Physical Pseudo Random Function in Radio Frequency Sources for Security

Di Qiu, Dave De Lorenzo, Sherman Lo, Dan Boneh, Per Enge, *Stanford University*

BIOGRAPHY

Di Qiu is a Ph.D. candidate in Aeronautics and Astronautics at Stanford University. She received her B.S in Aerospace Engineering from University of California, Los Angeles and her M.S. from Stanford University. Her current research interests are location-based security services, signal authentication and fuzzy extractors.

Dr. David De Lorenzo is a research associate at the Stanford University Global Positioning System (GPS) Laboratory. He received his M.S. in Mechanical Engineering from University of California, Davis and his Ph.D. in Aeronautics and Astronautics from Stanford University.

Dr. Sherman Lo is a research associate at the Stanford University Global Positioning System (GPS) Laboratory. He is the Associate Investigator for the Stanford University efforts on the Department of Transportation's technical evaluation of Loran.

Dan Boneh is an associate professor of Computer Science and Electrical Engineering at Stanford University. He is a well-known researcher in the areas of applied cryptography and computer security.

Per Enge is a Professor of Aeronautics and Astronautics at Stanford University, where he is the Kleiner-Perkins, Mayfield, Sequoia Capital Professor in the School of Engineering. He directs the Stanford GPS Research Laboratory.

ABSTRACT

There is tremendous market potential for location-based services (LBS), enabled by the rapid growth in the numbers of personal navigation devices and GPS-enabled mobile handsets. One of the major difficulties for LBS applications is accurate and reliable indoor positioning caused by the difficulty of acquiring and tracking GPS satellite signals in the absence of a clear unobstructed path between the satellite and the user. An alternative approach is to use terrestrial signal sources, such as cellular transmitters, TV or FM broadcast, or Wi-Fi access points. However, it is difficult to achieve accuracies comparable to outdoor GPS, since either the time resolution is inferior (for time-of-arrival methods) or the signal propagation characteristics are unknown or poorly modeled (for received signal strength methods).

Multiple RF signals can be used together to compute a location tag, which is a form of physical pseudo random function. There is no need to synchronize the different systems either on the transmitter or the receiver ends. The usable parameters for location tag generation include signal strength, time-of-arrival, and RF signal phase information. Increased parameter diversity, greater RF signal variety, and more transmitter numbers all increase the information entropy in the derived tags and improve position estimation robustness. The tradeoff of using many location parameters is the reduction in tag reproducibility as RF signals are contaminated by noises and biases.

The analytical results then are applied to real data sets. The use of location tags and a fuzzy extractor is investigated in an office building, a parking structure, and a soccer field on the campus of Stanford University. We show that under ideal conditions, the position tag based approached can achieve an accuracy of 3~6 meters in an indoor environment. Furthermore, the usage of location tags is not restricted to positioning; many other applications include equipment tracking, object identification, and data access control for security services, etc.

INTRODUCTION

In this paper we introduce a tag-based approach for location-based security services. The location dependent parameters extracted from radio frequency (RF) signals are used to derive a location tag, called “geotag” [1, 2]. Unlike other location tracking methods, the technique does not provide accurate estimation of location coordinates, such as latitude, longitude and altitude, from location measurements. We show that there is no need to map location measurements into an accurate global position for a number of location-based services. We use Loran and Wi-Fi as case studies to evaluate and analyze

the performance of location-based system. Loran, which operates at most of the northern hemisphere, has many advantages over satellite-based navigation systems for secure location-based service. To complement Loran for indoor environments, Wi-Fi is chosen as a second case study. Although Wi-Fi was initially designed for communications between electronic devices, the proliferation of Wi-Fi has a growing interest in indoor location-based applications [3]. Accurate tag-approached positioning technology helps support a range of applications, such as people tracking, health care, patient monitoring, emergencies, advertisement, marketing, and security services, etc. In this paper we use security application as example to analyze the performance of geotag.

- *Block-listing of security application*: An example of block-listing application is digital manners policy (DMP). Technologies for DMP [4] attempt to enforce manners at public locations. A DMP-enabled cell phone can be programmed by the phone provider to turn off the camera while inside a hospital, a locker room, or a classified installation. Or the phone can be programmed to switch to vibrate mode while inside a movie theater. Even though these ideas are highly controversial [5], we only focus on the technical aspect of the application in this paper. The device downloads an updated list periodically. When the device encounters a location tag on this blocklist, it turns the camera off. When the device leaves the blocked location the camera is turned back on. Hence, digital manners are enforced without ever telling the device its precise location.

- *White-listing of security application*: location-based access control is a white-listing example. Consider a location-aware disk drive: the drive can be programmed to work only while safely in the data center. An attacker who steals the device will not be able to interact with it. Location-based access control using encryption was studied by Scott and Denning [6] under the name Geoencryption.

