Geo-fencing: Confining Wi-Fi Coverage to Physical Boundaries

Anmol Sheth[1], Srinivasan Seshan[2], and David Wetherall[1,3]

[1] Intel Research, Seattle
[2] Carnegie Mellon University
[3] University of Washington

Abstract. We present a means of containing Wi-Fi coverage to physical boundaries that are meaningful to users. We call it *geo-fencing*. Our approach is based on directional antennas, and our motivation is to provide wireless access and privacy models that are a natural fit with user expectations. To evaluate geo-fencing, we use measurements from an indoor testbed of Wi-Fi nodes and APs with electronically-steerable directional antennas. We find that by combining directionality, power control and coding across multiple APs, we are able to successfully confine Wi-Fi coverage to clients located within target regions of varying shapes and sizes; we can select between nodes located as close as five feet from each other.

1 Introduction

Local wireless data communications, exemplified by Wi-Fi, are rapidly spreading beyond mobile computers to everyday consumer devices such as cell-phones, personal health monitors and digital cameras. Thus, users may have many wireless devices that they wish to connect to different wireless networks in various settings. Unfortunately, this is burdensome with current usage models because usability is in tension with access and privacy needs.

Current wireless usage requires that the user select which wireless network to use and provide credentials or other key information. The underlying reason for these requirements is that, unlike wired networks, wireless networks lack physical boundaries that are meaningful to users. Their extent is defined by RF propagation, and this creates an inherent disconnect between the users' view of where Wi-Fi service should be available and the actual service area. Since wireless signals go through walls, it is necessary to select which network is intended to provide service in a given location versus other networks that happen to overlap that location. Since wireless signals can be received by parties in nearby locations, it is necessary to encrypt communications to provide confidentiality. This is done with standard mechanisms such as Wi-Fi Protected Access (WPA and WPA2) [1].

We are exploring a different means of using wireless networks based on confining the Wi-Fi service areas to a well-defined physical region. This model, which we call *geo-fencing*, is motivated by the issues described above as well as user

H. Tokuda et al. (Eds.): Pervasive 2009, LNCS 5538, pp. 274–290, 2009.

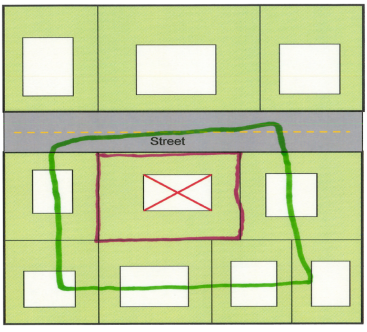


Fig. 1. Representative diagram drawn by a Wi-Fi user from the general public that shows his/her perceived Wi-Fi service area (green) and the smaller desired service area (magenta) for his/her home Wi-Fi network

perceptions of wireless networks. Both can be seen at play in Figure 1, which shows a diagram drawn by a participant in a user study that we conducted [2]. It shows the extent of perceived and desired Wi-Fi coverage for the participants' home network. Interestingly, the perceived coverage follows unrealistic, rectilinear boundaries and shows that users often lack a reasonable understanding of wireless behavior. Of particular interest is the desired coverage, which maps directly to a geographic boundary – the property line. This is an intuitive boundary for Wi-Fi service areas in the same way that rooms are an intuitive boundary for social privacy. We note that this view is similar to the Virtual Walls [3] framework for wireless privacy, which extends the metaphor of physical walls to virtual pervasive environments. Results of a user study suggests that it is easy to understand and use.

With geo-fencing, access is simplified because clients can be authorized to obtain basic connectivity simply by being inside the known region in the same way that, e.g., the users of a conference room are authorized to use the projector in the room. Similarly, access can be revoked as soon as clients leave the region. All of this can be done without involvement of the device owner or the wireless service provider because they do not need to set up cryptographic keys. Privacy is strengthened because information cannot be received by standard clients even in encrypted form beyond the target region. This is valuable because even with encryption, (i.e. WEP/WPA), users may be identified by observing network management traffic that is sent in the clear [4], and knowledge such as applications and even the name of the movie being streamed can be gleaned from side-channels such as packet lengths and timings [5]. Additionally, cryptographic mechanisms are cumbersome to use in relatively unmanaged environments, such as the home and Wi-Fi hotspots intended for a changing customer base. As a result many of these settings forego encryption.

The focus of this paper is to assess how well we can realize the geo-fencing model in practice. Our approach is to use multiple access points (APs) equipped with electronically steerable directional antennas as well as transmit power

control. The intuition is that coverage can be controlled by adjusting the orientation and transmit power of the directional antenna to focus signals on the intended area, and by tying connectivity to the intersection of the signals from multiple APs. This is an approximation because it is not possible to precisely confine wireless signals to arbitrary regions in real-world settings without artificial impediments like Faraday cages. Thus the security aspects of our approach should be interpreted as light-weight access control that significantly raises the bar for devices with commodity hardware, including omni-directional antennas, but will not defeat sophisticated attackers with bulky, high-gain antennas. Despite this limitation, we expect that geo-fencing will be sufficient by itself in many deployments, or can serve as the foundation of hierarchical mechanisms that provide defense-in-depth when stronger security is needed.

