical network changes (e.g. a critical event); centralized adaptive synchronization induces a significant amount of computation and communication overheads, which may be unsuitable for WSNs.

- *build appropriate system planning and network dimensioning tools* to be able to achieve optimal trade-offs between QoS properties, particularly for timeliness;

4.3. Reliability/Robustness

As outlined in section 3.3, WSN hardware must be designed to be resistant to harsh environmental and usage conditions and no to harm the flora, fauna or the ecological structure of the environment (e.g. batteries), hence this aspect must be taken into consideration. The increasing tendency for miniaturization, instantiated in technologies such as RFID (Radio-Frequency Identification), MEMS (Microelectromechanical Systems) or SoC/NoC (Systems/Networks on Chip) and for reduction of cost per node should not compromise (or at least at a reduced level) hardware robustness. Actually, the trends for integrating sensing, processing, memory, communication and mechanical functionalities in a single chip may even be explored to improve hardware robustness.

Common practices for robust software/algorithms can be allied with a careful resource management for improved system robustness and in general

to higher reliability, e.g.: 1) writing "generic" code that can accommodate a wide range of situations and thereby avoid having to insert extra code into it just to handle special cases (code added just for special cases is often buggier than other code, and stability problems can become particularly frequent and/or severe from the interactions among several such sections of code); 2) using formal techniques, such as fuzz testing, to test algorithms since this type of testing involves invalid or unexpected inputs/stimulus; 3) providing each application with its own memory area and prevent it from interfering with the memory areas of other applications or of the kernel.

Although the faul-tolerance techniques enumerated in section 3.3 are promising in terms of robustness and energy efficiency, further research is needed to address the scalability and network dynamics in designing fault-tolerant mechanisms. Some interesting topics to address in the future are:

- when faults occur in WSNs, MAC and routing protocols must accommodate the formation of new links and routes to the destination, transport protocols must adaptively decide how to retransmit, and application layer protocols must determine which part of the missing data is critical and what level of loss is tolerable; therefore, multiple levels of redundancy may be needed and a cross-layer approach exploring the interactions among different protocol layers is desirable.

- the mechanisms presented in 3.3 only consider reliability (logical correctness) of data delivery as a performance metric; trade-offs with other QoS metrics must be considered as well;

- the presence of faults in WSNs introduces uncertainty into standard operations such as answering queries, as data should not be extracted in a purely best-effort manner, but be produced with a clearly defined formal meaning; for instance, if only a subset of the sensor readings satisfies the application query, the network only reports part of the readings filtered by the query; however, the sink does not know whether the remaining reports were not received due to network faults or because results were filtered by the query; if a metric is defined to indicate the completeness of the returned answer, the sink would be better informed; therefore, it is essential to develop informative quality metrics for sensor applications (network semantics).

Most fault management techniques in WSNs have been integrated with

application requirements [120]. Design of a generic fault management technique for WSNs must take into account a wide variety of applications with diverse needs, different sources of faults, and various network configurations. In addition, scalability, mobility, and timeliness may also have to be considered.

4.4. Mobility

Most network protocols support joining and leaving of nodes. Nevertheless, they react to topological changes by dropping the broken paths and computing new ones, thus resulting in network inaccessibility times that lead to message delays and losses. Although some WSN architectures have explored the use of mobile data collectors (data mules), which collect data from the sensor nodes and deliver it to the sinks, there are no guarantees on timely data delivery. In contrast, critical applications such as patient monitoring, factory automation or intelligent transportation systems require strict bounds on latency and guaranteed data delivery. In this context, coordination among mobile nodes is required, thus an important challenge is how a WSN can compute, in a distributed way, the path that a mobile node should follow. This path can be updated depending on the changes of the environment (e.g. mobility of observers, other WSNs or the phenomenon).

Mobility may be particularly difficult to support in cluster-based WSN architectures, due to the cost for maintaining clusters with a set of mobile nodes. Therefore, mobility management mechanisms for cluster-based WSNs must be carefully designed. MAC and routing protocols must also be adaptive to dynamic changes resulting from mobility, as they must transparently readapt to node number and density changes.

Mobility management mechanisms must be designed based on realistic (real-world) models, derived from real-world data. Mobility speed, obstacles, radio link quality and propagation models, network scale, network density and network partitioning are important factors that must be considered. For instance, an efficient mobility management mechanism greatly depends on how far the nodes are able to estimate radio link quality (usually handoff is performed when the current radio link quality is overpassed by the link quality of an adjacent cell or cluster). Recent studies show that radio links cannot be identified just as “good” or “bad”. There is a “transitional region” that can lead to very variable quality and symmetry properties, which is yet to be fully and adequately characterized.

Mobility models and benchmarks should be used to evaluate communication protocols and middleware approaches. While most simulation tools for WSNs lack mobility support (eventually due to the lack of protocols with mobility support), future simulators for WSN systems should encompass mobility support and be based on the previously referred realistic models.

The design of a mobility management mechanism fully depends on the existence or not of a localization mechanism (this may impact routing decisions as well). Location information may be quite benefitial for better mobility support, but may also have a negative impact on network management, energy-efficiency and cost. Consequently, localization mechanisms that are scalable, distributed, accurate, cost-effective and energy-efficient must be devised.

In summary, future research should focus on supporting transparent, seamless, energy-efficient, real-time and reliable mobility management mechanisms in WSNs.

4.5. Security

The topics addressed in Section 3.5 have achieved important results but they have not yet reached an adequate level of maturity. Actually, we need a secure and efficient key distribution mechanism that is resilient to node compromise, allows incremental deployment and scales to large networks. In this context, we expect to see research in more efficient public-key schemes, e.g., elliptic curves, hardware support for public-key cryptography [121], and efficiently and securely engineering elliptic curve cryptography for real world implementation [122].

The deployment of WSN in unattended, often hostile, environments makes it easier for an adversary to gain physical (not only logical) access to these devices. An adversary can physically capture an object, tamper with it, and have it behave maliciously. The compromise of even a single node may be sufficient to completely compromise the whole routing service [123]. Completely preventing this risk by means of tamper-resistant hardware does not seem viable because strong tamper-resistance is too expensive and not always absolutely safe. Thus the challenge is to build networks that can operate correctly even in the presence of several compromised nodes, at least up to a certain threshold. A possible direction consists in tolerating compromized nodes by exploiting the network redundancy and the knowledge of the physical environment. Interesting results have been achieved both in the context

of secure routing [124] and secure aggregation [125], but this remains a continuining overall challenge.

