Low-Power Wireless Sensor Network Platforms

Jukka Suhonen, Mikko Kohvakka, Ville Kaseva, Timo D. Hämäläinen, and Marko Hännikäinen

Abstract Wireless sensor network (WSN) is a technology comprising even thousands of autonomic and self-organizing nodes that combine environmental sensing, data processing, and wireless multihop ad-hoc networking. The features of WSNs enable monitoring, object tracking, and control functionality. The potential applications include environmental and condition monitoring, home automation, security and alarm systems, industrial monitoring and control, military reconnaissance and targeting, and interactive games. This chapter describes low-power WSN as a platform for signal processing by presenting the WSN services that can be used as building blocks for the applications. It explains the implications of resource constraints and expected performance in terms of throughput, reliability and latency.

1 Characteristics of Low-Power WSNs

A WSN consists of nodes that are deployed in the vicinity of an inspected phenomenon [2] as shown in Fig. 1. In addition, a network may contain one or more sink nodes that request other nodes to perform measurements and collect the measured values for further use. Instead of sending raw data to the sink, a sensor node may collaborate with its neighbors or nodes along the routing path to provide application results [46]. The sink node typically acts as a gateway to other networks and user interfaces [22]. The backbone infrastructure that is connected to a sink may contain components for data storing, visualization, and network control.

J. Suhonen (✉) • V. Kaseva • T.D. Hämäläinen • M. Hännikäinen
Tampere University of Technology, Korkeakoulunkatu 1, FI-33101 Tampere, Finland
e-mail: jukka.suhonen@tut.fi; ville.a.kaseva@tut.fi; timo.d.hamalainen@tut.fi; marko.hannikainen@tut.fi

M. Kohvakka
Suntrica Ltd, Örninkatu 15B28, FI-24100 Salo, Finland
e-mail: mikko.kohvakka@suntrica.com

S.S. Bhattacharyya et al. (eds.), *Handbook of Signal Processing Systems*,
DOI 10.1007/978-1-4614-6859-2_13,

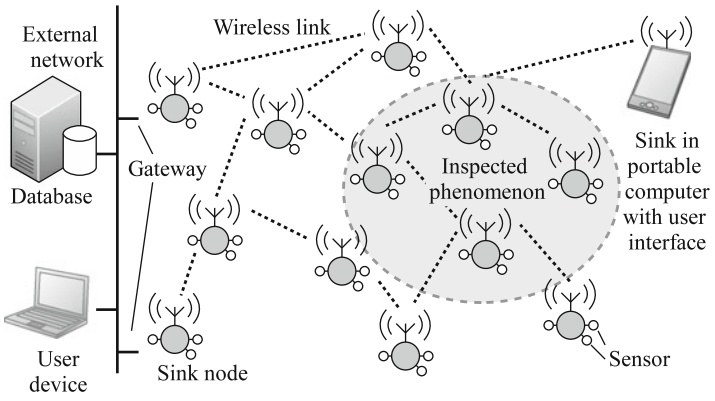

Fig. 1 A typical WSN scenario

Compared to the traditional computer networks, WSNs have several unique characteristics as listed in the following. A particular WSN installation might not require all of these characteristics, but many useful classes of WSNs share most or all of the properties described in this list.

- *Network size and density*: WSNs may consist of tens of thousands of nodes. The density of nodes can be high, depending on the application requirements for sensing coverage and robustness via redundancy.
- *Communication paradigm*: In WSNs, node identifiers are typically not important. Instead, WSNs are *data-centric*, which means that messages are not send to individual nodes but to geographical locations or regions based on the data content.
- *Application specific*: A WSN is deployed to perform a specific task, e.g. environmental monitoring, target tracking, or intruder alerting. As a result, the node platforms and communication protocols are designed to optimal performance on a certain application-dependent scenario. The application specific behavior enables data aggregation, and in-network processing, and decision making.
- *Network lifetime*: WSNs are typically deployed to observe certain physical phenomenon that range in duration from fractions of a second to a few months or even several years. As replacing batteries is not feasible due to large network size and deployment to possibly hazardous environment, nodes must optimize their energy usage for network lifetime.
- *Low cost*: To allow cost effective deployment of a large number of nodes, the cost of an individual sensor node should be minimized. Also, as recovering sensors after deployment in some application scenarios may not be feasible, sensors should be cheap enough to be considered disposable.
- *Resource constraints*: A typical WSN node combines low cost with small physical size and is battery powered. Thus, computation, communication, memory, and energy resources are very limited.

Table 1 Comparison of typical requirements in wireless computer networks and low-energy WSNs

Requirement	Computer network	Low-energy WSN
Resource constraints	Low	Very high (1–2 MIPS, 32–128 kB)
Adaptivity	Static	Dynamic environment
Scalability	Moderate (10 nodes)	High (10,000 nodes)
Latency	High (250 ms to 1 s)	High-low (1 s to 1 h)
Throughput	Very high (MB/s)	Low-moderate (bit/s to kbit/s)

- *Dynamic nature*: Wireless communications are inherently unreliable due to environmental interferences. The unreliability is especially evident in WSNs because of harsh operating conditions e.g. due to environmental changes in outdoors, node mobility, and nodes dying due to depleted energy sources. As a result, the unreliability causes network dynamics due to link breaks even when nodes are stationary.
- *Deployment*: To avoid tedious network planning of a large number of nodes, WSNs are often randomly deployed. This necessitates network self-configuration and autonomous operation.

1.1 Quality of Service Requirements

Quality of Service (QoS) is commonly expressed and managed by throughput, latency, jitter, and reliability. These QoS parameters also apply to the WSNs, but their importance differs from the legacy networks.

The requirements of low-energy WSNs compared to the traditional wireless computer networks, e.g. IEEE 802.11 Wireless LAN (WLAN), are summarized in Table 1. Sensing applications can tolerate high latency and low throughput but the reliability is particularly significant. In the traditional computer networks, the data is routed via highly reliable wired links, while only the end links may be wireless, utilizing e.g. cellular connections or WLAN. In WSNs, packets are forwarded via multiple wireless hops. On each wireless link, the packet error rates (PER) of 10–30 % are common, which significantly decreases the end-to-end reliability.

In addition to the traditional QoS metrics, other metrics can be identified for WSNs as presented in Fig. 2. While the reliability metric denotes the probability to transfer a single measurement through the network, the availability expresses the probability to receive a new measurement from a node within a certain waiting period [50]. The data accuracy describes the consistency of measurements (results are same in similar conditions) and the granularity of sensor values, sensing location, and time information. The security ensures that unauthorized parties do not gain access or tamper with the sensed data. The mobility is important in tracking WSNs as a node may be attached to moving objects. Due to the significance of the

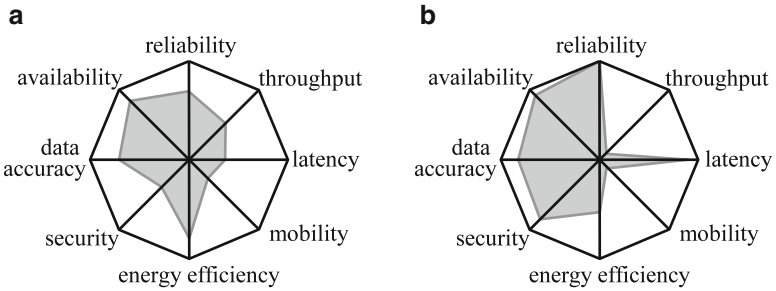

Fig. 2 Quality of Service (QoS) parameters in WSNs. (**a**) Typical environmental monitoring network emphasizing energy efficiency. (**b**) A control network emphasizing low latency and reliability

network lifetime, energy efficiency is considered as a QoS parameter. Usually, the other parameters have a trade-off with the energy efficiency, making it impossible to optimize all parameters at the same time.

As an example, the QoS requirements for two cases are presented in Fig. 2a and Fig. 2b. An environmental monitoring application sends sensor values periodically to a sink. As the sensed environment changes slowly, the measurement interval and thus throughput can be low, while missing a single sample is not critical. However, availability is still important, as too many samples may not be missed consecutively. In a control network, short messages are relayed infrequently between switches, lamps, and other accessories. Thus, the required bandwidth is low, but the timely and reliable delivery of commands is required.

Due to the diversity of applications and their contradictory requirements, a single solution is not suitable for every WSN application. Thus, the protocols and node platforms need to be tailored to meet the application requirements.

1.2 Services for Signal Processing Applications

A WSN offers following services for signal processing applications.

- *Environmental sensing*: Each WSN node contains at least one or several physical sensors. Instead of accessing nodes directly, e.g. via Inter-Integrated Circuit (I2C) bus, sensing services operate via standardized interfaces.
- *Data processing and storage*: Before the sensor values can be forwarded to a user, the values are preprocessed and stored locally. The limitations of computing and storage can be overcome by distributed computing services.
- *Data transfer*: Data transfer services allow collecting data for further use. The realized QoS is largely affected by the choice of networking protocols.

- *Localization*: A sensor value is naturally associated with a certain area. However, random deployment and mobility prevent concluding the location information from source node identifiers, which necessitates either online (distributed) or offline (centralized) localization services.
- *Time synchronization*: Several WSN applications, such as event alerts and tracking, require exact timestamping of sensor events to compare the order of events. As low cost sensor nodes do not have accurate time source, an agreement on global time is achieved with time synchronization service.

A WSN provides at least the sensing, data processing, and data transfer services. The localization and time synchronization services are not usually considered in proposed WSN standards but need customized solutions.

2 Key Standards and Industry Specifications

In the sensor industry, a vast number of sensors exists to measure physical parameters, such as temperature, pressure, humidity, illumination, gas, flow rate, strain, and acidity. Standardized sensor interfaces, data formats, and communication protocols are required to enable effective integration, access, fusion, and the use of sensor-derived data. The goal is to allow sensors from different manufacturers to work together without human intervention and customization.

2.1 IEEE 1451

IEEE 1451 standard family defines a set of open, network-independent communication interfaces for connecting transducers (sensors and actuators) to microprocessors, instrumentation systems and networks. In IEEE 1451, a single sensor, an actuator, or a module comprising several transducers and any data conversion or signal conditioning (e.g. signal amplification or filtering) is referred to as Transducer Interface Module (TIM). Transducer Electronic Data Sheet (TEDS) describes a TIM and defines a set of commands to control and read data from the TIM. TEDS virtually eliminates error prone, manual entering of data and system configuration and allows transducers to be installed, upgraded, replaced or moved with plug-and-play principle. IEEE 1451 provides interfaces for several standardized communication protocols by IEEE 1451.2 through IEEE 1451.6.

IEEE 1451.2 defines wired point-to-point communication. IEEE 1451.3 defines distributed multi-drop system, where a large number of TIMs may be connected along a wired multi-drop bus. IEEE 1451.4 specifies mixed-mode communication protocols, which carry analog sensor values with digital TEDS data. IEEE 1451.6 defines a high-speed Controller Area Network (CAN) bus. IEEE 1451.5 standard

Table 2 The properties of WSN communication standards

			Protocol layers					Security	
Standard	Frequency	Data rate	PHY	MAC	NWK	TRP	APS	ACL	Encr.
IEEE 802.15.4	868 MHz	20 kbps	✓	✓	–	–	–	✓	✓
	915 MHz	40 kbps	✓	✓	–	–	–	✓	✓
	2.4 GHz	250 kbps	✓	✓	–	–	–	✓	✓
ZigBee	–	–	–	–	✓	✓	✓	✓	✓
WirelessHART	2.4 GHz	250 kbps	✓	✓	✓	✓	✓	✓	✓
ISA100.11a	2.4 GHz	250 kbps	✓	✓	✓	✓	✓	✓	✓
Z-Wave	865 MHz	40 kbps	✓	✓	✓	–	✓	–	–
	915 MHz	40 kbps	✓	✓	✓	–	✓	–	–
Bluetooth									
Low energy	2.4 GHz	1 Mbps	✓	✓	✓	✓	✓	–	✓
ANT/ANT+	2.4 GHz	1 Mbps	✓	✓	✓	–	✓	✓	–
DASH7	433 MHz	27.8 kbps	✓	✓	–	–	–	–	–
IEEE 1902.1 RuBee	131 kHz	1.2 kbps	✓	✓	–	–	–	–	–

defines wireless sensors and thus, it is most closely related with WSNs. Supported communication technologies are IEEE 802.11a/b/g, IEEE 801.15.1, and IEEE 802.15.4.

