2005 IEEE International
Symposium on Signal Processing
and Information Technology

Electromagnetic Signatures of WLAN Cards and Network Security[1]

K.A. Remley, C.A. Grosvenor, R.T. Johnk, D.R. Novotny, P.D. Hale, M.D. McKinley
NIST Electromagnetics, Division 818
325 Broadway
Boulder, CO 80305-3328
{remley, chriss, johnk, novotny, hale, mckinm}@boulder.nist.gov

A. Karygiannis, E. Antonakakis
NIST Computer Security Division 893
100 Bureau Drive
Gaithersburg, MD 20899
{karygiannis, manos}@nist.gov

Abstract

The proliferation of wireless devices and the availability of new wireless applications and services raise new privacy and security concerns. Although network-layer anonymity protects the identities of the communication endpoints, the physical layer of many wireless communication protocols offers no such guarantee. The electromagnetic signal transmitted over an open communication medium can be monitored, captured, and analyzed in an effort to trace and identify users of wireless devices. In this paper we present preliminary results on the feasibility of identifying wireless nodes in a network by measuring distinctive electromagnetic characteristics or "signatures" of Wireless Local Area Network (WLAN) cards.

Keywords: wireless networks, microwave measurements, electromagnetic signature, wireless network security.

1. Introduction

Over the last few years the cryptographic protocols of IEEE 802.11b™ have been the subject of a great deal of scrutiny by security professionals and researchers alike. The 802.1x protocol provides stronger user authentication through the incorporation of an Extensible Authentication Protocol (EAP) dialog, while the 802.11i protocol offers enhanced data security over the 802.11b and the Wired Equivalent Privacy (WEP) protocol. Moreover, anonymizing authentication and routing protocols have been proposed in the literature to further protect user privacy and anonymity [1,2,3].

Although these network-layer protocols protect the identities of the communication endpoints, the physical layer of 802.11-based wireless communication offers no such guarantee. Any electromagnetic signal transmitted over the airwaves can be monitored, captured, and analyzed by any sufficiently motivated and equipped adversary within the 802.11 device's transmission range. A user's anonymity and privacy can be compromised if a node can be identified, or differentiated from another node, through the measurement of distinctive radio-frequency (RF) electrical characteristics or "electromagnetic signatures."

The electromagnetic signature technique described here is similar to "specific emitter identification," a real-time measurement used in military applications to distinguish between friendly and enemy radar signals [4,5]. The goal in that case is to associate a received pulse with a specific transmitter, while our goal is to identify a specific transmitter in a network. In either application, the distinctive electromagnetic signature characteristics arise from differences in circuit and antenna topology from manufacturer to manufacturer and from variability in circuit performance linked to manufacturing tolerances. At higher frequencies, such as 2.4 GHz (802.11b/g) or 5.2 GHz (802.11a), even

[1] Publication of the U.S. Government, not subject to U.S. copyright.

slight component variations in a transmitting circuit may have a pronounced effect on the emitted signal.

If distinctive electromagnetic signatures can be detected, a wireless device and its associated user can be tracked, and when coupled with a visual identification, can also be identified. The privacy implications of identifying electromagnetic signatures cannot be underestimated. This paper presents preliminary results on the potential for compromising user anonymity and privacy by measuring an electromagnetic signature of 802.11b Wireless Local Area Network (WLAN) cards.

2. Experimental Approach

To investigate the viability of using RF electromagnetic signatures to identify wireless nodes, we carried out measurements of six different WLAN cards (two of each from three different manufacturers) one at a time. We performed detailed measurements of spectral features of the signal and of the time-domain RF waveform emitted by each WLAN node. We also carried out a preliminary study on the sensitivity of the electromagnetic signature to the orientation of the node to the receiving antenna, which demonstrated that rotating the transmitting node can provide another type of electromagnetic signature. The orientation study also provides a first indication of the difficulty of field implementation of a system to detect electromagnetic signatures of WLAN nodes.