Another direction consists on program integrity verification, a technique enables to remotely verify the integrity of the program residing in each device whenever the device joins the network or has experienced a long service blockage. Software-based approaches to program integrity verification have been proposed for sensor networks [126, 127]. However, these approaches provide security under the assumption of a limited adversary. More research is thus necessary to overcome these limitations. In addition, efficient hardware support for integrity verification could be useful in order to make the integrity verification procedure more difficult to simulate and to indissolubly link the execution of such a procedure with the node under verification.

"Traditional" network QoS and network security have been considered as separate entities and research in these areas have largely proceeded independently. However, security impacts overall QoS and it is therefore essential to consider both security and QoS together when designing protocols for ad hoc environments as one impacts the other. The research community has recently acknowledged this gap. Some initial and promising results have been obtained [128, 129] but the topic is still in its infancy.

WSNs are more ubiquitous and pervasive than the Internet and therefore they tend to be a more invasive from the user privacy point of view. The Zigbee consortium [93] and the IEEE 802.15.4 [94] propose solutions aimed at preventing an unauthorized principal from accessing the WSN. However, these solutions reflect the perspective of a network administrator. A key challenge is to provide solutions that reflect the standpoint of the user, the ultimate owner of such a private information. The main challenges here are security and usability, On the one hand we need mechanisms that allow a user to retain control on who has access to his/her information On the other hand, these mechanisms must be usable by a normal computer-illiterate user. From this standpoint, Johnson and Stajano have made a preliminary work in the smart-home context [130]. However, more research is necessary.

4.6. Heterogeneity

As can be inferred from section 3.6, WSN research must tackle heterogeneity almost from scratch. New classes of resource-constrained embedded system devices should be clearly identified, defining frontiers between nodes with different characteristics and capabilities (e.g. motes, RFIDs, MEMS).

As technology rapidly evolves, tending for miniaturization, these frontiers are increasingly harder to define, bringing enormous challenges ahead.

WSN applications may require sensor/actuator nodes to measure different physical parameters, implying heterogeneous sensing technology. Also, the same physical quantity may be required to be measured by many WSN nodes (for reliability purposes, or just because there is the need to extract the minimum/average/maximum value of that parameter in a certain region), or even by different types of sensors ("design diversity" for redundancy or accuracy purposes). The quantity and diversity of these sensing technologies will bring important challenges (e.g. for hardware design, hardware abstraction layers design, calibration).

Another challenge is how to tackle the interoperability between sensor/actuator-level communication protocols. From past experience, there will be no "single" standard for sensor/actuator-level communication protocols. Wireless protocols such as IEEE 802.15.4, IEEE 802.15.6, ZigBee, 6loWPAN, Bluetooth Low Power, ISA SP100 or WirelessHART might need to interoperate between them and also with wired ones. Vertical integration of networks at different hierarchical levels will also be a major challenge. Higher bandwidth and more robust wired (e.g. ATM, Switched Ethernet) and wireless (e.g. WiFi/WiGig, WiMAX, UWB) networks will have to interoperate with sensor/actuator-level networks. Guaranteeing end-to-end QoS brings even more complexity into WSN protocol design, i.e. satisfying throughput, delay, reliability, security, energy-efficiency requirements across different network tiers is not straightforward. Moreover, network planning/management tools must tackle these heterogeneous systems in an efficient and straightforward fashion.

Heterogeneity in WSN systems is also instantiated at the operating systems and programming language levels. Operating systems such as TinyOS, Contiki, Mantis, nano-RK, ERIKA have been around for some time, each of them with specific characteristics. So, it is likely that future WSN systems (particularly at large-scale) might comprise computing devices running more than one operating systems, leading to additional design complexity. The same applies to programming languages/environments (e.g. nesC, C, JAVA) and simulation/debugging tools.

Hosting/client equipment and HMIs are also likely to be quite heterogeneous. Wearable computing equipments are likely to be used in a panoply of WSN applications (e.g. HMDs for industrial maintenance or mobile phones in participatory/urban sensing). Other equipment, such as database servers,

video-surveillance cameras, monitoring/control computers (industrial PCs, PLCs, RCs) mobile robots or transportation vehicles, industrial machinery (welding/painting/assembly robots, machine-tools, roller belts, cranes) will rise the level of heterogeneity to unprecedented levels.

WSN systems wll probably have to support several applications and services, imposing different QoS requirements which might dynamically change depending on spatiotemporal issues (e.g. WSN system for building automation may control security/access control, fire/smoke alarm systems, HVAC system, lights, doors, blinds, lifts/escalators, each of these with particular/dynamic requirements). Therefore, mechanisms such routing/MAC, admission control and scheduling, security, fault-tolerance or data aggregation must be designed to encompass such heterogeneous applications and services. The diversity of users (culture, technical skills) of a WSN system is also a challenge for system designers, namely in what concerns HMIs, safety and security requirements. Semantics should be further explored to ease the users role.

4.7. Energy sustainability

Energy sources are ubiquitous in the environment [20][111], so it is reasonable to consider that the energy required to permanently operate a WSN can be obtained through energy harvesting. There are currently several methods to harness energy from some of those sources. Nevertheless, some others are neglected, mostly due to challenges raised by the low energy density or feasibility of the energy harvesting method (e.g. ambient RF energy). All those sources have in common their random nature, a characteristic that still dictates the undesirable use of energy reservoirs, typically rechargeable batteries or, more recently, ultracapacitors [112]. Based on the above remarks, several approaches have to be exploited simultaneously, so that a system continues to operate perennially.

As the power levels achieved by miniature harvesters are usually low, wireless sensor nodes must be prepared to harvest energy from all the available energy sources surrounding it, in order to suffice nodes' power requirements. Moreover, in contrast to approaches that only attempt to minimize the energy consumption of each node, software (e.g. algorithms, protocols) design must also concern on adapting node-level system parameters (e.g. duty-cycling, transmission power, sensing reliability, etc) such that a maximal efficiency is obtained while respecting the energetic sustainability of the node.

