Hindawi Publishing Corporation
International Journal of Navigation and Observation
Volume 2012, Article ID 743625, 15 pages
doi:10.1155/2012/743625

Research Article

Receiver Design for Time-Based Ranging with IEEE 802.11b Signals

Reinhard Exel

Institute for Integrated Sensor Systems, Austrian Academy of Sciences, 2700 Wiener Neustadt, Austria

Correspondence should be addressed to Reinhard Exel, reinhard.exel@oeaw.ac.at

Received 3 December 2011; Revised 4 April 2012; Accepted 30 May 2012

Academic Editor: Armin Dammann

This paper presents a ranging receiver architecture able to timestamp IEEE 802.11b Wireless LAN signals with sub-100 picosecond precision enabling time-based range measurements. Starting from the signal model, the performance of the proposed architecture is assessed in terms of statistical bounds when perturbed by zero-mean additive white Gaussian noise (AWGN) as well as in case of multipath propagation. Results of the proposed architecture, implemented in a Field Programmable Gate Array-(FPGA-) based prototype, are presented for different environments. For AWGN channels, the prototype system is able to attain an accuracy of 1.2 cm while the ranging accuracy degrades in dynamic multipath scenarios to about 0.6 m for 80% of the measurements due to the limited bandwidth of the signal.

1. Introduction

Despite the fact that Global Navigation Satellite Systems (GNSSes) cover nearly 100% of the planet, satellite-based localization is not available within buildings as the roofing and walls deteriorate the signal to a degree where an error-less decoding is no longer possible. Mounting pseudolites, devices transmitting the navigation signals, under the roofs are certainly not a valid solution, not only due to legal restrictions. The differences between indoor and outdoor localization are more substantial than just the received power. Radio propagation within complex environments, typical for indoor scenarios, are challenging for high-speed wireless communication, but even tougher for any form of localization service.

Many localization concepts (e.g., based on ultrasonic, electromagnetic waves, inertial sensors) have been proposed to bridge the gap between GNSSes and the lack of indoor locating systems. Nevertheless, for indoor environments, there is still no general satisfactory solution available as different key factors, such as low power consumption and high refreshment rate are incompatible. One major reason why indoor radio localization systems are way behind satellite navigation solutions is that the majority of all current wireless communication standards have not been designed with position determination in mind. These signals are often referred to as Signals of Opportunity (SoO). In theory, adding a localization service upon an existing standard is always possible. However, the key parameters like accuracy, reliability, or cost depend on the restrictions of the wireless standard. As a result, retrofitting a localization service to an existing technology might turn out to be highly complex as, for example, the integration of the Enhanced 911 service into GSM networks. The degree of complexity depends primarily on the measurement principles ranging from Received Signal Strength (RSS) to time or angle measurements, or a combination of these. Some principles require proprietary hardware, while others only require software modifications, but impose other restrictions, such as limited range or accuracy. As a result, there is no generally best solution to retrofit localization to a communication standard.

In particular, Wireless LAN (WLAN) seems to be an interesting candidate for localization as it is a widely accepted industrial standard deployed in billions of mobile devices in home and office environments. RSS-based WLAN localization is a thoroughly investigated subject, and still the positional accuracy can be considered rather poor. Time-based localization methods like Time of Arrival (ToA) or Time Difference of Arrival (TDoA) are attractive not only for satellite-based positioning, but also for indoor applications. The fact

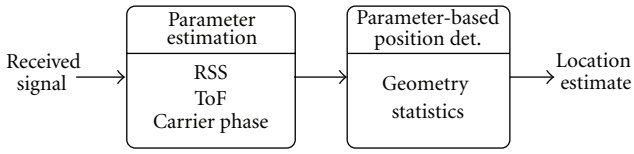

Figure 1: Two-step position determination.

that the measured time is a linear function of the range makes it an ideal candidate even for larger distances in contrast to RSS.

The outline of the paper is as follows. Section 2 describes the localization process and technologies related to WLAN locating. In the following section, the signal model and common cross-correlation TDoA estimation methods are discussed. The proposed receiver architecture able to measure the ToA by means of timestamping is found in Section 4. Section 5 discusses the error due to multipath propagation and mitigation techniques for the presented receiver architecture. Subsequently, a set of these receivers is used in a hardware implementation to assess the performance under various conditions in Section 6. The conclusion summarizes the findings, and finally an outlook for further investigations is given.

2. Related Work

2.1. The Localization Process. Locating a target in a radio localization system is based on the exchange of signals between the target and a number of base stations with known positions. In a network-based localization system, the location of the target can be calculated directly from the received signals collected by a locating unit or by the mobile device in case of handset-based localization. This approach is called direct position determination (DPD) [1]. Similarly, if an extraction of ranging parameters from the received signals precedes the position determination step, locating is based on a two-step approach as shown in Figure 1. While DPD offers higher performance for low signal-to-noise ratio (SNR) conditions [2], the joint position estimation increases the computational complexity of DPD and therefore decreases its practical applicability.

The simulations performed by [3] showed that DPD performs nearly identical than the conventional two-step approach, and DPD can only provide improved positional accuracy in case of difficult situations such as obstructed propagation paths. In this paper, we assume the commonly used two-step approach. The second step, position determination, can be grouped in subtasks starting with parameter conversion (propagation models, fingerprinting), preprocessing (filtering, weighting, selection), localization (nearest neighbor search, Bayesian or probabilistic approaches [4, 5]) up to tracking algorithms (Kalman or particle filtering, Markov models, neural networks [6]). Nevertheless, all these sophisticated methods depend on the quality of the parameter estimates of the first step. In this paper, we focus on the parameter estimation process, particularly for time-based WLAN ranging systems.

2.2. Related Work. RSS localization in WLANs is the most investigated solution as the measurement of the RSS is a mandatory feature in standard compliant WLAN devices. All that is required is to read the RSS information from the devices and collect it at the locating unit performing the localization based on fingerprinting or geometric approaches. One of the oldest RSS system is the RADAR system from Microsoft research [7] using fingerprinting techniques based on combining empirical measurements with signal propagation models. It can be considered as a network-based system as the APs collect the signal strength of all associated targets. In the recent past, a plethora of RSS propagation models have been proposed for WLAN modeling different environments, such as offices, parking lots, outdoor or industrial environments [8–10]. Despite all the effort and optimizations, the location accuracy of RSS solutions is poor, in the 2–20 m range depending on the environment and distance to the AP [11].

Time-based WLAN ranging has been analyzed by the authors of [12]. The basis for their approach is two-way ToA, where the target operates as interrogator sending ranging requests to the access point (AP). The round-trip time of the frame minus the turn-around time in the AP yields the time of flight in both directions. As neither the target nor the AP has any capabilities to perform accurate time measurements, the authors propose to use software timestamping within the Linux Kernel of the operating system (OS) in the AP and the target. Software timestamping is influenced by various jitter sources in the OS such as interrupt latency, bus arbitration, and therefore the measured round-trip times suffer from a large variance. With software modifications, the authors measured an average round-trip time of 269.83 μs with a standard deviation of 371 ns (corresponding to 111 m).

Even higher accuracy can be achieved directly in the physical layer. A WLAN mechanism exploiting the Request to Send/Clear to Send (RTS/CTS) handshake mechanism for two-way range measurements is presented in [13]. The authors have built a printed circuit board (PCB) supporting hardware timestamping, which starts a counter when transmitting an RTS frame. The counter stops when the CTS response frame from the target is received. Despite some concurrence and interference issues, which are mitigated through filtering and selection, the system is bound by the 22.72 ns resolution of the counter running with 44 MHz. To decrease the large variance of the measurement, robust linear regression techniques are used, averaging over 50 measurements. Even closer to the physical layer are methods processing the sampled baseband signal, for instance, methods based on dirty templates [14, 15], where a previously received signal is used as a correlation template. Alternatively, Generalized Cross Correlation-(GCC-) based ToA estimation methods are used for WLAN as well [16].

As alternative to cross-correlation, some authors have proposed to use subsample interpolation methods belonging to the group of super resolution methods, such as the Estimation of Signal Parameters via Rotational Invariance

Technique (ESPRIT), Root-MUltiple Signal Classification (RootMUSIC), or Matrix Pencil (MP) [17, 18]. Others prefer to estimate the ranging parameters in the frequency domain, such as the Prony method used by [19]. Compared with the matched filter approach, which is optimal in AWGN environments, these algorithms offer improved accuracy in multipath environments when the channel complies to a certain known model.

The Global Positioning System (GPS) also belongs to the group of time-based systems and can be considered similar to ToA WLAN localization. However, the properties of GPS are specifically designed for ranging applications, whereas WLAN was designed as more or less a cable replacement. The largest difference is that the GPS C/A code is permanently transmitted with a chip rate of 1.023 MChips/s and a data rate of just 50 bit/s [20]. In contrast, IEEE 802.11b WLAN employs a Carrier Sense Multiple Access (CSMA) scheme with 11 MChips/s and a data rate of up to 11 Mbit/s. As WLAN devices do not send constantly, they can naturally only be located during the transmission of frames. The received signal power and therefore the signal-to-noise ratio (SNR) in GPS are 60 dB and more lower than in WLAN, which is compensated in GPS by length of the Gold code used for signal correlation. In total, the higher chip rate of WLAN suggests that localization in WLANs should be even more accurate than GPS given the same channel conditions apply.

2.3. Previous Work. The work presented in this paper is based on previous investigations extended in terms of accuracy, multipath mitigation, and a detailed analysis of impairments. In [21], we described the basic measurement principle of WLAN ranging as a piggy-back solution to an existing WLAN transceiver architecture. Finally, we designed a stand-alone transceiver solution based on the Maxim 2822 transceiver chipset. The design considerations for the hardware platform are described in [22]. A predecessor of the receiver architecture achieving nanosecond precision is described in [23]. In all papers, we consider a network-based TDoA solution, where synchronized base stations capture the wireless signal and process it locally to generate ToA timestamps. These timestamps are submitted (together with frame identification information) to a central locating unit, which groups them by the unique frame check sum and performs parameter-based position determination, the second step of Figure 1. Taking timestamps in the base stations requires a priori knowledge of the modulation and frame format. Knowledge of the used modulation is required to decode the frame and to optimize the estimation algorithm. The structure of the wireless frame is necessary to detect a unique position within the frame (epoch) to take a timestamp. As the epoch is agreed among all base stations, the difference of two ToA timestamps yields a similar estimate as correlation-based approaches. The necessary synchronization of the base stations is only briefly discussed within this paper, different approaches based on wired and wireless synchronization can be found in [24]. As outlined in Section 6.1, all base stations are assumed to be supplied by a common clock sourced from an Ethernet switch.

