Wireless Home Automation Networks: A Survey of Architectures and Technologies

Carles Gomez and Josep Paradells, Technical University of Catalonia

ABSTRACT

Wireless home automation networks comprise wireless embedded sensors and actuators that enable monitoring and control applications for home user comfort and efficient home management. This article surveys the main current and emerging solutions that are suitable for WHANs, including ZigBee, Z-Wave, INSTEON, Wavenis, and IP-based technology.

INTRODUCTION

In recent years, wireless sensor and actuator networks have gained high momentum, receiving significant attention from academia, industry, and standards development organizations. One of the primary application domains of this technology is home automation. Wireless home automation networks (WHANs) enable monitoring and control applications for home user comfort and efficient home management.

A WHAN typically comprises several types of severely constrained embedded devices, which may be battery powered and are equipped with low-power radio frequency (RF) transceivers. The use of RF communication allows flexible addition or removal of devices to or from the network and reduces installation costs since wired solutions require conduits or cable trays. However, the dynamics of radio propagation, resource limitations, and the mobility of some devices challenge the design of WHANs.

Several organizations and companies have developed WHAN solutions according to different architectures and principles. This article surveys the main current and emerging architectures and technologies tailored to or suitable for WHANs. The next section illustrates use cases, and states the main features and requirements for WHANs. We then present an overview of ZigBee, Z-Wave, INSTEON, Wavenis, and IP-based approaches. We then discuss these solutions with regard to WHAN requirements plus additional technical and non-technical criteria. The final section is the conclusion of the article.

USE CASES AND MAIN FEATURES OF WHANS

WHANs enable a variety of use cases, as illustrated in Fig. 1. A non-exhaustive list of examples is provided below

Light control: A new light can be controlled from any switch, which reduces the need for new wired connections. Lights can also be activated in response to a command from a remote control. Furthermore, they can be turned on automatically when presence and luminance sensors detect that people are in a poorly illuminated room.

Remote control: Infrared technology has been used for wireless communication between a remote control and devices such as TVs, HiFi equipment, and heating, ventilating, and air conditioning (HVAC) systems. However, infrared requires line-of-sight (LOS) and short-distance communication. RF technology overcomes these limitations.

Smart energy: Window shades, HVAC, central heating, and so on may be controlled depending on the information collected by several types of sensors that monitor parameters such as temperature, humidity, light, and presence. Unnecessary waste of energy can thus be avoided. In addition, smart utility meters can be used to detect usage peaks and alert the household devices that may be causing them. Energy supply companies may also use WHANs to perform energy load management.

Remote care: Patients, and disabled and elderly citizens can benefit from at-home medical attention. Wearable wireless sensors can periodically report the levels of several body parameters (e.g., temperature, blood pressure, and insulin) for a precise diagnosis. If acceleration sensors suggest that a person has fallen, alarms can be activated immediately.

Security and safety: Advanced security systems can be based on several sensors (e.g., smoke detectors, glass-break sensors, and motion sensors) for detecting possible risk situations that trigger appropriate actions in response. For example, smoke detectors may activate fire alarms.

