Temporal Link Signature Measurements for Location Distinction

Neal Patwari, *Member*, *IEEE*, and Sneha K. Kasera, *Member*, *IEEE*

Abstract—We investigate *location distinction*, the ability of a receiver to determine when a transmitter has changed location, which has application for energy conservation in wireless sensor networks, for physical security of radio-tagged objects, and for wireless network security in detection of replication attacks. In this paper, we investigate using a measured temporal link signature to uniquely identify the link between a transmitter (TX) and a receiver (RX). When the TX changes location, or if an attacker at a different location assumes the identity of the TX, the proposed location distinction algorithm reliably detects the change in the physical channel. This detection can be performed at a single RX or collaboratively by multiple receivers. We use 9,000 link signatures recorded at different locations and over time to demonstrate that our method significantly increases the detection rate and reduces the false alarm rate, in comparison to existing methods. We present a procedure to estimate the mutual information in link and link signature using the Edgeworth approximation. For the measured data set, we show that approximately 66 bits of link information is contained in each measured link signature.

Index Terms—PHY layer, radio channel, measurements, location distinction.

1 Introduction

Location distinction is critical in many wireless network situations, including motion detection in wireless sensor networks, physical security of wireless objects with wireless tags, and information security against replication attacks.

Wireless sensor networks. Sensor location must be associated with measured sensor data and is needed in geographic location-based routing methods. Location estimation must be done in an energy efficient manner, especially for networks of sensors with small batteries that must last for years. The energy required to estimate location must be expended when a sensor node moves, however, energy-efficient localization systems shouldn't re-estimate location unless movement actually occurs. This implies that for energy efficiency in location estimation, sensor nodes must detect motion or a change in location.

Active RFID. Active RF tags are used to protect the physical security of objects. Radio frequency identification (RFID) tags are becoming a replacement for bar-codes and a means for improved logistics and security for products in stores and warehouses. Active RFID is desired for its greater range, but a tag must be in range of multiple base stations (BS) in order to be able to estimate its location. Location distinction is critical to provide a warning and to be able to focus resources (e.g., security cameras, personnel) on moving objects.

Secure wireless networks. Wireless networks are vulnerable to medium access control (MAC) address spoofing [13], [6]. As argued in [13], an adversary at a different location can claim to be another node by spoofing its address. One can use traditional cryptography methods to prevent this spoofing. However, these methods are susceptible to node compromise. A good location distinction technique that can distinguish the location of spoofed nodes from the authentic nodes can prevent these attacks.

Surprisingly, existing techniques fail to detect change in position in an efficient and robust manner:

- *Accelerometer Measurements*: Accelerometers detect changes in velocity, and have found application in movement detection [4], [34]. Its additional device cost could be prohibitive for applications such as bar-code replacement. Further, as it would not detect motion from a "sleep" state, an accelerometer needs continuous power, contrary to the low-power requirements of sensor network and RFID applications.
- *Doppler Measurements*: Doppler is the frequency shift caused by the velocity of a transmitter (TX). Doppler measurements, similarly, only detect motion while the device is moving, not after it stops moving, thus transmission can not be intermittent, like a packet radio.
- *Received Signal Strength (RSS) Measurements*: RSS measurements contain information about a link, and are particularly useful when using multiple measurements at different receivers, e.g., the signalprint of [13]. They can be used to detect movement of a TX [38]. However, in the network security application, adversaries can "spoof" their signalprint using array or MIMO antennas which send different signal strengths in the directions of different access points. Moreover, for wireless sensor networks, multinode collaboration is expensive in terms of energy.

- *N. Patwari is with the Department of Electrical and Computer Engineering, University of Utah, 50 S Central Campus Dr. Room 3280 MEB, Salt Lake City, UT 84112. E-mail: npatwari@ece.utah.edu.*
- *S.K. Kasera is with the School of Computing, University of Utah, 50 S Central Campus Dr. Room 3190 MEB, Salt Lake City, UT 84112. E-mail: kasera@cs.utah.edu.*

Manuscript received 15 June 2009; revised 12 Feb. 2010; accepted 23 June 2010; published online 5 Oct. 2010.
For information on obtaining reprints of this article, please send e-mail to: tmc@computer.org, and reference IEEECS Log Number TMC-2009-06-0233.
Digital Object Identifier no. 10.1109/TMC.2010.189.

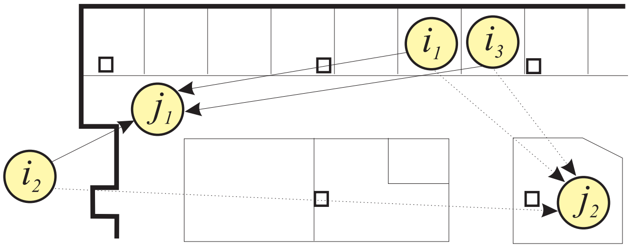


Fig. 1. Receivers j_1 and j_2 receive transmitted packets from transmitters i_1, i_2, and i_3. Each TX i_m sends packets on link (i_m, j_n), and can be distinguished at the RX j_n purely by its link signature.

Tracking the coordinate of a TX tag can be used as an intermediary to detect a change in location of the tag. As pointed out in [5], accuracies in typical indoor localization systems are around 3-4 m. Detection of smaller movements than the system accuracy would be difficult. In [5], RSS measurements are used directly to detect when two devices move together (e.g., with the same person) our work similarly avoids using localization as an intermediary, as a means to improve detection performance.

In this paper, we propose a robust location distinction mechanism that uses a physical layer characteristic of the radio channel between TX and RX, that we call a *temporal link signature*. The temporal link signature is the sum of the effects of the multiple paths from the TX to the RX, each with its own time delay and complex amplitude. Such a signature changes when the TX or RX changes position because the multipath in the link change with the positions of the endpoints of that radio link.

For example, consider the map of transmitters and receivers in Fig. 1. A radio link exists between nodes at i_1 and j_1. The RX of node j_1 can measure and record the temporal link signature of link (i_1, j_1). When node i_1 moves to location i_3, node j_1 can then distinguish the new link signature from the previously recorded link signature, and declare that it has moved. Alternatively, if an adversary impersonates the node at location i_1 from location i_2, the adversary's transmission to node j_1 will be detected to be from a different location, and the RX j_1 may then take a suitable action. While in either case, the detection of a link signature change can be reliably performed at one RX, node j_2 can also participate in the detection process for higher reliability and robustness.

In contrast to existing techniques, location distinction using temporal link signatures does not require continuous operation—a sensor can schedule sleep, and a wireless network can send packets intermittently. When awakened from sleep or upon reception of the subsequent packet, a RX can detect that a neighboring TX has moved since its past transmission. Unlike the RSS-based technique in [13], temporal link signatures can be measured at a single RX. We require *no additional complexity at the TX*, which keeps tag cost and energy consumption low.

The fact that a stationary TX unwittingly produces a measurable and consistent temporal link signature at a RX is also a user privacy concern. An eavesdropper could use a temporal link signature in a similar manner to a MAC address as a handle to identify a user and monitor the activity [14], [15]. In applications where user privacy is important, the user should alter the device's transmission in order to produce random changes in the link signature that an eavesdropper would measure.

In this paper, we make the following contributions. We define the temporal link signature and propose a location distinction algorithm which makes and compares measurements of temporal link signatures at a single RX in order to reliably detect a change in TX location. We propose a cooperative algorithm to use measurements at multiple receivers to achieve even higher robustness of location distinction. Using an extensive measurement set of over 9,000 temporal link signatures in a typical office environment, we detail the tradeoff between false alarm rate and detection rate, for single and multiple receivers. We provide an extensive comparison of temporal link signatures with an existing method which uses RSS-based signatures. We demonstrate that for a 5 percent probability of missed detection (MD), the temporal link signature method can achieve 8-16 times lower false alarm (FA) rate compared to the existing RSS-based method. Alternatively, for a 5 percent FA rate, the temporal link signature method can achieve 3.2 to 62 times lower probability of MD. For the 5 percent FA rate, the probability of MD is shown to be 0.05 percent, i.e., only one link change in every 2,000 is not distinguished by the proposed algorithm, when three receivers collaborate.

Finally, we evaluate the temporal and spatial statistics of temporal link signatures and show that the data is non-Gaussian, typically heavy tailed. We provide a means to estimate the mutual information (MI) between a measured link signature and the link. This MI quantifies the uncertainty about the link that the link signature measurement removes. We approximate the MI using the Edgeworth approximation as given by Hulle [37], which does not assume a particular distributional model of link signatures. We find the MI to be approximately 66 bits in our experimental setting.

The rest of this paper is structured as follows: Section 2 describes our models and methodology for obtaining link signatures. Section 3 describes results from extensive experimental measurements. Section 4 presents a study of the distribution of link signatures and a measurement-based estimation of mutual information. We summarize the existing work on location distinction in Section 5, and conclude and describe future directions in Section 6.

2 Methodology

We first define a temporal link signature and highlight the strong dependence of the link signature on the multipath radio channel. Next, we describe how it can be measured in typical digital receivers. We then describe a location distinction algorithm, that is, based on our link signatures and also develop a methodology to evaluate it. Finally, we describe our methodology for evaluating RSS-only signatures, which provides a comparison of our work to existing work.

2.1 Temporal Link Signature

The power of the temporal link signature comes from the variability in the multiple paths over which radio waves propagate on a link. A single radio link is composed of many paths from the TX to the RX. These multiple paths (multipath) are caused by the reflections, diffractions, and scattering of the radio waves interacting with the physical environment. Each path has a different length, so a wave propagating along that path takes a different amount of time to arrive at the RX. Each path has attenuation caused by path losses and interactions with objects in the environment, so each wave undergoes a different attenuation and phase shift. At the RX, many copies of the transmitted signal arrive, but each copy arriving at a different time delay, and with a different amplitude and phase. The sum of these time delayed, scaled, and phase shifted transmitted signals is the received signal.