2.2 WSN Communication Standards

The operating frequency band, nominal data rate, and protocol support of key WSN communication standards and industry specifications are listed in Table 2. The support for PHYsical (PHY), Medium Access Control (MAC), Network (NWK), and Transport (TRP) protocols denotes that a standard defines the layer in question. Application Support (APS) defines application profiles detailing the services, message formats, and methods required to access applications, therefore allowing interoperability between devices from different manufacturers. For security, Access Control Lists (ACLs) allow only certain nodes to participate in the network while data encryption prevents unauthorized use of data. The listed standards use 128-bit Advanced Encryption System (AES) for data encryption.

IEEE 802.15.4 network supports three types of network devices: a Personal Area Network (PAN) coordinator, coordinators, and devices. The PAN coordinator initiates the network and operates often as a gateway to other networks. Coordinators collaborate with each other for data routing and network self-organization. Devices do not have data routing capability and can communicate only with coordinators.

ZigBee standard defines network and application layers on top of the IEEE 802.15.4. The network layer supports star, peer-to-peer, and cluster-tree topologies. A ZigBee network has always one device referred to as a ZigBee coordinator that controls the network. The coordinator is the central node in the star topology, the

root of the tree in the tree topology, and can be located anywhere in the peer-to-peer topology. ZigBee defines a wide range of application profiles targeted at home and building automation, remote controls, and health care.

WirelessHART and ISA100.11a [20] are targeted at process industry applications where process measurement and control applications have stringent requirements for end-to-end communication delay, reliability, and security. The standards have similar operating principle and the convergence of the standards is planned in ISA100.12. Both standards build on top of the IEEE 802.15.4 physical layer and utilize a TDMA MAC that employs network wide time synchronization, channel hopping, channel blacklisting. A centralized network manager is responsible for route updates and communication scheduling for entire network. However, as the centralized control of TDMA schedules limits the network size and the tolerance against network dynamics, the usability of the standards in WSNs is limited to static networks.

Z-Wave is targeted for the control of building automation and entertainment electronics. It has been developed by over 120 companies including Zensys, Intel and Cisco. Supported network topologies are star and mesh. The maximum number of nodes in a network is 232, although Z-wave networks can be inter-connected via gateways.

Bluetooth Low Energy is an extension to the Bluetooth technology and is aimed at low energy wireless devices. The first defined applications comprise watch, Human Interface Device (HID), and sensor profiles. Compared to the traditional Bluetooth, the main functional differences are the use of variable packet length, entering power save mode automatically when a device is not transmitting, and the exchange data in attribute/value pairs.

ANT developed by Dynastream Innovations is based on a star-topology, but more complex topologies can be achieved by using several channels: each node can be simultaneously a master and a slave on different channels. Master nodes always receive, while slaves transmit when new data is provided. A practical limit for network size is few thousands nodes. ANT+ is an extension to the ANT protocol that includes profiles for data formats and channel parameters. The disadvantages of ANT are high power consumption in master nodes and low scalability due to random access transmissions.

DASH7 is based on ISO 18000-7 standard and is targeted at low data rate applications. Its main cited benefit stems from the 433 MHz operating frequency, which provides longer communication ranges and less crowded wireless channel than the typical 2.4 GHz frequency band [36]. DASH7 has the nominal communication range of 250 m at 0 dBm transmission power level, compared to 75 m of ZigBee and 10 m of Bluetooth (High Rate variant) [36].

IEEE 1902.1 (RuBee) fills the gap between WSN and Radio Frequency IDentification (RFID) technologies. It uses magnetic dipole antennas instead of electric field signals. Thus, the signal is unaffected by water, while metals either enhance or do not affect the signal. The small 1.2 kbps nominal data rate limits the applicability of RuBee.

3 Software Components

The software components in WSNs include sensor operating systems and middleware as shown in Fig. 3. The purpose is to ease the application development by providing network access and allowing support for heterogeneous platforms by abstracting hardware access.

3.1 Sensor Operating Systems

An operating system targets at easing the use of system resources. Its main functions are the concurrent execution and communication of multiple applications, access and management of Input/Output (I/O) devices, permanent data storage, and control and protection of system access between multiple users [48]. WSN operating systems are required to have an extremely small memory footprint while still providing the basic OS services. Furthermore, a WSN OS should support energy management to allow power saving and real time task scheduling [27].

TinyOS [17] is the most widely known OS for WSNs that uses the event-driven approach. An event-driven OS reacts to hardware interrupts that indicate e.g. reception of data from transceiver, a timer event, or finished sensing. TinyOS was originally implemented for Berkeley mote, but has been later ported to many other platforms. Software is divided into components encapsulated in frames. Each component has a separate command handler for upper layer requests and an event handler for lower layer events. The processing is done in atomic tasks.

Contiki is another event based OS. It supports Internet Protocol (IP) routing and dynamic loading of application images as an application program module can be linked to the OS kernel during runtime. Contiki implements a support for preemptive multi-threading through a library on top of the event-handler kernel. Both Contiki and TinyOS are released as open source.

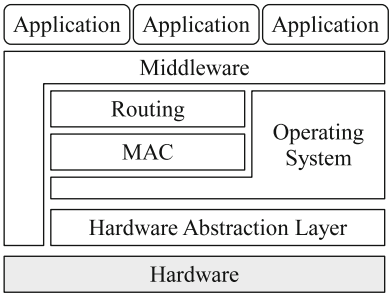

Fig. 3 Software architecture of a WSN node

3.2 Middlewares

Middleware is an application layer that consists of frameworks and interfaces that ease the application development, runtime configuration, and management in WSNs [46]. Several types of middlewares have been proposed for WSNs: middleware interfaces, database middlewares, virtual machines, mobile agents, and application driven middlewares [27]. The middleware interfaces aim to standardize hardware access, such as the transducer interface specification of IEEE 1451. Database middlewares overcome the memory constraints of individual sensor nodes by accessing the WSN as a distributed database. For example, TinyDB [31] is a query processing system implemented on top of the TinyOS. It supports basic Structured Query Language (SQL) type query operations and data aggregation for improving network energy efficiency. Virtual machines allow task propagation as a byte code, which enable its execution in heterogeneous sensor hardware.

A mobile agent is an object that in addition to the code carries its state and data. A mobile agent makes its migration and processing decisions autonomously. Typically, a mobile agent operates on top of a virtual machine to obtain platform independence and small object size.

The application driven middlewares support task allocation, networking, and distributed computing. The component library of the TinyOS includes the application driven middleware functionality as it provides methods for network communication and distributed services, and abstracts data acquisition, allowing programmer to concentrate on implementing the sensing applications.

4 Hardware Platforms and Components

Sensor node platforms implement the physical layer (hardware) of the protocol stack. The hardware activity measured as the fraction of time the hardware is in an active state (processing data or receiving/transmitting a packet) may be below 1 % in low data-rate monitoring applications. Thus, it is very important to minimize the power consumption in idle and sleep modes.

A general hardware architecture of a sensor node platform is presented in Fig. 4. The architecture can be divided into four subsystems:

- *Communication subsystem* enabling wireless communication,
- *Computing subsystem* allowing data processing and the management of node functionality,
- *Sensing subsystem* connecting the wireless sensor node to the outside world, and
- *Power subsystem* providing the system supply voltage.

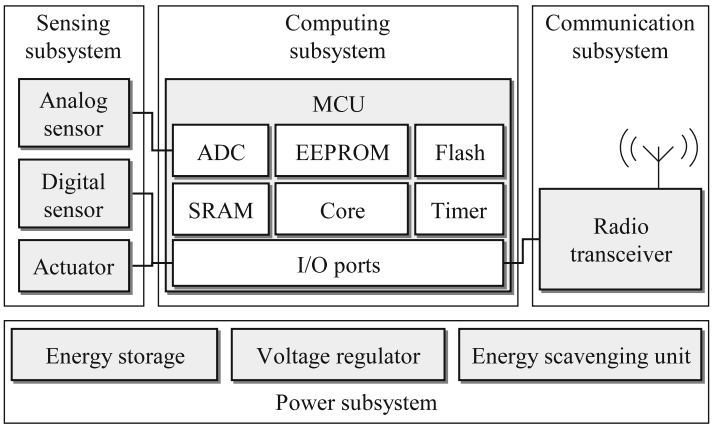

Fig. 4 Sensor node hardware architecture

4.1 Communication Subsystem

The communication subsystem consists of a wireless transceiver and an antenna. A wireless transceiver can be based on acoustic, optical or Radio Frequency (RF) waves. Acoustic communication is typically used for under water communications or measuring distances based on time-of-flight measurements [3]. The disadvantages are long and variable propagation delay, high path loss, noise, and very low data rate. Optical communication [55] has low energy consumption especially in reception mode, and it can utilize very small antenna. However, the alignment of a transmitter to a receiver is difficult or even impossible in large-scale WSN applications. RF communication combines the benefits of high data rate, long range and nearly omnidirectional radiation, making it the most suitable communication technology for WSNs. Disadvantages are large antenna size and higher energy consumption compared to the optical technology.

In general, an RF transceiver (radio) has four operation modes: transmit, receive, idle, and sleep. Radio is active in transmit and receive modes, when power consumption is also the highest. In idle mode, most of circuitry is shut down, but the transition to the active mode is fast. The lowest power consumption is achieved in sleep mode when all circuitry is switched off.

Most short-range radios utilized with WSNs operate in the 433 MHz, 868 MHz, 915 MHz, and 2.4 GHz license-free Industrial Scientific Medical (ISM) frequency bands. The 2.4 GHz band is the widest providing more channels, while obstacles have least effect on lower frequency bands. Depending on the frequency band and antenna type, operating range with 1 mW transmission power is from few meters to hundreds meters [25].

The characteristics of potential commercial low power radios are summarized in Table 3 [25]. Microchip, Nordic Semiconductor, and Texas Instruments utilize

Table 3 Radio features, current consumptions, and energy efficiencies

Radio	Data rate (kbps)	Band (MHz)	Buffer (B)	Sleep (μA)	RX (mA)	TX (mA)	RX (nJ/b)	TX (nJ/b)
MC MRF24J40	250	2,400	128	2	18	22	264	216
NS nRF2401A	1,000	2,400	32	0.9	19.0	13.0	39	57
NS nRF24L01	2,000	2,400	32	0.9	12.3	11.3	17	18
NS nRF905	50	433–915	32	2.5	14.0	12.5	750	840
RFM TR1001	115.2	868	no	0.7	3.8	12	313	99
RFM TR3100	576	433	no	0.7	7.0	10	52	36
SE XE1201A	64	433	no	0.2	6.0	11.0	516	281
SE XE1203F	152.3	433–915	no	0.2	14.0	33.0	650	276
TI CC2420	250	2,400	128	1	18.8	17.4	209	226
TI CC2500	500	2,400	64	0.4	17.0	21.2	127	102
TI CC1000	76.8	433–915	no	0.2	9.3	10.4	406	363
TI CC1100	500	433–915	64	0.4	16.5	15.5	93	99

Manufacturers: Microchip (MC), Nordic Semiconductor (NS), sRF Monolithics (RFM), Semtech (SE), Texas Instruments (TI)

on-chip buffers for the adaptation of a high-speed radio with a low-speed MCU. Current consumptions are specified at the lowest band and 0 dBm transmission power. The table indicates that data rate and frequency band has only a low effect on current consumption. The last two columns present the energy consumption with 3.0 V supply voltage, indicating that the radios operating at the 2.4 GHz frequency band are the most energy-efficient, which is mostly caused by their high data rates.

