WiFire: A Firewall for Wireless Networks

Matthias Wilhelm* Ivan Martinovic¶ Jens B. Schmitt* Vincent Lenders‡

*Disco Labs, TU Kaiserslautern
{wilhelm,jschmitt}@cs.uni-kl.de

¶EECS, UC Berkeley
martinov@eecs.berkeley.edu

‡Armasuisse, Switzerland
vincent.lenders@armasuisse.ch

ABSTRACT

Firewalls are extremely effective at enforcing security policies in wired networks. Perhaps surprisingly, firewalls are entirely nonexistent in the wireless domain. Yet, the need to selectively control and block radio communication is particularly high in a broadcast environment since any node may receive and send packets. In this demo, we present WiFire, a system that brings the firewall concept to wireless networks. First, WiFire detects and analyzes packets during their transmission, checking their content against a set of rules. It then relies on reactive jamming techniques to selectively block undesired communication. We show the feasibility and performance of WiFire, which is implemented on the USRP2 software-defined radio platform, in several scenarios with IEEE 802.15.4 radios. WiFire is able to classify and effectively block undesired communication without interfering with desired communication.

Categories and Subject Descriptors

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

General Terms

Security, Design, Experimentation

1. INTRODUCTION

Access to the wireless medium is hard to regulate and control as any device in the transmission range can eavesdrop and inject packets into a network with low effort. In this demonstration, we showcase WiFire, a system that helps regaining control over the RF spectrum by *enforcing* security policies at the physical layer. The idea is simple: WiFire scans the RF spectrum for packets that might reach the protected network, analyzes whether they comply to a given ruleset or not, and blocks them if necessary. WiFire achieves this by demodulating and decoding packets sequentially *during* their transmission, classifying each individual packet with a set of rules based on its content (such as the source or destination addresses, frame type or even parts of the payload) and jamming it before it reaches the receiver. This approach has many system challenges because of the real-time constraints of detection and subsequent jamming of packets. On the other hand, this approach enables WiFire to offer the service of a wireless firewall, i.e., enforcing a security policy from a single point of administration and control, without the need to make WiFire explicitly participate in the network. We show the feasibility and applicability of this concept with a demonstration of WiFire protecting an IEEE 802.15.4 network in several attack scenarios.

The system runs on the software-defined radio platform USRP2 and is implemented both in FPGA logic and firmware code to satisfy the hard timing constraints; a host PC is used to configure the operational parameters and collect firewall statistics and logging messages. In previous work [2], a predecessor of WiFire is described and its performance of selective jamming in 802.15.4 networks is evaluated. With the added rule checker, we aim to promote the idea of "friendly jamming" that can help to reach security goals in wireless networks [1].

SIGCOMM'11, August 15–19, 2011, Toronto, Ontario, Canada.
ACM 978-1-4503-0797-0/11/08.

2. WIFIRE'S OPERATION

WiFire proceeds in three steps in its operation: *(i)* spotting packets, *(ii)* distinguishing friends from foes, and *(iii)* destroying malicious packets.

Detecting packets. WiFire continuously monitors the wireless medium, spotting packets for analysis. WiFire exploits the fact that an attacker must be constructive to inject packets, it must comply to the correct frame format to ensure that its packets have a chance to be received. WiFire scans the medium for the physical layer header of 802.15.4, consisting of a preamble and start-of-frame delimiter (SFD).

Identifying malicious packets. When a packet transmission is detected, WiFire analyzes the signal and checks whether a rule in the stored ruleset matches. We have implemented an O-QPSK demodulator and an 802.15.4 frame decoder to access link layer fields or payload bytes while the packet is on the air, one byte at a time. This output stream is fed into an `iptables`-style rule checker that supports chains of rules consisting of an arbitrary combination of matches, i.e., functions that check for packet features. An example chain that can directly be interpreted by WiFire's rule checker is

```
wftables -A -m dot15.4-ftype --data
            -m dot15.4-dst --mode 2 --pan 0x11 --addr 10
            -j JAM                          # Rule 1
wftables -A -m dot15.4-ftype --ctrl
            -m ! dot15.4-src --mode 2 --pan 0x11 --addr 1
            -j JAM                          # Rule 2
wftables -A -j ACCEPT                       # Default policy
```

This ruleset specifies that all transmissions are allowed (the default policy), except for ...

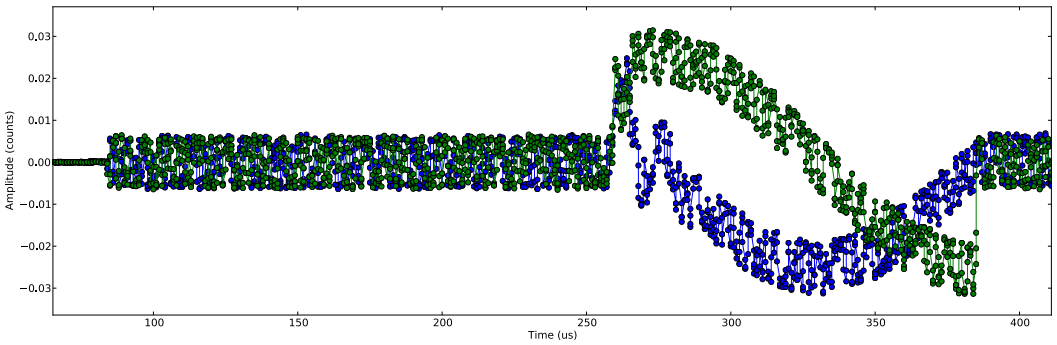

Figure 1: A sequence of baseband sampling points showing WiFire in action. An IEEE 802.15.4 transmission begins (with constant amplitude), and WiFire detects and analyzes the signal and decides whether the packet must be jammed or not. It then emits a short jamming burst (the sinusoidal signal) to distort 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 $32\,\mu$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`.