Radio Frequency Time-of-Flight Distance Measurement for Low-Cost Wireless Sensor Localization

Steven Lanzisera, David Zats, and Kristofer S. J. Pister

***Abstract*—Location-aware wireless sensor networks will enable a new class of applications, and accurate range estimation is critical for this task. Low-cost location determination capability is studied almost entirely using radio frequency received signal strength (RSS) measurements, resulting in poor accuracy. More accurate systems use wide bandwidths and/or complex time-synchronized infrastructure. Low-cost, accurate ranging has proven difficult because small timing errors result in large range errors. This paper addresses estimation of the distance between wireless nodes using a two-way ranging technique that approaches the Cramér–Rao Bound on ranging accuracy in white noise and achieves 1–3 m accuracy in real-world ranging and localization experiments. This work provides an alternative to inaccurate RSS and complex, wide-bandwidth methods. Measured results using a prototype wireless system confirm performance in the real world.**

***Index Terms*—Real-time location systems, sensor networks, two-way ranging (TWR).**

I. Introduction

Wireless networks have become a part of daily life, and the addition of location awareness can change the application landscape. Mobile phones have low resolution capabilities today, and this is changing the way people plan, navigate, and consume information. Today's indoor wireless networks are almost universally unaware of device location, but the combination of data communication, location awareness, and low power will enable a new host of applications. Battery-operated wireless devices for tagging, locating, and sensing data in factories, hospitals, and other environments will be widespread, reducing costs and improving quality.

Determining device location has two parts. The first phase involves measuring a relationship between nodes (e.g., distance and angle), and the second phase uses these relationships to estimate location [1]. Radio frequency (RF) received signal strength (RSS) measurements are commonly used to estimate range, but the accuracy of this technique is poor even in the best of conditions [2]. The primary alternative is the use of ultra-wideband (UWB) RF ranging, and good ranging performance has been demonstrated. Although UWB transmitters are simple to implement and extremely low power, UWB receivers have proven to be highly complex and consume a large amount of power when providing communication performance comparable to narrowband radios. Some narrowband methods have been proposed that require time-synchronized and/or high-performance, specialized base station devices, and this added complexity and cost limit the application of these systems [2], [3]. The second phase turns these ranges into locations and has been widely studied [4]. There is a need for low-cost, simple ranging technology that provides the meter-level accuracy required for many localization problems.

This paper presents a burst mode, two-way ranging (TWR) method that closely approaches the theoretical lower bound for ranging accuracy in a noise-limited environment and achieves meter level accuracy in multipath environments. All nodes in the network are identical, simple to implement, and do not require time-synchronized infrastructure. The *code modulus synchronization* (CMS) method has an online measurement component and an offline range extraction component, and this separation simplifies implementation and improves performance. Measurements are taken at several carrier frequencies and combined together to mitigate the impact of multipath channel characteristics. These techniques are not specific to an individual standard, modulation scheme, bandwidth, or RF platform. They can easily be added to the digital baseband processor of most existing transceivers, thereby adding time-of-flight (TOF) ranging capability.

A prototype of the system was implemented using a commercially available 2.4 GHz radio, analog-to-digital interface electronics, a field-programmable gate array (FPGA), and a microcontroller. A 2 MHz bandwidth, frequency shift keying ranging scheme was implemented that is compatible with the common IEEE 802.15.4 standard. Measurements over a noisy channel show that the Cramér–Rao Bound (CRB) is nearly achieved at moderate signal-to-noise ratios (SNRs). Measurements taken in several environments show 1 m accuracy outdoors and 1–3 m accuracy indoors.

II. Localization and Time-of-Flight (TOF) Ranging

Determining the location of a device is called *localization*, and the localization problem typically consists of estimating the distance between nodes and then using these ranges to estimate location. The accuracy of a localization system is limited by the accuracy of the range estimates and the geometry of the network devices to be localized. This section contains an introduction to

Manuscript received January 30, 2010; revised June 09, 2010; accepted August 19, 2010. Date of publication January 24, 2011; date of current version February 02, 2011. The associate editor coordinating the review of this paper and approving it for publication was Prof. Henry Leung.

S. Lanzisera is with the Lawrence Berkeley National Laboratory, Berkeley, CA 94720 USA (e-mail: smlanzisera@lbl.gov).

D. Zats and K. S. J. Pister are with the University of California, Berkeley, Berkeley, CA 94720 USA (e-mail: dzats@eecs.berkeley.edu; pister@eecs.berkeley.edu).

Digital Object Identifier 10.1109/JSEN.2010.2072496

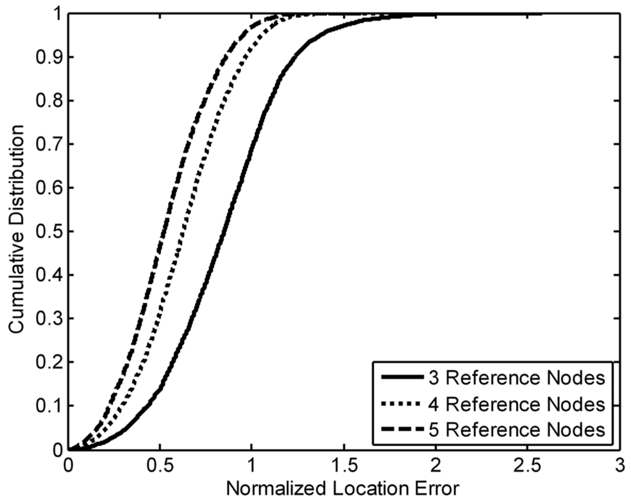

Fig. 1. CDF of location error normalized by the RMS ranging error.

localization, range estimation techniques, and typical application requirements.

A. The Localization Process and Accuracy Limitations

Multilateration is the basic process where range measurements between a device with unknown location and three or more reference devices are used to estimate a location in two dimensions. The best performing localization algorithms are similar to a minimum squared error (MSE) optimization with three or more range estimates. Fig. 1 shows the relationship between location error and range measurement error using MSE localization and randomly placed nodes. Increasing the number of reference nodes improves accuracy in the presence of range errors, therefore more reference nodes should be used than strictly necessary. The geometry of the reference nodes plays a significant role in device location. For example, if the reference devices are collinear, a unique location cannot be determined. If there are more reference nodes than required, geometry rarely limits localization accuracy. This area has seen significant research over the years, and the primary area for continued research in the second phase involves determining location when some measurements are highly erroneous [4].