4.2 Computing Subsystem

The central component of a platform is processor unit that forms the computing subsystem. The processor unit is typically implemented by a MCU, which integrates a processor core with program and data memories, timers, configurable I/O ports, Analog-to-Digital Converter (ADC) and other peripherals. Flash memory is typically used as a program memory, while data memory consists of Static Random Access Memory (SRAM) and Electronically Erasable Programmable Read-Only Memory (EEPROM). WSN nodes utilize typically 1–10 Million Instructions Per Second (MIPS) processing speed. Memory resources typically consists of 1–10 kB of data memory and 16–128 kB of program memory.

The characteristics of potential MCUs from different manufacturers are compared in Table 4. The energy-efficiencies of MCUs can be compared according to their current consumption at one MIPS processing speed. The comparison indicates that Semtech XE8802 and Texas Instruments MSP430F1611 MCUs are the most energy-efficient [25].

Table 4 The comparison of the features of low power MCUs

MCU	FLASH (kB)	SRAM (kB)	EEPROM (*B*)	Sleep (µA)	1 MIPS (mA)
Atmel AT89C51RE2 (8051)	128	8	0	75	7.4
Atmel ATmega103L (AVR)	128	4	4,096	1	1.38
Atmel AT91FR40162S (ARM)	2,048	256	0	400	0.96
Cypress CY8C29666	32	2	0	5	10
Freescale M68HC08	61	2	0	22	3.75
Microchip PIC18LF8722	128	3.9	1,024	2.32	1.0
Microchip PIC24FJ128	128	8	0	21	1.6
Semtech XE8802 (CoolRisc)	22	1	0	1.9	0.3
TI MSP430F1611	48	10	0	1.3	0.33

Table 5 Features of typical sensors

Physical quantity	Example sensor	Accuracy	Active current	Sensing time	Energy cons.
Acceleration	VTI SCA3000	1 %	120 µA	10 ms	3.6 µJ
Air pressure	VTI SCP1000	150 Pa	25 µA	110 ms	8.3 µJ
Humidity	Sensorion SHT15	2 %	300 µA	210 ms	190 µJ
Illumination	Avago APDS-9002	50 %	2.0 mA	1.0 ms	6.0 µJ
Infra-red	Fuji MS-320	–	35 µA	cont.	–
Magnetic field	Hitachi HM55B	5 %	9.0 mA	30 ms	810 µJ
Position	Fastrax iTRAX03	1.0 m	32 mA	4.0 s	380 mJ
Temperature	Dallas DS620U	0.5°C	800 µA	200 ms	480 µJ

4.3 Sensing Subsystem

There exists a large variety of low power sensors suitable for WSNs [1]. Important requirements for sensors are low power consumption and short sensing time, which determine the energy consumption of a single sensing. In addition, adequate accuracy is required within the entire temperature range. The features of some example sensors are presented in Table 5. Most of the sensors fulfill the requirements well.

A WSN node can also operate as a decision unit, which takes sensor readings from the WSN as input and generates action commands as output. These action commands are then transformed into actions by actuators. Besides an electric switch and a servo drive, an actuator can be a mobile robot. In order to improve the reliability of actions, the robot can be a WSN node and act based on its own sensor readings and the data of the other WSN nodes in the network [1].

4.4 Power Subsystem

The power subsystem stores supply energy and converts it to an appropriate supply voltage level. The subsystem consists of an energy storage, a voltage regulator, and optionally an energy scavenging unit.

The energy storage can be a non-rechargeable (primary) battery, a rechargeable (secondary) battery, or a supercapacitor [39]. Primary batteries are cheap and have the highest energy density. They are the most common power source for WSNs. Secondary batteries have lower energy density and are more expensive, but they can be recharged only 500–1,000 times. Compared to secondary batteries, supercapacitors have lower energy density and they are more expensive. However, their lifetime is in the order of a million charging/discharging cycles. Supercapacitors are suitable to be used with an energy generator, since energy is typically generated in peaks during short periods of time, and the amount of stored energy can be relatively low.

The most potential sources for energy scavenging are photovoltaics and vibrations [45]. Solar cells are mature technology and they can provide up to 15 mW/cm^3 power at outdoor conditions. In indoor conditions, achieved power reduces to 10 $\mu W/cm^3$. A promising method for converting vibration to source power is a piezoelectric conversion. Commonly occurring vibrations can provide up to 200 $\mu W/cm^3$ power. Other possible energy sources are temperature gradients (40 $\mu W/cm^3$ at 5 °C temperature differential) and air flow (380 $\mu W/cm^3$ at 5 m/s).

4.5 Existing Platforms

WSN platforms have improved significantly during the last decade along with the advances in low power processing and communication technology. Still, due to the strict energy constrains, and the visions of complex networking and data fusion, it is not possible to fulfill all the requirements with the current level of technology. Thus, the platform research can be divided into two branches: high performance platforms, and low power platforms [16].

The high performance platforms have been developed for researching complex data processing and fusion in sensor nodes. The design target has been the reduction of transmitted data by efficient data processing. These platforms utilize high performance processors having at least tens of MIPS processing performance and hundreds of kilobytes program and data memories. For long-lived battery operation, their energy consumption is not adequate. However, these high power platforms can be used as a part of a WSN for data processing and data routing. Examples of the high performance platforms are Piconode [43], μAMPS [33], and Stargate [7].

Low power platforms are aiming to maximize the lifetime and minimizing the physical size of nodes. These are obtained by minimizing hardware complexity and energy consumption. These platforms are capable for performing low data rate communication and data processing required for networking and simple applications. The most essential sensor node platforms are listed in Table 6 [25].

Table 6 Comparison of existing low-power sensor node platforms

Platform	MCU	Sensors	Radio	RF band (MHz)	Sleep (μA)	Size (mm^2)
Mica	ATmega103L	No	TR1000	915	200–300	1,856
Mica2	ATmega128L	No	CC1000	433,915	17	1,856
Mica2dot	ATmega128L	No	CC1000	433,915	17	492
MicaZ	ATmega128L	No	CC2420	2,400	30	1,856
BTnode ver3	Atmega128L	No	ZV4002/CC1000	2,400/433,915	3,000	1,890
Medusa MK-2	ATmega128L + ARM7	T,L,A	TR1000	915	27	4,500
EYES node	MSP430	No	TR1001	868	5.1	2,600
ScatterWeb ESB	MSP430	L,AC,A,IR	TR1001	868	8	3,000
TinyNode	MSP430	No	XE1205	433–915	5.1	1,200
Tmote sky	MSP430	H,T,L	CC2420	2,400	5.1	2,621
ProSpeckz	CY8C29666	No	CC2420	2,400	330	704
TUTWSN LR	PIC18LF8722	T,L,H,A,IR	nRF905	433	31	8,100
TUTWSN LE	PIC18LF8722	T,L,H,A,IR	nRF24L01	2,400	24	2,800

Sensors: Acceleration (A), Acoustic (AC), Humidity (H), Light (L), Passive Infra-Red (IR), Temperature (T)

Besides the Commercial Off-The-Self (COTS) platforms presented in the table, a lot of research work has been conducted for developing System-on-a-Chip (SoC) platforms targeting to even smaller size and higher energy-efficiency. For example, a WiseNET SoC sensor node [9] developed in Swiss Center for Electronics and Microtechnology integrates a low-power radio with CoolRISC MCU core, low-leakage memories, two Analog-to-Digital Converter (ADC) and power management blocks. The reception mode current consumption is only 2 mA, which is nearly one order of magnitude less than in typical low power radios. Yet, the data rate is only 25 kbps. The transmission mode current consumption at 10 dBm output power is 24 mA. The sleep mode current consumption of the radio block is 3.5 μA.

At best, low power platforms can perform various sensing tasks and they enable the extending of network lifetime to even years. However, this necessitates an energy-efficient MAC protocol, which maximizes the time node spends in the sleep mode.

5 Medium Access Control Features and Services

The MAC sublayer is the lowest part of data link layer and it operates on top of the physical layer. A MAC protocol manages radio transmissions and receptions on a shared wireless medium and provides connections for overlying routing protocol. Hence, it has a very high effect on network performance and energy consumption.

5.1 MAC Technologies

MAC protocols can be categorized into contention and contention-free protocols. In contention protocols, nodes compete for a shared channel, while trying to avoid frame collisions.

As the power consumption of the low power radios in the reception mode is high, the energy-efficiency of the conventional MAC approaches is not adequate for the low energy WSN as such. Further energy saving is achieved by *duty cycling*: time is divided into a short active period and a long sleep period, which are repeated consecutively. These low duty-cycle protocols can also be divided into two categories: unsynchronized and synchronized protocols, according to the synchronization of data exchanges.

ALOHA [44] is the simplest contention protocol, where nodes transmit data without coordination. Slotted ALOHA reduces collisions by dividing time into slots and transmitting data on the slot boundaries only. Carrier Sense Multiple Access (CSMA) further reduces collisions and improves achievable throughput by checking channel activity prior to transmissions and avoiding transmission during busy channel situations.

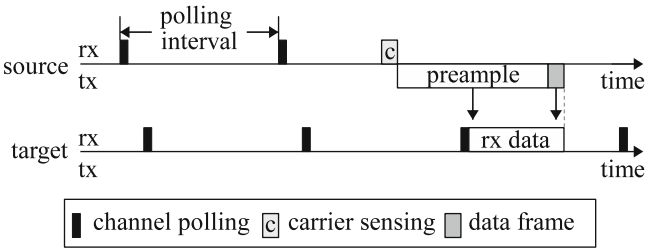

Fig. 5 Operation of unsynchronized low duty-cycle protocols

Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) [6] is a modification of CSMA, which reduces the congestion on a channel by deferring a transmission for a random interval (contention window). The contention window is increased if the channel is sensed to be busy (backoff), thus allowing the MAC to adjust to the network conditions. Still, collisions may occur due to a hidden node problem: nodes separated by two hops may not detect each other, and their transmissions may collide on a receiver that is located between the nodes. The hidden node collisions can be significantly reduced by performing a Request-To-Send (RTS)/Clear-To-Send (CTS) handshaking prior to a data transmission. Therefore, the handshaking is defined as an option in many CSMA/CA-based protocols. While contention-based protocols work well under low traffic loads, their performance and reliability degrades drastically under higher loads because of collisions and retransmissions.

In contention-free protocols, nodes get unique time slots or frequency channels for transmissions. Ideally, collisions are eliminated. Time Division Multiple Access (TDMA) divides time into numerous slots, where only one node is allowed to transmit on each slot. Other alternatives are Frequency Division Multiple Access (FDMA) and Code Division Multiple Access (CDMA), which provide contention-free operation by separate frequency channels and spreading codes, respectively. Contention-free protocols achieve high performance and reliability regardless of the traffic load. Yet, the bandwidth must be reserved in advance, which increases control traffic overhead.

