Hardware and Software Architecture of Wireless Sensor Networks

Aaditiya Venkat Kannan

***Abstract*—Conventional RF Wireless receivers, Bluetooth, Zigbee, 802.11 consume tens to hundreds of mW of battery power when operational. We consider this problem and format a solution for it. The only way by which the power budget needed for wireless sensor networks can be met is to organize the network such that the receivers are rarely switched on. The intermittent operation requires that the terminals have a sufficiently accurate common view of time to be able to switch on at correct moment. In many contexts this places unreasonable constraints on the distribution of timing within the network and the time-keeping ability of the terminals themselves. In event driven networks, where long idle periods are punctuated by occasional feverish activity, the overhead in maintaining synchronization can be unacceptable. Our motivation in designing the terminals described here is to get to a place where intermittent operation is no longer essential. In this mode of operation (the 'always on' receiver) a terminal that has something to say can do so immediately, knowing that its neighbors will be listening. The simplicity of this physical layer transaction has far reaching ramifications in the networking protocols and the level of network timing that has to be maintained; a further reduction in energy utilization comes about as a result. This whitepaper illustrates the basic hardware/software requirements as well as actual hierarchical development of the wireless sensor networks. It also includes the applications of wireless sensor network in the real world environment.**

***Index Terms*—Bluetooth, intermittent operation, receivers, wireless sensor networks, Zigbee.**

I. Introduction

Smart environments represent the next evolutionary development step in building, utilities, industrial, home, shipboard, and transportation systems automation. Like any sentient organism, the smart environment relies first and foremost on sensory data from the real world. Sensory data comes from multiple sensors of different modalities in distributed locations. The smart environment needs information about its surroundings as well as about its internal workings; this is captured in biological systems by the distinction between *exteroceptors* and *proprioceptors* .The challenges in the hierarchy of detecting the relevant quantities, monitoring and collecting the data, assessing and evaluating the information, formulating meaningful user displays, and performing decision-making and alarm functions are enormous. The information needed by smart environments is provided by Distributed Wireless Sensor Networks, which are responsible for sensing as well as for the first stages of the processing hierarchy.

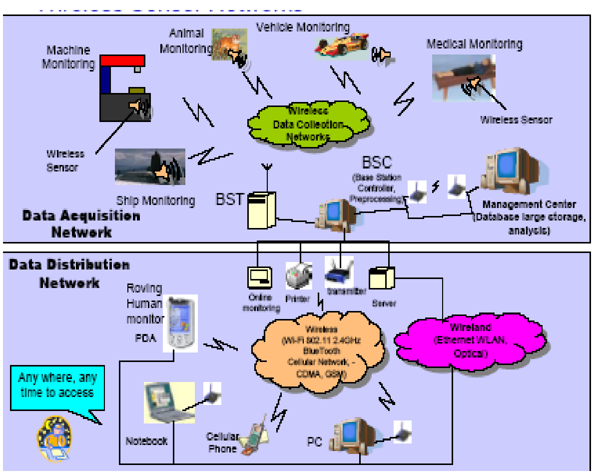

Fig. 1. Wireless sensor networks.

The Fig. 1 shows the complexity of wireless sensor networks, which generally consist of a data acquisition network and a data distribution network, monitored and controlled by a management center. The plethora of available technologies makes even the selection of components difficult, let alone the design of a consistent, reliable, robust overall system.

The study of wireless sensor networks is challenging in that it requires an enormous breadth of knowledge from an enormous variety of disciplines. In this paper we outline communication networks, wireless sensor networks and smart sensors, physical transduction principles, commercially available wireless sensor systems, self-organization, signal processing, decision-making and concepts for home automation.

II. Historical Development and Standards

A. Ethernet

The Ethernet was developed in the mid 1970's by Xerox, Intel, and was standardized in 1979. The Institute of Electrical and Electronics Engineers (IEEE) released the official Ethernet standard IEEE 802.3 in 1983 [1]. The Fast Ethernet operates at ten times the speed of the regular Ethernet and was officially adopted in 1995 [1]. It introduces new features such as full-duplex operation and auto-negotiation. Both these standards use IEEE 802.3 variable-length frames having between 64 and 1514-byte packets [1].

B. Token Ring

In 1984 IBM introduced the 4Mbit/s token ring network. The system was of high quality and robust, but its cost caused

Manuscript received August 23, 2013; revised March 25, 2014.

