Improving Localization, Security, and Throughput in Next-Generation 802.11 Networks

Jie Xiong
Department of Computer Science
University College London
j.xiong@cs.ucl.ac.uk

Kyle Jamieson
Department of Computer Science
University College London
k.jamieson@cs.ucl.ac.uk

***Abstract*—WiFi technology has developed significantly in the last ten years evolving from 802.11b/a/g/n to the latest 802.11ac. With the popularity of MIMO technology, one obvious trend we notice is that more antennas are attached to a single access point (AP). This unique opportunity is employed to improve the performance of wireless networks in several aspects: localization, security and throughput.**

With multi-antenna APs, ArrayTrack is proposed with angle-of-arrival (AoA) scheme to localize clients accurately indoors. Innovative multipath identification scheme is proposed to handle the challenging multipath issue in indoor environment. With six APs and eight antennas on each AP, ArrayTrack is able to achieve 30 cm median accuracy.

SecureArray is proposed to add another layer of security to the existing WiFi networks with multi-antenna APs. The location dependent AoA signature is employed to differentiate the legitimate clients and attackers. While multipaths are harmful in localization, they are useful in SecureArray because they make the signature unique. It is very difficult for the attacker to forge this signature unless it's located exactly at the client's location. SecureArray is sensitive enough to detect an attacker located only five centimeters away with high confidence.

802.11ac shifts from single-client to multi-client communication which significantly improves the throughput. However, we find that while the multiple antennas are currently co-located at the same position, spatially separating the antennas via RF cabling, and leveraging Multi-user MIMO through a Distributed Antenna System (DAS) is essential to getting the most out of Multi-user MIMO. With a power-balanced precoding scheme and a standards-compliant MAC, MIDAS is proposed which is able to outperform 802.11ac by more than 150% in terms of throughput.

I. Introduction

In the past few years, wireless data connectivity has continued its transition into an essential utility. Wireless networks are deployed everywhere including enterprises, campuses, airports, and homes. WiFi technology has also developed significantly evolving from 802.11b to the latest 802.11n and 802.11ac. 802.11n standard can provide much better performance and keep pace with the rapidly growing speeds provided by Ethernet. In order to achieve this higher performance, quite a few new features have been incorporated into 802.11n. The key feature is the use of Multiple Input Multiple Output (MIMO) [1], [2] technology. MIMO is a technique that exploits multipath propagation opportunities to improve capacity and diversity. When a signal is transmitted from access point A to client B, the signal reaches the receiving antennas via multiple paths. The data is split into multiple what are called spatial streams and these are transmitted through separate antennas to the antennas at the receiver. The current 802.11n standard supports up to four spatial streams which means four antennas are attached to a single 802.11n access point.

802.11ac standard is just finalized early this year. It incorporates multi-user MIMO scheme which is a big step forward from 802.11n. The key change for 802.11ac is the shift from single-client to multi-client communication pattern. Previously the AP can only talk to one client at a time while 802.11ac enables the AP to talk to several clients simultaneously. 802.11ac supports up to eight spatial streams which means eight antennas will be attached to the 802.11ac AP. The bandwidth supported is also increased to 160 MHz which is four times the bandwidth supported by 802.11n.

With the popularity of MIMO and standardization of 802.11n and 802.11ac, one interesting factor we observe is that: more and more antennas are attached to a single AP. A lot of commercial multi-antenna APs are already on the market as shown in Figure 1 from major vendors.

ASUS WL-500W
D-link DAP2690
Motorola AP7131

Fig. 1: Commercial 802.11n APs with multiple antennas.

We employ this unique opportunity of multiples antennas on an AP to improve wireless network performance, mainly in localization, security and throughput.

Localization: A fine-grained indoor localization system ArrayTrack [3] hosted on WiFi infrastructure is proposed. It is first implemented on WARP platform [4] as shown in Figure 2 and later on cheap off-the-shelf commodity hardware [5], where both demonstrate significant performance improvement over the existing systems. With multiple antennas on a single AP, angle of arrival (AoA) information can be generated when the client transmits. A typical AoA spectrum is shown in Figure 3. The location estimate can be obtained with AoA information from several such multi-antenna APs. ArrayTrack is a robust real-time localization system which achieves around 30 cm median accuracy. With more number of antennas on a single AP, the location accuracy can be further increased. The

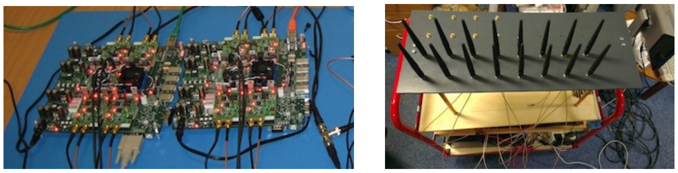


Fig. 2: *Left:* the SecureArray prototype AP is composed of two WARP radios, while a cable-connected USRP2 software-defined radio (not shown) calibrates the array. *Right:* The AP and antenna array mounted on a cart.

