Ad Hoc Wireless Sensor Networking: Challenges and Issues

Danilo Blasi(1), Vincenzo Cacace(1), Luca Casone(1), Marco Rizzello(1), Salvatore Rotolo(1)
Luciano Bononi(2)

(1) STMicroelectronics
(2) Department of Computer Science, University of Bologna, Italy

Wireless Sensor Networks (WSN) constitute an emerging application field of microelectronics that promises wide support of the interaction between people and their surroundings.
Because of the extremely variable nature of this interaction, the topic of WSN is still in its early stages of development and is giving rise to several challenges, from the design of a smart device that allows easy and reliable access to the environmental characteristics, to the creation of a wireless network of devices that cooperate to perform complex tasks. In this field, the cooperation among nodes is the most peculiar aspect reflecting directly on the network operation.
This paper gives an overview of the topic from the Ad Hoc networking concept perspective. Although the seeds of these concepts can be found in some already existing implementations (e.g., ZigBee), we believe many further refinements could be introduced to fully exploit the potential of the widely investigated Ad Hoc approach and the strength of the mutual

1. INTRODUCTION

It is easy to recognize the main changes of our daily life caused in the past decade by the effect of the 'marriage' of computation and communication technologies.

The synergy resulting from such a combination is producing a powerful technological push: the Wireless Sensor Networks (WSN) is emerging as the new revolution that will make a reality the vision of people like Gordon Bell and Mark Weiser [1], who envisaged the ability of microelectronics to form new computer classes and the capability of networking to support the Pervasive – or, Ubiquitous – Computing, i.e., the idea of integrating computation and communication into the environment, allowing the seamless interaction of computing entities with people in a 'natural' and 'automatic' way.

The potential of the WSN concept simply lies in the three words composing the acronym itself: '*Wireless*' puts the focus on the freedom that the elimination of wires gives in terms of mobility support and ease of system deployment; '*Sensor*' reflects the capability of micro-/nano-technology to provide the means to perceive and interact – in a wide sense – with the world; '*Networks*' gives emphasis to the possibility of building systems whose functional capabilities are given by a plurality of communicating devices, possibly distributed over large areas.

In this paper, we concentrate directly on the keyword 'Network,' presenting a general overview of the topic and identifying the main challenges that still require solutions for the effective introduction of some real innovation. Given the WSNs' peculiarities, which make them quite different from traditional (wired and wireless) networks, real, effective solutions may only be designed by exploiting the *cooperation* among many elements, i.e., the potential resources of each single network's member can be aggregated and organized to implement multifaceted features and to perform complex operations. In the 'network' perspective, this design approach leads to the 'Ad Hoc' networking approach [2].

Ad Hoc networks are commonly defined as a kind of general, infrastructure-less, cooperation-based, opportunistic network, possibly customized for specific scenarios and applications, as the Latin expression 'Ad Hoc' indicates something which is tailored to a given matter. This networking approach has to face frequent and random variations of many factors (radio channel, topology, data traffic, etc.), implying the dynamic management of a large number of parameters in the most efficient, effective, and reactive way.

To this end, a number of key research problems have been studied (and solutions have been proposed) by Ad Hoc networking researchers:

– self-configuration and self-organization in infrastructure-less systems;
– support for cooperative operations in systems with heterogeneous members;
– multi-hop peer-to-peer communications among network nodes;
– network's self-healing behavior providing a sufficient degree of robustness and reliability; and
– seamless mobility management and support of dynamic network topologies.

In the following sections, we will discuss more details of the Ad Hoc networking concepts applied to WSNs. In Section 2, we sketch the architecture of a generic WSN node, just to highlight some peculiarities – quite different from typical elements of a data network – that directly impact the networking operation. In Section 3, we investigate the most important requirements emerging on the basis of the communication features of WSN networks, and we show how an Ad Hoc approach could apply to specific applications, in terms of communication model and traffic characterization. Section 4 identifies some 'added values' of the WSN networking features. Section 5 illustrates some of the state-of-the-art solutions and offers a short perspective on what the proposed standards have already captured. Conclusions are reported in Section 6.

2. DEVICE FEATURES

A possible simplified functional architecture of a generic WSN device can be found in [2] and is shown in Fig. 1.

Altogether, the illustrated components form a complex system which can be configured according to a wide set of application

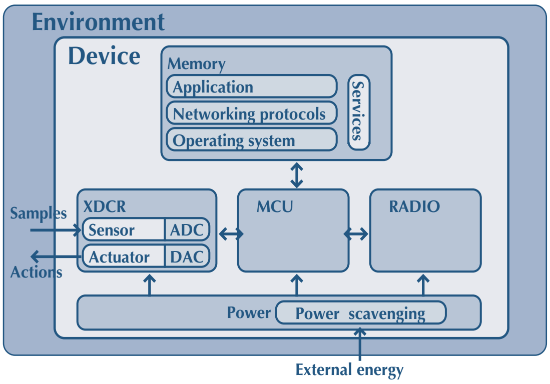

Figure 1: The functional architecture of a WSN device.

requirements. By means of a *transducing unit* (XDCR), which may host multiple kinds of sensors and/or actuators [3], the device interacts with the surrounding environment by collecting 'samples' of environmental characteristics (e.g., temperature, humidity, pressure, etc.) and by causing 'actions' (e.g., air conditioning, light level adjusting, fire alarming, etc.). A *processing unit* (MCU) controls the overall system and manages the procedures that make the device collaborating with the other network members to carry out the assigned tasks.

