SecureAngle: Improving Wireless Security Using Angle-of-Arrival Information (Poster Abstract)

Jie Xiong
University College London
J.Xiong@cs.ucl.ac.uk

Kyle Jamieson
University College London
K.Jamieson@cs.ucl.ac.uk

ABSTRACT

Wireless local area networks play an important role in our everyday lives, at the workplace and at home. However, wireless networks are also relatively vulnerable: physically located off-premises, attackers can circumvent wireless security protocols such as WEP, WPA, and even to some extent WPA2, presenting a security risk to the entire network. To address this problem, we propose *SecureAngle*, a system designed to operate alongside existing wireless security protocols, adding defense in depth. SecureAngle employs multi-antenna APs to profile the directions at which a client's signal arrives, using this *angle-of-arrival* information to construct unique *signatures* that identify each client. With these signatures, we are currently investigating how a SecureAngle-enabled AP can enable a "virtual fence" that drops frames injected into the network from a client physically located outside a building, and how a SecureAngle-enabled AP can prevent malicious parties from spoofing the link-layer address of legitimate clients.

Categories and Subject Descriptors

C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*Wireless communication*

General Terms

Experimentation, measurement, security

Keywords

Wireless, 802.11, SecureAngle, Angle of arrival

1. INTRODUCTION

In the past few years, wireless local area network connectivity has undergone a transition from a niche service into an essential utility widely used by the general public. Enterprises have rolled out large scale wireless LAN across entire campuses. Many homes with a broadband Internet link are equipped with a WiFi-enabled router, and most mobile devices now integrate wireless WiFi chipsets, allowing users easy network connectivity.

However, from a security perspective, wireless APs present a number of problems. Once a client is connected to a compromised AP, an attacker may both eavesdrop on users' traffic and inject traffic into the wired network. WLAN security protocols such as WEP, WPA, LEAP, and WPA2 have been proposed in the past few years, however they have a track record of being compromised [2, 7, 8]. Furthermore, once deployed, they are slow to be fixed: six years after WEP was known to be insecure, Bittau *et al.* reported that a full 76% of secured APs in London still used it [3].

We propose *SecureAngle*, a new approach to the above security problems. Recently, 802.11n APs have begun to appear on the market equipped with multiple antennas, to implement MIMO schemes. On top of the resulting throughput benefits of MIMO, we observe that with the right signal processing at the physical layer, a multi-antenna AP can also measure the differences in time between an incoming signal's arrival at each antenna, and use these measurements to identify the incoming signal's *angles of arrival* (AoA). This AoA information can then be applied to construct a signature that is unique to each client and extremely difficult to forge.

We will investigate two applications of SecureAngle:

Virtual fences. We will investigate restriction of WLAN use to the building containing the AP. This would be appropriate, for example, in an enterprise setting where the company is contained in a secured building, and it is desired that only clients within the building be allowed access to the WLAN. For this application, we don't require the AP to discriminate between two inside or two outside clients, but we do require that signatures for all clients inside the building can be discriminated from signatures for clients outside the building. One reason this may hold is that indoors, there is more extensive multipath propagation than outdoors.

Address spoofing prevention. Another application of AoA-based signatures is to detect when a client is spoofing the link-layer address of legitimate stationary clients. Link-layer address spoofing can grant unauthorized access, if the only method of security is address-based access control lists, and spoofing often forms the basis of more sophisticated attacks against the security protocols we mention above. Our approach is to require the administrator to manually "certify" a legitimate client's signature at some point in time, and compare all incoming packets' signatures to the certified signature. A central challenge here is that signatures may change to some degree when obstacles in the environment move, and therefore must be tracked and updated. There also must be a significant difference between the certified signature and an attacker's signature so that they can be discriminated from each other. We hypothesis that AoA signatures are stable and tractable enough to be of use in

SIGCOMM'10, August 30–September 3, 2010, New Delhi, India.
ACM 978-1-4503-0201-2/10/08.

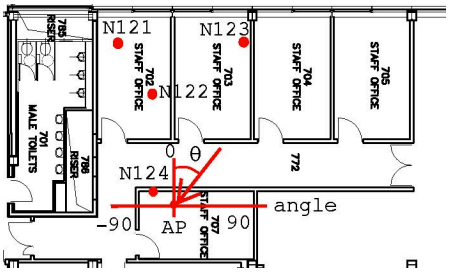

Figure 1: Floor plan with nodes position marked.

this and subsequent proposed applications, but leave the exact signature specification as an open research question.

2. RELATED WORK

Many schemes have been proposed to capture signatures that characterize wireless clients' identity and location. The most widely used physical layer information is received signal strength (RSS) [1, 4]. While readily available from commodity hardware, compared to the wealth of information available at the PHY of a multi-antenna SDR, RSS is a very coarse measure of the incoming signal, and is therefore prone to error if relatively few readings are available. Furthermore, attackers with directional antennas can subvert systems based on RSS measurements [5].

