

# Wireless Sensor Networks: The Biggest Cross-Community Design Exercise To-Date

Mischa Dohler\*

Senior Expert, France Telecom R&D, 28 Chemin du Vieux Chêne, 38243 Meylan Cedex, France

Received: April 24, 2007; Accepted: May 3, 2007; Revised: May 24, 2007

**Abstract:** Within academia, wireless sensor networks have witnessed a tremendous upsurge in the last decade, which is mainly attributed to their unprecedented operating conditions and hence unlimited research challenges. Within industry, the projected business opportunities are huge with, e.g. according to Frost & Sullivan, an expected market size of approximately \$2b by 2012 at a compound annual growth rate of 41.9%, therefore causing the interest in this technology to augment dramatically. Due to the unique design constraints, however, none of the grand communities - such as computing, telecommunications, physics, biology, etc. - can make such systems work efficiently on their own. The largest cross-community design exercise to-date is hence well underway which is well reflected in the nature of the intellectual property pools created in the past years. The aim of this paper is to expose and discuss a few early milestone as well as latest IT and telecommunications patents in this vibrant area.

**Keywords:** Wireless sensor networks, cross-layer design, energy constraint systems, embedded systems.

## 1. INTRODUCTION

### 1.1. General Background

Wired sensor networks - or simply sensor networks - have already been researched and deployed for decades; their wireless extension, however, has witnessed a tremendous upsurge in interest and activities in recent years [1]. Within academia, this is mainly attributed to the unprecedented operating conditions of wireless sensor networks (WSNs), i.e. a potentially enormous amount of sensor nodes reliably operating under stringent energy constraints; within industry, this is mainly attributed to the potentially large revenues.

WSNs allow for an untethered sensing of the environment. It is anticipated that within a few years, sensors will be deployed in a variety of scenarios and applications. For example, following the notation of [2, 3], the following typical application domains are expected:

- Home and Office
- Control and Automation
- Logistics and Transportation
- Environmental Monitoring
- Healthcare and Surveillance
- Security and Surveillance
- Tourism and Leisure
- Education and Training
- Entertainment

In these applications, the nodes will generally be invisible, battery-driven and deployed in great numbers in an ad hoc fashion, requiring communication protocols and embedded system components to run in an utmost energy efficient manner. The extremely stringent constraint on energy has, in fact, triggered traditionally separate research domains to operate jointly as will become apparent from subsequent exposures.

### 1.2. Academic Projects, Industrial Players & Standardisation Activities

The cradle of WSNs - which coined many of today's terms associated to WSNs - is generally considered to be Berkley's Smart Dust project [4]. This project not only demonstrated that it is feasible to have a very large number of de facto invisible nodes (dust) communicating wirelessly in an ad hoc fashion (smart), but also was the driver and inspiration for many subsequent projects and developments in this area.

Numerous other projects then followed, such as the WINS [5, 6], AWAIRS and PicoRadio [7] projects demonstrating the miniaturisation of the nodes. Projects like Great Duck, Zebra Net, Glacier, Herding, Ocean, Grape, Avalanche, EarthCope, CitySense, Vital Sign, Power, Tracking, Mines, etc., monitor flora, fauna as well as natural and human-made elements [8].

Other fast developing projects are the Bridges, SDIC, Car Control, GlacsWeb, SMWF and MyHeart projects: The Sustainable Bridges project [9] aims at developing a reliable and cost-effective solution for detecting structural defects in bridges, also allowing for the estimation of the remaining bridge lifetime. SDIC stands for Smart Dust Inventory Control [10], which allows the exact tracking of your products - from the packaging to the truck carrying the palettes. Cortex's Car Control project [11] automatically finds you the optimum route to the destination, where various sensor readings are included in the calculation; for

\*Address correspondence to this author at the France Telecom R&D, 28 Chemin du Vieux Chêne, 38243 Meylan Cedex, France; Tel: +33 4 76 76 45 14; Fax: +33 4 76 76 44 50;

E-mail: mischa.dohler@orange-ftgroup.com

The author does not take responsibility for misinterpretation of the claims of the patents nor does the content of this paper necessarily reflect the opinion of his employer France Telecom R&D. To the best of the author's knowledge, none of the cited patents is in litigation.

instance, traffic, weather, constructions, jam reporting, etc. The GlacsWeb project monitors the drifting behaviour of glaciers by aggregating pressure, movement and temperature data collected by sensors on top and within the glacier [12]. SMWF stands for Smart Mesh Weather Forecasting and is deployed in the Yosemite National Park, where various factors are measured, analysed and predicted over past and coming years, e.g. snowmelt. Finally, in MyHeart, sensors measure variables impacting upon cardio-vascular diseases, thereby facilitating an early diagnosis [13]. The system extends beyond the measurements of body internal variables, such as blood sugar level, pressure, etc; lifestyle factors ranging from choice of clothes, environment, etc., are also considered to draw preventive conclusions - giving smart sensors a cutting

Serious commercial players have also entered the arena in recent years offering either the service architecture and/or the node hardware platform supporting these services. A convincing example on the viability of WSNs is Coronis [14], a medium-sized company in the South of France, who have commercially deployed more than 1.3 Million sensors today; their prime target market is utility metering applications but this is shifting lately. Other players, such as Arch Rock [15], Crossbow [16], Moteiv [17], Dust Networks [18] and Maxfor [19], have opted to provide suitable platforms and tailored operating systems using, e.g., TinyOS [20]. Traditional and emerging manufacturers (Schneider, Philips, Coronis/ Elster, Intel, IBM, Motorola, Honeywell, Delta Dore, Siemens, Hitachi, Somfy, Assa Abloy, Hager, etc.) and service providers (France Telecom, etc.) have also strong R&D and commercial activities to facilitate and enhance the “ambient experience” of their existing clientele using WSNs. These companies use a plethora of technologies tailored to WSNs, such as Wavenis, ZigBee, Zwave, IO Homecontrol, KNX and more proprietary wireless technologies. For example, in the near future, France Telecom’s LiveBox users may be able to connect wirelessly various sorts of sensors to their LiveBox and thereby enhance home security, ambient living, etc. [21].

As mentioned above, various standardised short-range technologies are available today, some of which are suitable to WSNs and some of which are not. Technologies that are clearly out of scope are: radio frequency identification (RFID) and near field communication (NFC) due to their lack to support multihop communication; as well as Bluetooth (building on IEEE 802.15.1) and Wifi (building on IEEE 802.11x) due to their large energy consumption. (To be) standardised technologies of interest to the WSN deployment are, among others, Zigbee, Wibree, 6lowpan and Wavenis.

The Zigbee Alliance aimed at developing protocols that are suitable to embedded applications requiring low data rates and low power consumption. It is today by far the largest standardisation group for wireless control networks and wireless sensor networks. The PHY and MAC base on the IEEE 802.15.4 and devices operate in the ISM bands. The latter makes ZigBee very prone to be exposed to interference, because the ISM bands are nowadays heavily loaded with WiFi-type wireless systems.

Wibree is a technology mainly developed by Nokia and seen today as a serious competitor to Zigbee. Wibree joined the Bluetooth special interest group (SIG) to facilitate ultra-low power communication suitable for embedded systems. The Wibree link layer specification provides ultra low power idle mode operation, simple device discovery and reliable point-to-multipoint data transfer with advanced power-save and encryption functionalities. Supported communication rates are of up to 1 Mbps and communication distances are of 5-10 meters; Wibree, however, is also susceptible to interference because operating in the highly congested 2.4 GHz ISM band.

6lowpan is being developed within the Internet Engineering Task Force (IETF) and represents an Internet standard protocol for WSNs adapting IPv6 as a networking layer and therefore enabling standard IP applications to work. 6lowpan has been developed for use in conjunction with ZigBee chipsets, i.e. relaying eventually on IEEE 802.15.4 PHY/MAC. Compared to the other available technologies, relatively few implementations of 6lowpan are available, i.e. mainly from Archrock and Crossbow.

Wavenis has been developed by Coronis (now part of the Elster Group) as part of their technology facilitating automatic meter reading solutions. The PHY and MAC have excellent characteristics, where 100m communication ranges are easily achieved at very low power consumptions. Coronis have announced in September 2007 the opening of their Wavenis Open Standard Alliance, potentially leading to standardised and certified ultra low-power communication solutions. The possibility to approach other standardisation efforts, such as KNX and ZigBee, are also envisaged.

### 1.3. WSN and its Nodes

A typical WSN environmental monitoring application scenario is shown in Fig. (1). The nodes are generally distributed in a large-scale roll-out (e.g. from airplane), hence leading to random node placements with a fairly homogeneous density. Some nodes, however, can be placed along given structures (road, river, etc), leading to a random roll-out within a confined space. The sensor nodes typically report their sensing reports on a regular basis, as well as trigger alerts if large deviations in the sensed data are observed. The nodes are generally battery-run and hence energy constrained; they could also be recharged by, e.g., solar cells. Also, there is a limited set of processing units or gateways which collect the information gathered by the sensor nodes.

The typical constituents of a WSN node are shown in Fig. (2), which is essentially composed of a sensing unit, the radio, an energy source, some digital logic, a microcontroller and some memory. The sensing unit can be composed of sensors able to sense temperature, light, humidity, wind, rain, radioactivity, pH, chemicals, pressure, movement, acceleration, etc.; recent advances in physics, chemistry and biology have facilitated these sensing units to be very small [22]. The radio is usually composed of antenna, transmitter, receiver, filters, up and down converters and ADC/DACs;

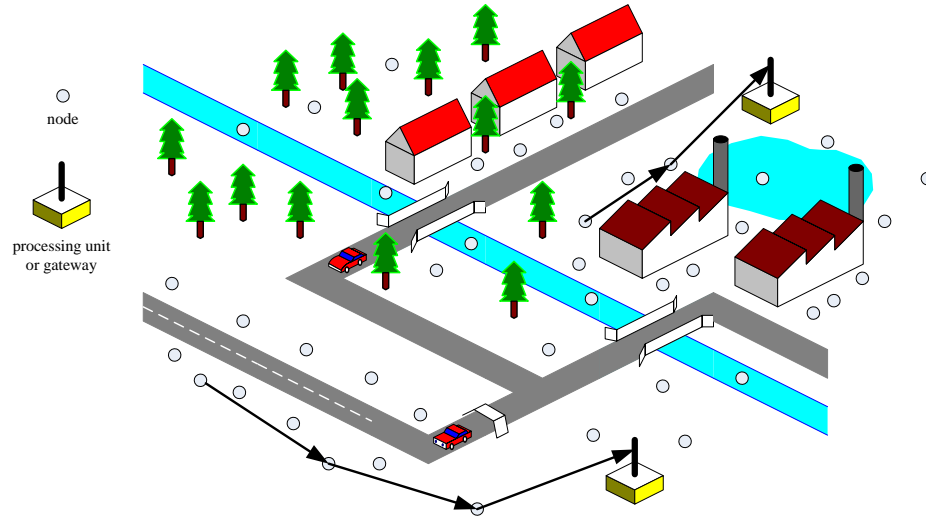


Fig. (1). Environmental monitoring by randomly distributed WSN nodes reporting to one or several processing units/gateways.