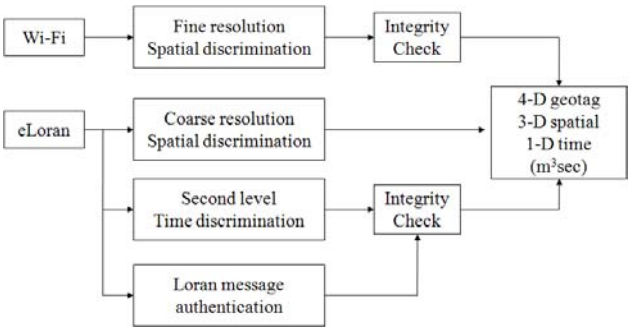

Figure 1. Loran Wi-Fi integration

Loran has many properties that are beneficial to the implementation of the above applications. It is a high power terrestrial signal and easily penetrates buildings and cities, where line-of-sight signals are not available. In addition, enhanced Loran (eLoran) has a data channel, which can carry data and authentication messages. The authentication feature of signals allows receivers to verify the source of the incoming signals and protects against spoofing. The signal attenuation at indoor environments degrades the accuracy and repeatability of geotag. To complement Loran, Wi-Fi is used to improve the spatial discrimination and precision of derived geotag. Figure 1 illustrates the integration of Loran and Wi-Fi geotag system. Loran signal gives coarse resolution, time message provides additional dimension in geotag generation, and authentication message ensures the integrity of Loran signals and protects against spoofing. Thus the generated geotag is four-dimensional. The resolution of Wi-Fi tags is finer in comparison with Loran tags.

The structure of the paper is organized as follows. We first describe system models of geotag for location-based security service and prove that a geotag is a physical pseudo random function. The paper then evaluates the system performance using Loran and Wi-Fi as case studies. An error tolerant algorithm, named fuzzy extractor, which improves the reproducibility of geotag in the presence of noise and biases, is discussed in the following section. Next we show the integration of Loran and Wi-Fi provides more precise location tags. This paper then summarizes and concludes with future directions of the research.

SYSTEM MODELS

Tag Approached Positioning

Secure location-based system works in two steps: calibration and verification, illustrated in Figure 2. The tag approached positioning technique highly depends on the initial calibration phase. This involves one should drive or walk around in the service areas with a location sensor such as Loran receiver or Wi-Fi enabled device. Geotag associated with the calibrated areas are computed based on the recorded location information and stored on a database for future use. The second phase is named positioning or verification phase. A user derives a geotag using received location parameters and matches it with the pre-computed ones on the database. Let T be the geotag derived at calibration phase and T' be the geotag at verification phase.

In this paper we introduce different methods for the geotag generation and the corresponding matching algorithms. The methods differ in the geotag

representation, efficiency in computation and implementation in practice.

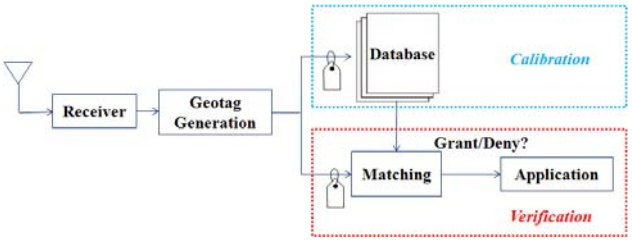

Figure 2. Secure location-based system

The first tag generation algorithm consists of three steps: extracting location-based parameters from the received RF signals, quantizing the parameters with adequate step sizes, and mapping the quantized parameters into a binary string. The binary mapping process can be done using a hash function, which is one-way and collision resistant. Let $x = \{x_1, x_2, \ldots, x_n\}^T$ be the location parameter vector, Δ is the quantization step size vector and the quantized parameter vector is $q_x = \left\lfloor \frac{x}{\Delta} \right\rfloor$. All these vectors have the size n, which is the total number of available location parameters. The matching process only involves the correlation of the new geotag and the previously stored ones.

While the first tag generation algorithm outputs a binary geotag, the second method only takes the extracted location parameters as a geotag $T = x$. This technique is similar to the location fingerprinting except we also use various location dependent parameters other than received signal strength [7]. There are two different approaches for the matching process: deterministic approach and probabilistic approach.

- Deterministic approach: the first deterministic approach is named nearest neighbor method (NMM) [8], which is common technique used for indoor location estimation and pattern matching. The algorithm measures the distance between location vector from verification phase T' and the previously stored vectors on the database. The generalized distance measure D is defined in Equation (1), where w is a weighting factor and p is the norm parameter. For instance, $w = 1$ and $p = 2$ are for the Euclidean distance. Based on the calculated distances between T' and the previously computed Ts, the location tag that gives the minimum distance is picked. It is necessary to set a threshold to guarantee the location is registered at calibration phase. A modification to NNM [9] that uses standard deviation σ of the location parameters is named weighted nearest neighbor method (WNNM). The new distance measure is shown in Equation (2), where C is a covariance matrix.