We report on an experimental study of geo-fencing run on an office testbed of 802.11b/g nodes with 2.4 GHz steerable directional antennas that play the role of APs and clients. We assess several approaches to orient the antennas and choose transmit power levels, from measurement-based fingerprinting to heuristics based on the angle of arrival (AoA) as estimated by the directional antennas. Finding the most effective configuration is a key challenge because the RF environment of an indoor setting, especially with multi-path interference, affects the directionality of the antennas. Nonetheless, the patterns provide sufficient isolation in gain to be able to confine coverage to desired regions of varying shapes and sizes. Our measurements show that with three directional antennas, geo-fencing can isolate regions of different shapes and sizes ranging from a small desk area of 5 feet $\times$ 5 feet to regions of large room sizes of 25 feet $\times$ 20 feet. Geo-fencing is able to successfully isolate individual clients located 5 feet away from the target client in our 50 feet $\times$ 30 feet testbed. For regions defined by a single target client, geo-fencing limits the maximum packet reception rate measured outside the target region to 50% while providing >90% packet reception to the target client. These measurements suggest that geo-fencing can be realized as a novel physical layer mechanism.

The rest of the paper is organized as follows. In Section 2, we present the requirements for the geo-fencing mechanism and our approach. We describe our testbed in Section 3. Section 4 then describes a measurement study of indoor directional antenna behavior. We use these results to sketch a geo-fencing design in Section 5. We evaluate this design using measurements in Section 6. We present related work in Section 7 and conclude in Section 8.

2 Goals and Approach

Geo-fencing enables deployment scenarios that would otherwise be cumbersome to achieve. For example, consider the scenarios where a public library or coffee shop wishes to provide Wi-Fi service to all patrons while they are within the facility, but wishes to deny service when they leave. In this section we list the goals that geo-fencing should meet to enable such scenarios and the approach.

2.1 Goals

Granularity and Region Definition. Providers should be able to confine transmissions to regular shaped regions that range from small room-sized regions to large areas as entire library or cafe. Providers should also be able to change the boundary definitions of the region as need changes.

Region Selectivity. Regions should be well-defined and client devices more than a few feet outside the defined regions should not be able access the network. While 0% packet reception outside of the region and 100% packet reception rate inside the region would be ideal, it cannot be practically achieved. Measurement studies of TCP [6] and UDP based applications, like Skype [7], show that these applications are unusable beyond a link layer loss rate of $> 25\%$. Based on these observations, we desire an absolute link layer packet reception rate threshold of $<70\%$ ($> 30\%$ loss) outside the region and a threshold of $>90\%$ ($< 10\%$ loss) within the region.

Manageable Infrastructure Overhead. We allow geo-fencing to take advantage of a larger number of APs to limit the region coverage more accurately. However, the system should not require an excessive (> 5) number of APs.

Client Compatibility. Our goal is to maintain compatibility with existing mobile client hardware. This means that we assume that only APs have directional capability.

2.2 Approach

While these goals are simple to state, they are challenging to achieve because of the realities of RF propagation. Coverage regions are irregular even with omni-directional antennas. This is because of signal reflections and other RF effects such as scattering that are significant in indoor environments and generally unknown a priori. Directional antennas have not been widely used indoors because their directionality is significantly degraded relative to outdoor settings. Nonetheless, we believe that the indoor use of directional antennas is valuable if their radiation pattern is adapted based on measurements of the environment.

Our approach is to use a distributed set of APs with directional antennas. Figure 2 shows an overview of our approach. AP1 and AP2 are Wi-Fi APs equipped with electronically steerable directional antennas that are configured to form a controlled signal overlap of their radiation patterns in the desired region. The signal overlap is formed by collecting measurements of packet reception rates from the desired region for different antenna configurations. By coding Wi-Fi frames across the two APs, successful packet recovery is restricted only within the region formed by the intersection of the two patterns.

To see why this approach may be possible, consider a simplified view of the capabilities of directional antennas. First, note that wireless radios have a narrow *transition range* ($< 5dBm$) below which no packets are received, and above which packets are received with near certainty. Second, the primary lobe of the antenna pattern can be represented as an isosceles triangle, as seen in Figure 2, and the

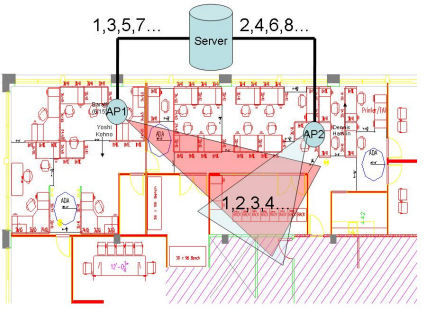


Fig. 2. Geo-fencing approach to confine Wi-Fi coverage to a specified region

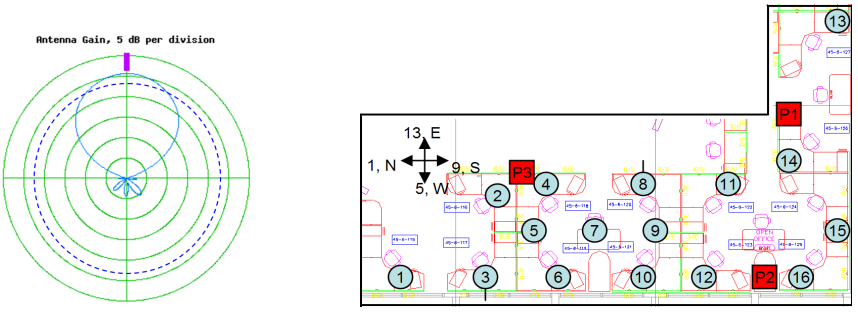
secondary lobes of the radiation pattern are negligible. Third, the size of this triangle can be varied using fine grained transmit power control and the triangle can be rotated around its primary vertex with an arbitrary granularity.

