COEXISTENCE OF DIFFERENT WIRELESS SENSOR NETWORKS

MAC Protocol Interference between X-MAC and Low Power Probing

Sven Zacharias, Thomas Newe, Sinead O'Keeffe and Elfed Lewis
Electronic and Computer Engineering, University of Limerick, Limerick, Ireland

Keywords: Wireless Sensor Network, WSN, Medium Access Control, MAC, Coexistence, Channel Interference, Competition, Interoperability.

Abstract: Wireless Sensor Networks (WSNs) are an emerging technology that will be widely deployed in the near future. Most WSNs operate on the 2.4 GHz band of the three free ISM frequency bands. The 2.4 GHz frequency band is already used by different wireless systems. With an increasing number of WSNs, the scenario of different WSNs operating on the same IEEE 802.15.4 frequency channel becomes more likely. WSN Medium Access Control (MAC) Protocols used today were not designed with this problem in mind. To date, the research focused on interference on the Physical Layer. This work analyses the jamming potential and the robustness of MAC Protocols, namely X-MAC and Low Power Probing (LPP), at the level of inter-network competition for medium access, when multiple WSNs are in range of each other operating on the same channel. The following parameters have been investigated and their effect on interference is shown: sampling time, channel check rate and payload.

1 INTRODUCTION

A Wireless Sensor Networks (WSNs) consists of many, theoretically up to thousands of sensor nodes. A single sensor node, called a mote, is a small and inexpensive device that is built from the following main parts: one or more sensors, a data processing unit, a wireless communication interface, and an energy source. Today's most suitable wireless transfer technologies for WSNs are based on the Institute of Electrical and Electronics Engineers (IEEE) 802.15.4 standard (IEEE, 2003), since it provides a simple, low-power stack for the Physical and Data Link Layers.

2 PHYSICAL LAYER

The IEEE 802.15.4 standard can physically operate on the three free Industrial, Scientific and Medical (ISM) frequency bands offering 27 channels: one at 868 MHz, ten in the 915 MHz band and 16 in the 2.4 GHz band. The only frequency band available worldwide is at 2.4 GHz, which is the most used ISM band utilised by many technologies and therefore the band is crowded (Zhou et al., 2006).

Possible sources of interference in the 2.4 GHz band can be the common microwave oven and harmonics of monitors. However, as revealed by a technical report of the Jennic Cooperation (Jennic, 2008) investigating the effects of different

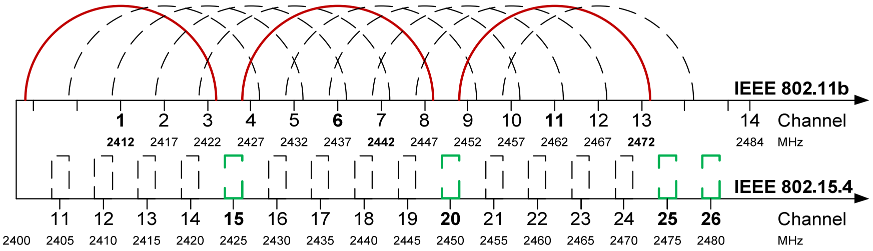
IEEE 802.11b
1 2 3 4 5 6 7 8 9 10 11 12 13 14 Channel
2412 2417 2422 2427 2432 2437 2442 2447 2452 2457 2462 2467 2472 2484 MHz
IEEE 802.15.4
11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 Channel
2400 2405 2410 2415 2420 2425 2430 2435 2440 2445 2450 2455 2460 2465 2470 2475 2480 MHz

Figure 1: Channels in the ISM 2.4 GHz base band used by IEEE 802.11b and IEEE 802.15.4. Bold channels are non-overlapping channels that are normally used. Do not scale spectral mask or output power from this drawing.