0163-6804/10/$25.00 © 2010 IEEE

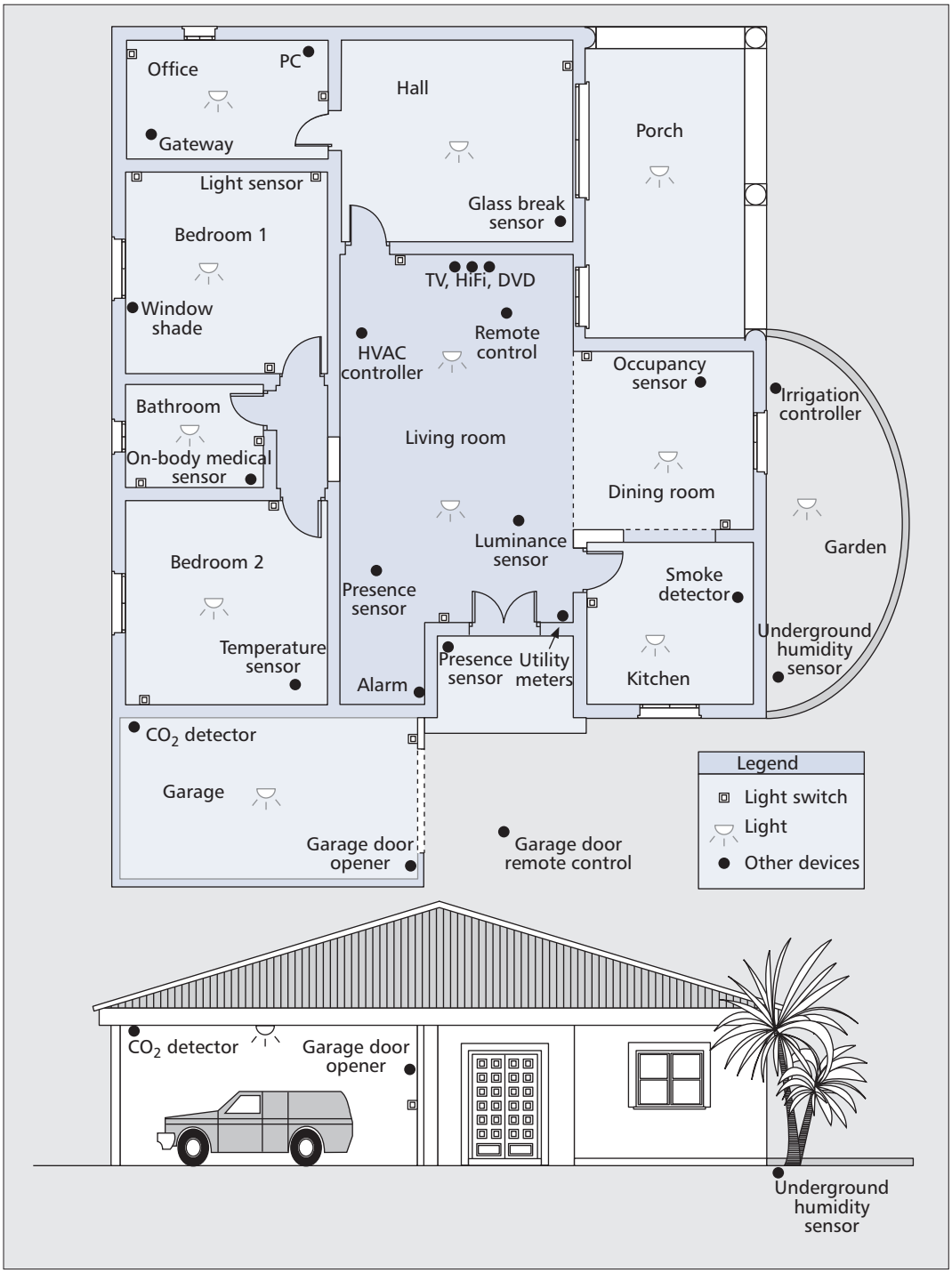

Figure 1. *An example of a WHAN-enabled home.*

Window shades, HVAC, central heating, etc. may be controlled depending on the information collected by several types of sensors that monitor parameters such as temperature, humidity, light, and presence. Unnecessary waste of energy can thus be avoided.

The main characteristics and requirements for WHANs are as follows:

- The node density is potentially high, and the number of nodes may be on the order of hundreds.
- The home is typically a multipath environment due to the presence of reflective surfaces (e.g., walls, floors, and tables).
- Residential scenarios are subject to interference. Industrial, scientific, and medical (ISM) bands are particularly crowded with the presence of WiFi, Bluetooth, cordless phones, and even microwave ovens.
- To facilitate end-to-end connectivity, multihop communications are required, so that intermediate nodes can retransmit data for nodes that are not within the sender's transmission range.
- Although most devices are static, the mobility of some of them and the dynamics of RF signal propagation require the network to be self-healing. The duration of connectivity gaps due to network topology changes should be low.
- The applications require WHANs to support various traffic patterns, such as point-

		ZigBee	6LoWPAN	Z-Wave	INSTEON	Wavenis
Physical layer	RF band (MHz)	868/915/2400		868/908 (all chips) 2400 (400 series chip)	904	433/868/915 (2400 also available)
	Range (m)	10–100		30 (indoors) 100 (outdoors)	45 (outdoors)	200 (indoors) 1000 (outdoors)
	Bit rate (kb/s)	20/40/250		9.6/40 (from 200 series chip) 200 (only 400 series chip)	38.4	4.8/19.2/100 (min./typ./max.)
	Modulation	BPSK/BPSK/O-QPSK		BFSK	FSK	GFSK
	Spreading technique	DSSS		No	No	Fast FHSS
	Receiver sensitivity (dBm)	–85 or better (2.4 GHz band) –92 or better (868/915 MHz bands)		–101 (at 40 kb/s)	–103	–110 (at 19.2 kb/s)
Link layer	MAC mechanism	TDMA + CSMA/CA (beacon mode) and CSMA/CA (beaconless mode)		CSMA/CA	TDMA + simulcast	CSMA/TDMA (synchronized networks) and CSMA/CA (otherwise)
	Message size (bytes)	127 (maximum)		64 (maximum MAC payload in 200 series chip)	14 (standard messages) 28 (extended messages)	N/A
	Error control	16-bit CRC, ACKs (optional)		8-bit check-sum, ACKs (optional)	8-bit CRC	BCH (32,21) FEC, data interleaving, scrambling. Per-frame or per-window ACKs (optional)
Communication modes	Unicast	Yes	Yes	Yes	Yes	Yes
	Broadcast	Yes	Yes	Yes	Yes	Yes
	Multicast	Yes (NWK and APL layers). Not supported by MAC	IP multicast (not optimized for LoW-PANs). Not supported by MAC	Yes	Yes	Yes
	Other modes	Indirect addressing	IPv6 anycast	No	No	N/A
Identifiers		16- and 64-bit MAC addresses 16-bit NWK identifiers	16- and 64-bit MAC addresses 28-bit IPv6 addresses (which can be compressed to 16-bit IDs)	32-bit (home ID), 8-bit (node ID)	24-bit module ID	48-bit MAC addresses
Device types		Coordinator, router, and end device	Edge router, mesh node (mesh under), router (route over), host	Controllers and slaves	Single type of device	Single type of device

Table 1 continued on the next page.