Given this view, a minimum of two directional antennas are required to confine coverage to a target area. This can be done by varying the transmit power and beam rotation so that the intersection of the antenna patterns forms a region where the signal from each antenna is above the transition range. For example, a narrowly defined region can be created by overlapping any two vertices, or the edge of one triangle with the vertex of the other. With this technique receivers do not require special hardware.

3 Testbed Description

We use the Phocus Array [8] electronically steerable directional antenna system for our experiments. Figure 3(a) shows the sample directional and omni-directional antenna pattern generated by this system. The directional antenna isolation is measured as the difference in gain between the main lobe and largest secondary lobe of the antenna radiation pattern. The antenna isolation in our system is 20 dB, and thus, the secondary lobes can be ignored so that the antenna pattern is modeled as an isosceles triangle. The antenna pattern can be electronically steered in 360° range with an angular granularity of 22.5°. Thus there are a total of 16 states and each pattern overlaps the adjacent pattern by 22.5°. The beamwidth of an antenna is defined as the angular separation between two identical points on opposite sides of the pattern's peak gain value. The Half Power Beam Width (HPBW) of the antenna system is 45°. Thus, there are only two states on either side of the antenna state with the peak gain which have a gain above the $(peak\ gain - 3dB)$ threshold.

An important point to note is that the peak gain of the antenna in directional mode is only 3-4 dB greater than the gain in omni-directional mode. That is, the antenna system does not so much boost gain in the target region as it sharply attenuates gain in the undesired region. This property is well suited for the geo-fencing application as it reduces the extent to which secondary lobes are formed by reflections of the wireless signal.



(a) (b)

Fig. 3. Figure (a) shows the directional and omni-directional antenna patterns. The scale is 5 dB per division with the origin at -5 dB. Figure (b) shows the layout of the indoor testbed with Wi-Fi nodes (circles) and steerable directional antennas (squares).

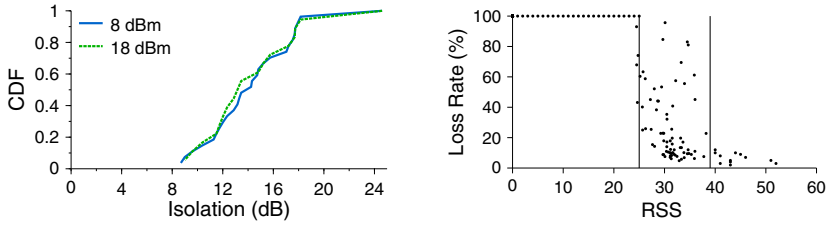
In addition to APs equipped with the steerable directional antennas, we use single board computers as sensors to gather measurement data. Each Wi-Fi sensor is equipped with an Atheros 802.11a/b/g wireless interface and omni-directional antenna. The stock Madwifi Linux driver was modified to log per packet statistics such as Received Signal Strength (RSS), and to measure the Packet Reception Rate (PRR) across time intervals by measuring gaps in the sequence numbers.

The floor plan for our testbed is shown in Figure 3(b). This testbed was deployed on one floor of size 50 feet × 30 feet in a typical office environment and consisted of 16 sensors (circles) and 3 directional APs (squares). The map also shows the antenna orientation states corresponding to the four primary directions. All three directional APs were oriented facing north. We deployed a sensor in each employee cubicle to provide high spatial resolution for our measurements. The average distance between adjacent sensors was 5 feet. The path between the sensors and APs was obstructed by cubicle walls, cabinets and other hardware equipment and most of the sensors do not have direct line of sight to the APs.

4 Characteristics of Directional Antennas

The key challenge in getting geo-fencing to work is to handle realistic wireless environments. The four primary characteristics of directional antennas that we depend on for geo-fencing are:

– *Antenna isolation:* This allows the antenna to selectively provide coverage between two regions by steering the antenna main lobe away from the undesired region and toward the target region. For geo-fencing to be effective, the antenna isolation should be greater than the transition range — the range below which no packets are received, and above which packets are received with near certainty.



(a) (b)

Fig. 4. Figure (a) shows distribution of the isolation measured across all the nodes in the testbed. Figure (b) shows the transition region for sensor 5.

- *Beamwidth:* The beamwidth of the directional antenna pattern directly impacts the base of the triangle pattern. With coarse grained control over antenna orientation, a wide beamwidth limits the smallest size of the regions that can be formed.
- *Scaling of antenna pattern:* Transmit power control should allow scaling of the triangle pattern to confine service to regions of different sizes.
- *Stability of antenna pattern:* The antenna patterns and the corresponding PRR should be stable over time and not be sensitive to mobility of people and objects in the environment. This directly impacts region selectivity without requiring frequent realignment of the antenna patterns.

To study these characteristics in our testbed, we gathered measurement data across all 16 sensors while transmitting from the three directional transmitters. The antenna radiation pattern was rotated across all 16 states sequentially and broadcast traffic was generated at each antenna orientation state for 10 seconds. The isolation of the directional antenna is measured at every sensor location by recording the maximum and minimum RSS across the 16 antenna orientation states.