B. Range Estimation Techniques

Measuring the range between two wireless devices has proven to be a challenging problem which has limited the use of location-aware wireless systems. RF RSS methods have been widely used due to simplicity. The RSS in free space decreases with the square of the distance between the transmitter and receiver, providing a one-to-one mapping from RSS to distance. In real environments, constructive and deconstructive interference cause the RSS to be unpredictable as a function of range, and this problem has been widely reported and recognized. Range measurements using RSS have proven to be unsuitable for most localization problems.

Measuring the RF signal TOF between nodes avoids many of the problems of RSS methods, but it is challenging on its own. RF signals travel at the speed of light, and one meter accuracy requires approximately 3 ns time resolution. On a low-cost, low-power system, it is difficult to achieve this accuracy. Typical radios can only resolve the time of events at the rate of their reference clock, resulting in resolution on the order of 50 ns (15 m), and special techniques and hardware must be employed to enable the required accuracy. RF TOFranging has seen widespread use in the global positioning system (GPS), but it has seen limited use in terrestrial systems due to problems with time accuracy, multipath channel effects, and system cost and complexity.

C. Application Requirements

Tagging and locating assets in buildings is the primary application for this technology, and room-level accuracy ($\sim 3\ \mathrm{m}$) is typically sufficient. Deployments must be low cost and should not require dedicated wiring. This prevents the widespread use of time difference of arrival techniques, which are typically time synchronized and require dedicated wiring. To further reduce cost, the transceiver should be compatible with the IEEE 802.15.4 standard widely used in wireless sensor networks (WSNs) [5].

III. Sources of TOF Ranging Error

TOF range estimation accuracy is primarily limited by clock synchronization, noise, sampling artifacts, and multipath channel effects. This section addresses each error source and currently available techniques for error mitigation.

A. Clock Synchronization

TOF ranging systems need to estimate the time of transmission and arrival using a common time reference. In a simple case, two wireless devices, A and B, measure their separation with B measuring the time of arrival of a signal sent by A. If the clocks are not perfectly synchronized, and B's notion of $t = 0$ is offset from A's, then this adds as an error to the measurement. The required time synchronization ($1\ \mathrm{ns} = 30\ \mathrm{cm}$) is too stringent for most systems.

Two-way time transfer (TWTT) is a TWR method that mitigates the effect of clock synchronization error [6]. It allows the time offset between A and B to be ignored. Both$A$ and B are responsible for measuring a time delay accurately using a local clock. If the time A sends the signal is t_{sA}, the time B receives the signal is t_{rB}, the time B replies to A is t_{sB}, the time A receives the signal back is t_{rA} such that $t_{sA} < t_{rB} < t_{sB} < t_{rA}$, then A measures $t_A = t_{rA} - t_{sA}$ and B measures $t_B = t_{sB} - t_{rB}$. The TOF , $\hat{\tau}$, can be estimated by combining these two measurements

$$\hat{\tau} = \frac{t_A - t_B}{2}. \tag{1}$$

In TWR, the measurement takes place over a relatively long period of time, so if the reference frequencies at the two nodes are not identical, an unknown bias will be added to the signal. The system must account for the clock frequency offset (i.e., clock drift) error. Mitigation methods have been developed for wireless systems, and one of these algorithms is required for TWR [5].

RF time difference of arrival (RF TDOA) techniques also combat time synchronization issues by having wired infrastructure time synchronized to better than 1 ns. The mobile devices transmit a signal, and the RF TDOA at the base stations is used to estimate range. The interested reader is directed to [2] and [7].

B. Noise

A range measurement degraded only by white noise is limited in accuracy by the signal energy-to-noise ratio, E_s/N_0, at the receiver and the occupied bandwidth, B. Ranging is a problem that has been studied in the context of radar applications, and the CRB provides a lower bound for the variance of the range estimate in white noise. For a one-way ranging system using IEEE 802.15.4 modulation, the CRB is

$$\sigma_{\hat{r}}^2 \geq \frac{c^2}{\frac{4\pi^2 B^2 E_s}{N_0}}. \tag{2}$$

The variance of the range estimate is $\sigma_{\hat{r}}^2$, c is the speed of light, and B is the occupied signal bandwidth in Hertz [8]. The SNR is related to E_s/N_0 in that

$$\frac{E_s}{N_0} = t_s B \cdot \mathrm{SNR} \tag{3}$$

where t_s is the signal duration during which the bandwidth is occupied. In many common signals, the bandwidth and duration are tied together such that $t_s B \approx 1$. Therefore, the E_s/N_0 ratio is approximately equal to the SNR. Signals with $t_s B > 1$ would exhibit better noise performance at lower SNR values, and ranging signals with this characteristic are called *pulse-compressed waveforms*. For a fixed-signal energy and noise density, increasing the bandwidth provides improvements in noise performance. This is one argument for wide bandwidth ranging systems, but the bandwidth required to achieve reasonable noise performance is not large. The CRB can be closely approached in many cases where $E_s/N_0 \gg 1$, and this is the intended target area for most communication systems. Both bandwidth and E_s/N_0 play significant roles in determining noise-limited performance [8].

In TWR systems such as radar or TWTT, the noise limit is reduced by the round trip nature of the measurement. In radar systems a single measurement is made that is twice the desired range, thus reducing $\sigma_{\hat{r}}^2$ by a factor of 4. In TWTT, two measurements are made and averaged to get the range estimate resulting in a $\sigma_{\hat{r}}^2$ reduction of 2. These effects simply add constants to the denominator of (2).

Fig. 2 shows the CRB as a function of bandwidth for E_s/N_0 of 10 dB and 26 dB. Signals with $t_s B$ products up to 1000 are easily achievable enabling large E_s/N_0. It is interesting to note that noise alone does not prevent 1 m accuracy for bandwidths down to a few megahertz.