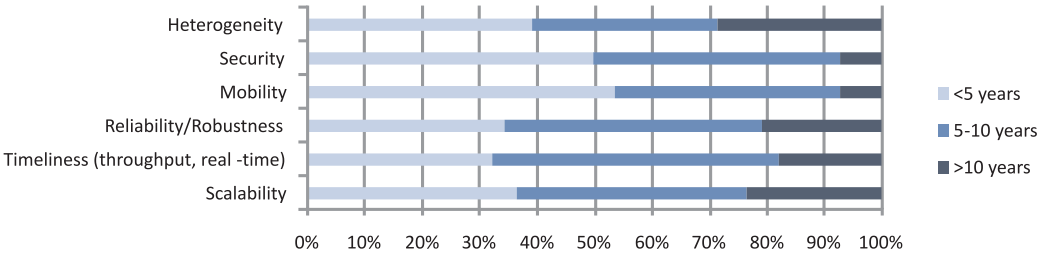

Figure 3: Survey: Non Functional Properties

Finally, another important issue is that nodes deployed in different places will probably have different harvesting opportunities. This means that it is absolutely necessary to align the workload allocation with the energy availability of each individual node. For that, network solutions and protocols such as MAC and routing will have to be redesigned, so they can deal with such changeable nodes and maintain the desired QoS.

5. Timeline

Non-functional properties (NFPs) are considered to be of paramount importance to Cooperating Objects and Wireless Sensor Network systems. This is reflected by the market analysis presented in [7] (Chapter 5) and also by the answers to a recent survey (CONET questionnaire filled by academics and industrialists). As already referred, heterogeneity, timeliness, reliability/robustness, mobility, security and heterogeneity are quality-of-service (QoS) properties that must be observed in all WSN systems and fulfilled for each particular application in both individual and integrated perspectives. Mobility is probably the only exception, in the sense that only some WSN applications will require mobility support.

Figure (3) (*source:* [7], Section 6.2.3) reflects the answers in what concerns how long it will take to get effective solutions for each NFP. The current state-of-the-art and state-of-technology reveals a strong immatureness and a clear lack of solutions (protocols, software/hardware architectures, technology) in respect to these NFPs. Current real-world applications and even research-oriented test-beds exist in a relatively small number and feature just up to some hundreds of sensor/actuator nodes. Market studies (e.g. On World) forecast mass deployments of WSN systems (sensor/actuator networks, pervasive Internet, smart environments) at a global scale, but this

seems to be a vision that will see the light only in more than one decade.

Research on improving the timeliness, security and reliability/robustness of WSN systems are still at a very early stage, particularly for the latter. Scalability is being considered by researchers (e.g. algorithms, methodologies, protocols), but results are still either incomplete, immature and/or yet to be validated through large-scale real-world applications. Almost no work exists on supporting mobility (nodes, node clusters) in WSNs. While successful results are not obtained using homogeneous WSN systems, it will be hard (almost impossible) to support high levels of heterogeneity, such as the coexistence and interoperability between heterogeneous hardware platforms, network protocols, operating systems, middleware and applications.

Power Efficiency and Energy Harvesting (which we fit into "Energy Sustainability") have been considered separately ([7], Section 6.2.1). For the former, a major breakthrough is expected in a short to medium term, because of the importance of this issue for the massive adoption of WSN technology and systems. Energy Harvesting seems to be a harder problem that will require more time to find solutions that can be widely used.

Even more difficult is to fulfil and balance all these NFP/QoS properties at the same time, i.e. in a holistic perspective, since most of them are contradictory (i.e. improving one of them may harm the others). While a minimum level of maturity in each NFP must be reached, a bigger challenge is to devise system/network dimensioning methodologies and tools that are able to support system designers on balancing these properties in a way that system/application requirements are met. This is why we preclude that mature solutions to fulfil these QoS properties in a holistic fashion might only be achieved in a decade or so.

6. Conclusion

As people increasingly depend on embedded computing systems, the quality of their service (QoS) is also of growing importance, particularly for Wireless Sensor Network (WSN) applications where humans, fauna, flora, the environment or any valuable good may be severely affected by their behavior.

However, the provision of QoS in WSNs is very challenging due to the following problems: (1) the usually severe limitations of WSN nodes (e.g. energy, computational and communication capabilities and security); (2) the harsh nature of the environments (impacting e.g. node lifetime, communication reliability); (3) the large-scale nature of most WSNs (impacting e.g.

timeliness, reliability, security); (4) the high interdependency between QoS properties (as they are often contradictory).

This paper aimed at identifying the most important non-functional properties that affect the overall quality of the service provided to the users - scalability, heterogeneity, timeliness, reliability, security, mobility and energy sustainability - outlining their relevance, state-of-the-art and future research directions.

The bigger challenge seems to be how to achieve an optimal trade-off between QoS metrics, according to the QoS requirements imposed by each application. We envision that the solution is to conceive models, methodologies and tools for network and system planning and dimensioning, based on (multicriteria) optimization techniques. System designers must have software tools for automatically setting each and every property, parameter and mechanism of the system, trying to fulfill and balance all QoS properties. We preclude that this will only be possible in a decade or so. Enough mature-ness must first be achieved in each individual QoS property before holistic solutions may see the light.

References

[1] J. Turley, "Embedded processors by the numbers," http://www.embedded.com/1999/9905/9905turley.htm, 1999.

[2] M. Alves, "The wireless sensor networks standards and cots landscape: can we get qos and "calm technology"?" Tutorial at EWSN'09. [Online]. Available: http://www.hurray.isep.ipp.pt/ART-WiSe

[3] W. Stallings, *Data and computer communications (5th ed.)*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1997.

[4] J. Irvine and D. Harle, *Data Communications and Networks: An Engineering Approach*. John Wiley and Sons, Ltd, 2001.

[5] B. Raman and K. Chebrolu, "Censor networks: a critique of "sensor networks" from a systems perspective," *SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 3, pp. 75–78, 2008.

[6] M. D. Weiser, "The Computer for the 21st Century," *Scientific American*, vol. 265, no. 3, pp. 94–104, Sep. 1991.

[7] P. Marron et al., Ed., *Cooperating Objects Roadmap 2009*, 1st ed. Logos Verlag, 2009.

[8] J. Stankovic, I. Lee, A. Mok, and R. Rajkumar, "Opportunities and obligations for physical computing systems," *IEEE Computer*, vol. 38, no. 11, pp. 25–33, 2005.