3. Signal Model and Range Estimation Techniques

3.1. Signal Model. The data of a WLAN frame, according to the IEEE 802.11b standard [25], is modulated using either Differential Binary Phase-Shift Keying (DBPSK) or Differential Quadrature Phase-Shift Keying (DQPSK) in combination with Direct Sequence Spread Spectrum (DSSS) or Complementary Code Keying (CCK) baseband modulation. Common to all encodings is that the transmitted baseband signal can be expressed by a sum of periodic pulses as given in

$$s(t) = \sum_m a_m g(t - mT). \tag{1}$$

$s(t)$ describes the baseband signal neglecting any modulation to an RF carrier, $g(t)$ is a real-valued baseband pulse, $1/T$ is the chip rate, a_m is the sequence of complex-valued chips, and m refers to the chip counter. In particular for WLAN, the chip rate is $1/T = 11000\,000\,\mathrm{s}^{-1}$, the alphabet of a_m is $\{+1, -1\}$ in case of BPSK, and $\{+1, +\jmath, -1, -\jmath\}$ in case of QPSK. Given that the chip sequence a_m is wide-sense stationary, the transmitted signal $s(t)$ is a wide-sense cyclostationary process with period T. The cyclostationary property is obvious as the generated sequence has the same statistical properties as a time-shifted process $s(t - kT)$ for any arbitrary integer k. The actual shape of the baseband pulse $g(t)$ is not specified, but only the spectral mask for the transmit pulse in subsection 15.4.7.4 of the 802.11b standard [25]. That is, the side lobes 11 or 22 MHz apart from the carrier frequency must be suppressed by -30 or -50 dB with respect to the carrier.

The baseband signal is modulated to the RF carrier and demodulated again in the receiver. If the carrier frequencies in the receiver and the target are sourced from different oscillators, the carrier frequencies are not exactly the same as each oscillator is subject to different tolerances and jitter. The frequency of an oscillator can be modeled as the sum of the nominal frequency ω_n, a frequency skew $\Delta\omega$, and a random term $\overline{\omega}(t)$ as shown in

$$\omega(t) = \omega_n + \Delta\omega + \overline{\omega}(t). \tag{2}$$

Hence, the received signal includes also a residual carrier frequency skew $\Omega = \omega_t - \omega_\mathrm{l} = \Delta\omega_t - \Delta\omega_\mathrm{l}$ with $\Delta\omega_t$ and $\Delta\omega_\mathrm{l}$ the frequency skews of the transmitter and receiver with respect to the nominal frequency ω_n. The received signal $y(t)$ delayed by τ and with a phase offset θ and skew Ω in presence of AWGN noise $n(t)$ can therefore be described by

$$y(t) = \sum_m a_m g(t - mT - \tau) e^{\jmath(\theta + \Omega t)} + n(t). \tag{3}$$

Depending on the length of the transmitted frame and the joint stability of ω_t and ω_l, the residual carrier frequency may be considered constant or variable with time. For the latter case, some kind of carrier recovery algorithm has to constantly track Ω and remove it. The removal of the residual carrier frequency is commonly termed carrier wipeoff. The IEEE 802.11 standard requests that the oscillator used for

generating the carrier may deviate ±20 ppm from the nominal frequency; hence, each carrier recovery algorithm must be able to deal with up to ±49 kHz frequency skew from its nominal value.

Not only the carrier can be subject to minor frequency skews. The chip rate of receiver and transmitter may slightly vary due to oscillator tolerances. As the chip rate is considerably lower than the carrier frequency by a factor of more than 200, the impact of imprecise clocks on the receiver performance is far lower. As 20 ppm chip frequency skew is equivalent to a time stretch of ±20 ns/ms, it cannot be neglected for WLAN ranging applications with typical frame durations in the millisecond range. It should be noted that the chip and carrier frequency skew may be correlated if sourced from the same physical oscillator. In this case, the carrier skew estimate can be used to calculate the chip skew as the carrier skew estimate is about 100 times less noisy than the chip skew estimate as shown by [26] for GPS.

3.2. Range Estimation Based on Cross-Correlation. The estimate $\hat{\tau}_{21}$ (the hat notation is used to indicate that the variable is an estimate) for the propagation time difference of a signal transmitted by a target and received by two synchronized base stations in a TDoA system can be calculated by cross-correlation of the two received waveforms. Consider two base stations receiving a continuous time signal $x_i(t)$ with different zero-mean noise realizations n_i uncorrelated to s. Let the signals have different amplitudes A_i and phases θ_i, then the signals can be modeled as

$$\begin{aligned} x_1(t) &= A_1 e^{\jmath\theta_1} s(t-\tau_1) + n_1(t), \\ x_2(t) &= A_2 e^{\jmath\theta_2} s(t-\tau_2) + n_2(t), \end{aligned} \tag{4}$$

with $s(t)$ the baseband signal (see (1)). Then, the TDoA estimate $\hat{\tau}_{21} = \hat{\tau}_2 - \hat{\tau}_1$ can be found by maximizing the cross-correlation function R_{x_1,x_2} by

$$\hat{\tau}_{21} = \max_{\tau} \left| R_{x_1,x_2}(\tau) \right| = \max_{\tau} \left| \int_{-\infty}^{\infty} x_1^*(t) x_2(t+\tau)\, dt \right|. \tag{5}$$

This approach works without the knowledge of the transmitted data or modulation, given the transmitted signal's autocorrelation has a significant peak. Hence, continuous wave signals cannot be used as their autocorrelation is periodic.

The performance of the estimator can be improved by passing the signals through a filter with matched frequency response $H(f)$; this method is referred to as Generalized Cross-Correlation (GCC) [27, 28]. As the correlation and filtering are computationally simpler in the frequency domain, the TDoA estimation is often calculated using the Fourier transform as shown in (6) with $X_i(f)$ the Fourier transform of $x_i(t)$:

$$\hat{\tau}_{21} = \max_{\tau} \left| \int_{-\infty}^{\infty} H(f) X_1^*(f) X_2(f) e^{\jmath 2\pi f \tau} df \right|. \tag{6}$$

Apart from cross-correlation approaches neglecting the DSSS modulation characteristics, Cyclic Cross-Correlation (CCC) approaches can be applied to the baseband signal as well. CCC algorithms exploit the fact that the autocorrelation function of a cyclostationary signal is periodic and can therefore be expressed by a sum of functions $R^{\alpha}_{x_1,x_2}(\tau)$ with cycle frequencies α as [29]

$$R_{x_1,x_2}(\tau) = E\left[x_1^*(t) x_2(t+\tau)\right] = \sum_{\alpha} R^{\alpha}_{x_1,x_2}(\tau) e^{\jmath 2\pi \alpha t}. \tag{7}$$

While the GCC method is simpler, Gardner and Chen [30] have shown that the CCC method yields better estimation results (lower variance) based on a Monte-Carlo analysis. One particular issue with CCC is that the cyclic cross-correlation is dependent on the sum of the time delays $\tau_1 + \tau_2$ and a search through all possible delay values has to be performed to find the correlation peak [31]. Teplitsky and Yeredor [32] have extended the previous work and have proven analytically that CCC is in general better than GCC when comparing the lower estimation bounds by introducing a cyclic-correlation-based CRLB.

Although cross-correlation is a feasible instrument for estimating the TDoA in the baseband (e.g., for audio applications like [33]), the presence of carrier and chip frequency skews imposes restrictions to correlation-based methods. If the carrier frequencies among receivers are not phase-locked, then the residual frequency skew after the mixer is not the same in all receivers; the θ_is, modeling the phase and frequency skew, in (4) are then receiver dependent and time variable. Hence, the signals $x_i(t)$ are cyclostationary and the cross-correlation depends on the actual frequency skews. TDoA estimation using GCC (assuming stationary signals) is therefore no longer applicable unless the residual carrier frequency skew is removed in advance. Although frequency-locked loops exist that remove the carrier frequency skew for any kind of signal, such as the delay-and-multiply carrier recovery [34], Classen and Meyr showed that these algorithms provide only a poor frequency estimate [35]. Hence, carrier synchronizers neglecting the chip timing information (also called NDϵ algorithms [36]) can only be used at high SNR, thus limiting the possible range for locating systems.

Even in presence of carrier frequency skews, CCC methods can still be used. However, the introduction of carrier frequency skews increases the complexity by adding one search dimension. As the chip rate of common WLAN devices is uncorrelated to the carrier frequency, the estimation problem is extended by another dimension.

A particular issue with distributed signal capturing and centralized correlation methods is the transport of the sampling data to the correlation unit. If the system is intended to capture the data continuously, then a high-speed connection is required. For WLAN, a sample rate of at least 44 MHz is required, and given that each sample contains 8 bits, it requires a connection with at least 352 Mbps per receiver. Hence, for a simple scenario with 4 receivers, even a 1 Gbps connection to the locating unit is not sufficient. Due to these substantial drawbacks of correlation-based localization in WLANs, this paper proposes to perform ToA estimation in each base station and to calculate the position based on the TDoAs (from the ToAs) in the locating unit. Hence, the TDoA estimation is factored into ToA timestamping in each

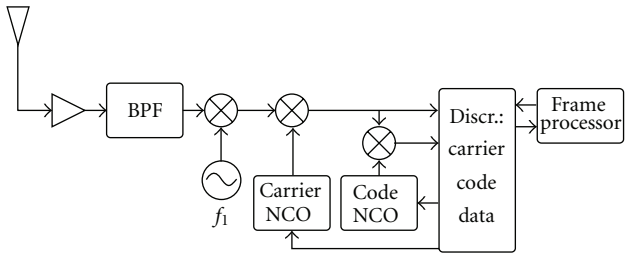

Figure 2: Generic receiver architecture.

base station instead of a joint estimation of the TDoAs using correlation methods.

