Meas. Sci. Technol. **21** (2010) 035202 (12pp) doi:10.1088/0957-0233/21/3/035202

Radio frequency (RF) time-of-flight ranging for wireless sensor networks

B Thorbjornsen, N M White, A D Brown and J S Reeve

Electronics and Computer Science, The University of Southampton, Southampton SO17 1BJ, UK

E-mail: bt05r@ecs.soton.ac.uk

Received 3 June 2009, in final form 26 October 2009
Published 25 January 2010
Online at stacks.iop.org/MST/21/035202

Abstract

Position information of nodes within wireless sensor networks (WSNs) is often a requirement in order to make use of the data recorded by the sensors themselves. On deployment the nodes normally have no prior knowledge of their position and thus a locationing mechanism is required to determine their positions. In this paper, we describe a method to determine the point-to-point range between sensor nodes as part of the locationing process. A two-way time-of-flight (TOF) ranging scheme is presented using narrow-band RF. The frequency difference between the transceivers involved with the point-to-point measurement is used to obtain a sub-clock TOF phase offset measurement in order to achieve high resolution TOF measurements. The ranging algorithm has been developed and prototyped on a TI CC2430 development kit with no additional hardware being required. Performance results have been obtained for the line-of-sight (LOS), non-line-of-sight (NLOS) and indoor conditions. Accuracy is typically better than 7.0 m RMS for the LOS condition over 250.0 m and 15.8 m RMS for the NLOS condition over 120.0 m using a 100 sample average. Indoor accuracy is measured to 1.7 m RMS using a 1000 sample average over 8.0 m. Ranging error is linear and does not increase with the increased transmitter–receiver distance. Our TOA ranging scheme demonstrates a novel system where resolution and accuracy are time dependent in comparison with alternative frequency-dependent methods using narrow-band RF.

Keywords: wireless sensor network (WSN), locationing, ranging, time-of-flight, two-way, phase measurement, narrow-band, synchronization, algorithm, integrated

(Some figures in this article are in colour only in the electronic version)

1. Introduction

The development of fully integrated, low-power, low-cost communications equipment over recent years have led to the development of wireless sensor networks (WSNs) for many monitoring, control and tracking applications [1–3]. Determining the position of sensor nodes within those networks is important in order to provide additional information to the quantity being measured. Sensor nodes are often deployed without a prior knowledge of their location and therefore a method to determine their absolute or relative position is required.

To locate 'blind' sensor nodes, a ranging or angle measurement is first made to a number of reference or 'anchor' nodes which have prior knowledge of their location with respect to a local or global coordinate system. An algorithm is then used to compute the position of the blind device in relation to the reference nodes. Thus, the process of locationing consists of two stages: (1) ranging or angle measurements; (2) the computation of the position of the blind device. In this paper, we focus on the problem of accurately estimating the point-to-point distance between two sensor nodes involved with the localization process of a WSN. Computation of a blind device position will be considered in our following publication.

There are five main methods of determining point-to-point distance. These include time-of-arrival (TOA) [4, 5], time-difference-of-arrival (TDOA) [3, 6], received-signal-strength-indication (RSSI) [7], near-field-electromagnetic-ranging (NFER) [8] and angle-of-arrival (AOA) [9]. Ranging in WSNs is challenging because of the constraints of sensor

nodes and the accuracy requirements of the locationing mechanism. Ranging accuracy is typically required below 1 m using simple hardware and resource-constrained sensor nodes with low-power operation (<27 mA transmit, 25 mA receive using 2–3.6 V supply in active mode [10]). Those sensor nodes also operate in an unsynchronized manner from inaccurate crystal device clocks ($C_0 \pm 40$ ppm without temperature compensation [10]). In addition to the technical challenges, low cost and physical size limitations also set stiff constraints. TOA and RSSI are the most widely used ranging methods.

TOA ranging involves the measurement of the transit time of a signal in order to estimate point-to-point distance. Its ability to operate well in high multipath environments and provide sub-metre ranging accuracy has been demonstrated using ultra-wideband (UWB) [6].

In contrast, RSSI involves measuring the attenuation of a signal through the wireless channel to estimate the transmitter–receiver distance. The simplicity of this technique has led to its implementation on many WSN hardware platforms. The requirement for complex models that are able to remove the large errors caused by signal multipath can limit the accuracy of RSSI.