[9] E. A. Lee, "Cyber-physical systems - are computing foundations adequate?" in *Position Paper for NSF Workshop On Cyber-Physical Systems: Research Motivation, Techniques and Roadmap*, October 2006.

[10] J. A. Stankovic, T. Abdelzaher, C. Lu, L. Sha, and J. Hou, "Real-Time Communication and Coordination in Embedded Sensor Networks," *Proceedings of the IEEE*, vol. 91, no. 7, pp. 1002–1022, 2003.

[11] J. Zhao and R. Govindan, "Understanding packet delivery performance in dense wireless sensor networks," in *SenSys '03: Proceedings of the 1st international conference on Embedded networked sensor systems*. New York, NY, USA: ACM, 2003, pp. 1–13.

[12] A. Woo, T. Tong, and D. Culler, "Taming the underlying challenges of reliable multihop routing in sensor networks," in *SenSys '03: Proceedings of the 1st international conference on Embedded networked sensor systems*. New York, NY, USA: ACM, 2003, pp. 14–27.

[13] G. Zhou, T. He, S. Krishnamurthy, and J. A. Stankovic, "Impact of radio irregularity on wireless sensor networks," in *MobiSys '04: Proceedings of the 2nd international conference on Mobile systems, applications, and services*. New York, NY, USA: ACM, 2004, pp. 125–138.

[14] A. Cerpa, J. L. Wong, L. Kuang, M. Potkonjak, and D. Estrin, "Statistical model of lossy links in wireless sensor networks," in *IPSN '05: Proceedings of the 4th international symposium on Information processing in sensor networks*. Piscataway, NJ, USA: IEEE Press, 2005, p. 11.

[15] C. Chen and J. Ma, "Mobile enabled large scale wireless sensor networks," *Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference*, vol. 1, pp. 333–338, Feb. 2006.

[16] B. Liu, P. Brass, O. Dousse, P. Nain, and D. Towsley, "Mobility improves coverage of sensor networks," in *MobiHoc '05: Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*. New York, NY, USA: ACM, 2005, pp. 300–308.

[17] S. Ravi, A. Raghunathan, P. Kocher, and S. Hattangady, "Security in embedded systems: Design challenges," *Trans. on Embedded Computing Sys.*, vol. 3, no. 3, pp. 461–491, 2004.

[18] S. Ravi, A. Raghunathan, and S. Chakradhar, "Tamper resistance mechanisms for secure, embedded systems," in *VLSID '04: Proceedings of the 17th International Conference on VLSI Design.* Washington, DC, USA: IEEE Computer Society, 2004, p. 605.

[19] M. Fetcenko, S. Ovshinsky, B. Reichman, K. Young, C. Fierro, J. Koch, A. Zallen, W. Mays, and T. Ouchi, "Recent advances in nimh battery technology," *Journal of Power Sources*, vol. 165, no. 2, pp. 544 – 551, 2007, iBA - HBC 2006 - Selected papers from the INTERNATIONAL BATTERY ASSOCIATION & HAWAII BATTERY CONFERENCE 2006 Waikoloa, Hawaii, USA 9-12 January 2006. [Online]. Available: http://www.sciencedirect.com/science/article/B6TH1-4MCW9T7-4/2/3d16368ff78e3c7b5bf30a61b9d91602

[20] J. A. Paradiso and T. Starner, "Energy scavenging for mobile and wireless electronics," *IEEE Pervasive Computing*, vol. 4, no. 1, pp. 18–27, 2005.

[21] J. P. Thomas, M. A. Qidwai, and J. C. Kellogg, "Energy scavenging for small-scale unmanned systems," *Journal of Power Sources*, vol. 159, no. 2, pp. 1494 – 1509, 2006. [Online]. Available: http://www.sciencedirect.com/science/article/B6TH1-4JBGJ45-6/2/ba83614ecb29098a9af8acdf590da792

[22] T. He, S. Krishnamurthy, J. Stankovic, T. Abdelzaher, L. Luo, R. Stoleru, T. Yan, L. Gu, G. Zhou, J. Hui, and B. Krogh, "VigilNet: An integrated sensor network system for energy-efficient surveillance," *ACM Transactions on Sensor Networks*, vol. 2, no. 1, pp. 1–38, February 2006.

[23] A. Arora, R. Ramnath, E. Ertin, P. Sinha, S. Bapat, V. Naik, V. Kulathumani, H. Zhang, H. Cao, M. Sridharan, N. Seddon, C. Anderson, T. Herman, N. Trivedi, C. Zhang, R. Shah, S. Kulkarni, M. Aramugam, and L. Wang, "Exscal: Elements of an extreme scale wireless sensor network," in *RTCSA '05: Proc. of the 11th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications*, 2005, pp. 102–108.

[24] Zigbee-Alliance, "Zigbee specification," http://www.zigbee.org/, 2005.

[25] G. Gupta and M. Younis, "Fault-tolerant clustering of wireless sensor networks," in *WCNC '03: IEEE Wireless Communication and Networks Conference*. IEEEPress, 2003.

[26] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocols for wireless microsensor networks," in *Proc. Hawaaian Int'l Conf. on Systems Science*, 2000.

[27] K. S. Prabh and T. Abdelzaher, "On scheduling and real-time capacity of hexagonal wireless sensor networks," in *ECRTS '07: Proc. of the 19th Euromicro Conference on Real-Time Systems*. IEEE Press, Los Alamitos, CA, 2007, pp. 136–145.

[28] A. Koubaa, M. Alves, and E. Tovar, "Modeling and worst-case dimensioning of cluster-tree wireless sensor networks," in *RTSS'06: Proc. of the 27th IEEE Real-Time Systems Symposium*. IEEEPress, 2006, pp. 412–421.

[29] O. Gnawali, K.-Y. Jang, J. Paek, M. Vieira, R. Govindan, B. Greenstein, A. Joki, D. Estrin, and E. Kohler, "The tenet architecture for tiered sensor networks," in *SenSys '06: Proceedings of the 4th international conference on Embedded networked sensor systems*. New York, NY, USA: ACM, 2006, pp. 153–166.

