Robustness against Interference in Wireless Sensor Networks

Sven Zacharias*, Thomas Newe

University of Limerick, *sven.zacharias@ul.ie*

Abstract. The response Networks (WSNs) are a novel technology combining sensory and distributed computing to sense large areas live and in detail. Since this emerging technology is at a point where it can be adopted for an increasing number of applications, reliability and interference of different networks become serious issues. This paper gives an overview of potential interference sources and their effects on the energy consumption for WSNs operating on the 2.4 GHz band of the IEEE 802.15.4 standard. It concludes with several practical solutions for developing reliable and robust WSN applications.

Introduction

Specifications. Wireless Sensor Networks (WSNs) are an emerging technology in the area of sensory and distributed computing. A WSN consists of sensor nodes, also called motes. Many sensor nodes, theoretically up to thousands or even millions, build a WSN. A single sensor node is a small and inexpensive device that is built of the following main parts: one or more sensors, a data processing unit, a wireless communication interface and an energy source.

The sensor nodes are designed to be spread without pre-configuration. They connect to a multi-hop ad hoc network and report their measurements or information, computed from the measurements, to a base station. This base station, also referred to as sink, is a gateway to another network, which is likely to be the Internet, or a computer that stores or reacts according to the received data.

1 Interference on the Physical Layer

The common communication interfaces for WSNs are based on the IEEE 802.15.4 standard [1]. It was originally developed for Low-Rate Wireless Personal Area Networks (LR-WPANs). WSNs normally use this standard behind its purpose of single-hop personal area communication and implement multi-hop communication over large areas. There is a high likelihood that the Physical Layer of most WSNs is at least partly managed by the communication module of the nodes [2].

There are three frequency basebands available, also known as the Industrial, Scientific and Medical (ISM) frequency bands. The detailed properties of these bands are named in Table 1.

Region	Frequenzy band (MHz)	Communication Channel	Data rate channel (kb/s)
World-wide	2,400 – 2,483.5	16	250
North America	902 – 908	10 (2003) / 30 (2006)	40 (2003) / 250 (2006)
Europe	868 – 868.8	1	20 (2003) / 100 (2006)

Table 1. The Industrial, Scientific and Medical (ISM) bands used in IEEE 802.15.4.

Many developers focus on the 2.4 GHz band, since it is available worldwide, it supports the highest data rate and many transmit modules are available. The trend of using this single frequency band leads to a crowded band due to the great amount of different applications using it. Additionally, other devices emit waves on this band: Bluetooth devices and Wireless Local Area Networks (W-LAN), wireless DECT phones, baby phones and other proprietary wireless devices. Microwave ovens and harmonics of monitors can also have the effect of interfering with the 2.4 GHz band. A technical report of the Jennic Cooperation [3] investigated the effects of different interference sources. This report reveals that W-LANs are the main source of interference, which is also noted in other publications [4].

SNE Simulation Notes Europe – Print ISSN 2305-9974 | Online ISSN 2306-0271
SNE 21(3-4), 2011, 171-176 | doi: 10.11128/sne.21.tn.10093

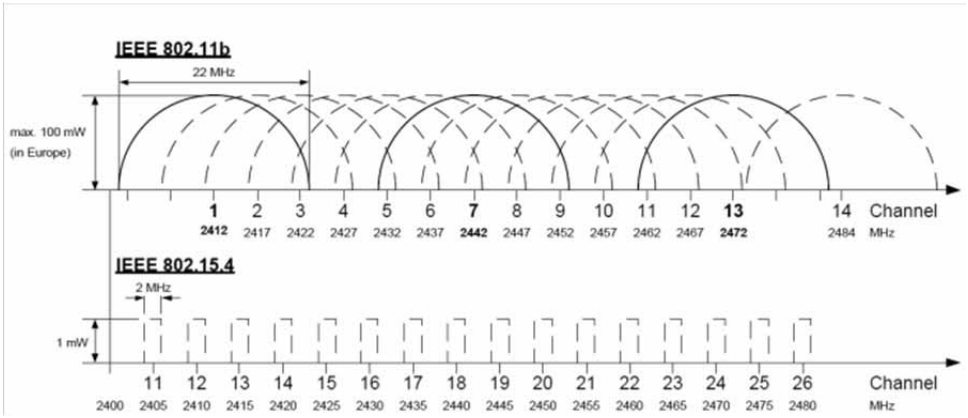

Figure 1. Channels of the 802.11b and 802.15.4 standard.