4. Proposed Receiver Architecture

In the previous section, we have identified that the localization of a target by means of timestamping is an attractive approach. Timestamping requires that all base stations use a commonly agreed algorithm to capture the instant when a frame is received at a base station, which can range from stopping a counter, when a certain part of the frame is received (like in [13]), or more sophisticated approaches. To outline our approach, let us assume a standard receiver architecture as depicted in Figure 2, where the received signal from the antenna is amplified, bandpass filtered, and mixed with the carrier signal generated from a local clock source. Due to the inevitable residual carrier frequency skew (caused by oscillator clock skews and Doppler shifts), it must be wiped off by a carrier numerical controlled oscillator (NCO). The code NCO regenerates the code replica and wipes off the spread code using a multiplier followed by an integrate-and-dump block.

In many DSSS receivers (e.g., GPS chipsets), the code NCO is purely binary, and therefore the NCO only outputs a sign function simplifying the multiplication to an adjustable inverter. The drawback of this approach is that the alignment of the code replica is quantized by the clock period of the NCO. In this case, the clock period of the NCO should be significantly shorter than the chip period of the received signal. For instance, the GPS receiver presented in [37] uses a 20 MHz NCO frequency for the GPS chip rate of 1.023 MChips/s and generates ToA estimates with 50 ns quantization. Carrier and code NCO are driven by discriminators, which compute an error signal and steer the NCOs. Algorithms aligning the code replica to the received data are termed clock synchronizers or timing recovery, whereas algorithms aiming to remove the carrier frequency skew and phase offset are commonly called carrier, frequency or phase recovery. Since the rise of digital communication, synchronizers have been a well-established field of research covered by dozens of publications and books, such as [34, 36, 38, 39]. As a result, a multitude of clock and carrier synchronization algorithms have been created.

4.1. Fractional Delay Ranging Receiver. For the proposed ranging WLAN Fractional Delay Ranging Receiver (FDRR), we assume that the received signal is sampled using a fixed local clock with period T_s shared among all base stations. After passing the signal through a matched filter compensating for the Channel Impulse Response (CIR) and in presence of noise $n(t)$, the phase offset θ, and the frequency skew Ω, the received baseband signal y sampled at time kT_s can be described by

$$y(kT_s) = \sum_m a_m g(kT_s - mT - \epsilon T) e^{J(\theta + \Omega k T_s)} + n(kT_s). \tag{8}$$

Despite the dependency of the baseband pulse shape $g(t)$ and data chips a_m, the received signal y is dependent on three other parameters, which have to be estimated by the receiver: the fractional delay ϵ, the phase offset θ, and the frequency skew Ω. These are unknown but deterministic and can be estimated by either a joint parameter estimation or by a separate estimation of each parameter. The former will result in the Maximum-Likelihood Estimation (MLE). The variance of the MLE is bound by the Cramer Rao Lower Bound (CRLB) [38, 39], the inverse of the Fisher information matrix. We assume that these terms are uncoupled, and therefore each parameter can be estimated separately without degrading the estimation. For ranging based on the baseband code, the interesting term in (8) is the fractional delay ϵ, estimated by the synchronizer, as it describes the delay of the received signal with respect to the local clock.

This leads to the modified receiver architecture shown in Figure 3. It differs from Figure 2 by the aspect that the NCOs have been included into the carrier and code wipeoff blocks (timing and phase recovery) and that the code synchronization is factored into a chip and spread code synchronization. This split is motivated by the fact that WLAN does not use the same spread code for all data rates, but the 11 bit Barker sequence for the 1 and 2 Mbps mode and CCK together with an increased symbol rate of 1.375 MS/s for the higher data rates.

The timing recovery calculates the fractional delay estimate $\hat{\epsilon}$ and finally interpolates and decimates the input signal with rate $1/T_s$ to the chip rate of the transmitter $1/T$. We have selected the squaring timing recovery belonging to the group of non-data-aided synchronizers generating a spectral line at the chip rate and multiples of it. It has been shown in [36] that the signal transitions of the chips a_m create a cyclostationary process with period T at the output of the squarer, that spectral line at the chip rate contains an estimate $\hat{\epsilon}$ for the chip timing. The argument of the Fourier coefficient c_1 of the squared magnitude of y yields the unbiased estimate $\hat{\epsilon}$ for the chip timing. It can be calculated by

$$\hat{\epsilon} = -\frac{1}{2\pi} \arg\left(\sum_{l=0}^{LN-1} |y_l|^2 e^{-J2\pi l/N} \right), \tag{9}$$

with y denoting the received sampled signal, $N = T/T_s$ the number of samples per chip, and L the number of chips to average. The estimation is the MLE under the assumption that the sampling rate is at least twice the required sampling rate of y, N is an integer, and the baseband pulse is assumed symmetric and real-valued ($g(t) = g(-t)$).

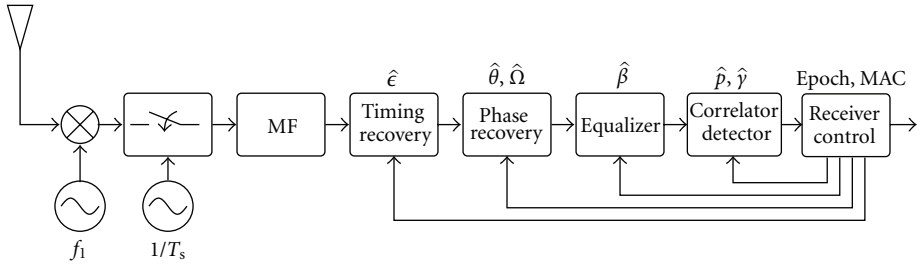

Figure 3: Proposed fractional delay ranging receiver architecture.

Table 1: Range estimates.

Parameter	Variable	Ambiguity	Resolution
Fractional delay	$\hat{\epsilon}$	91 ns	Arbitrary
Correlator lock-in	$\hat{p}$	1 μs	T_1 or 91 ns
Epoch	None	None	T_1 or 91 ns
Carrier freq. skew	$\hat{\Omega}$	None	Arbitrary
Carrier phase	$\hat{\theta}$	408 ps	Arbitrary
CIR	$\hat{\beta}$	None	Arbitrary

The residual frequency and phase offset are wiped off in the timing-aided (Dϵ) and data-aided (DA) carrier and phase recovery block, where the aiding information is provided by the receiver control unit. Other estimated parameters, such as the carrier phase and frequency, $\hat{\theta}$ and $\hat{\Omega}$, the equalizer coefficients $\hat{\beta}$, the DSSS lock-in position $\hat{p} = T \times (0, 1, \ldots, 10)$, and the carrier lock-in position $\hat{\gamma}$ are also marked above the corresponding blocks in Figure 3. A summary of the resolution and ambiguities of these estimates is given in Table 1.

The baseband code synchronization is factored into the timing recovery and correlator. The correlator lock-in position $\hat{p}$ is required to determine the correct chip for timestamping. As the evaluation of $\hat{\epsilon}$ together with $\hat{p}$ still yields an ambiguity of 1 μs (the length of the Barker DSSS sequence), the epoch is required to find the unique position within the frame. The epoch is agreed among all base stations and is found by decoding and analyzing of WLAN frame format (e.g., the first chip of the frame header).

The term resolution in Table 1 needs some further explanation. Consider the estimation of ϵ using a squaring synchronizer based on (9). As the fractional delay ϵ of the received signal with respect to the local sampling clock is available as a numerical term, it is not bound by any quantization, and therefore the resolution can be arbitrarily high. If we would simply monitor the arrival of a certain chip (epoch), the resolution would be bound by the duration of a chip (91 ns) or by the clock period T_1 of the receiver hardware, given that we mark a certain clock cycle as the arrival of the epoch. In the proposed FDRR, the fractional delay estimate $\hat{\epsilon}$ is propagated through the entire receiver and therefore the resolution is preserved.

However, there is a common misconception by several authors (e.g., [40–42]) that the ranging resolution is in general bound by the clock frequency of the timing source or receiver architecture. For instance, Bensky states on page 90 of his book [40] that a 1 m range or 6.67 ns time resolution requires a 150 MHz clock. Yet, for some particular receiver architectures, the resolution constraint is indeed valid. For instance, when evaluating the cross-correlation peak of a sampled signal, the resolution is limited, as the correlation peak cannot be narrower than a single sample. However, given that the sampling theorem is fulfilled, all required information is still contained in the sampled data. Different approaches have been proposed to mitigate the resolution constraint. Increasing the clock rate is one possible solution to increase the resolution, interpolation as described in [43] is the other solution. Our approach can be classified as an interpolating approach using CCC and exploiting the cyclostationarity at the chip period T of the WLAN signal. The full signal decoding is required to find the epoch, to identify the target, and to group different frames belonging to the same target.

Until now, we have considered taking a single timestamp at one specific instant in a frame, the epoch, and submit it to the locating unit calculating the position based on the timestamp set from different base stations. It is known from estimation theory that averaging as many realizations of a stochastic function as possible decreases the estimation variance by the improvement of the test statistic. For ranging, the estimation should be averaged, if possible, over the entire frame requiring very narrow bandwidths in the timing recovery. As a solution, we propose a two-step approach. The loop bandwidth in the timing recovery is optimized for chip synchronization, while the noisy outputs are filtered in a separate timestamping unit after the receiver control unit using a linear regression model. The timestamp optimization using linear regression, as described in the Appendix A, enables the calculation of the MLE timestamp for the center of each wireless frame.