[30] V. A. Kottapalli, A. S. Kiremidjian, J. P. Lynch, E. Carryer, T. W. Kenny, K. H. Law, and Y. Lei, "Two-tiered wireless sensor network architecture for structural health monitoring," in *SPIE '03: Proc. of 10th Annual International Symposium on Smart Structures and Materials*, 2003, pp. 8–19.

[31] J. Leal, A. Cunha, M. Alves, and A. Koubaa, "On a IEEE 802.15.4/ZigBee to IEEE 802.11 gateway for the ART-WiSe architecture," in *ETFA '07: Work-in-Progress session of the 12th IEEE Conference on Emerging Technologies and Factory Automation*. IEEEPress, 2007.

[32] R. B. GmbH, Stuttgart, "CAN specification, ver. 2.0," http://www.semiconductors.bosch.de/pdf/can2spec.pdf, 1991.

[33] B. Andersson, N. Pereira, W. Elmenreich, E. Tovar, F. Pacheco, and N. Cruz, "A scalable and efficient approach for obtaining measurements in CAN-Based control systems," *IEEE Transactions on Industrial Informatics*, vol. 4, no. 2, pp. 80–91, 2008.

[34] Z. Hu and B. Li, "Fundamental performance limits of wireless sensor networks," in *in Ad Hoc and Sensor*. Nova Science Publishers, 2004.

[35] J. Elson, L. Girod, and D. Estrin, "Fine-grained network time synchronization using reference broadcasts," in *Proceedings of 5th symposium on Operating systems design and implementation (OSDI'02)*, Boston, MA, USA, Dec. 2002, pp. 147–163.

[36] S. Ganeriwal, R. Kumar, and M. B. Srivastava, "Timing-sync protocol for sensor networks," in *Proceedings of 1st international conference on Embedded networked sensor systems (SenSys'03)*, Los Angeles, California, USA, Nov. 2003, pp. 138–149.

[37] M. Maróti, B. Kusy, G. Simon, and A. Lédeczi, "The flooding time synchronization protocol," in *Proceedings of 2nd international conference on Embedded networked sensor systems (SenSys'04)*, Baltimore, MD, USA, Nov. 2004, pp. 39–499.

[38] G. Werner-Allen, G. Tewari, A. Patel, M. Welsh, and R. Nagpal, "Firefly-inspired sensor network synchronicity with realistic radio effects," in *3rd international conference on Embedded networked sensor systems (SenSys'05)*, 2005, pp. 142 – 153.

[39] V. Rajendran, K. Obraczka, and J. J. Garcia-Luna-Aceves, "Energy-efficient, collision-free medium access control for wireless sensor networks," in *Proceedings of 1st international conference on Embedded networked sensor systems (SenSys'03)*, Los Angeles, California, USA, Nov. 2003, pp. 181–192.

[40] A. Rowe, R. Mangharam, and R. Rajkumar, "RT-Link: A time-synchronized link protocol for energy- constrained multi-hop wireless networks," in *Proceedings of the 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks (SECON '06)*, Reston, VA, USA, Sep. 2006, pp. 402–411.

[41] A. P. Sinem Coleri and P. Varaiya, "PEDAMACS: Power efficient and delay aware medium access protocol for sensor networks," *IEEE Transactions on Mobile Computing*, vol. 5, no. 7, pp. 920–930, 2006.

[42] M. Caccamo and L. Y. Zhang, "An implicit prioritized access protocol for wireless sensor networks," in *Proceedings of the 23rd IEEE Real-Time Syst. Symp. (RTSS'02)*, Austin, TX, USA, Dec. 2002, pp. 39–48.

[43] T. Watteyne, I. Augé-Blum, and S. Ubéda, "Dual-mode real-time mac protocol for wireless sensor networks: a validation/simulation approach," in *1st international conference on Integrated internet ad hoc and sensor networks InterSense'06*. New York, NY, USA: ACM, 2006, p. 2.

[44] IEEE, "IEEE standard for information technology - telecommnunications and information exchange between systems - local and metropolitan area networks - specific reuirements - part 14.4: Wireless medium access control (MAC) and physical layer (PHY) specifications for low rate wireless personal area networks (LR-WPANs)," October, 2003.

[45] A. Koubâa, M. Alves, and E. Tovar, "IEEE 802.15.4: a federating communication protocol for time-sensitive wireless sensor networks," IPP-HURRAY! Research Group, Institute Polytechnic Porto, Porto, Portugal, Tech. Rep. HURRAY-TR-060202, 2006.

[46] A. Koubaa, M. Alves, and E. Tovar, "GTS allocation analysis in IEEE 802.15.4 for real-time wireless sensor networks," in *Proceedings of 14th International Workshop on Parallel and Distributed Real-Time Systems (WPDRTS'06)*, Rhodes Island, Greece, Apr. 2006.

[47] A. Koubâa, M. Alves, and E. Tovar, "Energy/delay trade-off of the GTS allocation mechanism in IEEE 802.15.4 for wireless sensor networks," *International Journal of Communication Systems*, vol. 20, no. 7, pp. 791–808, Jul. 2007.

[48] A. Koubaa, M. Alves, and E. Tovar, "i-GAME: An implicit gts allocation mechanism in ieee 802.15.4," in *Proceedings of 18th Euromicro Conference on Real-Time Systems (ECRTS'06)*, Dresden, Germany, Jul. 2006.

[49] T. He, J. A. Stankovic, C. Lu, and T. Abdelzaher, "Speed: a stateless protocol for real-time communication in sensor networks," in *Distributed Computing Systems, 2003. Proceedings. 23rd International Conference on*, 2003, pp. 46–55.

[50] K. Akkaya and M. Younis, "An energy-aware qos routing protocol for wireless sensor networks," in *Distributed Computing Systems Workshops, 2003. Proceedings. 23rd International Conference on*, May 2003, pp. 710–715.

[51] E. Felemban, C.-G. Lee, E. Ekici, R. Boder, and S. Vural, "Probabilistic qos guarantee in reliability and timeliness domains in wireless sensor networks," in *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, vol. 4, March 2005, pp. 2646–2657 vol. 4.

[52] H. Li, P. Shenoy, and K. Ramamritham, "Scheduling messages with deadlines in multi-hop real-time sensor networks," in *11th IEEE Real Time and*

Embedded Technology and Applications Symposium RTAS'05, 2005, pp. 415 – 425.