A *memory unit* stores all processed data, networking control information, and the code to be executed by the MCU (e.g., application, networking protocols, operating system, services), thus providing the device with direct access to the information it needs. A *radio interface* unit connects the device to the network through the wireless channel and makes it able to share information with its peers via packets' exchange. The whole system is usually powered by a battery pack that might be recharged by additional ambient power scavenging units such as solar cells.

Besides flexibility, common WSN applications demand low cost devices, imposing severe constraints on the system design and configuration.

Typical WSN devices could be as large as coins, possibly resulting in limitations of processor power and memory. Moreover, they are often expected to be untethered, which emphasizes their capability of saving energy while allowing the completion of network operations. Furthermore, given the need for such devices to be used in hostile environments, the robustness of these devices becomes a central issue.

The kind of operations WSN devices may participate in when networked depends on the solutions to the above issues, as will be illustrated in the following sections. In this paper, we point out the two key factors that most differentiate WSNs from other data networks: the *application dependency*, which mainly impacts the communication features, and the *Ad Hoc networking approach*, which specializes in the monitoring and control contexts.

3. COMMUNICATION FEATURES

WSNs are operated for 'instrumenting' their surroundings [4]. They typically count on a large number of devices that are able to detect and/or react to external stimuli associated with events or objects of interest. As already mentioned when we introduced the concept of *cooperation*, these devices, when networked, may work together to perform complex monitoring and control tasks, depending on the intended application (e.g., the devices may be demanded to report simple detections of the presence of a moving object or the number of such kind of detections performed in a predefined time interval). The application dependency, combined with other peculiarities of WSNs (wireless channel usage, device heterogeneity, device redundancy, to name a few), impacts on the network communication model (i.e., the roles assumed by devices in the communication context, the rules adopted for information gathering and distribution) and on the characteristics of the data/control traffic injected into the network.

3.1 Communication model

Users of a WSN are likely interested in gathering information about environmental conditions, current events, objects, or living beings as well as in remotely enabling a conditioning system located inside some possibly hazardous place to regulate its environment's characteristics. Monitoring and control tasks can be *data centric*, that is, they could aim to react to the existence of a given set of information rather than being triggered by *who* produces some portion of the information set. This consideration becomes more relevant when taking into account that device redundancy is normally exploited to improve accuracy and reliability of the network operations; for instance, the correctness of a metering procedure can benefit from the collection of correlated data coming from multiple devices, in terms of both data availability (e.g., active originators may be replacing failed ones in producing data) and measure settling (e.g., mean of different samples). On the other hand, deploying a large number of transducing devices in a region for the purposes previously described would make the reference to each single network's member (e.g., address) less relevant. This is because it contributes to operating the network without being essential for that; in other words, the single device may become ‘anonymous’ in the communication context.

This line of reasoning distinguishes WSNs from traditional networks in the characterization of the *communication paradigm*; the *address centric* approach used in end-to-end transmissions between specific devices, with explicit indication of both source and destination addresses in each packet, could be replaced with an alternative (and somewhat new) *data centric* approach [5], [6]. Perhaps, a straightforward effect of such ‘address blindness’ would be related to the choice of the most suitable data diffusion strategy for data centric networks. As an example, in a WSN, a great amount of similar data (i.e., highly correlated samples) might be produced by multiple sensor devices that are reporting the occurrence of a common phenomenon. In a well-known data centric technique called *in-network aggregation* [5], [6], rather than separately propagating these data items to data consumers, redundant data items may be aggregated, depending on the target application, as they are flowing through the network, so that considerable energy and bandwidth savings can be achieved.

These considerations may lead designers to model this kind of network as a sort of distributed data repository where anonymous devices may behave as data originators (also denoted as *sources*) and/or data recipients (also denoted as *sinks*), depending on many factors (e.g., application requirements, device capabilities, and device resources). The typical network deployment would consist of the sources placed around the areas to be monitored and the sinks near easily accessible places, the sinks provided with adequate storage capacity to hold the data from the sources. Sources may send information to sinks in accordance with different scheduling policies: periodic (i.e., *time-driven* mode), event specific (i.e., *event-driven* mode), a reply in response to requests coming from sinks (i.e., *query-driven* mode), or some combination thereof [7]. It is worth noting that, if the sources are unaware of identities of the sinks (as would be the case with the data centric communication paradigm), their data will be ‘flooded’ over the network, eventually reaching their recipients. Conversely, if the sources know the sinks’ addresses, data packets can include such information to be forwarded only to their intended destinations.

Finally, a ‘mixed’ communication paradigm, which is data-centric (i.e., one based on anonymity) at the source side and address-centric at the sink side, can be defined for WSNs. To the best of our knowledge, such a mixed communication model has not been defined or investigated in the literature. A sink might publish its interest in data by issuing a query packet and by attaching its address so that every receiving source would be able to refer to it. Queries might also bring time or event indications along to give instructions about the data transmission scheduling to the receiving sources; in this way, time-driven and event-driven scheduling policies would be specializations of the query-driven one and thus allowed.

