Steganography in the 802.15.4 Physical Layer

Thomas Kho

CS 261 Project Proposal, 10/15/2007

Objective

The 802.15.4 protocol has a data rate of 250Kbps, modulated and spread to a chip rate of 2Mchip/s in the 2.4Ghz band. This suggests that up to 1.75Mbps of additional traffic can be repurposed for additional communication while maintaining communications fidelity with standards-compliant receivers. The objective of this project is to propose an information hiding system, analyze its properties, and implement such a system using programmable hardware.

Previous Work

Steganography is hiding information in noise, and techniques exist for a wide range of media: images, audio, plaintext, and network data, to name some. In networks, focus has been concentrated on the media access control layer and above.

Goals

A literature search has not yielded any previous work in steganography at the physical layer, where RF noise is natural and can be used to hide information. My interest in this project is to gain experience with network hardware, so my primary goal is for implementation, with theory and analysis secondary. Goals of this project include:

- Proposing a handful of steganographic systems (from basic to those that require application of some cryptography and information theory)
- Simulation of the digital components of the radio. Fig. 1 shows a block diagram of the pertinent components of a transmitter and receiver. In transmission, an encoder will take a 4-bit symbol and steganographic payload, and output 32 chips. The receiver sends the 32 chips to a decoder, which produces the original 4-bit message and the steganographic payload. The block diagram in a normal radio is similar: the encoder is a fixed LUT, and the decoder is a correlator.

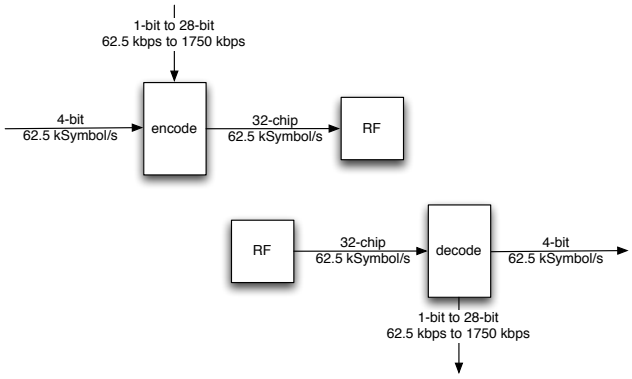

Fig 1. Block diagram of pertinent 802.15.4

- Analysis of simulation. Interesting analytical results include RX-sensitivity equivalency as a function of the the number of hidden chips.
- Implementation on programmable hardware.

Risks

- I will eventually need access to a pair of 802.15.4 programmable radios to implement changes to the transmitter and receiver. Kris Pister has hinted at an early-November date for this.
- Achieving a full 1.75Mbps covert signal while maintaining compliance with 802.15.4 receivers may not be theoretically possible, as the chip symbols defined for 802.15.4 are not orthogonal in the symbol space.