4.1 Directional Antenna Isolation

Previous measurement studies [9] show that the transition range, in absence of external interference and multipath, is 5 dB. Clearly, an isolation of 20 dB of the directional antenna radiation pattern (Figure 3(a)) should be sufficient.

Figure 4(a) shows the distribution of the antenna isolation measured across all the sensors in the testbed for two different transmit power levels at the APs (18 dBm and 8 dBm). The figure shows that there is a wide variation (8 to 24 dB) in the measured isolation across the distributed sensors. The median isolation is reduced from the expected 20 dB to 12 dB. The figure also shows that the distribution of isolation does not change for different transmit power level settings at directional APs as the RSS patterns scale proportionally with the transmit power level.

Figure 4(b) plots the packet loss rate (i.e., 1− PRR) measured at sensor 5 during each 10 second measurement against the average RSS of the received

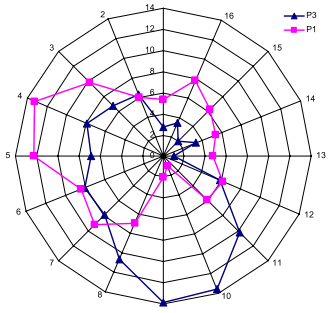


Fig. 5. Antenna radiation pattern of P1 and P3 measured at sensor 11

packets. The two vertical lines demarcate our estimate of the transition range. The transition range is bounded by a loss rate less than 10% to the right of the range, and a loss rate of greater than 90% to the left of the range. In this case, the width of the transition range is 14 dB. The average transition range measured across all the sensors in our testbed was 10 dB.

While the median isolation is only 2 dB higher than the average transition range width, the variability of the isolation achieved from the distributed antennas is sufficient to provide selective coverage between two regions.

4.2 Directional Antenna Beamwidth

Our measurements show that indoor multipath significantly increases the beamwidth of the pattern and also introduces large secondary lobes due to strong reflectors like metal cabinets in the environment. Figure 5 shows the antenna pattern measured by sensor 11 from antenna P1 and P3. The linear axis is in dB with 2 dB per unit. The radial axis represent the 16 possible orientations of the antenna with increments of 22.5° in counter-clockwise direction. For both the directional APs, the peak RSS is measured when the transmitter is pointing its main lobe directly at the receiver. The antenna radiation pattern measured at the receiver show that along with the main lobe, large secondary lobes are also formed due to multipath reflections. The patterns are also specific to the path between the transmitter and receiver as the secondary lobes are different for the two directional transmitters. Across all nodes in the testbed, the number of states that measure a receive gain above the half power threshold ($peak\ gain - 3dB$) ranges from 3 to 15. Thus, antenna orientation in isolation is not sufficient for geo-fencing. In the following section we show how transmit power control can be used to significantly limit the number of antenna states at which successful packet recovery is possible.

4.3 Transmit Power Control

Figure 6(a) shows the effectiveness of using transmit power control to vary the number of states with a high PRR, which directly impacts the angular coverage.

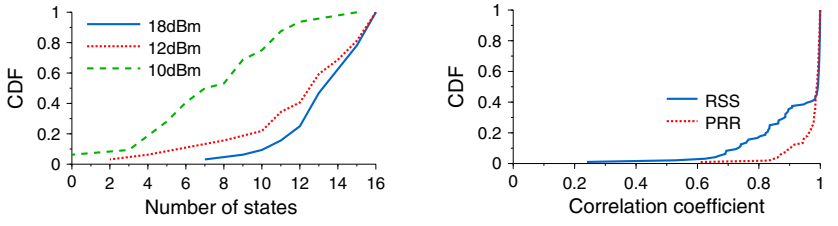


Fig. 6. Figure (a) shows the number of antenna orientation states with PRR > 90% from antenna P2 across all nodes in the testbed. Figure (b) shows distribution of auto-correlation of PRR and RSS patterns across 20 hours. The antenna patterns are stable over long time periods with the median of the distribution close to one.

The figure shows the distribution of the number of antenna states that provide a PRR > 90% from antenna P2 across all sensors in the testbed. We observe that transmit power control significantly reduces the median angular coverage from 12 states at 18dBm to 6 states at 10dBm. Similar distributions were measured for antennas P1 and P3. Thus, despite the wide antenna beamwidths, transmit power control can significantly help in reducing the angular coverage across which packets are received with a high PRR.

4.4 Stability of Antenna Patterns

To understand the temporal stability of the antenna radiation pattern, we measure the antenna's RSS pattern as well as its PRR pattern 10 times over a duration of 20 hours. The transmit power of the three APs was fixed at 12 dBm. To verify that the antenna patterns do not change from one measurement iteration to another, we compute the auto-correlation of the antenna patterns with lag set to one. Hence, for each sensor location we have a set of nine correlation coefficients computed. Figure 6(b) shows the distribution of the correlation coefficients for the PRR patterns and RSS patterns measured at each sensor. The median correlation coefficient is almost one. This shows that the PRR and RSS patterns are stable over long periods of time. This maintains the stability of the geo-fenced region and also reduces the need for frequent antenna alignment.