Zacharias S., Newe T., O'Keeffe S. and Lewis E..
COEXISTENCE OF DIFFERENT WIRELESS SENSOR NETWORKS - MAC Protocol Interference between X-MAC and Low Power Probing.
DOI: 10.5220/0003829601970202
In *Proceedings of the 1st International Conference on Sensor Networks* (SENSORNETS-2012), pages 197-202
ISBN: 978-989-8565-01-3

interference sources, Wireless Local Area Networks (WLANs) are the main source of interference. The interference of WLANs based on the IEEE 802.11b (IEEE, 2007) and the newer IEEE 802.11n (IEEE, 2009) standard on IEEE 802.15.4 have been studied in detail (Yang et al., 2011); (Petrova et al., 2007); (Bello and Toscano, 2009).

In order to minimise the risk of interference on WSNs, a WSN channel outside the band of the used WLAN channels is normally chosen, as shown for IEEE 802.11b in Figure 1. But Petrova et al. (2007) report that even outside of the used WLAN channels, IEEE 802.11n interferes with WSNs.

Due to WLANs and other external factors, the choice of non-interfered WSN channels is often limited to four or less. The default, pre-set channel in TinyOS and ContikiOS is 26. Hence it is likely that many WSNs operate on channel 26.

Trends like the Internet of Things and Machine to Machine communication will lead to many embedded wireless networks in the near future. So it becomes more and more likely that there will be a scenario of two WSNs operating on the same IEEE 802.15.4 channel and thus using the same Physical Layer (maybe even the same radio chip), but probably a different Data Link Layer.

3 MEDIUM ACCESS CONTROL (MAC) SUB-LAYER

Since a network consists of many participants, but the radio channel can only be used by a single participant at any time, the task of the MAC Sub-Layer is to avoid two or more nodes trying to transmit at the same time (packet collisions).

In classical networks, all transfer modules are always turned on due to the fact that energy is not constrained, thus the communication medium can be monitored at all times. This behaviour leads to the simplest form of MAC Protocol, called Carrier Sense Multiple Access (CSMA). The potential sender listens in order to determine if the channel is used by another device for transmitting. This check is called Clear Channel Assessment (CCA). If the channel is idle, the sender transmits its own message. If the channel is used, the potential sender performs a backoff algorithm, which means it waits for a random time and retries. An extension of this behaviour often used in WLANs is Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) with handshake. This handshake uses Request To Send (RTS) and Clear To Send (CTS) messages before each data transfer. It adds additional overhead but takes into account that the receiving node can be blocked by a device outside of the sender's communication range (Hidden Terminal Problem).

ContikiOS, which is the operating system used for the following experiments, includes two network stacks: uIP and Rime (Dunkels et al., 2007). uIP is a small TCP/IP stack and Rime is a lightweight communication stack designed for low power radios used in WSNs. This work uses the Rime stack. WSN MAC Protocols have to save energy, which is realised by turning the radio unit off most of the time. The channel check rate determines how often the radio is switched on. In ContikiOS, the term Radio Duty Cycling (RDC) Layer is used for the lower part of the MAC Layer that manages the sleep times of the radio. The MAC Layer Protocol in ContikiOS can provide retransmissions (CSMA) when the RDC Layer indicates a collision.

3.1 Radio Duty Cycling (RDC)

A huge number of RDC/MAC Protocols have been published. Summaries and comparisons of the most commonly used ones can be found in the literature (Demirkol et al., 2006); (Kredo II and Mohapatra, 2007); (Roy and Sarma, 2010). A possible taxonomy for MAC Protocols is:

- Unscheduled
  - Push, Sender-initiated, e.g. Low Power Listening (LPL), X-MAC
  - Pull, Receiver-initiated, e.g. Low Power Probing (LPP)
- Scheduled
  - Time Division Multiple Access (TDMA)

Scheduled approaches have many advantages, but they are mainly optimised for high traffic and therefore adapt poorly to network changes and need synchronisation (Cionca et al., 2008). Hence, unscheduled protocols are used for dynamic WSNs. In the following, the two unscheduled approaches Push and Pull are studied in further detail by means of X-MAC and LPP. Like most protocols, they have been designed for stand-alone usage, so that both coexistence with other protocols and competition for the medium have not been considered yet.

3.1.1 X-MAC

X-MAC (Buettner et al., 2006) is a pushing protocol based on the Low Power Listening (LPL) approach (Moss et al., 2007), where 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, called strobes, until it receives an acknowledgement;

then the message is sent. Non-sending nodes wake up for a short listening period after the sleep time in order to monitor the channel for strobes. Due to this behaviour, the idle listening time is reduced.

