

# ULRR

## Competition at the wireless sensor network MAC layer: low power probing interfering with X-MAC

Item Type	Article
Authors	Zacharias, Sven;Newe, Thomas
Citation	Journal of Physics: Conference Series;307, 012038
Publisher	IOP Publishing
Download date	2026-04-16 15:12:25
Item License	<a href="https://creativecommons.org/licenses/by-nc-sa/1.0/">https://creativecommons.org/licenses/by-nc-sa/1.0/</a>
Link to Item	<a href="https://hdl.handle.net/10344/3788">https://hdl.handle.net/10344/3788</a>

## Competition at the Wireless Sensor Network MAC Layer: Low Power Probing interfering with X-MAC

This content has been downloaded from IOPscience. Please scroll down to see the full text.

2011 J. Phys.: Conf. Ser. 307 012038

(<http://iopscience.iop.org/1742-6596/307/1/012038>)

View [the table of contents for this issue](#), or go to the [journal homepage](#) for more

Download details:

IP Address: 193.1.104.7

This content was downloaded on 24/04/2014 at 15:01

Please note that [terms and conditions apply](#).

# Competition at the Wireless Sensor Network MAC Layer: Low Power Probing interfering with X-MAC

**Sven Zacharias, Thomas Newe**

University of Limerick

E-mail: Sven.Zacharias@ul.ie

**Abstract.** Wireless Sensor Networks (WSNs) combine sensors with computer networks and enable very dense, in-situ and live measurements of data over a large area. Since this emerging technology has the potential to be embedded almost everywhere for numberless applications, interference between different networks can become a serious issue. For most WSNs, it is assumed today that the network medium access is non-competitive. On the basis of X-MAC interfered by Low Power Probing, this paper shows the danger and the effects of different sensor networks communicating on a single wireless channel of the 2.4 GHz band, which is used by the IEEE 802.15.4 standard.

## 1. Introduction

Wireless Sensor Networks (WSNs) are an emerging technology in the area of sensory and distributed computing. They enable new possibilities in measurements and monitoring by enabling very dense, large deployments of cheap, small hardware. Therefore, phenomena can be monitored live in full detail. A WSN consists of many sensor nodes (also called motes). These are small devices built of sensors, a microcontroller, a wireless communication interface and an energy source. To access the collected data, one or more base stations (also called sinks) act as data collectors, gateway and/or storage devices in the network. A key feature of WSNs is self-configuration without pre-configuring each single sensor node. Generally, sensor networks have to work reliable over a long time without human maintenance. Besides running out of energy, communication problems are one of the main dangers for reliability. In the following, the most common communication standards are presented and the crowd of communicating and potentially interfering devices is shown. Furthermore, a scenario where two WSNs that are operating and jamming each other on the same frequency channel is described and simulated. Finally some basic countermeasures are presented.

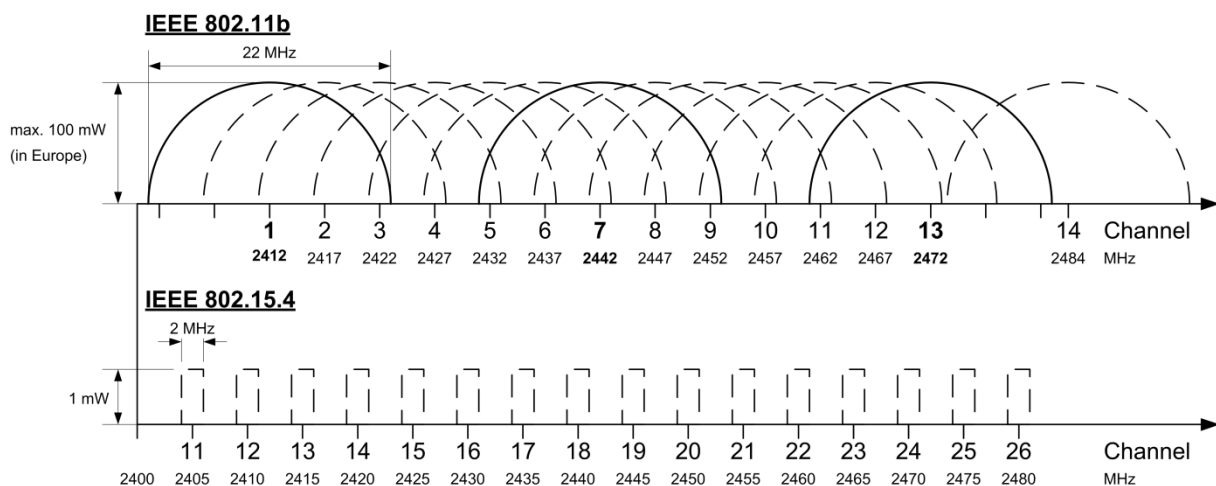
## 2. Wireless Transmitting Technologies on the 2.4 GHz band

The IEEE 802.15.4 standard is designed for low-rate Wireless Personal Area Networks (LR-WPANs) [1]. Contrary to its name this standard is not only used for small single-hop Personal Area Networks, but also for multi-hop sensor networks. Many standards, like ZigBee [2], WirelessHART [3] or 6LoWPAN [4] are based on 802.15.4 on the lower layers. 802.15.4 specifies two layers according to the Open Systems Interconnection (OSI) model: the Physical and the Medium Access Control sub-layer of the Data Link Layer.