C. Sampling Artifacts

It is commonly believed that the resolution of a TOF measurement depends directly on the sampling rate [3]. Known as *range binning* [9], this occurs when a matched filter is used to estimate the time of arrival with a sampling rate of up to $f_s = 2B$. Sampling adds error to the estimate because the estimate space is divided up into range bins that are c/f_s wide. Sampling adds uniform range uncertainty in each bin of σ_s^2

$$\sigma_s^2 = \frac{c^2}{12 \cdot f_s^2}. \tag{4}$$

In the case of the IEEE 802.15.4 example, with sampling at $1/B$, $B = 2$ MHz, the variance due to sampling can be calculated to be $(43m)^2$. Continuous tracking, filtering, or averaging can be used to improve the resolution, but this is not bandwidth or power efficient. Using just averaging, over 1000 measurements are required to achieve a variance of $(1m)^2$, and an improved TWTT method would require over 30 measurements [3]. To reduce this error, the signal can be oversampled. Fig. 3 shows the CRB for a 2 MHz bandwidth signal with E_s/N_0 of 26 dB, the standard deviation of the range error due to sampling, and the combined effect of both error sources. One must sample very fast to have the error dominated by the CRB rather than sampling when E_s/N_0 is at the high values possible in communications. As E_s/N_0 is reduced, the sampling rate required remains higher than twice the signal bandwidth, down to E_s/N_0 of about 3 dB. In IEEE 802.15.4 systems E_s/N_0 is typically

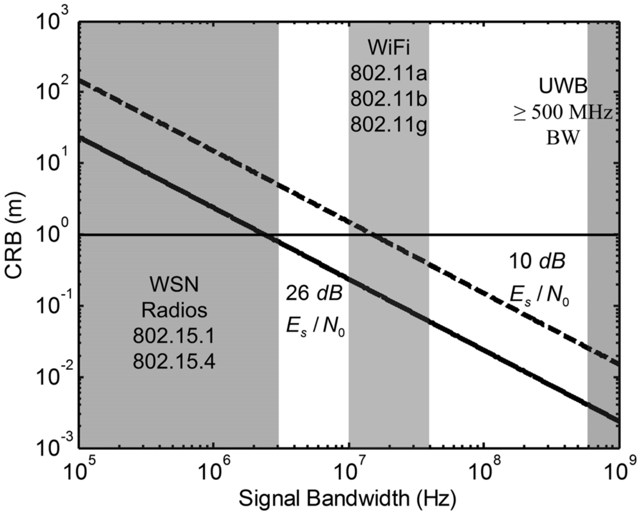

Fig. 2. CRB as a function of bandwidth.

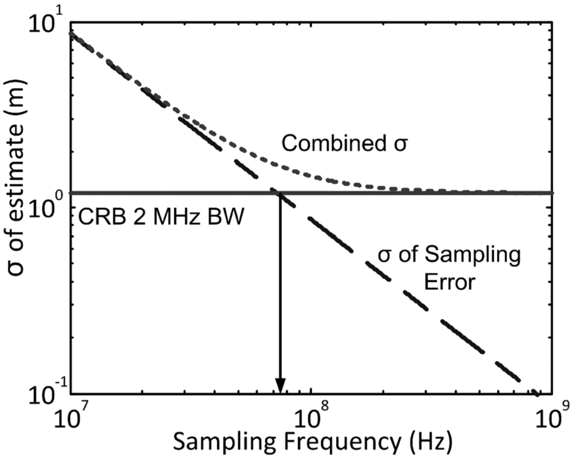

Fig. 3. Comparison of CRB to sampling induced error as a function of sampling frequency.

between 15 dB and 30 dB [10], enabling reasonable noise performance.

If the signal is sampled above Nyquist ($f_s > 2B$), the signal's entire information content is captured, and better time resolution than σ_s is possible. Interpolation between samples can yield significant improvements in resolution [5], but a major challenge is that many systems would need to perform this interpolation in real time, increasing system complexity and power consumption beyond reasonable limits [11].

D. Multipath Channel Effects

RF signals bounce off objects in the environment, causing the signal to arrive at the receiver through many paths. This is common indoors, and it is possible that the indirect paths have higher power than the direct path [12]. The communication environment is called the *channel,* and multipath channels are specific to the environment (e.g., office and outdoors) and the specific transceivers' geometry in that environment. The channel impulse response can be modeled as a series of complex delta functions in time

$$h_c(t) = \sum_{i=0}^{N} A_i \delta(t - \tau_i) e^{j\phi_i}$$

where A_i, τ_i, and ϕ_i are the amplitude, time, and phase delay of the ith path, with $i = 0$ representing the direct path. A_i, τ_i, and ϕ_i are random parameters, and a variety of distributions are commonly applied to them [12]. The transmitted signal, $m(t)$, is given as follows in phasor notation:

$$m(t) = \mathrm{Re}\{e^{j(\omega t + \theta(t))}\}.$$

In $m(t)$, the time-dependent phase term represents frequency or phase modulation, and the signals of interest have constant amplitude that can arbitrarily be set to unity. The received signal is the convolution of the transmitted signal and the channel with additive white noise

$$s(t) = m(t) * h_c(t) + n(t).$$

The noise term n will be ignored in this analysis, as it has negligible impact on multipath performance. If $h_c(t)$ consists of only two paths, we can write the entire received signal

$$s(t) = \mathrm{Re}\Big\{A_0 e^{j(\omega t + \theta(t-\tau_0))} e^{-j\omega\tau_0} e^{j\phi_0} + A_1 e^{j(\omega t + \theta(t-\tau_1))} e^{-j\omega\tau_1} e^{j\phi_1}\Big\}. \quad (5)$$

Although A_i, τ_i, and ϕ_i are random variables, they are frequency-independent over a given RF communication band. Over small periods of time, these parameters can be considered constant, and ω (carrier frequency) can be used to manipulate the relative phase of these paths.

Changing carrier frequency even by a few megahertz can dramatically affect the apparent multipath environment in narrowband systems. Moving one transceiver by just a fraction of a wavelength ($\lambda = 12$ cm at 2.4 GHz) will cause the receiver to see what looks like an entirely new multipath environment because the paths will interfere differently [13]. In some localization systems, the devices and environment may move slowly such that ranges taken over a short period of time can be considered to be taken in a static channel.

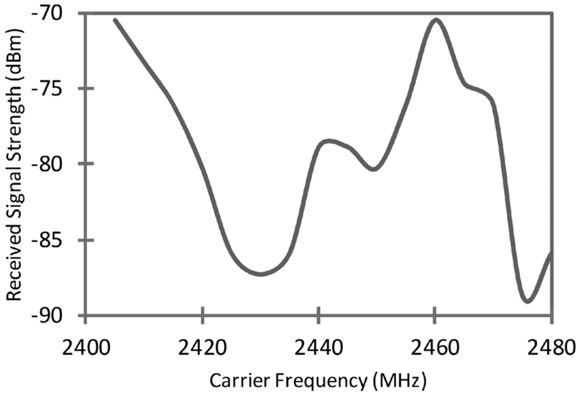

Fig. 4. Measured RSS as a function of frequency.