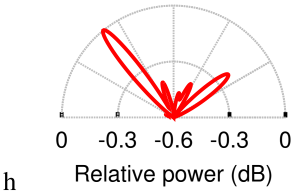


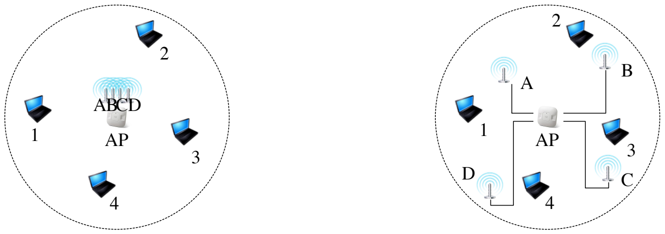
Fig. 3: The *AoA spectrum* of a client's received signal at a multi-antenna access point estimates the incoming signal's power as a function of its angle of arrival.

most challenging part of AoA localization is the presence of strong multipath indoors, which leads to performance degradation. A novel multipath identification scheme is proposed to handle this problem. It's noted that the line-of-sight (LOS) path signal is much more stable compared to the reflection-path signals. When a phone is held in somebodys hand or pocket, natural human movement presents a unique opportunity to identify the reflection paths and improve localization performance by taking several measurements and identifying the stable path peak on the AoA spectra.

Synchronicity (ongoing work) is a TDoA-based indoor localization system. TDoA was not popular previously in indoor localization because APs are usually not time synchronized and 802.11a/b/g/n APs don't have a large enough bandwidth for high time-domain resolution. With a larger bandwidth of 802.11ac and popularity of AP-synchronized distributed MIMO, we now relook at TDoA localization from a new perspective. We propose a novel spectrum identification scheme, which fundamentally breaks the bandwidth limit and outperforms the existing super resolution schemes. We employ a triangle inequality scheme to effectively handle the most challenging scenario where the line-of-sight path is 100% blocked. We are working on combining data from non-adjacent random-size channels to further increase localization accuracy.

Security: SecureArray [6] is a system proposed to add another layer of protection to today's wireless networks. Historically, attackers have found wireless networks relatively easy to break into, and compromise of the wireless network is often the first step to break into wired networks. Security protocols such as WEP, WPA, LEAP and WPA2 have been proposed in the past few years, but have a continuing track record of being compromised. SecureArray introduces this new AoA signature comparison scheme to enhance the security of 802.11 networks. With multiple antennas on the AP, AoA signature can be easily generated whenever the client transmits. While in ArrayTrack multipaths are harmful, they are useful in SecureArray because they make the AoA spectrum unique and difficult to be forged. This signature purely depends on the location and is unlikely for the attacker to forge unless the attacker is located exactly at the same location as the legitimate client. A novel random AoA spectrum perturbation scheme is proposed to significantly increase the attacker detection rate and reduce the false positive rate. SecureArray is sensitive enough to detect an attacker located only five centimeters away with high confidence.

Throughput: MIDAS [7] proposes a new deployment strategy for the latest 802.11ac standard to improve throughput performance. The key change for 802.11ac is the move from single-client to multi-client communication pattern. This shift significantly improves the overall throughput of the wireless network. However, we find that while the multiple antennas are currently co-located at the same position, spatially separating the antennas via RF cabling, and leveraging Multi-User MIMO through a Distributed Antenna System (DAS) as shown in Figure 4b is essential to getting the most out of Multi-User MIMO. The intuition behind this approach is a larger average signal level and smaller interference, leading to higher SINR and correspondingly higher throughput. Because of the larger spatial diversity with DAS deployment and the per-antenna power constraint with 802.11ac, we propose a power-balanced precoding scheme, which is able to achieve close to optimum performance without incurring large computational load. We also design a standards-compliant MAC protocol to realize the full potential of DAS-based 802.11ac. MIDAS outperforms 802.11ac by more than 150% in terms of throughput.



(a) A Co-located Antenna System (CAS)

(b) A Distributed Antenna System (DAS)

Fig. 4: CAS vs DAS deployment.

REFERENCES

[1] G. G. Raleigh and J. M. Cioffi, " Spatio-temporal coding for wireless communications," in *Proc. GLOBECOM*, 1996.

[2] A. J. Paulraj and T. Kailath, "US 5345599 A: Increasing capacity in wireless broadcast systems using distributed transmission/directional reception (DTDR)," 1993. Stanford Junior University.

[3] J. Xiong and K. Jamieson, "ArrayTrack: A Fine-Grained Indoor Location System," in *Proc. USENIX NSDI*, 2013.

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

[5] J. Gjengset, J. Xiong, G. McPhillips, and K. Jamieson, "Phaser: enabling phased array signal processing on commodity WiFi access points," in *Proc. ACM MobiCom*, 2014.

[6] J. Xiong and K. Jamieson, "SecureArray: improving wifi security with fine-grained physical-layer information," in *Proc. ACM MobiCom*, 2013.

[7] J. Xiong, K. Sundaresan, K. Jamieson, A. Khojastepour, and S. Rangarajan, "MIDAS: Empowering 802.11ac Networks with Multiple-inout Distributed Antenna Systems," in *Proc. ACM CoNEXT*, 2014.