NFER involves the measurement of the phase change of a signals magnetic and electric component to estimate distance. NFER operates on very low frequencies (within the AM broadcast band 530–1710 kHz) hence benefiting exhibiting propagation properties. However, as with UWB-based TOA ranging, this technique can interfere with other systems, and therefore, the Federal Communications Commission (FCC) limit the maximum transmission power. For this reason, UWB-based TOA and NFER ranging methods can only operate over a short range (<60 m) [8].

TDOA uses a set of synchronized reference nodes at known locations to determine the TDOA of ranging signals to or from a blind node for localization. Wired infrastructure is a requirement between the references to meet the timing requirements and transfer data. This is a costly overhead and limits TDOA applications to fixed referencing architectures.

AOA involves the use of complex antenna arrays to measure the arrival angle of a received signal. The requirement of complex antenna arrays make AOA an impractical solution for sensor nodes due the physical size of those antennas [4].

In this paper, we consider a narrow-band RF TOF ranging approach to meet the constraints posed by WSNs and accurately estimate the point-to-point range. Alternative TOF ranging schemes have used UWB signals to achieve sub-metre ranging resolution [6]; however, those are limited in the operational range (<100 m) because of the FCC regulation on transmission power. To meet the sub-metre ranging resolution using narrow-band RF, we consider the frequency difference between the transmitting and receiving device in order to measure sub-clock phase offset of received TOA signals. This approach is time dependent in comparison to alternative frequency-dependent techniques [4].

The algorithm, in its prototype, has been designed and tested using a TI CC2430 development kit. Ranging transactions are carried out using the 2.4 GHz ISM band on a single channel with the algorithm being developed for its compatibility with the IEEE 802.15.4 standard. The algorithm can similarly be implemented in other comparable communication schemes incorporating different modulation techniques.

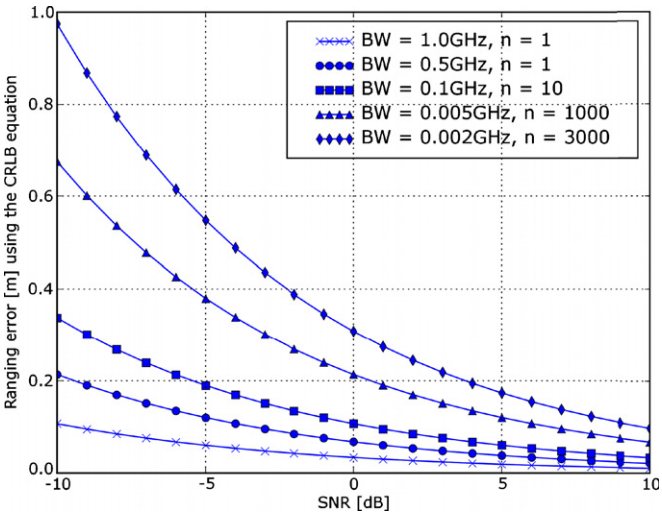

Figure 1. Lower bound of time-of-arrival ranging errors.

The remainder of this paper is organized as follows: section 2 details the preliminaries involved with TOA ranging; section 3 describes the ranging system; section 4 details the implementation of the prototype system and the expected accuracy; section 5 shows the preliminary testing results for the prototype system for LOS, NLOS and indoor conditions; and section 6 summarizes and concludes the research.

2. Preliminaries

2.1. Cramer–Rao lower bound for time-of-flight ranging estimates

The Cramer–Rao is an unbiased estimator for the lower bound variance of TOF measurements defined by equation (1) [11]. The variance (TOF time error) is defined as σ^2_{TOF}, β_f (Hz) is the spectral bandwidth of the received signal, n is the number of averaged TOF measurements and SNR is the energy per bit divided by the noise power (E_b/N_0):

$$\sigma^2_{\mathrm{TOF}} \geqslant \frac{1}{8\pi^2 \cdot \beta_f^2 \cdot \mathrm{SNR} \cdot n}. \tag{1}$$

From (1) it can be seen that a quadratic improvement to TOF estimates is made through increasing the signal spectral bandwidth, and hence is the reason why UWB is a good approach for accurate TOF ranging. Furthermore, the SNR is linearly proportional to TOF variance. The Cramer–Rao lower bound range distance error is defined as the product $c \cdot \sigma_{\mathrm{TOF}}$, where c is the speed of light [12]. Figure 1 shows Cramer–Rao lower bounds on the ranging error for five different spectral signal bandwidths with n averaged samples. It can be seen that sub-metre ranging accuracy can be achieved by using a spectral bandwidth of as low as 2 MHz and averaging 3000 samples ($n = 3000$). In contrast, if the signal spectral bandwidth can