5 Geo-fencing Technique

Based on our observations, our technique to confine Wi-Fi service to a target region is to align the distributed directional antennas to create controlled overlaps of the transmission patterns and to code packets across the distributed antennas. We define an *antenna configuration* as a combination of the orientation of the main lobe and transmit power level at an AP. The geo-fencing *system configuration* is a combination of antenna configurations across all the distributed APs.

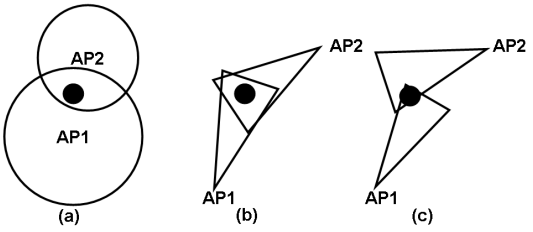


Fig. 7. Overview of three different antenna orientation approaches (a) Omni-directional approach (b) Angle-of-Arrival approach (c) Min-overlap approach.

5.1 Aligning Antenna Patterns

We outline four different approaches for selecting antenna configurations for geo-fencing that we evaluate in the next section. The omni-directional approach (Figure 7(a)) forms the baseline that we use to compare the effectiveness of directional antennas for geo-fencing. The Angle of Arrival (AoA) approach (Figure 7(b)) and the Minimum Overlap heuristic approach (Figure 7(c)) assume triangle-shaped antenna patterns. These approaches require packet reception rate measurements of antenna configurations only from the sensors located within the target region. The dense fingerprinting approach (not pictured) uses measurements from all sensors located inside and outside the target region to optimize the antenna configuration. It provides our ground truth as it accounts for the realistic wireless environment.

Omni-directional approach: The most basic approach is to use omni-directional APs and create controlled overlaps of the antennas patterns by only using transmit power control. Here we find the combination of transmit power levels at the distributed APs which minimizes the maximum PRR at the non-target sensors. The difficulty with this approach is that lack of spatial confinement of the wireless signal and coarse grained transmit power control limits the definition of regions.

Angle-of-Arrival (AoA) approach: A potential approach to select the antenna orientation would be for each AP to form the smallest ideal triangle-shaped antenna pattern and orient the mid-point of the base of the triangle (AoA state) with the target region. Figure 7(b) shows this approach. The mid-point corresponds to the peak gain point of the antenna pattern. The AoA state from an AP to a target region can be approximated by determining the antenna orientation that results in the highest RSS measured by the sensors located within the target region. The smallest antenna pattern can be formed by adjusting the transmit power of the Wi-Fi radio. This approach results in much smaller and controlled overlapping regions than the omni-directional approach.

Minimum Overlap Heuristic approach: For a selected transmit power level, there could be multiple antenna states adjacent (clock-wise and counter clock-wise) to the AoA state that also result in high PRR within the target region. The minimum overlap heuristic, Figure 7(c), aims to minimize the distance of the

target region from the boundary of the edge of the triangle pattern, essentially putting the region at the edge or vertex of ideal triangle of coverage. The heuristic approach selects the same transmit power level as the AoA approach, but selects antenna orientation states that are adjacent to the AoA state within a window of $\pm$ 2 states.

Dense Fingerprinting approach: As the antenna patterns are irregular and specific to the path between the transmitter and receiver, the dense fingerprinting approach is based on measuring the effective PRR across all the distributed sensors for every antenna configuration. These measurements are collected at a central server which then selects the best system configuration that minimizes the peak PRR outside the intended region.

5.2 Coding Packets Across Distributed APs

To make information available only inside the geo-fenced region, we code packets across the set of APs. Sensors located outside the region may then receive signals from some APs, but cannot decode the overall signal because they are unlikely to receive signals from all the APs. Coding may be done either by transmitting independent packets from different APs, or by using a central point to divide the contents of each packet across the AP transmissions. The former is simple, while the latter provides better containment. For our evaluation, we consider a coding technique based on Shamir's *secret sharing technique* [10]. A client at a given location must then receive packet fragments from all APs to decode the complete packet.

6 Evaluation

The primary metric used to evaluate the effectiveness of geo-fencing on our testbed is Packet Reception Rate (PRR) measured at the sensors within the target region and outside the target region. Our goal is to provide a PRR <70% outside the target region (< 90% PRR with retry limit set to 1) and a PRR >90% (>99% PRR with retry limit set to 1) within the region. In the following subsections, we attempt to answer four key questions:

- *Are multiple directional antennas needed to make geo-fencing work and, if so, how many?* We find that directional antennas provide significantly better confinement than omni-directional antennas. With three directional antennas, we can reduce the maximum PRR outside the target region to 50%, which is significantly lower than the 70% threshold.
- *Can geo-fencing support regions of different shapes and sizes?* We show that while the PRR outside the target region rises slightly with region size, geo-fencing is effective for regions ranging from a small desk area of 5 feet $\times$ 5 feet to the size of a large room (20 feet $\times$ 20 feet).
- *How effective are the different antenna alignment approaches?* Our evaluation shows that even the most simple approach based on Angle-of-Arrival

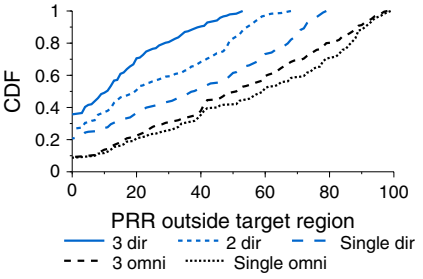


Fig. 8. Isolation achieved with using single/multiple omni/directional antennas.

performs significantly better than the omni-directional approach. The dense fingerprinting based approach, that takes into account measurements from distributed points, provides the best confinement.