4.2. Theoretical Bounds. The performance of various ranging estimators can be assessed by statistical bounds, which are used for comparison in Section 6. In the field of estimation theory, there exist a number of such bounds, one of them is the CRLB defining the lowest bound for the variance of an unbiased estimator. The CRLB is based on the assumption that the Probability Density Function (PDF) $p(x; \vartheta)$ of x parametrized on ϑ obeys the regularity condition, that

the expectation of the derivative of the log-likelihood of $p(x;\vartheta)$ is zero as stated in

$$E\left[\frac{\partial \ln p(x;\vartheta)}{\partial \vartheta}\right] = 0. \tag{10}$$

Then, the CRLB defines a lower bound for any unbiased estimator as

$$\operatorname{var}\left(\hat{\vartheta}\right) \geq \frac{1}{-E\left[\partial^2 \ln p(x;\vartheta)/\partial \vartheta^2\right]}, \tag{11}$$

where the derivative is evaluated at ϑ. When the CRLB is applied to the ToA estimation problem, the ToA variance with c the propagation speed is bound by [44]

$$\sqrt{\operatorname{var}\left(\hat{d}\right)} \geq \frac{c}{2\sqrt{2}\pi\sqrt{\mathrm{SNR}}\beta}, \tag{12}$$

where $\hat{d}$ is the range estimate and SNR refers to the signal-to-noise ratio. β represents the effective bandwidth of the signal, which is the square root of the second moment of the spectrum, expressed by the Fourier transform of the pulse, $S(f)$, normalized over the energy of the signal E by

$$\beta = \sqrt{\frac{1}{E}\int_{-\infty}^{\infty} f^2 \,|S(f)|^2 df}. \tag{13}$$

Increasing the effective bandwidth β or the SNR improves the ToA ranging variance. This objective can be achieved by using a large signal bandwidth as in Ultra-Wideband (UWB) communication systems. For WLAN with raised-cosine pulses (e.g., with a roll-off factor of 50%), the effective bandwidth is 2.96 MHz and therefore the variance can only be decreased by increasing the SNR.

5. Multipath

5.1. Multipath Modeling. Multipath propagation is present when the transmitted signal arrives at the receiver via multiple echoes. In contrast to interference with AWGN, the multipath components (MPCs) have similar statistical properties and are correlated to the direct signal. If the number of MPCs is L, the received signal $r(t)$ can be written as the sum of weighted and delayed transmit signals $s(t)$ in form of a tapped delay line model perturbed by zero-mean AWGN $n(t)$ by

$$r(t) = \sum_{l=1}^{L} \alpha_l s(t-\tau_l) + n(t). \tag{14}$$

The complex-valued channel coefficients are represented by α_l, and the path delays by τ_l. The CIR decays for long delays due to the path loss. The terms, where the channel coefficients are nonzero, define the multipath spread. If the target, the base stations, and the Interfering Objects (IOs) are static, then the channel coefficients can be considered time-invariant. For practical applications with moving objects, this assumption does not hold and the time variability of the channel coefficients must be taken into account [45].

When multipath is present, the tracking loop of the timing recovery locks on the composite signal consisting of the line-of-sight signal (LOS) and the MPCs as the receiver is unable to differentiate between this perturbed signal and the desired signal. An MLE receiver tries to find the ToA by maximizing the cross-correlation function of the received signal r with the stored template x (e.g., by means of a matched filter). In presence of multipath, the cross-correlation function R_{xr} is no longer identical to the auto-correlation function (ACF) R_{xx}, it is rather a weighted sum of shifted ACFs as

$$R_{xr}(t) = \sum_{l=1}^{L} \alpha_l R_{xx}(t-\tau_l). \tag{15}$$

Hence, the cross-correlation function becomes a non-symmetric function with a correlation peak that may be shifted with respect to the correlation peak of the direct signal. The estimation error due to the distortion is known as multipath error. It is dependent on the current channel coefficients (amplitude, phase, delay), which are defined by the propagation conditions. As the phase of the channel coefficients changes for movements as small as the carrier wavelength, the error is not predictable by a receiver in the vicinity. This small-scale multipath effect is well known for GPS and addressed by a number of mitigation strategies such as modified synchronizer discriminator functions (e.g., narrow correlators for delay-locked loops [46]).

In spite of the limited realism, it is a common model to describe multipath propagation by the two-path channel model, where the CIR consists only of two terms, the LOS signal and a single multipath component. We consider the CIR as time-invariant, which represents the case of zero Doppler spread or infinite coherence time, respectively. This setup is, for instance, present if all transmitters, receivers, and IOs are static. Without loss of generality, we assume in the two-path scenarios that the LOS signal has unity amplitude ($\alpha_1 = 1$ in (14)), zero phase, and zero delay $\tau_1 = 0$. The simplified CIR is therefore

$$h(t) = \delta(t) + \alpha_2 \delta(t-\tau_2). \tag{16}$$

5.2. Multipath Ranging Errors. Even for the two-path channel model, three parameters influence the multipath error: the amplitude $|\alpha_2|$, the phase $\phi = \arg(\alpha_2)$, and the delay τ_2.

Let us recall that a spectral-line generating squaring synchronizer, as used by our proposed FDRR, squares the absolute of the signal and calculates the Fourier coefficient c_1. The argument of c_1 times $-1/(2\pi)$ yields an unbiased estimate $\hat{\epsilon}$ of the chip timing, with T the chip period and r_c the composite received signal as

$$\hat{\epsilon} = -\frac{1}{2\pi}\arg\int_{-\infty}^{\infty} |r_c(t)|^2 e^{-\jmath 2\pi t/T} dt. \tag{17}$$

If we insert the composite signal $r_c(t) = r(t) + \alpha_2 r(t-\tau_2)$, generated by convolution of the direct signal with (16), into (17) and exploit the cosine formula, the multipath error e_{MP}

can be derived as the difference between the estimates of the composite and direct signal by

$$e_{\mathrm{MP}} = -\frac{cT}{2\pi}\Big[\arg\int_{-\infty}^{\infty}\Big(r^2(t) - 2|\alpha_2|\cos\phi r(t)r(t-\tau_2) + |\alpha_2|^2 r^2(t-\tau_2)\Big)e^{-(\jmath 2\pi t/T)}dt - \arg\int_{-\infty}^{\infty} r^2(t)e^{-(\jmath 2\pi t/T)}dt\Big]. \tag{18}$$

It can be seen that the multipath error depends not only on α_2 (amplitude and phase) and τ_2, but also on the received signal $r(t)$ itself. As the squaring synchronizer works in non-data-aided (NDA) mode, it operates on the plain received signal without taking any symbol decisions in the receiver into account. $r(t)$ is cyclostationary with the chip period T given that the alphabet sequence a_m used to generate $r(t)$ is uncorrelated (see (1)). A useful interpretation for wide-sense cyclostationary signals is that the ACF can be expressed by a sum of functions $R_{rr}^{\alpha}(t)$ with cycle frequencies α [29] (cf. (7)). As the ACF of a cyclostationary signal is insensitive to a shift T, the nth Fourier coefficient of the ACF can be calculated by setting $\alpha = n/T$ as

$$R_{rr}^{n/T}(\tau) = \frac{1}{T}\int_{-T/2}^{T/2} r\left(t-\frac{\tau}{2}\right)r^*\left(t+\frac{\tau}{2}\right)e^{-(\jmath 2\pi nt/T)}dt. \tag{19}$$

The Fourier coefficients $R_{rr}^{n/T}(\tau)$ are also referred to as cyclic autocorrelation functions [47]. Using (19), the timing estimate of (17) evaluates $\arg(R_{rr}^{n/T}(\tau))$ for $n = 1$ and $\tau = 0, \tau_2$. Hence, the multipath error can be rewritten as

$$e_{\mathrm{MP}} = -\frac{cT}{2\pi}\Big[\arg\Big(R_{rr}^{1/T}(0) - 2|\alpha_2|\cos\phi R_{rr}^{1/T}(\tau_2) + |\alpha_2|^2 R_{rr}^{1/T}(0)e^{-(\jmath 2\pi\tau_2/T)}\Big) - \arg R_{rr}^{1/T}(0)\Big]. \tag{20}$$

For certain multipath amplitudes, the error can be depicted in form of a ranging error envelope by varying the multipath delay and selecting the phase that generates the largest multipath error. The ranging error envelopes for 10, 30 and 50% multipath field strength are depicted in Figure 4. The graph was generated based on a simulation using uncorrelated data encoded with BPSK baseband modulation, filtered by a raised-cosine filter with 50% roll-off factor, and the WLAN chip period of 91 ns. The x-axis depicts the multipath delay, and the y-axis shows the multipath ranging error. Positive multipath errors arise in case the MPC is inphase with the direct signal as the delay shifts the correlation peak into the future. Negative multipath errors are created by destructive interference. It can be observed that destructive interference causes large ranging errors, even if the multipath delay is rather short. These results for a single path, corresponding to ToA ranging, can be applied for TDoA as well, if any two points within the error envelope are added. Thus, the TDoA multipath ranging error may be even twice as large.

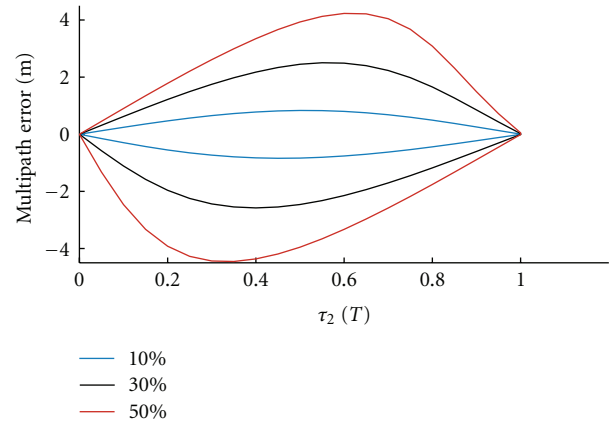

Figure 4: Multipath error envelope.

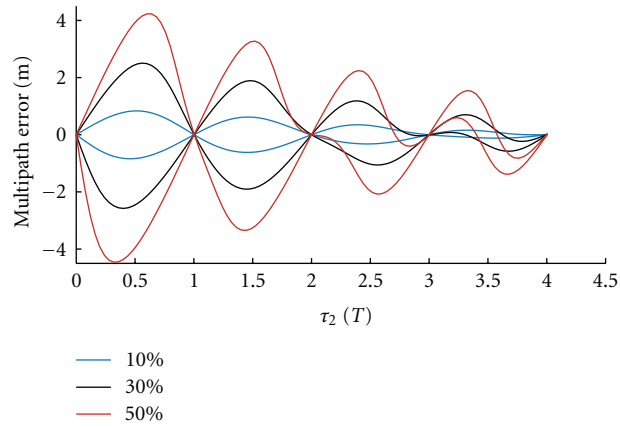

Figure 5: Envelope for MPCs with long delays.