In the *mixed model*, the efficiency of data delivery obtained by limiting it only to the interested collectors would not be exploitable in any way for the query distribution, as it is not supposed to differentiate among anonymous sources. Nevertheless, for most applications, the sinks’ interest should be directed towards sources located inside specified target regions, for instance, lamp switches in a building room [6], [8]. To allow this to occur, queries might somehow specify their target regions so that every receiver of a query packet might determine whether or not it belongs to the reported target region, or, in other terms, whether or not it is a candidate source with respect to that query. Obviously, with these assumptions, the adoption of a localization system that enables devices to know their current position (see Sec. 3.3) becomes mandatory.

3.2 Traffic characterization

One of the key aspects of WSNs is the possibility of easily tasking sensor devices to produce information about a certain phenomenon by giving them the necessary instructions about the type of information to be produced, the type of actions to be taken for getting that information, and the time-plan for the reports' production. In addition, a general agreement among all network members on the coding of the above instructions/information would ease the system control and increase the efficiency; in other words, adopting the terminology used in [6], data and/or control messages in WSNs should be *named*, that is, structured by the aggregation of 'attribute-value' pairs that all network members can interpret. To this end, all devices should refer to the same *code-book*, locally stored as a reference, defining a list of attributes (e.g., type of event, position, time, intensity, accuracy, etc.) and their respective set of valid values. Besides defining a common 'language,' the naming techniques could be exploited for allowing in-network aggregation (introduced in the Sec. 2.1) of multiple data with respect to some common attributes.

The benefits of the in-network processing, the need for saving limited network resources, as well as the utility-based filtering of information to be transmitted would make preferable the extraction of essential features from detected phenomena, instead of detailed reproduction. For example, a video coming from a camera (e.g., for detecting intruders or fire) could be as helpful as a simple signal sent to the control system, but it would require more resources and a more complex transmission management.

Consequently, WSNs are not commonly expected to carry multimedia data flows or, in other words, sequences of time-correlated information that cannot be handled one at a time. Nonetheless, some kind of quality of service (QoS) support should be provided for managing 'time critical' data (e.g., fire alarms) whose delivery may require upper bounded time interval (i.e., latency). To meet such a requirement, transmission scheduling solutions for preventing the network congestion which would cause unacceptable delivery delays should be addressed, even by considering that congestion may be frequent in WSNs, due to several factors (e.g., use of a shared wireless medium, limited bandwidth and buffer size, high level of local contention, and the multi-hop nature of WSN) that are discussed in Sec. 4.

3.3 A key service: the Localization system

The location information management is an essential feature in most WSN applications [2]. In most cases, the data gathered by devices are really useful if and only if they are stamped with location and time information; for example, a temperature value without indication of where and when it was detected is considered meaningless.

The location information could be exploited for both application and networking scopes, for example, to gather data from a specified geographic zone, as already described in Sec. 3.1. According to the mixed communication model, an efficient routing protocol might introduce some smart rules for delivering queries only to nodes inside target zones, and corresponding data only to queries' originators, respectively [6]. Discovery and tracking services (e.g., people, assets) are possible examples of location-enabled application functionalities required in industrial scenarios.

The location information should be reliable and available, no matter where the device is placed. Technologies such as the Global Positioning System (GPS) [9] could be used to obtain the location information needed, but they may be sensitive to external disruptive factors or to physical obstacles, regardless of any considerations about costs and power consumption. A similar reasoning can be extended to the use of a centralized location information database, which may not be fault-tolerant enough when implemented by one single location server. Hence, the aim of achieving robustness may suggest building up a distributed or replicated localization system [10].

Besides reliability and availability, another main feature of the localization system is its accuracy. Again, a GPS without signal corruption provides quite accurate absolute location information. Alternatively, under less favorable conditions, the accuracy should be evaluated in relation to the *ranging* capability of devices. This consists of making devices able to estimate the distance from their *neighbors* (i.e., devices able to exchange data packets directly) on the basis of measurements of the received signal strength and/or the propagation time (e.g., *time of arrival*, ToA) of predictable control signals. Ultra Wide Band (UWB) [11] – the impulse-radio version [12] – is an example of technology that can provide high ranging accuracy by estimating the round trip time between transmitter and receiver. A number of such technologies and solutions are presented in literature [10]; methods based on triangulation allow 'blind' devices to infer their position from the collection of measurements obtained by assuming the knowledge of reference points, called 'anchors', even for devices without ranging capability [13].

4. NETWORKING FEATURES

WSNs are a class of wireless networks that may be generally conceived in two different topologies, i.e., *star* and *mesh* [14]; the former is basically a one-hop topology, where all terminals communicate with a central node, while the latter refers to the most general multi-hop topology, where multiple nodes implement a distribution system for data communication among wireless terminals.

The focus of this paper is on mesh-configured networks. Such kinds of network can be 'self-contained' when information/ commands generated by nodes/terminals are directed towards resident nodes/terminals; nevertheless, gateway nodes may be provided to allow connections with the 'external world' – e.g., Internet. Mesh-configured WSNs are supposed to have no need of any fixed, centralized management infrastructure, while they are instead to rely on the adoption of the cooperation-based *Ad Hoc* networking approach [2, 15]. Each node, besides being a sensing or actuating device, may act as router, at which point it is able to receive packets generated by other devices and forward them to the next hop along a multi-hop path towards their final destination.