– *What type of special hardware does an adversary require to defeat geo-fencing?* Our evaluation shows that geo-fencing denies access to clients with commodity hardware. Clients would need a median omni-directional gain of 8 dB to raise their PRR to 90%, which can only be achieved by bulky high-power antennas. Most mobile clients clients have omni-directional antennas with a gain of 2-3 dB.

To answer these questions, we conducted experiments using the testbed described in Section 3. Traffic was generated at a rate of 1 Mbps UDP CBR broadcast traffic at a fixed modulation rate of 54 Mbps. Packets were coded using the coding scheme described in Section 5.2. Unless otherwise specified, we use the dense fingerprinting approach in all our evaluation and in Section 6.3 we compare the effectiveness of the other approaches.

6.1 Omni-Directional vs. Directional Antennas

We motivate the need to use multiple directional antennas by comparing the isolation achieved with that of omni-directional antennas. The target region is defined by a single sensor. For each sensor, we select the AP and transmit power that achieves greater than 90% PRR at the target sensor but minimizes the maximum PRR measured at all other sensors. We performed this configuration selection for each of the 16 potential sensors, measuring the PRR at all 15 non-target sensors. For both cases, the single best AP and power setting is selected, while for the directional case the best orientation is also considered.

First, we consider one AP. Figure 8 shows the CDF of the PRR measured by all non-target sensors. Even a single directional antenna provide much better confinement of Wi-Fi signals than omni-directional antennas. In the omni-directional case (line "Single omni"), half the sensor locations have a PRR above 70%, while in the directional case (line "Single dir") only approximately 30% of the sensors have a PRR above 70%.

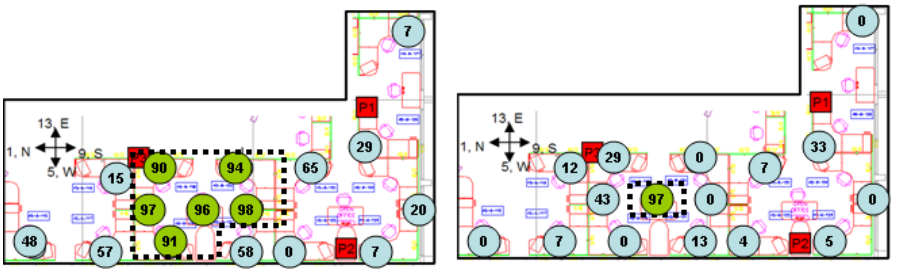
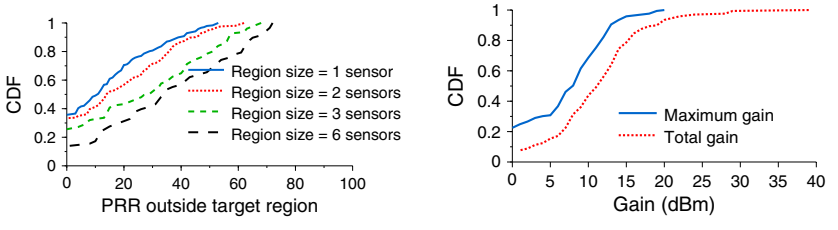


Fig. 9. Target regions of different shapes and sizes can be geo-fenced. Figure shows a target region of the size of a room and a target region of the size of a single desk.



(a) (b)

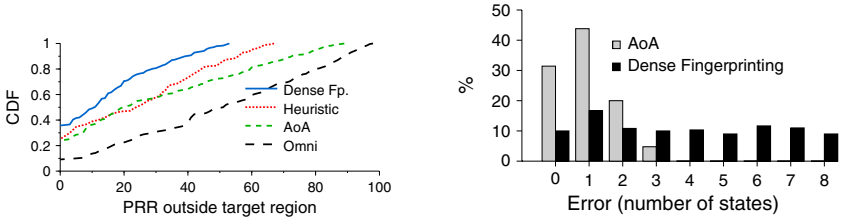
Fig. 10. Figure (a) shows the effectiveness of geo-fencing with increasing region size. Figure (b) shows the distribution of the maximum and total gain required for a node outside the region to receive $> 90\%$ of the packets.

We now consider multiple APs. Figure 8 shows the limitations of coding network traffic across multiple omni-directional APs (line "3 omni"). It only marginally improves isolation over a single omni-directional antenna. The figure also shows a significant improvement when the number of directional APs are increased. With two APs (line "2 dir"), the maximum PRR measured outside the region reduces to 68%. While this is below the required threshold of 70% required for geo-fencing, adding an extra AP reduces the maximum PRR by almost 25% (line "3 dir"). The median PRR is 11% and the maximum PRR is 52%, making geo-fencing significantly more effective.

6.2 Varying Region Sizes and Shapes

We evaluate the effectiveness of geo-fencing regions of different shapes and sizes by increasing the number of sensors in the target region. Target regions of size n sensors are formed by selecting the closest $n-1$ sensors for every sensor in the testbed.