Since the received signal is a linear combination of the transmitted signal, we can consider the radio channel or a link as a linear filter. For the link or channel in between TX i and RX j, the channel impulse response (CIR), denoted $h_{i,j}(\tau)$, is given by [17], [33]

$$h_{i,j}(\tau) = \sum_{l=1}^{L} \alpha_l e^{j\phi_l} \delta(\tau - \tau_l), \tag{1}$$

where α_l and ϕ_l are the amplitude and phase of the lth multipath component, τ_l is its time delay, L is the total number of multipaths, and $\delta(\tau)$ is the Dirac delta function. Essentially, the filter impulse response is the superposition of many impulses, each one representing a single path in the multiple paths of a link. Each impulse is delayed by the path delay, and multiplied by the amplitude and phase of that path.

The received signal, $r(t)$, is then the convolution of the channel filter and the transmitted signal $s(t)$

$$r(t) = s(t) \star h_{i,j}(t) + n(t), \tag{2}$$

with $n(t)$ as additive noise. All receivers measure $r(t)$ in order to demodulate the information bits sent by the TX. In this paper, we additionally use $r(t)$ to make a band-limited estimate of $|h_{i,j}(t)|$. We call this (noisy) estimate the *temporal link signature*.

2.1.1 Temporal Link Signature Estimation

If the SNR of $r(t)$ is high enough so that bits are correctly demodulated, then $s(t)$, the transmitted signal, can be recreated in the RX. Even in resource constrained scenarios, when packets can be successfully decoded by a less computationally constrained RX, the original waveform $s(t)$ can be reconstructed, thereby facilitating our methods. In general, estimating $h_{i,j}(t)$ from known $r(t)$, and $s(t)$ in (2) is a deconvolution problem, but for a number of reasons, we do not actually need to perform a deconvolution:

- Generally, digital signals have power spectral densities which are relatively flat inside the band (the frequency range of the channel) to maximize spectral efficiency [30]. Specifically, $|S(f)|^2$ is approximately equal to a constant, here denoted $\mathcal{P}_s$, for all f within the band.
- There is no need to exactly recreate $|h_{i,j}(t)|$, an approximation is sufficient for our purpose.

As a result, we estimate the temporal link signature using only convolution, rather than deconvolution. To show this, we first rewrite (2) in the frequency domain as

$$R(f) = S(f)H_{i,j}(f) + N(f),$$

where $R(f), S(f), H_{i,j}(f)$, and $N(f)$ are the Fourier transforms of $r(t), s(t), h_{i,j}(t)$, and $n(t)$, respectively. Then, we multiply $R(f)$ with the complex conjugate of the Fourier transform of the recreated transmitted signal, $S^*(f)$

$$S^*(f)R(f) = |S(f)|^2 H_{i,j}(f). + S^*(f)N(f). \tag{3}$$

Note that this multiplication in the frequency domain is a correlation in the time domain. As $|S(f)|^2$ is nearly constant within the band, (3) is a bandlimited version of $H_{i,j}(f)$ plus noise. Finally, the temporal domain is recovered from (3) by taking the inverse Fourier transform. We denote the impulse response estimate from TX i at RX j as $h_{i,j}(t)$

$$h_{i,j}(t) = \frac{1}{\mathcal{P}_s} \mathcal{F}^{-1}\{|S(f)|^2 H_{i,j}(f) + S^*(f)N(f)\},$$

where $\mathcal{F}^{-1}\{\cdot\}$ indicates the inverse Fourier transform. If $\mathcal{P}_s$ is known at the RX, for example, using 802.11h [31], it can be readily removed as given in (4). If $\mathcal{P}_s$ fluctuates due to transmit power changes that are unknown at the RX, the system would normalize the amplitude of all $h_{i,j}(t)$ estimates, as discussed in Section 2.2.2. Applying (1) to the expression in (4), we can see that the estimated CIR is simply a noisy, low-pass filtered version of the original channel impulse response

$$h_{i,j}(\tau) = \sum_{l=1}^{L} \alpha_l e^{j\phi_l} \nu(\tau - \tau_l) + \tilde{n}(\tau), \tag{4}$$

where $\nu(\tau)$ and $\tilde{n}(\tau)$ are the inverse Fourier transforms of $|S(f)|^2$ and $S^*(f)N(f)$, respectively. The function $\nu(t)$ does not have infinite bandwidth like the ideal impulse function $\delta(t)$ which it replaces, however, its amplitude at $\tau = 0$ is the energy in the signal $s(t)$. The $\nu(\tau - \tau_l)$ terms are large compared to $\tilde{n}(\tau)$, first because the SNR must have been above a minimum threshold for the RX to correctly demodulate the transmitted symbols, and second because the correlation with $s(t)$ is effectively a matched filter across all symbol periods, which increases the SNR of (4) compared to demodulation.

In a discrete-time RX, transmitted signals are sent in packets, and the received signal is sampled. We denote $h_{i,j}^{(n)}(\tau)$ as the CIR in (4) estimated from the nth transmitted packet. In addition, we do not consider phase information in the temporal link signature. Due to the clock and oscillator frequency differences between two nodes, the measured $h_{i,j}^{(n)}(\tau)$ will have a phase that changes over n; using a magnitude is a means to eliminate these effects. Thus, the sampled impulse response vector serves as the temporal link signature, $\mathbf{h}_{i,j}^{(n)} = [|h_{i,j}^{(n)}(0)|, \ldots, |h_{i,j}^{(n)}(\kappa T_r)|]^T$, where T_r is the sampling rate at the RX and $\kappa + 1$ is the number of samples.

2.1.2 Modulation-Dependent Implementations

The calculation of (4) can be done regardless of modulation, but for particular modulation types, the process is even easier. This paper does not develop new channel state estimation methods; our techniques are advantageous because they can exploit already existing channel state estimation algorithms, like [23], [36].

For example, consider receivers for orthogonal frequency division multiplexing (OFDM)-based standards, such as in IEEE 802.11a/g and 802.16. Such receivers can be readily adapted to calculate temporal link signatures since the signal amplitude and phase in each subchannel provides a sampled version of the Fourier transform of the signal. In effect, the Fourier transform operation is already implemented, and $R(f)$ is directly available. Use of $R(f)$ directly in an OFDM-like system has been evaluated by [25]. In our work, calculation of the temporal link signature requires an additional inverse FFT operation.

Most of the calculation necessary for the computation of temporal link signatures is already performed in existing code-division multiple access (CDMA) cellular base station receives, and in access points for WLANs operating on the 802.11b standard. CDMA receivers first correlate the received signal with the known pseudonoise (PN) signal. They then use the correlator output in a rake receiver, which adds in the power from several multipath components. Our temporal link signature in (2) is the correlation of the received signal with the transmitted signal $s(t)$. In contrast, the PN correlator correlates only with one period of a PN signal, which is one symbol duration of $s(t)$. The link signature of (2) can be estimated by averaging the PN correlator output over the course of many symbols. This would represent little additional calculation compared to the PN correlation operation. An implementation of this method for 802.11b signals using the universal software radio peripheral (USRP) receiver has been implemented and is available for download [1].

2.2 Normalization

Two types of normalization are important when measuring link signatures: (1) time delay, and (2) amplitude.

2.2.1 Time Delay

One problem exists when describing time measurements - transmitters and receivers are typically not synchronized. Thus, the temporal link signature, $h_{i,j}^{(n)}(t)$ has only a relative notion of time t. For example, consider the case that the next temporal link signature on the same link $(i,j), h_{i,j}^{(n+1)}(t)$, is equal to $h_{i,j}^{(n)}(t+\Delta t)$, where Δt is a timing offset error. If the timing error is not removed in some way, the temporal link difference between the nth and $n+1$st measurement would be very high, simply because of the lack of synchronization.

Hence, we normalize the time delay axis at each new link signature measurement by setting the time delay of the line of sight (LOS) multipath to be zero. In (4), this means that $\tau_1 = 0$. This can be implemented with a threshold detector when a measured impulse response *first* exceeds a threshold, the delay is set to 0. All link signatures in this paper are time-delay-normalized.

2.2.2 Amplitude

For purposes of robustness to replication attacks, we consider that an attacker has the capability to increase or decrease the transmit power of his device. One way to mitigate this attack is to amplitude normalize each measured CIR, that is, eliminate any effect of the transmit power on the measurement. We discuss the option of amplitude normalization of the measured impulse response, to form the *normalized link signature*, in Section 3. For the rest of this paper, when we refer to normalized link signatures, we specifically mean amplitude normalization. For a normalized link signature, the measured impulse response is normalized to unit norm

$$\tilde{\mathbf{h}}_{i,j}^{(n)} = \mathbf{h}_{i,j}^{(n)} / \|\mathbf{h}_{i,j}^{(n)}\|, \tag{5}$$

where $\|\cdot\|$ indicates the euclidean (l_2) norm.

In the following sections, we use $\mathbf{h}_{i,j}^{(n)}$ to refer generically to the link signature. When using a normalized link signature, $\tilde{\mathbf{h}}_{i,j}^{(n)}$ will be substituted into any expression in place of $\mathbf{h}_{i,j}^{(n)}$.

2.3 Algorithm

We use the temporal link signature modeled above to construct a location distinction algorithm as follows:

1. Given RX j and nodes $i \in \mathcal{N}_j$ (where $\mathcal{N}_j$ is the set of neighbors of j) a history of the most recent $N-1$ link signatures is measured and stored,

   $$\mathcal{H}_{i,j} = \{\mathbf{h}_{i,j}^{(n)}\}_{n=1}^{N-1}.$$

   These histories are assumed to be recorded while TX i is not moving and not under a replication attack. Still, $\mathbf{h}_{i,j}^{(n)}$ differ due to normal temporal variations in the radio channel, and measurement noise. To quantify this variation, RX j calculates the *historical average difference* $\sigma_{i,j}$ between the $N-1$ measurements in $\mathcal{H}_{i,j}$

   $$\sigma_{i,j} = \frac{1}{(N-1)(N-2)} \sum_{\mathbf{g}\in\mathcal{H}_{i,j}} \sum_{\mathbf{h}\in\mathcal{H}_{i,j}\backslash\mathbf{g}} \|\mathbf{h}-\mathbf{g}\|. \tag{6}$$

   The normalization constant $\frac{1}{(N-1)(N-2)}$ comes from the $N-1$ size of the history set $\mathcal{H}_{i,j}$. Only half of the terms $\|\mathbf{h}-\mathbf{g}\|$ need to be calculated since distance is symmetric.
2. The Nth measurement $\mathbf{h}^{(N)}$ is then taken. Here, we use $\mathbf{h}^{(N)}$ to denote the Nth measurement of the temporal link signature as given in (4), leaving out the subscript $_{i,j}$ since it isn't known yet that the signature matches with link (i,j). The normalized minimum euclidean (l_2) distance $d_{i,j}$ between $\mathbf{h}^{(N)}$ and the history $\mathcal{H}_{i,j}$ is calculated as

   $$d_{i,j} = \frac{1}{\sigma_{i,j}} \min_{\mathbf{h}\in\mathcal{H}_{i,j}} \|\mathbf{h}-\mathbf{h}^{(N)}\|, \tag{7}$$

   where $\sigma_{i,j}$ is given in (6). Note that many other distance measures are possible, but we choose the l_2 as a simple proof-of-concept measure.
3. Next, $d_{i,j}$ is compared to a threshold γ, for a constant $\gamma > 0$. When $d_{i,j} > \gamma$, the algorithm decides that the difference in the measured link signature and its history is not due to normal temporal variations but the measured link signature is that of a different link (from a new transmission location) and a location change is detected.