5.2 Unsynchronized Low Duty-Cycle MAC Protocols

Unsynchronized low duty-cycle MAC protocols [40] are based on a Low Power Listening (LPL) mechanism, where nodes poll channel asynchronously to test for possible traffic, as presented in Fig. 5. Transmissions are preceded with a preamble that is longer than the channel-polling interval. Hence, the preamble part acts like a wake up signal. If a busy channel is detected, nodes begin to listen to the channel until a data packet is received or a time-out occurs.

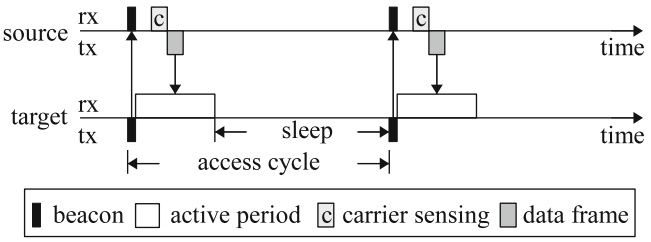

Fig. 6 Operation of synchronized low duty-cycle protocols

The drawback of the basic LPL mechanism is that the transmission and reception of long preamble increases energy consumption significantly. Therefore, several variations are proposed to reduce the preamble energy. For example, in X-MAC [4], a sender transmits multiple short preambles with the address of the intended receiver. Each preamble is followed by a short reception period. Upon receiving a preamble, the destination node sends an acknowledgment (ACK) between the preambles. Other nodes can enter early a sleep mode for reducing overhearing. After receiving the ACK, the source node begins the transmission of a data frame.

The preamble can be eliminated completely by utilizing an additional transceiver referred to as a wake-up radio [13]. The wake-up radio mechanism is based on the assumption that the listen mode of the wake-up radio is ultra low power and it can be active constantly. At the same time, the normal data radio is in the sleep mode as long as packet transmission or reception is not required. The wake-up radio protocols are successful in avoiding overhearing and idle listening in the data radio. Their major problems are the energy consumption and cost of the wake-up radio. In addition, the difference in the transmission ranges between data and wake-up radio may pose significant problems.

Unsynchronized protocols are relatively simple and robust, and require a small amount of memory compared to synchronized protocols. A general drawback is rather high overhearing, since each node must receive at least the beginning of each frame transmitted within radio range. Thus, they suit best for relatively simple WSNs utilizing very low data rates. Unsynchronized protocols tolerate dynamics in networks, but their energy-efficiency is limited by the channel sampling mechanism [58].

5.3 Synchronized Low Duty-Cycle MAC Protocols

Synchronized low duty-cycle MAC protocols utilize scheduling to ensure that nodes agree on the data exchange times. Due to the synchronized operation, nodes know the exact moments of active periods in advance, thus eliminating the need of long preambles. As a global synchronization is very difficult in large networks, the synchronization is often realized by receiving beacon frame from one or more neighbor nodes, as shown in Fig. 6. The beacon frame includes synchronization and

status information, such as the duration of the active period and the time between active periods. After a beacon, nodes exchange frames during the active period. The active period is followed by a sleep period to save energy. Together, the active period and the sleep period are referred to as an *access cycle*. The access cycle is repeated periodically.

For establishing the synchronized operation, neighboring nodes are typically discovered by a network scan. The network scan means a long-term reception of frequency channels for receiving beacons from neighbors, since their schedules and frequency channels are unknown. Clearly, this is energy-hungry. However, the synchronized operation after the network scan is very energy-efficient [58].

While the channel access in the unsynchronized protocols is usually contention-based, the synchronized MAC protocols use either contention-based, contention-free, or hybrid channel access mechanism.

Sensor-MAC (S-MAC) [57] utilizes purely contention-based channel access by using CSMA/CA with RTS/CTS mechanism. The protocol utilizes a fixed active period length and an adjustable, network specific wake up period. Neighboring nodes may coordinate their active periods to occur simultaneously to form virtual clusters. At the beginning of an active period nodes wake up and exchange synchronization (SYNC) frames for synchronizing their operation. The fixed access cycle length causes idle listening, which decreases energy efficiency. T-MAC [52] is a variation of the S-MAC that improves the energy-efficiency by adjusting the active period according to traffic. It utilizes a short listening window after the CTS phase and each frame exchange. If no activity occurs during the listening window, node returns to sleep mode.

IEEE 802.15.4 [19] standard defines a MAC layer that can use both contention-based and contention-free channel access. It operates on beacon-enabled and non-beacon modes. In the non-beacon mode, a protocol is based on a simple CSMA/CA. Energy-efficient synchronized low duty-cycle operation is provided by the beacon-enabled mode, where all communications are performed in a superframe structure. The superframe is divided into three parts: the beacon, Contention Access Period (CAP) and Contention Free Period (CFP). CAP is a mandatory part of a superframe during which channel is accessed using a slotted CSMA/CA scheme. CFP is an optional feature of IEEE 802.15.4 MAC, in which a channel access is performed in dedicated time slots. CFP can be utilized only for a direct communication with a PAN coordinator. Thus, its applicability and benefits are very limited in multi-hop networks. The cluster-tree type IEEE 802.15.4 network can provide comparably good energy-efficiency in static and sparse networks. The hidden node problem reduces performance in dense networks, since any handshaking prior to transmissions is not used.

TUTWSN MAC [25,27] is another example of protocol that uses both contention-based and contention-free channel access. The superframe structure is similar to the IEEE 802.15.4. However, instead of using carrier sensing, CAP and CFP are divided into fixed time-slots. To allow implementation on the simplest radios without carrier sensing capabilities, TUTWSN MAC uses slotted ALOHA on CAP. Each time slot

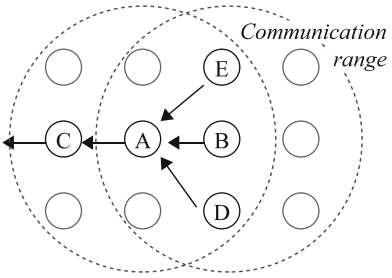

Fig. 7 Network topology in WSN MAC performance evaluation

is further divided into two subslots, first subslot is for data frame and the following subslot is for acknowledgment. The use of contention free slots is preferred as it eliminates collisions and thus increases reliability. The CAP is used only for joining a cluster and requesting reservations on CFP.

In the synchronized low duty-cycle protocols, the major advantage is that a sender knows a receiver's wake up time in advance and thus can transmit efficiently. In dynamic networks, synchronized links are short-lived and new neighbors need to be searched frequently, which increases energy consumption rapidly. In contention based protocols, a major disadvantage is the energy cost of receiving an entire active period [40]. Contention-free protocols have better energy-efficiency in stationary networks, but their performance reduces rapidly as network dynamics increases.

5.4 Performance Comparison

This section analyzes the performance of the low-energy MAC protocols. The results are based on the models presented in [25] and [58]. The models have the following assumptions:

- Each sensor node measures one sensor sample and forwards it to a next-hop node during one data generation interval.
- Each data frame is followed by an acknowledgment for fair comparison.
- There are no transmission errors nor collisions.
- There is no contention, and carrier sense attempts produce an idle result.
- The power consumption of idle listening equals to the reception mode power.
- The active time of MCU equals to the active time of radio.

Therefore, the performance models focus on the power consumption of the channel access mechanisms, while the effects of data processing, contention, and control frame exchanges are eliminated. For contention based protocols, the results are slightly better than in practice.

Energy consumptions are analyzed for a router node (A), and a leaf node (B) presented in Fig. 7. Both nodes have eight neighbors (n). Data generation interval (T_{DATA}) is equal for each node, and it varies from 1 to 1,000 s. Arrows in the figure

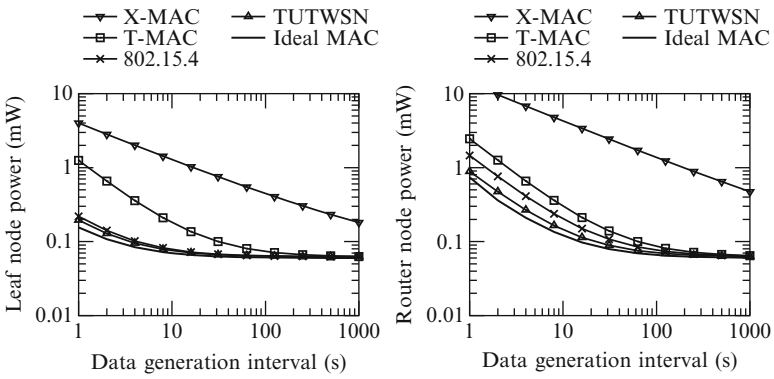

Fig. 8 Optimal power consumption of MAC protocols

indicate data routing directions. The traffic load is accumulated in routers, since they transmit their own data and the multi-hop routed data from n_{DL} nodes. For example, the router node C routes data from four nodes ($n_{DL} = A, B, D, E$).

Average power consumption (P) of a protocol is calculated by normalized transmission (t_{TX}) and reception (t_{RX}) activities and their power consumptions as

$$P = t_{TX}P_{TX} + t_{RX}P_{RX} + (1 - t_{TX} - t_{RX})P_S. \quad (1)$$

The normalized activity is determined by dividing the duration of an activity by the interval of the activity resulting in a percentage value of the activity. Data exchanges are normalized by T_{DATA} during which all nodes in the network generate exactly one data frame. Similarly, the transmission and reception activity for maintaining synchronization is normalized by T_{SYNC}.

The performance analysis assumes the commonly used TI CC2420 transceiver and Atmel ATmega128L MCU. As the transceiver and MCU constitute the majority of power consumption, other power consumption sources are ignored in the analysis.

Other analysis parameters are as follows. For fair comparison, all protocols use 8 B control frame (Beacon/ACK/RTS/CTS) length and 32 B data frame length. In IEEE 802.15.4 and T-MAC protocols, 2 ms average contention window is used, which conforms the default settings of IEEE 802.15.4 when there is no collisions. T-MAC uses 90 s synchronization interval, while TUTWSN utilizes 2 ALOHA slots per CAP. For realistic results, 20 ppm maximum clock drift was assumed. The clock drift reflects the inaccuracy of the timing crystals, which must be compensated by extra listening of the channel as a neighbor node might begin its transmission earlier or later than expected.

The power consumption with the analyzed protocols is presented in Fig. 8. In this analysis, the access cycle length (synchronized protocols) and the listening interval (LPL-based X-MAC protocol) are adjusted for lowest possible energy consumption. In the synchronized protocols, the optimal access cycle length ranges from 2 to 2,000 s as the data generation interval ranges from 1 to 1,000 s. The longer access

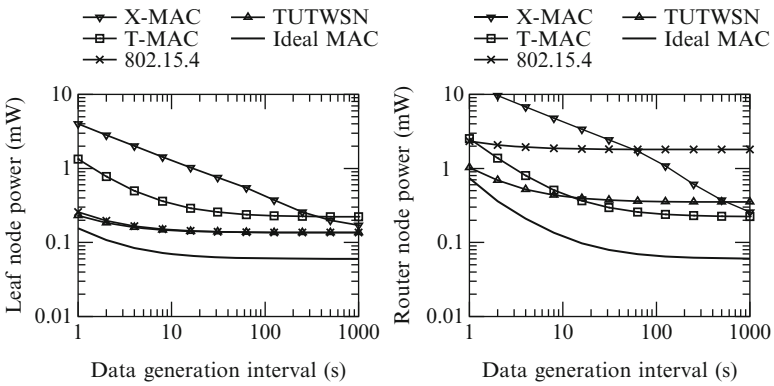

Fig. 9 Power consumption of MAC protocols, when maximum per-hop delay is 1 s

cycle saves energy, as beacons need to sent less frequently, while shortening the access cycle gives more capacity. The active period length is long enough to allow one data transmission. In the unsynchronized X-MAC, the channel listening interval ranges from 0.1 to 3.3 s. Long listening intervals make LPL-based protocols energy inefficient, because the transmission time of the preamble signal is relative to the channel listening interval.

