Demo Abstract: Generation of Controllable Radio Interference for Protocol Testing in Wireless Sensor Networks

Carlo Alberto Boano and Kay Römer
Universität zu Lübeck
Lübeck, Germany
{cboano, roemer}@iti.uni-luebeck.de

Zhitao He and Thiemo Voigt
Swedish Institute of Computer Science
Kista, Sweden
{zhitao, thiemo}@sics.se

Marco Antonio Zúñiga
Digital Enterprise Research Institute
National University of Ireland, Galway
marco.zuniga@deri.org

Andreas Willig
Technische Universität Berlin
Berlin, Germany
awillig@tkn.tu-berlin.de

Abstract

Radio interference plays a central role for the performance of Wireless Sensor Networks (WSN). Interference not only leads to packet loss, but it also affects the function of MAC and routing protocols. Hitherto, testing the impact of interference on WSN experimentally has been difficult because of the unavailability of low-cost tools to create reproducible and well-controlled interference patterns.

In this demo we present a simple and inexpensive method to generate controllable and repeatable interference patterns for 802.15.4 devices. The demo is presented as a game, where a user is required to achieve a given interference level.

Categories and Subject Descriptors

B.8.1 [**Performance and Reliability**]: Reliability, Testing, and Fault-Tolerance

General Terms

Experimentation, Performance, Reliability

Keywords

Radio Interference, Interference Generation, WSN

1 Introduction and Motivation

Radio interference strongly affects the reliability and robustness of WSN communications. In order to overcome these effects, researchers need to study the impact of the various patterns of interference on protocols. Unfortunately, the generation of controlled and reproducible interference on real nodes is not a simple task.

There are three main approaches to generate interference patterns in WSN, but they are either expensive, inaccurate, or complex. First, we have specialized hardware devices such as Software-Defined Radios (SDR) that can generate precise interference patterns, but are costly. A second group consists of commercial off-the-shelf radios such as Wi-Fi or Bluetooth transmitters that have problems limiting the interference to a particular 802.15.4 channel. Wi-Fi affects multiple adjacent channels, while Bluetooth is a sub-band interferer. With Bluetooth it is also difficult to control the precise timing of interference on the target channel. The third and most popular technique are packet-storms, where another IEEE 802.15.4 node broadcasts packets continuously at a predefined rate. Packet storms have high calibration costs and, again, it is not easy to exert tight control over the precise packet generation times, leading to periods without interference. Our experience with this method has shown that, even when carefully tuning packet length, transmission power, inter-packet time, and distance, it is very hard to create repeatable and precise interference patterns [1].

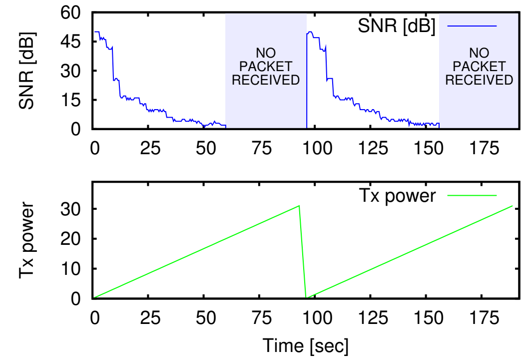

Figure 1. Generation of customized interference using the special test modes of the CC2420 radio chip. The figure shows how a progressive increment of the output power of the interfering carrier (bottom figure) reduces the SNR of an ongoing communication up to a point where packets are lost (top figure).

We propose a simple method to generate repeatable and precise patterns of interference that exploits the special test modes [1] of the Chipcon CC2420 radio chip. These modes allow sending a continuous carrier on a specific channel at precisely controllable instants, without any need to consider the timing behaviour of a MAC protocol. The carrier can be either unmodulated or modulated and the interference level is tuned only by varying the transmission power and the distance from the interferee(s). This mechanism permits not only the emulation of interference caused by packet transmissions [1], but also the generation of more specialized custom patterns, such as the one shown in Figure 1.