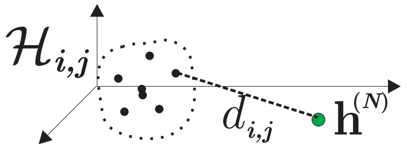


Fig. 2. Graphical diagram of history $\mathcal{H}_{i,j}$, new measurement $\mathbf{h}^{(N)}$, and dotted line connecting $\mathbf{h}^{(N)}$ to its closest point in the history. The normalized distance $d_{i,j}$ is the length of the line divided by $\sigma_{i,j}$.

4. When $d_{i,j}$ is less than the threshold, the measurement is assumed to be from the same link, and we denote $\mathbf{h}_{i,j}^{(N)} = \mathbf{h}^{(N)}$ and include it in $\mathcal{H}_{i,j}$. For constant memory usage, the oldest measurement in $\mathcal{H}_{i,j}$ is then discarded. The algorithm returns to step 2 for the $N+1$st measurement.

The process is shown graphically in Fig. 2. It is analogous to a clustering algorithm operating on high-dimensional data. We do not assume that points in $\mathcal{H}_{i,j}$ come from a particular distribution, and thus, we do not present "optimal" detection algorithms.

The action taken when a TX is detected to be at a distinct location is application dependent. For sensor motion detection or object security applications, the cooperative sensor localization algorithm might be triggered. When a replication attack is suspected, the RX might collaborate with other receivers to confirm the change in the node location.

2.4 Algorithm Evaluation Methodology

In this section, we describe our methodology for determining the accuracy of the detection algorithm.

We first want to develop a methodology to demonstrate that the link signature due to a TX at a location i' and the RX at a location j, is different from the link signature history between i and j, where $i' \neq i$, by more than the threshold γ. We denote the difference by $d_{i-i',j}$ and refer to it as the *spatial link difference*. Second, we want to demonstrate that the link signature measured while the TX is at the same location i and the RX is at j, will be different from the link signature history between i and j by less than the threshold γ. We denote this difference by $d_{i,j}^{(N)}$ and refer to it as the *temporal link difference*.

The location change detection test can be viewed then as a choice between two events H_0 and H_1,

$$\begin{aligned} H_0: \quad & d_{i,j} = d_{i,j}^{(N)}, \\ H_1: \quad & d_{i,j} = d_{i-i',j}. \end{aligned}$$

Since the $d_{i,j}$s are random variables, their conditional density functions are denoted $f_{d_{i,j}}(d|H_0)$ and $f_{d_{i,j}}(d|H_1)$. Detection theory gives the performance of a detector using the probability of false alarm P_{FA} and probability of detection P_D. These are [20]

$$\begin{aligned} P_{FA} &= \int_{x=\gamma}^{\infty} f_{d_{i,j}}(x|H_0)dx, \\ P_D &= \int_{x=\gamma}^{\infty} f_{d_{i,j}}(x|H_1)dx. \end{aligned} \tag{8}$$

Note also that we also refer to the probability of missed detection as P_M, where $P_M = 1 - P_D$. Since these probabilities are a function of γ, we can trade lower false alarm rate for lower probability of detection, and vice versa. The objective of experimental evaluation is to evaluate this tradeoff and to show examples of achievable performance.

2.5 Multiple Receiver Link Differences

In this paper, we also explore the use of multiple receivers to make the use of link signatures extremely robust, as displayed in Fig. 1. This relies on collaboration between two or more nodes.

In sensor networks, collaboration should be largely avoided in order to reduce communication energy, but it may be used in a small fraction of cases in order to confirm with higher reliability that a TX's location has changed. Sensor and ad hoc networks typically rely on redundancy of links, so each node is expected to have multiple neighbors. For prevention of replication attacks, collaboration may be normal, and any access points in radio range would collaborate. WLAN coverage regions often overlap, and hence, multiple access points may receive signals from the same TX. As WLANs become more ubiquitous, access point densities may increase and we would expect more overlap.

We define the set $\mathcal{J}$ to be the set of receivers involved in the collaborative location distinction algorithm for TX i. The algorithm proceeds as described in Section 2.3 with each RX calculating $d_{i,j}$, but after step 2, nodes $j \in \mathcal{J}$ send differences $d_{i,j}$ to a central processor (which could be any $j \in \mathcal{J}$). The central processor combines the results into a mean distance $d_{i,\mathcal{J}}$

$$d_{i,\mathcal{J}} = \frac{1}{|\mathcal{J}|} \sum_{j \in \mathcal{J}} d_{i,j}.$$

Afterwards, steps 3 and 4 of the algorithm proceed using $d_{i,\mathcal{J}}$ in place of the single RX distances $d_{i,j}$.

Denoting $d_{i,\mathcal{J}}^{(N)}$ to be the temporal link difference and $d_{i-i',\mathcal{J}}$ to be the spatial link difference, the detection test is now a choice between

$$\begin{aligned} H_0: \quad & d_{i,j} = d_{i,\mathcal{J}}^{(N)}, \\ H_1: \quad & d_{i,j} = d_{i-i',\mathcal{J}}. \end{aligned}$$

The conditional pdfs are now denoted $f_{d_{i,\mathcal{J}}}(d|H_0)$ and $f_{d_{i,\mathcal{J}}}(d|H_1)$, and the probability of false alarm P_{FA} and probability of detection P_D are computed as in (8) replacing $d_{i,j}$ with $d_{i,\mathcal{J}}$. Section 3.4 explores the multiple RX link differences experimentally.

2.6 Comparison with RSS-Only Signatures

In [13], the authors propose to identify attackers by means of Received Signal Strength (RSS) measurements only. An RSS-only method simply uses the RSS measured at multiple receivers as a feature vector. For comparing our work with existing efforts, we will also evaluate the performance of RSS-only methods. In the RSS-only case, let $P_{i,j}^{(n)}$ denote the nth measured received signal strength, between TX i and RX j, in dBm. Similarly, for multiple receivers $\mathcal{J}$, the feature vector is denoted $\{P_{i,j}^{(n)}\}_{j \in \mathcal{J}}$. The algorithms described in Sections 2.3 and 2.5 remain the same, but $\mathbf{h}_{i,j}^{(n)}$ is replaced with $P_{i,j}^{(n)}$.

Typically, RSS-only schemes use a narrowband measurement of RSS [13]. We first evaluate the performance of narrowband RSS in this paper. A narrowband measurement of RSS is made by integrating the channel filter, and then, taking the squared magnitude,

$$P_{i,j}^{(n)} = 10\log_{10}\left|\int_0^\infty h_{i,j}^{(n)}(t)dt\right|^2. \tag{9}$$

Equivalently, the integral can be seen as the frequency gain of the channel at $f = 0$, i.e., the center frequency of the complex baseband channel filter.

In addition, in order to be fair in comparing RSS-only schemes with wider bandwidth temporal link signature measurements, we also report the performance of using a very wideband measurement of RSS in this paper. The wideband measurement of RSS is made by integrating the squared magnitude of the channel filter

$$P_{i,j}^{(n)} = 10\log_{10}\int_0^\infty \left|h_{i,j}^{(n)}(t)\right|^2 dt, \tag{10}$$

which in the limit as bandwidth → ∞, is equal to the sum of the power in each multipath [33]. The measurement system has a 80 MHz bandwidth, and the measured RSS is an average across that bandwidth. Because frequency-selective fading has a coherence bandwidth on the order of 1 MHz for an indoor channel and on the order of 100 kHz for outdoor channels [33], the measurement system effectively averages out frequency selective fading effects. The resulting wideband RSS measurement has much less temporal variability than those typically measured using narrowband receivers. We believe that the *relative* performance of location distinction based on RSS and temporal link signature measurements will stay the same when applied to systems of different bandwidth.

3 Experimental Verification

Our proposed location distinction method relies heavily on the variability of the link signature, both in space and in time. Thus, accurate performance evaluation is done by using a set of link signature measurements recorded in a large network over time. We describe the measurement set and the evaluation results in this section. Different data from the described measurement campaign has been previously reported to evaluate radio localization algorithms [28]. Data from this campaign is publicly available on the CRAWDAD measurement repository [27].

3.1 Environment and System

The measured environment is in a typical modern office area. There are 44 device locations, shown in Fig. 3, within a 14 m by 13 m rectangular area. The campaign measures the channel between each pair of the 44 device locations, one at a time. All $44 * 43 = 1{,}892$ TX and RX permutations are measured. At each permutation of TX and RX locations, the RX measures $N = 5$ link signatures, over a period of about 30 s. The nth normalized measurement on link (i, j) is denoted $\mathbf{h}_{i,j}^{(n)}$, for $n = 1, \ldots, 5$. A total of $44 \cdot 43 \cdot 5 = 9{,}460$ measurements are recorded.