$$D = \frac{1}{n}\left(\sum_{i=1}^{n} \frac{1}{w_i} | x'_i - x_i |^p \right)^{1/p} \quad (1)$$

$$D^2 = (\vec{x} - \vec{x}')^T C^{-1} (\vec{x} - \vec{x}') \quad (2)$$

- Probabilistic approach: the approach models location tags with conditional probability and uses Bayesian concept to estimate location [8]. At calibration phase, not only the location parameters but also the corresponding standard deviations should be estimated and saved for verifications. Assuming the location parameters have Gaussian distributions, we use the probability density function shown in Equation (3) to compare the calculated likelihoods. The location tag that gives the maximum probability is picked.

$$P = \frac{1}{n} \sum_{i=1}^{n} \left[\frac{1}{\sqrt{2\pi}\sigma} \exp\left(-\frac{(x'_i - x_i)^2}{2\sigma^2} \right) \right] \quad (3)$$

Performance Metrics

The problem of deciding whether the computed geotag is authentic or not, can be seen as a hypothesis testing problem. The task is to decide which of the two hypotheses H_0 (accepting as an authorized user) or H_1 (rejecting as an unauthorized user) is true for an observed location measurement. The system can make two types of errors: 1) mistaking the measurements from the same location to be from two different locations and accepting hypothesis H_1 when H_0 is true, called false reject; and 2) mistaking the measurements from two different locations to be from the same location and accepting H_0 when H_1 is true, called false accept. Both false reject rate (FRR) and false accept rate (FAR) depend on the variations of the location parameters, quality of the location sensor and the step sizes chosen to quantize the parameters. These two types of errors can be traded off against each other by varying the quantization steps. A more secure system aims for low FARs at the expense of high FRRs, while a more convenient system aims for low FRRs at the expense of high FARs.

Physical Pseudo Random Function (PPRF)

By definition [10], a pseudo random function (PRF) is a deterministic function f: $X \rightarrow Y$ which is efficient and computable. It takes two inputs x, $k \in X$. Consider x to be a variable, k be a random seed, $f(x, k) = y$ and $y \in Y$.

In this section we show that the interaction between RF signals and a receiver is a PPRF. We define the inputs are the RF signals from multiple transmitters and the signals are a form of representation of a particular location. The

deterministic function is a physical process to capture and condition the incoming signals, extract the location parameters, and map them into a geotag, which is the output of the PPRF. The random seed can be any randomness in the hardware devices such as antenna and receiver used to complete the physical process.

Some important properties of the derived PRF are efficiency, distinguishability and unpredictability. The physical process that converts RF signals to a geotag is efficiently computable. The second desired feature of location-based PPRF is the distinguishability. The algorithm must be able to generate distinguishable location tags given different input signals. In addition, the derived PPRF is unpredictable at a distance: someone who is twenty meters away from a target location cannot predict the tag at the target. The experimental evidence for this claim was discussed previously in [11].

There are some requirements on the physical system used to generate a geotag. First, the system should be easy to fabricate. This is important because we anticipate a mass production of the system to be deployed in the real world. In addition, the system should be structurally stable. We expect that derived geotag is reproducible and this requires not only the RF signals but also the physical system must remain stable over time.

LORAN AS CASE STUDY

Loran has many characteristics that can be used to generate a robust geotag. First, Loran is a high power, low frequency signal. This means that it is hard to spoof or jam. The signal can reach places such as urban canyons and indoor environments. In addition, it is being modernized to a next generation system known as enhanced Loran (eLoran), which will have a data channel that can carry authentication message and benefit its use for location-based security services [12]. The modernization will also reduce the amount of temporal variation in some of the location-based parameters. Furthermore, Loran uses static transmitters and, as a result, there are many parameters that are location-dependent. Each parameter offers different certain amount of information or potential information density. Parameters with higher density result in higher security levels. The possible useable Loran parameters are *time of arrival* or *time difference* (TOA/TD), *envelope to cycle difference* (ECD), *signal strength* (SS), and *absolute or relative signal to noise ratio* (SNR/ΔSNR).

Loran Geotag Evaluation

In this section we use real Loran data to evaluate the precision and spatial decorrelation of Loran geotag. Precision is defined as the ability of a location parameter to be consistently reproduced. Spatial decorrelation measures how a location parameter varies from one location to another. It is desired to have high precision and high spatial decorrelation for the location parameters.

We selected three different environments to perform the test: parking structure, soccer field and office building. At each location we used multiple test points and collected data for 5 minutes at each test point. An H-field antenna and Locus SatMate receiver were used for the data collection. Locus SatMate receiver averages and outputs LORAN location parameters every minute.

