Demo: Bankrupting the Jammer

Farhana Ashraf, Yih-Chun Hu and Robin Kravets
University of Illinois at Urbana-Champaign
{fashraf2,yihchun,rhk}@illinois.edu

Sensor nodes have inherently limited energy. To increase network lifetime, most existing protocols for sensor networks are designed to achieve maximum energy-efficiency, without considering the presence of jamming attacks. This omission leads to significant assymetry of cost. Essentially, a jammer can waste significant energy of the sensors while spending only little energy of its own [3], enabling jammers with even limited energy to launch successful attacks against a wireless sensor network. In this demo, we consider an attacker and several senders, each with limited energy and the same power limitations, and show how to make jamming less effective.

Current solutions to defend WSNs against such cheap jammers (e.g., channel surfing [2], randomized SFDs [1]) are all based on hiding an ongoing packet transmission from reactive jammers that only jam when they think or know there is an active data transmission. However, these solutions require tight syncrhonization between each sender-receiver pair to ensure successful data delivery. Moreover, these solutions provide no defense against cheap jamming when the packets are detected. In response, instead of trying to outsmart the jammer, we take a different approach that attacks the jammer and makes jamming more expensive.

We propose `Jam-Buster` – a low overhead jam-resistant framework that improves the resilience of WSN communication to jamming by making jamming more expensive. Due to *Multi-block Payload Packets*, the jammer incurs more transmission cost to jam a packet. The *Random Wakeups* force the jammer to pay more idle listening cost to detect an ongoing transmission since the jammer can no longer predict future data transmission times using statistical analysis.

Multi-block payload packet enables the receiver to recover uninterfered data bytes from partially jammed packets. The sender divides the data into k blocks and calculates the CRC for each block. The sender then packs the k blocks along with the k CRCs inside the packet payload. This enables the receiver to verify each block independently for interference and limits the jammer's effectiveness to only those blocks with which the jamming signal overlaps. The challenge here is to identify the optimal k. As the sender increases k, the receiver can achieve more fine-grained recovery from the jamming signal. However, more blocks increase the total CRC overhead paid by the sender and thus reduce the net data bytes inside the packet. To resolve this, `Jam-Buster` models the system as a non-cooperative game and operates at the k that ensures the Mixed Strategy Nash Equilibrium.

Random Wakeup breaks the periodic pattern of the data transmission times caused by the correlation between the data transmission and the periodic wakeup times. Sensors divide their time into fixed size slots called *wakeup frames*. Each node wakes up randomly within a wakeup frame. Because of the random wakeups, it is impossible for the jammer to predict future data transmission times without explicit knowledge of all wakeup parameters. Thus, random wakeup reduces the effectiveness of the jammer by shortening the jammer's lifetime since the jammer now must remain awake longer to detect ongoing transmissions.

While *Multi-block Payload Packet* and *Random Wakeups* can be independently adopted as a defense, the combination of the two results in very expensive jamming due to high transmission and listening costs for the jammer. To demonstrate the feasibility and effectiveness of our system, we have implemented `Jam-Buster` on Tmote Sky motes. In our setup, all sensors are connected to laptops via USB ports. As the sensors exchange data messages in the presence of a reactive jammer, the laptops collect statistics about the goodput and the energy performance of the system. During the demo, using customized java applications running on the laptops, we will provide visual represention of the overall as well as the instantenous effectiveness of `Jam-Buster`.

Categories and Subject Descriptors

C.2.0 [**General**]: Security and protection (e.g., firewalls)

General Terms

Security

This material is supported in part by USARO award W-911-NF-0710287, NSF award CNS 06-26825 and NSF award CNS-0953600

Copyright is held by the author/owner(s).
MobiSys'11, June 28–July 1, 2011, Bethesda, Maryland, USA.
ACM 978-1-4503-0643-0/11/06.

[1] A. Wood, J. Stankovic, and G. Zhou. DEEJAM: Defeating energy-efficient jamming in IEEE 802.15. 4-based wireless networks. In *SECON*, 2007.

[2] W. Xu, W. Trappe, and Y. Zhang. Channel surfing: defending wireless sensor networks from interference. In *IPSN*, 2007.

[3] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In *MobiHoc*, 2005.