The multipath error depends on the cyclic function $R_{rr}^{1/T}$ evaluated at 0 and τ_2 according to (20). It can be seen that the multipath error is zero, whenever the delay τ_2 matches a multiple of the chip period T because the error terms in (20) are inphase with $R_{rr}^{1/T}(0)$. Figure 5 depicts the same error as Figure 4 but also shows the impact of MPCs with delays larger than the chip period T. The NDA timing recovery based on the cyclic autocorrelation function has the disadvantage that only the center term $R_{rr}^{1/T}(\tau_2)$ of (20) decays for larger delays. As a result, the MPCs with delays larger than the chip period still contribute to the multipath error as depicted in Figure 5.

The drawback that the multipath error can be influenced by far specular reflections is alleviated, if we consider that the extra time delay causes an additional path loss. In addition, depending on the environment, large smooth surfaces acting as specular reflectors are unlikely. In terms of resolvability, delays, which are longer than the chip period, can be resolved (e.g., by spectral estimation of the equalizer or pseudospectrum estimates of superresolution methods). As a consequence, we can conclude that the multipath ranging error is mainly induced by MPCs with short delays, which are unfortunately not resolvable due to the limited bandwidth and the lack of the pulse shape definition.

5.3. Multipath Mitigation. Multipath can cause significant ranging errors in the order of several meters as the receiver tracks the composite signal. Despite particular antenna designs which attenuate the MPCs, multipath can also be tackled by signal and data processing using nonparametric, parametric, and averaging techniques. Nonparametric techniques use a modified receiver template, which rather tracks the derivative of the pulse shape than the pulse shape itself, such as a narrow correlator setup commonly used in GPS receivers. The modified template is designed to achieve a sharper correlation result that is less influenced by multipath propagation. Parametric techniques rely on a certain CIR model and estimate the nuisance parameters such as phases, amplitudes, and delays of the MPCs. A common approach within this group is superresolution techniques in the time and frequency domain [48].

A necessary assumption for all estimation methods is that the signal (or at least its autocorrelation and covariance) is either known in advance or the receiver is able to reconstruct this information. Whereas the digital information and signal constellation of each chip in the baseband can be reconstructed, the WLAN pulse shape is not defined and may vary from device to device. Hence, an estimation of the CIR is not possible because the transmitted signal cannot be reconstructed. On the other hand, nonparametric multipath mitigation techniques, such as narrow correlators with an early-late spacing of $0.1\,T$ resulted in the same multipath error as the squaring synchronizer (Figure 4). The reason for the discrepancy with the multipath mitigation improvements reported by other authors (e.g., [49]) stems from the fact that commonly a triangular ACF (responding to the transmission of rectangular pulses) is assumed, while the bandwidth limitation of WLAN imposes a rounded (raised-cosine) ACF of the signal and therefore diminishes the advantages of special correlator arm arrangements.

Multipath is in particular the limiting factor for point positioning applications. When the channel is static and therefore the channel coherence time is infinite, the range estimate may include a constant ranging bias. In principle, multipath mitigation through averaging can be done by any kind of frequency or space diversity, which is able to change the CIR or minimize the coherence time. If the target changes the position by about 10 times the carrier wavelength, the small-scale fading effects and connected to these the multipath errors average. For WLAN, this equates to a displacement of more than 1 m. Spatial averaging is impractical as it prohibits point positioning and requires a constant movement to generate varying CIRs.

Frequency diversity is another option to mitigate multipath errors as different carrier frequencies change the CIR. The main disadvantage of this approach is that changing the WLAN channel causes a loss of connection, if not enforced simultaneously by the AP and all associated targets. Yet, we still propose this method as it is one of the few methods, which requires only software modifications of the target, namely, preplanned channel hopping. As shown in the next section, frequency diversity can significantly improve the multipath performance.

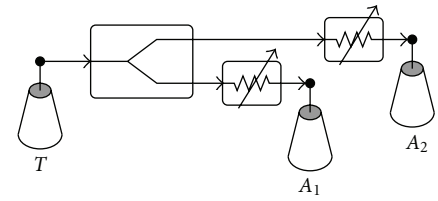

Figure 6: Cabled setup for assessing the synthetic performance.

6. Results

This section presents the results of the FDRR architecture introduced in Section 4 based on a digital logic implementation using an FPGA platform. Several measurements have been performed to assess the synthetic performance (perfect channel) and the practical performance in line-of-sight and multipath conditions.

6.1. Measurement Setup and Platform. The proposed FDRR architecture has been implemented using the SMart integrated Localization Extension 3 (SMiLE 3) base station hardware, which is a revised version of our previous hardware described in [22]. It consists primarily of an RF mixer IC to convert the WLAN signal to the baseband, a dual-channel ADC/DAC, an FPGA for signal processing and message handling, and an Ethernet connection to communicate the captured ranging parameters to the locating PC calculating the positions. Two methods for synchronizing the base stations are available: Ethernet synchronization and Board-Link. Ethernet synchronization exploits the fact that the transmit signal of a 100Base-TX Ethernet link is synchronous to the source oscillator of the transmitter. When all SMiLEs are connected to a common switch, the base stations are able to recover the transmit Ethernet clock from the received Ethernet signal and can build a synchronous network with phase-locked sampling clocks $1/T_s$. The same can be done when connecting two base stations with a dedicated clock cable named Board-Link. Still, as the startup time of all base stations is not synchronized, clock offsets between the base stations exist. These offsets can be resolved by transmitting a WLAN frame from a known position and compensating for the propagation time to the base stations. This step is referred to as clock offset calibration.

Various measurements have been conducted by deploying either two or four base stations for one- and two-dimensional setups. The RF mixer of SMiLE 3 platform has a dependency of the delay on the premixer and postmixer amplification by a few nanoseconds. In all measurements, these systematic errors are compensated by a table lookup.

6.2. Synthetic Performance. First, we assess the synthetic performance of the hardware, when the RF signal between the base stations is connected via cables and attenuators as depicted in Figure 6. The setup consists of a transmitter T sending frames with adjustable frame length and period to two base stations A_1 and A_2. The transmitter's RF signal is fed into an 18 dB splitter, and each of the branches is

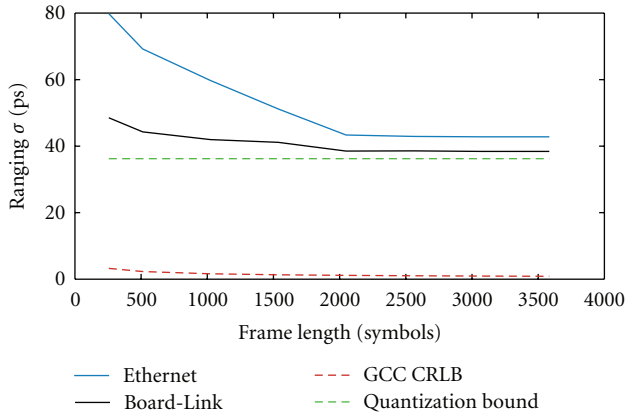

Figure 7: Ranging performance: frame length dependency.

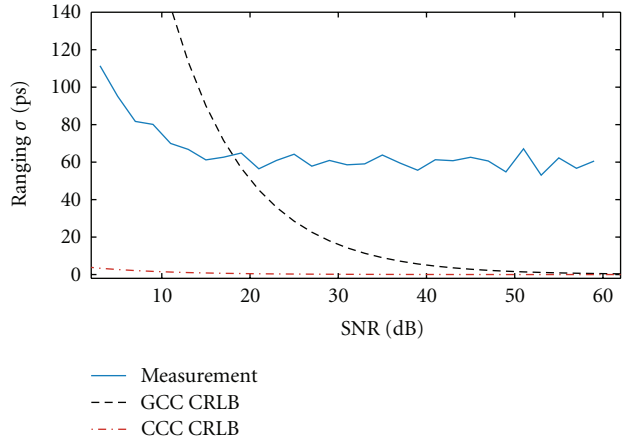

Figure 8: Ranging performance: SNR dependency.

connected by attenuators to one base station. Each base station captures the frame, timestamps it, and transmits the timestamp together with the frame check sum and the identification MAC address to the locating PC, which subtracts the timestamps and records the TDoA.

The measurement results for both synchronization approaches (Ethernet and Board-Link) for variable frame lengths are depicted in Figure 7. It is remarkable that the SMiLE 3 hardware is able to consistently achieve range measurements with a TDoA standard deviation slightly above 40 ps, equivalent to 1.2 cm. Note that the clock calibration removes not only the clock offsets, but also minor delay differences caused by the cabling.

The resolution $Q = 88.77$ ps of the fractional delay estimate $\hat{\epsilon}$ (and therefore the timestamps) has been selected as 1/1024 of the chip duration T as this represents a good compromise between resolution and logic demands in the FPGA. Given that the quantization errors in both receivers are uncorrelated, the standard deviation of the resulting triangular distribution is $\sigma = Q/\sqrt{6} = 36.24$ ps. In Figure 7, this is shown as quantization bound. Compared to the hardware implementation of [13] with a quantization of 22.72 ns (equivalent to $\sigma = 9.28$ ns), our hardware implementation offers a more than 200 times lower standard deviation.

The GCC CRLB for $N = (256 - 3584) \times 11$ chips can be calculated by (12). It assumes an SNR of 49.9 dB (the estimated SNR Figure due to the jitter of the ADC sampling clock) per chip, an effective bandwidth of 2.96 MHz, 11 chips per symbol (1 Mbps), and no correlation between the receivers. For this particular setup with high SNR, the CRLB imposes no real limit. Note that the performance is only impaired by the synchronization, in particular for short frames, as seen by the difference between Ethernet and Board-Link. The reason of the degraded Ethernet performance can be found in the large phase noise of the Ethernet clock distribution scheme.

When attenuators are inserted into the cabling between the target and the base stations, an increased distance and degradation of the SNR can be tested. For the experiment a frame length of $N = 1024 \times 11$ chips has been selected. The graph showing the variance of each SNR value is depicted together with the CRLBs in Figure 8. The ranging standard deviation stays approximately constant at 60 ps for SNRs above 12 dB and slightly increases for lower SNR values until the signal can no longer be decoded. Interestingly, the measurement shows to be better than the GCC CLRB using (12). This may seem as a contradiction to the definition of the CRLB as lowest bound for the variance of an unbiased estimator, albeit the definition is in fact not violated.