The measurement system is comprised of a direct-sequence spread spectrum (DS-SS) TX and RX. The system transmits and receives an unmodulated pseudonoise (PN) code signal with a 40 MHz chip rate at center frequency is 2,443 MHz. Both TX and RX have sleeve dipole antennas at 1 m height above the floor. The RX is essentially a software radio which records I and Q samples at a rate of 120 MHz. The FFT of the received signal, $R(f)$, is multiplied by the conjugate of the known transmitted signal spectrum, $S^*(f)$ as described in (3). Then, the IFFT is taken to calculate $\mathbf{h}_{i,j}^{(n)}$.

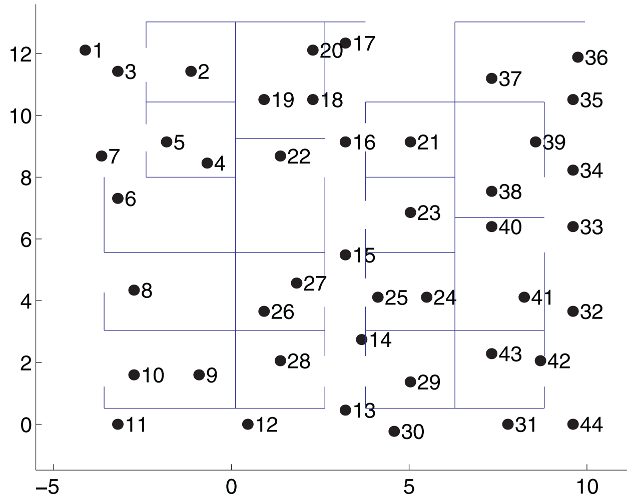


Fig. 3. Measurement area map and device locations.

These measurements are conducted after normal business hours (after 6pm), and as a result, the physical environment is relatively static, with only one or two people working in the environment. Daytime measurements in a busy office will be an important for future measurement-based verification.

About 1 percent of the time, a link signature has a very low signal-to-noise ratio (SNR) due to interference. Whenever a high noise floor is measured for a link, that measurement is dropped, thus some links have $N < 5$ measurements. All results have considered the actual N of each link (i, j).

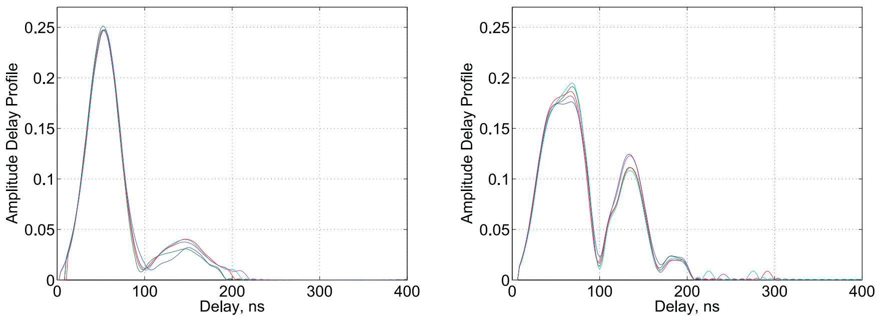
3.2 Example Links

Fig. 4 shows examples of the measured temporal link signatures. Fig. 4a shows the measurements for link (13, 43), i.e., $\{\mathbf{h}_{13,43}^{(n)}\}_{n=1\ldots5}$. Fig. 4b shows the measurements for link (14, 43).

3.2.1 Bandwidth Limitations

The bandwidth of the system is finite, and hence, Fig. 4 does not show each multipath as a pure impulse function. Rather, each multipath contribution is triangular in shape with a rounded peak. In our measurement system, the theoretical 3-dB width of the triangle is about 25 ns. Usually, several multipath arrive spaced more closely than the 25 ns width, and the multipath sum together to make a wider peak than would be seen if only a single signal was received.

Limited bandwidth does *not* mean that multipath structure is lost. Even though multipath are spaced more closely than 25 ns, the effects of the multipath are still apparent. In Fig. 4b, the wide (100 ns) width of the first peak shows evidence of temporally distinct multipath, more so than in the first 100 ns of Fig. 4a. The different widths of the first peaks increases the spatial link difference $d_{13-14,43}$.



(a) (b)

Fig. 4. Normalized temporal link signatures (five each) on links (a) $(13, 43)$ and (b) $(14, 43)$.

Thus, even though the measurement of the channel is band limited and makes it difficult to visually identify individual multipath, the different links are measurably different due to the different multipath contributions in each link.

3.2.2 Leave-One-Out Distances

To evaluate algorithm performance, we must separate the $N = 5$ measurements from link (i, j) into a history $\mathcal{H}_{i,j}$ and a single additional measurement. Here, the history $\mathcal{H}_{i,j}$ contains the first $N - 1$ measurements, i.e., $\mathbf{h}_{i,j}^{(n)}$ for $n = 1$, 2, 3, and 4.

From $\mathcal{H}_{i,j}$ and the Nth measurement for each link, we calculate the spatial link difference and temporal link differences (see Section 2.4) for the two example links. From (6), we calculate $\sigma_{13,43} = 1.48 \times 10^3$, and $\sigma_{14,43} = 0.60 \times 10^3$. Using these normalization constants, we calculate temporal link differences of $d_{13,43}^{(N)} = 0.19$ and $d_{14,43}^{(N)} = 0.76$.

For the spatial link difference, we can compare any of the $N = 5$ measured link signatures on link (i', j) with the history $\mathcal{H}_{i,j}$. Thus, we have five experimental values for the spatial link difference $d_{i-i',j}$, defined in Section 2.4, for each triplet (i, i', j).

As seen from the location map in Fig. 3, node locations 13 and 14 are very close in location, in fact, they are both in the same hallway, about 2.4 m apart. However, at RX 43, their temporal link signatures are noticeably different. Quantitatively, the spatial link differences, $d_{13-14,43}$, range from 3.43 to 3.83. For the opposite directional comparison, the spatial link difference $d_{14-13,43}$ ranges from 8.55 to 11.49. Compared to the temporal link differences of 0.19 and 0.76, respectively, the spatial link differences are more than 10 times greater. Any γ between 0.8 and 3.4 would effectively distinguish between the temporal and spatial variation on each link.

3.3 Single Receiver Motion Detector Performance

To show the performance of the motion detector in general, we demonstrate that for any RX location, the movement of a TX between any two locations would be reliably detected. For this purpose, we have used the measured link signatures to calculate the temporal link differences $d_{i,j}^{(N)}$ for all pairs $(i, j), i \neq j$, and the spatial link differences $d_{i-i',j}$ for all triplets (i, i', j), where $i \neq i' \neq j$.

Link Signature Differences: First, we calculate the temporal link differences when using temporal link signatures which are not amplitude normalized. The histograms of $d_{i,j}^{(N)}$ and $d_{i-i',j}$ are shown in Fig. 5a. Given a threshold γ, one could

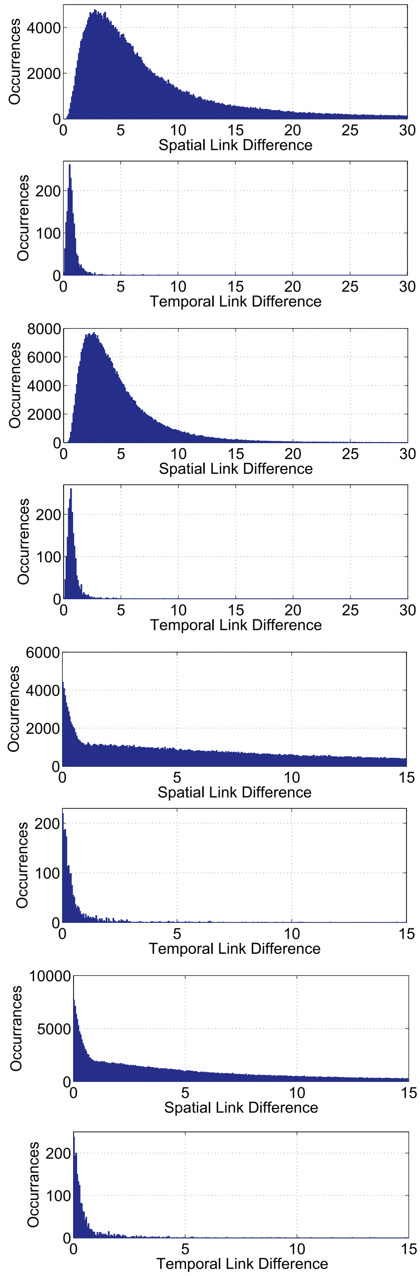


Fig. 5. Histograms of single-RX spatial and temporal link differences for (a) non-normalized link signatures, (b) amplitude-normalized link signatures, (c) wideband RSS, and (d) narrowband RSS signatures.

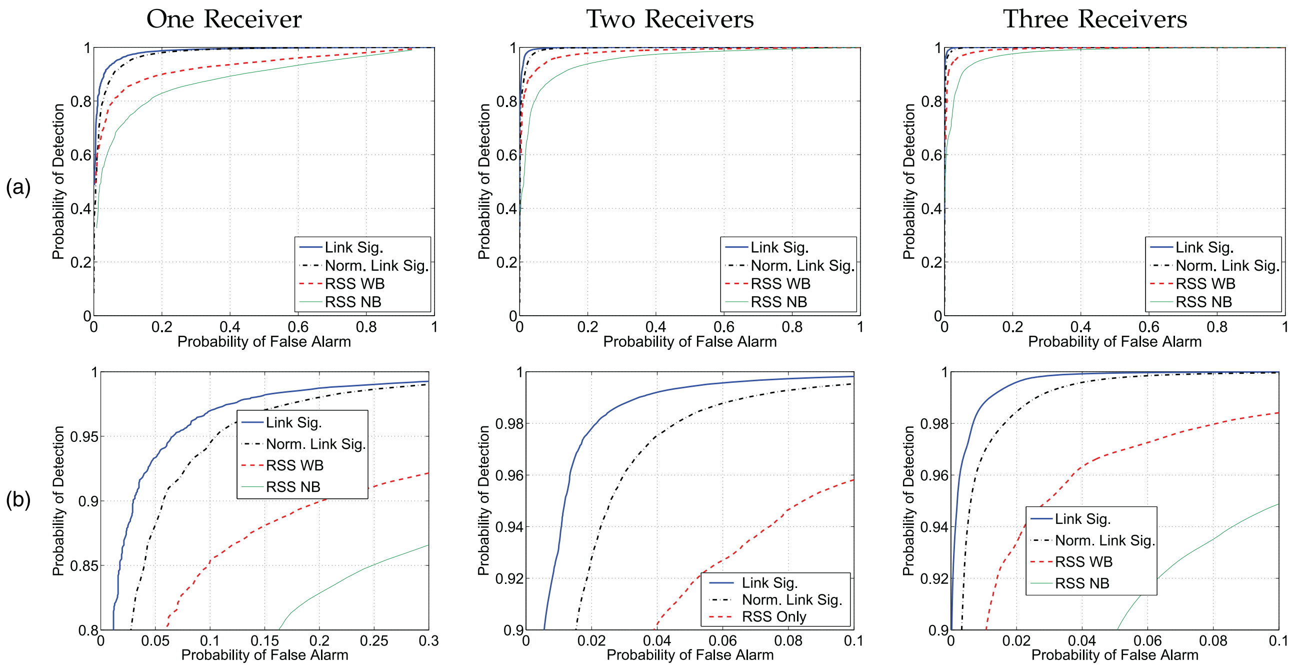


Fig. 6. ROC curves for one, two, or three receivers, (a) full views and (b) magnified views of high-performance region. Note that the scales of magnification in row (b) are different for one RX, and for two to three receivers.

calculate the false alarm rate P_{FA} and probability of detection P_D as given in (8) by finding the area under the curve to the left of the bottom plot, and to the left of the top plot, respectively.

