# Airshark: A System for Automating Wireless Diagnostics and Analysis

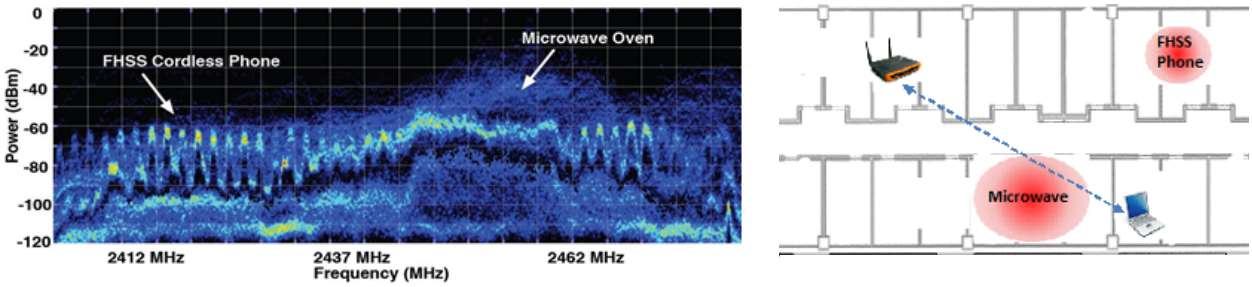
http://research.cs.wisc.edu/wings/projects/airshark

## 1. Project Description

Wireless interference is a conundrum that has confounded network administrators and users alike. Often times, in an enterprise wireless LAN (WLAN) environment, users encounter problems that are sporadic, hard to reproduce, and hence difficult to debug. For instance, the following is a dialog that we observed in an enterprise network:
- *User 1:* "Is anyone else finding the wireless network to be slow and flaky?"
- *User 2:* "I found it slow and flaky yesterday. Re-starting the laptop seemed to solve the problem."

The first user complained to the IT department about these problems. An hour later, after the network administrator showed up and tried to debug the problem, he send out this note:
- *Admin:* "We continued to hear reports of problems, but could not reproduce the problems "on demand' nor do we have enough details to identify the real issues."

When the wireless infrastructure works, its untethered operation is a great boon to users. However, at moments of failures, they are a cause of great frustration. We believe that wireless networks today lack effective tools for allowing efficient diagnostics. The goal of this project is to build *a new and unique wireless diagnostics toolkit, called Airshark, that allows users and network administrators to quickly and efficiently debug performance problems in the RF medium.*




(a) Non-WiFi interferers in WiFi spectrum as observed by a sophisticated spectrum analyzer.

(b) Airshark's view of non-WiFi interference as observed by the WiFi client.

**Figure 1: Airshark implemented in software atop standard WiFi interfaces detect the type of interferer, their location, and the relative impact of these interferers (indicated by the size of the blob) as they affect the WiFi traffic usually varying in real-time based on both WiFi traffic characteristics and the non-WiFi interference pattern.**

**Design of Airshark:** The goal of Airshark is to allow a WiFi device to determine the sources of interference *as and when they impact performance.* In particular, Airshark reports the source of interference, their likely location, and the extent of their impact on the WiFi device in real-time. For instance, a frequency hopping cordless phone in the neighborhood of a WiFi-capable iPod Touch could be marginally disruptive to a streaming movie a user is watching in the iPod Touch. However, a microwave oven in the vicinity could be responsible for causing more significant disruptions in performance. Airshark is designed to be *a software toolkit* that can systematically detect, quantify, and localize such sources of interference, in *a real-time and passive manner.* In the above example, the Airshark module might report that a nearby frequency hopping phone has an interference impact of 0.3 (in a scale from 0 to 1) while a microwave oven has an impact of 0.9.