Therefore, each device has to multiplex (share) the available link bandwidth with all active neighbors. Because the WSN density and utilization needs may be high, the bandwidth may be negatively affected. On the other hand, WSNs are not expected to be communication intensive at the application layer, as their devices are expected to have low communication duty cycles, reducing the average long-term per-device bandwidth requirement [16].

While the traffic bandwidth requirement is not the main WSN networking issue, the *reliability* is strongly expected to be fulfilled [2]. Any WSN is deeply involved in and related to the monitored environment, and any change occurring to the surroundings will significantly influence its performance; nevertheless, the network must be able to tolerate and 'survive' any change by implementing proper reactions and adaptation mechanisms sustaining communications for both sensed data and commands. In order to comply with the *self-working paradigm*, a WSN should implement a set of viable WSN management guidelines, including:

- *self-configuration*, i.e., the ability to automatically and autonomously set relevant parameters to operate according to some given specifications;
- *self-organization*, i.e., ability to detect the presence of the other network devices and to modify the working behavior, accordingly;
- *self-adaptation*, i.e., ability to automatically interpret feedback information and to adjust optimal settings to well operate in the environment; and
- *self-healing*, i.e., ability to detect devices' and links' failures, by providing autonomous reactions to restore operating conditions – *without human intervention*.

To obey the self-working paradigm, WSN protocols should be designed with strong attention to both *device coordination* and *redundancy exploitation* issues, both of which might have to cope with the network member resource heterogeneity.

4.1 Heterogeneity exploitation

Network node heterogeneity will involve both hardware and software.

Possible hardware differences include the transducing capabilities, computational power, storage room, power supply (e.g., power line, battery), and many others. Being somehow complementary to the redundancy, the *hardware heterogeneity* can be exploited to improve the way the whole network's resources are used, thus helping to improve the network's resilience to failures and prolonging the whole system lifetime. The *resource awareness* can be a good guideline to follow in the protocol design process. Basically, it may govern the assignment of the most important and critical network management roles (e.g., router, gateway, coordinator, etc.) to the devices with the greatest number of resources; further, it may improve the energy consumption optimization by allowing dynamic transmission power adjustments or packet exchange rate minimization.

Greater availability of hardware resources on any device may be translated into the possibility of putting on that device more computation intensive codes (e.g., protocol stack, application programs) – i.e., the hardware heterogeneity may turn into *software heterogeneity*. For instance, similarly to what has been already proposed by the IEEE 802.15.4 group [14], WSN devices may be classified into *terminals* and *nodes*: terminals can be identified as the network's 'users', or 'end points', so that they can act as source and/or sink only and participate in a restricted set of network operations; conversely, nodes are meant to run the full set of networking functionalities (e.g., coordination, address assignment, packet relaying, etc.). Altogether, the nodes form a distribution system for packets coming from or directed to terminals, while simultaneously giving them the possibility to access the network services. Software heterogeneity should be considered while dealing with the devices' coordination, since it puts some ties on the way nodes can share their functionalities; for instance, any failed node can be replaced only by another one having similar resources. Moreover, it could require smart capabilities sharing policies, since the network may potentially provide several functions, though widely "scattered" throughout itself.

4.2 Device coordination

Device *coordination* is the way the network may achieve both self-configuration and self-organization. Basically, it means that devices have to work together to make the network effective. Even if coordination may be achieved through either centralized or distributed protocols, the latter are usually preferable; in fact, distributed approaches, despite being less efficient, are likely more fault-tolerant and, therefore, more suited to the typical WSN scenarios.

Distributed protocols could be partially supported by pseudo-centralized management and coordination schemes even in the absence of any fixed infrastructure, by making devices able to self-organize into some form of stable hierarchy. This is the case of the *clustering algorithms* (see, for instance, the ZigBee Cluster-Tree organization [17], or Ref. [18, 19]), where some nodes may be elected to play a leading role such as the cluster-head. The clustering concept is differently applied to WSNs with respect to address-centric networks, according to the used communication model (see Sec. 3.1). For instance, cluster-heads may be their clusters' representative (e.g., the cluster identifier is set to the cluster-head's one) [3] in networks where member addressing is needed, while they are often used to perform data in-network aggregation to decrease the number of transmitted messages in WSNs [20]. The advantage of clustering can be better exploited under the distributed management and coordination viewpoint when such algorithms are smart enough to assign leading roles to devices having more capabilities and resources than others (see Sec. 4.1). In case of node failures and/or topology changes, clustering algorithms must be able to dynamically perform 'cluster re-organization' procedures by adapting the role assignment. For example, [20] suggests a randomized rotation of the role of the cluster-head so that uniform energy dissipation due to data collection and merging is obtained. In addition, the clustering scheme should be properly assisted and considered in the cross-layered design of network communication protocols t6 cope with resources, stability, and performance issues [19]. Hence, WSN coordination functionalities must not rely exclusively on a single device (or a static group of devices) so that the effectiveness of the operations can be preserved also under conditions of failure.