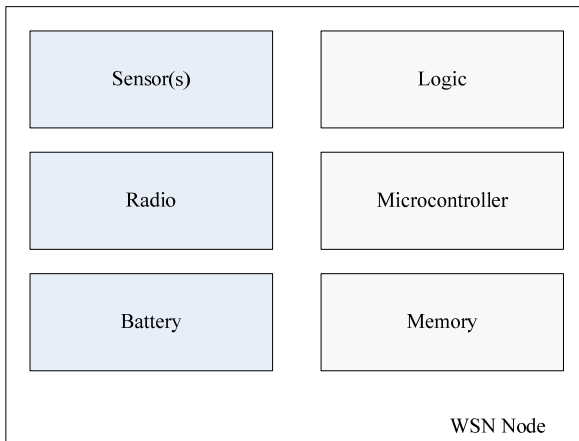


Fig. (2). Typical constituents of a WSN node.

because of the fairly low transmission distances, the energy to transmit a bit is almost identical to the energy needed to receive a bit. The battery is traditionally small and powerful but of finite longevity; for instance, a Li battery CR2450 stores 5 kJ. The data logic takes care of the data processing and nowadays consumes between 10-100 pJ per byte operation. The microcontroller controls the data flow and its energy depends strongly on its hardware realisation; for instance, an ARM9 32b 300Mips consumes between 200-400 nJ per instruction, whereas a CoolRisc 8b 1Mips only 1nJ.

Embedded into the hardware is the operating system (OS) which, for WSNs, is typically less complex than general-purpose OSs. For instance, the OS does not need to include user interfaces or support thereof. Another example is the lack of memory in the sensor nodes, which complicates or even prevents known mechanisms related to virtual memory, etc. The hardware itself is clearly not much

different from prior embedded approaches and OSs, such as eCos and  $\mu\text{C}/\text{OS}$ , are theoretically well applicable; however, they are mainly supporting real-time applications which is often not needed in WSNs.

To this end, TinyOS [20] has emerged as the first OS tailored to the non real-time needs of WSNs by using an event-driven approach. That is, with the occurrence of an external event (e.g. sensor reading), an appropriate event handler is called to handle the event by posting tasks which are then scheduled by the OS's kernel. Other OSs have subsequently emerged, such as Contiki, FlexCap, MANTIS, BTnut, SOS, Nano-RK, etc. The OSs and programs are usually written in a special programming language; for instance, TinyOS uses nesC which has been designed to detect race conditions between tasks and event handlers. Although most nodes are currently programmed in C, other programming languages are currently on the market, such as galsC, SNACK, SCTL, DCL, c@t, etc.

Since OSs, sensor network programming and middleware are not the focus of this paper, they are not discussed in further details here.

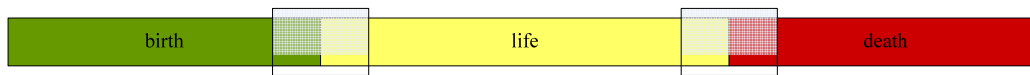
#### 1.4. Network Phases

As depicted in Fig. (3), the working cycle of a WSN can be divided into three phases, i.e.

- birth:(self-)organisation, configuration, optimisation, etc.
- life: maintenance, (self-)healing
- death:node failure, breakdown in connectivity, etc.

where the duration of each phase will strongly depend on the implemented algorithms discussed in previous sections.

**Birth Phase.** A WSN is said to be born if at least one sensing node is capable of reporting data to an attached collection point. In practice, several hundreds of nodes will be attached to at least one data processing point, which requires the network to organise, configure and ideally



**Fig. (3).** Typical cycle of a wireless sensor network with ambiguous zones between birth, life and death.

already optimise mechanisms for forthcoming data gathering. Clearly, one has several choices of declaring a WSN to be born, i.e.:

- at least one of the nodes communicates with at least one data collecting unit;
- the entire communication structure has been set-up in a fully connected fashion;
- a given percentage of the network is capable of communicating; etc.

In dependency of the application, one choice or another will be more suitable. This, however, also implies that the duration of the start-up, i.e. birth, phase will be application dependent. Independent of the application, however, the aim of any innovative approach ought to be to minimise the time and, most notably, energy spent in this phase.

**Life Phase.** This is the prime phase of interest for WSN, as in this phase the network performs its application dependent detection, sensing and reporting tasks. In this phase, the main issue is to maintain the communication structure and facilitate its reparation in the case of failure or changes. It should clearly be the aim to invent communication mechanisms which facilitate the lifetime to be optimised whilst maintaining a predefined QoS; for instance, the lifetime will differ for a network which is required to have all nodes 100% available for reporting duties from a network which does not require full connectivity all the time. Also, solutions which take care of the association and disassociation of nodes are required to be energy optimised.

**Death Phase.** A WSN is said to enter its death phase when the communication mechanisms commence to break down. This breakdown may originate from node failures, energy drainage, drastic topological changes, malicious attacks, etc. Again, the point upon which a network is declared to be dead may not be unique due to application specific requirements. Some choices of decision are:

- the first node in the network fails
- the last node being able to connect to the collecting point fails
- the coverage area is inferior to a predefined level; etc.

Independent of the application, one ought to aim at minimising the time the network loses in its last phase. Also mechanisms should be provided which facilitate an easy ‘reincarnation’ of the network, e.g. by means of pinpointing dead nodes for replacement.

### 1.5. Design Challenges

From the above, it is hence clear that WSNs bear some fundamental design differences w.r.t. other known state-of-the-art networks which is mainly manifested in the following issues:

- Application: wide variety ( $\neq$  any wireless system)
- Control: decentralized ( $\neq$  cellular, broadcast, satellite)
- Info Flow: highly directed ( $\neq$  ad hoc)
- Energy: highly constrained ( $\neq$  any wireless system)
- Run-Time: very long ( $\neq$  any wireless system)
- Nodes: huge amounts ( $\neq$  any wireless system)

This means that, unlike other systems, WSNs need to be:

- highly application tailored (should work for many applications)
- highly energy efficient (at all layers and functionalities)
- highly scalable (at arbitrary number of nodes)
- highly secure (robustness, integrity and confidentiality)

In addition, in [1], it has been argued that a further - largely unexplored - shift in WSN design paradigm is needed to facilitate successful deployment, where argumentation is based on experiences gained with Coronis' real-world sensor network roll-outs [14] and relates to:

- network start-up,
- tailored network life-span, and
- rechargeable batteries.

As for the network start-up, a very large fraction of energy is consumed during network ramp-up; hence, protocols need to be developed which use minimum energy to initialize the network. This remains a largely unexplored topic potentially yielding important intellectual property rights.

As for the tailored life-span, a non rechargeable as well as chargeable battery has a limited life-time, typically 10-15 years; hence, algorithms need to be optimised such that they facilitate a proper functioning over the given battery life-span. Current algorithms - including a large amount of patented ones - aim at maximising the network lifespan which may very well be counteracted by a limited battery lifetime.

Finally, as for the rechargeable batteries, recent trends suggest that more and more nodes are equipped with rechargeable batteries; hence, algorithms need to be redesigned such that they facilitate communication when the battery is recharged, i.e. at fairly regular intervals, in contrast to a continuous communication. Whilst a solid patent pool is available on mechanisms facilitating a recharge of the batteries, supporting algorithms are fairly scarce.

### 1.6. Horizontal OSI Layers & Cross-Layer Design

Algorithms are implemented onto before-described node and network architectures, giving life and functionality to WSNs. Such an implementation usually follows the OSI layered approach with some of the layers being designed jointly with adjacent layers to enhance performance; the latter is also known as cross-layer design. The OSI layers important to WSNs are shown in Fig. (4); these include the physical (PHY), data link (MAC), network (NTW) and application (APL) layers.



Fig. (4). Part of the OSI Layer important to WSNs.

**PHY.** The prime function of the PHY is to prepare the data stream, which it received from the MAC layer, for transmission over the medium with minimum error. Of importance here is to design algorithms which are robust to noise and interference, and which have a low complexity. Typical elements of the PHY are the channel coder, interleaver and cyclic redundancy check (CRC). In the context of WSNs, the use of channel coders is not evident due to its complexity and the fact that the transmission power is not the only major factor of power consumption; the use of the interleaver is also not obvious, due to the fairly slow-fading channels thereby leading to prohibitively long interleaver depths; the use of CRC, however, is essential.

**MAC.** The prime function of the Medium Access Control (MAC) is to coordinate the one-hop neighbourhood transmission over a given medium among competing users. Of importance here is to design algorithms which coordinate transmission, minimise collisions, and which guarantee certain fairness among users. Typical MAC families are either contention-less or contention-based, where in a centralised scenario one would use the contention-less and in a distributed scenario the contention-based (note that other solutions are also possible). In the context of WSNs, contention-based solutions will be required at least during network ramp-up and also if the traffic load is low; however, contention-less allocations can be negotiated once the network is running and the load turns out to be high.

**NTW.** The prime function of the NTW is to facilitate an end-to-end data transmission from source to sink via

potential relaying nodes. Of importance here is to design algorithms which minimise the consumption of energy, choose the optimum routing path, minimise routing overheads, etc., and also facilitate some form of QoS in terms of throughput, delays, etc. In the context of WSNs, routing protocols designed for ad hoc networks are not directly applicable due to energy constraints. Also, the direction of information flow is usually towards one or very few directions, i.e. towards the directions of the processing unit(s) or gateway(s).