The GCC CRLB applies to the cross-correlation of the entire baseband signal with a noise-free template in each receiver given that there are N independent range measurement pulses. The low standard deviation even at low SNRs stems from the fact that the timing recovery exploits the cyclostationarity of the signal by calculating the argument of Fourier coefficient c_1. Let the captured signal be $\mathbf{y}$, and let $\mathbf{x}$ be defined by $x_k = |y_k|^2$ with $k = 1, 2, \ldots, N$ samples (squaring synchronizer), then N frequency bins can be calculated by the Fourier series expansion, of which only one, c_1, is evaluated. Consequently, the Neyman-Fisher factorization (21) can be applied [50]. If the PDF $p(\mathbf{x}; \epsilon)$ can be factored into a function $g()$ depending only on $\mathbf{x}$ via $T(\mathbf{x})$, and $h()$ is a function only depending on $\mathbf{x}$, then $T(\mathbf{x})$ is a sufficient statistic for ϵ:

$$p(\mathbf{x}; \epsilon) = g(T(\mathbf{x}), \epsilon) h(\mathbf{x}). \tag{21}$$

For the estimation of the fractional delay, c_1 is a sufficient statistic. If the WLAN frame consists of N independent samples and the noise is uncorrelated to the signal, then the frequency selectivity (by evaluating only c_1) improves the SNR by the same factor N. Therefore, the ranging standard deviation improves by $\sqrt{N}$. As the averaging itself (without frequency selectivity) improves the CRLB already by $\sqrt{N}$, for a cyclostationary signal with N pulses, $\sqrt{N}$ appears twice in the denominator of the CRLB (12). Consequently, the CRLB is identical to a signal with N times the bandwidth, or N^2 times the SNR as

$$\sqrt{\operatorname{var}\left(\hat{d}\right)} \geq \frac{c}{2\sqrt{2}\pi\sqrt{\mathrm{SNR}}N\beta}. \tag{22}$$

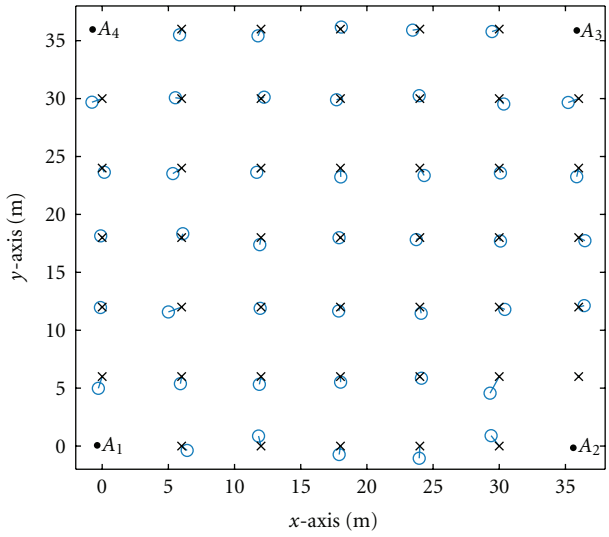

FIGURE 9: 2D position measurement in LOS conditions.

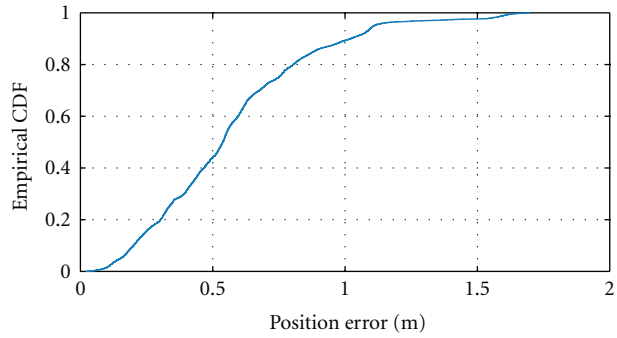

FIGURE 10: 2D position error.

This bound is depicted as CCC CRLB in Figure 8. The actual receiver design diverts from this approach as it uses an NDA timing recovery, which has an increased variance compared to a decision-directed timing recovery for conditions with an SNR below 7 dB in case of BPSK modulation, as shown by the closed-form evaluation in [51]. The CCC CRLB assumes perfect synchronization and no chip frequency skews. In practical implementations, chip frequency skews are always present, and therefore the loop bandwidth in the timing recovery must be sufficiently large to track frequency changes. As a result, the noise over a larger bandwidth needs to be collected for tracking reasons, thus leading to an increased variance.

6.3. Performance in LOS Conditions. In all the following measurements, a Linksys WRT54GL wireless access point has been used sending beacons with $N = 944$ chips with an interval of approximately 10 ms. The target is equipped with a standard dipole antenna with horizontal polarization, which ensures angular-independent uniform signal coverage. The target is moved within the area of interest, and the position of the target is calculated in the locating unit based on the parameter estimates captured by the base stations. Once the setup is built up, the initial clock offset calibration is performed and the same offsets are used for all positions of the measurement.

A two-dimensional medium-scale measurement has been performed on a flat meadow with four base stations positioned in the corners of a 36 m square. The square has been divided into sections of 6 m forming a grid. To assess the point localization performance, the target is located on each grid point and the position estimates are recorded. The base stations and the target are mounted on tripods with a height of 1.6 m to enable LOS propagation without the Fresnel zone touching the ground.

Figure 9 shows the true positions marked with crosses, and the measured positions marked with circles. It displays that the positions determined by the range estimates follow the true position with high accuracy. The empirical Cumulative Distribution Function (CDF) of the position error is shown in Figure 10. In 80% of all measurements, the distance between the true position and the measured one is below 0.81 m. The maximum error is 1.70 m.

An evaluation of the measured data shows that the TDoA RMS error of the unfiltered timestamps is 2.45 ns. As the TDoA standard deviation is only 390 ps, the largest contribution to the RMS error is the offset. Compared to the synthetic range measurements, the standard deviation is larger and a significant average offset exists. Offsets may arise due to positioning errors of the target and the base stations. These errors are inevitable as the markings of the positions on the meadow are accurate to approximately ± 10 cm. As shown in Section 5, large measurement errors may also originate from multipath propagation. A possible interpretation of the RMS error is that a small fraction of the signal is reflected from the ground leading to multipath-induced offsets.

6.4. Multipath Performance. For the assessment of the multipath performance, we consider a one-dimensional setup as there is only a single range to be extracted, and the ranging and position error are independent of the geometric setup in contrast to multidimensional locating. This allows for a more intuitive interpretation of the results as only a single time error is present. Clearly, the setup can be extended to more dimensions as well.

In the experiment, the target T is moved along the perpendicular path that joins the base stations A_1 and A_2, positioned 6 m apart from each other. The setup is depicted in Figure 11 together with the hyperbolas for multiples of 5 ns propagation time difference. Given that the path is centered between the base stations, the hyperbola becomes a straight line and any movement along this axis should not change the TDoA. Hence, the measured range corresponds to the TDoA ranging error. The setup is placed in an office environment surrounded by cupboards, desks, chairs, and other typical furniture. The rooms within the office building are separated by drywalls.

The results of the unfiltered ranges for this experiment are shown in Figure 12. At the start of the measurement,

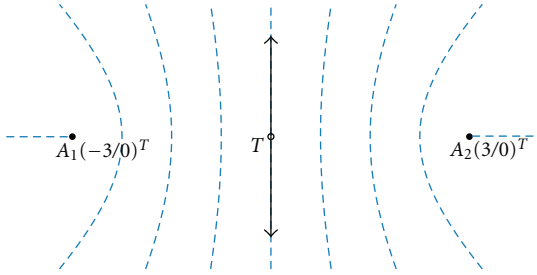

Figure 11: Multipath measurement setup.

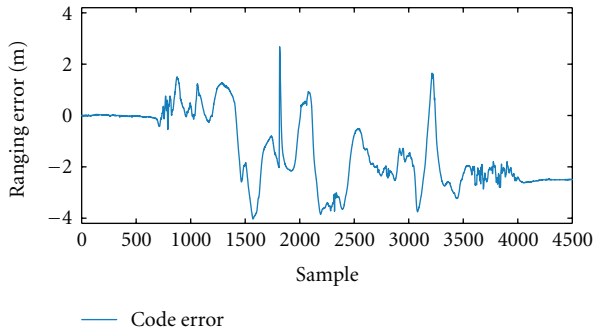

Figure 12: Multipath ranging error.

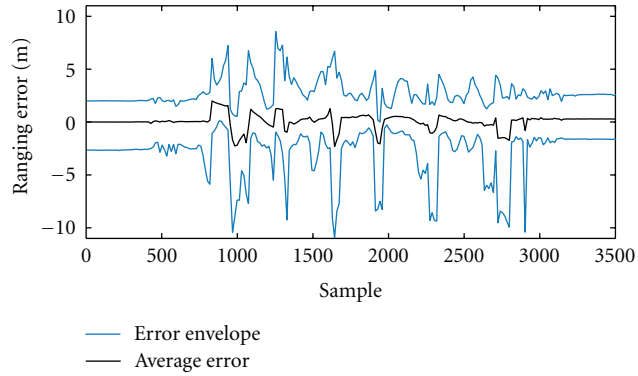

Figure 13: Frequency hopping multipath ranging error.

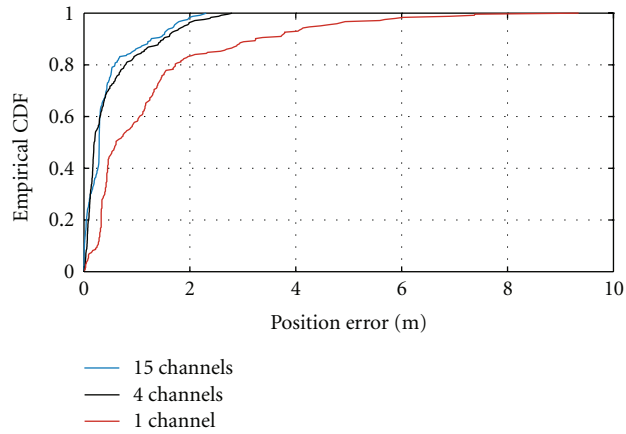

Figure 14: Frequency hopping ranging error for 1, 4, and 15 channels.

the offset is calibrated, and, as a result, the TDoA bias is set to zero. When the target is moved on the perpendicular line, the propagation conditions change and the multipath error varies resulting in an error of up to 4 m. After 4200 samples, the movement of the target is stopped and the multipath error becomes static again. However, the error is not zero, but approximately −2.1 m. Two problems are associated with locating in multipath environments: the synchronization at the start of the experiment is already biased, and each range measurement includes an unknown bias as well. The synchronization bias is caused by the fact that the selected synchronization approach requires one device (the target) to transmit from a known position to calibrate the receiver offsets. Yet, this calibration may already introduce a bias by multipath propagation. Both biases can be partially mitigated by Frequency-Hopping Spread Spectrum (FHSS) through all available WLAN channels.