[53] T. Abdelzaher, K. S. Prabh, and R. Kiran, "On real-time capacity limits of multihop wireless sensor networks," in *RTSS' 04: Proc. of the 25th IEEE Real-Time Systems Symposium*. IEEE Press, Los Alamitos, CA, 2004.

[54] J. Gibson, G. Xie, and Y. Xiao, "Performance limits of fair-access in sensor networks with linear and selected grid topologies," in *GLOBECOM '07: 50th IEEE Global Communications Conference Ad Hoc and Sensor Networking Symposium*, 2007.

[55] P. Jurcik, R. Severino, A. Koubâa, M. Alves, and E. Tovar, "Real-time communications over cluster-tree sensor networks with mobile sink behaviour," in *RTCSA '08: Proc. of the 14th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications*, 2008.

[56] A. S. Tanenbaum and M. V. Steen, *Distributed Systems: Principles and Paradigms*. Upper Saddle River, NJ, USA: Prentice Hall PTR, 2001.

[57] F. Y. G. Zhong, "Gradient broadcast: A robust data delivery protocol for large scale sensor networks," *ACM Wireless Networks (WINET)*, vol. 11, pp. 285–298, 2005.

[58] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 5, no. 4, pp. 11–25, 2001.

[59] S. Meguerdichian, F. Koushanfar, M. Potkonjak, and M. Srivastava, "Coverage problems in wireless ad-hoc sensor networks," *INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, vol. 3, pp. 1380–1387 vol.3, 2001.

[60] F. Xue and P. R. Kumar, "The number of neighbors needed for connectivity of wireless networks," *Wirel. Netw.*, vol. 10, no. 2, pp. 169–181, 2004.

[61] V. Isler, S. Kannan, and K. Daniilidis, "Sampling based sensor-network deployment," *Intelligent Robots and Systems, 2004. (IROS 2004). Proceedings. 2004 IEEE/RSJ International Conference on*, vol. 2, pp. 1780–1785 vol.2, Sept.-2 Oct. 2004.

[62] Y. Zhao, R. Govindan, and D. Estrin, "Residual energy scan for monitoring sensor networks," *Wireless Communications and Networking Conference, 2002. WCNC2002. 2002 IEEE*, vol. 1, pp. 356–362 vol.1, Mar 2002.

[63] R. A. F. Mini, A. A. F. Loureiro, and B. Nath, "The distinctive design characteristic of a wireless sensor network: the energy map," *Computer Communications*, vol. 27, no. 10, pp. 935 – 945, 2004, protocol Engineering for Wired and Wireless Networks. [Online]. Available: http://www.sciencedirect.com/science/article/B6TYP-4BMY15B-2/2/9acdbb590e792dea4a44b6eb48360ff2

[64] Y. Sankarasubramaniam, Özgür B. Akan, and I. F. Akyildiz, "Esrt: event-to-sink reliable transport in wireless sensor networks," in *MobiHoc '03: Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing*. New York, NY, USA: ACM, 2003, pp. 177–188.

[65] C.-Y. Wan, S. B. Eisenman, and A. T. Campbell, "Coda: congestion detection and avoidance in sensor networks," in *SenSys '03: Proceedings of the 1st international conference on Embedded networked sensor systems*. New York, NY, USA: ACM, 2003, pp. 266–279.

[66] C. yih Wan, A. T. Campbell, and L. Krishnamurthy, "Pump-slowly, fetch-quickly (psfq) : A reliable transport protocol for sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 23, pp. 862–872, 2005.

[67] S.-J. Park, R. Vedantham, R. Sivakumar, and I. F. Akyildiz, "A scalable approach for reliable downstream data delivery in wireless sensor networks," in *MobiHoc '04: Proceedings of the 5th ACM international symposium on Mobile ad hoc networking and computing*. New York, NY, USA: ACM, 2004, pp. 78–89.

[68] N. Ramanathan, K. Chang, R. Kapur, L. Girod, E. Kohler, and D. Estrin, "Sympathy for the sensor network debugger," in *SenSys '05: Proceedings of the 3rd international conference on Embedded networked sensor systems*. New York, NY, USA: ACM, 2005, pp. 255–267.

[69] Q. Han, I. Lazaridis, S. Mehrotra, and N. Venkatasubramanian, "Sensor data collection with expected reliability guarantees," in *PERCOMW '05: Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications Workshops*. Washington, DC, USA: IEEE Computer Society, 2005, pp. 374–378.

[70] J. Considine, F. Li, G. Kollios, and J. Byers, "Approximate aggregation techniques for sensor databases," in *ICDE '04: Proceedings of the 20th International Conference on Data Engineering*. Washington, DC, USA: IEEE Computer Society, 2004, p. 449.

[71] V. Rajendran, K. Obraczka, Y. Yi, S.-J. Lee, K. Tang, and M. Gerla, "Combining source- and localized recovery to achieve reliable multicast in multi-hop ad hoc networks," in *NETWORKING 2004, Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communication, Third International IFIP-TC6 Networking Conference, Athens, Greece, May 9-14, 2004, Proceedings*, ser. Lecture Notes in Computer Science, vol. 3042. Springer, 2004. [Online]. Available: citeseer.ist.psu.edu/704792.html

[72] J. Zhao, R. Govindan, and D. Estrin, "Computing aggregates for monitoring wireless sensor networks," *Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on*, pp. 139–148, May 2003.

[73] G. Tolle and D. Culler, "Design of an application-cooperative management system for wireless sensor networks," *Wireless Sensor Networks, 2005. Proceeedings of the Second European Workshop on*, pp. 121–132, Jan.-2 Feb. 2005.

[74] J.-J. Lim, D. Kiskis, and K. Shin, "System support for management of networked low-power sensors," *Network Operations and Management Symposium, 2006. NOMS 2006. 10th IEEE/IFIP*, pp. 436–447, April 2006.

[75] L. Ruiz, J. Nogueira, and A. Loureiro, "Manna: a management architecture for wireless sensor networks," *Communications Magazine, IEEE*, vol. 41, no. 2, pp. 116–125, Feb 2003.

[76] D. Saha, A. Mukherjee, I. Misra, M. Chakraborty, and N. Subhash, "Mobility support in ip: a survey of related protocols," *Communications Magazine, IEEE*, vol. 18, no. 6, pp. 34–40, 2004.