3.1.2 Low Power Probing

Low-Power Probing (LPP) (Musaloiu-E. et al., 2008) can be roughly described as the inverse approach to X-MAC. Instead of the sender initiating the communication, the receiver is announcing its ability to receive messages, basically pulling messages. In LPP, all nodes are duty cycled and wake up for just a short time. If a node is awake, it sends a small packet, called probe, to signal that it is awake and then it listens for a short time for replies. A sending node turns its radio on and listens for the probe of the communication partner.

Additionally, LPP simplifies routing. The data is pulled hop by hop to the base station instead of pushed for which the sender needs to know an address of a node closer to the base station.

Figure 2 shows the principle of both approaches.

3.2 Competition between MAC Protocols

The interference between different WSNs has been studied only recently: Bello and Toscano (2009) show the interference of WSNs operating on adjacent channels. Bertocco et al. (2008) investigate interference of two WSNs. They evaluate a ZigBee WSN interfered by Bluetooth, WLAN and another ZigBee WSN on the same channel and show how CSMA/CA affects the Packet Error Rate (PER). Boano et al. (2010) investigate the factors influencing the robustness against interference of WSNs and use a "Semi-Periodic Interferer" to simulate a WSN on the same channel. Finally, they present an enhanced, more robust version of X-MAC. The security aspect of an intended jamming of a WSN has also been studied in detail (Xu et al., 2005).

4 EXPERIMENTAL SETUP

All experiments are conducted using TelosB sensor nodes (MEMSIC, 2010) in a normal office environment, thus the environment is full of WLAN signals, laptop/desktop computers and other electronic and metallic equipment. Channel 26 is chosen, since this channel is less interfered with by WLANs, as previously mentioned. To be sure that missed packets are not due to external interference, interfered and non-interfered trials are done in alternating order. Also the received signal strength indicator (RSSI) is logged for every packet to ensure a good connection. Additionally, to rule out external factors and gain better insight into the causes for the results, all experiments have been simulated in Cooja. The "Unit Disk Graph Medium" and a random start up time of maximal 3 s (which is comparable to the start of nodes by hand) have been used. Due to the limited space and the fact that the simulation corresponds to the experiments, only the experimental results are presented here.

The software for the experiments is written in ContikiOS version 2.4. X-MAC is used in two versions, with and without CSMA. CSMA supports a four packet big buffer and tries a single retransmission. LPP provides a packet buffer size of four packets. In the following setup, the observed network will be called *collector* and the interfering network will be called *jammer*.

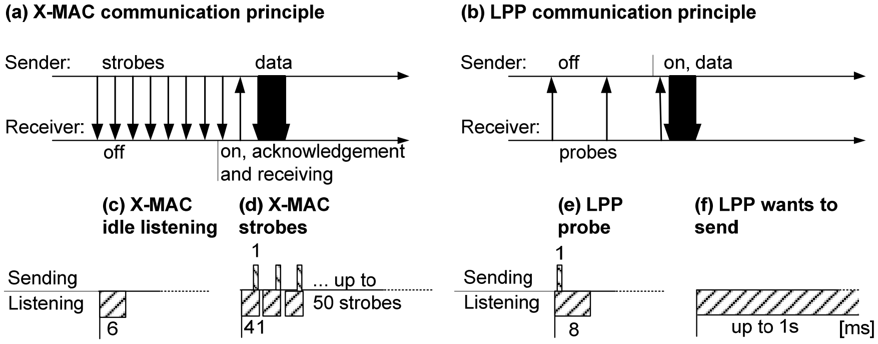

Figure 2: (a) In X-MAC, the sender actively tries to establish the communication by sending strobes. (b) In LPP, the receiver is pulling data with the help of probes. (c-f) The standard timing of X-MAC and LPP with a channel check rate of 4 Hz: (c) X-MAC listens for 6 ms at the beginning of each cycle and then sleeps for 244 ms. (d) If X-MAC wants to transmit, it sends strobes until it receives an acknowledgement or reaches 50 reiterations. (e) LPP sends a probe every 250 ms waits for incoming data and then sleeps. (f) A potential sender wakes up and listens for an incoming probe for a maximum of 1s.