		ZigBee	6LoWPAN	Z-Wave	INSTEON	Wavenis
Network layer	Multihop solution	Mesh routing, tree routing, and source routing	RPL	Source routing	Simulcast	Tree routing
	Hop limit	30/10/5 (mesh routing/tree routing/source routing)	255	4	4	N/A
	Multihop solution state	$O(N)$ (mesh routing), $O(1)$ (many-to-one routing)	$O(N)$ (root), $O(N_{DAGs})$ (other devices)	$O(N^2)$ (controller), $O(N_{prec})$ (routing slaves), no state (slaves)	No state	$O(N)$ (root), $O(1)$ (other devices)
End-to-end reliability		ACKs and control of duplicate packets	TCP/UDP/other	ACKs	ACKs and NAKs	—
Application layer	Command space	65,536 (clusters)	—	32,768	65,536	—
	Device type space	65,536	—	N/A	65,536	—
Security		Integrity, confidentiality, access control, and key management	Integrity, confidentiality, and access control (IEEE 802.15.4). Key management not currently supported.	128 bit AES encryption (400 series chip)	Encryption (e.g., rolling codes)	3DES and 128 bit AES encryption
Translation gateway needed for Internet connectivity		Yes	No	Yes (not needed for IP-Wave)	Yes	Yes
Implementation size		45–128 kbytes (ROM), 2.7–12 kbytes (RAM)	24 kbytes (ROM), 3.6 kbytes (RAM)	32–64 kbytes (flash), 2–16 kbytes (SRAM)	7 kbytes (Flash), 4 kbytes (external EEPROM), 256 bytes (internal EEPROM), 256 bytes (SRAM)	48 kbytes (flash), 400 bytes (RAM), 20 bytes (non-volatile memory)
Specification publicly available		Yes	Yes	No	No	No

Table 1. *Summary of the main features of ZigBee, 6LoWPAN, Z-Wave, INSTEON, and Wavenis.*

to-point (e.g., a switch transmits a command to a light), point-to-multipoint (e.g., a remote control transmits a command to a group of devices), and multipoint-to-point (e.g., several sensors report measured values to a central control).

- Delay is not critical for some monitoring applications, but a WHAN should provide quick results in the detection of emergency situations and in the actions of the user.
- WHANs should offer Internet connectivity to allow remote home monitoring and management.
- Some applications (e.g., an intruder alarm system controlled by WHAN technology) require the protection of security services.
- The nodes may have a small memory capacity (e.g., a few kilobytes of RAM) and may exhibit limited processing capability (with processors running typically at tens of megahertz). Some nodes may draw their power from batteries or even some form of power harvesting.

Solutions for WHANs

This section presents an overview of solutions that have been specifically tailored to or are suitable for WHANs. Further details and the main characteristics of each solution are shown in Table 1.

ZigBee

ZigBee is a wireless networking technology developed by the ZigBee Alliance for low-data-rate and short-range applications. The ZigBee protocol stack is composed of four main layers: the physical (PHY) layer, the medium access control (MAC) layer, the network (NWK) layer, and the application (APL) layer. In addition, ZigBee provides security functionality across layers (Fig. 2a). The two lower layers of the ZigBee protocol stack are defined by the IEEE 802.15.4 standard, while the rest of the stack is defined by the ZigBee specification.

The initial version of IEEE 802.15.4, on which ZigBee is based, operates in the 868 MHz, 915 MHz, and 2.4 GHz bands, which are available in

The ZigBee PRO solution also offers many-to-one routing for communication between several devices and a central controller or sink node. This node may reply back to the devices using source routing. Only ZigBee coordinators and routers participate in routing operations.

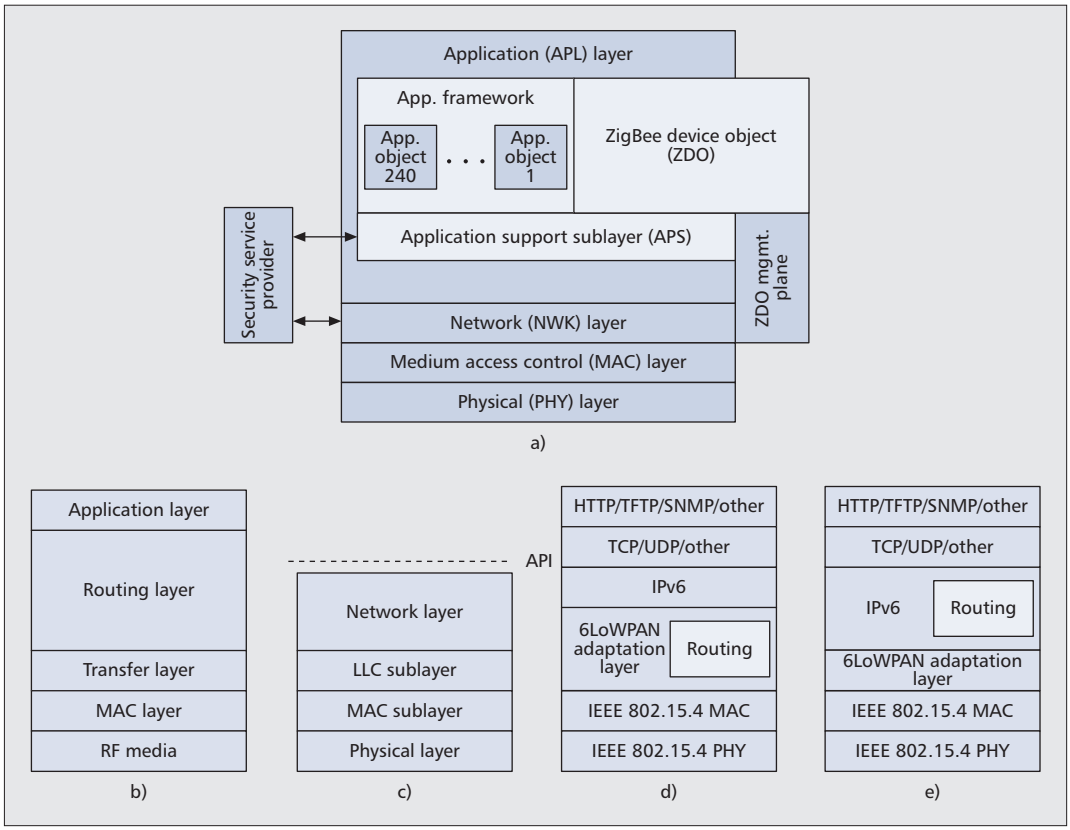

Figure 2. *Protocol architectures suitable for WHANs: a) ZigBee; b) Z-Wave; c) Wavenis; d) 6LoWPAN (mesh under); e) 6LoWPAN (route over).*

