Buletinul Ştiinţific al Universităţii "Politehnica" din Timişoara

Seria ELECTRONICĂ şi TELECOMUNICAŢII
TRANSACTIONS on ELECTRONICS and COMMUNICATIONS

Tom 49(63), Fascicola 2, 2004

Design Rules for Lightweight Short-Range Wireless Networks

Axel Sikora[1]

Abstract – The proliferation of mobile computing devices including laptops, personal digital assistants (PDAs), and wearable computers has created an enormous demand for wireless personal area networks (WPANs). WPANs originally enabled convenient interconnection of devices around an individual person or computer. From this starting-point, a broad variety of new wireless appliances has been developed, allowing proximal devices to share information and resources. Major fields of application for these wireless short-range networks are industrial, scientific, and medical (ISM), but also consumer electronics and smart home appliances. Many of these applications are very cost-sensitive, however depend on a high degree of interoperability thanks to standardization. This contribution deals with concrete design guidelines to combine these two challenges for IEEE802.15.4 [3] and ZigBee [5] networks.

Keywords: WPAN, Short-Range Wireless Network, Design Rules, IEEE802.15.4, ZigBee

I. INTRODUCTION

Short-range wireless connectivity is a convenient add-on for many applications, as they can be controlled remotely. However, up to now, mostly proprietary point-to-point connectivity was offered for closed systems. This is true for many commercial systems, e.g. remote control in home and industrial automation, and for scientific research, e.g. [4]. With the upcoming definitions of IEEE802.15.4 [3] and ZigBee [5], there is the big chance to use only one network. Standardization promises huge advantages:

- It allows the use of networks independant of the application. Up to date, there is still a huge number of networking technologies which are dedicated to applications. This holds true for the many wired fieldbus and industrial Ethernet protocols, but also for the various proprietary wireless protocols, being used in 433 MHz, 868 MHz, and 2,4 GHz-band. If all applications use a common network technology,
  - the control of medium access control (MAC) functionality is eased, due to the inherent detection of other stations' activity.
  - the networks may become interconnected. Cluster and mesh topologies may be implemented, where some stations additionally provide routing and relaying for the network.
  - applications become interoperable, as the same data objects are used.
- If many applications use the same technology, the quantity of required chips is severely increased.
  - This enables mass production at the silicon foundries, leading to low cost.
  - This enables early scaling of wireless circuitry in order to use newest process technologies. This again reduces cost in production, but also allows the reduction of power consumption.
  - Monolithic integration becomes profitable only for high volumes. It allows further decrease of cost and power consumption, and of form factor.
  - The number of silicon foundries will be increased, allowing better choice for system designers and second sourcing.
- If the number of designs is big enough, tools and libraries will be supported. This may concern network planning and analyses, as well as programming tools and libraries.
- Design houses and consultants invest only in standardized solutions to address the largest possible market.
- Security can never be achieved by scrutinity but by using open solutions being developed and discussed by the community.

[1] Department of Information Technology, University of Cooperative Education Loerrach, Hangstrasse 46-50, D79539 Loerrach, Germany, e-mail: sikora@ba-loerrach.de

However, there are caveats connected with standardization.

- It leads to additional overhead in the systems, if functionality has to be implemented just for conformity's sake.
- It may lead to a longer time-to-market as the process of standardization implies reconciliation and compromises of different market-players.
- In some cases, not the best solutions are standardized, but those most acceptable for all parties in the standardization bodies.
- Standardized components can be interconnected. Apart from the huge benefit of internets, interdependency of systems is increased.

II. WPAN STANDARDS IEEE802.15.4 AND ZIGBEE

The history of the new standards IEEE802.15.4 [3] and ZigBee [5] begins in the second half of the nineties with the discussion of "HomeRF Lite". The formerly monolithic approach was then differentiated into two modules, which are shown in Fig. 1.