**APL.** The prime function of the application layer is to support a given application level protocol, which can include data gathering, information processing, etc. Of importance here is to design applications which are of low complexity and which can tolerate the peculiarities of the underlying NTW, MAC and PHY layers.

### 1.5. Vertical System Functions

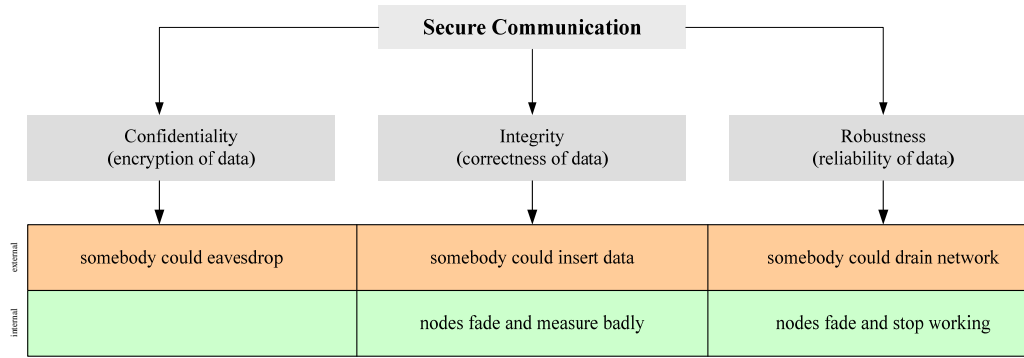
Functions, procedures and algorithms which involve various OSI layers include security and location determination. Both functions are vital to a proper functioning of WSNs; without security, data readings can be compromised; without location determination, data readings cannot be spatially associated. Whilst in traditional wireless communications systems these functionalities can be added at a later design stage, the stringent energy constraint in WSNs makes a joint design with other functional blocks imperative.

**Security.** Also WSNs are exposed to security threats which, if not properly addressed, exclude them to be deployed in a plethora of envisaged civilian and military scenarios. The wireless and distributed nature of WSNs drastically increases the spectrum of potential security threats; this is further amplified by the serious constraints in node battery power, thereby preventing previously known security approaches to be deployed. Above mentioned issues require special attention during the WSN design process, so as to facilitate a commercially attractive deployment.

Albeit traditionally being associated to encryption only, a secure communication in a wireless network encompasses three main elements, i.e. confidentiality (encryption of data), integrity (correctness of data), and robustness (reliability of data); as previously said, because of the limited power budget in WSNs, we expect that these issues need to be tackled jointly and in conjunction with other design issues.

Also, the identified three security issues need to cater for network internal and external threats. For instance, confidentiality can be breached if external sources eavesdrop on ongoing data communications. Integrity can be violated if external sources insert incorrect data packets, or if nodes start to break down internally and hence commence measuring and relaying data unreliably. Robustness can be defied if external sources try to exhaust the WSN or block data, or if nodes start to break down internally and hence cease functioning. This has been summarised in Fig. (5).

Further example security issues which may arise are the abnormal behaviour of nodes which exhibit an egoistic conduct, such as not obeying network rules, or forwarding no or false packets. Other important issues may arise in the context of Denial of Service (DoS) attacks, malicious



**Fig. (5).** Different types of secure communication: confidentiality, integrity and robustness.

address space allocations, advertisement of variable addresses, a wrong neighbourhood, external attacks aimed at injecting dummy traffic to drain the network power, etc.

The choice of the security solutions will have an impact onto hardware, choice of identification, application layer, network layer and possibly also on the medium access control. Therefore, the augmenting importance of innovative solutions related to security will certainly be reflected in associated patent pools.

**Location Determination.** The determination of the node's location is of prime importance for many WSN applications. GPS-like solutions are clearly not realistic, because WSN nodes are supposed to operate at low complexity and power consumption. Therefore, other methods have to be devised, such as relative triangulation, train-gulation using anchor nodes, etc. All these methods will involve various OSI layers and, again, a design separate from other functionalities will render location determination algorithms energy-inefficient.

### 1.8. Summary and Paper Structure

Patents emerge from innovative solutions which cannot be obtained in a straightforward manner from the known state-of-the-art. Due to their starkly different design constraints, WSNs are currently an ideal area to build patent pools. Indeed, a search for 'sensor' yields more than 100,000 patent hits; for "wireless sensor" yields about 5000; and for "wireless sensor networks" still more than 100.

Without any claim of an exhaustive survey, important key patents in the arena of WSNs facilitating communication (i.e. not the sensors themselves) are discussed in subsequent sections. It shall be noted, however, that patents in Japanese, Chinese and Korean - not having English, German or French translations - could unfortunately not be included.

The remainder of this paper is structured as follows. In Section 2, patents related to horizontal OSI layers will be discussed, i.e. PHY, MAC, NTW and APL layers. Whilst such approach may not follow latest cross-layer trends in WSN design, we found it this way easiest to expose the large gamut of available information. In Section 3, patents cross-relating various OSI layers are dwelled upon, i.e. self-organisation and topology control algorithms, location determi-

nation, security and energy harvesting. Finally, conclusions are drawn in Section 4, where we also speculate on future developments in this vibrant area.

Prior to proceeding to subsequent sections, however, we shall discuss a very first patent using wireless sensor network readings to enhance other mechanisms, notably the instability-prone ALOHA MAC protocol [23]. The inventors there proposed to used sensors readings to stabilise ALOHA where a grid or deterministically or randomly deployed sensors gathers energy measurements and then use neural networks to estimate (predict) the number of collisions per slot and also whether a given transmitter (successful or not) was a member of an earlier group of colliding callers. Thereupon the backoff mechanism is modified, i.e. the random backoff timings which are traditionally fixed for a given ALOHA roll-out. Their proposed technique is beneficially applicable in the cellular reverse link which extensively uses ALOHA type contention resolution protocols. In addition, their sensor readings can be used to predict the location of users and hence advanced beamforming techniques can be applied to further boost system capacity.

Finally, we shall also discuss here a milestone patent related to WSNs by David Gelvin, Lewis Girod, Gregory Pottie, *et al.* from Sensoria Corporation (USA) entitled "Wireless Networked Sensors" published in 2001 [24]; note that numerous related patents have subsequently emerged, such as [25-30]. In [24], reference is made to the Wireless Integrated Network Sensor (WINS) Next Generation (NG) nodes which provide distributed network and Internet access to sensors, controls, and processors that are deeply embedded in equipment, facilities, and the environment. The WINS project was initiated in 1993 by the Defence Advanced Research Projects Agency (DARPA). The Low-power Wireless Integrated Microsensors (LWIM) programme was a pioneering milestone in the development of WINS and provided support for the development of low power microelectro-mechanical systems (MEMS) and low power electronics. The patented WINS framework is generic and relates to monitoring, control and remote reconfiguration capabilities in transportation, manufacturing, healthcare, environmental monitoring, etc. (see previous section on application domains). The proposed framework is one of the first of its kind and combines microsensor technology, low

power distributed signal processing, low power computation, and low power, low cost wireless networking capability in a single system. It includes proposition for hardware and algorithmic implementations, i.e. suitable PHY and MAC layers, as well as auto-organisation and routing mechanisms, data query databases, etc.

## 2. CLASSICAL OSI LAYERS: PHY, MAC, NTW & APL

Responsible for getting the data stream over the wireless medium at minimum error, the PHY is a vital component in WSNs. Power consumption of transmission and reception are of prime concern and any solution minimising it hence welcome. To this end, it is no surprise that Ultra-Wide Band (UWB) - known to facilitate communication at lowest possible energy per bit - play a central role in the patent pool of PHY algorithms of WSNs. This is further boosted by the fact that UWB has been well supported by industry and standardisation bodies (see, e.g., the low data-rate PHY option of IEEE 802.15.4). Other technologies, as alluded to in Section 1.2, will not be dealt with due to space limitations.

For interference limited systems (i.e. highly congested and contested systems large-scale sensor roll-outs), the MAC is central to energy consumption and hence many patents have emerged in this area, each proposing solutions with different trade-offs.

In contrast to above, network and application layers have not yet been enjoying large patent pools; nonetheless, important patents are also summarised below.

### 2.1. Physical Layer Patents

Coronis [14] has confirmed that one of today's prime problems is that WSN nodes forming a mesh network are often out of range, i.e. the achievable signal-to-noise ratio (SNR) is too low to accomplish successful packet transmission. Various PHY techniques exist to improve the low SNR, most notably multiple-input-multiple-output (MIMO) space time coding techniques. Dohler [31] proposed a pioneering approach facilitating the implementation of these techniques to nodes which cannot accommodate multiple antenna elements by using distributed space-time coding techniques. As per Fig. (6), an information source broadcasts its data (voice, video, sensor readings) which is received by spatially adjacent nodes. The latter form a virtual antenna array (VAA) and - prior to transmitting the data to the next VAA - encode it in a distributed fashion using known or specially designed space time coding techniques. It has been shown in many works that such deployment yields significant performance gains; see, for instance, [32].

Also related to above mentioned connectivity problem, a power control mechanism has been proposed in [33] which is well applicable to WSNs. The said power control mechanism adopts transmission powers according to terrain's obstacles so as to optimise performance criteria. Such a technique is particularly useful in the context of WSNs, because sensors are likely to be dispersed within an environment with very different propagation characteristics; for instance, a sensor placed on the floor will have a different power propagation characteristics than a sensor embedded into a wall.

Dowla *et al.* from University of California proposed to use UWB to facilitate scalability, power conservation, channel estimation, and node synchronisation in WSNs [34]. Their framework also caters for SNR, acquisition timing and tracking enhancement. They proposed to transmit from one or more nodal WSN node positions a plurality of UWB pulse pairs with each of the transmitted pulse pairs (doublets) separated by a predetermined lag interval,  $D$ , unique to each multiple access channel. Each of the pulse pairs comprises a predetermined encoded data and a reference signal, and are arranged to be received at a predetermined symbol repetition period,  $T$ . The WSN also feedback-loops one or more times a predetermined portion of the pulse doublets by shifting the pulse pairs by the symbol repetition period with each iteration through a feedback loop. The encoded data of the received pulse pairs is then delayed by  $D$  and the plurality of reference signals produced by the looped pulse pairs multiplied with the delayed versions of the encoded data. The multiplied plurality of reference signals and the delayed versions of encoded data are then threshold-tracked by means of a variable size integration window. This generates a high energy plurality of pulse pairs and from this the output bit stream.