### 2.1. Physical Layer

The Physical Layer of IEEE 802.15.4 supports 27 channels in the three unlicensed Industrial, Scientific and Medical (ISM) frequency bands. The 2.4 GHz band, being the highest frequency band, offers some advantages: it provides the highest data rate and is useable worldwide. Since this band is also used by other applications, the transmitting units are also cheap. At the moment the usage of the 2.4 GHz band seems to be the most common choice for WSNs.

But the 2.4 GHz band has some clear disadvantages: the waves are not very penetrating at these high frequencies and there are lots of other technologies using this band. The most common applications sharing these frequencies are microwave ovens, wireless DECT phones, baby phones and other proprietary wireless devices, as well as harmonics of monitors, Bluetooth devices and Wireless Local Area Networks (W-LAN). A very good overview of possible interference sources and their effects is provided by the technical report of the Jennic Corporation [5]. The following will focus on W-LANs, especially IEEE802.11b, since they are, as shown in the technical report, far more interfering than Bluetooth, which uses Frequency Hopping. Boano et al. [6] analyse the stability of MAC-Layers, namely NULLMAC, X-MAC [7], Low-Power Probing [8], Low-Power Listening and CoReDac [9], against interference in general. They also optimise X-MAC to stand interference better and present a new, more robust, version of X-MAC.



**Figure 1.** Comparison of the usage of the 2.4 GHz band by IEEE 802.11b and IEEE 802.15.4. Do not scale spectral mask or output power from this drawing. Bold channels are non-overlapping channels (recommended to be used in Europe).

Figure 1 gives an impression of the crowd in the frequency band, which is caused by W-LANs operating according to the IEEE 802.11b standard. The IEEE 802.11b channels are 22 MHz wide and their Channel Centre Frequencies are 5 MHz away from each other, so that they overlap each other. In comparison to the later, the channels of the IEEE 802.15.4 standard are shown. They do not overlap, because they are also spread by 5 MHz, but they are just 2 MHz wide.

A common recommendation in Europe is to use channel 1, 7 and 13 for W-LAN routers in order to avoid interference with other W-LANs. Thus, the IEEE 802.15.4 channels 15, 16, 21 and 22 are not interfered with W-LANs. In the United States, the W-LAN channel recommendation is to use channel 1, 6 and 11, so that the IEEE 802.15.4 channels 15, 20, 25 and 26 would be most suitable for WSNs in this location.

Gnawali et al. [10] show the effect of an interfering W-LAN on the Tutornet testbed used for the evaluation of the Collection Tree Protocol.

It is very likely that in the near future, the frequency bands will be even more used. For WSN deployments, the chosen frequency channel will become more and more important. Since W-LANs

are sending quite continuously, they are easy to detect or the used channels may even be known to the creator of a WSN. Because of the size and the ad hoc nature of a WSN, it is not always possible to check the full area for interference. Especially side effects of other WSNs may not be detected in a quick pre-deployment channel test, because WSNs send with very low output energy and sometimes very rarely. The idea of a self-managing or at least out-of-the-box pre-configured network is crucial for the success of WSNs, so that complex pre-deployment checks are not suitable for most applications. More applications, e.g. Smart Meters for the Smart Grid, will be deployed in near future as off-the-shelf hardware probably having a fixed preselected channel.

With an increasing density of WSNs a new problem can occur: two separate WSNs working on only one 802.15.4 channel. This problem may also occur when the WSN developer uses the default options for his platform or if he ships a preconfigured product for end-users.

### *2.2. Medium Access Control sub-layer*

The Medium Access Control sub-layer of the Data Link Layer joins above the frequency band described in the previous section. As described in the last section there is the chance of two or more networks operating on one channel, and thereby the Medium Access Control of two or more different WSNs will compete to use the channel. There are plenty of MAC protocols for different types of networks and applications. A good overview of MAC protocols for Wireless Sensor Networks is provided by Demirkol et al. [11].

*2.2.1. Common design goals of Medium Access Control protocols.* The most important goal in WSNs is to save energy, since energy is the most restricted resource and if a node runs out of energy it is no longer part of the network. Therefore, it does not only stop sampling, but it also cannot forward messages anymore in a multi-hop network. The main reasons causing energy waste on the MAC layer are Collisions, Idle Listening, Control Packet Overhead and Overhearing as stated by Roy and Sarma [12]. They present a good summary of different MAC protocols and its energy consumptions.