SecureAngle has unique advantages over the above work because it is very difficult for an attacker to generate a signal that arrives at the AP from the same directions as another client without being co-located with the latter. SecureAngle is the first work we are aware of that uses AoA-based signatures indoors, where reflections from walls and objects are relatively strong. Although Wong et al. [9] investigate the use of AoA information for localization, they stop short of a full system design and do not address the problem of indoor multipath reflections as we will.

3. EXPERIMENTAL RESULTS

Our experimental testbed is setup with a 4-antenna WARP [6] as the AP and Soekris boxes as transmitting clients. The WARP FPGA is programmed to support 4x4 MIMO reception at 2.4GHz. AP and four Soekris boxes named N121, N122, N123 and N124 are marked on the floor plan as shown in Figure 1. The 4 antennas of the WARP are arranged in a line with 6.1 cm (half the RF wavelength) separation.

Four Soekris boxes are put in different offices and transmit one by one separately. The WARP AP records the transmitted signals and outputs the sampled time domain information (both amplitude and phase) for further processing. We implement the Schmidl-Cox algorithm in Matlab to detect the preamble of packets and apply the MUSIC method to calculate AoA information. Figure 2 summarizes the results for all clients: the X axis is the ground-truth angle for each client with respect to the AP's antennas and Y axis is the AoA of the strongest incoming signal.

We then force two Soekris boxes to transmit simultaneously by turning off CSMA/CA. We modify Schmidl-Cox algorithm to detect overlapped packets even if the second packet (P2) is weaker than the first one. Both packets are detected and the AoA pseudo-spectrums (likelihood versus angle) for both transmitters are shown in Figure 3 (upper).

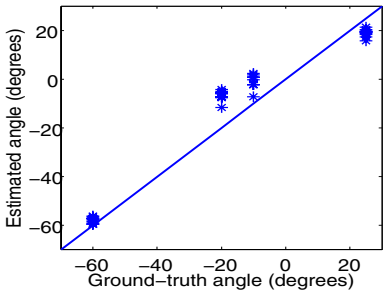

Figure 2: Estimated client bearing to the AP versus ground-truth, for each of the four clients.

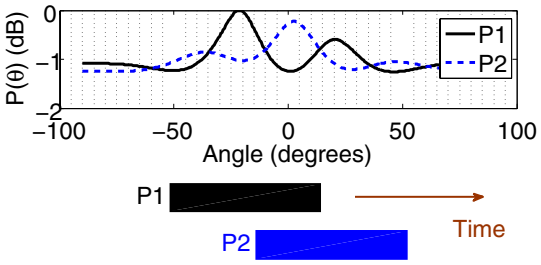

Figure 3: Upper: AoA pseudo spectrum (likelihood versus angle) for two colliding packets (lower)

The two curves in Figure 3 (upper) correspond to the two packets (lower) from two different Soekris boxes. Multiple peaks on the curve indicate multipath reflections in the indoor environment for each transmission. With 4 antennas, maximum of 3 peaks can be captured which corresponding to one direct path and two multipaths.

4. REFERENCES

[1] P. Bahl and V. Padmanabhan. RADAR: An in-building RF-based user location and tracking system. In *Proc. of the* IEEE INFOCOM *Conf.*, volume 2, pages 775–784, Mar. 2000.

[2] M. Beck and E. Tews. Practical attacks against WEP and WPA. In *Proc. of* ACM *WiSec Conf.*, pages 79–86, Mar. 2009.

[3] A. Bittau, M. Handley, and J. Lackey. The final nail in WEP's coffin. In IEEE *Symp. Security and Privacy*, 2006.

[4] D. Faria and D. Cheriton. Radio-layer security: Detecting identity-based attacks in wireless networks using signalprints. In ACM *WiSe Workshop*, 2006.

[5] N. Patwari and S. Kasera. Robust location distinction using temporal link signatures. In *Proc. of the* ACM *MobiCom Conf.*, pages 111–122, Sept. 2007.

[6] Rice Univ. Wireless Open Access Research Platform (WARP). http://warp.rice.edu/trac.

[7] B. Schneier, Mudge, and D. Wagner. Cryptanalysis of Microsoft's PPTP authentication mechanisms, Oct. 1999.

[8] E. Tews, R. Weinmann, and A. Pyshkin. Breaking 104-bit WEP in less than 60 sec. *Springer* LNCS, 4867:188–202, 2008.

[9] C. Wong, R. Klukas, and G. Messier. Using WLAN infrastructure for angle-of-arrival indoor user location. In *Proc. of the* IEEE VTC *Conf.*, pages 1–5, Sept. 2008.