In [35], the concepts of [31] and loosely [34] have been unified to provide a wireless UWB-based space-time WSN. The proposed technique requires sensor nodes of enhance capabilities as it is presupposed that each node has several antenna elements and supports fairly complex signal processing tasks. [35] proposes to use spread-spectrum techniques as an access method and hence exploits frequency diversity; the space-time approach, in addition, extracts spatial and temporal diversity. The proposed method is hence highly robust and reliable.

Finally, [36] proposes a fairly useful utility given the increasingly congested frequency bands, i.e. a link assessment and frequency monitoring system. It has been proposed to sample active WSN links and determine its noise measure. Similar to cyclostationary techniques, a correlation measure based on the spectral distance between the noise measures for each pair of frequencies is determined. Proximate frequencies are then assembled into a group, where the proposed grouping algorithm makes sure that the number of groups is less than the total number of frequencies. From each group one representative is chosen and used to perform the link quality assessment for each occurring link.

### 2.2. Medium Access Control Patents

Generally, there are two MAC families available today, i.e. reservation-based MACs (TDMA/FDMA/ec) and contention-based MACs (ALOHA/CSMA/etc). Whilst reservation based MACs guarantee collision-free communications, they come along with a large managerial overhead. Contention-based MACs, on the other hand, work in a decentralised fashion but collisions (at least two packets are transmitted at the same time), idle listening (receiver does not know whether he is intended receiver), overhearing (reception of irrelevant frames) and protocol overheads are not avoidable [37, 38]. In the case of WSNs, it is hence not clear which process - i.e. having a reservation-based or contention-based MAC - is more energy-efficient. Proposed

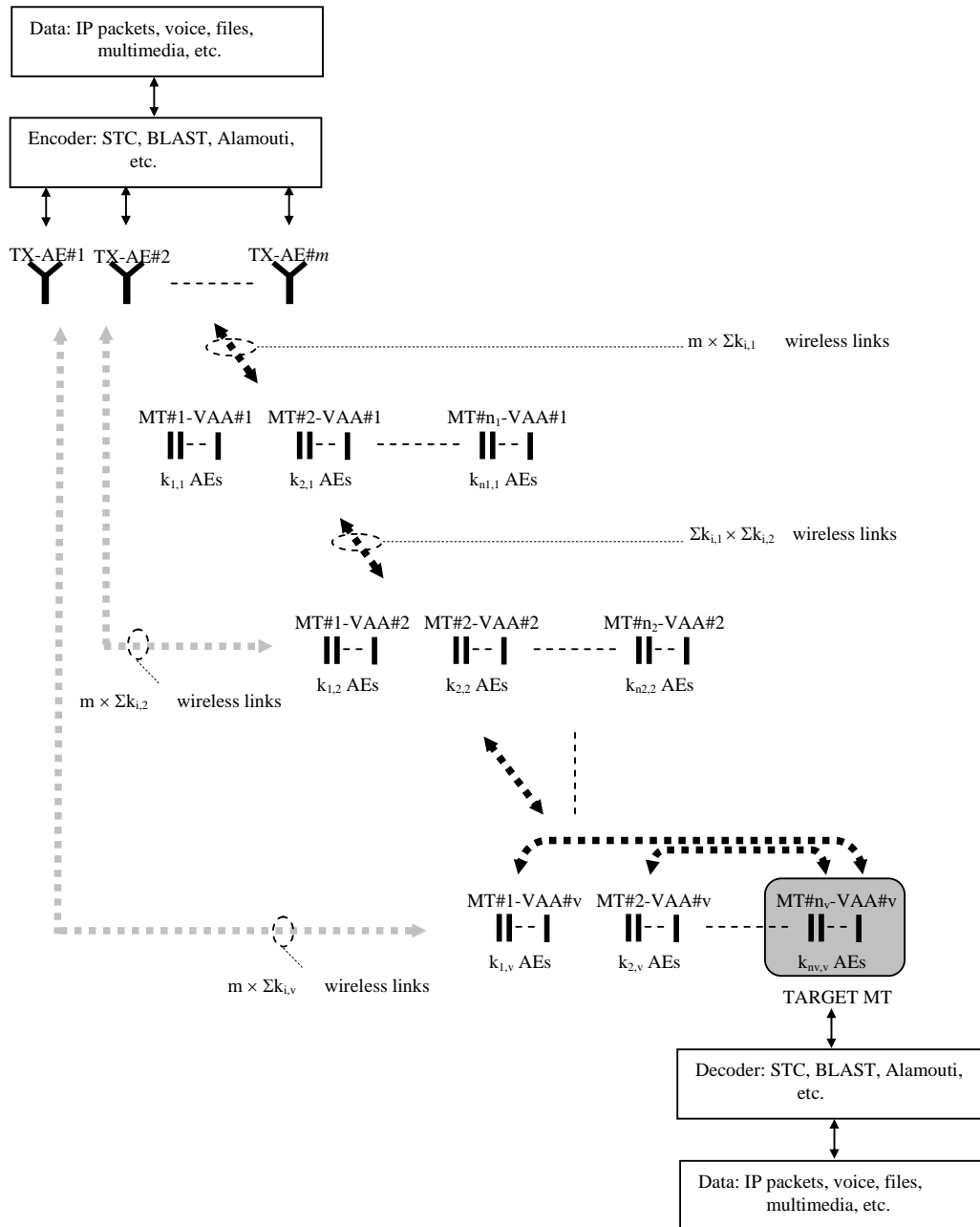


Fig. (6). Implementation of distributed space-time coding techniques onto WSN nodes using the technique of VAA [32].

MAC solutions trade various factors, some of which are discussed below.

To this end, [39] proposes a MAC for high density WSNs with periodic data reportings by the nodes. A distributed frame-based MAC protocol (DFB-MAC) is proposed, which does not require any prior or centralised infrastructure. Relying on the periodicity of the generated data traffic, the nodes passively monitor the channel which allows determining which time slots are used and which are vacant in the frame. After a certain monitoring time, the node commences using the unused time slots and hence facilitates data

transmission; latency is generally higher than in other MAC protocols and beyond a given traffic volume the throughput is deterministically zero, but the lack of control overhead is appealing.

Varaiya *et al.* from the University of California proposed a TDMA based MAC for wireless sensor nodes by using a more powerful supervisor station, which could be the data collection point or gateway with unlimited transmission and processing power [40]. The proposed centralised system uses the supervisor station to synchronise and explicitly schedule the nodes' transmissions, thereby significantly saving on the

nodes battery power. This approach is equally applicable to super-nodes being plugged into the mains. Another characteristic of the proposed scheme is that the supervisor station can regularise the generated and scheduled traffic and hence obtain failure information if scheduled time slots are not populated.

The inventor of [41] proposes a MAC which achieves energy savings by employing a wake-up signal with more processing gain than for the normal traffic, as well as dynamic adjustment of the periodicity of synchronisation messages and a neighbour node discovery technique. The processing gain of the wake-up signal is increased by either transmitting at higher power or using a lower rate. The periodicity of synchronisation messages from a synchronised node depends on many factors, such as the number of hops to be traversed to reach the sink, remaining power level in the synchronisation node and the pattern of already sent synch messages. Finally, the neighbour discovery technique relies on the approach where a node sends a node discovery message in dependency of its remaining energy level.

The inventors of [42] propose an interesting MAC solution which extends the preamble-sampling based solutions of Fig. (7) (top) to a micro-frame (MF) preamble-sampling based solution of Fig. (7) (bottom). In this type of MAC protocol, each data frame is preceded by a sequenced number of micro-frames which achieves energy savings as follows. A transmitting node broadcasts the micro-frames and adjacent nodes randomly wake up and get a micro-frame which not only contains a sequence number but also some information about the destination, which allows the receiver to go to sleep for a known period of time before waking up and receiving the packet if intended for him, or simply go to sleep because the packet is for somebody else. Since the radio at the receiving station is off and usually many receiving stations surround a transmitting node, significant energy savings can be achieved.

This principle is extended in [43], where the inventors propose to make the response time proportional to some

inherent metric in the receiving nodes. For instance, this could be the inverse of the energy state of each node, where nodes with a high energy level would respond fast and nodes with a low energy state more slowly. Such a MAC automatically balances the energy state within large networks and hence exhibits properties of auto-adaptation. In addition, it does not need any information on neighbouring nodes and hence keeps memory requirements to a minimum. This is further exemplified in Fig. (8), where the receiving nodes' inherent metrics  $f$  makes node  $A$  respond fastest and node  $B$  slowest.

[44] proposes to achieve energy savings by dividing the network into clusters where the nodes in each cluster sleep and wake together. This has several advantages, most notably nodes can sleep immediately after data scheduling, nodes and clusters can intelligently adjust their waking patterns, etc. The cluster head in charge may impose a fixed duty cycle on the cluster, sending a periodic beacon while the cluster is awake to tell the nodes within the cluster when to start sleeping and how long to sleep [44]. This beacon can also be used to update and adjust the waking pattern, either lengthening or shortening a given wake period.