- **Site 1.** The first data set was collected at 21 different test points on the top floor of a parking structure at Stanford University. This place has open sky view and no obstruction from the environments but there are some metal structures nearby. The altitude is relatively high compared with the other two sites. The dimension of the parking structure is approximately 70 x 50 meters.
- **Site 2.** The second data set selected 16 test points in a soccer field. This environment has some obstructions from trees and buildings. The field has a dimension of 176 x 70 meters so the distribution of

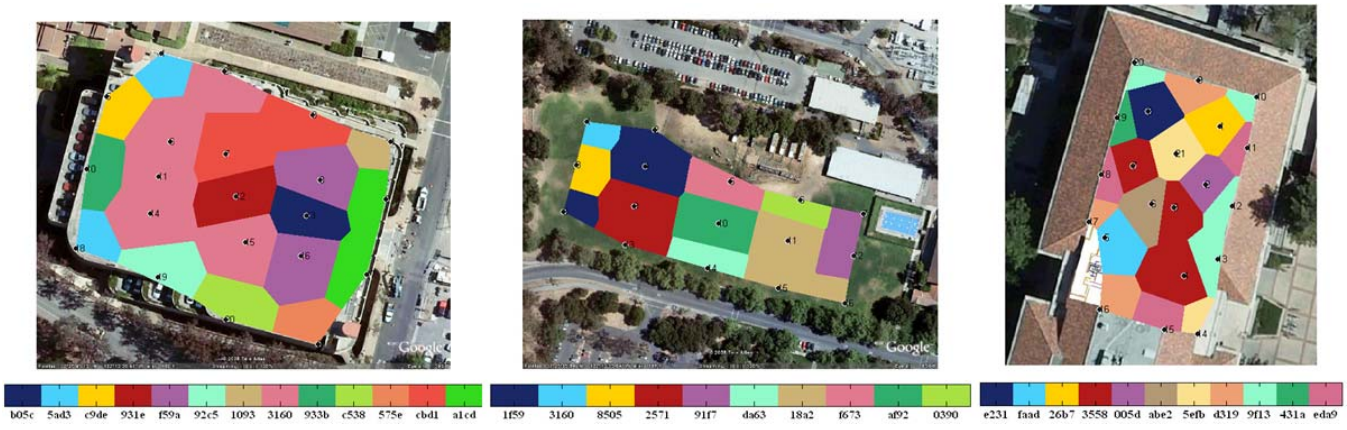

Figure 3. Loran tag: parking structure (left); soccer field (center); office building (right)

the test locations are less dense compared to the other two sites.

- **Site 3.** The third data set, which has 21 test points, was collected on the top floor both inside and outside a four story office building. The concrete building with metal frames attenuates signal strength more but introduces more randomness in the location parameters, which can be beneficial to the computation of location tags.

We used the triple (TD, ECD, SNR) from four stations in the west coast chain (GRI 9940). Quantization steps are chosen based on the measured SNR. Low SNR signals are often attenuated more and pick up more noises. Thus, features from low SNR stations are less consistent and larger quantization steps should be applied. We then create cells and map the tags into the cells accordingly. The color map is superimposed on the Google map. A color bar is used to label the hexadecimals of the first 16-bit of tag. Each black dot together with the numbered label at the center of the cells represents a test location. The visualization of geotag is shown in Figure 3. The averaged cell sizes for the parking structure, soccer field and office buildings are 20 meters, 40 meters and 12 meters, respectively. The estimated cell size is limited to the separations between the test points.

In the case of office building, Satmate receiver was not able to track two low SNR stations: George and Searchlight due to the signal attenuations from walls and other obstructions. Thus the amount of information to form a geotag is reduced. To complement Loran in the indoor environments, we choose Wi-Fi as the second case study.

WI-FI AS CASE STUDY

The increasing deployment of Wi-Fi devices by individuals and organizations in homes, offices, and campuses opens an opportunity for Wi-Fi indoor positioning. Most mobile devices, such as laptops, PDAs, and cellular phones, are equipped with Wi-Fi devices. The infrastructure can be used to provide indoor location-base applications without deploying additional equipment. One drawback of Wi-Fi positioning system is the limited coverage due to the transmitting range of access point (AP). Thus, an integration of LORAN and Wi-Fi produces more robust location tags.

Wi-Fi Signal Characteristics

Many Wi-Fi positioning systems use received signal strength (RSS) and/or medium access control (MAC) address from nearby access points to derive symbolic locations. A symbolic location refers to proximity of known objects or abstract ideas of location [3] instead of physical coordinates such as latitude and longitude. Thus MAC address and RSS can be used location parameters to generate a Wi-Fi geotag.

The data collection equipments consist of a Wi-Fi enabled laptop and a Garmin GPS receiver. A software named WirelessMon is used to periodically scan the environment and record the tracked AP MAC addresses and RSSs to a log file. The software appends the records of latitude and longitude to the log file when the GPS receiver is attached to the Wi-Fi device.