Aaditiya Venkat Kannan is with Anna University, India (e-mail: aadivenkat_92@yahoo.co.in).

DOI: 10.7763/JACN.2014.V2.113

it to fall behind the Ethernet in popularity. IEEE standardized the token ring with the IEEE 802.5 specification [1]. The Fiber Distributed Data Interface (FDDI) specifies a 100Mbit/s token-passing, dual-ring LAN that uses fiber optic cable [1]. It was developed by the American National Standards Institute (ANSI) in the mid 1980s, and its speed far exceeded current capabilities of both Ethernet and IEEE 802.5 [1].

C. Gigabit Ethernet

The Gigabit Ethernet Alliance was founded in 1996, and the Gigabit Ethernet standards were ratified in 1999, specifying a physical layer that uses a mixture of technologies from the original Ethernet and fiber optic cable technologies from FDDI [1].

D. Client-Server

Networks became popular in the late 1980's with the replacement of large mainframe computers by networks of personal computers. Application programs for distributed computing environments are essentially divided into two parts: the client or front end, and the server or back end [1].

E. Peer-to-Peer Networking

Peer-to-Peer networking architectures have all machines with equivalent capabilities and responsibilities. There is no server, and computers connect to each other, usually using a bus topology, to share files, printers, Internet access, and other resources [1].

F. 802.11 Wireless Local Area Network

IEEE ratified the IEEE 802.11 specification in 1997 as a standard for WLAN. Current versions of 802.11 (i.e. 802.11b) support transmission up to 11Mbit/s. WiFi, as it is known, is useful for fast and easy networking of PCs, printers, and other devices in a local environment [1]. Current PCs and laptops as purchased have the hardware to support WiFi [1].

G. Bluetooth

Bluetooth was initiated in 1998 and standardized by the IEEE as Wireless Personal Area Network (WPAN) specification IEEE 802.15. Bluetooth is a short range RF technology aimed at facilitating communication of electronic devices between each other and with the Internet, allowing for data synchronization that is transparent to the user [1]. Supported devices include PCs, laptops, printers, joysticks, keyboards, mice, cell phones, PDAs, and consumer products [1].

H. IrDA

IrDA is a WPAN technology that has a short-range, narrow-transmission-angle beam suitable for aiming and selective reception of signals [1].

III. Wireless Sensor Networks

Sensor networks are the key to gathering the information needed by smart environments, whether in buildings, utilities, industrial, home, shipboard, transportation systems automation, or elsewhere [2]. Recent terrorist and guerilla warfare countermeasures require distributed networks of sensors that can be deployed using, e.g. aircraft, and have self-organizing capabilities [2]. In such applications, running wires or cabling is usually impractical. A sensor network is required that is fast and easy to install and maintain [2].

A. IEEE 1451 and Smart Sensor

Wireless sensor networks satisfy these requirements. Desirable functions for sensor nodes include: ease of installation, self-identification, self-diagnosis, reliability, time awareness for coordination with other nodes, some software functions and DSP, and standard control protocols and network interfaces [3].

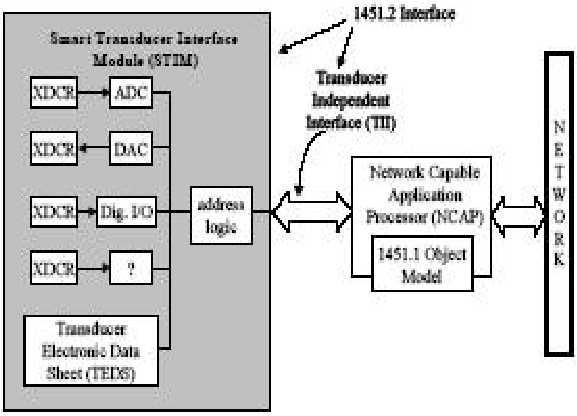

Fig. 2. The IEEE standard 1451 for wireless sensor networks.

There are many sensor manufacturers and many networks on the market today. It is too costly for manufacturers to make special transducers for every network on the market [3]. Different components made by different manufacturers should be compatible. Therefore, in 1993 the IEEE and the National Institute of Standards and Technology (NIST) began work on a standard for Smart Sensor Networks. IEEE 1451, the Standard for Smart Sensor Networks was the result. The objective of this standard is to make it easier for different manufacturers to develop smart sensors and to interface those devices to networks.