Amplitude-Normalized Link Signature Differences: We can similarly calculate histograms for when the algorithm uses amplitude-normalized histograms, described in Section 2.2.2 and given in (5). We see in Fig. 5b that the spatial link differences have significantly decreased but are still higher than the temporal link differences.

RSS-Only Link Signature Differences: Finally, we evaluate wideband (WB) and narrowband (NB) RSS-only link signatures, as described in Section 2.6. For one RX, the feature vector is just a scalar, the RSS measured at RX j of the message transmitted by i. While multiple RX RSS-only feature vectors are proposed in [13], and are compared to the multiple RX temporal link signatures in Section 3.4, we first show the characteristics of single-RX RSS-only location distinction. The histograms of spatial and temporal link differences are shown in Figs. 5c and 5d, for wideband and narrowband, respectively. Notice that spatial link differences can be large, but there is a high concentration of spatial link differences near zero, and this concentration is worse for narrowband RSS. This concentration near zero leads to relatively high probability of a missed detection even when the threshold γ is close to zero.

3.3.1 Detector Performance

The receiver-operating characteristic (ROC) curve is a classical method for displaying the tradeoff between false alarms and missed detections in a detection algorithm. The ROC curve plots from (8) probability of false alarm P_{FA} against probability of detection P_D. The threshold γ is not shown explicitly, but for a particular value of γ, the detector would achieve a particular $P_{FA}(\gamma)$ and $P_D(\gamma)$. We test a wide range of γ and plot $P_D(\gamma)$ versus $P_{FA}(\gamma)$ in a single plot for a single ROC curve. Fig. 6 shows in the left column the ROC curves for each detection method: temporal link signatures, amplitude-normalized temporal link signatures, wideband RSS, and narrowband RSS.

3.3.2 A Few “Bad” Links

A few links (i, j) are responsible for a large share of the missed detections. These few links typically have a history, $\mathcal{H}_{i,j}$, of link signature measurements which vary considerably, and as a result, $\sigma_{i,j}$ is very high. An example is described further in Section 3.5. Since distance $d_{i,j}$ is normalized by $\sigma_{i,j}$, the spatial link differences are very low. These links have many other TX locations i' which have spatial link differences $d_{i-i',j} < \gamma$. In other words, many missed detections come from these few links (i, j) with unusually high temporal variations.

Consider the single RX location distinction system designed for $P_{FA} = 0.05$, using temporal link signatures. Fig. 6 shows that for one RX and $P_{FA} = 0.05$, the system achieves $P_M = 0.0663$. Listing the triplets (i, i', j) which are missed, we count how many missed detections came from each pair (i, j). The data indicates that the worst 5 percent of links account for 45.8 percent of the missed detections. That is, the miss rate would be cut in almost half if these 5 percent of links had not participated in the location distinction algorithm. This indicates that if the worst links can be identified and a different method used, that the performance of a location distinction algorithm could be improved even more than demonstrated in our work.

3.4 Multiple Receiver Motion Detector Performance

As described in Section 2.5, more than one RX can collaborate, if necessary, to further increase the robustness of link signatures. In this section, we evaluate the algorithm presented in Section 2.5 to verify this claim using the

TABLE 1
False Alarm Rates P_{FA} for Constant 95 Percent Detection Rate

Method	1 Rx	2 Rx	3 Rx
LS	0.0655	0.0119	0.0019
NLS	0.1052	0.0258	0.0061
RSS WB	0.5164	0.0844	0.0295
RSS NB	0.6676	0.2432	0.1023

TABLE 2
Probability of Miss P_M for Constant 5 Percent False Alarm Rate

Method	1 Rx	2 Rx	3 Rx
LS	0.0666	0.0058	0.0005
NLS	0.1198	0.0170	0.0024
RSS WB	0.2130	0.0828	0.0312
RSS NB	0.3662	0.1846	0.1019

experimental data. The evaluation of the multiple-RX algorithm proceeds as follows:

1. Find the histograms of the multiple-RX spatial and temporal link differences.
2. Use them to determine the probability of detection and probability of false alarm for a given threshold.
3. Plot the results in an ROC curve.

The first step involves checking all combinations of receivers and transmitters. First, the two (or more) RX locations must be chosen from the 44 experimentally measured locations to form the set $\mathcal{J}$. Next, from the remaining locations, one original TX location, i, and a second TX location, i' are chosen. Then, a temporal link difference $d_{i,\mathcal{J}}^{(N)}$ and a spatial link difference $d_{i-i',\mathcal{J}}$ are calculated.

3.4.1 Two Receivers

There are $\binom{44}{2}$ ways to choose locations for two receivers out of the 44 measured, and then, $42 * 41$ ways to choose i and i', for a total of 1.63×10^6 different TX/RX arrangements analyzed using the measurement set. From the histograms of $d_{i,\mathcal{J}}^{(N)}$ and $d_{i-i',\mathcal{J}}$ for each measurement type, the plot of false alarm rate versus detection rate (the ROC plot) is shown in the middle column of Fig. 6. Note, the magnified plot in row (b) shows a smaller range of P_{FA} and P_D compared to that for one RX in row (b), in order to show the relative accuracies of the higher-accuracy collaborative algorithm.

3.4.2 Three Receivers

For the case when three receivers are used, there are $\binom{44}{3}$ ways to choose the RX locations out of the 44 measurement locations, and then, there are $41 \cdot 40$ ways to choose i and i' for a total of 2.17×10^7 different arrangements analyzed using the measurement set. From the histograms of the spatial and temporal link differences for each measurement type, the false alarm rates and detection rates are calculated and shown in the right-most column of Fig. 6.

3.4.3 Summary

Table 1 compares the four methods, link signatures (LS), normalized link signatures (NLS), wideband received signal strength (RSS WB), and narrowband received signal strength (RSS NB), given a system design requirement to have a 95 percent detection rate (or 5 percent probability of miss). With one RX, link signatures could achieve this requirement with a 6.55 percent probability of false alarm. With three receivers, this same detection rate could be achieved with only a 0.19 percent probability of false alarm. In comparison, RSS WB methods require a 51.64 percent and 2.95 percent probability of false alarm for one and three receivers, respectively. In relative terms, the false alarm rate is eight and 16 times higher for the RSS WB case.

Table 2 presents a complementary view. If instead the system requirements state a maximum false alarm rate, Table 2 shows the lowest probability of miss which can be achieved. If, we tolerate a 5 percent false alarm rate, then for link signatures at one RX, we can keep the miss rate down to 6.66 percent. When using three receivers, this miss rate is 0.05 percent, i.e., 1 miss in every 2,000 tests. The RSS WB method for the same false alarm rate is capable of achieving a miss rate of 21.30 percent and 3.12 percent for one, and three receivers, respectively. Compared to a method using temporal link signatures, the RSS WB method would have 3.2 and 62 times as many cases in which it could not distinguish two spatially distinct links. The temporal link signature method improves more quickly than the RSS-only method as receivers are added. In Table 2, P_M decreases by a factor of 11 with each additional collaborating RX measuring temporal link signatures. In contrast, P_M decreases by a factor of 2.6 with each additional RX measuring only RSS.

In comparison of methods, amplitude-normalization degrades detector performance, but normalized link signatures still significantly outperform the RSS-only method. Also, wideband measurements of RSS are seen to be useful; the RSS WB method always performs significantly better than the RSS NB method.

3.5 Highly Dynamic Environments

In contrast to the typical variation in temporal link signatures shown in Fig. 4, Fig. 7 shows one of the worst examples inamd the measurement set of temporal link signature variation. It is likely that phase changes or changes in shadowing to multipath components occurred during the recording of the

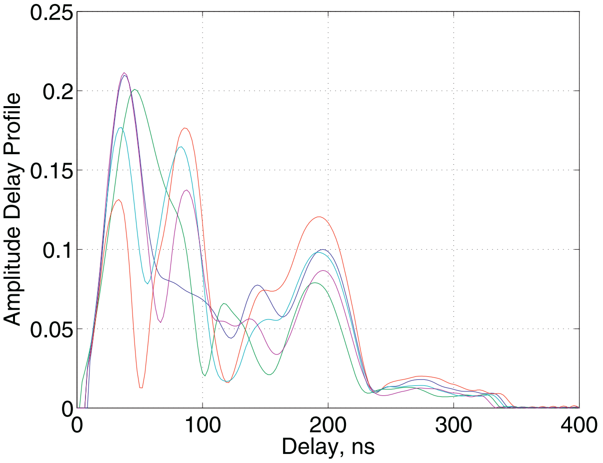


Fig. 7. The five recorded temporal link signatures of link $(18, 24)$ show some of the most extreme variability in the measurement set.

five link signature measurements, in particular for the multipath with low delays. (Note that the process of amplitude normalization artificially increases the normalized amplitude for the multipath at high delays for the link signatures with low amplitude multipath at low delays.) This link $(18, 24)$ has high $\sigma_{i,j} = 0.424$, about 3-4 times greater than the typical historical average difference. Other distance measurements, $d_{i-i',j}$, for $i \neq i'$, are normalized by this high $\sigma_{i,j}$, and are thus, more likely to fall below the threshold γ and become "missed detections." Link $(18, 24)$ is one of the very few "bad" links which cause a large proportion of the missed detections.