Our first test is to examine the spatial decorrelation and coverage of Wi-Fi APs. Downtown Menlo Park shown in Figure 4 was chosen to perform this test and we drove around in the neighborhood with the Wi-Fi enable laptop and Garmin GPS receiver. The driving paths are plotted in green on the Google map. The AP density in the area is approximately 1155/km^2. To examine the spatial decorrelation of Wi-Fi APs, the center point shown as red marker was picked as a master location. Based on the recorded latitudes and longitudes, we calculated the separations between other point and the center point, and the percentage of APs that are shared with the referent location. As the distance is 200m away from the center

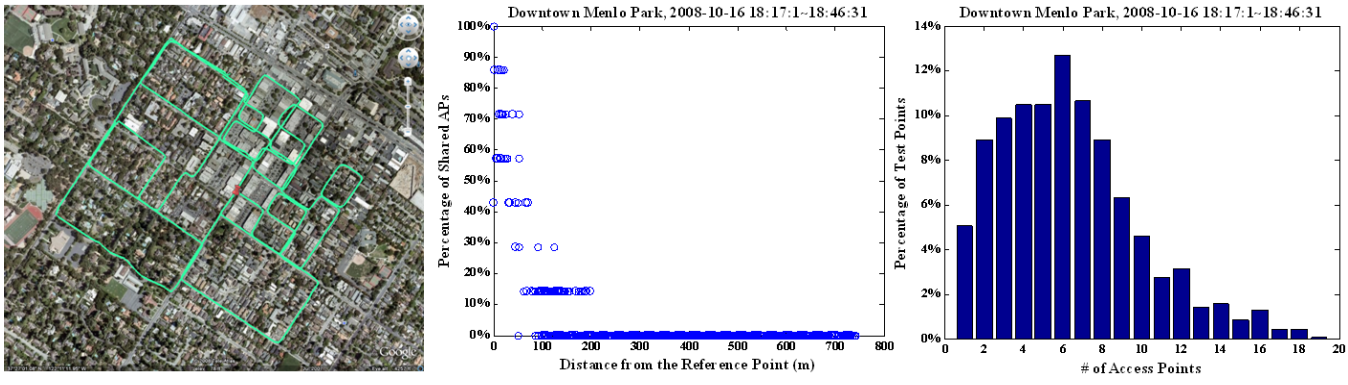

Figure 4. Downtown Menlo Park (left); Spatial decorrelation (middle); AP spatial distribution (right)

point, two locations have no overlap in the tracked APs. Even with 10m separation, the overlap is approximately 86%. Most of the test points tracked above 4 APs according to the histogram shown on the right of Figure 4. The available APs +provide more parameters in the geotag computer and high spatial discrimination.

Residential Area

Next we study the Wi-Fi signal properties using measurements collected in residential area for 8 hours shown in Figure 5. The AP with the strongest RSS represents the connected node. The RSS measurements have a temporal variation in the range of 10 dBm or less. Generally speaking, stronger APs have less temporal variations in RSS. Both thermal noise and multipath contribute to the temporal variations of the measured RSS. The multipath fading effect is the result of destructive or constructive combination of multiple signals at a receiver, and causes the signals fluctuate around a mean value. Multipath is a common error in indoor environments due to signal refraction, reflection and diffraction from the environments.

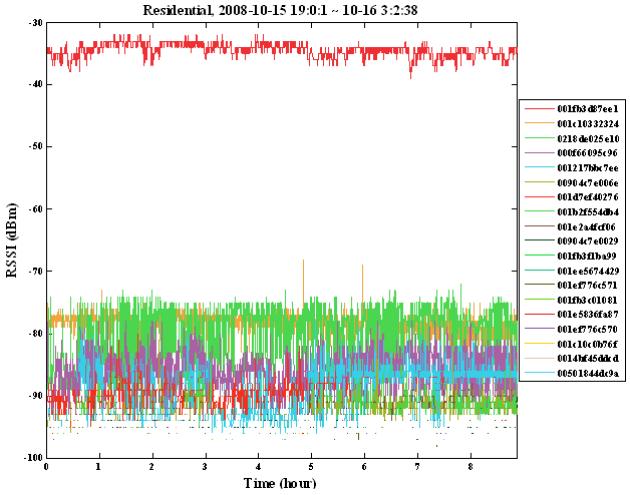

Figure 5. Wi-Fi RSS measurements in residential area

Signal strength is a common metric to determine propagation distance from a radio source in many RF based systems. A propagation model is needed to convert the RSS into distance. To characterize this, we collected RSS readings for 3 minutes at varying distance from an AP. The left plot in Figure 6 illustrates the Wi-Fi RSS as a function of distance between the observed AP and the receiver. Each dot represents the mean of the collected RSS measurements at the particular test point. We observe a correlation between RSS and the distance. In practice, it is difficult to come up a model that suits for all the environments, especially indoors. The propagation is not necessarily linear. The signal attenuation can be based on path propagation, reflection, diffraction, diffusion and transmission through various materials [13]. The sum of all the components is taken to get the RSS. Moving objects like people can cause not only attenuation but also fluctuation. The conversion from RSS to propagation distance works only when the signal strength attenuation is predictable and there is no extra attenuation from the composites of walls, structure of buildings, moving objects and multipath effects, etc. For instance, the attenuation factor is different for brick walls, wood and glass. A structure with different materials or composites complicates the modeling of the attenuation factor.