[77] A. T. Campbell, "Comparison of ip micromobility protocols," *Wireless Communication, IEEE*, vol. 9, pp. 72–82, Fev 2002.

[78] F. Abduljalil and S. Bodhe, "A survey of integrating ip mobility protocols and mobile ad hoc networks," *Communications Surveys & Tutorialse, IEEE*, vol. 9, no. 1, pp. 14–30, 2007.

[79] T.-Y. Wu, C.-Y. Huang, and H.-C. Chao, "A survey of mobile ip in cellular and mobile ad-hoc network environments," *Ad Hoc Networks, IEEE*, vol. 3, no. 3, pp. 351–370, May 2005.

[80] M. Laibowitz and J. A. Paradiso, "Parasitic mobility for pervasive sensor networks," in *in Proc. 3rd Ann. Conf. Pervasive Computing (Pervasive 2005), Springer-Verlag, 2005. 29. A.S. Holmes et al., ???Axial-Flow Microturbine with Electromagnetic Generator: Design, CFD Simulation, and Prototype Demonstration,??? Proc. 17th IEEE Int???l Micro Electro.* Springer-Verlag, 2005, pp. 255–278.

[81] Y. Zou and K. Chakrabarty, "Distributed mobility management for target tracking in mobile sensor networks," *Transactions on Mobile Computing, IEEE*, vol. 6, no. 8, pp. 872–887, June 2007.

[82] P. Corke, S. Hrabar, R. Peterson, D. Rus, S. Saripalli, and G. Sukhatme, "Autonomous deployment and repair of a sensor network using an unmanned aerial vehicle," in *in IEEE International Conference on Robotics and Automation*, 2004, pp. 3602–3609.

[83] A. Muneeb, V. Thiemo, and U. Z. Afzal, "Mobility management in sensor networks," in *Proceedings of Workshops Proceeding of 2nd IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS'06)*, San Francisco, California, 2006, p. 10, pages 131-140.

[84] T. Sun, N.-C. Liang, L.-J. Chen, P.-C. Chen, and M. Gerla, "Evaluating mobility support in zigbee networks," in *EUC*, 2007, pp. 87–100.

[85] T. Camp, J. Boleng, and V. Davies, "A survey of mobility models for ad hoc network research," *Wireless Communications and Mobile Computing (WCMC): Special issue on Mobile Ad Hoc Networking: Research, Trends and Applications*, vol. 2, pp. 483–502, 2002.

[86] *BonnMotion - a mobility scenario generation and analysis tool*, University of Bonn, 2005, http://www.cs.uni-bonn.de/IV/bomonet/BonnMotion.htm.

[87] V. Rajendran, K. Obraczka, and J. Garcia-Luna-Aceves, "Energy-Efficient, Collision-Free Medium Access Control for Wireless Sensor Networks," *Wireless Networks*, vol. 12, no. 1, pp. 63–78, 2006.

[88] I. Chlamtac, A. Faragó, and H. Zhang, "Time-spread multiple-access (tsma) protocols for multihop mobile radio networks," *IEEE/ACM Trans. Netw.*, vol. 5, no. 6, pp. 804–812, 1997.

[89] Y. Xu, J. Heidemann, and D. Estrin, "Geography-informed energy conservation for ad hoc routing," in *Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking*, USC/Information

Sciences Institute. Rome, Italy: ACM, July 2001, pp. 70–84. [Online]. Available: http://www.isi.edu/ johnh/PAPERS/Xu01a.html

[90] H. Luo, F. Ye, J. Cheng, S. Lu, and L. Zhang, "Ttdd: two-tier data dissemination in large-scale wireless sensor networks," *Wirel. Netw.*, vol. 11, no. 1-2, pp. 161–175, 2005.

[91] W. R. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive protocols for information dissemination in wireless sensor networks," in *MobiCom '99: Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking.* New York, NY, USA: ACM, 1999, pp. 174–185.

[92] N. Baccour, A. Kouba, M. Jama, H. Youssef, M. Zuniga, and M. Alves, "A Comparative Simulation Study of Link Quality Estimators in Wireless Sensor Networks," in *17th IEEE/ACM International Symposium on Modelling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS'09)*, London, UK, 2009, pp. 21–23.

[93] "Zigbee alliance website, online at: http://www.zigbee.org/en/index.asp."

[94] LAN/MAN Standards Committee of the IEEE Computer Society, *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs)*, Sep. 2006, revision of 2006.

[95] C. Karlof, N. Sastry, and D. Wagner, "Tinysec: a link layer security architecture for wireless sensor networks," in *SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems.* New York, NY, USA: ACM Press, 2004, pp. 162–175. [Online]. Available: http://dx.doi.org/10.1145/1031495.1031515

[96] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *CCS '02: Proceedings of the 9th ACM conference on Computer and communications security.* New York, NY, USA: ACM, 2002, pp. 41–47.

[97] S. Zhu, S. Setia, and S. Jajodia, "Leap+: Efficient security mechanisms for large-scale distributed sensor networks," *ACM Trans. Sen. Netw.*, vol. 2, no. 4, pp. 500–528, 2006.

[98] D. J. Malan, M. Welsh, and M. D. Smith, "Implementing public-key infrastructure for sensor networks," *ACM Transactions on Sensor Networks*, vol. 4, no. 4, pp. 1–23, 2008.

[99] H. Chan, V. D. Gligor, A. Perrig, and G. Muralidharan, "On the distribution and revocation of cryptographic keys in sensor networks," *IEEE Trans. Dependable Secur. Comput.*, vol. 2, no. 3, pp. 233–247, 2005.

[100] G. Dini and I. M. Savino, "S2rp: a secure and scalable rekeying protocol for wireless sensor networks," *Mobile Adhoc and Sensor Systems (MASS), 2006 IEEE International Conference on*, pp. 457–466, Oct. 2006.

[101] K. Ghumman, "Location-aware combinatorial key management scheme for clustered sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 17, no. 8, pp. 865–882, 2006, senior Member-Mohamed F. Younis and Senior Member-Mohamed Eltoweissy.

[102] S. Rafaeli and D. Hutchison, "A Survey of Key Management for Secure Group Communication," *ACM Computing Surveys*, vol. 35, no. 3, pp. 309–329, September 2003.

[103] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770–772, November 1981.