Histories larger than five will help to better represent the possible variation due to dynamic environments. Statistical methods for high-dimensional data can be used to subdivide or cluster the history, and graph measures such as spanning tree size can be used instead of (6) to quantify temporal variation within a history. Future measurement sets with larger histories would be required for further improvement.

Future work will also need to address the threat that an adversary could purposefully change the environment in between the legitimate TX and RX in order to cause a legitimate user to be detected as being at a different location. This possibility can be addressed by a separate authentication method.

4 Link Signature Spatial Information

In this section, we quantify in bits the location information contained in a measurement of link signature. We first show that our link signature measurement is non-Gaussian, typically heavy-tailed. Then, we provide a method to estimate the mutual information (MI) between a measured link signature and the link. Essentially, we quantify the comparison between spatial and temporal differences in link signatures using MI. We compare:

- $\bar{\mathbf{h}}_{i,j} \triangleq \mathrm{E}[\mathbf{h}_{i,j}^{(n)}]$, the mean amplitude-normalized link signature measurement for link i, j. Rather than use the physical TX and RX locations $\mathbf{z}_i$ and $\mathbf{z}_j$, we are directly interested in the mean coordinate of each link in vector space. Differences in $\bar{\mathbf{h}}_{i,j}$ are the spatial differences between links at different locations.
- $\mathbf{h}_{i,j}^{(n)}$: A single measurement of the amplitude-normalized link signature for link i, j. Temporal changes make the measurement $\mathbf{h}_{i,j}^{(n)}$ different from the mean for link i, j.

Given these two random variables, we estimate the MI between the mean link signature for a given link and any given link signature measurement, that is, $I(\bar{\mathbf{h}}_{i,j}; \mathbf{h}_{i,j}^{(n)})$. We provide a method that a measured data set, as described in Section 3 to estimate MI for the measured environment. Characterization of MI for other environments can be performed using the procedure we describe, on other measured data sets.

Because the mean link signature measurement is used as a link (TX and RX location) identifier, this mutual information answers the question, "How much uncertainty about the link ID is removed by measuring a link signature?" The mutual information also answers the following question about the channel capacity. How much information can be conveyed about link identification by a measurement of link signature? For the reasons discussed in Section 2.2.2, we assume amplitude normalization of link signatures.

The estimation of mutual information proceeds using marginal and joint differential entropies

$$I(\bar{\mathbf{h}}_{i,j}; \mathbf{h}_{i,j}^{(n)}) = \mathrm{h}(\mathbf{h}_{i,j}^{(n)}) + \mathrm{h}(\bar{\mathbf{h}}_{i,j}) - \mathrm{h}(\mathbf{h}_{i,j}^{(n)}, \bar{\mathbf{h}}_{i,j}), \tag{11}$$

where $\mathrm{h}(\cdot)$ denotes differential entropy. Both $\mathbf{h}_{i,j}^{(n)}$ and $\bar{\mathbf{h}}_{i,j}$ are high-dimensional correlated random vectors, so the estimation of their entropies is made difficult by the curse of dimensionality [8] and the finite number of available samples. We first show why simple distributional models (multivariate Gaussian, or Gaussian mixture) are not accurate for our data. Next, we use the Edgeworth approximation to estimate the differential entropies of interest and finally provide the results for our measured data set.

4.1 Insufficiency of Distributional Assumptions

In this section, we test two common distributional assumptions for the random vectors $\mathbf{h}_{i,j}^{(n)}$ and $\bar{\mathbf{h}}_{i,j}$, and show that neither is sufficient to characterize the measured data set.

We first evaluate whether the vectors $\bar{\mathbf{h}}_{i,j}$ and $\mathbf{h}_{i,j}^{(n)}$ are multivariate Gaussian random vectors. We apply the Kolmogorov-Smirnov (KS) hypothesis test [7] to decide between hypothesis H_0: Y_k is distributed as $\mathcal{N}(\mu, \sigma^2)$, versus hypothesis H_1: Y_k is not distributed as $\mathcal{N}(\mu, \sigma^2)$, where Y_k is kth real or imaginary part of a component of either $\bar{\mathbf{h}}_{i,j}$ or $\mathbf{h}_{i,j}^{(n)}$. Since both vectors are complex and of length 25, there are a total of 100 KS marginal tests. With a set $\alpha = 0.05$ false alarm threshold, the KS test decides to reject H_0 for 99 out of 100 tests, thus the marginal distributions are not Gaussian. Therefore, the vectors $\bar{\mathbf{h}}_{i,j}$ and $\mathbf{h}_{i,j}^{(n)}$ can not be multivariate Gaussian.

Many multivariate methods first decorrelate a random vector prior to its differential entropy estimation [19]. We first find $\bar{U}$ and U the left singular matrices of the covariance matrices of $\bar{\mathbf{h}}_{i,j}$ and $\mathbf{h}_{i,j}^{(n)}$, respectively, by singular value decomposition. Then, the uncorrelated vectors $\bar{\mathbf{X}}$ and $\mathbf{X}$ are computed as $\bar{\mathbf{X}} = \bar{U}^T \bar{\mathbf{h}}_{i,j}$ and $\mathbf{X} = U^T \mathbf{h}_{i,j}^{(n)}$. Note that multiplication by an orthogonal matrix does not change the differential entropy of a random vector. This is because the differential entropy of a linear transformation of a random vector increases by a factor of the log of the determinant of the transformation matrix [9].

Most components of $\bar{\mathbf{X}}$ and $\mathbf{X}$ have heavier tails than a Gaussian distribution. Hence, we test an assumption that the components of $\bar{\mathbf{X}}$ and $\mathbf{X}$ can be represented as two-part zero-mean Gaussian mixture distributions, i.e.

$$f_{X_k}(x_k) = \frac{\lambda_1}{\sqrt{2\pi\sigma_1^2}} e^{-x_k/\left(2\sigma_1^2\right)} + \frac{1-\lambda_1}{\sqrt{2\pi\sigma_2^2}} e^{-x_k/\left(2\sigma_2^2\right)}, \tag{12}$$

where X_k is a component of either $\bar{\mathbf{X}}$ of $\mathbf{X}$. We use an expectation maximization algorithm to estimate λ_1, σ_1, and σ_2. Then, we perform the KS test to decide between H_0: X_k is distributed as (12), versus H_1: X_k is not distributed as (12). The KS tests reject H_0 for 41 out of 100 components, so more than half (59 percent) of components agree with the new model. However, the data does not support the model for all components. Repeating the tests for l-part zero-mean Gaussian mixtures with $l > 2$ does not improve model agreement, as measured by the KS test. Some components show some asymmetry in their heavy-tailed characteristics, and are thus, not modeled well via a zero-mean Gaussian mixture. A small number of components have tails lighter than a Gaussian distribution, and thus, also not well modeled by (12). We conclude that a single multivariate distribution is unlikely to capture the characteristics of the measured data. In any case, we desire a general procedure to estimate MI from a data set, not one based on the specific distribution of the measurements presented in Section 3.

4.2 Entropy via Edgeworth Approximation

In order to compute differential entropy without a distributional model, we apply the multivariate Edgeworth approximation of Hulle [37]. The Edgeworth expansion is generally applied to estimate the density of a random variable using its higher order cumulants, up to order five [3]. The Edgeworth approximation is known to be advantageous in terms of convergence as a function of sample size P_a and computational complexity compared to the Parzen window estimator [2] and the nearest-neighbor estimator of [22] when the data has high dimension d. Compared to the estimation of differential entropy when using the Gaussian approximation, the multivariate Edgeworth approximation accounts for the non-Gaussian behavior quantified by higher order cumulants of the vector. Specifically, the approximation given by Hulle [37] is,

$$\begin{aligned}\mathrm{h}(\mathbf{X}) \approx \mathrm{h}(\phi_{\mathbf{X}}) - \frac{1}{12}\Bigg[&\sum_i (\kappa^{i,i,i})^2 + 3\sum_{i\neq j}(\kappa^{i,i,j})^2 \\ &+ \frac{1}{6}\sum_{i<j<k}(\kappa^{i,j,k})^2\Bigg],\end{aligned} \tag{13}$$

where $i, j, k \in \{1, \dots, d\}$, where d is the dimension of vector $\mathbf{X}$, $\mathrm{h}(\phi_{\mathbf{X}})$ is the differential entropy of a multivariate Gaussian random vector with covariance matrix $C_{\mathbf{X}}$, i.e., $\mathrm{h}(\phi_{\mathbf{X}}) = \frac{1}{2}\log|C_{\mathbf{X}}| + \frac{d}{2}\log 2\pi + \frac{d}{2}$, and $\kappa^{i,j,k}$ is the normalized cumulant over dimensions i, j, and k. The normalized cumulant is estimated from data as

$$\kappa^{i,j,k} = \frac{1}{P_a}\frac{1}{\sigma_i\sigma_j\sigma_k}\sum_{n=1}^{P_a} X_i^{(n)} X_j^{(n)} X_k^{(n)},$$

where $X_i^{(n)}$ is the ith element of the nth realization of $\mathbf{X}$, and σ_i^2 is the variance of the ith element of $\mathbf{X}$, for $i \in \{1, \dots, d\}$.

