LOW POWER WIFI

Version: 0.4 (August 14, 2012)

Edited by: Edosoft Factory, S.L (Edosoft)

Project Data

Acronym: ISN

Name: Low Power Wifi WSN

ITEA number: 09034

Consortium:

- Vrije Universiteit Brussel
- Freemind
- MTP
- Edosoft
- MAIS

Document data:

Doc name: Sensor Data Stream Protocol (SDSP)

Doc version: 0.4

Doc type:

Version	Date	Remarks
0.1	July 16, 2012	First Draft
0.2	July 27, 2012	Added Comparison with conventional WiFi
0.3	August 13, 2012	Added Comparison with ZigBee
0.4	August 14, 2012	Preliminary version

Contents

Figures

1. Purpose

This document contains the State-of-the-art of Low Power Wifi in the scope of the Interoperable Sensor Networks (ISN) project. This document integrates the deliverable *State-of-the-art: communication, technology, interoperability*, which addressed the state-of-the-art study on communication protocols done in the first part of the project.

2. Introduction

WiFi (IEEE 802.11) is typically used to provide high speed, moderate range of IP data transfer between computers or portable devices and local area networks where the data rate is main design parameter. Systems optimized for these applications are fast, but they are not energy efficient. However, with proper system design and usage patterns, WiFi devices can operate efficiently and achieve a battery life of several years in sensors and other low power applications. Low power WiFi devices have the advantage of a native IP network compatible and known protocols and management tools. [2][3][4]

3. State of the art

Until recently, WiFi was not considered feasible for applications based on wireless sensor networks. WiFi had gone to laptops and mobile phones where the batteries can be recharged after several hours of operation, or line of devices that function as access points. With the increasing market for smart objects and wireless sensor networks have developed application-specific integrated circuits that are optimized for sensor applications. These products achieve a power profile similar to other architectures PHY / MAC wireless low power, while taking advantage of a well-established protocol: [5][6]

- More than 2 million WiFi devices certified.
- Robust standard with an industry alliance of nearly 300 members.
- Encryption, authentication and security end to end in the network.
- Better network management mechanisms.

These benefits make Low Power WiFi ideal for building applications related with wireless sensor networks and embedded systems.

4. Differences between Low Power WiFi & WiFi

Conventional high power Wi-Fi chips are optimized for fast response, low latency and high data rates, but the low power Wi-Fi chips are optimized for low power consumption, especially when the device is in Standby mode. For example, meanwhile a Wi-Fi device is actively listening to the channel even when no data is being transmitted to provide a good response and low latency, the low power Wi-Fi devices stay in a “low-power” mode that minimizes power consumption when data is not being transferred.

A representative operating scheme for a typical low power application is showed in the next image.

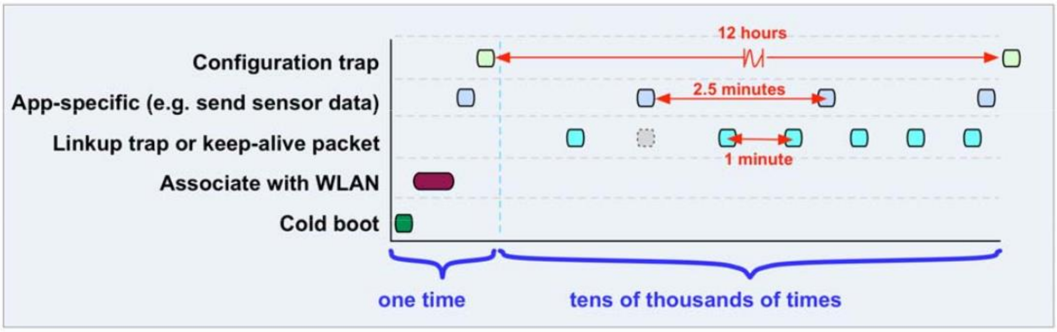

Figure 1: Operating Schema for a typical Low Power Application

After an initial set of startup tasks, a low-power device spends a lot of time doing nothing. The device must wake up periodically to support various tasks related with application or network. In the image the device sends a packet once per minute to alert that it is still active and online. Every 2.5 minutes, the low-power device awakens to send sensor data. Twice a day, the device sends a configuration Trap to a Simple Network Management Protocol (SNMP) server, to check for pending configuration changes (such as a new sensor time interval). Between each of these very brief operations, the device is in a low-power Standby state. Even during the periods in which it is awake, the device is actually sending or receiving data for only a small portion of the time.[10]

To implement a Low-Power WiFi scheme, the conventional design approach must be changed in order to minimize the power consumed during the vast majority of the time.