The senders of the collector network send a unicast message to the base station every five seconds, 100 messages in total. The packet has a payload of 4 bytes consisting of an unsigned integer counter and a timestamp. Additionally, data from lower layers are added, and thus the packet has a total size of 36 bytes for X-MAC and 21 bytes for LPP. This is considerably less than the 127 bytes allowed for a single IEEE 802.15.4 data frame, hence every message is sent in a single frame. The message is only slightly longer than an X-MAC strobe of 28 bytes or a LPP probe of 13 bytes. This overhead is realistic for a simple temperature measurement system for example. The default values were used for the on- and off-times of the radios, the number of retries and all other parameters. Thus, both protocols have comparable energy consumptions while being idle. The channel is checked at a rate of 4 Hz, thus cycles of 250 ms occur, the resulting standard timing is illustrated in Figure 2 (c-f).

The nodes were placed close (< 20 cm) to the base station on a desk, in direct line of sight and thus the distance or orientation of the nodes is not affecting the transfer. The collector network builds a single-hop star topology and the jammer network consists of a sender and a base station. All nodes are in communication range of each other.

The base stations in these experiments are duty cycled as well, since they would just be a hop closer to the real base station in a multi-hop network. They do not send data messages. All nodes are started manually, thus the start times vary slightly. Every trial is conducted ten times in order to provide a reliable data set.

4.1 Network Scalability

The scalability of a non-interfered collector network is tested in order to provide a comparison between high traffic and interference.

Table 1: Packet Error Rates (PERs) [%] of the scalability experiment.

		Scalability (sender)	
		3	5
X-MAC	mean	3.93	50.58
	median	0.67	49.30
	stdev	10.14	5.52
X-MAC/ CSMA	mean	3.47	15.44
	median	0.17	17.00
	stdev	5.36	5.90
LPP	mean	8.20	11.38
	median	0.17	7.70
	stdev	16.46	12.20

The resulting mean, median and standard deviation of the PERs over ten repeats for this experiment are shown in Table 1. Even with only three sending nodes, some packets are lost due to collisions. The PERs of all protocols increase due to the traffic of two additional senders. The lost packets almost always belong to a single node. If a deadlock between nodes occurs due to bad timing then it stays unresolved until the end of the experiment due to the fixed duty cycling. This results in a constant, high packet loss for a single node.

4.2 Interference Experiments

For all of the following interference experiments, this work uses a collector network (consisting of a base station and three sending nodes) and a jammer network (consisting of a sender and a base station).

Experiment 1) Scalability versus Interference: This experiment compares the effects of having two additional senders in a network (Table 1) with two interfering nodes using a different protocol. X-MAC and X-MAC/CSMA are interfered by LPP and LPP is interfered by X-MAC. The parameters used (sampling time, channel check rate and payload) are exactly the same for the collector and jammer network. The effect of the interference, shown in Table 2, is an increased PER that is lower than the PER of the scaled up networks for X-MAC and LPP and roughly the same for X-MAC/CSMA. The X-MAC collector network is losing almost all packets or packets at regular intervals from a sender. LPP is almost unaffected.

Experiment 2) Decreased Sampling Time: To increase the effect of interference the number of sent packets on the jammer network is raised by setting the sampling interval to 1 s. The packets contain the same payload as the packets of the collector network. Both networks use the same channel check rate. As shown in Table 2, this only leads to an increased PER for X-MAC.

Experiment 3) Decreased Channel Check Rate: To investigate the effect of the channel check rate, the sampling rate is set to 2 Hz for the jammer network. This results in fewer data transfer contacts, but increases the number of strobes/probes needed to synchronise (the channel is checked twice in a second and each second, a packet is sent). The PER is not changing considerably (see Table 2), which is due to the fact that the actual message is similar in length compared to the strobes/probes.