The frequency dependence of the channel can be observed by measuring the RSS profile across carrier frequency in an indoor environment for fixed transmitter and receiver geometries, as shown in Fig. 4. At some carrier frequencies, the signal experiences deconstructive interference (referred to as *fading*), while at others it has much higher signal strength due to constructive interference. Without knowing the channel characteristics, knowledge of the RSS at one frequency tells you little about the RSS at a nearby or distant frequency. Communication signals with bandwidth larger than the reciprocal of the time between the first and last significant paths (the *delay spread*) are largely immune from fading because it is sufficient for a most of the signal bandwidth to be observable at the receiver.

In a ranging system, however, the delay spread is not the critical parameter. If a receiver can estimate the first path arrival, this will be the shortest length, and thus the desired estimate. If the system is unable to resolve the individual paths, the estimate is blurred by the multipath effects, resulting in estimation error. Therefore, the typical interpath delay, $t_{\Delta p}$, is the critical value. Indoors, inter-path delays of 5–10 ns are common and must be resolved if accuracy is to be better than a few meters [14]. The bandwidth required for this is greater than $1/t_{\Delta p}$, or > 100 MHz.

There are several techniques available for reducing the impact of multipath, and they fall into three basic categories: 1) increasing bandwidth; 2) estimating the channel impulse response; and 3) multipath bias reduction. The first two methods have received some attention from researchers with varying degrees of success. The third category has not received significant attention in the literature, and a basic algorithm to reduce multipath bias is presented in Section IV.

Typical WSN radios do not use large bandwidths capable of resolving the individual paths, but the recent IEEE 802.15.4a standard has a UWB physical layer option. UWB transceivers use more than 500 MHz of bandwidth, which is sufficient to resolve the individual paths in the channel. Unfortunately, continuing research shows that although UWB transmitters are simple and low power to implement, UWB receivers with comparable

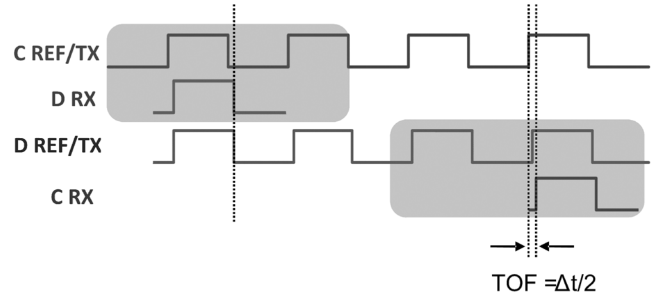

Fig. 5. Baseband signals used in code modulus synchronization.

performance (communication range and linearity) consume dramatically more power than their narrowband counterparts [14].

The second method for attempting to mitigate the impact of multipath interference is through indirect channel estimation, either through a super-resolution method or frequency domain channel characterization. A super resolution algorithm is one that provides range resolution that is better than $1/B$ when there is sufficient E_s/N_0 to resolve meaningful channel information. The interested reader is referred to [2], [13], [15] for more information. In IEEE 802.15.4, the achievable accuracy appears to be insufficient; the estimated time resolution would be $\sim 125\ \mathrm{ns}$ or $> 30\ \mathrm{m}$.

IV. Ranging Error Mitigation Techniques

This section presents two new methods that, when combined together, combat the error sources discussed in Section III. *Code modulus synchronization* is a new method of round-trip TOF ranging that mitigates the effects of sampling and poor time synchronization. A *frequency diverse range estimation* method is also presented that successfully improves range estimation accuracy, while not requiring time-synchronized infrastructure, complex base stations, or special wide bandwidth transceivers.

A. Code Modulus Synchronization (CMS)

Code modulus synchronization (CMS) emulates a full duplex ranging system using half-duplex radios such as those used in WSNs.The delay between reception and retransmission must be managed carefully. CMS uses a periodic signal (such as a square wave or a pseudorandom code) modulating an RF carrier as the ranging signal so that large Bt_s is possible. Fig. 5 shows the operation of the CMS using a square wave baseband signal. The first node, C, generates a local baseband ranging signal, shown on the top line (C REF/TX). This code is used to modulate the carrier and, in the shaded region, is transmitted to the second node D. D has a local clock with the same period as at C, but the phase of the clocks are offset. As a result, D knows the length of the incoming code, but it does not know the phase offset in the clocks. D samples and demodulates this signal, and exactly one circularly shifted copy of the code is stored in memory (shown on line 2, D RX, in the shaded region). At this point, D has a local copy of the code that is circularly shifted due to the clock phase offsets between C and D, and this reference code is shown on line 3 (D REF/TX). After C has sent the code and D has received the code, the transceivers switch states, and D is now the source of the code. Node D transmits two copies of the circularly shifted code it received back to C, and this transmission is shown in the shaded box over line 3. Node C receives the signal and records it synchronized to its local reference shown on line 1. Because of the round-trip nature of the system, the circular shift that occurred going from C to D is exactly undone going from D to C. After C has received the code, the transceivers are shut off, and all of the real-time processing is completed.

Node C then computes the cross correlation between the code it recorded and the code that it sent; the measured code offset is the time of flight. Because this system relies on sampling the signal above Nyquist, the received code can be interpolated to improve resolution up to the noise limit of the system. The correlation and code offset estimation are not done in real time, enabling the computation to be done at any time using any method the user desires. This system can approach the CRB in a single measurement, substantially improving over other TWR methods.

Multiple copies of the code can be sent in order to increase E_s/N_0. The receiving system can accumulate (average) multiple copies of the code to increase t_sB, but each is exactly one copy of the code that is circularly shifted in the same way as the other received copies. Averaging of multiple copies is important for achieving good noise performance, and it does not change the system's ability to resolve the TOF accurately.