Europe, North America and worldwide, respectively. The data rates are 20 kb/s, 40 kb/s, and 250 kb/s, respectively. Binary phase shift keying (BPSK) is used in the first two bands and orthogonal-quadrature phase shift keying (O-QPSK) is used for the 2.4 GHz signals. These communication mechanisms are combined with direct sequence spread spectrum (DSSS).

There are two methods for channel access in IEEE 802.15.4: beacon-enabled and beaconless. The first one assumes that there is a node acting as the personal area network (PAN) coordinator, which transmits beacons for network synchronization. With this scheme, the time between beacons is divided into three periods:

- A contention access period (CAP) in which carrier sense multiple access with collision avoidance (CSMA/CA) is used
- A contention-free period (CFP), in which a node can transmit in an allocated guaranteed time slot (GTS)
- An inactive period, in which nodes may remain in sleep mode

In the beaconless mode, devices employ a plain CSMA/CA scheme. IEEE 802.15.4 allows the use of acknowledgment (ACK) frames for unicast transmissions.

ZigBee defines three device roles:

- The ZigBee coordinator, which corresponds to an IEEE 802.15.4 PAN coordinator
- The ZigBee router
- The ZigBee end device

The latter is normally a simple device with very low capabilities.

The ZigBee NWK layer specifically supports addressing and routing for the tree and mesh topologies. The tree topology, which is adequate for data collection, is rooted at the ZigBee coordinator. This scheme includes a mechanism for address assignment, which also facilitates multihop data delivery. In a mesh topology, routes are created on demand and are maintained using a set of mechanisms based on the ad hoc on-demand distance vector (AODV) routing protocol. This solution is used for arbitrary point-to-point traffic. The ZigBee PRO solution also offers many-to-one routing for communication between several devices and a central controller or sink node. This node may reply back to the devices using source routing. Only ZigBee coordinators and routers participate in routing operations.

The development of ZigBee application objects (i.e., the applications themselves) can take advantage of application profiles. There are two relevant ZigBee application profiles for WHANs. The first one is the ZigBee Home Automation Public Application Profile [1], which defines device descriptions, commands, attributes, and other standard practices for ZigBee applications in a residential or light commercial environment; the main application areas considered are lighting, HVAC, window shades, and security. The second one is the ZigBee Smart Energy Profile [2], which focuses on energy demand response and load management applications. With regard to the home area, this profile focuses on communication between home devices and the energy service portal (ESP), which connects a ZigBee Smart Energy WHAN with the communication network of an energy

supply company. A ZigBee Smart Energy WHAN has higher security requirements than a regular ZigBee WHAN. Hence, nodes of the latter cannot interoperate with the first ones unless they support the Smart Energy profile. Finally, the future ZigBee RF4CE specification will offer a simple device-to-device remote control solution for consumer electronics, which will not use full-featured mesh networking capabilities.

Z-Wave

Z-Wave is a wireless protocol architecture developed by ZenSys (now a division of Sigma Designs) and promoted by the Z-Wave Alliance for automation in residential and light commercial environments. The main purpose of Z-Wave is to allow reliable transmission of short messages from a control unit to one or more nodes in the network [3]. Z-Wave is organized according to an architecture composed of five main layers: the PHY, MAC, transfer, routing, and application layers (Fig. 2b).

The Z-Wave radio mainly operates in the 900 MHz ISM bands (e.g., 868 MHz in Europe and 908 MHz in the United States). Z-Wave allows transmission at 9.6 and 40 kb/s data rates using binary frequency shift keying (BFSK) modulation. The recent Z-Wave 400 series single chip supports the 2.4 GHz band and offers bit rates up to 200 kb/s.

The MAC layer of Z-Wave defines a collision avoidance mechanism that allows the transmission of a frame when the channel is available. Otherwise, the transmission attempt is deferred for a random period of time. The transfer layer manages the communication between two consecutive nodes. This layer provides an optional retransmission mechanism based on ACKs.

Z-Wave defines two types of devices: controllers and slaves. Controllers poll or send commands to the slaves, which reply to the controllers or execute the commands.

The Z-Wave routing layer performs routing based on a source routing approach. When a controller transmits a packet, it includes the path to be followed in the packet. A packet can be transmitted over up to four hops, which is sufficient in a residential scenario and hard-limits the source routing packet overhead. A controller maintains a table that represents the full topology of the network. A portable controller (e.g., a remote control) tries first to reach the destination via direct transmission. If that option fails, the controller estimates its location and calculates the best route to the destination. Slaves may act as routers. Routing slaves store static routes (typically toward controllers) and are allowed to send messages to other nodes without being requested to do so.

Slaves are suitable for monitoring sensors, in which the delay contributed by polling is acceptable, as well as for actuators that perform actions in response to activation commands. Routing slaves are used for time-critical and non-solicited transmission applications such as alarm activation.