Two factors have to be taken into account while dealing with the distributed protocol design process, namely the *network dimension* and the *network topology dynamics*. The former, easily appreciable through different system parameters (e.g., number of nodes, network extension, node density, etc.), is very important while assessing the protocols' *scalability*, i.e., their ability to tolerate performance degradation 'smoothly', and thus acceptably, when the network's dimension grows [21]. The latter tells us how fast the network topology is prone to change because of the occurrence of disruptive events (e.g., failures of nodes running out of energy, mobility, variable channel conditions, etc.), which impacts the ability of protocols to maintain their correct working behavior.

4.3 Redundancy exploitation

Redundancy exploitation means designing protocols able to take effective advantage of the existence of multiple information sources, network devices, routing paths, and so on. Networking protocols, to be properly deemed as self-healing and self-adapting, should be capable of smartly and dynamically choosing among several available resources; in case some resources become unavailable, the protocol must be able to select and to start using the remaining ones.

Many examples of redundancy exploitation can be found among routing solutions for WSNs. Reference [22] proposes an energy-aware routing protocol that maintains a set of paths alternately used to convey data packets so that the energy budget of any single path will not be depleted quickly. In [6], the Directed Diffusion strategy performs in-network aggregation of redundant data coming from different sources, building up a robust routing mesh that gets data from multiple sources to multiple sinks. Reference [23] proposes a variant of Directed Diffusion called Gradient-Based Routing. Its key idea is to allow network devices to know the hop distance from a common sink and to force data to pass through nodes with decreasing distances until the data is delivered to the sink; exploiting the typical high density of WSNs and the likely presence of multiple relayers with the same distance from the sink, the forwarding process becomes highly reliable. Device redundancy is exploited also by some MAC schemes. GeRaF [24] is a technique that integrates routing, MAC, location awareness, and topology management to forward packets just towards their intended destinations. In this scheme, a node calculates its priority in acting as a relayer of a received broadcast message on the basis of its position towards the final destination; thus, a set of best positioned nodes may volunteer to relay the message, possibly originating multiple paths to be followed.

As the resource unavailability is more likely to occur as a consequence of node failures – e.g., node breakages or energy depletion – the management of such failures is a main issue in WSNs. A failure classification is thus helpful here, as it allows for a better understanding of which management policies are required to handle them. A straightforward categorization can split them between *predictable* or *unpredictable* ones. The former require an *explicit signaling* approach to anticipate correct actions before the failure occurrence; the latter can be handled only through *reaction-based* (adaptive) mechanisms, as failures occur in an unpredictable way. Given that the unpredictable events in WSN scenarios are likely to occur more often than the predictable ones, the self-adapting and self-healing capabilities are expected to be more effectively supported by a reaction-based (i.e., adaptive) mechanism. This policy may then realize an acceptable trade-off between simplicity and efficiency issues with both kinds of events.

5. SOME 'AD HOC CONCEPTS' IN THE EXISTING STANDARDS

Today's users, industrial, professional, or consumer, are maturing in their awareness of and practice in the adoption of pervasive computation and communication systems like WSNs. The 'sensor and control arena' has been enriched by a wide range of possible choices, which unfortunately are mostly composed of many proprietary solutions that are almost incompatible. Standardization efforts are generally a positive factor in moving producers and vendors to concrete actions for developing largely reusable and interoperable components and/or devices, with benefits in terms of time to market, reliability, and cost reduction for users. Without standards, which require us to put 'progress' ahead of 'self-interest', there would be no mass production or mass communication and, as such, no modern economy and progress.

In the WSN field, several standard efforts have been started recently; most of them have been in evolution for several years and are now beginning to have market impact that will grow over the next few years. There are standards related to wireless communications and sensor management promoted by the *Institute of Electrical and Electronics Engineers* (IEEE) and those focusing on the application scenarios promoted by *Industrial Alliances*. We will consider only the networking-related standards, starting from a short description of *IEEE 802.15.4* that addresses the lower layers of the ISO/OSI networking reference model for wireless personal area networks (WPAN). Then, we will introduce *ZigBee*, based upon *IEEE 802.15.4*, as an industrial standard technology for providing both network and application management with enlarged capabilities obtained by taking up some of the solutions to the typical challenges of the Ad Hoc networks; these will be highlighted along with a short description of ZigBee's main peculiarities.

5.1 IEEE 802.15.4

The IEEE 802.15 working group defines the physical layer (PHY) and the medium access sub-layer (MAC) for low-complexity, low-power consumption, low bit-rate WPAN connectivity; currently, among the four IEEE 802.15 different frameworks, the IEEE 802.15.4 is considered the most relevant for WSN scenarios.

A global RF standard for WSN is fundamental because it would accelerate the technology evolution by identifying leading directions, and it could yield benefits such as the lowering of design costs and the interoperability at the communication level. Moreover, at the raw physical level, standards have to cope with the issue of frequency band allocation. Different regulations in different regions of the world should not be a problem for most applications, whereas the most used wireless technologies, including all those suitable for WSNs, fall in the ISM bands; this could bring the advantage of interoperability but also a concentration of technologies, with possible problems for the coexistence of different wireless systems.