W-LANs based on the IEEE 802.111b standard have the same baseband and much more sending power than WSNs and can be seen as a major interference source, especially in urban areas. IEEE 802.11b as well as IEEE 802.15.4 separates their band into channels. 802.11b divides the band into 14 channels: each is 22 MHz wide and the Channel Centre Frequencies have a distance of 5 MHz between each other. Thus the channels overlap. For WSNs, there are 16 channels provided, each is 2 MHz wide and they are also distanced 5 MHz between each other. The counting of the WSN channels starts at 11, since there are more channels available on the lower frequency bands (see Table 1). Figure 1 gives an illustrative overview of the channels of both standards. W-LANs are often configured according to a rule of thumb: by using channels 1, 7 and 13 W-LANs do not interfere with each other. This would lead to the fact that the channels 15, 16, 21 and 22 are chosen for WSNs. In North America, the recommended channels for W-LANs are 1, 6 and 11, since channel 13 and 14 are not used.

Thus the theoretically best choices for WSNs are channels 15, 20, 25 or 26. Boano et al. [5] show the effects of an interference source on different MAC-protocols: NULLMAC, X-MAC [6], Low Power Probing [7], Low Power Listening [8] and CoReDac [9]. They also identify mechanisms to make MAC-protocols more robust against interference and to improve the X-MAC protocol that is implemented in ContikiOS in order to be more robust against interference on the Physical Layer.

2 Interference on the MAC-Layer

The Medium Access Control (MAC) Sublayer regulates the medium access and therefore is the most crucial operation for duty cycling of the nodes. Different nodes have to be awake at the same time to communicate. There are plenty of MAC-protocols for WSNs published, of which good overviews can be found in the literature [10, 11]. As shown in the previous section, the frequency band of the Physical Layer is crowded and the number of channels is limited. Hence, having two WSNs using a single channel is a risk that has to be taken seriously.

The effects of two WSNs on the same channel that are operating locally close to each other are different to the effects of interference on the Physical Layer, since there is not a pure jamming of the medium, but a competition for it. There are two possible scenarios of WSNs operating in range of each other on the same channel:

- Two or more WSNs using the same MAC-protocol: The networks behave equally on the MAC-Layer. The effects on the applications are not enormous, since most MAC-Layers are designed to provide scalability.
- Two or more WSNs with different MAC-protocols. This scenario was not taken into account when most WSN MAC-protocols were designed. A common assumption is that fairness needs not to be considered, since WSNs are typical signal applications with all nodes working together [10, 11]. This scenario is investigated in the following.

2.1 MAC-Layer Protocols

In the following, two MAC-protocols are studied in further detail and, like most protocols, they have been designed for stand-alone usage, thus competition was no design concern.

X-MAC is a short preamble MAC-protocol. It uses an enhanced version of Low Power Listening (LPL) to save energy. The nodes turn off their radios for most of the time. If a node is about to send, it turns on its radio and sends short preambles (strobes) until it receives an acknowledgement.

If it receives an acknowledgement, the message is send. Non-sending nodes wake up after a sleep time for a short listening period to monitor the channel for strobes. Due to this behaviour, the idle listening time is reduced [6].

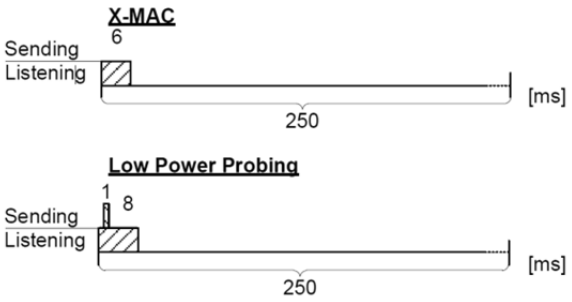

Figure 2. Idle Listening timing of X-MAC and Low Power Probing. (Do not scale from this drawing).