INSTEON

INSTEON [4] is a solution developed for home automation by SmartLabs and promoted by the INSTEON Alliance. One of the distinctive features of INSTEON is the fact that it defines a mesh topology composed of RF and power line links. Devices can be RF-only or power-line-only, or can support both types of communication. INSTEON RF signals use frequency shift keying (FSK) modulation at the 904 MHz center frequency, with a raw data rate of 38.4 kb/s.

INSTEON devices are peers, which means that any of them can play the role of sender, receiver, or relayer. Communication between devices that are not within the same range is achieved by means of a multihop approach that differs in many aspects from traditional techniques. All devices retransmit the messages they receive, unless they are the destination of the messages. The maximum number of hops for each message is limited to four (as in Z-Wave). The multihop transmission is performed using a time slot synchronization scheme, by which transmissions are permitted in certain time slots, and devices within the same range do not transmit different messages at the same time. These time slots are defined by a number of power line zero crossings. RF devices not attached to the power line can transmit asynchronously, but the related messages will be retransmitted synchronously by RF devices attached to the power line. In contrast to classical collision avoidance mechanisms, devices within the same range are allowed to transmit the same message simultaneously. This approach, which is called simulcast, relies on the very low probability of multiple simultaneous signals being cancelled at the receiver.

Wavenis

Wavenis is a wireless protocol stack developed by Coronis Systems for control and monitoring applications in several environments, including home and building automation. Wavenis is currently being promoted and managed by the Wavenis Open Standard Alliance (Wavenis-OSA). It defines the functionality of physical, link, and network layers [5]. Wavenis services can be accessed from upper layers through an application programming interface (API) (Fig. 2c).

Wavenis operates mainly in the 433 MHz, 868 MHz, and 915 MHz bands, which are ISM bands in Asia, Europe, and the United States. Some products also operate in the 2.4 GHz band. The minimum and maximum data rates offered by Wavenis are 4.8 kb/s and 100 kb/s, respectively, with 19.2 kb/s being the typical value. Data are modulated using Gaussian FSK (GFSK). Fast frequency-hopping spread spectrum (FHSS) is used over 50 kHz bandwidth channels.

The Wavenis MAC sublayer offers synchronized and non-synchronized schemes. In a synchronized network, nodes are provided with a mixed CSMA/time-division multiple access (TDMA mechanism for transmitting in response to a broadcast or multicast message. In such a case, a node allocates a time slot that is pseudo-randomly calculated, based on its address. Before transmission in that slot, the node performs carrier sense (CS). If the channel is busy, the node computes a new time slot for the transmission. For non-synchronized networks, in applications in which reliability is a critical

The initial version of IEEE 802.15.4, on which ZigBee is based, operates in the 868 MHz, 915 MHz, and 2.4 GHz bands, which are available in Europe, North America and worldwide, respectively. The data rates are 20 kb/s, 40 kb/s, and 250 kb/s, respectively.

Despite the initial skepticism of many researchers about the suitability of the Internet architecture for sensor networks, today good performing implementations of IPv6 stacks are available for these environments.

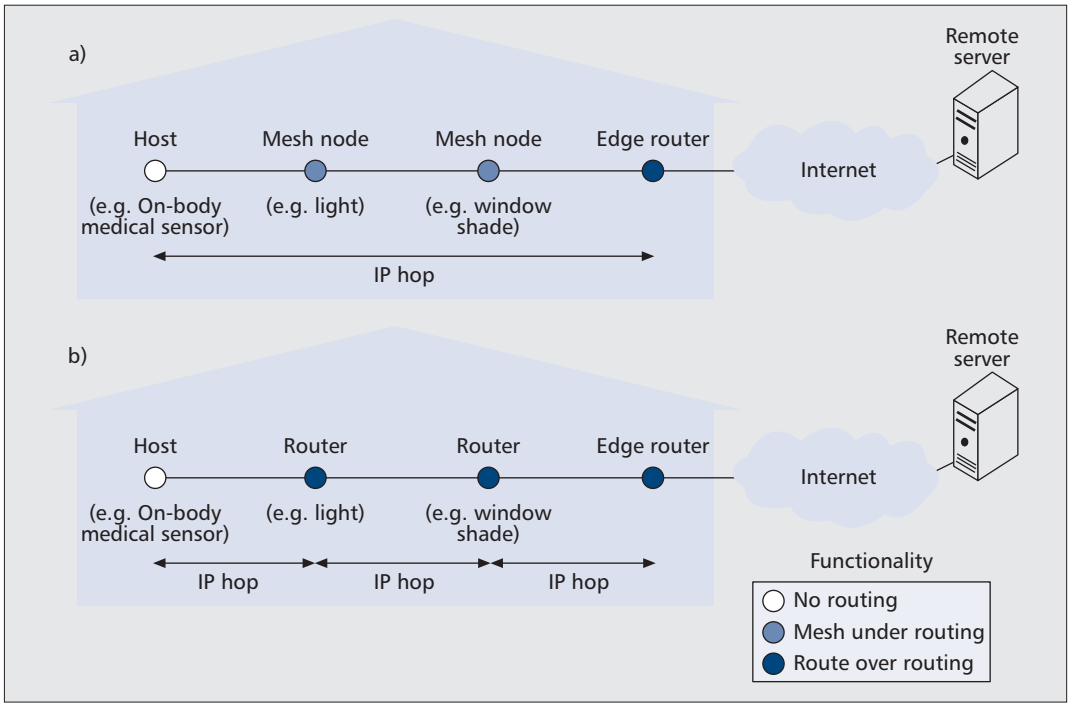

Figure 3. *Example of a 6LoWPAN-based WHAN. Mains-powered devices are appropriate as routers: a) mesh under; b) route over.*

requirement (alarms, security, etc.), CSMA/CA is used. The Wavenis logical link control (LLC) sublayer manages flow and error control by offering per-frame or per-window ACKs.