SenSys'09, November 4–6, 2009, Berkeley, CA, USA.
ACM 978-1-60558-748-6

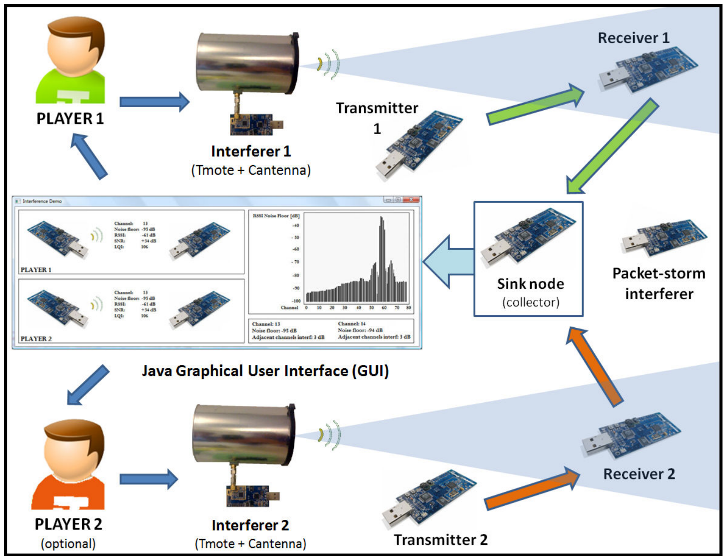

Figure 2. Architecture of Interference Game.

2 Demo Description

Testing of WSN protocols on real nodes requires the generation of precise patterns of interference, for example by controlling the SNR of ongoing communications or by creating temporary interruptions of connectivity. It is also often desirable to selectively affect only certain nodes. We illustrate these aspects by means of a simple engaging interactive game based on a direct interaction with the audience. The game consists in achieving a predefined SNR value between a pair of communicating nodes by means of generating interference from a simple sensor node. The interfering mote will be connected to a Cantenna [3] in order to control the direction of interference. All nodes run Contiki [2].

The user will tune the interference level by clicking the buttons available in the Tmote Sky platform: each click on the user button will increase the transmission power by one unit, while a click on the reset button will decrease it to zero. When the cantenna is pointed towards the receiving node, the SNR of the communication with the transmitter will start dropping as the transmission power of the interferer increases. Data about connectivity and SNR between sender and receiver is reported to a sink node attached to a laptop. The game can be either single or multi-player. In the multi-player case, two pairs of communicating nodes are used, and the user who achieves the predefined SNR first wins the game. Figure 2 depicts the system architecture.

The user(s) can monitor in real-time the SNR of the ongoing communications on a Graphical User Interface (GUI). The GUI will also show a software-based spectrum analyzer of the 2,4 GHz ISM band based on values scanned by the CC2420 radio on the sensor node. This will be very helpful to depict in real-time the generated interference in all channels, including the adjacent ones. The spectrum analyzer will also show the different shapes of interference that can be generated and the effects of additive interference in case both users point their cantennas towards the same node.

We will also show that the interference generated by the CC2420 test modes is compatible to the one that a packet-storm based interferer would produce. Moreover, we will show that by switching on and off the radio in special test modes we can mimick a time-slotted interference or even emulate the transmission of single packets.

3 Conclusions

In this demo we show that by using the carrier-only mode of the Chipcon CC2420 radio chip, we can generate repeatable and precise patterns of interference in a simple and inexpensive way. Since the generation of controllable interference with inexpensive equipment is a desirable tool to test WSN algorithms, we believe that the technique presented in this demo will facilitate the design of interference-resilient protocols. The mote-based spectrum analyzer will simplify the understanding and explanation of interference effects.

4 Acknowledgments

We would like to thank Pedro José Marrón, Jonas Meyer, Olga Saukh, and Robert Sauter for lending us the cantenna.

This work has been partially supported by the European Commission under the contracts No. FP7-2007-2-224053 (CONET, the Cooperating Objects Network of Excellence) and FP7-ICT-224282 (GINSENG). This research has been also partially financed by VINNOVA, the Swedish Agency for Innovation Systems, and by an IRCSET Postdoctoral fellow Grant PD200857, SFI Grant No. SFI08CEI1380. This work has been also partially supported by the Cluster of Excellence 306/1 "Inflammation at Interfaces" (Excellence Initiative, Germany, since 2006).

5 References

[1] C. Boano, Z. He, Y. Li, T. Voigt, M. Zuniga, and A. Willig. Controllable Radio Interference for Experimental and Testing Purposes in WSN. In *Proc. of SenseApp'09*, Zurich, Switzerland, October 2009.

[2] A. Dunkels, B. Grönvall, and T. Voigt. Contiki - a Lightweight and Flexible Operating System for Tiny Networked Sensors. In *Proc. of EmNetS'04*, Tampa, Florida, USA, November 2004.

[3] O. Saukh, R. Sauter, J. Meyer, and P. Marrón. Motefinder: A deployment tool for sensor networks. In *Proc. of REALWSN'08*, Glasgow, UK, April 2008.