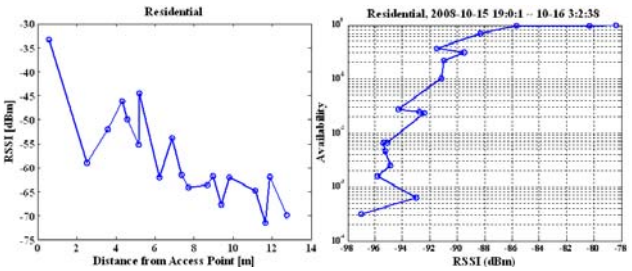

Figure 6. Residential: RSS as a function of distance between AP and receiver (left); AP availability as a function of measured RSS (right)

The availability or response rate of an AP is defined as the percentage of time that a receiver is able to track it. A set of Wi-Fi scans from an AP are collected and the availability can be computed based on the fraction of times that the AP is observed and the total number of scans. The right plot in Figure 6 illustrates a strong correlation between the AP availability and RSS. The AP availability can be location dependent if there is no extra attenuation. As the receiver is close to the AP, it is expected the availability is high. As the receiver moves away from the AP, there are more attenuations and the availability becomes low. However, the accuracy of availability measure depends on the total number of scans and the quality of the Wi-Fi enabled device. More scans will provide better estimation and the quality of Wi-Fi enabled device also plays an important role.

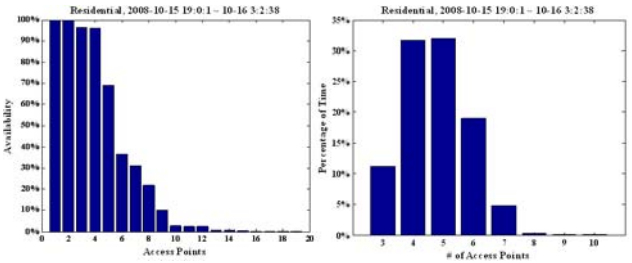

Figure 7. Residential: availability histogram (left); availability of number of APs tracked (right)

The left plot in Figure 7 illustrates the availability of all the APs tracked during the 8 hours. The first four strongest APs have relatively high availability. If more than 4 APs are used to compute a geotag, there is no

guarantee that the geotag is reproducible at a latter time. The right plot shows the AP density distribution, which is equivalent to the geotag FRR with the corresponding number of APs.

The FRR and cell size of the quantized space can be traded off against each other by varying the number of APs used to generate a geotag, illustrated in Figure 8. More number of APs provides high spatial decorrelation or discriminations, thus a small quantized space can be achieved. However, increasing the number of APs also increases the likelihood to use low availability AP and lowers the reliability of the system. For instance, with 8 APs, we can achieve a cell size of 3.5 m but the very poor reproducibility in the derived geotag. In this scenario, an optimal number of APs for geotag generation should be 4. With 4 APs, we can achieve reasonably low FRR and small cells size.

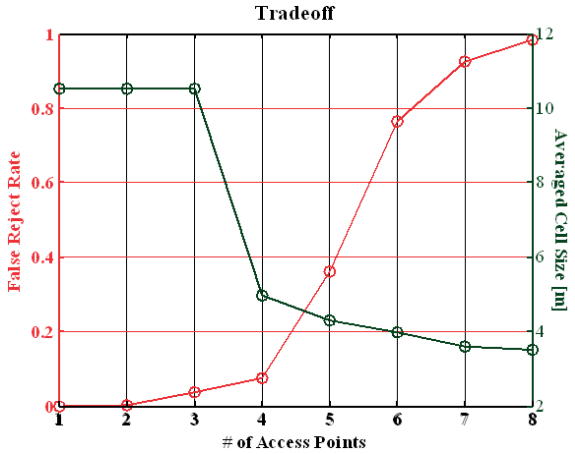

Figure 8. Residential: Tradeoff between FRR and cell size

Office Building

A second data set was collected in an office building for 4 hours. This is the same office building where we collected Loran signals. The RSS measurements fluctuate more in this environment in comparison with the residential area as there are more attenuations and signal blockage due to moving people in the office. Human body is composed of large percentage of water, which has a resonance frequency at 2.4 GHz and greatly attenuates the Wi-Fi signals [3].

The visualization of the quantized cells is shown in Figure 9. The location tags are computed using 4 APs and the averaged cell size is approximately 6m. The availability of observed APs is shown in the middle of Figure 9. Although the total number of APs tracked in the office is more than that in the residential area, the availability of tracked APs is poor. Same tradeoff analysis is conducted to examine the optimal number of APs used to generate a geotag. The FRR is high in comparison with the residential FRR. To achieve a reproducible tag, only the AP with the strongest RSS can be used. Even with 2 APs, the FRR is high, 0.15. The average cell size is reduced from 11m to 6m as the number of APs increase from 1 to 8.