The wireless cards from each of the three manufacturers were built on the Prism2 chipset packaged in a Compact Flash[2]. The processor used was an Intrinsyc CerfCube 255 running the Familiar distribution of Linux. CerfCubes are typically used for embedded applications development, but may also act as servers or repeaters in a wireless network. Each CerfCube executed the following simple script, providing a repetitive symbol pattern in the received signal.

```
while [ 1 ]
  do
  ping 85.85.85.85
done
```

[2] Use of brand names does not constitute an endorsement by the National Institute of Standards and Technology. Other products may work as well or better.

Our measurement set-up consisted of an ultrawideband (UWB) horn antenna which fed an amplifier chain to improve the signal-to-noise ratio. This set-up is shown schematically in Fig. 1. To minimize noise and unwanted signal interactions, the CerfCube transmitting node and the receive antenna were placed inside the NIST anechoic chamber, which is lined with an absorbing material on all six sides to minimize wall reflections. This controlled environment also guaranteed a high level of measurement repeatability and provided shielding, so that interfering signals were minimized. The WLAN node was placed on a dielectric pedestal at the same height as the receiving antenna approximately three meters away, as shown in the photograph of Fig. 2.

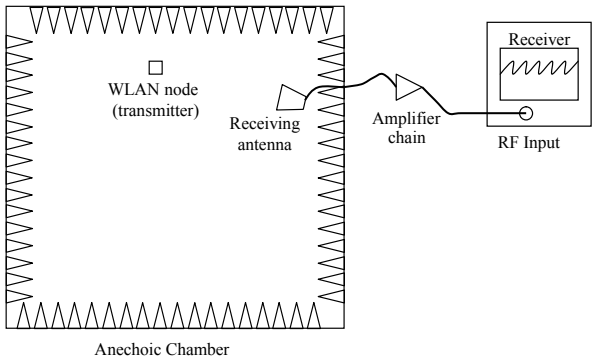

Figure 1: Measurement Setup for the WLAN card measurements. The CerfCube transmitter and the receiving antenna were placed in an anechoic chamber to provide isolation. "Receiver" refers to either a vector signal analyzer or a real-time oscilloscope.

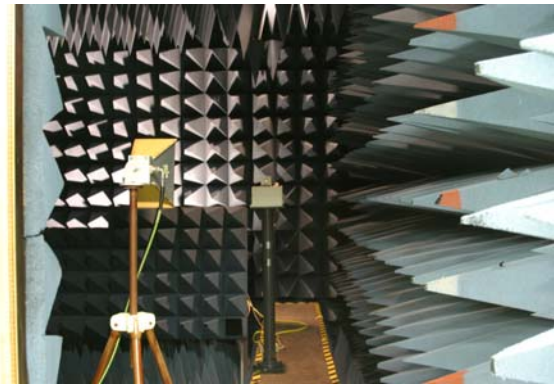

Figure 2: WLAN transmitting node (on pedestal) and receiving antenna (in foreground) in NIST's anechoic chamber.

Spectral Measurements: We carried out spectral measurements using a vector signal analyzer (VSA). This instrument records a time-domain waveform and downconverts it to baseband where it is digitized and transformed to the frequency domain. The VSA is thus able to record a high level of spectral detail in its 36 MHz measurement bandwidth. To capture the 40 MHz passband plus the spectral features on either side of the passband of the WLAN signals, we carried out measurements above and below the passband. The six spectra in Figure 3 show measurements of two WLAN cards from each of three manufacturers whose measured upper and lower spectral segments have been stitched together. Larger-scale figures in which the details of the measurements are more clearly visible are provided in the Appendix.

