



Figure 1: A sequence of baseband sampling points showing WiFire in action. An IEEE 802.15.4 transmission begins (with constant amplitude), and WiFire detects and analyzes the signal and decides whether the packet must be jammed or not. It then emits a short jamming burst (the sinusoidal signal) to distort the signal, destroying the packet at the receiver.

1. data frames coming from node 10 in the current networks (with the identifying PAN ID), and
2. control frames that are sent from other source addresses than 1.

Rule 1 is used to block all data traffic from a node of choice, virtually separating it from the network. This can be used to enforce a fast *node revocation*, e.g., when the keying material of this node is leaked. Rule 2 enforces that only node 1 (e.g., the PAN coordinator) can send control messages on the current channel to protect other nodes from being hijacked.

Preventing packet reception. WiFire prevents packet receptions by jamming. The intended receiver then either misses the packet completely or detects a corrupted frame with a failed integrity check. This approach to prevent receptions gives WiFire the *transparency* property: protected devices do not need to know about WiFire’s presence, no protocol adaptations or control messages from the firewall are necessary. Therefore, WiFire can be added to existing legacy networks to “patch” their security problems, filtering out malicious packets. At the same time, WiFire is friendly to co-existing networks despite its active nature: (i) it uses efficient jamming waveforms and short jamming durations (down to $32\mu\text{s}$ for 802.15.4), (ii) it limits its activity to times of attack, and (iii) it can be restricted to selected regions with physical layer means such as directional antennas. During normal operation, WiFire monitors the channel passively and reacts to immediate threats only. Fig. 1 shows WiFire in action: it has analyzed an incoming packet, detected a policy violation, and, thus, interferes with a part of the packet to prevent its reception.

3. THE DEMONSTRATION

In the demo we show that the concept of a wireless firewall based on real-time detection and selective jamming is technically feasible and provides interesting perspectives in securing wireless networks.

3.1 Scenarios

We use an 802.15.4-based wireless sensor network and an attacker using the KillerBee framework [3] to show several usage scenarios for WiFire. With its rule-based system, WiFire can be easily adapted to specify and block adversarial flows while leaving the legitimate flows intact. We show that WiFire protects effectively from flooding attacks, node capturing and injection attacks.

We offer several ways to observe WiFire’s operation: (i) packet reception rate measurements on the sensor motes to show that selected flows can be effectively blocked, and (ii) a GNU Radio-based monitor application that provides visualizations such as in Fig. 1 in real-time.

3.2 Interaction

We want to offer an interactive demo to the attendees, e.g., to let them choose the network topology, and the placement of the firewalls antennas and sensor motes. Additionally, the set of active rules for WiFire to enforce are adaptable on the fly, enabling attendees to evaluate the performance of our implementation in settings of their choice.

3.3 Discussion

We are aware that the idea of active protection measures such as jamming is a rather controversial one, so we also like to hear the opinions of the attendees of SIGCOMM ’11 and discuss with them about possible problems and limitations of this idea, especially attacks against WiFire on the physical layer. On the other hand, as this concept is applicable to a variety of wireless technologies and scenarios, we expect that a number of additional ideas will come up on applications and uses for WiFire.

3.4 Experimental Platform

While the main theme of the demo is the wireless firewall, WiFire itself can also be used as an experimental platform to generate finely controllable interference for repeatable testbed experiments. We are able to present further uses that the platform may find in wireless network testbeds, and how researchers can employ WiFire in their experimentation work. We will provide all necessary resources of WiFire online to interested researchers after the conference.

4. REFERENCES

- [1] I. Martinovic, P. Pichota, and J. B. Schmitt. Jamming for good: a fresh approach to authentic communication in WSNs. In *Proc. of ACM WiSec ’09*, pages 161–168. ACM, Mar. 2009.
- [2] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders. Reactive jamming in wireless networks: how realistic is the threat? In *Proc. of ACM WiSec ’11*, pages 47–52. ACM, June 2011.
- [3] J. Wright. KillerBee—practical ZigBee exploitation framework (presented at ToorCon ’10), Oct. 2010. Available at <http://code.google.com/p/killerbee>.