Nevertheless, the available frequencies are only the starting point for operating wireless links. In order to make equipment, software, protocols, and applications, all made by different manufactures, interoperable, the industry needs to set standards. The IEEE 802.15.4 Standard [25], approved in 2003 and amended in 2006 with a "b" version, is contributing to all of these aims, and several compliant products are already available on the market, even if more as development kits only than real end-products. The standard provides for a low bit-rate (i.e., up to 250kbps, or 1 Mbps in "b" version) connectivity in the *Personal Operating Space* (POS), typically 10/100 meters, through 27 RF channels in the ISM RF bands, in order to guarantee wide adoption in several market segments worldwide.

The most innovative IEEE 802.15.4 feature is the full support of *mesh networks* for battery powered nodes, through the classification of devices into two different types – i.e., Full Function Device (FFD) and Reduced Function Device (RFD). An IEEE 802.15.4 network should include at least one FFD operating as the PAN coordinator for special (but not centralized) functions, whereas all the other FFDs would contribute to realize the WSN backbone; RFDs, which are usually intended as the 'leaf' nodes of the WSN spanning tree, perform simple tasks more related to sensing than networking. An RFD can communicate only to one FFD, while an FFD can communicate to both RFDs and FFDs.

This asymmetry of roles arises from the fact that RFDs have minimal resources (energy and memory) and basically act as 'parasites' of FFDs functions by limiting working activity to (typical) 1% duty-cycle.

As anticipated, the Standard has recently come out of revision, introducing simplifications to the overall architecture and resolving some design ambiguities and inconsistencies, while improving interoperability worldwide. Concurrently, under development is IEEE 802.15.4a, which essentially regulates the use of UWB physical medium with enhanced technical and protocol specifications, thus allowing high bit-rate transmissions and new management features like ranging/localization (described in Sec. 3.3).

5.2 ZigBee

On the basis of the current IEEE 802.15.4 specifications, a consortium of more than 200 companies is negotiating and working on the adoption of an industrial standard called ZigBee, whose name and working principle is inspired by the social behavior of bees that work together to tackle complex tasks. ZigBee exploits cooperation to allow for the multi-hop exchange of messages, as described in Sec. 4, and adds the logical network, security, and applications management on top of the referenced IEEE 802.15.4 standard by defining the upper layers of the protocol stack, from network to application (see Fig. 2). In addition, ZigBee defines *application profiles* [17], which refer to a set of template-based description of device configurations, each one specialized for working to a common cooperative and distributed application. Aside from its technical aspects, one of the main tasks of the ZigBee Alliance is to certificate interoperability among devices made by different manufacturers, thus expanding their potential adoption.

Technically speaking, ZigBee is a fairly good standardization effort that is gaining wide acceptance of big players, but it is currently subject to several refinement attempts, which would risk reducing its market momentum. The first official release of the standard, known as “ZigBee v.1.0” and dated December

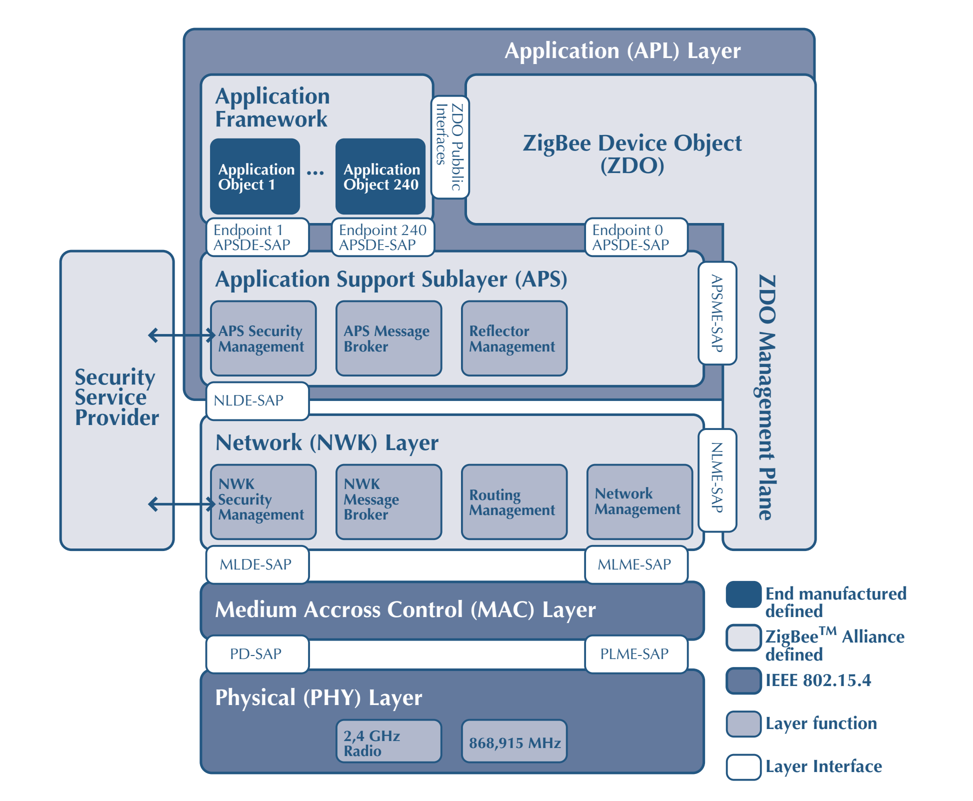

Figure 2: The ZigBee protocol stack.