Experiment 4) Increased Payload: The payload sent by the jammer network is enlarged to see the effect of increased packet length. A longer packet results in a longer continuous blocking of the channel. The payload is increased to 42 bytes. The X-MAC and X-MAC/CSMA collector is interfered by LPP with a 59 byte packet and LPP by X-MAC with a 74 byte packet. The effect on the PER does not considerably differ from Experiment 2, only X-MAC/CSMA shows a higher PER, as shown in Table 2. This shows that the payload and thereby the packet length has a small effect due to the overhead of the strobes and probes. X-MAC can send up to a maximum of 50 strobes to establish the data exchange. LPP always sends a probe at each duty cycle. Compared to these strobes/probes, the data packet length is almost negligible.

Experiment 5) Pobes versus Data Packets: To show that the overhead traffic generated by probes is more relevant than the data packets, the sampling time is set up to 25 s. Despite the sampling time change, LPP still generates the same amount of probes. The resulting PER, shown in Table 2, is still as high as in Experiment 2 and Experiment 4 while the sent application data decreased by the factor of five. This shows that the overhead is more important than the actual data sent.

Experiment 6) LPP jammed by X-MAC/CSMA: In all the experiments described so far, LPP is jammed by X-MAC without CSMA. In this experiment, LPP is jammed by X-MAC/CSMA. The retransmissions caused by CSMA generate additional traffic on this jammer network. As shown in Table 2, this additional traffic slightly increases the PER.

4.3 Discussion

The PER is not equally distributed among the repetitions of the experiments. In the results of the single trials three different cases can be identified: full loss of all 100 packets of a single sender, packets loss occurring in regular intervals, or no packet loss. These patterns match with patterns shown in Cooja simulations, so it can be asserted that the packet errors are not caused by external interference. Since theses packet losses are due to collisions between the jammer and collector network, timing is a vital key factor.

For X-MAC and X-MAC/CSMA, the interference has roughly the same effect as the increased traffic of more communication partners using the same MAC Protocol.

LPP seems not to be affected by the jammers. This result matches with Boano et al. (2010), since the latter shows that a “Packet Queue with Fast Drain” helps to avoid interference. LPP is using a similar concept by default, since it has an included buffer, which is transmitted in a row when the handshake succeeds. But LPP seems to fail in scaling to more nodes and jams other WSNs with its permanent probing. Since the major traffic is generated by the overhead in the network, the actual data sent has a small effect on the PERs.

5 CONCLUSIONS

To date, robustness against interference with other technologies has been widely investigated, but the interference between WSNs operating on the same channel has not been focused on to date. In WSN MAC Protocol design, the assumption of an isolated WSN is still dominant. This work gives a first attempt to direct attention to the problem of inter-WSN interference.

The parameters: sampling time, channel check rate and payload of the jamming network have been experimentally investigated. For the setup being used, their effects on the PER are surprisingly small, since most of the traffic is overhead. The results show that the packet errors caused by a second network using a different protocol are roughly the same size as the packet errors caused by traffic of additional nodes on the same network.

In this work, only the parameters of the

Table 2: Packet Error Rates (PERs) [%] of the interference experiments.

		Jammer network (sampling interval, channel check rate)					
		5 s, 4 Hz	1 s, 4 Hz	1 s, 2 Hz	1 s, 4 Hz, payload	25 s, 4 Hz, probes	1 s, 4 Hz CSMA
Experiment number		1	2	3	4	5	6
X-MAC	mean	38.77	53.10	40.23	50.67	50.13	-
	median	36.83	47.33	45.67	44.00	53.67	-
	stdev	20.55	26.47	14.30	26.09	16.03	
X-MAC/ CSMA	mean	18.10	19.17	17.13	28.80	21.37	-
	median	15.17	15.00	10.83	20.83	22.33	-
	stdev	15.26	16.99	15.36	23.74	7.70	
LPP	mean	0.17	0.23	6.63	4.50	-	5.87
	median	0.17	0.17	0.00	0.33	-	0.33
	stdev	0.17	0.26	19.46	12.83	-	16.39

interfering network have been changed. Valuable insight into the problem could be provided in future studies by investigating the parameters of the collector network and their effect on its vulnerability to interference. A larger setup including multi-hopping would exacerbate the interference problem. The conduction of the experiments in a shielded environment would exclude external interference and thereby deliver less noisy measurements.