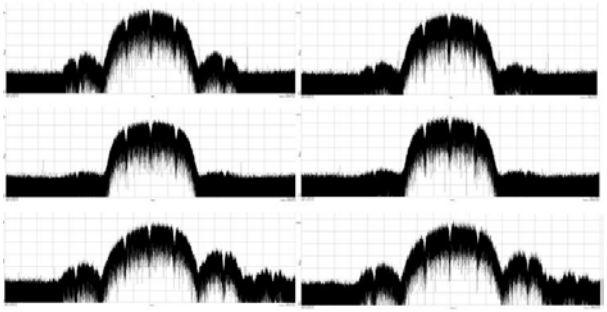

Figure 3: Signal spectra of six WLAN cards from three different manufacturers, one manufacturer per row. Frequency is on the x-axis and magnitude is shown in dBm on the y-axis. The differences in the symmetry of the main passband, as well the level and symmetry of the sidebands are evident. See the Appendix for a larger figure in which the details of the measurements are more clearly visible.

Several features are readily apparent. The main lobe of the received signals from manufacturers 1 and 2 (top and middle rows) are more symmetric than that from manufacturer 3 (bottom row). The sidebands (the minor lobes on either side of the main passband) for the cards from manufacturers 1 and 3 are higher than those of manufacturer 2. The cards from manufacturer 3 show an additional sideband at a higher frequency that does not appear for the other manufacturers. Minor differences are also apparent between cards from the same manufacturer. For example, the sidebands from manufacturer 1 on the lefthand graph are higher than those on the righthand graph. These types of spectral features constitute electromagnetic signatures that allow us to readily distinguish not only among cards from different manufacturers, but also among cards from the same manufacturer when the transmitting node is held in an isolated, fixed position.

Time-Domain Measurements: We next measured the time response of the six cards using a 20 gigasample per second (GS/s) real-time oscilloscope. These measurements were carried out in the anechoic chamber, using the configuration shown in Figs. 1 and 2. Figure 4 shows segments of the waveforms we acquired from all six cards that include the start of the bursted 802.11b signal. The two cards in the top row are from manufacturer 1, the middle row are from manufacturer 2, and the bottom row are from manufacturer 3. Note that while the cards do transmit a repeating pattern, the first few symbols of the card from manufacturer 2 are different from the others. The waveforms have been normalized so that the total power in the acquired waveform equals one.

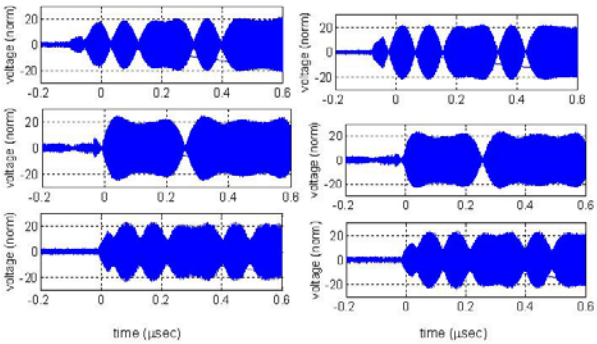

Figure 4: Time-domain measurements of two WLAN cards from each of three manufacturers. Note the differences in the shape of the first pulse, the depth of the nulls, and the shape of the symbols themselves. See the Appendix for a larger figure in which the details of the measurements are more clearly visible.

Distinguishing features between the six cards are subtle, but noticeable and quantifiable using signal processing metrics such as cross correlation. By inspection we can easily distinguish between manufacturers by looking at the depth of the nulls between symbols: The nulls for the card from manufacturer 3 are less deep than the nulls from the other two manufacturers. We can also see a difference in null depth in the two cards from manufacturer 1. We are additionally able to distinguish between the cards by looking at the height and shape of the first pulse. The roughness of the waveforms provides another indication of manufacturer. The ease with which we are able to distinguish between cards and manufacturers demonstrates potential for the development of viable electromagnetic fingerprinting techniques.

Orientation of Cards: Another form of electromagnetic signature of the WLAN cards concerns the orientation of the transmitting node relative to the receiving antenna. To investigate this effect, we rotated the network card box around its axis and looked at general signal emission effects such as

maximum and minimum emission levels and radiation pattern characteristics. We looked at the various network cards using two types of antennas: commercial dual-ridged guide (DRG) antennas and our own NIST-developed, broadband, phase-linear, transverse-electromagnetic horn (TEM) antennas.