In TWTT, the time-of-arrival must be determined at both nodes involved in the range estimation, but in CMS only one node performs this calculation. Therefore, while CMS enables better sampling performance, the full processing gain of the system is not realized at the second node. This causes an apparent noise penalty. At the same time, CMS consists of a single range estimate just like in radar, resulting in the same factor of 2 noise benefit compared to TWTT. Ignoring the impact of the transmitter and receiver transfer functions for simplicity, the effective E_s/N_0 for TWTT is

$$\left(\frac{E_s}{N_0}\right)_{\mathrm{TWTT}} = \frac{\overline{S_r^2}}{\overline{N^2}} \cdot \alpha n$$

where α is the number of code copies averaged and n is the code length. The time-of-arrival is not estimated at node C in CMS, and the signal sent from D to C contains noise from the first leg of the trip. For CMS, then, E_s/N_0 is

$$\left(\frac{E_s}{N_0}\right)_{\mathrm{CMS}} = \left(\frac{E_s}{N_0}\right)_{\mathrm{TWTT}} \cdot \frac{\alpha}{\overline{N^2} + \alpha}.$$

The last factor in (5) represents the noise penalty of CMS versus TWTT under the constraint $\overline{S_r^2} + \overline{N^2} = 1$. This term is unity at infinite SNR because there is no penalty (processing gain provides no benefit without noise). At very low SNR ($(n^2)^- \approx 1$), the penalty term is approximately 1/2 if no averaging is used ($\alpha = 1$). The worst-case performance degradation is at low SNR, and this factor is cancelled by the factor of 2 difference between the TWTT averaging effect and the CMS single measurement effect. For moderate to large values of α, the penalty term approaches unity (no penalty). CMS with averaging provides better noise performance than TWTT, and it is easy to avoid the sampling penalties common in TWTT.

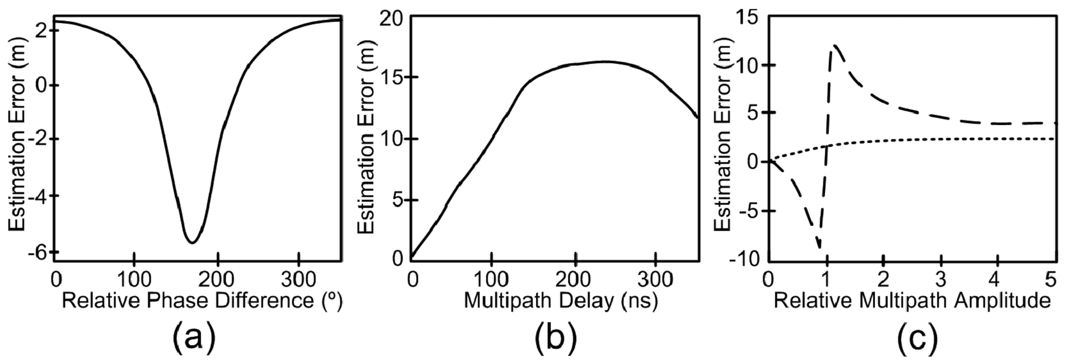

Fig. 6. Impact of multipath signal on range error for relative mulitpath (a) phase, (b) delay, and (c) amplitude.

After a single measurement, the variance, σ_r^2, for TWTT or the enhanced version of TWTT presented in [3], is given by (4). Comparing (4) to the CMS bound, given by

$$\sigma_r^2 = \frac{c^2}{\frac{16\pi^2 B^2 E_s}{N_0}}$$

we find that CMS has a better single measurement variance

$$\frac{\sigma_{r,\text{CMS}}^2}{\sigma_{r,\text{TWTT}}^2} = \frac{3f_{\text{sample}}^2}{\frac{4\pi^2 B^2 E_s}{N_0}}.$$

Substituting for f_{sample} the factor βB where β represents how much faster the sampling is than the signal bandwidth, we find that if

$$\beta < 2\pi\sqrt{\frac{E_s}{3N_0}}$$

then CMS provides better performance than TWTT. This result is directly in line with Fig. 3, where signals must be highly oversampled to achieve performance approaching the CRB unless CMS is used.

B. Frequency Diverse Range Estimation

We present a multipath mitigation technique that requires minimal processing and relies on the properties of the multipath environment and the signal demodulator. Measurements taken at several carrier frequencies are combined to reduce the bias in the TOF estimate. The impact of multipath on the demodulator output is critical to understanding this technique.

The signal demodulator is a simple digital frequency detector. The most common receiver for IEEE 802.15.4 is a low intermediate frequency (low-IF) receiver with FM demodulation at the low-IF. The incoming modulated sinusoid has its period measured with a counter from rising edge to rising edge and falling edge to falling edge. The counter output is applied to a lookup table to determine the demodulation value. This structure is simple, produces a multibit output, and has reasonable noise performance.

The simplest multipath situation has a direct path and a single other path that arrive with some relative time delay, t_d, and carrier phase, θ. Both t_d and θ affect the demodulator output, but only θ depends on ω (see (5)). In the case of IEEE 802.15.4, minimum shift keying (MSK), a version of frequency shift keying, is used. In MSK the modulation signal is square and changes between ω_1 and ω_2. In Section III-C, we assumed that ω was constant for the two paths. Immediately after a ω_1 to ω_2 change, however, the direct path is at ω_2 and the second path is at ω_1. Now, the composite received signal is the sum of two sinusoids at different frequencies and has rapid magnitude and phase changes. These changes are nonsinusoidal and affect the demodulator output.

The multipath induced bias is a function of the relative multipath amplitude, phase, and delay, and the bias can be positive or negative depending on the relative phase of the paths. This is an important fact because it is intuitive to believe that only positive biases are possible. Simulations of the two path multipath environment are presented in Fig. 6. Fig. 6(a) shows how varying θ impacts the range estimate when the relative delay and amplitude are fixed to 20 ns and 1/2, respectively. The trend associated with varying relative multipath delay when θ is set for maximum error and the relative multipath amplitude is set to 1/2 are shown in Fig. 6(b). As the relative delay increases, the magnitude of the bias increases. Eventually the delay is large enough that it can be differentiated from the direct path, and the error decreases. Fig. 6(c) shows the case when θ is set for maximum and minimum error, relative delay is fixed at 20 ns, and for varying relative multipath amplitudes. The key conclusions are that both positive and negative biases occur, and the magnitude of the biases increases with delay.

From the trends in Fig. 6, it is instructive to consider how to best estimate the true time of flight when presented with a series of measurements taken over the same channel with different phase relationships. To generate measurements with different phase relationships, the measurements are taken at different carrier frequencies. From the figures, it appears that an average value will reduce the overall bias. A more detailed study of the bias over a wider set of conditions is required to develop a heuristic for reducing overall bias.