To better understand the shape of the target regions formed, Figure 9 shows examples of geo-fencing a large target region and a small target region (5 feet $\times$ 5 feet). The figure also shows the PRR measured by the sensors located inside



(a) (b)

Fig. 11. Figure (a) shows the effectiveness of the different antenna alignment approaches for three antennas. Figure (b) shows the distribution of the deviation of the antenna orientations selected by the two approaches from the actual measured angles.

and outside the target region. From the figure, we observe that for large target regions, sensors located immediately outside the target region do receive a much higher PRR as compared to sensors located farther away from the target region. Geo-fencing is more effective for smaller target regions and the PRR outside the target region is significantly lower. Figure 10(a) shows the CDF of the isolation achieved for target regions specified by 1, 2, 3 and 6 sensors. Geo-fencing is effective even for target regions sizes consisting of 6 sensors (size of 20 feet $\times$ 20 feet). The median PRR measured is 34% and the maximum PRR outside the target region is below the 70% threshold.

6.3 Antenna Alignment Approaches

In this section, we evaluate the four different antenna alignment approaches described in Section 5 to understand the tradeoff between the different approaches. Figure 11(a) shows the isolation in PRR measured outside the target region for each approach. Geo-fencing using omni-directional APs cannot confine access to Wi-Fi service and more than 30% of the sensors located outside the target region receive a PRR $>$ 70%. Using directional antennas significantly increases the isolation between target and non-target region. The median of the minimum overlap heuristic approach is the same as the AoA approach in our testbed. However, the heuristic approach significantly reduces the maximum PRR from 89% to 67%, which meets the target PRR for preventing access to Wi-Fi service from from outside the target region.

Among the four approaches, the dense fingerprinting approach provides the maximum isolation. To better understand the isolation achieved by the dense fingerprinting approach, we compare the antenna configuration selected by the AoA and dense fingerprinting approach. While there was not a significant difference in the transmit power level between the two approaches ($\pm$ 2 dB), the antenna orientation states differed significantly. Figure 11(b) shows the distribution of the deviation of the antenna orientations selected by the two approaches from the actual measured angle between the AP and client. We observe that the antenna orientations selected by the dense fingerprinting approach deviate significantly from the orientation selected by the AoA approach. More than 35%

of the measurements of dense fingerprinting approach deviate by more than five states (90°) from the AoA state. From this distribution, we conclude that the orientation selected by dense fingerprinting approach is not always a part of the primary main lobe. The antenna orientation selected by the dense fingerprinting based approach often aligns the secondary lobes formed due to indoor multipath reflections along the target region. For example, in Figure 5, for target sensor 11 the dense fingerprinting approach may select the smaller secondary lobe formed between states 11 and 12 instead of the wide main lobe formed between states 2 and 6. Thus, the dense fingerprinting based approach achieves better isolation as it accounts for the RF reflectors present in the indoor environment.

6.4 Antenna Gain Requirements

For an adversary located outside the target region to gain access, it would need a high PRR (>90%) from each AP. The direct approach to do this would be to use a single high gain omni-directional antenna. Our measurement analysis show that the additional gain required is significantly higher than the antenna gain of commodity omni-directional antennas that are embedded in devices like laptops and cell phones.

Figure 10(b) shows the distribution of total gain required, defined as the sum of the gains in each direction, and maximum gain required in any one direction by an adversary. The additional required gain is measured by first estimating the width of the transition range at every sensor location. Based on the measurement of the RSS for the particular geo-fenced configuration, we calculate the additional gain required to achieve a PRR >90% for every non-target sensor. For example, for the transition range shown in Figure 4(b), if the average signal strength measured at the sensor for a particular antenna configuration is 25 dB, then it would require an additional 14 dB gain to achieve a signal strength of 37 dB [1] and a high PRR (> 90%).

From the figure we observe that even for a dense deployment, where the sensors are less than 5 feet away from each other, the median of the total gain required is 11 dB. The median of maximum gain in any one direction is measured to be 8 dB. Thus commodity omni-directional antennas embedded in devices like laptops and PDAs, which have a gain of 2-3 dBi, are not sufficient to gain access.

7 Related Work

Wi-Fi localization-based access control: There are commercial [11] as well as academic research prototypes [12,13] that provide location based access control in Wi-Fi networks. Based on the access control policy and the estimated location of the client, the client is either granted or denied access. Although similar in flavor to geo-fencing, these systems do not confine radio signals to the intended service area, and are consequently prone to eavesdropping. Compared

[1] Atheros radios report signal strength measurements as the measured signal power level above the preset noise floor of -80 dBm.

to the use of dense arrays of low power Wi-Fi APs [14] for customizing service regions, geo-fencing is expected to provide better control over the boundaries of the coverage area with less infrastructure.

Link-layer security mechanisms: Generally, access control in 802.11 networks is achieved by higher layer cryptographic security techniques such as WEP and WPA/WPA2 [1]. However, these techniques are not suited for hot spot style Wi-Fi deployments which require providing temporary access to clients. The primary limitation for the widespread use of these security mechanisms is tedious key distribution, as evidenced by the number of open APs seen in war driving studies [15].