Clearly, the synchronized protocols are potentially the most energy efficient choices for a WSN MAC. However, the energy efficiency has a trade-off with latency. The maximum per hop forwarding delay, assuming no packet errors and collisions, is the same as the access cycle length or channel listening interval. The average per hop delay is half of the maximum delay.

Figure 9 shows the power consumption of the protocols with comparable delays. On each case, the access cycle length is limited to 1 s. X-MAC uses 0.1–0.8 s between 1–64 s data generation intervals, as it allows better energy-efficiency.

TUTWSN and IEEE 802.15.4 are the most energy-efficient choices for leaf nodes, as they minimize idle listening. In T-MAC, the power consumption of a leaf is high, because the protocol does not make a distinction between router and leaf nodes. In this comparison, 802.15.4 has the highest has the highest router node power consumption among synchronized MACs as its active period (CAP) length is fixed, which causes a lot of idle listening. T-MAC and TUTWSN are more energy-efficient because they have mechanisms to minimize idle listening. T-MAC adjusts the active period length based on the traffic, whereas TUTWSN prefers contention free channel access and adjusts the amount of reserved slots dynamically according to the traffic.

The LPL-based X-MAC protocol is the least energy-efficient when network traffic is high, but has the lowest power consumption when data generation interval is low as a node uses energy only to transmit data and does not have to maintain synchronization. T-MAC is the most energy-efficient synchronized protocol when data generation interval is long, because its energy-efficient synchronization

mechanism. In IEEE 802.15.4 and TUTWSN, beacon frames are transmitted every access cycle, which means that at long data generation interval, the power consumed due to beacon reception dominates.

The results indicate clearly that there is no single purpose, fit-for-all low-energy WSN MAC. The optimal MAC depends on the required delays and data generation intervals. For example, a synchronized MAC can be selected over a LPL MAC even in very low traffic networks, if the delay is not critical. This is the case e.g. in environmental networks in which samples need to be collected only once per hour. Another consideration is the role of the nodes. If the backbone network consists of router nodes that are mains powered, IEEE 802.15.4 would be a good choice as its leaf nodes have very low energy consumption.

6 Routing and Transport

As WSNs are designed to operate in large geographic areas, forwarding data directly to the target node would not be feasible as the required transmission energy increases proportionally to the square of the distance. Therefore, data is routed along several hops. A routing layer operates on top of the MAC layer. As several alternative routes to a destination node may exist, the routing decision has a significant effect on load balancing, end-to-end reliability, and latency. Furthermore, the route construction and maintenance methods used in a routing protocol determine energy-efficiency and mobility support. Due to resource constraints, WSN routing protocols often also combine transport layer functionality.

6.1 Services

The basic service for a routing protocol is the multihop forwarding a packet from a source to a destination. However, a routing protocol may also provide:

- *QoS support* allowing route selection based on different QoS-metrics, such as end-to-end latency, reliability, or energy usage.
- *Multicast and broadcast support* allowing efficient packet delivery to several nodes at once.
- *Mobility support* enabling source, intermediate, and/or destination node mobility.
- *End-to-end reliability* ensuring that a packet is not lost and performing retransmission if necessary.
- *Congestion control* to avoid packet drops due to traffic congestion.
- *Fragmentation* to enable transmission of large contents

Overall, the supported services are largely limited by the used routing paradigm and technology. The end-to-end reliability, congestion control, and fragmentation logically belong to a transport layer protocol. However, due to resource constraints

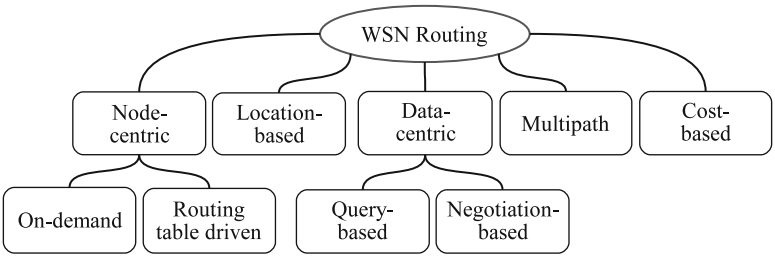

Fig. 10 WSN routing paradigms

and the need for cross-layer optimizations, many WSN routing protocols support for these services.

6.2 Routing Paradigms and Technologies

WSN routing protocols can be classified based on their operation as node-centric, data-centric, location-based, multipath, or cost-based [21, 34] as shown in Fig. 10. The classes are not exclusive as a routing protocol may be both data-centric and query based, while having features seen in location based protocols.

6.2.1 Node-Centric Routing

Node-centric approach is the traditional approach used in the computer networks in which nodes are addressed with globally unique identifiers. While the paradigm allows compatibility with the existing protocols, the requirement of required unique addressing is challenging in WSNs. Due to the large network size and error prone nature of sensor nodes, a decentralized address maintenance is preferred. However, as a network may partition or network segments may join, ensuring a consistent addressing scheme involves a lot of messaging and is energy-consuming.

Node-centric protocols typically rely on routing tables containing an entry for each route identified by destination address and next hop node for the target. The routing table may be constructed *proactively* by discovering routes to all potential targets, but this increases memory requirements and would not be practical in large networks. Instead, the node-centric protocols designed for ad-hoc wireless networks, such as Dynamic Source Routing (DSR) [22], or Ad-hoc On-demand Distance Vector routing (AODV), use *on-demand* (reactive) approach in which routes are constructed only when needed. The drawback compared to the proactive approach is the route construction delay when sending first packets.

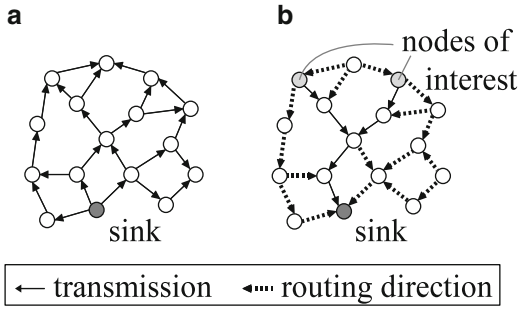

Fig. 11 Interest based routing. (**a**) sink advertises its interests to the network. (**b**) nodes matching the interest transmit data to the sink

6.2.2 Data-Centric Routing

As WSNs are inherently data oriented, the data centric routing is a more natural paradigm than the node-centric approach. In data-centric routing, data is routed based on its content rather than using sender or receiver identifiers. As the data-centric routing is already content aware, data-aggregation can be naturally performed.

Data centric routing may take interest based, negotiation based, or query based approaches. In the interest based approach, a sink node request data from the network by sending a request describing the data it wants to every node in the network [21]. A node forwards the interest and directs its routing tree toward the sink node as shown in Fig. 11. Then, nodes that fulfill the requirements as defined in the interest start transmitting data to the sink. Although the route construction is proactive, the interest based routing is scalable as the number of sinks (data consumers) is low compared to the number of nodes (data sources).

Negotiation-based protocols exchange negotiation messages before actual data transmission takes place [26]. This saves energy, as a node can determine during the negotiation that the actual data is not needed. For negotiation protocols to be useful, the negotiation overhead and data descriptor sizes must be smaller than the actual data. Query based routing protocols request a specific information from the network. A query might be expressed with a high level language such as SQL. For example, a query might request "average temperature around area *x,y* during the last hour". The query can be routed via a random walk or directed at a certain region [29]. After the query has been resolved, the result is transmitted back to the source.

6.2.3 Location-Based Routing

Location-based routing uses geographic location information to make routing decision. The approach is natural to WSNs, as sensor measurements usually relate to a specific location. A basic principle in the geographic routing is to select a next hop neighbor that is closer to the target node than a forwarding node. However, a problem with such greedy forwarding is that routing may fail due to hole in the network. Proposed solutions to the problem include switching to a different mode

when a hole is detected, such as in Greedy Perimeter Stateless Routing (GPSR) [23] where packet is routed around a hole according to right-hand rule. Another method is to express packet's route with mathematical formula as proposed in Trajectory Based Forwarding (TBF) [35]. Nodes forward packet to a neighbor that is closest to the defined route (trajectory). With the help of global knowledge of the network, a route that avoids holes can be selected.

The most significant benefit of the location-based routing is its scalability. Routing tables or a global knowledge of the network topology is not typically required, which reduces both data memory requirements and routing overhead. Also, geographic routing usually tolerates source and intermediate node mobility. However, determining the position for each node can be problematic. The use of positioning chips such as GPS increases the price and energy consumption, while manual configuration is not suitable for large scale networks.

6.2.4 Multipath Routing

In the multipath routing, a packet traverses from a source node to a target node via several paths. The main goal is to increase reliability, as a packet can be received via an alternative path even if the routing in some path fails. However, the multipath routing has a trade-off between the reliability and energy, as it increases network load and energy usage due to the extra transmissions.

Flooding packet to every node in the network is the simplest case of multipath routing. In flooding, each node forwards a new flood packet to all of its neighbors. To suppress duplicates, already received flood packets are not forwarded. Flooding is commonly used during the setup phase of several WSN routing protocols, but is not used for routing as such because packets can easily congest network and thus decrease reliability.

Controlled multipath routing algorithms limit the number of alternative routes. For example, in gradient broadcast [56] data is forwarded along an interleaved mesh. Each packet is assigned with a budget that is initialized by the source node. The budget consists of the minimum cost to send a packet to the sink and an additional credit. When a node receives the packet, it compares remaining budget against the cost required to forward the packet to the sink. If the cost is smaller or equal than the budget, the node forwards the packet. As the credit increases the budget, it allows forwarding the packet along other than minimum cost paths. Thus, the credit determines the amount of redundancy for the packet and has a trade-off between used energy and reliability. If credit is zero, packet must be forwarded along minimum cost path.

6.2.5 Cost-Based Routing

In cost-based routing, each node is assigned with a cost value that is relative to the distance between a node and a sink. The cost may be calculated from an any

metric, e.g. the number of hops or the required energy to forward a packet to the sink. The benefit of the cost-based routing is that the knowledge of forwarding path states is not required: a node forwards its data by sending it to any neighbor that has lower cost. The drawback is that the routes must be created proactively. Also, although data to the sink is forwarded efficiently, another routing mechanism, such as flooding, must be used for data traveling in the other direction. However, the trade-off can be acceptable since most of the traffic is usually toward the sink.

6.3 Hybrid Transport and Routing Protocols

Pump-Slowly, Fetch-Quickly (PSFQ) [53] combines the functionality of transport and routing layers to achieve a low communication cost. Data is transmitted with relatively slow speed by delaying forwarding with two configured time values T_{min} and T_{max}. In broadcast networks, the T_{min} parameter allows a node to receive a frame multiple times. A node then evaluates the necessity to forward the frame based on how many times it was received. If a sequence number gap in a received frame is detected, PSFQ uses a negative acknowledgment to request all missed frames. The frame is requested in less than T_{min}, which allows reducing latency on error situations.