We first noticed that the radiated emissions were predominantly in the horizontal polarization. We also noticed that there were definite minima in the radiation pattern of the transmitter as we rotated it axially. We gathered measurements at angles of 0, 45, and 90 degrees relative to the receiving antenna. For each set of cards from the three different manufacturers, we found that the amplitude of the received signal varied as a function of angle. The pattern characteristics differed significantly depending on the manufacturer, which is probably due to different network card transmit antenna and matching-circuit designs. Thus, radiated patterns provide yet another metric for identifying a particular network card.

Manufacturer	Pattern Maximum	Pattern Minimum
1	0 °	45 °
2	45 °	90 °
3	45 °	-45°

Table 1. Angular Pattern Maxima and Minima for Various Network Card Manufacturers.

3. Conclusions

The preliminary work presented here indicates that it may be viable to collect a set of distinguishing features from various WLAN 802.11b cards, at least in a controlled environment. Our controlled environment consisted of a single transmitting unit placed in a shielded, reflectionless environment and held at a fixed orientation to the receiver. One application for this type of scenario would be authentication of known nodes in a network.

However, questions remain as to the efficacy of electromagnetic fingerprinting for node identification, and these issues will be the focus of future work. Some of these include the distinctiveness of node RF characteristics, that is, is it possible to identify enough features to uniquely identify nodes or differentiate one node from another? How susceptible are these features to being altered by environmental effects, proximity to other nodes, and other effects such as temperature and aging? To implement electromagnetic fingerprinting systems in the field may require a range of instrumentation, although the accuracy required in each application may dictate which instruments are used. It may be possible to create networks whose nodes intentionally contain distinctive RF features for stronger authentication by manipulating software, hardware, or a combination of both. These features may even be designed to change dynamically, allowing for new network authentication mechanisms. As wireless devices continue to proliferate, electromagnetic fingerprinting systems may also be used by network forensics experts. The impact on anonymity and privacy may be profound if such a system is found to be viable, and new applications beyond the network security domain are likely to emerge.

4. References

[1] D. Chaum, A. Fiat, and M. Naor. Untraceable electronic cash. In Advances in Cryptology — Crypto ’88 (Lecture Notes in Computer Science), pages 319–327. Springer-Verlag, 1990.

[2] David Goldschlag, Michael Reed, and Paul Syverson "Onion Routing for Anonymous and Private Internet Connections," Communications of the ACM, vol. 42, num. 2, February 1999.

[3] Michael G. Reed, Paul F. Syverson, and David M. Goldschlag "Protocols using Anonymous Connections: Mobile Applications," Security Protocols, 5th International Workshop Proceedings, B. Christianson, B. Crispo, M. Lomas, and M. Roe (editors), Springer-Verlag LLNCS 1361, 1998, pp. 13-23.

[4] J. Dudczyk, J. Matuszewski, M. Wnuk, Applying the radiated emission to the specific emitter identification, Microwaves, Radar and Wireless Communications, 2004. MIKON-2004, 15th International Conf., vol. 2, May 17-19, 2004, pp. 431 – 434.

[5] Specific emitter identification (SEI) and classical parameter fusion technology L.E. Langley, WESCON/'93, Sept 28-30, 1993, pp.377 – 38.