Wavenis defines only one type of device. The Wavenis network layer specifies a four-level virtual hierarchical tree. The root of the tree may play the role of a data collection sink or a gateway, for instance. A device that joins a Wavenis network intends to find an adequate parent. For this purpose, the new device broadcasts a request for a device of a certain level and a sufficient quality of service (QoS) value. The QoS value is obtained by taking into consideration parameters such as received signal strength indicator (RSSI) measurements, battery energy, and the number of devices that are already attached to this device.

IP-Based Solutions

Despite the initial skepticism of many researchers about the suitability of the Internet architecture for sensor networks, today good performing implementations of IPv6 stacks are available for these environments [6]. In fact, IPv6 has solutions ready for network autoconfiguration and statelessness, and satisfies the large address space needed for such networks. In parallel, the Internet Engineering Task Force (IETF) has been carrying out the standardization of mechanisms for extending the Internet for sensor and actuator networks. Furthermore, the use of IP for these devices is being promoted by the recently founded IP for Smart Objects (IPSO) Alliance. While the work done by the IETF is currently in progress, IP-based sensor networks are emerging and could dramatically increase the capillarity of the Internet. In the near future, fully standardized IP-based solutions for WHANs will be available.

The IETF IPv6 over Low-Power Wireless PAN (6LoWPAN) Working Group (WG) has defined the frame format and several mechanisms needed for the transmission of IPv6 packets on top of IEEE 802.15.4 networks. These networks are referred to as LoWPANs. The mechanisms offered by 6LoWPAN are:

- Fragmentation, since IPv6 mandates support for 1280-byte packets and the maximum IEEE 802.15.4 frame size is 127 bytes
- Header compression, which can compress a common 40-byte IPv6 header to a 2-byte header
- IPv6 address auto-configuration
- IPv6 neighbor discovery for LoWPANs

If a LoWPAN follows the mesh topology, a routing protocol is needed. Two schemes are envisaged for routing in LoWPANs: mesh under and route over. In mesh under (Figs. 2d and 3a), routing is performed below IP using IEEE 802.15.4 addresses. In this configuration the whole LoWPAN appears as a single IP link. In route over (Figs. 2e and 3b), every radio hop is equivalent to an IP hop, and routing occurs at the IP layer. As of the writing of this article, the IETF Routing Over Low Power and Lossy Networks (ROLL) WG is developing the IPv6 Routing Protocol for Low power and lossy networks (RPL), which is a likely candidate protocol for the route over configuration. RPL maintains directed acyclic graphs (DAGs), which may be rooted at sink nodes, and naturally supports multipoint-to-sink and sink-to-multipoint communications. Point-to-point communications are also supported, but routes between arbitrary nodes may not be optimal, since they are constrained to the DAG structures.

There are different types of 6LoWPAN devices. An edge router interconnects a LoW-

PAN with another network. A mesh node and a router perform routing tasks in the mesh under and route over configurations, respectively. A host is a simple device that only sources or sinks IPv6 packets (Fig. 3).

Discussion

This section discusses the solutions described above with regard to a set of criteria that take into account the requirements for WHANs plus additional technical and non-technical considerations.

Physical Layer

Modulation and Spread-Spectrum Techniques — Z-Wave and INSTEON use narrowband signals with FSK modulations, which are easy to implement. Wavenis uses GFSK, which has greater spectral efficiency than FSK. In contrast, IEEE 802.15.4-based technologies use PSK modulations, which are more complex but offer better signal-to-noise ratio (SNR). On the other hand, the IEEE 802.15.4 and Wavenis physical layers have spread-spectrum techniques, which provide protection against multipath and narrowband interference.

Single-Channel vs. Multichannel — IEEE 802.15.4 offers several channels in the 915 MHz and 2.4 GHz bands. Hence, in ZigBee and 6LoWPAN, it is possible to build mechanisms against interference based on selecting the least interfered channel. In fact, the ZigBee coordinator can decide to re-form the whole network in a new channel if severe interference is detected by any node. In contrast, INSTEON, Wavenis, and Z-Wave (except for the 400 series single chip of the latter) operate in a single channel in sub-gigahertz bands. This approach exploits the fact that these bands are currently less prone to interference than the 2.4 GHz band in residential scenarios and simplifies hardware design. However, it is uncertain how much interference will be present in the sub-gigahertz bands in the future. In this regard, the recent Z-Wave 400 series chip has a frequency agility mechanism whereby the receiver simultaneously listens on three different channels, and the transmitter can use the least interfered one.

Link Layer

Reliability — Z-Wave and INSTEON employ simple 8-bit checksums, while ZigBee and 6LoWPAN exploit the more powerful 16-bit one used in IEEE 802.15.4. Wavenis uses more advanced bit error control techniques (Table 1). With the exception of INSTEON, the considered solutions provide optional link layer ACKs for reliable link layer transmission. This feature allows the solutions to be customized in accordance with the requirements of applications. For example, reliability may be traded for energy and bandwidth savings for alarm or remote care applications.

Delay — Figure 4 plots the expected latencies of a command transmission from a sender to a one-hop receiver for reliable and unreliable modes. The results are theoretical, under ideal conditions (except for Z-Wave results, which are experimental [7]). For reliable mode, the round-trip time including transmission of an ACK is provided. For comparison purposes, 900 MHz channels are assumed, and INSTEON end-to-end reliable mode is included in the analysis. On/off and level control commands are considered for ZigBee. For 6LoWPAN, the range of minimum and maximum values is given, assuming the use of UDP and a payload that fits into a single IEEE 802.15.4 frame.