Directional antennas: Unlike static directional antennas that cannot be electronically steered, steerable directional antennas allow dynamic steering of the antenna orientation [8]. Commercial products, like BeamFlex [16], use these antennas and change the antenna orientation on a per-packet basis to improve coverage and performance in wireless LAN deployments. Most cellular network deployments extend the range of the network by using multiple directional antennas co-located at a central tower [17], where each directional antenna services a sector of 90-180°. In [18], the authors use directional antennas to extend the range of a Wi-Fi link to 100-200 kms. The only other work that we are aware of that uses steerable directional antennas is MobiSteer [19]. MobiSteer aims at improving performance of 802.11 links in the context of communication between a moving vehicle and roadside APs.

8 Conclusion

In this paper we present *geo-fencing* — a novel physical layer mechanism that allows users to define service areas of the Wi-Fi access points to a specified physical region. Geo-fencing uses distributed steerable directional antennas to confine Wi-Fi signals to a specified region in an indoor environment. Geo-fencing confines Wi-Fi service areas by making use of a combination of power control, antenna beam orientation at each AP, and coding of packets across the distributed APs. Our measurements show that with three directional antennas, geo-fencing can isolate regions of different shapes and sizes ranging from a small desk area of 5 feet $\times$ 5 feet to regions of large room sizes of 20 feet $\times$ 20 feet. Geo-fencing is able to successfully isolate individual clients located 5 feet away from the target client in our 50 feet $\times$ 30 feet testbed. For regions defined by a single target client, geo-fencing limits the maximum packet reception rate measured outside the target region to 50% while providing >90% packet reception to the target client.

References

1. Edney, J., Arbaugh, W.A.: Real 802.11 Security: Wi-Fi Protected Access and 802.11i, vol. 1. Addison-Wesley, Reading (2001)

2. Klasnja, P., Consolvo, S., Jung, J., Greenstein, B., LeGrand, L., Powledge, P., Wetherall, D.: When I am on Wi-Fi, I am Fearles: Privacy concerns and practices in everyday Wi-Fi use. In: Proceedings of ACM CHI Conference on Human Factors in Computing Systems (to appear, 2009)
3. Kapadia, A., Henderson, T., Fielding, J.J., Kotz, D.: Virtual walls: Protecting digital privacy in pervasive environments. In: LaMarca, A., Langheinrich, M., Truong, K.N. (eds.) Pervasive 2007. LNCS, vol. 4480, pp. 162–179. Springer, Heidelberg (2007)
4. Pang, J., Greenstein, B., Gummadi, R., Seshan, S., Wetherall, D.: 802.11 user fingerprinting. In: MobiCom 2007: Proceedings of the 13th Annual International Conference on Mobile Computing and Networking (September 2007)
5. Saponas, T., Lester, J., Hartung, C., Agarwal, S., Kohno, T.: Devices that tell on you: privacy trends in consumer ubiquitous computing. In: SS 2007: USENIX Security Symposium, Berkeley, CA, USA, pp. 1–16. USENIX Association (2007)
6. Balakrishnan, H., Padmanabhan, V., Seshan, S., Katz, R.: A comparison of mechanisms for improving TCP performance over wireless links. IEEE/ ACM Transactions on Networking 5(6), 756–769 (1997)
7. Sat, B., Wah, B.: Analysis and evaluation of the skype and google-talk voip systems. In: IEEE International Conference on Multimedia and Expo., pp. 2153–2156. ACM Press, New York (2006)
8. Fidelity Comtech, `http://www.fidelity-comtech.com/`
9. Charles, R., Ratul, M., Maya, R., David, W., John, Z.: Measurement-based models of delivery and interference in static wireless networks. In: SIGCOMM 2006: Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications, pp. 51–62. ACM, New York (2006)
10. Shamir, A.: How to share a secret. Communications of the ACM 22(11), 612–613 (1979)
11. Aruba, `http://www.arubanetworks.com/`
12. Bahl, P., Padmanabhan, V.: RADAR: An in-building RF-based user location and tracking system. In: INFOCOM (2), pp. 775–784 (2000)
13. Haeberlen, A., Flannery, E., Ladd, A.M., Rudys, A., Wallach, D.S., Kavraki, L.E.: Practical robust localization over large-scale 802.11 wireless networks. In: MobiCom 2004: Proceedings of the 10th annual international conference on Mobile computing and networking, pp. 70–84. ACM, New York (2004)
14. Chandra, R., Padhye, J., Wolman, A., Zill, B.: A location-based management system for enterprise wireless lans. In: Proceedings of the 3rd ACM/USENIX Symposium on Networked Systems Design and Implementation (NSDI), pp. 115–130 (2007)
15. Bittau, A., Handley, M., Lackey, J.: The final nail in wep's coffin. In: Symposium on Security and Privacy, pp. 386–400. IEEE Computer Society, Washington (2006)
16. BeamFlex, `http://www.ruckuswireless.com/technology/beamflex.php/`
17. Rappaport, T.: Wireless Communications: Principles and Practice, vol. 2, Reading, Massachusetts (2001)
18. Patra, R., Nedevschi, S., Surana, S., Sheth, A., Subramanian, L., Brewer, E.: WiLDNet: Design and implementation of high performance wifi based long distance networks. In: 4th USENIX Symposium on Networked Systems Design and Implementation, pp. 87–100 (2007)
19. Navda, V., Subramanian, A.P., Dhanasekaran, K., Timm-Giel, A., Das, S.: Mobisteer: using steerable beam directional antenna for vehicular network access. In: MobiSys 2007: Proceedings of the 5th international conference on Mobile systems, applications and services, pp. 192–205. ACM, New York (2007)