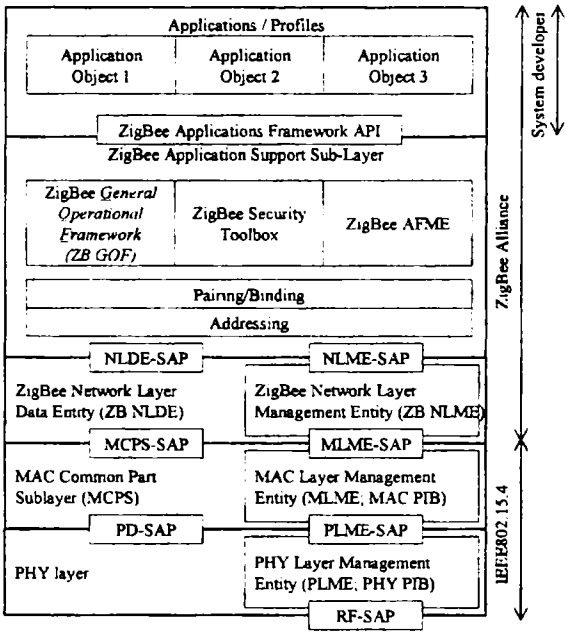


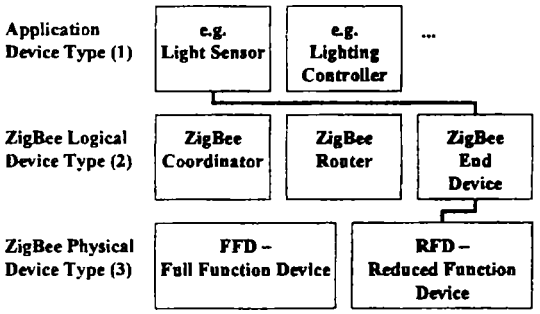
Fig. 1. Protocol Stack of IEEE802.15.4 and ZigBee [5]

- IEEE802.15.4 describes Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs). It was approved 12 May 2003 by the IEEE-SA Standards Board.
- ZigBee specifies network layer, security toolbox and application profile. It is due to be ratified by ZigBee Alliance within this year. This schedule was postponed several times, giving room to the argument that standards impede short time to market.

III. LEVELS OF STANDARD CONFORMANCE

A. *Modularity within the standards*

There are two directions of modularity envisaged in the IEEE802.15.4 and ZigBee standards. The horizontal modularity describes different classes of devices, shown in Fig. 2. This differentiation was included to allow the optimum design of low-cost applications with as little overhead as possible. The functionality of the different devices and the constraints of the different device classes is described in Table 1.



(1) Distinguishes the type of device from an end-user perspective – Specified in Profiles
(2) Distinguishes the Physical Device Types deployed in a specific ZigBee network
(3) Distinguishes type of ZigBee hardware - Based on 802.15.4 RFD and FFD definitions

Fig. 2: Device Classes in IEEE802.15.4 and ZigBee

Device Classes	Characteristics
Reduced Function Device	limited to star topology
	cannot become a network coordinator
	talks only to a network coordinator
Full Function Device	any topology
	capable to become a network coordinator
	may talk to any other device
End Node	limited to star topology
	cannot become a network coordinator
	talks only to a network coordinator
Routing Device	may route traffic within the network, but may not capable to talk to next networking hierarchy
Gateway Device	may transfer traffic to next networking hierarchy, but may not be capable to route traffic within the network

Table 1: Characteris of device classes in IEEE802.15.4 and ZigBee

As the standards follow a layered communication model, vertical modularity allows the implementation of the separate layers. The features and the constraints of these solutions is described in Table 2.

Level of Standardization	Characteristics
Layer 1:	Devices use the cheap and low-power RF chips with proprietary ≥ L2-protocols
Layer 2:	Devices use the IEEE802.15.4-library for medium access, but use proprietary ≥ L3-protocols
Layer 3:	Devices use the ZigBee network funktionality with own application protocols
Layer 7:	Devices use ZigBee application profiles

Table 2: Characteristics of standardized devices with vertical modularity

B. *Necessity of compromises*

Albeit this modular approach first implementations of the described standards show, that the complexity even of the smallest system is much higher than originally anticipated. This holds true especially for the size of program memory, which currently seems much too large to fit into an 8-bit MCU with 32 or 64kByte of flash memory together with an application of reasonable size. As memory footprint continues to be of major importance to allow lowest cost and power consumption, the necessity arises to compromise the complex standards. This is – unfortunately – caused by the fact that the modularity of the above described IEEE802.15.4 is still too coarse-grained for real life products. As this holds true for software-based products, the situation clearly is different for hardware-based solutions. However, IEEE802.15.4 was defined with a software implementation in mind, which may complicate hardware design. Currently, no developments for full MAC functionality are observed. Up to date, only partial hardware-accelators are available, e.g. AES-128 encryption and decryption [1].
It has to be clearly stated that the author is a supporter of standards. However, the ideas of scientific research can not be directly implemented in real-life products. Therefore, this contribution describes rules for the bottom-line of light versions of the standards, that reasonably support coexistence and interoperability. This seems to be ever more important as there are already various approaches for light versions simple-MAC-implementations which do not follow these basic rules.