Figure 13 depicts the results of the FHSS TDoA measurements by the average error and ranging error envelope. The average error refers to the TDoA average of one FHSS sequence using 15 channels separated by 5 MHz with no other filtering applied. The TDoA error envelope is defined by the maximum and minimum TDoA of each FHSS sequence and can be understood as a bound for the multipath error when using a single channel. As in the previous setup, the measurement is calibrated at the start of the system. Yet, already at this point, the TDoA range varies from channel to channel by ±2.6 m. During the movement of the target TDoA multipath errors of up to 12 m arise on some channels. The diversity introduced by FHSS leads to a reduced multipath error, in this particular setup the TDoA falls within −2.3 up to 2.0 m, which is a significant improvement compared to a single channel.

As FHSS over 15 channels takes 150 ms with 10 ms frame period, the question arises, if a similar performance can be achieved with fewer channels. If only 4 channels are evaluated (1, 5, 9, and 13), the TDoA ranging error is slightly higher with maximum range offsets of −2.8 up to 2.4 m. The empirical CDF for the unfiltered ranging error is shown in Figure 14 for FHSS using 4 or 15 channels as well as using only one channel (channel 1 at 2412 MHz). When using all 15 channels, in 80% of all measurements, the ranging error is below 0.59 m, and 0.79 m in case of 4 channels. When using no FHSS, for the same probability, the error is below 1.73 m. It should be noted that these results show a significant improvement compared to the WLAN locating system of [13], who reported a multipath error using a single channel of 4 m. Yet the results are not entirely comparable because the authors used a hardware with 22.72 ns timestamp resolution, and therefore the measurement required filtering of about 50 measurements.

Interestingly, multiple measurements in different environments showed that ranging errors using FHSS are significantly larger when the target is moving, while for stationary targets the FHSS-averaged ranging bias is always below 1 m.

A possible interpretation is that fast-fading channels generate temporary ranging errors as the channel conditions change during the reception of the frame, while the equalizer is set into tracking mode and cannot compensate for the distortions. This open point is to be investigated in the future.

7. Conclusion

In this paper, we proposed a novel fractional delay ranging receiver architecture for ranging purposes in IEEE 802.11b WLANs. The particular feature of this architecture is that the timing recovery estimates the chip timing by a CCC approach and outputs its fractional delay estimate to all subsequent blocks. It has been shown that the proposed architecture can achieve a timestamping precision in the sub-100 picosecond range, which imposes a significant improvement to previously presented architectures. This high precision makes noise filtering techniques more or less obsolete.

The multipath-induced ranging bias, however, imposes the largest restriction to WLAN ranging. As WLAN has a narrow signal bandwidth and the baseband pulse is not defined, common multipath mitigation techniques, such as narrow correlators, showed no improvements. Yet this is not a limitation caused by a poor receiver implementation but justified by the fact that the wideband CIR is not resolvable with the limited signal bandwidth. The problem can be mitigated by performing frequency hopping or by averaging the TDoA estimates over all selected channels. With frequency hopping, the multipath error improved from 1.73 m with a probability of 80% for a single channel to 0.59 m when using all channels. As the WLAN channels overlap, using only 4 channels resulted in almost the same multipath resilience.

The future development of the system will focus on minimizing the impact of multipath propagation as further improvements in terms of ranging variance have virtually no impact on the practical accuracy. The receiver architecture already implements an equalizer compensating for the CIR of the channel. It is planned to develop an algorithm which reconstructs the specific pulse shape of each transmitter based on the equalizer coefficients captured from all base stations. With the knowledge of the pulse shape, parametric multipath mitigation techniques, such as superresolution methods, can be applied and multipath compensation values can be calculated. Particularly for point positioning with a static CIR, this technique has the potential to significantly reduce the multipath error without the necessity to transport the sampled signals of each base station to the central locating PC.

Appendix

A. Timestamp Optimization

The linear regression model enables to generate an optimized timestamp exploiting the high accuracy of the fractional timing delay $\hat{\epsilon}$ together with averaging. In a real-world timing recovery, the loop bandwidth of the code-tracking loop cannot be reduced to any arbitrary low number for a number of reasons. Recall that in WLAN chip frequencies may deviate up to 40 ppm between transmitter and receiver. A synchronizer should be able to compensate for the frequency skew and any random clock fluctuations within reasonable amount of time and follow the chip rate of the transmitter. This presents a lower limit on the code-tracking loop. Yet, for ranging, the loop bandwidth should be very narrow. As a solution, we propose a two-step approach. The loop bandwidth in the timing recovery is optimized for chip synchronization, while the noisy outputs are filtered in a separate timestamping unit after the receiver control unit. We assume that the timestamps vector $\mathbf{y}$ follows a simple linear regression model as

$$\mathbf{y} = \alpha + \beta\mathbf{x} + \mathbf{e}, \tag{A.1}$$

with α the unknown time offset, β the unknown chip frequency skew, $\mathbf{x}$ a vector containing the local clock at the timestamp instances and $\mathbf{y}$ the actual timestamps, and $\mathbf{e}$ the random uncorrelated error vector. This model assumes that there are no major chip frequency drifts within the timespan of interest (the frame duration). In this case, the MLE boils down to the linear regression of the data. The expectation of β and α can be calculated by the quotient of the covariance and the variance of $\mathbf{x}$ and $\mathbf{y}$ as

$$\begin{aligned} \hat{\beta} &= \frac{\operatorname{cov}[\mathbf{x},\mathbf{y}]}{\operatorname{var}[\mathbf{x},\mathbf{y}]}, \\ \hat{\alpha} &= E[\mathbf{y}] - \hat{\beta}E[\mathbf{x}]. \end{aligned} \tag{A.2}$$

Either these parameters are directly transmitted to the location unit or a filtered version of a timestamp for any arbitrary position in the frame can be calculated. For a TDoA architecture, this can be simplified as the locating unit uses range differences from two base stations. The distance estimation $\hat{d}_{i1}$ between base station i and base station 1 can be written as the difference of two timestamps as

$$\hat{d}_{i1} = c\left(\hat{\alpha}_i + \hat{\beta}_i\mathbf{x}_i - \hat{\alpha}_1 - \hat{\beta}_1\mathbf{x}_1\right), \tag{A.3}$$

with $\hat{\alpha}_i$ and $\hat{\beta}_i$ the corresponding linear regression coefficients for each base station. It can be assumed that the velocity v of a possible WLAN target is limited to about 5 m/s. For a baseband chip frequency $f_c = 1/T$ of 11 MHz, this limits the Doppler frequency shift Δf defined by

$$\Delta f = -f_c\frac{v}{c}, \tag{A.4}$$

with c the speed of light, to about 0.18 Hz or 17 ppb. For a typical frame duration of 1 ms, the Doppler effect will contract the frame by just 16 ps. As all base stations are assumed synchronized and the effect of the Doppler shift is negligible for the baseband signal, the expectations of the chip frequency skews $\hat{\beta}_i$ can be considered as the same for all base stations ($\hat{\beta}_i = \hat{\beta}_1$). As the base stations are synchronized ($\mathbf{x}_i = \mathbf{x}_1$), the range difference only depends on the estimated offsets $\hat{\alpha}_i - \hat{\alpha}_1$. Substituting (A.2) into (A.3) shows that the

TDoA only depends on the averaged timestamps of two base stations as

$$\hat{d}_{i1} = c(E[\mathbf{y}_i] - E[\mathbf{y}_1]). \quad (A.5)$$

The constraint that the chip frequency skews must be identical among all base stations is not required, if we define that the timestamp epoch to be at the center of the frame with $b_{\text{epoch}} = E[\mathbf{x}]$. If we use this definition and substitute (A.2) into (A.1), the center timestamp is just the expectation of $\mathbf{y}$ independent of the chip frequency skews $\hat{\beta}_i$. Defining the epoch at the center of the frame is rather unconventional as typical timestamping or ranging systems like UWB or IEEE1588 use an epoch at the start, such as the start frame delimiter [52].

Acknowledgments

This paper was partly financed by the province of Lower Austria, the European Regional Development Fund, the FIT-IT project *ε-WiFi* under Contract 813319 in cooperation with Oregano Systems and the EU under the FP7 STREP flexWARE Contract no. 224350.

References

[1] O. Bar-Shalom and A. J. Weiss, "Direct position determination using MIMO radar," in *Proceedings of the IEEE 25th Convention of Electrical and Electronics Engineers in Israel (IEEEI '08)*, pp. 575–579, December 2008.

[2] O. Bar-Shalom and A. J. Weiss, "Efficient direct position determination of orthogonal frequency division multiplexing signals," *IET Radar, Sonar and Navigation*, vol. 3, no. 2, pp. 101–111, 2009.

[3] P. Closas, C. Fernández-Prades, and J. A. Fernández-Rubio, "Cramer—Rao bound analysis of positioning approaches in GNSS receivers," *IEEE Transactions on Signal Processing*, vol. 57, no. 10, pp. 3775–3786, 2009.

[4] M. Ibrahim and M. Youssef, "CellSense: a probabilistic RSSI-based GSM positioning system," in *Proceedings of the 53rd IEEE Global Communications Conference (GLOBECOM '10)*, December 2010.

[5] A. Kushki, K. N. Plataniotis, and A. N. Venetsanopoulos, "Intelligent dynamic radio tracking in indoor wireless local area networks," *IEEE Transactions on Mobile Computing*, vol. 9, no. 3, pp. 405–419, 2010.

[6] K. Derr and M. Manic, "Wireless based object tracking based on neural networks," in *Proceedings of the 3rd IEEE Conference on Industrial Electronics and Applications (ICIEA '08)*, pp. 308–313, June 2008.