Simulated multipath channels generated by the IEEE 802.15.4a working group for indoor office and residential environments were used to simulate 200 multipath environments [16]. For each channel, range was estimated on each of the 16 IEEE 802.15.4 carrier frequencies in the 2.4 GHz band, using an algorithm consistent with the methods presented in this

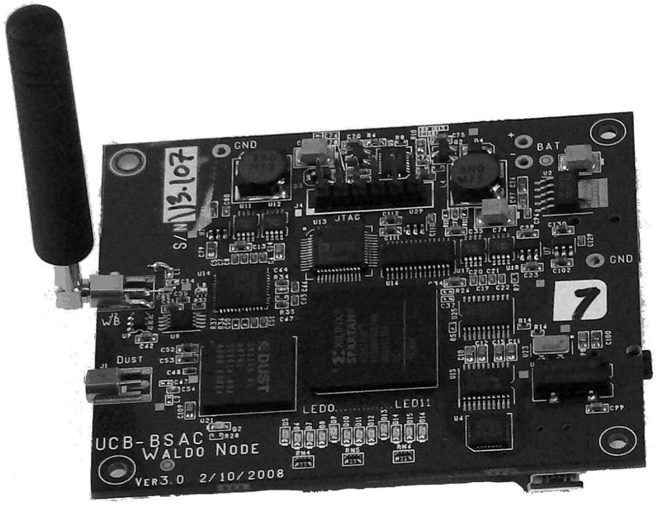

Fig. 7. Photograph of the 7.5 × 6 cm Waldo software defined radio platform.

work. The median of the 16 estimates had the best error performance, with over 80% of the simulated channels producing errors less than 3 m. The mean value produced worse estimates ($80\text{th percentile} \sim 6\text{ m}$). The median value performs better because it is less influenced by single measurements that are far from the median. These "outlier" measurements occur when the channel is in deep-fade.

The median of the estimates provides a reduced bias estimate of the TOF, is simple to compute, and requires no phase-coherent measurements, greatly simplifying implementation. This method is selected for use in the implemented ranging demonstrations.

V. Prototype Ranging System

The presented ranging system is a combination of new algorithms that require custom, yet simple, hardware to implement. To demonstrate these ideas, a software-defined radio platform, dubbed *Waldo*, was developed (see Fig. 7). This platform consists of a 2.4 GHz radio, digital to analog interfaces, an FPGA, a microcontroller, and the corresponding Verilog and embedded C code required for correct system operation. Waldo is designed for battery-operated field use, and no external PC or other hardware is required.

The presented ranging system was implemented on Waldo, and the test signal occupies a 2 MHz RF bandwidth using binary frequency shift keying at a deviation of $\pm 0.75\text{ MHz}$ at 1 Mchip/s (similar to IEEE 802.15.4). The received signal is sampled at a low IF of 5 MHz and demodulated in the digital domain. The demodulated data is limited to 2 MHz bandwidth and is sampled at 16 MHz yielding range bins of 19 m.

The entire ranging procedure from the perspective of the node originating the ranging operation (Node C in Fig. 5) is shown in Fig. 8. The ranging operation starts with the exchange of a packet and acknowledgement between the two nodes. This packet contains configuration information required for ranging. A range operation following the procedure outlined in Section IV-A using each of the sixteen carrier frequencies available to IEEE 802.15.4 transceivers. After these measurements have been completed, the resulting data is analyzed in software to estimate the time offset for each carrier frequency. The estimated time offset varies from frequency to frequency, as described in Section IV-B. All 16 measurements are reported, and the median of these 16 values is used as the TOF estimate.

In this implementation, 32 copies of the 2 chip signal are averaged after demodulation for a t_sB product of 64, while maintaining code modulus synchronization. The peak estimation algorithm uses a linear regression across several correlation points on either side of the peak and calculates where these two lines intersect. This method is faster and has equivalent noise performance to a low-pass interpolation of the correlation data followed by a traditional *dual correlator* peak search.

VI. Prototype Experimental Results

The implemented system is capable of performing range measurements with noise performance (repeatability) meeting or exceeding those demonstrated by systems with greater instantaneous bandwidth and/or sampling rate [17], [18], while having better than 3 m accuracy in ranging and localization experiments.

A. Noise Performance

To verify performance in a noise channel, two Waldo devices were connected via a RF cable and a variable attenuator. Fig. 9 shows the standard deviation of ranging measurements as a function of baseband SNR, the CRB for this system, and the range binning limit (previous work) [3]. One thousand measurements were taken at a single frequency and baseband SNR to generate each point in the figure. At high values of SNR, the system does not achieve the CRB because of the limited dynamic range of the digital baseband processor. CMS performs within a factor of 2 of the CRB, demonstrating that at an SNR of 6 dB ($E_s/N_0 = 30\text{ dB}$) equivalent performance using TWTT would have required a sampling rate of 60 MHz for a 2 MHz bandwidth signal.

B. Ranging Demonstrations

Ranging experiments were performed both indoors and outdoors to verify the performance of the proposed algorithms and the Waldo platform. A localization experiment was also performed to show that several identical, non-time-synchronized, battery-powered Waldo nodes could be used to form a network and localize a node in the network.

Two Waldo nodes were used to perform ranging estimates in a parking lot with some cars but mostly open space. The two nodes were not connected together in any physical way, and the only method of communication was through the wireless link. A range estimate using the proposed TOF method and RSS were taken at distances ranging from 1 to 45 m. The TOF and RSS range estimates are shown in Fig. 10. The TOF estimate is simply multiplied by the speed of light to yield the slope of unity shown in the plot. The equation that empirically minimized the mean-squared ranging error in this set of measurements was used for the RSS estimates. Even with this advantage, RSS performance is very poor compared to TOF. Approximately 80% of the TOF measurements are accurate to within 1 m, but not even 20% of the RSS based estimates are accurate to within 1 m.