The wake-up scheduling of the MAC proposed in [45] reduces the energy consumption and data delay of levels of nodes by using a crossed ladder pattern according to Fig. (9). The network control at the root assigns multiple parents with different wakeup schedules to each node in the network. This multi-parent assignment reduces the delay in transmission of information through the network and also increases energy efficiency per node. This multi-parent node assignment, however, is a NP-complete graph colouring problem and heuristics are needed. Exemplified by Fig. (9), we assume a WSN nodes controlled by a crossed ladders wakeup pattern. The crossed ladders pattern in this example combines two ladders so that the nodes in one of the network levels (the crossing level nodes) wake up only once per period  $T$ , which has a pre-specified duration. Therefore, the crossing level nodes will save more energy than others. The

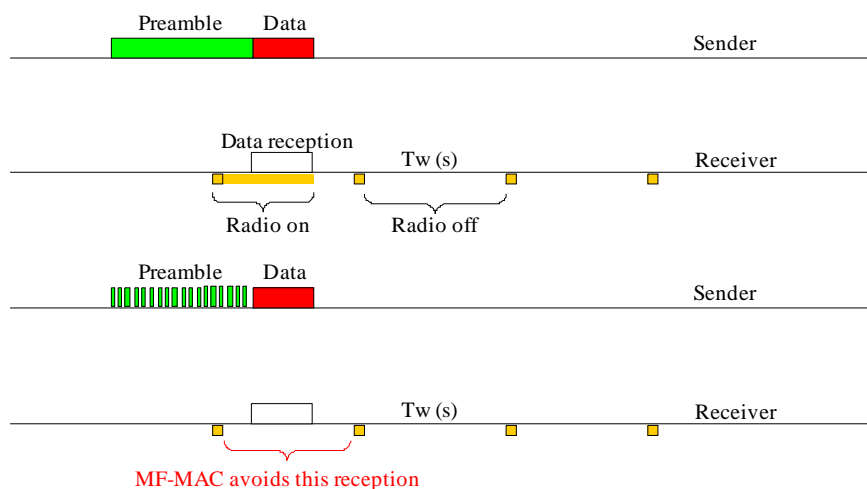


Fig. (7). Top: traditional preamble based MAC [40]; bottom: micro-frame enhanced preamble based MAC according to [42].

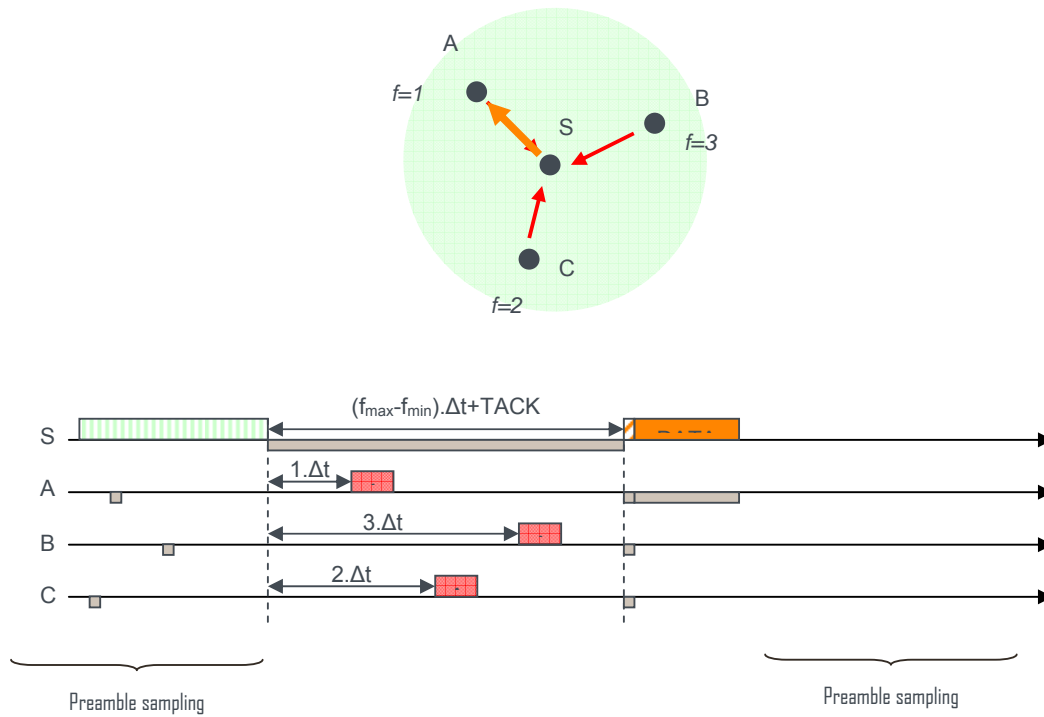


Fig. (8). 1-hopMAC avoiding neighbourhood knowledge [43].

### 2.3. Routing Protocol Patents

Generally, sensor routing protocols can be classified into three categories [46]: one-hop, flat and cluster-based hierarchical protocols. In the case of one-hop protocols, a node sends data directly to the sink. This is practically often not achievable because sensor nodes have limited transmission. Flat approaches, on the other hand, have a node transmitting data to the sink by forwarding its data to one of its neighbours according to some routing requirements. This multi-hop approach clearly suffers from latency problems, among others. In the case of cluster-based routing protocols, clusters are formed with a cluster head via which all communications happens. Cluster heads may also be super nodes which are less or not energy-constrained; also, a cluster-head can also perform some data aggregation.

Networking patents aim at minimising the energy needed to route information from a source sensor via multiple hops to a supervisor node or processing unit or gateway. Such routing usually requires the nodes to be aware of the routing path, an information which is potentially very energy consuming. In addition, due to the unidirectional information flow from a plurality of sensors towards one or very few gateways, the energy of the nodes close to the gateway drains quicker. Furthermore, the wireless channel between the nodes causes the shortest path in terms of hop-count not necessarily to be the least energy consuming path. Several of these factors are hence treated in subsequent patents.

In [47], the inventors aim at balancing energy consumptions caused by inhomogeneous use of nodes on the way to the data sink. Whilst a large amount of prior solutions assumed each node to be equally charged, it is clear that nodes closest to the sink will be required to transmit more

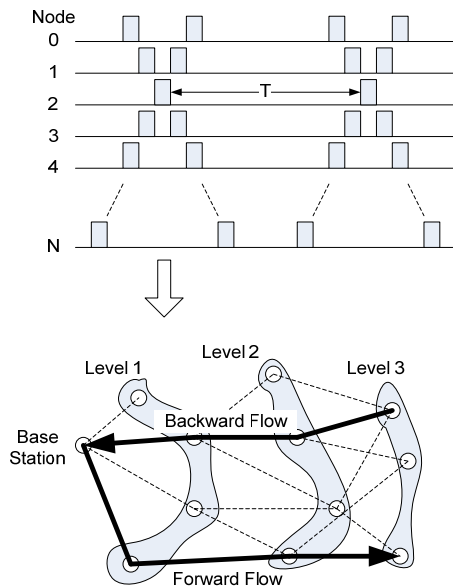


Fig. (9). Crossed ladders wake-up pattern according to [45].

crossed ladders pattern here induces nodes in level 2 to wake up once per period  $T$  while the other nodes of the network wake up twice per period.

traffic than, for example, a node at the WSN edge. The solution presented in [47] cross-couples network and (contention-based) MAC layers by assigning to each node a contention penalty parameter that is used to represent the probability of a transmission colliding with another transmission across a link in a contention region. Data is then routed along the smallest contention penalty path and thereby balancing energy expenditure within the WSN.

The inventors of [48] observe that it would be desirable that the sensors spend their energy mostly for the primary designated job, i.e. sensing of the data and transmission, and not for routing overheads, etc. To facilitate this, [48] proposed a heterogeneous WSN edge-based mechanism in utilising a powerful basestation with beamforming capabilities which allows gathering location information of the nodes, synchronisation among the nodes and routing through the nodes. It also simplifies tasking and query mechanisms. Technically, the sensors in the beam area pick up the beam's ID which becomes their area ID. When data is sent towards the basestation, this ID is included as well as a detailed status report which is analysed by the basestation. Based on this report, the basestation sends control messages into the beam area providing optimised routing instructions and routing paths.

Zhang [49] proposed to extend the IPv6 addressing mechanism to WSNs, an approach still disputed due to the large address space and hence large extra communication energy costs (see IETF's 6lowpan standardisation group). The approach includes the IEEE 802.15.4 PHY, MAC and adaptation layers. This, so is argued, facilitates seamless and remote connectivity to the next generation Internet.

The inventors of [50] propose a directed and hence optimised flooding mechanism where only nodes with minimum hop-count are involved in the forwarding process from the sensing node towards the sink. They argue that some form of initial flooding will always be needed which - in combination with contention-based MACs - can lead to severe contention and hence energy drainage; they refer to this as "broadcast storm problem". This problem is usually alleviated by building a flooding tree, where finding an optimum flooding tree was shown to be NP-complete. [50] hence proposes a sub-optimum routing tree where the flooding of packets is accomplished in the direction of the sink based on directional information. This is achieved by allowing the sink to inform the sensors of its position, after which the nodes calculate the minimum hop-count towards

the sink and insert this count into the packet to be flooded; the nodes receiving this packet compare the inserted hop-count with their own one and discard the packet if this hop-count is smaller than their own but write in their own count if it is larger. This is repeated until the directed flooding is accomplished.

The inventors of [51] proposed a creative way for accomplishing energy-aware routing. In there, a node delays the forwarding by a deterministic amount which depends on some node inherent properties. For instance, a node requests a route to be established towards the sink by using some (directed) flooding or a sink requests some sensed data to be transmitted. Each node on its way then delays the forwarding e.g. inversely to its energy state; referring to Fig. (10), this guarantees that the establishment of the routing path is done along the route with most residual and not necessarily least-total energy.

[52] overcomes the fixed addressing approach of WSN nodes in body area networks, where it is proposed to use instead a patient identification field containing a patient identification number that is unique to the wireless body network.

[46] pointed out that many routing protocols fail to deal with time-critical applications because synchronisation among nodes is usually not considered. Also, maintaining global routing tables up-to-date is very energy inefficient for networks with some dynamicity. They hence propose a local on-demand protocol that facilitates the energy expenditure to be balanced between the nodes in the network. This is achieved by inserting local node information (LNI) into transmitted messages which can be exploited by adjacent nodes to update their local topology knowledge and - in the case of node arrival/departure - can handle the routing updates locally. Only if such a local repair process fails, a global (energy consuming) reorganisation is initiated. An example of such local behaviour is that nodes having lower battery power available may decide not to transmit the LNI messages so that adjacent nodes choose another node for data forwarding.

Without going into details, [53] proposes a method for two or more WSN domains to communicate via the Internet by using an Internet communication tunnel.