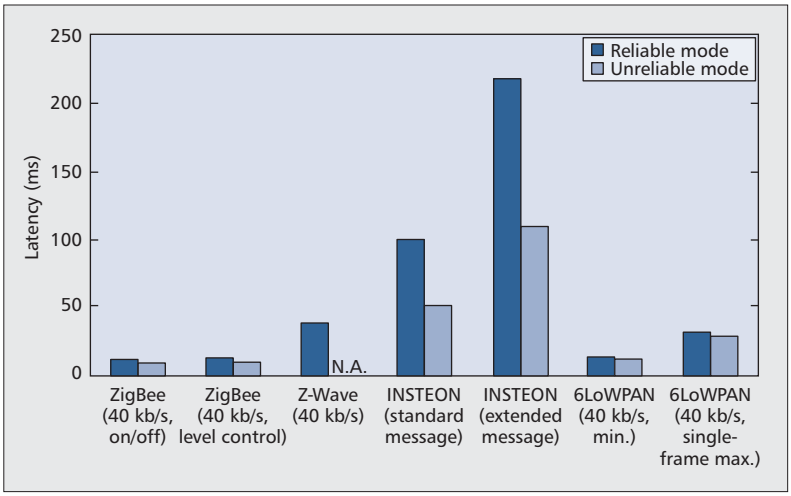

Figure 4. *Expected latencies of a command transmission from a sender to a one-hop receiver. The data rate for ZigBee, Z-Wave, and 6LoWPAN is 40 kb/s. INSTEON nominal data rate is 38.4 kb/s. (Note: Z-Wave results are experimental.)*

Network Layer

Routing/Multihopping State — In Z-Wave, only the controller stores and maintains a routing table (routing slaves, which have preconfigured routes toward a number of destinations, N_{prec}, are an exception). In contrast, the ZigBee Home Automation Public Application Profile recommends the use of large routing tables to account for the high density expected in a residential scenario, which increases memory requirements on ZigBee nodes. The routing state in all nodes that use ZigBee mesh routing is $O(N)$, where N is the number of active destinations in the network. However, in many-to-one routing, the state is $O(1)$. In Wavenis, each device only stores its own route to the root; hence, the routing state is also $O(1)$. The root, which may not exhibit the same constraints as the other nodes, stores the routes to reach each node. The same reasoning applies for a DAG root in RPL. The routing state of the other RPL devices is $O(N_{DAGs})$, where N_{DAGs} is the number of DAGs in the network. INSTEON devices use simulcast instead of routing, which avoids the need to store state for making multihop communications possible.

Routing Metrics — The use of link quality metrics is particularly beneficial in home environments, where multipath and interference may affect performance. ZigBee and 6LoWPAN can take advantage of the link quality indicator (LQI) offered by IEEE 802.15.4, which is imple-

Being an Internet standard, 6LoWPAN is (and CoRE protocols will be) open and its implementation does not require a license, which means that it can reach a larger audience than competing technologies.

mented in many radio chips using a bit error rate (BER) estimate. However, Wavenis uses a link quality estimator based on RSSI, which may not be accurate due to interference and multipath. Z-Wave selects routes based on a hop count metric and is unaware of link quality.

Route Change Latency — Because INSTEON uses simulcast instead of routing, when an intermediate device becomes unavailable, data can still reach the destination through alternative paths (if they exist) without suffering a connectivity gap. The other solutions, which use routing, experience the latency incurred for detecting the link failure and finding an alternative path (if it exists). The route change latency (RCL) in Z-Wave is 1 s on average, while it is between 50 and 100 ms in ZigBee [8]. Detection of a link failure may be fast if the link layer operates in acknowledged mode. An absence of link layer ACKs after the transmission of a data frame may indicate a link failure. Otherwise, the routing protocol may have to rely on the reception of control messages for connectivity maintenance, which typically leads to link failure detection delays on the order of seconds.

End-to-End Reliability

ZigBee, Z-Wave, and INSTEON offer simple end-to-end acknowledgment and retransmission mechanisms. ZigBee also filters duplicate packets. In 6LoWPAN, when reliable transport is needed, implementers have resorted to using UDP augmented with sequence numbers, ACKs, and retries. In fact, TCP may be too complex for very limited devices, and it underperforms in wireless scenarios.

Application Layer

ZigBee, Z-Wave, and INSTEON have a set of well defined commands and attributes for various WHAN applications. This functionality does not currently exist for 6LoWPAN. Moreover, traditional application layer Internet protocols (e.g., HTTP and SNMP) and data encoding formats are not naturally suited to 6LoWPAN-based WHANs, given the constraints of the devices and the 50–60-byte transport layer payloads available in LoWPANs. The new IETF CoRE WG will develop new or adapted application-layer protocols and data encoding formats. WHAN is considered a target scenario [9].

Security

ZigBee and 6LoWPAN take advantage of the security services offered by IEEE 802.15.4 at the link layer (Table 1), which use the 128-bit key Advanced Encryption Standard (AES) algorithm. Key management is provided in ZigBee by the APL layer, but it has not yet been specified for 6LoWPAN. While the Z-Wave 200 and 300 series chips do not offer security services, the 400 series chip supports 128-bit AES encryption. INSTEON offers various encryption methods but recommends the use of simple rolling-code encryption, as used in garage door openers. Wavenis also supports several encryption algorithms, including 128-bit AES.