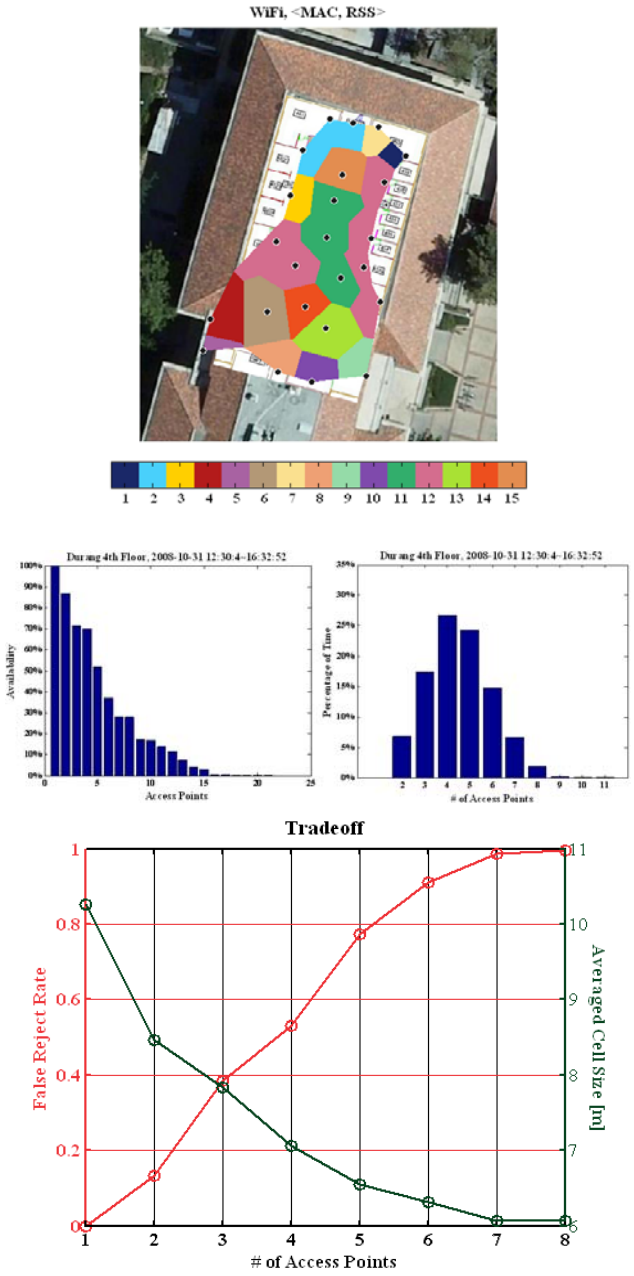

Figure 9. Performance analysis in the office building

Fuzzy Extractors

To achieve high geotag reproducibility, error-tolerant algorithm, named fuzzy extractor, can be applied to location data. By definition, it is an error tolerant algorithm to extract desired information from noisy input [14]. We developed both Euclidean metric and Hamming metric fuzzy extractors based on the error patterns of

location data. Euclidean metric fuzzy extractor can be used for the errors introduced by random noise, seasonal bias and quantization error while the Hamming metric fuzzy extractor is for the case of offline transmitter or missing parameters. The details of fuzzy extractor constructions are discussed in [15]. We show the improvement in Wi-Fi geotag FRR using secret sharing based Hamming metric fuzzy extractor. The key idea of this fuzzy extractor construction is to use a subset of registered APs at calibration phase to reproduce the geotag. The number of APs in the subset is a design parameter and can be chosen by a user at the calibration phase.

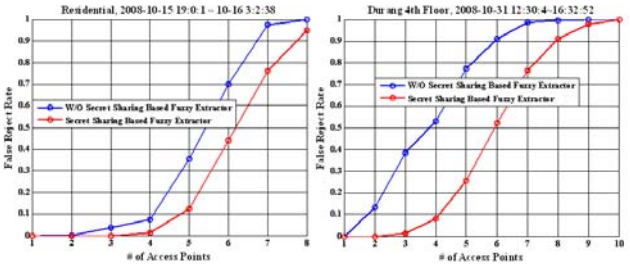

Figure 10. Performance with fuzzy extractor

The performance comparison with and without using a fuzzy extractor is shown in Figure 10. The performance in the residential area is shown on the left while the right plot indicates the estimated FRR in the office building. The reproducibility of Wi-Fi geotag without and with using fuzzy extractor is illustrated as blue and red colors respectively. We note a dramatic improvement in the geotag FRR with the Hamming metric fuzzy extractor. For instance, with 4 APs, FRR is reduced by 83% for the residential area and 85% for the office building.