Finally, related to [54], Kris Pister from Dust Networks proposed in [55] a novel method of packet switched transportation by using digraphs. These are used to define

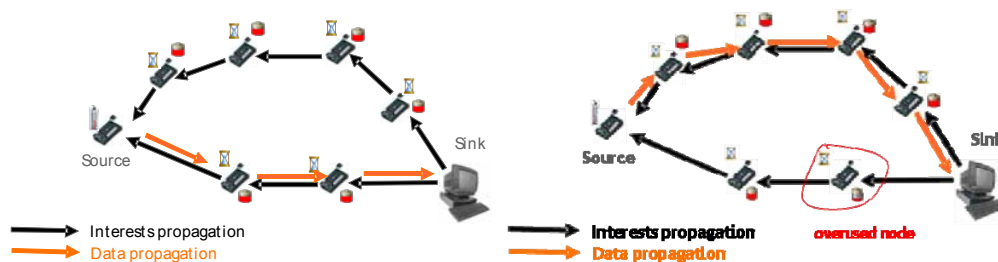


Fig. (10). Turning diffusion from minimum energy (left) into maximum residual energy (right) routing [51].

paths among nodes where a graph identifier is used instead of the real destination address. All nodes build such connectivity mesh using digraphs on a real-time basis. Packets hence travel only along available paths and go around dead nodes, lost links, etc., without any need for additional computation, route request messages, or dynamic routing tree construction.

#### 2.4. Data Aggregation & Query Patents

Typical WSN nodes include today, among other components, an operating system and a central processing unit. They are designed to measure and possibly (pre-)process physical observations, such as vibration, pressure, temperature, humidity, radiation, sound, light, etc. Some of these observations are regular, some sporadic; some observations are strongly correlated in time and/or space. It is hence the aim of aggregation patents to propose system designs which facilitate suitable data aggregation so as to minimise the communication energy expenditure. Query patents, on the other hand, obey designs the way databases are build and data is requested in such a way that energy expenditure is also minimum. Again, this trades various design factors, some of which are discussed below.

The inventors of [56] provide a generic information architecture permitting the WSN nodes to be reached through the Internet by databases, mining engines and users not necessarily located at the same point. They claim that their approach serves as an enabling interface between the Internet and the physical world, where these physical contact points may be anywhere in the world. The proposed approach enacts distributed WSN state discovery and maintenance by means of a quasi-recursive traversing and interrogating algorithm (also referred to as modelling agent) from a remote location to a single or plurality of WSN nodes. This facilitates the construction and maintenance of a relational database model of the WSN nodes on a database server. In addition, the nodes may be mobile and communication between them not necessarily restricted to the wireless interface, i.e. they also may be wired. The modelling agent dynamically updates the WSN nodes' data and link states into a logical database. This database can be queried to get access, visualisation and the use of a stream of information generated by the WSN. The nodes are assumed to be uniquely addressable; they communicate among each other with appropriate networking protocols and with the database server through one or more access points or gateways. Technically, the invention proposes, for discovery and maintenance, to apply at every gateway a quasi-recursive algorithm triggering the agent to visit a first sensor node, mark the first node visited and push the marked first node onto a stack. Whilst this stack is non-empty, query the node at the top of the stack for a list of current links to the node at the top and compare the list of current links to a list of historical links to the node at the top of the stack and update the historical link and historical node information. If there are no unmarked nodes reachable from a current link then it is proposed to pop the stack, otherwise to visit the next reachable unmarked node, to mark the next node and to push it onto the stack [56]. The agent then builds the database model by updating relational database logical design tables at each step of the discovering step. To incorporate updates

due to node associations and disassociations, the interrogating algorithm is periodically reapplied. It is stated that the periodicity of updates is preferably such that a near real-time topology of the sensor network is maintained; however, energy consumption due to these updates has not been considered in the design.

Joseph Paradiso *et al.* from MIT proposed an interesting approach facilitating data aggregation which, however, is not strictly speaking related to the application layer. As such, they proposed in [57] an apparatus which transports wireless sensors to a desired measurement location by coupling it to a moving host. Such a coupling is maintained until either the measurement has been accomplished and/or the host moves away from the desired location. They argue that such parasitic behaviour can also be used to close communication gaps by placing the relay node in coverage holes. The hosts can be anything from vehicles, humans, animals, fluids, etc. To accomplish the parasitic scheme, the following is needed: a sensing device and wireless interface, as well as some means for attaching to and detaching from the moving host (for active nodes e.g. a propelling mechanism; for passive nodes e.g. a hook). Active nodes can encourage hosts to start moving in the desired direction and keep moving for a specified time. Furthermore, a database can be maintained which lists desirable and undesirable locations, etc.

In [58], an energy efficient data aggregation method for WSNs has been proposed but, unfortunately, no further details are available.

In [59], the inventors proposed statistical data gathering and aggregation techniques to decide whether the WSN node observes an 'interesting' event which is worthwhile to be transmitted to the sink. To this end, the decision engine in the node receives a quantised value of the event reporting and, from the distribution of the sequence of these quantised values, decides whether the sensor is observing a real/worthwhile event; if so, the observation is forwarded to the sink. The rationale behind this is that nodes are often designed to measure episodic events which are characterised by increased burstiness, changing mean levels, appearance of trends in the measured variables that are otherwise statistically stationary, or appearance of dynamic phenomena that distinguish the interesting events from the background noise [59]. Techniques using limiting thresholds are traditionally applied to distinguish the interesting event from background noise but it suffers from the shortcoming that setting the threshold wrongly seriously deteriorates the reliability of the decision. The inventors hence propose to gauge the distribution of the received quantised values by using appropriate significance tests. In a variation of this, they propose to keep a quantisation bin for each quantised value and gauge then on the change in frequency of usage of a given quantisation bin. In yet another extension, they propose to use the Sequential Probability Ratio Test (SPRT) to determine whether the calculated frequency has deviated by the specified amount from the mean frequency in the quantisation bin. More variations are also proposed in [59], as well as suitable tests (positive mean test, negative mean test, nominal variance test, inverse variance test, positive first difference test, etc.).

Laurent Maleysson, now General Director of Coronis [14], and his colleagues proposed in [60] a wireless meter reading system. In 2001, this was quite a novel approach to this problem where meters have traditionally been read manually. Coronis, partially based on this patent, is enjoying roll-outs of more than 1 Million wireless meter reading sensors. In a preferred embodiment, they proposed that such metering solution ought to include an external modem module (EMM), a hub and a data collection system, where the EMM communicates with one or more utility meters. It preferably chooses a communication format that is compatible with the communication format of the utility meter so that no modifications are required. Clearly, the EMM gets the meter data from the utility meter and converts it to a format which is transmitted over a given frequency band. This signal then reaches a hub, where it is translated into an analogue or digital telephone communication format. Finally, this is transferred to the data collection system for use by the utility as desired, e.g. utility billing, tracking, control, etc.

More algorithms are of course available at PHY, MAC, NTW and APL - both in published as well as patented form - however, the above cited patents are somehow canonical versions of patents derived thereof.

### 3. TOPOLOGICAL ORGANISATION, LOCATION DETERMINATION & SECURITY

OSI layer transversal mechanisms include topology control, determination of node locations and security. A few patents have emerged recently in this area and they shall be discussed in subsequent sections.

#### 3.1. Topological Organisation

In [61], the authors propose a suitable organisation protocol which includes the formation of clusters. Each cluster is composed of a plurality of WSN nodes and each node is in possession of multiple radios thereby supporting simultaneous communications among sensors. This facilitates multi-hopping between the clusters via gateway nodes with two radio interfaces. Each node comprises at least one network discovery and self-assembly protocol which automatically forms the local network clusters using the radios and also determines with which other nodes to communicate and which role to take (leader, gateway, simple node). Routing, MAC and scheduling protocols are also proposed but are beyond this paper.

In [62], it is argued that special distributed mechanisms are vital in controlling the topology of a WSN, most notably the cluster size which, on one hand, determines the amount of power needed to reach the next cluster head and, on the other hand, the amount of relaying hops and hence (redundant) relaying traffic. Topology control is traditionally done by adjusting transmission and receiver sensitivity levels and have a goal to maintain network connectivity and optimise various performance metrics, such as network lifetime and throughput; the adjustment is usually done by means of some geographic information on the nodes' position which is not realistic for WSNs. To this end, [62] proposes that each node sends a discovery message in all directions (without discussing the energy cost associated with this procedure). Each node hence discovers a set of

neighbouring nodes using the set of responsive incoming signals. Each node then makes a local decision about a substantially optimal transmission power with which to communicate with at least a subset of the discovered neighbouring nodes. This approach has been shown to increase network lifetime by allowing each node to locally determine an efficient and sufficient power with which to communicate with (specific) other nodes in the network, whilst maintaining connectivity.

Parkin [63] is an important patent and bases on the observation that - whilst many WSN algorithms are designed to maximise the network lifetime once the network is already deployed - the actual energy consuming process is during ramp-up of the network when no organisational structures are yet available; this has also been confirmed by real-world roll-outs, such as Coronis' meter reading solutions [14]. Confirmed by theory [64], they also observe that building clusters during ramp-up is a suitable solution to WSNs. This is traditionally achieved by means of cluster head election processes, the two most popular being Lowest ID (LID) and Highest Degree (HD) election. It is known, however, that LID can cause node isolation and hence significant message energy to solve this connectivity problem. The HD process itself may consume a lot of energy due to overhead which is needed to determine which nodes have the highest connectivity degree. The inventors of [63] hence propose a cluster head election process of low energy. To this end, one node in the WSN is selected to broadcast the commencement of the initialisation by means of an initialisation message which contains a timing variable of the maximum time allowed for initialisation; if this maximum time is already known then this variable not need to be stored. Upon reception of the initialisation message, each node starts a timer which is initialised to a predetermined start time, and also randomly picks a number between a start time (which might be unique to each node) and the maximum allowed initialisation time. This random time is then used to compete for coordinator status, i.e. when the timer of a node matches its internally generated random number; the node transmits a request for coordinator by broadcasting a respective request to its neighbours. Upon receiving a request for coordinator status message, the receiving node relinquishes its right to become a coordinating device and becomes a slave device to the node that transmitted the request (i.e. the coordinator device) [63]. Acknowledgements might be sent; furthermore, a node may receive more than one coordinator request requiring one of a set of possible solutions detailed in [63]. Interestingly, the elected coordinators are nearly uniformly distributed and no node is left unconnected. Furthermore, the entire process requires only one transmission from regular nodes and several low duty cycle transmissions from elected coordinators.