4.3 Results

From the decorrelated measured data vectors, we use (13) to estimate the three differential entropies in (11) to find $\mathrm{h}(\mathbf{h}_{i,j}^{(n)}) = -314.0$, $\mathrm{h}(\bar{\mathbf{h}}_{i,j}) = -322.1$, and $\mathrm{h}(\mathbf{h}_{i,j}^{(n)}, \bar{\mathbf{h}}_{i,j}) = -702.4$ bits (note differential entropy may be negative [9]). Then using (11), we find $I(\bar{\mathbf{h}}_{i,j}; \mathbf{h}_{i,j}^{(n)}) = 66.2$ bits. We note that if the vectors were multivariate Gaussian, the $\mathrm{h}(\phi_X)$ terms would provide the exact differential entropies, and the mutual information would have been found to be $I(\bar{\mathbf{h}}_{i,j}; \mathbf{h}_{i,j}^{(n)}) = 50.7$ bits. There is a difference of 15.5 bits between the mutual information estimate when assuming Gaussianity versus using the Edgeworth approximation. Because the Gaussian approximation uses only the covariance from the data, and the Edgeworth approximation given by Hulle [37] uses the third-order cumulants of the data, the difference quantifies the improvement in MI estimate gained by including third-order cumulants.

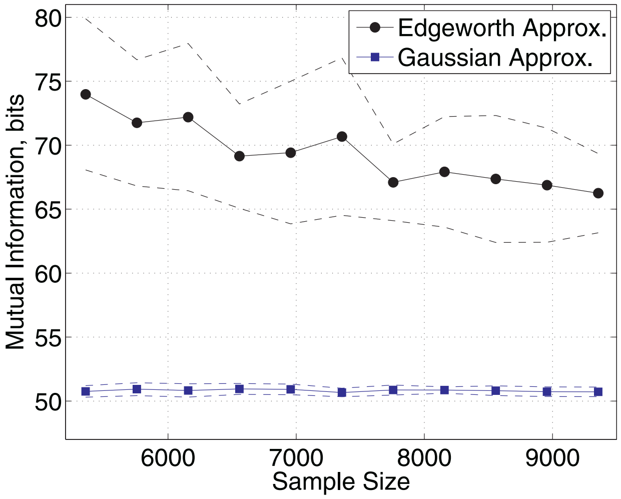


Fig. 8. Mutual information $I(\bar{\mathbf{h}}_{i,j}; \mathbf{h}_{i,j}^{(n)})$ estimated with Gaussian and Edgeworth approximations, with $\pm 1\sigma$ confidence intervals shown about each estimate, versus sample size B.

Noting that the estimated cumulants $\kappa^{i,j,k}$ form the basis of the Edgeworth approximation, which are themselves influenced by the outliers in the measured data, it is critical to verify that the estimated MI itself is robust to outliers in the data. For this purpose, we use the *bootstrap* [11] to estimate the variance of the estimated MI. In short, we resample B data points from the measured data points with replacement, and then use the resampled data to estimate the MI. By performing many resamplings, we can estimate the mean and variance of the MI estimator, as a function of B. Results for the estimated MI are shown in Fig. 8, for both Edgeworth and Gaussian approximations, along with the $\pm 1\sigma$ confidence interval about the mean. For $B = P_a = 9{,}460$, the standard deviation of the Edgeworth approximation MI estimate is found to be 3.1 bits. The results show that the Edgeworth approximation results in MI significantly higher than would be predicted by the Gaussian approximation.

4.4 Discussion

Our results, based on our experimental data, show that measuring link signature removes about 66 bits of uncertainty about the mean link signature. If the mean link signature for each link is known (from past measurements) and unique, then a link signature measurement removes 66 bits of uncertainty about which link was measured. These estimates are not obtained by assuming a known distribution, rather, by the Edgeworth approximation, which uses the third order cumulants in addition to the covariance, and thus, is a higher order approximation than would be obtained by a multivariate Gaussian assumption.

5 Related Work

There are three potential applications for location distinction mentioned in Section 1, and this section presents the related work and existing methods used in these areas.

5.1 Motion Detection in Wireless Sensor Networks

Motion detection can done by processing video camera feeds [35], [26]. However, when an object is not in view of a camera, or in the dark, its motion cannot be detected. Furthermore, detection of movement is not the same as recognition of the moved object [26], so if the objective is tracking of unique objects, camera-based approaches cannot easily handle large numbers of objects.

The RSS-based *signalprint* method of [13] could be used to detect motion based on the RSS at multiple receivers, but requires more than a single RX. Doppler and accelerometer measurements require continuous measurement in order to reliably detect a change, since once a device has stopped, Doppler and accelerometer measurements no longer indicate a movement. In contrast, a link signature change is lasting, so that a measurement long after a device has stopped moving will indicate a change from the previous measurement. Enabling, low duty cycle is key to reducing energy consumption in wireless sensors [32].

5.2 Physical Security Using Wireless Tags

Motion detection for security often includes in each tag an accelerometer or "bump sensor" [16]. In addition to the energy costs mentioned above, it is desirable for inexpensive tags to avoid the cost of an additional sensor. Higher probability of detection will be expected of active tracking systems to justify the expense of placing a tag on every object. Our work provides a lower energy method to detect motion of an active tag, without any additional sensor, using link signature characteristics.

5.3 Information Security for Replication Attacks

For the purpose of providing security against replication attacks, our work builds on the insightful work of Li, Xu, Miller, and Trappe [25]. In [25], the authors propose exploiting the multipath channel's frequency and spatial variation at a RX to distinguish two transmissions coming from different locations. Furthermore, in [25], *multiple tone probing* is used, in which the TX sends N carrier waves, separated by the coherence bandwidth of the channel. The amplitudes of these carriers at the RX are used as a feature vector to describe the channel. Experiments measure one link over time; a mobile link, and a three-node network of a legitimate TX and RX, and an attacker. Work in [39], [42], [40], [41] expands analysis of the frequency response approach. In [42], [40], the frequency response vector is assumed to be complex multivariate Gaussian with exponentially decaying variance, and the temporal variation is assumed to be a first-order auto-regressive (AR-1) random process, with complex multivariate Gaussian increments. Under these assumptions, likelihood ratio tests, and theoretical performance can be analyzed and simulated. In [41], the model assumptions are applied to analyze detection in MIMO systems.

Our work expands on the exploitation of multipath to uniquely identify a link. First, an arbitrary packet transmission is used to measure the channel, rather than special carrier waves. Second, we exploit the magnitude of the channel characteristic in the time domain, rather than in the frequency domain. Frequency measurements of $H_{i,j}(f)$ are related to $h_{i,j}(t)$ by a Fourier transform. However, phase changes to multipath with significantly different time delays do not alter $|h_{i,j}(t)|$, even when they alter $H_{i,j}(f)$ and $|H_{i,j}(f)|$.[1] Finally, our work uses the results of a vast measurement campaign to more completely demonstrate, and quantify using mutual information, the spatial variation of multipath channels, to an extent that was not possible in [25]. These results are necessary to demonstrate the accuracy and quantify the performance of location distinction.

The use of multiple receivers to enlarge the feature space is explored by Faria and Cheriton [13]. Their work used the RSS measured at multiple receivers, called the *signalprint*, to detect a class of identity attacks, and the authors present extensive experimental results. The low dimensionality of the feature space and the variability of RSS makes it difficult to uniquely identify TX locations. In particular, those transmitters separated by short distances (up to 5 m or 7 m) [13] can be confused, depending on the number of access point measurements. In our work, we dramatically expand the feature space and demonstrate an order of magnitude reduction in the miss rate or false alarm rate.

Regarding the use of RSS as a authentication feature, it must noted that a transceiver with an array antenna could use beamforming methods to send energy in different directions in an attempt to appear similar to another node. Furthermore, a link's RSS *can* be eavesdropped, since protocols require nodes to adapt depending on signal quality. Two adaptations are the use of power control, and the adaptation of modulation type as a function of link quality. Link signature measurements cannot be inferred from the interactions between nodes and access points.

Other radio-layer authentication research includes:

1. Location-Based Authentication: A wireless network can be used to locate a TX based on angle-of-arrival [24], [18] or signal strength [12] measurements. These methods can be hampered by synchronization issues (i.e., angular orientation and antenna pattern) and variable multipath and shadowing effects. Link signature methods do not attempt to localize a node, but in contrast, they are *enhanced* by the variability of the multipath channel.
2. Device-Based Authentication: Manufacturing variation may make one device's transmitted signal measurably different from another [21]. If such device characteristics can be measured at an access point, they could also be measured (and recreated) by a capable eavesdropper. Link signatures cannot be eavesdropped by an eavesdropper at a different location than the RX; and cannot be arbitrarily recreated except at the identical TX location.
3. GPS-Based Authentication: In [10], signals from GPS receivers are used to form signatures unique to each location. Each node and access point must have a GPS receiver, which limits the method to outdoor and cost-insensitive applications.

[1] Phase changes rapidly with small changes in diffraction geometry or scatterer position at centimeter scales. Time delays may also change, but they are measurable in $|h_{i,j}(t)|$ only when large compared to the inverse bandwidth, on the order of meters.

In comparison to our past work [29], this paper presents a method to estimate the MI between a link and its measured link signature, which quantifies the amount of uncertainty about the link removed by measurement of a link signature. We investigate the distribution of the measured data set, and then, apply the Edgeworth approximation, which does not assume a particular distributional model, to estimate required differential entropies. This paper also compares narrowband and wideband implementations of the RSS signalprint method and shows the superior performance of the wideband implementation of the method.

6 Conclusion and Future Work

We have presented a new methodology for robust location distinction using temporal link signatures. Through extensive measurements, we have demonstrated that our approach allows order-of-magnitude reductions in false alarm rate or miss rate compared to RSS-based methods. We estimate the link information in a channel impulse response measurement, from a measured data set, to be about 66 bits, using the multivariate Edgeworth approximation.

The measurement set utilized in this paper used a 40 MHz chip rate DS-SS system (significantly wider than the 11 MHz chip rate of the 802.11b protocol) and covered relatively short path lengths (an average path length of 7.7 m). In general, wider bandwidths and longer path lengths generate a richer link signature space and make measured link signatures more unique as a function of TX and RX locations. The tradeoff between bandwidth, path length, and detection performance must be characterized in future work.

Acknowledgments

This material is based upon work supported by the US National Science Foundation under Grants #0748206, #0831490, #0855261, and #1035565. This work was also partially supported by ONR/ARL MURI Grant #W911NF-07-0318 and a Technology Commercialization Project Grant from the University of Utah Research Foundation.

References

[1] Sensing and Processing Across Networks (SPAN) Lab Website, http://span.ece.utah.edu, 2010.