C. *Requirements for light versions*

Basic requirements

To propose trade-off to a standard is a dangerous activity as this may call the whole standard into question. Therefore, these trade-offs shall follow strict rules. These rules are now described. In this chapter, the overall rules are listed, where in the next chapter the appropriate IEEE802.15.4 extensions are discussed.

- Rule 1: Lightweight devices shall not disturb standard devices.
- Rule 2: Standard devices shall understand messages from lightweight devices.
- Rule 3: Lightweight devices shall ignore messages not included in the lightweigt standard and shall not be obstracted.
- Rule 4: All routines in the lightweight devices covering parts of the full standard shall comply with the format and the behavior. This is essential for a smooth migration path to future enhancements.

Lightweight MAC protocol

Based on the above, the bottom-line functionality of a lightweight MAC protocol is described:

- Rule 1: All devices shall follow the 802.15.4 frame format, so that all other standard-compliant devices may understand the messages of the light devices. This clearly does not impose major overhead on these devices, as the IEEE-frame format allows a minimum size of headers:
  - 6 Bytes PHY header are compulsory. Out of those, 4 Bytes are for synchronization purposes, which cannot be omitted in any other non-standard systems.
  - 5 Bytes MAC header are minimum, when working without any addresses. Out of those, 2 Bytes are for Frame Check Sequence, which also should not be omitted in any system.

  However, it does not seem to be necessary that light-devices understand full-blown systems. This approach can be observed in many other networking standards, e.g. in CAN-standard [2], where systems with extended 29-Bit long addresses (V2.0B compliant) may be intermixed with older systems with their 11-Bit long addresses.
- Rule 2: All devices shall understand 802.15.4 beacon frames. However, it does not seem to be necessary to implement all options. IEEE802.15.4 enables reliable networking with an enhanced processing for orphaned devices with many options that blow up the memory footprint. In simple network topologies without enhanced real-time requirements, the same reliability can be achieved with the use of watchdog timers and re-transmission of association requests.
- Rule 3: All devices shall support CSMA/CA-medium access as defined in IEEE802.15.4 non-slotted access. This is a major retrenchment as the conformity to slotted access sets high requirements on the real-time capability of devices. The slotted medium access is

synchronized with the beacons that define contention access periods (CAP) and contention free periods (CFP). However, if the guaranteed time slots (GTS) in the CFP are not kept free, as some light devices do not run a time-based access scheme, this has a destructing impact on the quality of service in the slotted network.
Therefore, it seems to be necessary, that a device – not supporting slotted access – detects a beacon with GTS definition, should leave this channel by selecting another channel (rule 4).

- Rule 4: All devices shall support a dynamic channel selection (DCS) to ease coexistence as much as possible. Unfortunately, DCS is described only in ZigBee standard. Nevertheless, it seems to be indispensable that light devices with no support for slotted access leave the channel as fast as possible.

D. Light ZigBee protocol?

As the ZigBee standard is not yet ratified, it is still too early to desribe possible lightweight ZigBee rules. However, it seems to be understood by the ZigBee alliance that fine-grained vertical modularity is of major importance for the market success. This can be illustrated with routing. Routing normally is a functionality that may be done with a limited program code, but with higher consumption of data tables. For the ZigBee-standard, it is currently envisaged to run three routing levels:

- Non-routing devices (end nodes).
- Minimum routing nodes (RN-), that have no routing table and engage in limited route discovery.
- Full routing nodes (RN+), that have routing tables and engage in route discovery to fill it.

The same holds true for security solutions. However, it is highly questionable, if this approach is useful.

- Encryption algorithms, e.g. AES-128, call for hardware implementations, especially when the host-processor is a low-frequency 8-Bit-MCU. For these hardware accelerators, a uniform solution with long encryption keys may mean less cost than a modular approach with different key lengths.
- Short encryption keys, i.e. 64 or even 32 Bits for symmetric encryption, do not provide security. This is especially the case for future-proof systems that shall be operation for decades.

IV. CONCLUSIONS

It is reasonably possible to design lightweight wireless short-range devices already today which have good a migration path, minimum impact on full standard-compliant networks and additionally offer lowest cost and power-consumption. This article described the most important rules the design of those lightweight systems.

REFERENCES

[1] http://www.chipcon.com/files/CC2420_Data_Sheet_1_2.pdf
[2] "Road vehicles -- Controller area network (CAN)" ISO Standard 11898; http://www.iso.org
[3] http://www.ieee802.org/15/pub/SG4a.html
[4] http://webs.cs.berkeley.edu/
[5] http://www.zigbee.org.