2004, is currently shipped by many platform providers. It is typically referred to as the “Home Control” version of the stack. Unfortunately, its lifetime is marked, and it is changing in a non-backward-compatible way, while maintaining the overall skeleton. For the time being, the Alliance has decided to propose ZigBee in two flavors: a base version featuring the Home Automation market only, named “ZigBee”, which is an enhancement of the “old v.1.0,” and a “ZigBee Pro” version, most likely available starting in 2007, which will incorporate several features we listed in the previous sections.

The new releases improve ZigBee networks’ scalability and performance through full support of mesh networking, abandoning the hierarchical organization of the “old v.1.0” known as “Cluster-Tree,” and bringing in the so-called “many-to-one routing” feature, which allows a concentrator (a gateway or more generally a sink) to establish routes from all nodes in the network without large increases in route table size and without creating a broadcast storm within the network.

This is a first step in the direction of a data centric paradigm (see *mixed mode* in Sec. 3.1), which, together with the support for “multicast,” will fill the gap with the 802.15.4b added support. Even more relevant is the new “alternate addressing scheme,” which will replace the tree organization by stochastically assigning the network level addresses and resolving conflicts where originated. This will result in a lighter management of addressing issues – as the address of the node will no more depend on its physical position on the tree – enhancing the scalability and thus allowing pure mesh topologies as well as node mobility.

The concept of reliability is hence strengthened by mesh networking because its many different and dynamic paths could be exploited for routing. The “frequency agility” feature enhances reliability as well. Starting from the assumption that the channel and the entire RF band conditions can vary dynamically in both time and space, this feature will allow the operation to continue reliably and in an unattended way in the presence of well-known interference sources, like WiFi or Bluetooth, or in the presence of an unusable operating channel as well. This is a big step towards the *self-working paradigm* (see Sec. 4).

The heterogeneity exploitation is also being considered for the 2007-later on versions, by adding features like “end-device management” and “battery powered routers”, allowing, respectively, the employment of battery-powered devices as leaf nodes - by designating the relevant parent router as a proxy - and even permitting the deployment of battery-powered router nodes, given that in the current version they are supposed to be ‘mains’ (i.e. line) powered.

If all these are networking add-ons that will differentiate “ZigBee Pro” from previous versions, two important enhancements will have been produced at the application level, starting from the “ZigBee” stack. The old mechanism used to describe and identify the application profiles has been updated with the new “ZigBee Cluster Library (ZCL),” which can be imagined as a code-book (see Sec. 3) where all devices, classified on the basis of functional domains, have been described in terms of their attributes/properties in an application-independent fashion; as an example, the same description for a temperature sensor can be adopted even if it will be used in a Home or Industrial Automation application.

All these are only a part of the discussed features in the ZigBee Alliance. This can be expected, given that such an organization counts several members with different strategies and requirements, such as OEMs as well as application-oriented and semiconductor companies. Now momentum has come, and 2007 will be the year expected for launching ZigBee to the mass market. At the same time, ZigBee will continue to enhance its capabilities; mobility management, location awareness, QoS, power awareness, network-wide and time synchronization, and new routing strategies will be the ZigBee response to the classical Ad Hoc paradigm challenges.

6. CONCLUSIONS

WSNs are an emerging application field that deserves the great attention of the microelectronics industry and research. This paper presents an overview of WSNs with special focus on networking challenges and issues due to the peculiarities of such networks, mainly identified as application-dependency and natural demand for the 'Ad Hoc' approach. ZigBee / IEEE802.15.4 promises this kind of network availability in a fairly short time, but, in our opinion, further steps still need to be taken before making WSNs truly user-friendly.

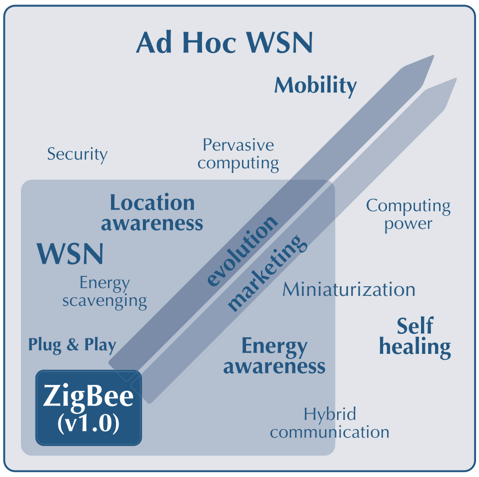

Figure 3: Challenges and issues of WSNs.

The bubble diagram in Fig. 3 provides a list of main issues that the natural technology evolution and the market raise. Some of them have already been tackled by ZigBee / IEEE802.15.4, while some others are still representing challenges for academic and industrial researchers, in both the fields of general and Ad Hoc WSNs.

According to recent marketing reports such as those found in [26], today's wireless sensor industry is being driven by customer demand for reliability, simplicity, price and availability, independent of the standardization processes, whose advancement is often limited by external influences and political or strategical issues. This can be seen today in the home automation market, where leading companies are simply and readily reacting to customer needs, while the standards often adapt to the market-based process. The companies with the products that solve real customer needs and desires in a timely manner will likely become the standard in the home market.