Low-Power Probing (LPP) is roughly the inverse approach to X-MAC. Instead of the sender announcing its will to send a message, the receiver is announcing its possibility to receive messages. When using LPP, all nodes are duty cycled and wake up for just a short time.

If a node is awake, it sends small packets (probes) to signal being awake and then it listens for a short time. A sending node turns its radio on and listens for the probe of the node that it wants to send to. When receiving it, the message is send [7]. The ideal idle listening cycle of X-MAC and LPP is shown in Figure 2. The cycles defined by the default parameters of the ContikiOS implementation generate a roughly comparable usage of the medium as the following figure reveals.

3 Energy Estimation

Since sensor nodes are likely to be battery powered, energy consumption is the key factor for the lifetime of a WSN. The estimation of the lifetime of a WSN can be complex, hence the network structure changes every time a node fails. The reliable estimation of the energy consumption of a single node is the base for further estimations. Today simulators offer a good estimation for energy consumption of single nodes in a friendly environment. In the following, COOJA, the simulator included in ContikiOS, is used. The TelosB sensor node [12] is the used hardware device. ContikiOS supports module on-time counters, thus the energy consumption can be estimated by multiplying the on-times of different modules by typical currents of the different modules. The used formula including the current factors is given in Equation 1.

The factors are taken from the shell power application included in ContikiOS and are discussed by Dunkels et al. in the publication of the software-based online energy estimation [13]. Similar factors can be found in other publications [12, 14]. In Table 2, measured values are compared with estimated values of a COOJA simulation. The used program was a simple non-interfered direct communication between a sender and a base station. The messages were sent randomly delayed in an interval of less than 5 seconds, and the energy was measured at the sender with the help of an Agilent 66321D Mobile Communications DC Source for a duration of 60 seconds. A section of the measurement is plotted in Figure 2 in full detail. NULLMAC is a protocol without any duty cycling, thus all modules are turned on all the time. The peaks of X-MAC and LPP show the radio being turned on for receiving or sending.

	NULLMAC	X-MAC	LPP
Estimated current (mA)	20.52	1.21	1.47
Measured current (mA)	18.89	0.95	1.07

Table 2. Measured and estimated currents of a TelosB sensor node. The measurement value is the mean value of a 60 sec. measurement. The estimation is based on the on-time counter simulated by COOJA for about 40 min.

$$\text{Estimated electric current [mA]} = \frac{\text{listen}\times 20[\text{mA}] + \text{transmit}\times 17.7\,[\text{mA}] + \text{cpu}\times 1.8[\text{mA}] + \text{lpm}\times 0.545[\text{mA}]}{\text{cpu} + \text{lpm}}$$

Equation 1. Energy consumption estimated by on-times of different modules with typical currents of the different modules.

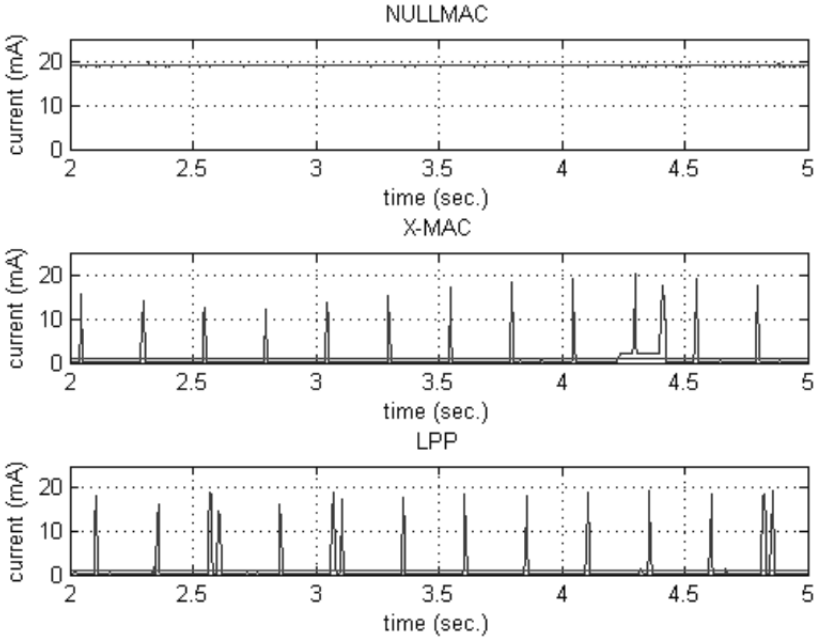

Figure 2. Measured current drawn by different MAC-Layer protocols on a TelosB node shown as a 3 sec. long section.
(mean value line calculated of full 60 sec. easurement).