Internet Connectivity

A significant advantage of 6LoWPAN is the fact that it is intrinsically interoperable with the Internet. Connecting a 6LoWPAN-based WHAN to the Internet does not require the use of a protocol translation gateway. Instead, a 6LoWPAN-based WHAN can be connected to the Internet by means of an IP router, offering end-to-end IP communication. This approach avoids issues in terms of security, management, and consistency in QoS policies.

Remarkably, while the rest of the WHAN solutions considered in this article were designed without native IP support, most of them have identified convergence with IP as a key element to satisfy current market requirements. By mid-2009, ZigBee announced the incorporation of IETF standards into its specification portfolio, and Sigma Designs introduced the IP-Wave chip, which runs an IP stack on the Z-Wave single-chip solution. Over the same period, members of the Wavenis-OSA board of directors declared that IP is being considered as layer three for future Wavenis specifications.

Implementation Size

ZigBee, Z-Wave, and INSTEON implement protocol architectures up to application-layer functionality. ZigBee requires the largest footprint (Table 1) because it has a large panoply of elaborate mechanisms for a broad range of applications. In contrast, Z-Wave and INSTEON are specifically developed for home automation and offer simpler solutions. INSTEON is the WHAN technology that requires the least memory for its implementation, mainly due to the simplicity of simulcast. Wavenis, which does not specify services on top of the network layer, consumes a small amount of RAM but requires a medium flash memory size. Current 6LoWPAN implementations (including routing and transport layer protocols, but excluding application layer protocols) require less ROM/flash than ZigBee, Z-Wave, and Wavenis.

Standardization and Market Adoption

A drawback of INSTEON, Z-Wave, and Wavenis is the fact that their specifications are not publicly available. While access to the ZigBee specification is open, its implementation requires ZigBee Alliance membership. In contrast, being an Internet standard, 6LoWPAN is (and CoRE protocols will be) open, and its implementation does not require a license, which means that it can reach a larger audience than competing technologies.

The presence of ZigBee products in the market has been delayed in comparison with those based on other solutions. The first WHAN ZigBee products were certified in August 2009. In contrast, Z-Wave, Wavenis, and INSTEON products have been in the market for years. Furthermore, millions of Wavenis devices are currently deployed worldwide, mainly for smart utility networks. However, the deployment of an estimated 30 million ZigBee-equipped smart meters is underway in North America. On the other hand, 6LoWPAN has already been implemented by several vendors. A major deployment

of 6LoWPAN and the future CoRE protocols will be the Smart Energy Version 2 (SE 2) effort. SE 2 aims at providing end-to-end connectivity between energy providers and consumers, and it has been recognized as part of the Smart Grid roadmap of the U.S. National Institute of Standards and Technology [10].

Conclusion

The article has surveyed the most relevant current and emerging solutions suitable for or tailored to WHANs: ZigBee, Z-Wave, INSTEON, Wavenis, and IP-based solutions. Whereas ZigBee and 6LoWPAN were designed for general purposes, the rest of the solutions were developed for specific applications. The increasing functionalities of some solutions and convergence toward IP suggest that future WHAN applications will benefit from enhanced quality, security, and interoperability.

Acknowledgments

This work was supported in part by the Spanish Government through project TEC2009-11453. The authors thank María del Pilar Pérez Aróstegui for her contribution to the article.

References

[1] ZigBee Alliance, "ZigBee Home Automation Public Application Profile," revision 25, v. 1.0, Oct. 2007.
[2] ZigBee Alliance, "ZigBee Smart Energy Profile Specification," revision 15, Dec. 2008.
[3] Z-Wave, "Z-Wave Protocol Overview," v. 4, May 2007.
[4] P. Darbee, "INSTEON: The Details," Aug. 2005.
[5] A. Garcia-Hernando *et al.*, Eds., *Problem Solving for Wireless Sensor Networks*, Springer, July 2008.
[6] J. Hui and D. Culler, "IP is Dead, Long Live IP for Wireless Sensor Networks," *Proc. 6th ACM Conf. Embedded Net. Sensor Sys.*, Raleigh, NC, Nov. 2008, pp. 15–28.
[7] G. Ferrari *et al.*, "Wireless Sensor Networks: Performance Analysis in Indoor Scenarios," *EURASIP J. Wireless Commun. Net.*, vol. 2007, article ID: 81864.
[8] M. Knight, "Wireless Security — How Safe is Z-Wave?," *Comp. & Control Eng. J.*, vol. 17, no. 6, Jan. 2006, pp. 18–23.
[9] C. Bormann, D. Sturek, and Z. Shelby, "Problem Statement for 6LoWPAN and LLN Application Protocols," Internet draft, July 2009, work in progress.
[10] US NIST Smart Grid; http://www.nist.gov/smartgrid

Biographies

Carles Gomez (carlesgo@entel.upc.edu) received his M.Sc. and Ph.D. degrees from the Technical University of Catalonia in 2002 and 2007, respectively. He is an assistant professor at the same university. He has worked in several publicly funded research projects, and is co-author of several papers published in journals and conferences. His current research interests include performance of wireless multi-hop networks (in particular, sensor networks) and the Internet of Things.

Josep Paradells (teljpa@entel.upc.edu) is a professor at the Technical University of Catalonia. He is head of the Wireless Networks Group (WNG). He has participated in national and European publicly funded research projects and collaborated with the main Spanish telecommunications companies. He has published his research results in conferences and journals. His expertise areas are network convergence and ambient intelligence, combining theoretical studies with real implementations.

The increasing functionalities of some solutions and convergence toward IP suggest that future WHAN applications will benefit from enhanced quality, security and interoperability.