Finally, [65] offers a framework to facilitate auto-configuration and auto-organisation of the WSN and the installation of communication protocols at network ramp-up. It has been proposed to simultaneously proceed with the election of leaders, a virtual communications backbone and suitable communication protocols facilitating the sensor readings to be delivered to a given set of sinks. To this end, the allowable addressing space is shared and dynamically allocated; it is maintained and managed by a subset of the

nodes in the network which play a particular role in the organisation. Thanks to the fusion of the auto-configuration and auto-organisation mechanisms, a newly arriving node can use the already ramped-up communication structure to obtain a valid address; it hence uses only one procedure to carry out two tasks. Resorting simultaneously to the two mechanisms makes it possible to make the network operational more quickly than a traditional approach where the stages of configuration and organisation are done sequentially, and thereby saving a significant amount of energy.

### 3.2. Location Determination

Many communications protocols presuppose the knowledge of the location of WSN nodes. It has not been proposed to use GPS which is clearly not applicable to energy-constrained WSNs, nor would it yield results for indoor roll-outs. Other localisation methods include the use of train-gulation-based multidimensional scaling, convex optimisation, and semi-definite programming relaxation; these, however, also have their drawbacks. Subsequent protocols hence aim at alleviating this problem and propose location determination solutions tailored to WSNs. Generally, however, the resolution of the local determination algorithms depends on the precision of the underlying clocks as well as the sampling rate of the transceivers. Subsequent patents hence discuss various trade-offs to achieve location determination.

The inventors of [66] provide a method for determining the location of nodes in a three dimensional space up-to a few centimetres and also allows determining the relative drift and offset w.r.t. neighbouring nodes. The mechanism can be divided into three distinct phases, each phase has one or more communication cycles, and each cycle carries out the exchange of information among the nodes. In more details, the three phases are the measurement, information exchange and computation phase. The measurement phase consists of several measurement cycles, where in each cycle each node transmits a packet containing its identifier and transmit time stamp according to its own clock. Each node also receives the neighbours' packets and records the receive time stamp of each packet. In the information exchange phase, each node transmits the neighbours' receive time stamps. Finally, during the computation phase, each node computes the spatial location and clock attributes of the other nodes relative to itself, which are described in details in [66].

The inventors of [67] describe a solution which facilitates localisation of WSN nodes quickly enough for real-time applications as well as for large-scale roll-outs with several tens of thousands of nodes. This is achieved iteratively, where at each iteration only a part of the total nodes' location is estimated, which is aided by the knowledge of anchor nodes and those nodes the position of which had already been estimated. At each iteration, the selected subset of nodes and anchors, together with their distance measurements from three known anchor nodes and known anchor locations, form a semi-definite programming relaxation problem, which can easily be solved by means of known algorithms. The choice of subset selection can be done dynamically and be based on some intelligent rules. Nodes, the location of which has been determined with satisfactory precision, are declared as anchor nodes. The algorithm can

be used in two and three dimensional realisations, as well as be applied to static and dynamic networks.

The inventor of [68] proposes an interesting approach for location determination by fusing inputs from systems providing qualitatively and quantitatively entirely different readings. Such a data fusion is based on the Dempster-Shafer theory of evidence. In the invention, it is assumed that the device fuses data from a GPS receiver, a wireless signal detector, a pedometer, and a digital compass, among others. It is argued that GPS-based solutions target outdoors but do not consider indoors, whereas embedded sensing systems work primarily indoors but are not designed for outdoors. Multiple sensors and data fusion can overcome this separation by leveraging the relative strengths and weaknesses of available readings in different environments [68]. The fusion is achieved by running several standard classification algorithms on the received data, e.g., an artificial neural network, a Bayesian classifier, an inductive decision tree classifier, etc. The outputs from the individual classifiers are then finally fused to make a decision on the location of the measurement taking node.

Srinivasan [69] proposes a hybrid localisation method where the WSN nodes switch between different localisation techniques in dependency of the network conditions. This gives potentially the best possible location accuracy for the set of known location determination algorithms. The innovative issue of this patent is the way the switching point is determined, where the inventors propose either to use a confidence metrics imposed by topological constraints or even to use statistical switching based on prior simulation or measurement results.

### 3.3. Security

Although security is strictly speaking, facilitated by one of the OSI layers, it shall be treated here because the energy consumption needed for the exchange of keys strongly depends on underlying MAC and routing protocols.

As outlined in the first section of this paper, security is utmost vital to WSNs; however, due to the severe constraints in energy, a unique solution for all types of sensors cannot exist. For instance, early Smart Dust sensors with the ATMEL 90LS8535 processor had only 8 Kb of program memory, 512 bytes for data memory and processors with 32 8-bit general registers that run at 4 MHz; in contrast, the MIPS R4000 processors are over an order of magnitude more powerful [70]. Either processor hence requires a special solution to accommodate security. Security usually bases on cryptography, although other methods have also begun to emerge for WSNs. It is fairly well established that the typical asymmetric (public-key) cryptosystems is impractical because too power consuming.

To this end, the inventors of [70] argue that symmetric-key ciphers, low-energy authenticated encryption modes and hash functions are advantageous in protecting WSN communications. They also observe that a single-key solution is dangerous because it takes one node to be captured or reverse-engineered to be able to intercept communication in the entire network. A potential solution would be a pair-wise private sharing of keys between every two WSN nodes; however, this requires a pre-distribution and storage of a

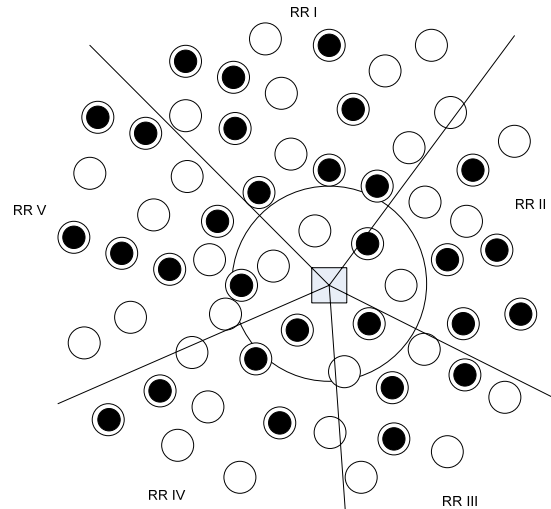
very large number of keys. Re-keying could also be invoked, where keys are changed on the run, but this is very energy consuming from a communication point of view since transmission and reception of packets consume energy. To alleviate these problems, they propose a probabilistic key sharing among the WSN nodes by making use of a simple shared-key discovery protocol for key distribution, revocation, and node re-keying. The core of the invention is a random pool of keys selected from the key space; prior to deployment and under strict supervision, each WSN node chooses a random subset of keys (referred to as key ring) from the key pool as well as their identifiers. Any two nodes able to find a common key with a given probability within their key rings may use that key as their shared secret to initiate communication. To facilitate this, the network has to undergo a shared key discovery phase of the key management scheme, which can be coupled with any auto-organisation and auto-configuration protocol (see Section 3.1). Also, if a node is compromised or new nodes arrive, re-keying is envisaged.

As already alluded to above, [71] pointed out that public key cryptography has been severely limited by the problem of allowing users to reliably identify the public keys of their intended communication partners. Knowing of its potential overhead, they propose to construct a Public Key Infrastructure (PKI), where this approach designates one or more trusted public keys known by the members of the PKI. Any system having access to these trusted public keys can sign digital certificates containing the public keys of users and devices in the PKI. The grand problem addressed by the PKI is how to achieve key management and key distribution; however, unfortunately, the creation and management of PKIs is difficult and complex. [71] hence proposes a method for creating a simple-to-use secure credential infrastructure by using a location-limited channel, a.k.a. "instant PKI" which is simple to establish, configure and use without diminishing the security provided by the PKI.

US patent [72] is very similar to [71] in the sense that a random subset of keys is used to facilitate encryption. However, as per Fig. (11), they choose to use a more powerful sink node located in the centre of the WSN which triggers the key election procedure. WSN nodes then choose from a locally broadcasted key-ID list one key to be stored on each node and all other initially stored keys are deleted. They also propose an iterative mechanism which allows reaching the WSN edge. The proposed method is ideally applicable to reverse multicast traffic to the sink node, which is the pre-dominant traffic pattern in WSNs.

#### 4. CURRENT & FUTURE DEVELOPMENTS

The aim of this paper was to expose the rational and contents of latest patents related to wireless sensor networks (WSNs). Due to their unique constraints, most notably finite energy and low processing power, WSNs pose entirely novel challenges and a viable design is only feasible if all of the traditional domains, ranging from physics to IT, fuse. Whilst we have omitted patents created in the fundamental domains, such as physics, chemistry and biology, we have concentrated on patents in computing and communications. We have shown that even sub-communities therein need to



**Fig. (11).** Iterative local broadcast through routing regions (RR) until farthest node is reached [72].

cooperate to facilitate a useful design. For instance, low energy data aggregation methods are only feasible if computer scientists working on data bases work closely together with communication engineers working on MAC and routing protocols.

We have described patents classified by the OSI-layer, i.e. including PHY, MAC, network and application layers; we have also dwelled on more cross-functional patents, i.e. related to auto-organisation, location determination and security. Since the MAC takes a central role in the energy consumption of WSNs, a large amount of patents have emerged there, closely followed by tailored routing protocols and PHY layer solutions. The amount of published patents related to WSN-tailored data query and aggregation is sparse as of today (summer 2007).

In the near future, clearly, this gap will be closed and patents related to entire system solutions will emerge. In particular, there is a strong need for mechanisms which are highly scalable and provide network ramp-up, auto-organisation/configuration/healing, communication protocols, security and data management in a unified low-energy approach. This does not mean that a single solution shall exist; however, a global modelling framework for above-said issues would be advantageous to facilitate commercially viable designs.

Energy limitations and large-scale roll-outs being the predominant features of WSNs, an increasing number of patents tailored to these features are likely to appear in the near future.