SPEED [51] is a routing protocol that combines non-deterministic location-based forwarding with inbuilt congestion control mechanism and soft latency guarantees. The protocol does not guarantee strict limit for latency, but defines an end-to-end delay that is proportional to the distance between source and destination nodes. Thus, it maintains a certain delivery speed. In SPEED, the next hop is selected randomly among the neighbors with the probability that is proportional to the link speed. Only the nodes that advance towards the target and meet the delivery time can be selected. The link speed is calculated by dividing the distance between nodes (obtained with the geographic location information) by measured link delay. The next hop selection is combined with feedback received from neighbors. If a node cannot forward a packet due to congestion or a hole in the network, it sends a backpressure beacon, which reduces the forwarding probability to that node.

7 Embedded WSN Services

This section describes localization and synchronization in WSNs. On one hand, these can be seen as services that enable building various WSN applications, such as surveillance or tracking system. On the other hand, signal processing is used in various localization and synchronization algorithms that might benefit from an implementation with an embedded processing chip.

7.1 Localization

Ubiquitous localization has been widely studied during the recent years. In general, the solutions focus on finding effective location estimation algorithms and measurements that correlate with location. Localization can be categorized to range-based, proximity-based, and scene analysis [14]. The underlying technologies vary from pure RF-based, to UltraSound (US), InfraRed (IR), and multimodal solutions.

7.1.1 Range-Based Localization

Range-based approaches rely on estimating distances between localized nodes and anchor nodes, which know their locations a priori. This process is called ranging. Received Signal Strength (RSS) is a common RF-based ranging technique. Distances estimated using RSS can have large errors due to multipath signals and shadowing caused by obstructions [37]. The inherent unreliability has to be addressed in the used localization algorithms. In [24], RSS is replaced with multiple varying power level beacon transmissions.

Several location estimation techniques can be used in range-based localization. Utilized methods include trilateration, weighted center of gravity calculation, and Kalman filtering. Many mathematical optimization methods, such as the steepest descent method, sum of errors minimization, and Minimum Mean Square Error (MMSE) method, have been used to solve range-based location estimation problems.

7.1.2 Proximity-Based Localization

Proximity-based approaches exploiting RF signals [5, 18] estimate locations from connectivity information. Such solutions are also commonly referred to as range-free in the literature.

In the strongest base station method [18] the localized node's location is estimated to be the same as the location of the anchor node it is connected to. In [5], the unknown location is estimated using connectivity information to several anchor nodes. Only a very coarse grained location can be estimated using the strongest base station method. The solutions presented in [5] improve the granularity slightly. Nevertheless, in order to reach small granularities the connectivity-based schemes require a very dense grid of anchor nodes. Their, strength is fairly simple implementation and modest HW requirements.

7.1.3 Scene Analysis

Scene analysis consists of an off-line learning phase and an online localization phase. The off-line phase includes recording RSS values corresponding to different

anchor nodes as a function of the users location. The recorded RSS values and the known locations of the anchor nodes are used either to construct an RF-fingerprint database [30], or a probabilistic radio map [8, 59]. In the online phase the localized node measures RSS values to different anchor nodes. With RF-fingerprinting the location of the user is determined by finding the recorded reference fingerprint values that are closest to the measured one (in signal space). The unknown location is then estimated to be the one paired with the closest reference fingerprint or in the (weighted) centroid of k nearest reference fingerprints. Location estimation using a probabilistic radio map includes finding the point(s) in the map that maximize the location probability.

The applicability and scalability of scene analysis is limited by the time consuming collection and maintenance of the RF sample database. Also, searching through the sample database or radio map is computationally intensive. The Joint Clustering (JC) technique [59] uses location clustering to reduce the computational cost of searching the radio map. It improves the scalability of the searching algorithm to some extent. MoteTrack [30] achieves similar effect by disseminating the RF-fingerprint database to a WSN and decentralizing the localization procedure.

7.1.4 Ranging Technologies

In general, RF signal strength based localization possesses fundamental limits due to the unreliability of the measurements [8]. There is strong evidence that, at best, accuracy in the scale of meters can be achieved regardless of the used method [8].

US-based approaches [41, 42] use time-of-flight ranging and can achieve high accuracies. However, anchor nodes need to be positioned and orientated carefully due to the directionality of US and the requirement for Line-of-Sight (LoS) exposure. A dense network of anchor nodes is needed due to the LoS requirement, short range of US, and the fact, that typically ranging measurements to at least four anchor nodes are needed. The addition of US transmitters and receivers increases HW costs and reduces energy-efficiency compared to purely RF-based solutions. Some schemes [42] require multiple US transmitters/receivers per one HW platform further increasing the HW costs.

IR-based solutions [54] are based on inferring proximity. They can localize nodes inside the range of LoS IR transmissions. IR-based schemes suffer errors in the presence of obstructions. Also, differing light and ambient IR levels, caused by for example fluorescent lighting or direct sunlight, produce difficulties [41]. The anchor network costs are high because a dense matrix of IR sensors is needed in order to avoid dead spots.

In the presence of a myriad of location sensing techniques data fusion has become and attractive location estimation method. It can combine measurements from multiple sensors while managing measurement uncertainty. In [10] Fox et al. survey Bayesian filtering techniques capable of multisensor fusion. Probabilistic fusion methods require relative large amounts of computation. Thus, in the presence

of resource constrained nodes, a centralized implementation running in a more powerful base station is often the only feasible choice. For example in the Localization Stack [15] the fusion layer is implemented in Java.

7.2 Synchronization

The most straightforward way to achieve accurate synchronization would be to equip every node with a Global Positioning System (GPS) receiver, Universal Time Coordinated (UTC) signal receiver or an accurate atomic clock. However, in reality this would be infeasible in WSN nodes due to increased size, cost, and energy consumption. Thus, synchronization has to be achieved by using a specific synchronization protocol.

Although effective in the Internet, the widely used Network Time Protocol is too resource consuming for WSNs. Furthermore it requires external configuration making ad hoc operation impossible. The IEEE 1588 standard for a precision clock synchronization protocol for networked measurement and control systems has the similar shortcomings. Next, synchronization protocols designed for WSNs and targeting at network-wide synchronization via multiple hops will be overviewed.

The protocol in [47] is based on the assumption that the clock value of a node of the linear form: $t_i = a_i t + b_i$, where t_i is the local clock value of node i, a_i is the drift, b_i is the offset, and t presents real time. The goal of the protocol is not to achieve network-wide global time but instead each node performs pairwise synchronization with each of its neighbors maintaining a list of clock parameters (a and b) for every neighbor.

The Timing-sync Protocol for Sensor Networks (TPSN) [11] uses two frames to synchronize a pair of nodes. The global time synchronization algorithm of TPSN builds a spanning tree. In the tree, every node knows its level and its parent. Remote clock estimation is performed between adjacent levels. The tree construction is initiated by the reference node which is assigned level 0. The child nodes flood the level discovery frames until leaf nodes are reached. The tree is static for the lifetime of the reference node except for the joining of new node using a level discovery frame.

Similarly to TPSN, the Lightweight Tree-based Synchronization (LTS) protocols [12] synchronize a pair of nodes with two frames. Global synchronization is achieved by creating a minimum height spanning tree. The protocol uses multiple reference nodes to improve time reference robustness. Fault tolerance against dynamic channel variations, changes in topology, changes in size, and node mobility is achieved by re-creating the spanning tree on every re-synchronization.

The Flooding Time Synchronization Protocol (FTSP) [32] uses link layer timestamping and linear regression to estimate neighbor node clock parameters. The protocol floods all the synchronization frames through the network. This gives good tolerance against failures. Furthermore, an algorithm for electing a new reference

node when the current one fails is presented. A node starts acting as reference node after a constant timeout when it has not receive any synchronization frames. This results in possibly many new reference nodes of which only the one with the minimum ID remains after the synchronization flooding resumes.

Delay Measurement Time Synchronization (DMTS) [38] uses one message to synchronize a sender and all the receivers in its neighborhood. The multi-hop DMTS algorithm uses a leader selection algorithm to select a time reference for the whole network. The time reference is at tree level 0. The time is periodically flooded trough the network by broadcasting it from level to level. Synchronization frames from only lower level nodes are accepted. This is continued until leaf nodes are reached.

The Time-Diffusion synchronization Protocol (TDP) [49] consist of active and inactive cycles. At the start of every active cycle a subset of nodes is selected as masters who can relay synchronization data. The timing messages sent by the masters create individual tree structures for every master. Furthermore, the protocol includes a method for detecting outliers. TDP does no rely on external time servers making it fully self-contained. Furthermore, the creation of new synchronization trees in every cycle increase the fault tolerance.

Li et al. [28] propose a diffusion method where nodes achieve global synchronization by spreading local synchronization information to the entire system. The method does not rely on a single time reference which betters the robustness of the protocol. However, any malfunctioning node affects the time accuracy of the whole network. The authors present a solution for this by replacing a fraction of the normal nodes by tamper-proof nodes.

8 Case Study on WSN Performance

In this section, the low power WSN performance is examined with TUTWSN [27]. TUTWSN comprises hardware platforms built from COTS components and communication protocols.

Two variations of the protocol are presented: low-energy and low-latency. The design requirements for these variants are presented in Table 7. The low-energy TUTWSN is targeted at sensing applications requiring moderate throughput, long network lifetime, and forwarding latencies that are in the order of seconds per hop. The low-latency TUTWSN is targeted at localization and target tracking applications requiring very low end-to-end delays and light throughput. It uses a heterogeneous approach by allowing ultra low power mobile nodes, while the

Table 7 Design requirements of TUTWSN low-energy and low-latency protocols

TUTWSN variant	Network size	Measurement interval	End-to-end latency	Router power	Node power	Lifetime
Low-energy	Thousands	30 s–15 min	$<$10 min	Battery	Battery	2 years
Low-latency	Hundreds	0.5–10 s	$<$6 s	Mains	Battery	4 years

energy consumption of router nodes forming a backbone network is higher. Both protocol variations enable multihop networking with one or more sinks and share a common hardware platform. The program memory usage of the low-energy and low-latency TUTWSN protocols were 100 and 60 kB, respectively. The data memory usage was less than 4 kB in both cases. Thus, the protocols represent feasibility of the very resource constrained WSN hardware.

A TUTWSN node is controlled by a 8-bit Microchip PIC18LF8722 MCU and Nordic Semiconductor nRF24L01 transceiver. The transceiver is used with 1 Mbit/s data rate, which ensures short transmission and reception times, allowing node to spend most of the time in low-power states. The node is powered by two AA batteries.

8.1 Low-Energy TUTWSN

Low-energy TUTWSN uses a clustered topology, in which each cluster operates on its own frequency referred to as a cluster channel. This increases scalability and avoids collisions between clusters.

The experimented configuration of TUTWSN MAC utilize 2 s access cycle, 4 ALOHA slots, and 8 reserved slots. The frame size is 32 B due to hardware limitations. As data is sent only in the reserved slots, the total throughput at MAC layer is 1 kbit/s. The routing protocol uses cost-based approach while supporting several sinks by maintaining a separate cost for each sink [27]. A node initially searches its neighbors with a network scan. When a new neighbor is found, a node sends a cost request to it. A node selects the next hop and sets its cost based on the received replies. Additionally, a node periodically recalculates its costs and broadcasts an advertisement to its neighbors. This way, nodes can react to the changes in the network conditions that manifest as varying cost levels.