[104] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and D. j. Tygar, "SPINS: Security protocols for sensor networks," in *Proceedings of the Seventh Annual International Conference on Mobile Computing and Networks*, Rome, Italy, July 16–21 2001, pp. 189–199.

[105] D. Liu and P. Ning, "Multilevel μtesla: Broadcast authentication for distributed sensor networks," *ACM Transaction on Embedded Computing Systems*, vol. 3, no. 4, pp. 800–836, 2004.

[106] G. Anastasi, M. Conti, M. D. Francesco, and A. Passarella, "Energy conservation in wireless sensor networks: A survey," *Ad Hoc Netw.*, vol. 7, no. 3, pp. 537–568, 2009.

[107] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Comput. Netw.*, vol. 52, no. 12, pp. 2292–2330, 2008.

[108] V. Raghunathan, A. Kansal, J. Hsu, J. Friedman, and M. Srivastava, "Design considerations for solar energy harvesting wireless embedded systems," in *IPSN '05: Proceedings of the 4th international symposium on Information*

processing in sensor networks. Piscataway, NJ, USA: IEEE Press, 2005, p. 64.

[109] A. Kansal, J. Hsu, S. Zahedi, and M. B. Srivastava, "Power management in energy harvesting sensor networks," *Trans. on Embedded Computing Sys.*, vol. 6, no. 4, p. 32, 2007.

[110] S. Roundy, D. Steingart, L. Frechette, P. Wright, and J. Rabaey, "Power sources for wireless sensor networks," *Wireless Sensor Networks*, pp. 1–17, 2004///. [Online]. Available: http://www.springerlink.com/content/b0utgm8ahnphll3l

[111] A. Hande, T. Polk, W. Walker, and D. Bhatia, "Indoor solar energy harvesting for sensor network router nodes," *Microprocess. Microsyst.*, vol. 31, no. 6, pp. 420–432, 2007.

[112] C. Park and P. Chou, "Ambimax: Autonomous energy harvesting platform for multi-supply wireless sensor nodes," vol. 1, Sept. 2006, pp. 168–177.

[113] P. H. Chou and C. Park, "Energy-efficient platform designs for real-world wireless sensing applications," in *ICCAD '05: Proceedings of the 2005 IEEE/ACM International conference on Computer-aided design.* Washington, DC, USA: IEEE Computer Society, 2005, pp. 913–920.

[114] R. Morais, S. G. Matos, M. A. Fernandes, A. L. G. Valente, S. F. S. P. Soares, P. J. S. G. Ferreira, and M. J. C. S. Reis, "Sun, wind and water flow as energy supply for small stationary data acquisition platforms," *Comput. Electron. Agric.*, vol. 64, no. 2, pp. 120–132, 2008.

[115] P. Mitcheson, E. Yeatman, G. Rao, A. Holmes, and T. Green, "Energy harvesting from human and machine motion for wireless electronic devices," *Proceedings of the IEEE*, vol. 96, no. 9, pp. 1457–1486, Sept. 2008.

[116] M. Renaud, P. Fiorini, R. van Schaijk, and C. van Hoof, "Harvesting energy from the motion of human limbs: the design and analysis of an impact-based piezoelectric generator," *Smart Material Structures*, vol. 18, no. 3, pp. 035 001–+, Mar. 2009.

[117] V. Leonov, T. Torfs, P. Fiorini, and C. Van Hoof, "Thermoelectric converters of human warmth for self-powered wireless sensor nodes," *Sensors Journal, IEEE*, vol. 7, no. 5, pp. 650–657, 2007. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4154682

[118] G. J. Snyder and E. S. Toberer, "Complex thermoelectric materials," *Nature Materials*, vol. 7, pp. 105–114, Feb. 2008.

[119] Z. Wang, V. Leonov, P. Fiorini, and C. Van Hoof, "Micromachined thermopiles for energy scavenging on human body," June 2007, pp. 911–914.

[120] L. Paradis and Q. Han, "A survey of fault management in wireless sensor networks," *J. Netw. Syst. Manage.*, vol. 15, no. 2, pp. 171–190, 2007.

[121] R. Roman, C. Alcaraz, and J. Lopez, "A survey of cryptographic primitives and implementations for hardware-constrained sensor network nodes," *Mob. Netw. Appl.*, vol. 12, no. 4, pp. 231–244, 2007.

[122] A. Cilardo, L. Coppolino, N. Mazzocca, and L. Romano, "Elliptic curve cryptography engineering," *Proceedings of the IEEE*, vol. 94, no. 2, pp. 395–406, Feb. 2006.

[123] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," in *In First IEEE International Workshop on Sensor Network Protocols and Applications*, 2003, pp. 113–127.

[124] J. Deng, R. Han, and S. Mishra, "Insens: Intrusion-tolerant routing for wireless sensor networks," *Computer Communications*, vol. 29, no. 2, pp. 216–230, January 2006.

[125] B. Przydatek, D. Song, and A. Perrig, "Sia: secure information aggregation in sensor networks," in *SenSys '03: Proceedings of the 1st international conference on Embedded networked sensor systems.* New York, NY, USA: ACM, 2003, pp. 255–265.

[126] T. Park and K. G. Shin, "Soft tamper-proofing via program integrity verification in wireless sensor networks," *Mobile Computing, IEEE Transactions on*, vol. 4, no. 3, pp. 297–309, 2005. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1413187

[127] A. Seshadri, M. Luk, A. Perrig, L. van Doorn, and P. Khosla, "Scuba: Secure code update by attestation in sensor networks," in *WiSe '06: Proceedings of the 5th ACM workshop on Wireless security.* New York, NY, USA: ACM, 2006, pp. 85–94.

[128] Z. Shen and J. P. Thomas, "Security and qos self-optimization in mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 7, no. 9, pp. 1138–1151, 2008.

[129] T. Pazynyuk, J. Li, G. S. Oreku, and L. Pan, "Qos as means of providing wsns security," in *ICN '08: Proceedings of the Seventh International Conference on Networking (icn 2008)*. Washington, DC, USA: IEEE Computer Society, 2008, pp. 66–71.

[130] M. Johnson and F. Stajano, "Usability of security management: Defining the permissions of guests," in *Proceedings of the 14th Security Protocols Workshop*, Cambridge (UK), 2006.