The recent partnership between ST and Ember Corporation [27] will enable ST to become one of the leading providers of the ZigBee networking systems. However, ST has also started thinking about the next generations of WSN devices in order to preserve its competitiveness while gaining a competitive advantage by adding improvements at the device and software levels. In this sense, STMicroelectronics contributes to the growing knowledge of WSN solutions, continuously fed by relationships with the academic world. Distributed localization algorithms, geographical routing, and fairness and congestion control at MAC layer are only some of R&D areas under investigation, areas whose importance has been extensively pointed out in the paper.

REFERENCES

[1] M. Weiser, "The Computer for the 21st Century," Scientific American, 265(3), pp. 94-104, 1991.

[2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "A survey on sensor networks," IEEE Communications Magazine, 40(8), pp. 102-114, 2002.

[3] D.J. Baker, A. Ephremides, and J.A. Flynn, "The design and simulation of a mobile radio network with distributed control," IEEE J. Sel. Areas Commun., Sac-2(1), 226, 1984.

[4] D. Estrin, L. Girod, G. Pottie, and M. Srivastava, "Instrumenting the World with Wireless Sensor Networks," Proc. of ICASSP, 2001.

[5] B. Krishnamachari, D. Estrin, and S. Wicker, "Modeling Data-Centric Routing in Wireless Sensor Networks," Proc. of IEEE Infocom, 2002.

[6] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva, “Directed Diffusion for Wireless Sensor Networking,” Proc. of IEEE/ACM Transactions on Networking, 11(1), 2003.

[7] Y. Yao and J. Gehrke, “The Cougar Approach to In-Network Query Processing in Sensor Networks,” Proc. of SIGMOD, 31(3), 2002.

[8] Y. Yu, D. Estrin, and R. Govindan, “Geographical And Energy-Aware Routing: A Recursive Data Dissemination Protocol For Wireless Sensor Networks,” Technical report UCLA-CSD TR-01-0023, 2001.

[9] “Navstar Global Positioning System Surveying,” ASCE Publications, Technology & Industrial Arts, 2000.

[10] N. Patwari, J.N. Ash, S. Kyperountas, A.O. Hero III, R.L. Moses, and N.S. Correal, “Locating the Nodes - Cooperative localization in wireless sensor networks,” IEEE Signal Processing Magazine, pp. 54-69, 2005.

[11] M.G. Di Benedetto and G. Giancola, “Understanding Ultra Wide Band Radio Fundamentals,” Prentice Hall Communications Engineering and Emerging Technologies Series, 2004.

[12] IEEE 802.15 WPAN Low Rate Alternative PHY Task Group 4a (TG4a)

[13] D. Niculescu and B. Nath, “DV Based Positioning in Ad Hoc Networks,” KLUWEIR Journal, 2003.

[14] http://standards.ieee.org/reading/ieee/std/lanman/restricted/802.15.4-2003.pdf

[15] S. Rotolo, D. Blasi, V. Cacace and L. Casone, “From WLANs to Ad Hoc Networks, a new Challenge in Wireless Communications: Peculiarities, Issues and Opportunities,” in Handbook Of Wireless Local Area Networks: Applications, Technology, Security, and Standards, CRC Press, pp. 2.15-154, 2005.

[16] E.H. Callaway, **Wireless Sensor Networks – Architectures and Protocols**, Auerbach Publications (CRC Press), 2004.

[17] ZigBee Alliance internal documents (http://www.zigbee.org)

[18] D. Simplot-Ryl, I. Stojmenovic and J. Wu, “Energy-Efficient Backbone Construction, Broadcasting and Area Coverage in Sensor Networks,” in Handbook of Sensor Networks: Algorithms and Architectures, John Wiley & Sons Inc., pp. 343-380, 2005.

[19] L. Bononi, M. Di Felice, L. Donatiello, D. Blasi, V. Cacace, L. Casone, S. Rotolo, “Design and Performance Evaluation of Cross Layered MAC and Clustering Solutions for Wireless Ad Hoc Networks,” Performance Evaluation 63 (2006), Elsevier, pp. 1051-1073

[20] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “Energy-Efficient Communication Protocol for Wireless Micro sensor Networks,” Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS ‘00), 2000.

[21] F. Martincic and L. Schwiebert, “Introduction to Wireless Sensor Networking,” in Handbook of Sensor Networks: Algorithms and Architectures, John Wiley & Sons Inc., pp. 1-40, 2005.

[22] R. C. Shah and J. Rabaey, "Energy Aware Routing for Low Energy Ad Hoc Sensor Networks," IEEE Wireless Communications and Networking Conference (WCNC), 2002.

[23] C. Schurgers and M.B. Srivastava, "Energy efficient routing in wireless sensor networks," MILCOM Proceedings on Communications for Network-Centric Operations: Creating the Information Force, 2001.

[24] M. Zorzi and R. R. Rao, "Geographic random forwarding (GeRaF) for ad hoc and sensor networks: energy and latency performance," IEEE Transactions on Mobile Computing, 2(4), 2003.

[25] IEEE Std 802.15.4™-2003 Standard: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs).

[26] K. West, "Wireless Sensor Technology and Market Tracking Service: ZigBee, ZWave, Insteon, RFID, IEEE 802.15.4 and their Competition," Report abstract WTRS, 2005.

[27] http://www.ember.com/

■ Contact: st.journal@st.com ■