8.1.1 Scalability

In a low-duty cycle MAC protocol (such as IEEE 802.15.4 or TUTWSN MAC), the maximum number of nodes (α) in an interference area can be determined by the access cycle length (T_{AC}), the superframe length, the average number of member nodes in each cluster, and the number of utilized non-interfering frequency channels (n_{CH}) as

$$\alpha = \frac{T_{AC} n_{CH} (1 + n_S)}{t_{SF} + t_{guard}}, \tag{2}$$

where t_{SF} is the length of a superframe, t_{guard} is a short guard time between consecutive superframes. α is maximized by minimizing the superframe and guard time lengths and by maximizing T_{AC}, n_{CH}, and n_S. It can be clearly seen in the equation that by utilizing a high data-rate radio operating at a wide frequency band provides the highest scalability.

Table 8 Average power consumption and estimated lifetime with a 2,000 mAh battery

	Power consumption (μW)		Lifetime (years)	
Access cycle length (s)	Subnode	Headnode	Subnode	Headnode
2	153	740	4.5	0.9
4	120	533	5.7	1.3
8	103	327	6.6	2.1

In the experimented 2.4 GHz TUTWSN implementation, $T_{AC} = 4$ s, $t_{SF} = 280$ ms, and each superframe is followed by a 220 ms guard period to allow time for data processing. In TUTWSN sensor node platforms, the interference range in indoor conditions is around 100 m equaling to the area of 31,400 m^2. Eight member nodes can be connected to each cluster head. The limit is due to data memory as various statistics is kept from each member. With the utilized transceiver provides 82 channels with 1 MHz channel separation. In practice, 41 channels are non-overlapping (2 MHz separation) and 2,880 nodes can be located within an interference range. If only one channel were used ($n_{CH} = 1$), α would be reduced to 72 nodes within the interference range.

The network depth is limited by the routing protocol. As routing cost is expressed in 8-bit integer value and per-hop cost ranges between 1 . . . 8, the maximum network depth is 32.

8.1.2 Power Consumption

Power consumption of the platform was tested in a multihop network consisting of 2 sinks, 13 headnodes, and 12 subnodes (27 nodes in total). Each node measured its temperature and transmitted a packet every 10 s to the nearest sink. The maximum hop count was 3.

The average headnode and subnode power consumptions with 2, 4, and 8 s access cycle lengths are presented in Table 8. A short access cycle consumes more power as beacons must be sent and received more frequently. Depending on the used access cycle length, the lifetime with a conservative estimate of 2,000 mAh capacity is estimated between 4.5 and 6.6 years with a subnode and 0.9 and 2.1 years with a headnode. The power consumption of a headnode is significantly higher as it must also receive channel during CAP and forward traffic.

8.1.3 Availability and End-to-End Reliability

The practical performance of a low-power network was measured in an indoor deployment consisting of 120 nodes and 8 sinks. Nodes sent sensor data in 60 s intervals and diagnostics data (incl. battery voltage, buffer usage, and link reliabilities) in 120 s intervals. As a result, a node generated a data packet on average

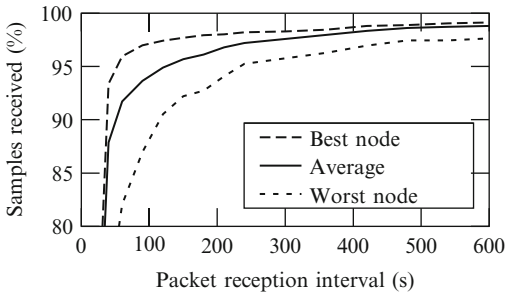

Fig. 12 Node availability in the experimented network

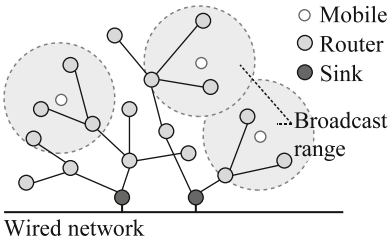

Fig. 13 Low-latency TUTWSN topology. The router nodes forward data via multiple hops to one or multiple sinks. Mobile nodes broadcast their data to the router nodes

in 40 s intervals. Each node transmitted its data to the nearest sink. An average routing path length was 4 and the maximum hop count to the sink was 6.

The reliability of the network was estimated with an availability metric. If a node does not have problems, the reception interval at a sink equals to the data generation interval. Retransmissions and packet drops increase the interval required to reach a certain availability.

The average availability of nodes, and the availability of the most and least reliable nodes are presented in Fig. 12. On average, 95 % of traffic is received in less than 140 s interval. The availability increases only slightly after 99 % as the reception interval is increased, denoting that 1 % of traffic is lost. The unreliability is caused by the limited data memory, as each node can only hold 20 packets. Thus, packet are dropped as buffers overflow. This situation is likely to occur when a node has lost a link and cannot forward its data but is still receiving traffic from other nodes.

8.2 Low-Latency TUTWSN

The low-latency network consists of router nodes and mobile nodes as shown in Fig. 13. The router nodes are responsible of data forwarding via a multihop network to one or multiple sinks. The low-latency TUTWSN operates on single network wide communication channel. The channel access method with routers and mobile nodes are different. Routers sense channel continuously, which consumes power but allows fast data forwarding. The channel access is realized with ALOHA protocol

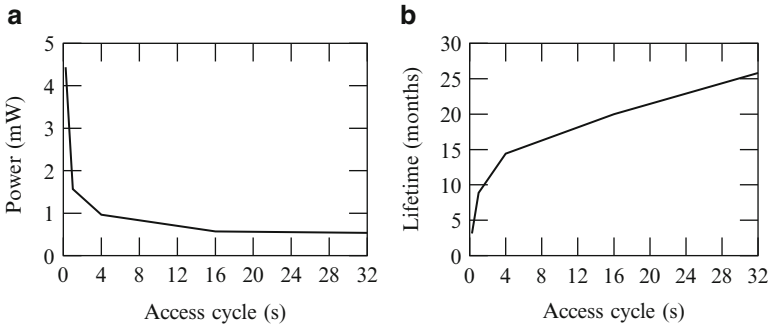

Fig. 14 Estimated mobile node power consumption and lifetime with 2,000 mAh batteries

and randomized backoffs. A CSMA protocol would improve bandwidth usage efficiency compared to ALOHA, but the functionality is not included in the most low-cost and low-power radio transceivers.

The channel access of a mobile node is designed to minimize energy consuming idle listening. A mobile node broadcasts beacon frames periodically but with slightly randomized intervals to avoid collisions. Then, the node briefly listens to the channel. The beacon can be piggybacked with application generated data. A router node that receives the beacon waits a random time to avoid collisions and sends an acknowledgment to the mobile node. If the beacon frame containing data is not acknowledged, a mobile node temporarily shortens its beacon generation interval, thus reducing the delay between retransmission attempts. A beacon frame is forwarded to a sink only if it contains application data.

For routing, a cost-based protocol is used. Cross-layer design is utilized decrease delays and improve implementation efficiency. The routing layer uses network beacons to advertise cost information to neighbors and to acquire in depth information from the neighborhood. Using this information, the routing protocol calculates routes and fills the routing table. When forwarding data, the MAC layer can look up next hop information straight from the routing table without the need to cycle the packets to the routing layer. This reduces queuing, processing, and stack handover delays.

8.2.1 Power Consumption and Network Lifetime

As the routers are active all the time their power consumption does not depend on network behavior nor operating mode. The average measured power consumption for a router node is 78 mW. With a conservative estimate of 2,000 mAh battery capacity, the lifetime of a router is estimated to be 8 days. Thus, to achieve feasible network lifetime, the router nodes should be equipped with big enough batteries or be mains powered.

The average mobile node power consumption was measured using 0.25, 1, 4, 16, and 32 s access cycle lengths. The results are presented in Fig. 14a. The lifetimes of

Table 9 Fixed multi-hop scenario delay results

Percentile (%)	Maximum delay (s)	Average delay per hop (s)
99	2.1	0.4
99.5	2.5	0.4
99.9	3.6	0.5
100	4.4	0.7

Packets were relayed over 1–8 hops

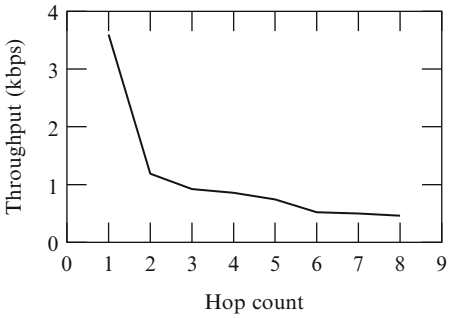

Fig. 15 Fixed multi-hop scenario throughput results. Packets were relayed over 1–8 hops. The data always originated from the end of the hop chain

a mobile node with the same access cycles and using 2,000 mAh battery capacity are shown Fig. 14b. The lifetime ranges from 3.1 months to 2.1 years. However, it is unlikely that a node needs to transmit e.g. every 0.25 s for its whole lifetime. Thus, longer lifetimes and low-latency operation can still be achieved when using shorter access cycles only when needed.

8.2.2 Delay and Throughput

The performance of the low-latency network was tested using a network where the nodes communicated via a fixed multi-hop route to a sink. This enables accurate analysis of the network behavior over varying amount of hops. The delay results are presented in Table 9.

The scenario consisted of an eight-hop chain of nodes. Ninety-nine percent of the packets reached the sink in 2.1 s and all the packets were received within 4.4 s. Figure 15 presents the throughput as a function of hop count. In the experiments, the data always originated from the end of the hop chain. The throughput ranges from 3.5 kpbs to 500 bps.

9 Summary

WSN is a recently emerged technology that does not have de-facto platforms, standards, or technologies. The limitations in the current manufacturing techniques cause a trade-off between size, price, performance, and lifetime of a sensor node.

Thus, due to contradictive requirements of different WSN applications, there is no general purpose WSN technology. Instead, platform components and communication protocols must be specifically selected to meet the application demands.

An ideal WSN platform would combine the hundreds of MIPS processing power and several MBs memory of the high performance platforms with the 1 mA average and 1 µA sleep mode currents of low-energy platforms. However, it is unlikely that this can be achieved in the near future only by improving manufacturing technologies. A combination of low-energy protocols and hardware acceleration is required, which opens up applications for signal processing systems.

In low-power platforms, transceiver consumes most of the energy. Thus, it is possible to lower energy consumption by trading communication time with processing time by preprocessing data, data fusion, and aggregation. Accelerating computing intensive tasks, such as encryption, would leave processing power for other task. In addition, accelerated compression would allow more complex sensing, as images, sound, and video could be transferred energy-efficiently. ASIC implementation of communication protocols and applications could improve performance and decrease power consumption. However, as a trade-off, the network would lose its reprogrammability capabilities and configurability.

Overall, the processing power and capacity of a single sensor node is small. However, the large number of sensor nodes enable massively parallel distributed data processing and storage. Thus, the feasibility and useful features of WSNs lie in the co-operation of the sensor nodes.