A modification of the MAC Protocol duty cycling supporting variable timings could avoid the deadlock. The authors believe that the problem of inter-WSN interference will gain more research interest in the near future.

ACKNOWLEDGEMENTS

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. Thanks to the anonymous reviewers for their valuable comments and suggestions.

REFERENCES

Bello, L. L. and Toscano, E., 2009. Coexistence issues of multiple co-located IEEE 802.15.4/zigbee networks running on adjacent radio channels in industrial environments. *Industrial Informatics, IEEE Transactions on*, 5(2):157 –167.

Bertocco, M., Gamba, G., and Sona, A., 2008. Is CSMA/CA really efficient against interference in a wireless control system? An experimental answer. In *Emerging Technologies and Factory Automation, 2008. ETFA 2008. IEEE International Conference on*, pages 885–892. IEEE.

Boano, C. A., Voigt, T., Tsiftes, N., Mottola, L., Römer, K., and Zuniga, M. A., 2010. Making sensornet mac protocols robust against interference. In *7th European Conference on Wireless Sensor Networks*, Coimbra, Portugal.

Buettner, M., Yee, G., Anderson, E., and Han, R., 2006. X-MAC: A short preamble MAC protocol for duty-cycled wireless sensor networks. In *Proceedings of the 4th International Conference on Embedded Networked Sensor Systems,* Boulder, Colorado, USA, pages 307–320.

Cionca, V., Newe, T., and Dadarlat, V., 2008. TDMA protocol requirements for wireless sensor networks. In *Sensor Technologies and Applications, 2008. SENSORCOMM '08. Second International Conference on*, pages 30 –35.

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

Dunkels, A., Österlind, F., and He, Z., 2007. An adaptive communication architecture for wireless sensor networks. In *Proceedings of the Fifth ACM Conference on Networked Embedded Sensor Systems (SenSys 2007)*, Sydney, Australia

Kredo II, K. and Mohapatra, P., 2007. Medium access control in wireless sensor networks. *Computer Networks*, 51(4):961–994.

IEEE Computer Society. 2003. *IEEE Standard 802.15.4™-2003 - Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)*

IEEE Computer Society. 2007. *IEEE Standard 802.11™-2007 - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*

IEEE Computer Society. 2009. *IEEE Standard 802.11n™-2009 – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 5: Enhancements for Higher Throughput*

Jennic Cooperation, 2008. Co-existence of IEEE 802.15.4 at 2.4 ghz. Application Note, Revision 1.0.

MEMSIC Inc., 2010. *TelosB Mote Platform Datassheet.*

Moss, D., Hui, J., and Klues, K., 2007. Tep 105-low power listening. http://www.tinyos.net/tinyos-2.x/doc/pdf/tep105.pdf - Retrieved Sept. 2011.

Musaloiu-E., R., Liang, C.-J. M., and Terzis, A., 2008. Koala: Ultra-low power data retrieval in wireless sensor networks. In *Proceedings of the 7th International Conference on Information Processing in Sensor Networks*, IPSN '08, pages 421–432, Washington, DC, USA. IEEE Computer Society.

Petrova, M., Wu, L., Mahonen, P. and Riihijärvi, J., 2007. Interference measurements on performance degradation between colocated IEEE 802.11 g/n and IEEE 802.15.4 networks. In *Networking, 2007. ICN'07. Sixth International Conference on*, pages 93–93. IEEE.

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

Xu, W., Trappe, W., Zhang, Y., and Wood, T., 2005. The feasibility of launching and detecting jamming attacks in wireless networks. In *Proceedings of the 6th ACM International Symposium on Mobile ad hoc Networking and Computing*, MobiHoc '05, pages 46–57, New York, NY, USA. ACM.

Yang, D., Xu, Y., and Gidlund, M., 2011. Wireless coexistence between IEEE 802.11- and IEEE 802.15.4-based networks: A survey. *International Journal of Distributed Sensor Networks*, Article ID 912152:17.

Zhou, G., Stankovic, J. A., and Son, S. H., 2006. Crowded spectrum in wireless sensor networks. In *Proceedings of Third Workshop on Embedded Networked Sensors (EmNets)*.