B. Smart Sensor, Virtual Sensor

Major components of basic architecture of IEEE 1451 include STIM, TEDS, TII, and NCAP see Fig. 2. A major outcome of IEEE 1451 studies is the formalized concept of a Smart Sensor [3]. A smart sensor is a sensor that provides extra functions beyond those necessary for generating a correct representation of the sensed quantity. Included might be signal conditioning, signal processing, and decision-making/alarm functions [3]. A general model of a smart sensor is shown in the figure. Objectives for smart sensors include moving the intelligence closer to the point of measurement; making it cost effective to integrate and maintain distributed sensor systems; creating a confluence of transducers, control, computation, and communications towards a common goal; and seamlessly interfacing numerous sensors of different types. The concept of a Virtual Sensor which is a component of smart sensor is also depicted. A virtual sensor is the physical sensor/transducer, plus the associated signal conditioning and digital signal processing (DSP) required to obtain reliable estimates of the required sensory information [3].

C. *Sensors for Smart Environments*

TABLE I: MEASUREMENTS OF WIRELESS SENSOR NETWORKS

	Measurand	Transduction Principle
Physical Properties	Pressure	Piezoresistive, capacitive
	Temperature	Thermistor, thermo-mechanical, thermocouple
	Humidity	Resistive, capacitive
	Flow	Pressure change, thermistor
Motion Properties	Position	E-mag, GPS, contact sensor
	Velocity	Doppler, hall effect, optoelectronic
	Angular velocity	Optical encodes
	Acceleration	Piezoresistive, piezoelectric, optical fiber
Contact Properties	Strain	Piezoresistive
	Force	Piezoelectric, piezoresistive
	Torque	Piezoresistive, optoelectronic
	Slip	Dual torque
	Vibration	Piezoresistive, piezoelectric, Optical fiber, Sound, Ultrasound
Presence	Tactile/contact	Contact switch, capacitive
	Proximity	Hall effect, capacitive, magnetic, seismic, acoustic, RF
	Distance/range	E-mag (sonar, radar, lidar), magnetic, tunneling
	Motion	E-mag, IR, acoustic, seismic(vibration)
Biochemical	Biochemical agents	Biochemical transduction
Identification	Personal features	Vision
	Personal ID	Fingerprints, retinal scan, voice, heat plume, vision motion analysis

Many vendors now produce commercially available sensors of many types that are suitable for wireless network applications. See for instance the websites of SUNX Sensors, Schaevitz, Keyence, Turck, Pepperl & Fuchs, National Instruments, UE Systems (ultrasonic), Leake (IR), CSI (vibration). The physical principles as shown in Table I may be used to measure various quantities. MEMS sensors are by now available for most of these measurands.

IV. HARDWARE

A. *Receiver*

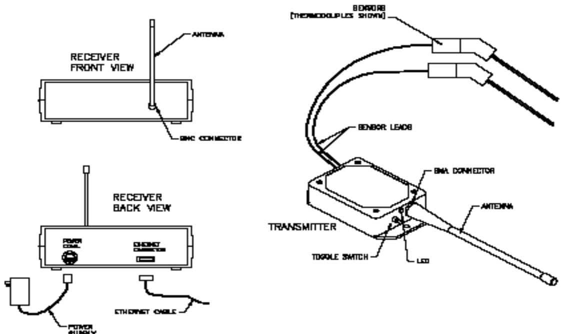

Fig. 3. Hardware for wireless sensor networks.

The receiver in its current implementation see Fig. 3 is a desktop box measuring approximately 8” long by 6” wide by 2.5” high. It has a male BNC connection on the front for antenna mounting, a standard female Ethernet cable connector on the back for its network connection, and a female 5-pin DIN connector on the back for its power connection.

To install the receiver:

- Place the receiver right-side up in a convenient location.
- Connect the short range antenna supplied with the system to the receiver.
- Connect a male Ethernet cable to the unit. The Ethernet connection should then be carried into the user’s existing TCP/IP network via a free hub port or other mechanism.
- Connect the male 5-pin DIN connector on the power supply supplied with the system to the receiver.
- Plug the power supply into any 110VAC outlet. The receiver will power up and become fully operational.

B. *Transmitter(s)*

Each transmitter in the current implementation see Fig. 3 is a flange mount box measuring approximately 4.25” long by 2.25” wide by 1” high. It has a male reverse SMA antenna connector, a green LED and a two-position toggle switch on its top. The switch turns the transmitter’s power on/off and the LED, if lit, indicates the power is on. Each transmitter has a connection port on its bottom. A sensor or sensors are connected by wire through this connection port. In the current implementation, sensors are being installed at the factory. Each transmitter contains a replaceable 3.6 VDC lithium AA battery (Tadiran Part number TL5903 recommended).