The estimation may seem to be imprecise, but since the measurement has just been taken for 60 seconds in the running program and the estimation used default factors, which may vary from node to node due to non-conformity of the electronic components. Although randomly send intervals are used, the results can be still seen as good indicators for the lifetime of a node.

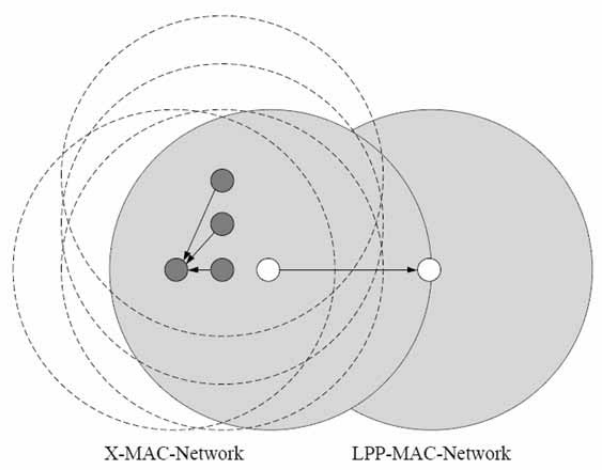

Figure 3. Simulation setup: nodes and their communication range.

3.1 Simulation Setup

A real-world experiment for MAC-protocol interference is hard to set-up, since the timing of the nodes is very important for stimulating certain patterns of behaviour and for causing a competitive situation. Therefore this paper relies on simulation.

The experiment was simulated for five different numbers of sensor nodes. Each of these different network sizes was simulated with and without interference, thus in total 10 simulations were completed. The main network operates with X-MAC while interference network uses LPP.

A single LPP node was in the range of all X-MAC nodes. In Figure 3 the network organisation is illustrated.

The main network runs an application sending a message every 5 seconds, concluding in 100 messages in total. The message consists of a timestamp and a counter. The interfering WSN sends a message every second.

3.2 Simulation Results

The simulation reveals that by an enforced bad timing, the rate of successfully delivered packets takes a nosedive. The duty cycle intervals are synchronous and X-MAC is not able to overcome this interference deadlock. The number of received packets is shown in Table 3. The table also shows logged errors of the MAC-Layer. Analysing only this logged data can help to estimate the delivery rate at the sending node, but is not accurate enough to guarantee delivery. For example, acknowledgements with packet sequence numbers and checksums are mechanisms to ensure a reliable delivery. But these mechanisms produce additional traffic and consume more energy.

Since no mechanism was implemented to ensure delivery, the total energy consumption of the WSN was not seriously affected. A cancelled send attempt is not consuming much energy, because X-MAC is announcing its sending with short strobes.

But by relating the estimated used energy to the successfully send packets, the impact of the interference is significant: The non-interfered WSN needs about 0.03 mA for a successfully sent packet and the worst effected interfered network (two X-MAC sender network) consumes about 0.11 mA per packet.

Number of sending nodes	Received packets at the base station	Errors logged at the sender
1	99/100	0
2	56/200	10 sending drops
3	159/300	144 cyclic redundancy check (crc)
4	400/400	0
5	500/500	0

Table 3 Received packets at the base station and logged errors at the sending nodes.

4 Conclusion

It was shown that the channels for WSNs are crowded and that there is the increasing chance of two or more WSNs operating locally close to each other on the same 802.15.4 channel. In this case, as shown in the simulation, competition for the medium access can occur. The following methods can be used in order to improve the robustness against interference either on the Physical Layer (channel jamming) or in form of competition of two different MAC-protocols. The list does not include mechanisms to guarantee delivery.