Competition was not taken into account when most of the MAC protocols were designed [11], [12]. The authors review this view under the critical perspective that WSNs will be deployed in huge amounts and as argued earlier the likelihood of competition in WSNs will increase.

## **3. Simulation**

The simulation was designed to investigate the effect of different MAC protocols operating on the same channel as it could happen on the edge of two WSNs. There are plenty of different protocols published. This work studies the behaviour of two asynchronous MAC protocols. These protocols are similar in structure, and the protocols can be tested with equal parameters. Since X-MAC and LPP are implemented in Contiki OS, these versions were used for the experiment.

### *3.1. X-MAC*

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

Non-sending nodes wake up after a sleep time for a short listening period to monitor the channel for strokes. Due to this behaviour, the idle listening time is reduced [7].

### *3.2. Low-Power Probing*

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 note that it wants to send to. When receiving it, the message is sent [8].

### 3.3. Network configuration

X-MAC and LPP were used with their default parameters. The channel is checked by both protocols at a rate of 4 Hz.

X-MAC is parameterised by *on-time*, *off-time*, *strobe-time* and *strobe-wait-time*. These specify how long the receiver listens, how long the radio is turned off, the maximum duration of sending strobes if no acknowledgment is returned and the duration of checking for other strobes to receive messages.

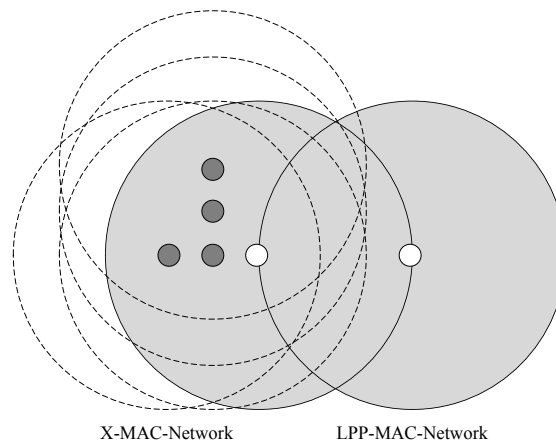
LPP has two parameters to control the duty cycling: *listen-time* and *off-time*. Listen-time states the duration of listening for a probe and off-time is the time duration between two listen periods.

The default Contiki parameters create a roughly comparable energy consumption for X-MAC and LPP.

### 3.4. Network configuration

Up to five senders report to one base station, all using X-MAC. Each sender sends a short message including a time stamp and counter. This packet can be seen as representative for a measured value and the measurement time. The sender address is added by the lower layer, thus it has not been included on the application layer. Each sender sends a packet every five seconds and this occurs 100 times. In order to test the effect of a different WSN network operating nearby, a second network of two nodes trying to transmit via the LPP protocol every second was simulated also. There was one LPP node in range for interference. Figure 2 shows the simulated scenario. By using the COOJA simulator, it is possible to time the nodes very precisely. So all nodes boot up at the same time, but their sending times were offset by one second each. Hence, there was no interference between nodes of the X-MAC network.

The experiment was executed from two up to six X-MAC senders. Each configuration was simulated without interference and with interference by the second network.



**Figure 2.** Simulated scenario of an X-MAC WSN interfered by a LPP WSN.

### 3.5. Results

The results of the simulations have been analysed for two basic features, namely the amount of successfully delivered data packets on the application layer and the estimated energy consumption of the sending nodes. Table 2 shows the number of packets arriving on the application layer. This reveals that the most significant effect on the WSNs is lost packets. In many applications, e.g. industry

automation and health care, this problem has to be addressed, since reliable transmission is crucial. Table 2 also reveals that the network configurations with two and three sending nodes are heavily affected. This is due to the fact that the sending intervals are static, thus a bad timing of the two networks (where the timing is similar) can lead to a worst case scenario, in which almost every transmission is blocked. The sending window is in the region of milliseconds, so that these effects can be difficult to investigate in real deployments. In the X-MAC-layer protocol, the errors on sending nodes were logged. These logs can only help to estimate the delivery rate, since not all errors are logged and so the logs are not accurate enough to guarantee delivery.