As for the energy limitations, power harvesting solutions, such as [73-75] will be central to the functioning of any WSN. This will have implications on all other functionalities; for instance, if power can be harvested every 24h only, then MAC and routing protocols need accordingly be adapted.

As for the large-scale roll-outs, faults will occur with increasing likelihood where it is impossible to correct these in a network of tens of thousands of nodes. Therefore, patents related to fault correction will gain in importance; for instance, the provision of patches as proposed in [76] could be a solution.

I hope that these insights are of significance for emerging and future real-world installations, such as data collection, remote control solutions, wireless telemetry, automatic monitoring, metering solutions and smart environments such as homes, hospitals, and buildings of all kinds.

## ACKNOWLEDGEMENTS

The author would like to thank Abdelmalik Bachir (LIG/INPG), Gabriel Chegaray (France Telecom R&D), Thomas Watteyne (CITI/INSA & France Telecom R&D) and Jacques Pulou (France Telecom R&D) for the fruitful discussions and the provision of some figures and text. He would also like to thank the anonymous reviewers who helped to greatly improve the quality of the paper. This work was partially conducted under contract ARESA ANR-05-RNRT-01703.

## REFERENCES

- [1] Dohler M, *et al.* "The ARESA Project: Facilitating Research, Development and Commercialization of WSNs," *IEEE SECON 2007*, San Diego, USA, June 2007, to be published.
- [2] Embedded WiSeNts, IST Project FP6-004400, <http://www.embedded-isents.org>.
- [3] e-Sense, IST Project FP6-IP-027227, <http://www.ist-e-sense.org>.
- [4] Kahn JM, Katz RH, Pister KSJ. Next century challenges: Mobile networking for 'smart dust'. *Proc. MOBICOM*, Seattle, 1999; also at <http://www-bsac.eecs.berkeley.edu/archive/users/warneke-brett/SmartDust/index.html>
- [5] Burnstein A, Bult K, Chang D, Chang F, *et al.* "Wireless Integrated Microsensors", *Proceedings Sensors EXPO 1996*, Anaheim, CA., 1996.
- [6] Pottie G, Kaiser W. Wireless integrated network sensors. *Commun ACM* 2000; 43: 51-58.
- [7] Rabaey J, Ammer J, da Silva JL, Patel D. "PicoRadio: Adhoc wireless networking of ubiquitous low-energy sensor/monitor nodes," *IEEE Computer Society Workshop on VLSI 2000*, Orlando, FL April 2000; 9-12.
- [8] Römer K, Mattern F. "The design space of wireless sensor networks," *IEEE Communications Magazine* 2004; 11(6): 54-61.
- [9] Marron PJ, Saukh O, Kruger M, Grosse CU. Sensor Network Issues in the Sustainable Bridges Project, *EWSN*, Istanbul, Turkey, January 31 - February 2, 2005.
- [10] Kahn JM, Katz RH, Pister KSJ. "Mobile Networking for Smart Dust," *ACM/IEEE MobiCom 99*, Seattle, USA, 1999.
- [11] Sihavaran T, *et al.* Cooperating Sentient Vehicles for Next Generation Automobiles, *MobiSys'04*, Boston, USA, 2004.
- [12] Martinez K, Ong R, Hart J. Glacsweb: a sensor network for hostile environments," *IEEE SECON*, Santa Clara, USA, 2004.
- [13] Pacelli M, Loriga G, Taccini N, Paradiso R. Sensing Fabrics for Monitoring Physiological and Biomechanical Variables: E-textile solutions, *3<sup>rd</sup> IEEE-EMBS International Summer School and Symposium on Medical Devices and Biosensors*, MIT, Boston, USA, Sept.4-6, 2006.
- [14] Coronis, [www.coronis.com](http://www.coronis.com).
- [15] Arch Rock, [www.archrock.com](http://www.archrock.com).
- [16] Crossbow, [www.xbow.com](http://www.xbow.com)
- [17] Moteiv, [www.moteiv.com](http://www.moteiv.com).
- [18] Dust Networks, [www.dust-inc.com](http://www.dust-inc.com)
- [19] Maxfor, [www.maxforco.kr](http://www.maxforco.kr).
- [20] TinyOS Community, [www.tinyos.net](http://www.tinyos.net).
- [21] Gilles P. "Ubiquitous Networks & Smart Devices: New Telecom Services & Evolution of Human Interfaces," *ITU Workshop on Ubiquitous Network Societies*, Geneva, April 6-8 2005.
- [22] Michael JS, Jamie RL. Smart dust: nanostructured devices in a grain of sand. *Chem Commun* 2005; 11: 1375.
- [23] Wicker, S. B., Fine, T. L.: US20026404750 (2002).
- [24] Gelvin, D.C., Girod, L.D., Kaiser, W.J., Merrill, W.M., Newberg, F., Pottie, G.J., Sipos, A.I., Vardhan, S.: WO0126068 (2001).
- [25] Gelvin, D.C., Girod, L.D.: WO0126335 (2001).
- [26] Gelvin, D.C., Girod, L.D.: WO0126334 (2001).
- [27] Gelvin, D.C., Girod, L.D.: US20046832251 (2004).
- [28] Gelvin, D.C., Girod, L.D.: US20046826607 (2004).
- [29] Gelvin, D.C., Girod, L.D.: US20056859831 (2005).
- [30] Gelvin, D.C., Girod, L.D.: US20046735630 (2004).
- [31] Dohler, M., Aghvami, A.H.: WO0403003672 (2004).
- [32] Dohler M, Li Y, Vucetic B, Aghvami AH, Arndt M, Barthel D. Performance Analysis of Distributed Space-Time Block Encoded Sensor Networks. *IEEE Trans Vehicular Technol* 2006; 55 (7): 1776-1789.
- [33] De Amorim, C.L., Kostin, S.: WO05069716 (2005).
- [34] Dowla, F.U., Nekoogar, F., Spiridon, A.: US2005286610 (2005).
- [35] Miao, G.J.: US20067002470 (2006).
- [36] Lal, D., Keshavarzian, A.: US2007129011 (2007).
- [37] Ye W, Heidemann J, Estrin D. "An energy-efficient MAC protocol for wireless sensor networks". *IEEE Infocom*, New York, NY, July 2002; 1567-76.
- [38] Bachir A. Lifetime Extension of WSNs by means of Routing and MAC Protocols, LIG-INPG, Grenoble, France, January 2007.
- [39] Shao, H.-R., Vuran, M.-C., Shen, C.: US2005074025 (2005).
- [40] Varaiya, P., Coleri, E.S.: US2005122231 (2005).
- [41] Yoon, C.-J.C.: US2006128349 (2006).
- [42] Barthel, D., Bachir, A.: WO07031685 (2007).
- [43] Watteyne, T., Bachir, A., Augelblum, I.: FR0605491 (2007).
- [44] Kushalnagar, N., Chhabra, J., Yarvis, M.: US2006209715 (2006).
- [45] Keshavarzian, A., Venkatraman, L.: US2007097895 (2007).
- [46] Yoon, C.-J.: GB2426411 (2006).
- [47] Kim, S.-J., Wang, X., Madihan, M.D.: US2007058664 (2007).
- [48] Mao, S., Hou, Y.T.: US2006077918 (2006).
- [49] Zhang, H.G.: CN1794732 (2006).
- [50] Choi, J.M., Ko, Y.B., Kim, J.H.: KR060006583/US2006013154 (2006).
- [51] Bachir, A., Barthel, D.: WO06114511 (2006).
- [52] Falck, T., Masegosa, D.M.P.: WO06100620 (2006).
- [53] Shin, Y.S., Choi, H.S., Park, I.L.G., Park, S.M.: US2007060147 (2007).
- [54] Pister, K.S.: US2006029060 (2006).
- [55] Pister, K.S., Zats, Y., Contant, R.A., Treuhaft, N.: EP1730910 (2006).
- [56] Mulgand, S., Mohindra, S., Fricke, R.: WO02058327 (2002).
- [57] Paradiso, J.A., Laibowitz, M.J.: US2006046664 (2006).
- [58] Lee, S.K., Yoo, J.J., Park, W.C., Kim, Y.H.: KR050108533 (2005).
- [59] Whisnant, K.A., Gross, K.C.: US2007055476 (2007).
- [60] Brunn, B.T., Macconnell, J.W., Maleysson, L., Lofstad, E.: US20016333975 (2001).
- [61] Elson, J., Girod, L.D., Kaiser, W.J., Merrill, W., Newberg, L.F., Schiffer, B., Sohrabi, K.: US2003012168 (2003).
- [62] Bahl, P., Li, L., Wang, Y.-M., Wattenhofer, R.P.: US2002044533 (2002).
- [63] Perkins, M.R., Correal, N.S., Huang, J., Huang, Y.: WO04049079 (2004).
- [64] Dohler M, Watteyne T, Barthel D, Valois F, Lu J. Kumar's, Zipf's and Other Laws: "How to Structure an Optimum Large-Scale Wireless (Sensor) Network"? , *European Wireless, April 2007, Conference CD-ROM*, invited paper 2007.
- [65] Lu, J., Valois, V., Barthel, D., Dohler, M.: FR0651143 (2006).
- [66] Agrawala, A.K., Larsen, R.L., Shankar, A.U., Szajda, D.C.: US2005020275 (2005).

- [67] Jin, H.H.: WO07002286 (2007).
- [68] Kulyukin, V.A.: US2007018890 (2007).
- [69] Srinivasan, B., Ravula, S.: US2007111735 (2007).
- [70] Eschenauer, L., Gligor, V.D.: US2005140964 (2005).
- [71] Smetters, D.K., Durfee, G.E., Balfanz, D., Grinter, R.E., Stewart, P.J., Wong, H.-C.: EP1513288 (2005).
- [72] Girao, J., Westhoff, D., Acharya, M.P.: US2007078817 (2007).
- [73] Cohen, M.H.: US2007109121 (2007).
- [74] Langley II, J.B., Liaw, B.Y., Wecker, S.A.: WO07059367 (2007).
- [75] Kokossalakis, G., Kausel, E.: WO07076039 (2007).
- [76] Broad, A.S., Miller, M., Horton, M.A.: US20077176808 (2007).