Appendix

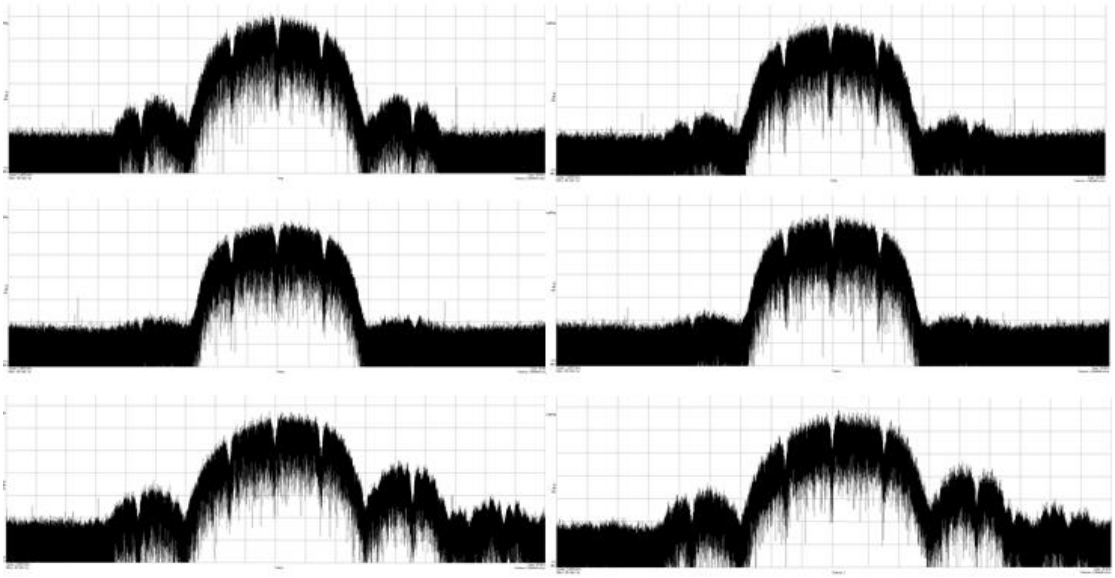

Figure 5

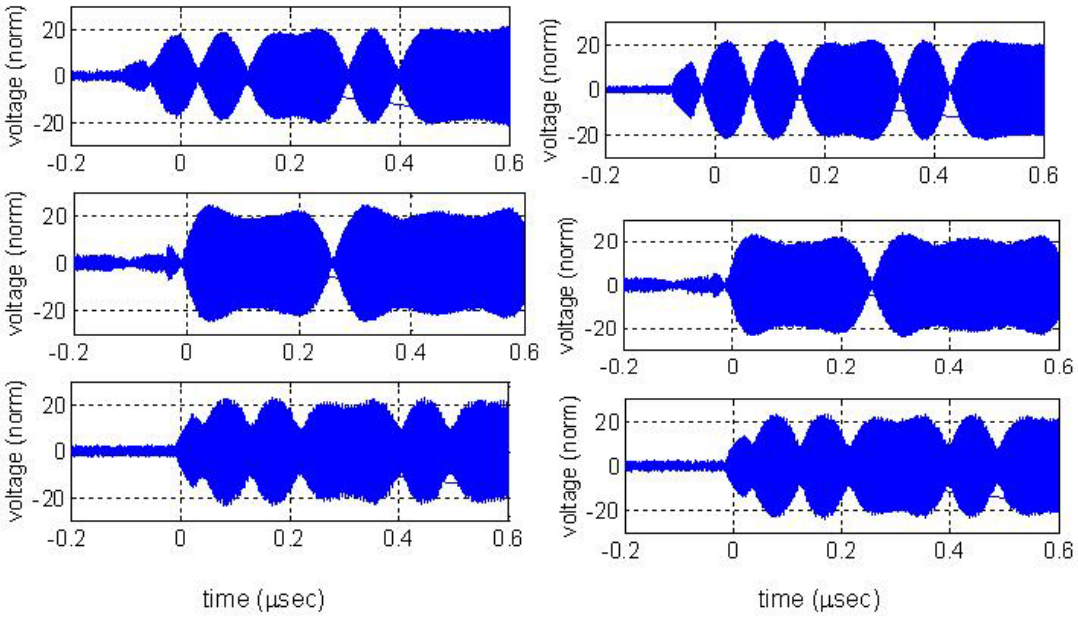

Figure 6