Loran and Wi-Fi Integration

The integration of LORAN and Wi-Fi produces better precision in the location tags as more parameters contribute high spatial discriminations. In addition, increased parameter diversity, greater RF signal variety, and more transmitter numbers all increase the information entropy in the derived tags and improve position estimation robustness. There is no need to synchronize the different systems either on the transmitter or the receiver ends. The performance of LORAN and Wi-Fi integration is illustrated in Figure 11. The MAC address and RSS from 4 Wi-Fi APs are used in generating the tags. The Loran location parameters are TD, SS and ECD from four west coast stations. The resulted quantized cells have a minimum size of 2.7m and average size of 6m. The average cell size is reduced by 32% with the addition of Wi-Fi signals.

CONCLUSION

We proposed Loran and Wi-Fi integration for location-based security services: in which location is used as a validation to allow or restrict certain action in security applications. Verification tags are computed from location based parameters extracted from RF signals. This location-based service can be applied to many applications, such as DMP, inventory control and data access control.

The properties of Loran signal can benefit the design of location-based security services and tag-approached positioning. Wi-Fi signal provide a more spatial variations to Loran in the indoor environments. We show that the improvement in the quantized cell size is approximately 32%. Fuzzy extractors should be applied to achieve a reproducible tag on both Loran and Wi-Fi signals.

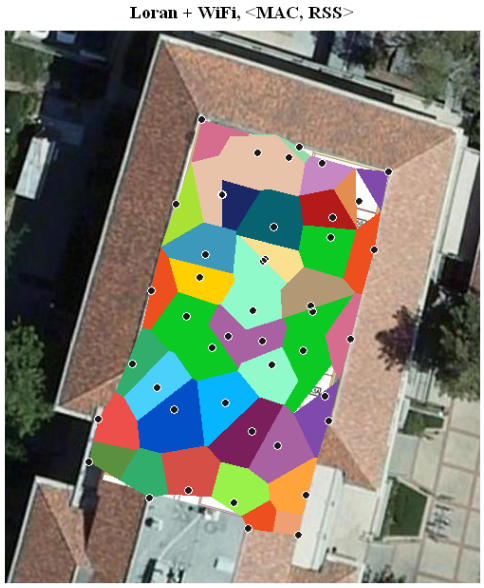

Figure 11. Loran and Wi-Fi integration

ACKNOWLEDGMENTS

The authors would like to thank Mitch Narins of the FAA, Loran Program Office for supporting this effort. In addition, we would like to thank US Coast Guard (USCG) Loran Support Unit (LSU) for the use of their equipment in our testing.

REFERENCES

[1] D. Qiu, S. Lo, and P. Enge, "Geoencryption Using Loran", *Proceeding of ION NTM 2007*.

[2] D. Qiu, "Security Analysis of Geoencryption: A Case Study using Loran", *Proceeding of ION GNSS 2007*.

[3] K. Kaemarungsi, "Design of indoor positioning systems based on location fingerprinting technique," Ph.D. Thesis, 2005.

[4] J. Hruska. "Microsoft patent brings Miss Manners into the digital age". June 11, 2008.
[5] B. Schneier. "Kill Switches and Remote Control". A blog covering security and security technology. July 1, 2008.
[6] L. Scott and D. Denning, "Location Based Encryption & Its Role In Digital Cinema Distribution", *Proceedings of ION GPS/GNSS 2003*, pp288-297.
[7] P. Bahl and V. N. Padmanabhan, "RADAR: An in-building RF-based user location and tracking system," *IEEE infocom 2000*, Tel Aviv, Israel, 26-30 Mar 2000, vol. 2,pp. 775-784.
[8] T. Roos, P. Myllymaki, H. Tirri, P. Misikangas, and J. Sievanen, "A probabilistic approach to WLAN user location estimation," *International Journal of Wireless Information Networks*, vol. 9, no. 3, pp. 155-164, July 2002.
[9] S. Saha, K. Chaudhuri, D. Sanghi, and P. Bhagwat, "Location determination of a mobile device using IEEE 802.11b access point signals," *IEEE Wireless Communications & Networking Conference (WCNC)*, New Orleans, Louisiana, US, Mar 16-20 2003, vol.3, pp. 1987-1992.
[10] Bruce Schneier, Applied Cryptography, John Wiley & Sons, Inc. 1996.
[11] D. Qiu, S. Lo, and P. Enge. "A Measure of LORAN Location Information", *Proceeding of ION PLANS 2008*.
[12] International LORAN Association (ILA), "Enhanced LORAN (eLORAN) Definitions Document", January 2007. Available at the ILA website.
[13] Y. Cheng, Y. Chawathe, A. LaMarca, and J. Krumm, "Accuracy characterization for metropolitan-scale WiFi localization," *Proceedings of Mobisys 2005*.
[14] Y. Dodis, L. Reyzin, and A. Smith. "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data". *Eurocrpt'04*, vol. 3027 of LNCS, pp523-540. Springer-Verlag, 2004
[15] D. Qiu, D. Boneh, S. Lo and P. Enge, "Robust geotag generation from noisy location data for security applications," *Proceeding of ION ITM 2009*.