References

1. Akyildiz, I.F., Kasimoglu, I.H.: Wireless sensor and actor networks: Research challenges. Elsevier Ad Hoc Networks **2**(4), 351–367 (2004)
2. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless sensor networks: a survey. Elsevier Computer Networks **38**(4), 393–422 (2002)
3. Baunach, M., Kolla, R., Mhlberger, C.: Beyond theory: Development of a real world localization application as low power wsn. In: Proc. 32nd IEEE Conference on Local Computer Networks (LCN'07), pp. 872–884. Dublin, Ireland (2007)
4. Buettner, M., Yee, G., Anderson, E., Han, R.: X-MAC: A short preamble MAC protocol for duty-cycled wireless sensor networks. In: Proc. 4th ACM Conf. Embedded Networked Sensor Systems (SenSys'06), pp. 307–320. Boulder, Colorado, USA (2006)
5. Bulusu, N., Heidemann, J., Estrin, D.: GPS-less low-cost outdoor localization for very small devices. Personal Communications, IEEE [see also IEEE Wireless Communications] **7**(5), 28–34 (2000)
6. Colvin, A.: CSMA with collision avoidance. Computer Communications **6**(5), 227–235 (1983)
7. Crossbow Technology, Inc.: Stargate X-Scale processor platform. Available: http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/6020-0049-01_B_STARGATE.pdf (2004)
8. Elnahrawy, E., Li, X., Martin, R.P.: The limits of localization using signal strength: a comparative study. In: Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004. 2004 First Annual IEEE Communications Society Conference on, pp. 406–414 (2004)
9. Enz, C.C., El-Hoiydi, A., Decotignie, J.D., Peiris, V.: WiseNET: An ultralow-power wireless sensor network solution. Computer **37**(8), 62–70 (2004)

10. Fox, V., Hightower, J., Liao, L., Schulz, D., Borriello, G.: Bayesian filtering for location estimation. Pervasive Computing, IEEE **2**(3), 24–33 (July-Sept. 2003). DOI 10.1109/MPRV.2003.1228524
11. Ganeriwal, S., Kumar, R., Srivastava, M.B.: Timing-sync protocol for sensor networks. In: SenSys '03: Proceedings of the 1st international conference on Embedded networked sensor systems, pp. 138–149. ACM, New York, NY, USA (2003). DOI http://doi.acm.org/10.1145/958491.958508
12. Greunen, J.V., Rabaey, J.: Lightweight time synchronization for sensor networks. In: WSNA '03: Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications, pp. 11–19. ACM, New York, NY, USA (2003). DOI http://doi.acm.org/10.1145/941350.941353
13. Guo, C., Zhong, L., Rabaey, J.: Low power distributed MAC for ad hoc sensor radio networks. In: Global Telecommunications Conf. (GLOBECOM'01), vol. 5, pp. 2944–2948. San Antonio, TX, USA (2001)
14. Hightower, J., Borriello, G.: Location systems for ubiquitous computing. Computer **34**(8), 57–66 (2001)
15. Hightower, J., Brumitt, B., Borriello, G.: The location stack: a layered model for location in ubiquitous computing. Mobile Computing Systems and Applications, 2002. Proceedings Fourth IEEE Workshop on pp. 22–28 (2002). DOI 10.1109/MCSA.2002.1017482
16. Hill, J., Horton, M., Kling, R., Krishnamurthy, L.: Wireless sensor networks: The platforms enabling wireless sensor networks. Communications of the ACM **6**(47), 41–46 (2004)
17. Hill, J., Szewczyk, R., Woo, A., Hollar, S., Culler, D., Pister, K.: System architecture directions for networked sensors. In: Proc. 9th ACM Int'l Conf. on Architectural Support for Programming Languages and Operating Systems (ASPLOS'00), pp. 94–103. Cambridge, MA, USA (2000)
18. Hodes, T.D., Katz, R.H., Servan-Schreiber, E., Rowe, L.: Composable ad-hoc mobile services for universal interaction. In: MobiCom '97: Proceedings of the 3rd annual ACM/IEEE international conference on Mobile computing and networking, pp. 1–12. ACM, New York, NY, USA (1997). DOI http://doi.acm.org/10.1145/262116.262121
19. IEEE 802.15.4: IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPAN) (2006)
20. ISA: ISA100.11a release 1. Available: http://www.isa.org/source/ISA100.11a_Release1_Status.ppt (2007)
21. Al Karaki, J.N., Kamal, A.E.: Routing techniques in wireless sensor networks: A survey. IEEE Wireless Communications **11**(6), 6–28 (2004)
22. Karl, H., Willig, A.: Protocols and Architectures for Wireless Sensor Networks. John Wiley & Sons Ltd (2005)
23. Karp, B., Kung, H.T.: GPSR: Greedy perimeter stateless routing for wireless networks. In: Proc. 6th annual Int'l Conf. on mobile computing and networking (MobiCom'00), pp. 243–254. Boston, MA, USA (2000)
24. Kaseva, V.A., Kohvakka, M., Kuorilehto, M., Hännikäinen, M., Hämäläinen, T.D.: A wireless sensor network for RF-based indoor localization. EURASIP Journal on Advances in Signal Processing (2008). DOI 10.1155/2008/731835
25. Kohvakka, M.: Medium access control and hardware prototype designs for low-energy wireless sensor networks. Ph.D. thesis, Tampere University of Technology, Tampere, Finland (2009)
26. Kulik, J., Heinzelman, W., Balakrishnan, H.: Negotiation-based protocols for disseminating information in wireless sensor networks. Kluwer Wireless Networks **8**(2), 169–185 (2002)
27. Kuorilehto, M., Kohvakka, M., Suhonen, J., Hmlinen, P., Hnnikinen, M., Hmlinen, T.D.: Ultra-Low Energy Wireless Sensor Networks in Practice - Theory, Realization and Deployment. John Wiley & Sons Ltd (2007)
28. Li, M.Q., Rus, M.D.: Global clock synchronization in sensor networks. IEEE Trans. Comput. **55**(2), 214–226 (2006). DOI http://dx.doi.org/10.1109/TC.2006.25

29. Liu, J., Zhao, F., Petrovic, D.: Information-directed routing in ad hoc sensor networks. IEEE Journal on Selected Areas in Communications **23**(4), 851–861 (2005)
30. Lorincz, K., Welsh, M.: MoteTrack: A robust, decentralized approach to RF-based location tracking. In: In Proceedings of the International Workshop on Location- and Context-Awareness (LoCA 2005) at Pervasive 2005. Oberpfaffenhofen, Germany (2005)
31. Madden, S., Franklin, M.J., Hellerstein, J.M., Hong, W.: The design of an acquisitional query processor for sensor networks. In: Proc. ACM Int'l Conf. on Management of Data (SIGMOD'03), pp. 491–502. San Diego, CA, USA (2003)
32. Maróti, M., Kusy, B., Simon, G., Ákos Lédeczi: The flooding time synchronization protocol. In: SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems, pp. 39–49. ACM, New York, NY, USA (2004). DOI http://doi.acm.org/10.1145/1031495.1031501
33. Min, R., Bhardwaj, M., Cho, S.H., Ickes, N., Shih, E., Sinha, A., Wang, A., Chandrakasan, A.: Energy-centric enabling technologies for wireless sensor networks. IEEE Wireless Communications **9**(4), 28–39 (2002)
34. Niculescu, D.: Communication paradigms for sensor networks. IEEE Communications Magazine **43**(3), 116–122 (2005)
35. Niculescu, D., Nath, B.: Trajectory based forwarding and its applications. In: Proc. 9th annual Int'l Conf. on Mobile computing and networking (MobiCom'03), pp. 260–272. San Diego, CA, USA (2003)
36. Norair, J.P.: Introduction to DASH7 technologies. Tech. rep., DASH7 Technology Working Group (2009)
37. Patwari, N., Ash, J.N., Kyperountas, S., Hero III, A.O., Moses, R.L., Correal, N.S.: Locating the nodes: cooperative localization in wireless sensor networks. Signal Processing Magazine, IEEE **22**(4), 54–69 (2005)
38. Ping, S.: Delay measurement time synchronization for wireless sensor networks. Tech. Rep. IRB-TR-03-013, Intel Research Berkeley Lab (2003)
39. Pitcher, G.: If the cap fits... New Electronics pp. 25–26 (2006)
40. Polastre, J., Hill, J., Culler, D.: Versatile low power media access for wireless sensor networks. In: Proc. 2nd Internation Conf. on Embedded Networked Sensor Systems (Sensys'04), pp. 95–107. Baltimore, MD, USA (2004)
41. Priyantha, N.B., Chakraborty, A., Balakrishnan, H.: The cricket location-support system. In: MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking, pp. 32–43. ACM Press, New York, NY, USA (2000)
42. Priyantha, N.B., Miu, A.K.L., Balakrishnan, H., Teller, S.: The cricket compass for context-aware mobile applications. In: MobiCom '01: Proceedings of the 7th annual international conference on Mobile computing and networking, pp. 1–14. ACM Press, New York, NY, USA (2001)
43. Reason, J.M., Rabaey, J.M.: A study of energy consumption and reliability in a multi-hop sensor network. ACM SIGMOBILE Mobile Computing and Communications Review **8**(1), 84–97 (2004)
44. Roberts, L.: ALOHA packet system with and without slots and capture. ACM SIGCOMM Computer Communication Review **5**(2), 28–42 (1975)
45. Roundy, S., Wright, P.K., Rabaey, J.: A study of low level vibrations as a power source for wireless sensor nodes. Computer Communications **26**(11), 1131–1144 (2003)
46. Rmer, K., Kasten, O., Mattern, F.: Middleware challenges for wireless sensor networks. ACM SIGMOBILE Mobile Computing and Communications Review **6**(4), 59–61 (2002)
47. Sichitiu, M., Veerarittiphan, C.: Simple, accurate time synchronization for wireless sensor networks. In: WCNC '03: Proceedings of the IEEE conference on Wireless Communications and Networking, vol. 2, pp. 1266–1273 (2003)
48. Stallings, W.: Operating Systems Internals and Design Principles, 5 edn. Prentice-Hall (2005)
49. Su, W., Akyildiz, I.F.: Time-diffusion synchronization protocol for wireless sensor networks. IEEE/ACM Trans. Netw. **13**(2), 384–397 (2005). DOI http://dx.doi.org/10.1109/TNET.2004.842228

50. Suhonen, J., Hmlinen, T.D., Hnnikinen, M.: Availability and end-to-end reliability in low duty cycle multihop wireless sensor networks. Sensors **9**(3), 2088–2116 (2009)
51. Tian He, Stankovic, J.A., Lu, C., Abdelzaher, T.: SPEED: A stateless protocol for real-time communication in sensor networks. In: Proc. 23rd Int'l Conf. on Distributed Computing Systems, pp. 46–55. Providence, RI, USA (2003)
52. van Dam, T., Langendoen, K.: An adaptive energy-efficient MAC protocol for wireless sensor networks. In: Proc. 1st Int'l Conf. on Embedded Networked Sensor Systems (Sensys'03), pp. 171–180. Los Angeles, CA, USA (2003)
53. Wan, C.Y., Campbell, A.T., Krishnamurthy, L.: Pump-slowly, fetch-quickly (PSFQ): A reliable transport protocol for sensor networks. IEEE Journal on Selected Areas in Communications **23**(4), 862–872 (2005)
54. Want, R., Hopper, A., Falcao, V., Gibbons, J.: The active badge location system. ACM Transactions on Information Systems **10**(1), 91–102 (1992)
55. Wolf, M., Kress, D.: Short-range wireless infrared transmission: the link budget compared to RF. IEEE Wireless Communications Magazine **10**(2), 8–14 (2003)
56. Ye, F., Zhong, G., Lu, S., Zhang, L.: GRAdient broadcast: a robust data delivery protocol for large scale sensor networks. Kluwer Wireless Networks **11**(3), 285–298 (2005)
57. Ye, W., Heidemann, J., Estrin, D.: An energy-efficient MAC protocol for wireless sensor networks. In: Proc. 21st Annual Joint Conf. of the IEEE Computer and Communications Societies (INFOCOM'02), vol. 3, pp. 1567–1576. New York, NY, USA (2002)
58. Yoon, S.: Power management in wireless sensor networks. North Carolina State University, PhD Thesis (2007)
59. Youssef, M.A., Agrawala, A., Shankar, A.U.: WLAN location determination via clustering and probability distributions. In: Pervasive Computing and Communications, 2003. (PerCom 2003). Proceedings of the First IEEE International Conference on, pp. 143–150 (2003)