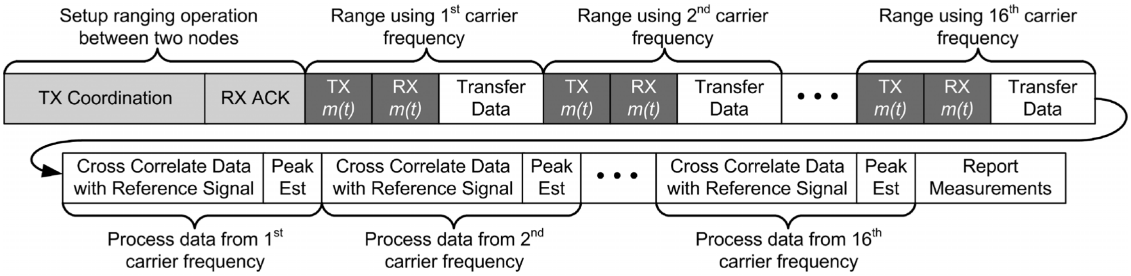
Setup ranging operation between two nodes
Range using 1st carrier frequency
Range using 2nd carrier frequency
Range using 16th carrier frequency
TX Coordination
RX ACK
TX m(t)
RX m(t)
Transfer Data
TX m(t)
RX m(t)
Transfer Data
• • •
TX m(t)
RX m(t)
Transfer Data
Cross Correlate Data with Reference Signal
Peak Est
Cross Correlate Data with Reference Signal
Peak Est
• • •
Cross Correlate Data with Reference Signal
Peak Est
Report Measurements
Process data from 1st carrier frequency
Process data from 2nd carrier frequency
Process data from 16th carrier frequency

Fig. 8. Activity at the initiating node for a ranging operation including setup, CMS ranging operations (dark gray), and data processing (white).

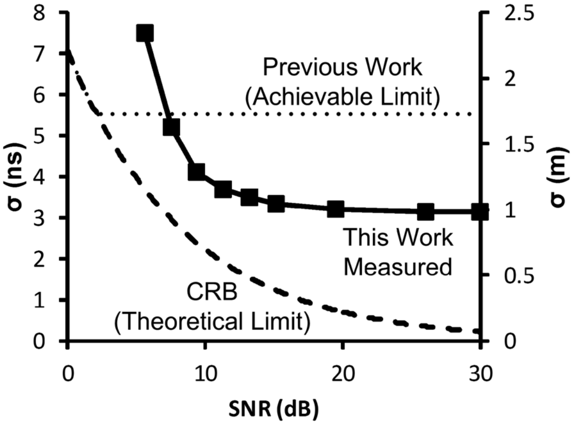

Fig. 9. Measured noise performance as a function of SNR.

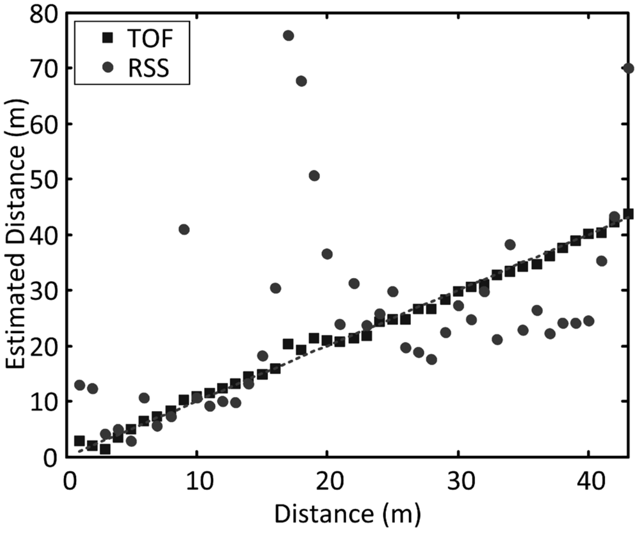

Fig. 10. Measured outdoor ranging performance.

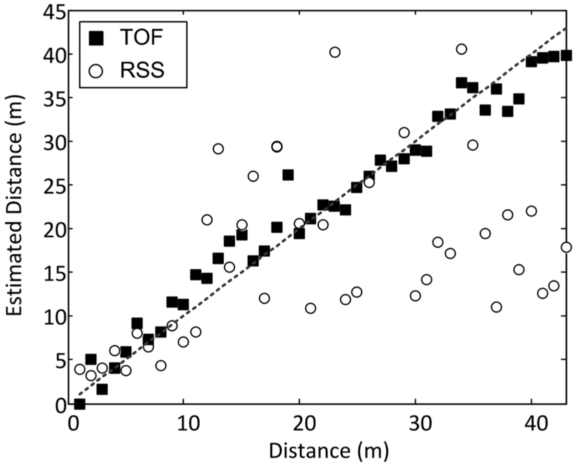

Fig. 11. Measured indoor ranging performance.

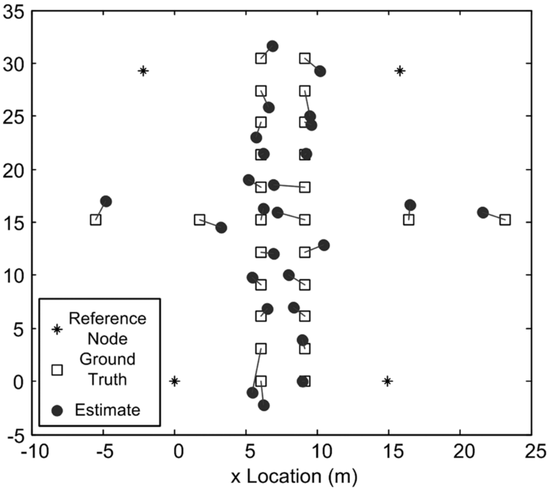

Fig. 12. Results of a four reference node localization experiment.

Indoor range estimates using the same setup were performed to verify that reasonable ranging accuracy can be achieved in environments typical to local area and sensor networks. The TOF and RSS measurements shown in Fig. 11 were taken in a cluttered hallway. The achieved accuracy for TOF was better than 1 m 50% of the time and better than 3 m 80% of the time. RSS achieved 8 m accuracy less than 50% of the time. There were no calibration steps or changes to the system firmware, software or calculation methods between this environment and the outdoor environment.

The localization experiment was performed in a relatively open area between two buildings. The approximate dimensions of the space are 50 m by 40 m with some trees and bushes in the area and buildings along two sides. Internode distances of up to 70 m were available, and communication and ranging could be performed at these distances. Four static nodes were setup on tripods, and a node was carried through the field. The results of the localization experiment are shown in Fig. 12, where the diamonds are reference nodes, the boxes are ground truth, and the circles are estimated location. Localization accuracy is better than 2 m for 80% of the estimates using a simple MSE estimate for location.