**Table 2.** Delivered packets and errors logged by the X-MAC protocol on sending nodes.

<b>Number of sending nodes</b>	<b>Received packets interfered / non-interfered</b>	<b>Logged errors on sending nodes interfered / non-interfered</b>
1	99/100	- / -
2	56/200	10 sending drops / -
3	159/300	144 cyclic redundancy check (CRC) errors / -
4	400/400	- / -
5	500/500	- / -

To compare the energy consumption of the simulated networks, the Contiki-included module on-time counters have been used. The energy is calculated by multiplying the on-times by consumption factors given in Equation 1.

$$\frac{\text{estimated electric current [mA]} = \text{listen} \times 20[\text{mA}] + \text{transmit} \times 17.7[\text{mA}] + \text{cpu} \times 1.8 [\text{mA}] + \text{lpm} \times 0.545[\text{mA}]}{\text{cpu} + \text{lpm}} \quad (1)$$

The parameter *listen* is the time the radio is in receive mode, *transmit* the time in transmit mode, *cpu* the time the microprocessor has been running and *lpm* the time the microcontroller has been in low power mode. These factors are based on the shell power application included in Contiki. The online energy estimator of Contiki is described by Dunkels et al. [13].

The total energy consumption is not significantly affected by the interference, since no resending was established. The transmission was cancelled often after the sending of the strobos, thus the energy consumption for an aborted sending is quite small. It has to be taken into account that no resending on a higher layer was implemented to understand that the energy consumption has not increased in total. By calculating the energy rate per packet the isolated WSNs achieve values of about 0.03 mA per successfully sent packet. In contrast, the inferred two X-MAC sender network increased to 0.11 mA per successfully sent packet.

#### 4. Conclusion

This work has shown the danger of having two or more WSNs or parts of them operating on a single communication channel. Though by duty cycling the usage of the medium is quite rare, the chances of side-effects exist and have been described here. The interference of different MAC-layer protocols has not been tested to date. The following can be considered as possible solutions to avoid interference:

- Channel Hopping/Spread Spectrum: The frequency channel is changed permanently. This provides relief against single channel interference and increases the protection from eavesdropping. The disadvantage is the additional complexity and the need to keep the nodes

synchronous, which can become difficult in big multi-hop or ad hoc networks. Bluetooth is using this technology.

- Random sample/sending intervals: This is a simple method to limit the danger of sending synchronously with another node of the same or of another network.
- Channel pre-deployment check: If the deployment area can be tested, measurements helping to find interference sources and jamming signals can help to design a good working, efficient and reliable WSN.
- Low power sending: Messages should be sent with just the power needed to reach the next hop. This helps to save energy, because multi-hopping consumes less energy than directly transmitting to a more distant node and is less interfering.

Since the amount of deployed WSNs will surely increase in the next few years, interference and cooperation of different systems will become an active research area. This work has shown a particular case and further research is needed. Interference models are not only needed on the Physical layer, but also on the MAC layer.

### 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] Institute of Electrical and Electronics Engineers 2003 *Standard 802.15.4-2003*
- [2] ZigBee Alliance [www.zigbee.org](http://www.zigbee.org) (accessed March 2011)
- [3] Gerrit Lohmann 2010 *Wireless Introduction* (HART Communication Foundation)
- [4] IPv6.com - the source for ipv6 information, training, consulting & hardware [ipv6.com/articles/sensors/IPv6-Sensor-Networks.htm](http://ipv6.com/articles/sensors/IPv6-Sensor-Networks.htm) (accessed March 2011)
- [5] Jennic - Technology for a changing world 2008 *Co-existence of IEEE 802.15.4 at 2.4 GHz*
- [6] Boano C A, Voigt T, Tsiftes N, Mottola L, Römer K and Zuniga M A 2010 Making Sensor MAC Protocols Robust Against Interference *7th European Conference on Wireless Sensor Networks* (Coimbra)
- [7] Buettner M, Yee G, Anderson E and Han R 2006 X-MAC: a short preamble MAC protocol for duty-cycled wireless sensor networks *Proceedings of the 4th international conference on Embedded networked sensor systems* (New York) pp 307-320
- [8] Musaloiu-E. R, Liang, C-J M and Terzis A 2008 Koala: Ultra-Low Power Data Retrieval in Wireless Sensor Networks *Proceedings of the 7th international conference on Information processing in sensor networks* (IEEE Computer Society) pp 421-432
- [9] Voigt, T and Österlind, F 2008 CoReDac: Collision-free command-response data collection *13th IEEE Conference on Emerging Technologies and Factory Automation* (Hamburg)
- [10] Gnawali O, Fonseca R, Jamieson K, Moss D and Levis P 2009 Collection tree protocol *Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems* (ACM) pp 1-14
- [11] Demirkol I, Ersoy C and Alagoz F 2006 MAC protocols for wireless sensor networks: a survey *Communications Magazine* vol 44 (IEEE) pp 115-121
- [12] Roy A and Sarma N 2010 Energy Saving in MAC Layer of Wireless Sensor Networks: a Survey *National Workshop in Design and Analysis of Algorithm*
- [13] Dunkels A, Österlind F, Tsiftes N and He Z 2007 Software-based On-line Energy Estimation for Sensor Nodes *Proceedings of the Fourth Workshop on Embedded Networked Sensors* (Cork)