A big challenge solved in designing Airshark is to allow a WiFi device to determine various non-WiFi sources of interference. Traditionally this has been a hard problem since WiFi systems are unable to decode these non-WiFi transmissions. Hence, to discern different types of non-WiFi interferers, users and administrators attempt to use specialized spectrum analysis hardware, e.g., Spectrum XT (from Fluke Networks), AirMaestro (from Bandspeed Networks), and the WiSpy USB-based units (from Metageek), Some of these units have limited spectrum resolution and cannot provide high quality detection of such sources of interference. The unique capability of Airshark is to build all interferer detection capabilities *purely as a software module on top of off-the-shelf WiFi interfaces.* As a result, this solution can be readily installed in client devices directly without the need for additional and sophisticated

wireless hardware. In the future, any device with a capable WiFi interface can implement and leverage the benefits of Airshark. We believe that Airshark is a core wireless diagnostics module that can be leveraged by WiFi systems to understand existing causes of interference and design better mitigation strategies. Such capability implemented over common WiFi platforms do not exist in the market today and provides Airshark with a unique angle to potential commercial success.

**Approach:** Airshark leverages sub-carrier level FFT samples that are available from the wide range of WiFi interfaces (e.g., the Atheros AR92xx chipsets onwards). We build a decision-tree based learning algorithm that can identify devices in real-time. Each Airshark capable WiFi device can use this algorithm to determine different interferer types. Furthermore, we use some time-frequency properties of these non-WiFi transmissions as observed by these WiFi devices to both approximately localize these interferers and quantify their impact on ongoing WiFi transmissions. The details of the algorithmic techniques are described in our recently published work [2, 3].

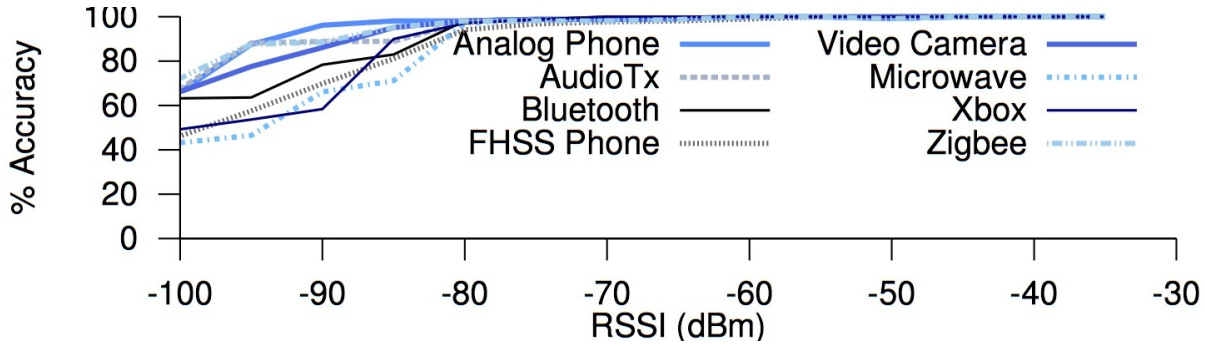



**Figure 2: Our preliminary lab prototypes demonstrate near perfect accuracy of Airshark in determining interference sources at a large range of received signal strength ($>$ -80 dBm). The performance gracefully degrades at lower signal strengths. A number of non-WiFi interferers were tested in these experiments.**

**Current status:** In the last one year, we have done significant design and experimentation on the Airshark software module through initial laboratory prototypes (Figure 2 shows some preliminary results). These results of this experimentation was reported in two recent publications [2, 3]. More importantly, the broad technical community picked up on this work and our plan got some preliminary publicity in a number of online and technical forums (including Slashdot, The UK Register, Boing Boing, etc.). In addition, two different wireless analytics companies have approached us for potential licensing arrangements once a real and functional standalone version of the software can be completed. Finally, we are also in preliminary discussions with one of the largest WiFi enterprise vendors on integration of this technology into their Access Points.

**Intellectual property:** Airshark, as described in our recent papers [2, 3], is fairly unique are is being patented with the USPTO provide necessary IP protection in our commercialization plan.

**Relation to an emphasis area:** The project is related to the *radio network management and systems innovations* emphasis area. WiFi-based mobile devices pervade all aspects of our lives — work, pleasure, business, and social interactions. As these devices have experienced an explosive growth, adequate tools to debug various RF and network performance have been an increasing necessity. The proposed Airshark toolkit is a unique and highly innovative system that fits well with this specific area.