VII. CONCLUSION

Code modulus synchronization, a burst mode, TWR method, approaches the CRB without excessive over sampling, an improvement over previously published methods. Frequency diverse ranging is an easily implemented strategy that improves ranging performance in multipath environments. Combined, these techniques achieve 1 m ranging accuracy outdoors and 1–3 m accuracy indoors. A localization experiment further verifies performance. In communication systems where the E_s/N_0 is typically large, the effect of sampling has dominated noise-induced error in TWR systems, but CMS avoids this pitfall. Complex hardware and networks limit the application of location-aware networks, but the system presented here avoids this complexity without the need for specialized base stations, time synchronization, UWB, or other expensive and complex equipment.

REFERENCES

[1] N. Patwari *et al.*, "Locating the nodes: Cooperative localization in wireless sensor networks," *IEEE Signal Proc. Mag.*, vol. 22, no. 4, pp. 54–69, Jul. 2005.

[2] M. Pichler, S. Schwarzer, A. Stelzer, and M. Vossiek, "Multi-channel distance measurement with IEEE 802.15.4 (Zigbee) devices," *IEEE J. Sel. Topics Signal Proc.*, vol. 3, no. 5, pp. 845–859, Oct. 2009.

[3] K. Ahmed and G. Heidari-Bateni, "Improving two-way ranging precision with phase-offset measurements," in *Proc. IEEE Global Commun. Conf.*, 2006, pp. 1–6.

[4] K. Pahlavan *et al.*, "Indoor geolocation science and technology," *IEEE Commun. Mag.*, vol. 40, no. 2, pp. 112–118, Feb. 2002.

[5] S. Lanzisera and K. S. J. Pister, "RF ranging methods and performance limits for sensor localization," in *Localization Algorithms and Strategies for Wireless Sensor Networks*, G. Mao and B. Fidan, Eds. New York: Information Science Reference, 2009, p. 526.

[6] D. Kirchner, "Two-way time transfer via communication satellites," *Proc. IEEE*, vol. 79, no. 7, pp. 983–990, Jul. 1991.

[7] C. Hoene and J. Willmann, "Four-way TOA and software-based trilateration of IEEE 802.11 devices," *IEEE Personal, Indoor and Mobile Radio Commun.*, pp. 1–6, 2008.

[8] H. L. Van Trees, *Detection, Estimation, and Modulation Theory*. New York: Wiley, 2001.

[9] M. Richards, *Fundamentals of Radar Signal Processing*. New York: McGraw-Hill, 2005.

[10] S. Lanzisera, A. Mehta, and K. Pister, "Reducing average power in wireless sensor networks through data rate adaptation," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2009, pp. 1–6.

[11] S. Srirangarajan and A. Tewfik, "Localization in wireless sensor networks under non line-of-sight propagation," in *Proc. IEEE Global Commun. Conf.*, 2005, pp. 3477–3481.

[12] Q. H. Spencer, B. D. Jeffs, M. A. Jensen, and A. L. Swindlehurst, "Modeling the statistical time and angle of arrival characteristics of an indoor multipath channel," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 3, pp. 347–360, Mar. 2000.

[13] T. Watteyne, S. Lanzisera, A. Mehta, and K. Pister, "Mitigating multipath fading through channel hopping in wireless sensor networks," in *Proc. IEEE Int. Conf. Commun.*, May 2010, pp. 1–5.

[14] B. Lachartre *et al.*, "A 1.1 nJ/b 802.15.4a-compliant fully integrated UWB transceiver in 0.13 μm CMOS," in *Proc. Int. Solid State Circuits Conf.*, San Francisco, CA, 2009, pp. 312–313.

[15] N. Dharamdial, R. Adve, and R. Farha, "Multipath delay estimations using matrix pencil," *IEEE Wireless Commun. Networking*, vol. 1, pp. 632–635, Mar. 2003.

[16] A. F. Molisch *et al.*, IEEE 802.15.4a Channel Model – Final Report, Tech. Rep. Doc. IEEE 802.15-04-0662-02-004a, 2005.

[17] T. C. Karalar and J. Rabaey, "An RF ToF based ranging implementation for sensor networks," in *Proc. IEEE Int. Conf. Commun.*, 2006, pp. 3347–3352.

[18] S. Schwarzer, M. Vossiek, M. Pichler, and A. Stelzer, "Precise distance measurement with IEEE 802.15.4 (ZigBee) devices," in *Proc. EEE Radio and Wireless Symp.*, 2008, pp. 779–782.

Steven Lanzisera received the B.S. degree in electrical engineering from the University of Michigan, Ann Arbor, in 2002 and the Ph.D. degree in electrical engineering and computer sciences from the University of California, Berkeley, in 2009.

He was an Engineer with the Space Physics Research Laboratory, University of Michigan, from 1999 to 2002, where he worked on spacecraft integration and testing. He is currently a Researcher in the Environmental Energy Technologies Division at Lawrence Berkeley National Laboratory, where he studies energy use in buildings with a focus on distributed sensing, controls and appliance energy efficiency. He has published research on embedded systems, wireless communication, networking, integrated circuits, building energy efficiency, and public policy.

David Zats received the B.S. degree in computer science and engineering from the University of California, Los Angeles, in 2007 and the M.S. degree in electrical engineering and computer sciences from the University of California, Berkeley, in 2009. He is currently working towards the Ph.D. degree at the University of California, Berkeley, where his research focus is energy consumption in datacenter networks.

As Research Assistant at the Center for Embedded Networked Sensing (CENS), he worked on networks of wireless image sensor nodes.

Kristofer S. J. Pister received the B.A. degree in applied physics from the University of California, San Diego, in 1982, and the M.S. and Ph.D. degrees in electrical engineering from the University of California, Berkeley, in 1989 and 1992.

From 1992 to 1997, he was an Assistant Professor of Electrical Engineering with the University of California, Los Angeles. In 1997, he joined the Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, where he is currently a Professor and a Co-Director of the Berkeley Sensor and Actuator Center. He coined the term Smart Dust and pioneered the development of ubiquitous networks of communicating sensors. During 2003 and 2004, he was on industrial leave as CEO and then CTO of Dust Networks, a company that he co-founded to commercialize low-power wireless mesh networking for sensors. In addition to wireless sensor networking, his research interests include MEMS-based micro-robotics and low-power circuit design.