[7] P. Bahl and V. N. Padmanabhan, "RADAR: an in-building RF-based user location and tracking system," in *Proceedings of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE-INFOCOM '00)*, pp. 775–784, March 2000.

[8] M. Emery and M. K. Denko, "IEEE 802.11 WLAN based real-time location tracking in indoor and outdoor environments," in *Proceedings of the Canadian Conference on Electrical and Computer Engineering (CCECD '07)*, pp. 1062–1065, April 2007.

[9] S. Ivanov, E. Nett, and S. Schemmer, "Automatic WLAN localization for industrial automation," in *Proceedings of the 7th IEEE International Workshop on Factory Communication Systems (WFCS '08)*, pp. 93–96, May 2008.

[10] S. Mazuelas, A. Bahillo, and R. Lorenzo, "Robust indoor positioning provided by Real-Time RSSI values in unmodified WLAN networks," *IEEE Journal of Selected Topics in Signal Processing*, vol. 3, no. 5, pp. 821–831, 2009.

[11] H. Leppäkoski, S. Tikkinen, and J. Takala, "Optimizing radio map for WLAN fingerprinting," in *Proceedings of the Ubiquitous Positioning Indoor Navigation and Location Based Service (UPINLBS '10)*, pp. 1–8, October 2010.

[12] M. Ciurana, D. Giustiniano, A. Neira, F. Barcelo-Arroyo, and I. Martin-Escalona, "Performance stability of software ToA-based ranging in WLAN," in *Proceedings of the International Conference on Indoor Positioning and Indoor Navigation (IPIN '10)*, pp. 1–8, September 2010.

[13] A. Bahillo, S. Mazuelas, R. M. Lorenzo et al., "Accurate and integrated localization system for indoor environments based on IEEE 802.11 round-trip time measurements," *Eurasip Journal on Wireless Communications and Networking*, vol. 2010, Article ID 102095, 2010.

[14] H. Reddy, M. G. Chandra, S. G. Harihara, P. Balamuralidhar, J. Sen, and D. Arora, "WLAN-based local positioning using distorted template," in *Proceedings of the International Symposium on Communications and Information Technologies (ISCIT '07)*, pp. 1043–1048, October 2007.

[15] H. Reddy, M. G. Chandra, P. Balamuralidhar, S. G. Harihara, K. Bhattacharya, and E. Joseph, "An improved time-of-arrival estimation for WLAN-based local positioning," in *Proceedings of the 2nd International Conference on Communication System Software and Middleware and Workshops (COMSWARE '07)*, pp. 1–8, January 2007.

[16] S. König, M. Schmidt, and C. Hoene, "Precise time of flight measurements in IEEE 802.11 networks by cross-correlating the sampled signal with a continuous barker code," in *Proceedings of the IEEE 7th International Conference on Mobile Adhoc and Sensor Systems (MASS '10)*, pp. 642–649, November 2010.

[17] J. Benesty, J. Chen, and Y. Huang, "Time-delay estimation via linear interpolation and cross correlation," *IEEE Transactions on Speech and Audio Processing*, vol. 12, no. 5, pp. 509–519, 2004.

[18] T. J. S. Khanzada, A. R. Ali, and A. S. Omar, "Time difference of arrival estimation using super resolution algorithms to minimize distance measurement error for indoor positioning systems," in *Proceedings of the 12th IEEE International Multitopic Conference (IEEE INMIC '08)*, pp. 443–447, December 2008.

[19] I. A. Ibraheem and J. Schoebel, "Time of arrival prediction for WLAN systems using prony algorithm," in *Proceedings of the 4th Workshop on Positioning, Navigation and Communication (WPNC '07)*, pp. 29–32, March 2007.

[20] E. Kaplan and C. Hegarty, *Understanding GPS: Principles and Applications*, Artech House, London, UK, 2005.

[21] P. Loschmidt, G. Gaderer, and T. Sauter, "Location based services for IEEE 802.11a/b/g Nodes," in *Proceedings of the IEEE International Workshop Real-Time Networks (RTN '07)*, pp. 64–70, Pisa, Italy, July 2007.

[22] R. Exel, J. Mad, G. Gaderer, and P. Loschmidt, "A novel, high-precision timestamping platform for wireless networks," in *Proceedings of the IEEE Conference on Emerging Technologies and Factory Automation (ETFA '09)*, pp. 1–8, September 2009.

[23] R. Exel, G. Gaderer, and P. Loschmidt, "Localisation of wireless LAN nodes using accurate TDoA measurements,"

in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '10)*, pp. 1–6, April 2010.

[24] A. Nagy, R. Exel, P. Loschmidt, and G. Gaderer, "Time-based localisation in unsynchronized wireless LAN for industrial automation systems," in *Proceedings of the IEEE Conference on Emerging Technologies and Factory Automation (ETFA '09)*, September 2011.

[25] IEEE, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Std., 2003.

[26] F. Van Graas and M. Braasch, "GPS interferometric attitude and heading determination: initial flight test results," *Navigation, Journal of the Institute of Navigation*, vol. 38, no. 4, pp. 297–316, 1991.

[27] A. Brutti, M. Omologo, and P. Svaizer, "Comparison between different sound source localization techniques based on a real data collection," in *Proceedings of the Hands-free Speech Communication and Microphone Arrays (HSCMA '08)*, pp. 69–72, May 2008.

[28] B. Kwon, Y. Park, and Y. S. Park, "Multiple sound sources localization using the spatially mapped GCC functions," in *Proceedings of the ICROS-SICE International Joint Conference (ICCAS-SICE '09)*, pp. 1773–1776, August 2009.

[29] W. A. Gardner and C. M. Spooner, "Comparison of autocorrelation and cross-correlation methods for signal-selective TDOA estimation," *IEEE Transactions on Signal Processing*, vol. 40, no. 10, pp. 2606–2608, 1992.

[30] W. A. Gardner and C. K. Chen, "Signal-selective time-difference-of-arrival estimation for passive location of man-made signal sources in highly corruptive environments—I: theory and method," *IEEE Transactions on Signal Processing*, vol. 40, no. 5, pp. 1168–1184, 1992.

[31] M. D. E. Gisselquist, "A comparison of stationary and cyclostationary TDOA estimators," in *Proceedings of the Military Communications Conference (MILCOM '06)*, pp. 1–7, October 2006.

[32] M. Teplitsky and A. Yeredor, "TDOA estimation for cyclostationary sources: new correlations-based bounds and estimators," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '09)*, pp. 3309–3312, April 2009.

[33] B. Cheng, C. Chen, Z. Xu, H. Li, and X. Guan, "Wireless sensor networks based localization for audio-source: a GCC-GA method," in *Proceedings of the IEEE International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM '10)*, pp. 1–6, June 2010.

[34] U. Mengali and A. D'Andrea, *Synchronization Techniques for Digital Receivers*, Plenum Press, 1997.

[35] F. Classen and H. Meyr, "Two frequency estimation schemes operating independently of timing information," in *Proceedings of the IEEE Global Telecommunications Conference*, vol. 3, pp. 1996–2000, Houston, Tex, USA, Nov 1993.

[36] H. Meyr, M. Moeneclaey, and S. Fechtel, *Digital Communication Receivers*, John Wiley & Sons, 1998.

[37] I. Lita, D. A. Visan, and H. Popa, "Localization system based on enhanced software GPS receiver," in *Proceedings of the 29th International Spring Seminar on Electronics Technology: Nano Technologies for Electronics Packaging (ISSE '06)*, pp. 350–354, May 2006.

[38] H. Van Trees, *Detection, Estimation, and Modulation Theory, Part I*, vol. 1, John Wiley & Sons, 2001.

[39] J. Proakis and D. Manolakis, *Digital Communications*, Prentice Hall, 4th edition, 2006.

[40] A. Bensky, *Wireless Positioning Technologies and Applications*, Artech House, 2007.

[41] I. Guvenc, S. Gezici, and Z. Sahinoglu, "Ultra-wideband range estimation: theoretical limits and practical algorithms," in *Proceedings of the IEEE International Conference on Ultra-Wideband (ICUWB '08)*, pp. 93–96, September 2008.

[42] S. Parichha and M. Molle, "Localization and clock synchronization need similar hardware support in wireless LANs," in *Proceedings of the IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication (ISPCS '08)*, pp. 131–136, September 2008.

[43] F. Viola and W. F. Walker, "A spline-based algorithm for continuous time-delay estimation using sampled data," *IEEE Transactions on Ultrasonics, Ferroelectrics, and Frequency Control*, vol. 52, no. 1, pp. 80–93, 2005.

[44] C. E. Cook and M. Bernfeld, *Radar Signals: An Introduction to Theory and Application*, Artech House, 1993.

[45] A.-F. Molisch, *Wireless Communications*, John Wiley & Sons, West Sussex, UK, 1st edition, 2006.

[46] J.-M. Sleewaegen and F. Boon, "Mitigating short-delay multipath: a promising new technique," in *Proceedings of the ION GPS*, September 2001, http://www.septentrio.com/content/mitigating-short-delay-multipath-promising-new-technique.

[47] W. A. Gardner, A. Napolitano, and L. Paura, "Cyclostationarity: half a century of research," *Signal Processing*, vol. 86, no. 4, pp. 639–697, 2006.

[48] X. Li and K. Pahlavan, "Super-resolution TOA estimation with diversity for indoor geolocation," *IEEE Transactions on Wireless Communications*, vol. 3, no. 1, pp. 224–234, 2004.

[49] M. S. Braasch, "Performance comparison of multipath mitigating receiver architectures," in *Proceedings of the IEEE Aerospace Conference*, pp. 31309–31315, March 2001.

[50] S. Kay, *Fundamentals of Statistical Signal Processing, Volume I: Estimation Theory*, Prentice Hall, 1993.

[51] A. Masmoudi, F. Bellili, S. Affes, and A. Stéphenne, "Closed-form expressions for the exact cramér-Rao bounds of timing recovery estimators from BPSK, MSK and square-QAM transmissions," *IEEE Transactions on Signal Processing*, vol. 59, no. 6, pp. 2474–2484, 2011.

[52] IEEE, *IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*, IEEE Std, 2008.