## 2. Commercial viability

Systems such as Airshark is a growing necessity in the WiFi marketplace. The market, as we see it, exist in two parts.

- *Client side diagnostic tools:* Examples include Spectrum XT (from Fluke) and WiSpy devices (from Metageek). These solutions build custom spectrum analysis hardware and are attached as USB-based units onto laptops.

- *Access Point side diagnostic tools:* Examples include AirMaestro (from Bandspeed) and Spectrum Expert (Cognio, now Cisco). These are also specialized spectrum analysis hardware chipset solutions which are being integrated into Access Points for real-time wireless diagnostics and analysis.

Infiniti Research in its 2011 report estimates that the size of the global enterprise wireless (WiFi) network management market will reach $718 million in 2014 [1]. A system based on Airshark will have unique advantages

over many of the current incumbents in this space (since Airshark is based on off-the-shelf WiFi hardware, while existing solutions use custom wireless hardware) and can provide a significant foundation in entering this market.

Further, the success stories of the two companies that operate purely in the client side (Metageek and Fluke) that required relatively low amounts of capital to achieve profitability provide significant hope that a commercially successful entity, that is based on high quality and unique IP, is feasible in this space.

## 3. Milestones and plans for future commercialization

As described Airshark and its various components have already been developed as initial prototypes in the laboratory. In this initial development, we did not have direct access to the spectrum FFT data from a WiFi interface, but we were provided this access by a strategic commercial partner (a large enterprise WLAN vendor). In the next 12 months, we intend to complete the following technology milestones:

- *Release of a standalone Airshark (beta) software system (Month 4):* We plan to complete a fully standalone version of the client-side Airshark on both the Windows and Mac platform. The unique part of this Airshark system is the learning software system that is built on top of the spectrum FFT samples. This is the part that will be built by the project team. However, a relevant piece of this system will be a modified WiFi drivers that provide us the relevant spectrum FFT samples. While it is possible for this project team to build these driver modules, our plan is to offload this driver building task to a specific driver development company that specializes in building such driver software. Discussions are already ongoing with multiple such companies who will provide us with the necessary driver. Our unique IP sits in the Airshark software module that sits on top of this driver that this project team completely controls.

- *Release of the standalone Airshark v1.0: (Month 6):* The completed version of this software will be made publicly available in two additional months. This version of the software will include non-WiFi interferer detection capability only (and will not include the non-WiFi device localization and impact quantification components).

- *Release of Airshark v2.0 (Month 9):* The next version of Airshark will incorporate the two pieces missing in v1.0, namely the non-WiFi device localization and impact quantification. This capability would allow the system to not only detect that there are, say a microwave oven or an analog phone causing interference to a WiFi device, both also help users and administrators locate them on a map and determine *how much* interference each such interferer is causing.

- *Airshark SDK completed for potential OEM integration (Month 12):* In a few more months, we will create and make available the entire software suite in an SDK format for potential OEM-style integration by partners.

Our approach to commercialization will explore two parallel paths. For the client side solution, we will make the software-only solution available for direct downloads to potential customers from our website (this will include the standalone versions). However, since customer acquisition is always a challenge initially (and depends quite a bit on investment made in marketing strategies), we would also make the entire system be available as a SDK for integration into other existing client-side solutions. As a result, we will explore OEM-style licensing opportunities in this space.

For the Access Point side, we focus solely on the OEM-style licensing model with existing large enterprise WLAN vendors in this space. We have existing and ongoing relationships with multiple such vendors (both in the client and Access Point side) to start such explorations.

# References


[1] Infinite Research Limited. global wireless IP network management market 2010-2014. Available at: http://www.marketresearch.com/Infiniti-Research-Limited-v2680/, May 2011.

[2] S. Rayanchu, A. Patro, and S. Banerjee. Airshark: Detecting non-WiFi devices using commodity WiFi hardware. In *Internet Measurement Conference*, Nov. 2011.

[3] S. Rayanchu, A. Patro, and S. Banerjee. Catching whales and minnows using WiFiNet: Deconstructing non-WiFi interference using WiFi hardware. In *USENIX Networking Systems Design and Implementation*, Apr. 2012.