- The device must be highly integrated to shorten connections, minimize capacitances and inductances and reduce overall energy consumption. All major system functions like MAC, encryption, task management, network functions, radio management, baseband processing, etc. should ideally be incorporated on a single die.
- The device must be capable of flexible and fast power management, include a both fast-response states with reduced power consumption, and very-low-power Standby or Idle states when no activity is required.
- Must be possible wake-up to full capacity and fully-operational condition in a shot time.
- Network operations must be arranged so that connection maintenance and remote device management requires a minimal drain of energy resources.

4.1 Comparison of conventional and Low Power WiFi typical performance

Parameter	Convencional WiFi	Low-Power WiFi	Units

Power Consumption	Standby/Idle	Not Applicable	<4	µW
	Processor + clock sleep	13	0.2	MW
	Data processing	115	56	MW
Receive sensivity, 1Mbps		-91	-91	DBm
Time to wake from Standby		Not Applicable	10	Ms
Time to wake from processor + clock sleep		75	5	ms

Figure 2: Comparison of conventional and Low Power WiFi typical performance

5. Low Power WiFi

Low power WiFi devices are designed conforms the IEEE 802.11 standards and benefits from areas such as security (802.11i), meshing (802.11s) and Quality of Service (QOS, 802.11e). Relative to other technologies for low-power applications such as Zigbee/802.15.4, low power WiFi takes advantage of the benefits of the IP and WiFi protocols:

- WiFi sensors use IP-over-Ethernet networking environment, so there is not necessary an expensive Gateway to handle functions such as address translation or custom provisioning.

- WiFi sensors are able to obtain unique IP addresses either through static assignment or through DHCP queries.

- WiFi sensors support ARP for address conflict resolution.

- Sensor nodes can be managed and configured remotely using SNMP, a well-supported network management protocol. The node can have an SNMP agent that can respond to the SNMP manager’s GET and SET commands, and send SNMP configuration traps to the manager.

- WiFi sensors support link-layer encryption and authentication and related WiFi Protected Access (WPA/WPA2), Pre-Shared Key (PSK), Extensible Authentication Protocol (EAP), as well as Transport layer security (TLS/ SSL).

- WiFi sensors can benefit from 802.11’s provision for collision avoidance. Every Wi-Fi packet contains a Network Allocation Vector (NAV), informing all stations that hear it that the sending Station wishes to reserve the medium for a time interval long enough to complete the current transmission. A low-power Wi-Fi device can use the NAV value received to reduce power consumption during the requested interval, and avoid attempting a transmission which is likely to collide with that of another Station.

- Wi-Fi systems benefit from a large installed base and consequent broad-based familiarity with configuration, use, and troubleshooting at the physical and link layers.

5.1 Comparison of Low Power WiFi and ZigBee

Feature	ZigBee	Low-Power WiFi
5-10 years battery life	Y	Y
Installed infraestructure	N	Y
Low TCO	N	Y
Security	N	Y
Manageability	N	Y
Realiability	N	Y
Data rate scalability	N	Y
IT knowledge	N	Y

Figure 3: Comparison of Low Power WiFi and ZigBee

6. References

[1] http://www.itea2.org/

[2] A. Wang, W. Heinzelman, and A. Chandrakasan, “Energy-Scalable Protocols for Battery-Operated Microsensor Networks,” Proc. SiPS ‘99, Oct. 1999, pp. 483-492.

[3] A. Chandrakasan et al., “Design Considerations for Distributed Microsensor Systems,” Proc. CICC 1999, pp. 279-286.

[4] N. Ota and W.T.C. Kramer. TinyML: Meta-data for Wireless Networks.P. H. Chou, and Chulsung Park, “Energy-efficient platform designs for real-world wireless sensing application,” in Proc. 2005 IEE/ACM International Conf. Computer-aided design, San Jose, 2005.

[5] “Low power design methodologies,” edited by Jan M. Rabaey and Massoud Pedram, Boston, Kluwer Academic Publishers, 1996.

[6] L. Benini, G. Castelli, A. Macii, E. Macii, et al., “A discrete-time battery model for high-level power estimation,” Design, Automation and Test in Europe Conference, pp.35-39, 2000.

[7] Phani K. Neelakantham. “Wireless Netwoking Study of IEEE 802.11 Specification” 2002

[8] Dr.S.S.Riaz Ahamed. TheRole of ZigBee Technology in Future Data Communication System 2009

[9] Nikos Grammalidis,Fire Detection and Management through a Multi-Sensor Network for the Protection of Cultural Heritage Areas from the Risk of Fire and Extreme Weather, 2010

[10] “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”, IEEE 802.11, June 12, 2007.

[11] “Power Consumption and Energy Efficiency Comparison of WLAN Products”, Atheros Communications, 2003