- Pre-deployment channel investigation: The creator of a WSN should be aware of potential interference sources and could make some measurements to find potential interference sources. The possibilities might be limited for large or ad-hoc networks, but for indoor deployment at least a W-LAN channel check should be done.
- Random sending intervals on Application Layer: A simple way to improve the robustness, without modifying any of the lower layers, is to send data in random intervals.
- Packet buffer and train: Boano et al. [5] recommend holding packets in a buffer so that cancelled send attempts can be redone. The buffer can also be emptied at once with a so-called train when first sending was successful .
- Low power sending: Messages should be sent with just the power needed to reach the next hop. This helps to save energy, since multi-hopping consumes less energy than directly transmitting to a more distant node and is less interfering.
- Channel Hopping/Spread Spectrum: By changing the channel permanently, the effect of a single interfered channel is minimised. Eavesdropping is also getting more difficult. On the other hand, this adds complexity and management overhead. The nodes have to be synchronised, which is a complex task in multi-hop or ad-hoc networks. Bluetooth uses Channel Hopping.

Acknowledgement

The authors wish to thank the following for their financial support: the Embark Initiative and Intel, who fund this research through the Irish Research Council for Science, Engineering and Technology (IRCSET) postgraduate Research Scholarship Scheme.

References

[1] IEEE. *IEEE Standard 802*.15.4™-2003, 2003

[2] Chipcon. *CC2420 2.4 GHz IEEE 802.15.4 / ZigBee-ready RF Transceiver*. June 2004 Datasheet

[3] Jennic - Technology for a changing world. *Co-existence of IEEE 802.15.4 at 2.4 GHz*. Application Note Revision 1.0, February 2008

[4] O. Gnawali, R. Fonseca, K. Jamieson, D. Moss, P. Levis. *Collection tree protocol*, Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems, SenSys '09, pages 1–14, New York, NY, USA, 2009

[5] C. A. Boano, T. Voigt, N. Tsiftes, L. Mottola, K. Römer, M. A. Zuniga. *Making sensornet mac protocols robust against interference*, Proceedings of the 7th European Conference on Wireless Sensor Networks, Coimbra, Portugal, February 2010

[6] M. Buettner, G. Yee, E. Anderson, R. Ha.: *X-MAC: A short preamble MAC protocol for duty-cycled wireless sensor networks*, Proceedings of the 4th international conference on Embedded networked sensor systems, SenSys '06, 2006

[7] M.-E. Razvan, C.-J. M. Liang, A. Terzis. *Koala: Ultra-low power data retrieval in wireless sensor networks*, Proceedings of the 7th international conference on Information processing in sensor networks, IPSN '08, pages 421–432, Washington, DC, USA, 2008

[8] K. Klues, D. Moss, J. Hui. *Tep 105 -low power listening*, http://-www.tinyos.net/tinyos-2.x/doc/html/tep105.html, last visited April 2011

[9] T. Voigt, F. Österlind. Coredac: *Collision-free command-response data collection*, 13th IEEE International Conference on Emerging Technologies and Factory Automation, Hamburg, Germany, September 2008

[10] A. Roy, N. Sarma. *Energy saving in mac layer of wireless sensor networks: a survey*, In National Workshop in Design and Analysis of Algorithm (NWDAA), India, 2010

[11] I. Demirkol, C. Ersoy, F. Alagoz. *Mac protocols for wireless sensor networks: a survey*, Communications Magazine, *IEEE*, 44(4):115 – 121, April 2006

[12] MEMSIC Inc. (formerly Crossbow): *TelosB Mote Platform Datassheet*, 2010

[13] A. Dunkels, F. Österlind, N. Tsiftes, Z. He. *Software-based on-line energy estimation for sensor nodes*, Proceedings of the fourth workshop on Embedded Networked Sensors (Emnets IV), Cork, Ireland, June 2007

[14] A. Prayati, C. Antonopoulos, T. Stoyanova, C. Koulamas, G. Papadopoulos: *A modeling approach on the telosb wsn platform power consumption*, Journal of Systems and Software, 83(8):1355 – 1363, 2010

Accepted ASIM SST Wismar, May 2011
Submitted: May 2011
Accepted November 10, 2011