To install a transmitter:

- Install the sensor(s) leads to the terminal blocks in the transmitter. In the current implementation, sensors are being applied at the factory and no more detail is given here.
- Mount the transmitter in a convenient location using the attachment holes provided on the mounting flange.
- Screw in the short-range antenna supplied with the transmitter to the SMA connector on the transmitter.
- Toggle the power switch to the ‘ON’ position as indicated by the green LED.
- The transmitter will power up and become fully operational.

C. *Receiver IP Address*

In the current implementation the IP address of the receiver is hard-coded in firmware and is factory-set at 192.168.1.111. This address can be changed by accessing setup.html. Under current conditions, the receiver may be dropped into a peer-to-peer network, and without further configuration, be seen by any peer. If the receiver is dropped into a client/server network, the network manager must 'mask' the receiver into view by methods available in the network management system.

D. *Radio Considerations*

The periodic transmitters in the 418 MHz band are operated under CFR 47 part 15.231 which governs periodic operation in the bands 40.66 to 40.7 and frequencies above 70 MHz. The standard implementation uses a short-range antenna which provides line of sight communication between transmitters and receiver of 200-500 feet. Additional range can be gained through the use of a high gain directional antenna attached to the receiver. Walls, metal cabinets, etc. tend to interfere with communication ranges. System performance can be affected if a transmitter is constantly in motion such as a moving vehicle. Errors can be generated causing incorrect sampling [4].

V. Software

Internet Browser Use

The receiver has an on-board web server that allows a user with a web browser to view and configure the data being gathered by the receiver from the transmitters. In the current configuration the URL of the receiver is http://192.168.1.111. By entering this URL into the Address box of the browser, the user will be presented with the 'home' page of the receiver. The page is entitled 'Welcome to the Data Acquisition Program' and has a column on the left side headed 'Sensors'. Below this heading, the Address of any transmitter (and its sensors) currently being sampled by the receiver will appear, along with a readout of the last capture event and the number of data points captured. A further information point is given at the bottom of the Sensors column indicating how much of the receiver's on-board memory has been consumed by data. In the current implementation, the on-board memory can be completely consumed causing an overflow error.

VI. Applications

Civil structural monitoring (strain, fatigue and corrosion), Industrial sensing networks (temperature, pressure, displacement, tilt), Agricultural maintenance networks (temperature, humidity, etc.), Environmental site monitoring (MEMs chemical sensors) Military security networks (infra-red, magnetic, seismic)**,** Temperature, Tumidity, Vehicular movement, Lightning condition, Pressure [5].

VII. Conclusion

Today large, expensive and dumb
– Tomorrow tiny, cheap and smart.

Wireless sensor networks will soon become as important as the Internet. Just as the Internet allows access to digital information anywhere, sensor networks will provide vast arrays of real-time, remote interaction with the physical world. The industrial automation business will be generating significant growth in this new arena.

Within the next few years, this significant new technology will help run factories, optimize widely spread processes, monitor the weather, detect the spread of toxic gases in chemical spills, and even provide precious extra time in advance of tornados and earthquakes.

References

[1] B. A. Forouzan and S. C. Fegan, *Data Communication and Networking*, 4th ed.

[2] C. S. R. Murthy and B. S Manoj, "Adhoc Wireless Networks," *Architecture and Protocols*, 2008.

[3] D. Patranabis, *Sensors and Transducers*, 2nd ed., 2010,

[4] National Institute of Standards and Technology. [Online]. Available: http://www.nist.gov/el/isd/ieee/1451intro.cfm"

[5] H. Karl and A. Willig, *Protocols and Architecture for Wireless Sensor Networks*.

Aaditiya Venkat Kannan was born in Chennai, India on September 24, 1992 in a family of a chartered accountant father and a mother who is a homemaker. He finished his schooling at Padma Seshadri Bala Bhavan Senior Secondary School, Chennai and joined the prestigious Easwari Engineering College affiliated to the Anna University in Chennai, Tamil Nadu, India, to pursue his bachelor's in engineering with his chosen major as electronics and communication, towards which he showed a great passion and is currently in his final year of course.

Mr. Aaditiya Venkat Kannan is a member of the Institute of Electrical and Electronics Engineer and The Institution of Electronics and Telecommunication Engineers.