[2] I.A. Ahmad and P.E. Lin, "A Nonparametric Estimation of the Entropy for Absolutely Continuous Distributions," *IEEE Trans. Information Theory,* vol. 22, no. 3, pp. 372-375, May 1976.

[3] O.E. Barndorff-Nielsen and D.R. Cox, *Inference and Asymptotics.* Chapman & Hall, 1989.

[4] T. Burchfield and S. Venkatesan, "Accelerometer-Based Human Abnormal Movement Detection in Wireless Sensor Networks," *Proc. First ACM Int'l Workshop Systems and Networking Support for Healthcare and Assisted Living Environments,* pp. 67-69, 2007.

[5] G. Chandrasekaran, M. Ergin, M. Gruteser, R. Martin, J. Yang, and Y. Chen, "DECODE: Detecting Co-Moving Wireless Devices," *Proc. Fifth IEEE Int'l Conf. Mobile Ad Hoc and Sensor Systems (MASS '08),* pp. 315-320, 2008.

[6] Y. Chen, W. Trappe, and R.P. Martin, "Detecting and Localizing Wireless Spoofing Attacks," *Proc. IEEE Comm. Soc. Conf. Sensor Mesh and Ad Hoc Comm. and Networks (SECON '07),* pp. 193-202, 2007.

[7] W.J. Conover, *Practical Nonparametric Statistics.* John Wiley & Sons, 1971.

[8] J.A. Costa and A.O. Hero III, "Geodesic Entropic Graphs for Dimension and Entropy Estimation in Manifold Learning," *IEEE Trans. Signal Processing,* vol. 52, no. 8, pp. 2210-2221, Aug. 2004.

[9] T. Cover and J.A. Thomas, *Elements of Information Theory.* John Wiley & Sons, 1991.

[10] D.E. Denning and P.F. MacDoran, "Location-Based Authentication: Grounding Cyberspace for Better Security," *Computer Fraud and Security,* pp. 12-16, Feb. 1996.

[11] B. Efron and R. Tibshirani, *An Introduction to the Bootstrap.* Chapman & Hall, 1997.

[12] D.B. Faria and D.R. Cheriton, "No Longterm Secrets: Location-Based Security in Overprovisioned Wireless LANs," *Proc. Third ACM Workshop Hot Topics in Networks (HotNets-III),* Nov. 2004.

[13] D.B. Faria and D.R. Cheriton, "Radio-Layer Security: Detecting Identity-Based Attacks in Wireless Networks Using Signalprints," *Proc. Workshop Wireless Security (WiSe '06),* pp. 43-52, Sept. 2006.

[14] B. Greenstein, D. McCoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall, "Improving Wireless Privacy with an Identifier-Free Link Layer Protocol," *Proc. ACM MobiSys,* pp. 40-53, 2008.

[15] M. Gruteser and D. Grunwald, "Enhancing Location Privacy in Wireless LAN through Disposable Interface Identifiers: A Quantitative Analysis," *Mobile Networks and Applications,* vol. 10, no. 3, pp. 315-325, 2005.

[16] W.E. Guthrie, J. Joseph, and F. Pappadia, "Tagging System Using Motion Detector," US Patent 5 844 482, Dec. 1998.

[17] H. Hashemi, "The Indoor Radio Propagation Channel," *Proc. IEEE,* vol. 81, no. 7, pp. 943-968, July. 1993.

[18] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks," *Proc. Network and Distributed System Security Symp. (NDSS '04),* pp. 45-57, Feb. 2004.

[19] A. Hyvärinen, "Survey on Independent Component Analysis," *Neural Computing Surveys,* vol. 2, pp. 94-128, 1999.

[20] S.M. Kay, *Fundamentals of Statistical Signal Processing.* Prentice Hall, 1993.

[21] T. Kohno, A. Broido, and K.C. Claffy, "Remote Physical Device Fingerprinting," *Proc. IEEE Symp. Security and Privacy,* pp. 211-225, 2005.

[22] L. Kozachenko and N.N. Leonenko, "Sample Estimate of the Entropy of a Random Vector," *Problems of Information Transmission,* vol. 23, no. 2, pp. 95-101, 1987.

[23] E.G. Larsson, G. Liu, J. Li, and G.B. Giannakis, "Joint Symbol Timing and Channel Estimation for OFDM Based WLANs," *IEEE Comm. Letters,* vol. 5, no. 8, pp. 325-327, Aug. 2001.

[24] L. Lazos and R. Poovendran, "SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks," *Proc. ACM Workshop Wireless Security (WiSe '04),* pp. 21-30, 2004.

[25] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing Wireless Systems via Lower Layer Enforcements," *Proc. ACM Workshop Wireless Security (WiSe '06),* pp. 33-42, Sept. 2006.

[26] D. Murray and A. Basu, "Motion Tracking with an Active Camera," *IEEE Trans. Pattern Analysis and Machine Intelligence,* vol. 16, no. 5, pp. 449-459, May 1994.

[27] N. Patwari, utah/CIR (v. 2007-09-10) dataset, http://crawdad.cs.dartmouth.edu/meta.php?name=utah/CIR, 2009.

[28] N. Patwari, A.O. Hero III, M. Perkins, N. Correal, and R.J. O'Dea, "Relative Location Estimation in Wireless Sensor Networks," *IEEE Trans. Signal Processing,* vol. 51, no. 8, pp. 2137-2148, Aug. 2003.

[29] N. Patwari and S.K. Kasera, "Robust Location Distinction Using Temporal Link Signatures," *Proc. ACM MobiCom,* Sept. 2007.

[30] J.G. Proakis and M. Salehi, *Communication System Engineering,* second ed. Prentice Hall, 2002.

[31] D. Qiao and S. Choi, "New 802.11h Mechanisms Can Reduce Power Consumption," *IEEE IT Professional,* vol. 8, no. 2. pp. 43-48, Mar./Apr. 2006.

[32] J.M. Rabaey, M.J. Ammer, J.L. da Silva Jr., D. Patel, and S. Roundy, "Picoradio Supports Ad Hoc Ultra-Low Power Wireless Networking," *IEEE Computer,* vol. 33, no. 7, pp. 42-48, July 2000.

[33] T.S. Rappaport, *Wireless Communications: Principles and Practice.* Prentice-Hall, 1996.

[34] J.R. Smith, K.P. Fishkin, B. Jiang, A. Mamishev, M. Philipose, A.D. Rea, S. Roy, and K. Sundara-Rajan, "RFID-Based Techniques for Human-Activity Detection," *Comm. ACM,* vol. 48, no. 9, pp. 39-44, 2005.

[35] A.M. Tekalp, *Digital Video Processing.* Prentice-Hall, 1995.

[36] M. Torlak and G. Xu, "Blind Multiuser Channel Estimation in Asynchronous CDMA Systems," *IEEE Trans. Signal Processing,* vol. 45, no. 1, pp. 137-147, Jan. 1997.

[37] M.M. Van Hulle, "Edgeworth Approximation of Multivariate Differential Entropy," *Neural Computation*, vol. 17, no. 9, pp. 1903-1910, 2005.

[38] K. Woyach, D. Puccinelli, and M. Haenggi, "Sensorless Sensing in Wireless Networks: Implementation and Measurements," *Proc. Int'l Symp. Modeling and Optimization in Mobile Ad Hoc and Wireless Networks*, Apr. 2006.

[39] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication," *Proc. IEEE Int'l Conf. Comm. (ICC '07)*, pp. 4646-4651, June 2007.

[40] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "A Physical-Layer Technique to Enhance Authentication for Mobile Terminals," *Proc. IEEE Int'l Conf. Comm. (ICC '08)*, pp. 1520-1524, May 2008.

[41] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "MIMO-Assisted Channel-Based Authentication in Wireless Networks," *Proc. Conf. Information Sciences and Systems (CISS '08)*, pp. 642-646, Mar. 2008.

[42] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Using the Physical Layer for Wireless Authentication in Time-Variant Channels," *IEEE Trans. Wireless Comm.*, vol. 7, no. 7, pp. 2571-2579, July 2008.

Neal Patwari received the BS and MS degrees from the Virginia Polytechnic Institute and State University in 1997 and 1999, respectively, and the PhD degree from the University of Michigan, Ann Arbor, in 2005, all in electrical engineering. He was a research engineer at Motorola Labs, Florida, between 1999 and 2001. Since 2006, he has been at the University of Utah, where he is an assistant professor in the Department of Electrical and Computer Engineering, with an adjunct appointment in the School of Computing. He directs the Sensing and Processing Across Networks (SPAN) Lab, which performs research at the intersection of statistical signal processing and wireless networking. His research interests include radio channel signal processing, in which radio channel measurements are used to improve security and networking and to perform localization. He received the US National Science Foundation CAREER Award in 2008 and the IEEE Signal Processing Society Best Magazine Paper Award in 2009. He has served on technical program committees for IEEE conferences SECON, ICDCS, DCOSS, ICC, RTAS, WoWMoM, ICCCN, and MILCOM. He is an associate editor of the *IEEE Transactions on Mobile Computing*. He is a member of the IEEE.

Sneha Kumar Kasera received the master's degree in electrical communication engineering from the Indian Institute of Science, Bengaluru, India, and the PhD degree in computer science from the University of Massachusetts Amherst. He is an associate professor in the School of Computing, University of Utah, Salt Lake City. From 1999 to 2003, he was a member of technical staff in the Mobile Networking Research Department of Bell Laboratories. He has held research and development positions at Wipro Infotech and at the Center for Development of Advanced Computing, Bengaluru. His research interests include computer networks and systems encompassing mobile and pervasive systems and wireless networks, network security and reliability, social network applications, overload and congestion control, multicast communication, and Internet measurements and inferencing. He is a recipient of the 2002 Bell Labs President's Gold Award for his contribution to wireless data research. He has served on many technical program committees including those of ACM MobiCom, ACM Sigmetrics, IEEE INFOCOM, IEEE ICNP, and IEEE SECON, among others. He serves on the editorial boards of the *IEEE Transactions on Networking*, ACM/Springer *Wireless Networks (WINET)*, and Elsevier *Computer Networks (COMNET)* journals. He is a member of the IEEE.