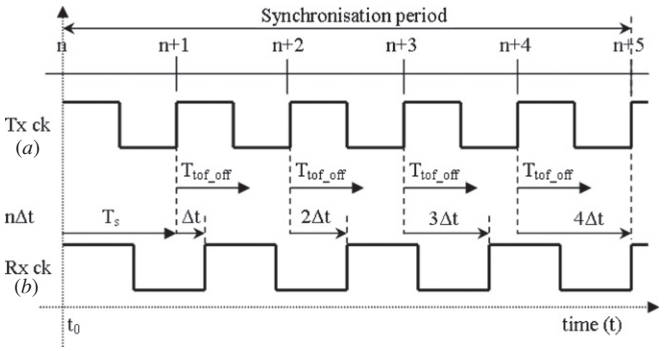

Figure 2. Schematic view of TOA phase measurement using correlator frequencies T_s and $(T_s + \Delta t)$ over successive range measurements. Transmit and receive assumed on rising clock edges.

be increased, a quadratic gain is made. This is not always ideal because of the FCC regulation on transmission power using ultra-wideband. Using less bandwidth and averaging greater numbers of ranging measurements is therefore a favourable approach. Time averaging has also been found to reduce the effects of multipath signal propagation and additive white Gaussian noise (AWGN) [12]; however, the use of multiple measurements increases the processing time which may introduce limitations on the estimation time and hence limit the applications of the ranging scheme (i.e. make it unsuitable for real-time tracking systems). For those reasons, a trade-off must be made in the choices of system parameters including signal bandwidth, signal power, chip-rate and ranging accuracy requirement.

2.2. Measurement resolution

In alternative narrow-band RF TOF measurement systems, resolution is limited by the time quantization introduced by the sampling period of the receiver's signal correlator [4], we denote this by equation (2). ΔR is the TOF ranging resolution (m), c is the speed of light (m s^{-1}) and T_s (s) is the sampling period of the receiver signal correlator:

$$\pm\Delta R = \frac{cT_s}{2}. \tag{2}$$

Ranging resolution in WSN applications is typically required to be within ± 1 m, and therefore $T_s \leqslant 6.66$ ns; this corresponds to a signal correlator sampling rate $F_s \geqslant 150$ MHz [4]. This is not ideal in low-power WSN hardware because of the increased power requirements of higher frequency oscillators ($I[\mathrm{A}] = \mathrm{d}Q/\mathrm{d}t$, as $\mathrm{d}t \to 0$, $I \to \infty$). For this reason, we consider a novel time-dependent TOF ranging method as an alternative to frequency-dependent methods. We achieve $T_s \leqslant 6.66$ ns by considering ranging transactions between a transmitter and receiver with signal sampling periods T_s and $(T_s + \Delta t)$. The time difference Δt allows sub-clock phase offset measurement over multiple ranging transactions as shown in figure 2. Ranging transactions arriving at the receiver before $T_{\mathrm{tof\_off}}$ have period τ and are binned in b_0. Ranging transactions arriving after $T_{\mathrm{tof\_off}}$ have $\tau + 1$ clock periods and are binned in b_1. $T_{\mathrm{tof\_off}}$ corresponds to the sub-clock period or phase measurement of the TOF period.

The number of ranging transactions n required to obtain the phase offset measurement is determined from $n = T_s/\Delta t$, and we define this as the synchronization period. The TOA period with phase offset measurement is finally extracted by finding the arithmetic mean as shown in equation (3):

$$\tau_{\mathrm{TOF}} = \frac{1}{n}\sum_{i=1}^{n}(b_0 + b_1). \tag{3}$$

Ranging transactions are offset by one clock period for each measurement with the constraints $(0 < \Delta t \leqslant 0.5T_s)$ and Δt divisible by T_s in order to achieve TOA ranging with phase offset measurement. The period Δt fundamentally limits the resolution of the TOF estimates. The effects of noise, multipath signal propagation and frequency inaccuracies may be reduced by oversampling over the synchronization period. Using this technique, TOF ranging estimates are time dependent as opposed to the previous frequency-dependent methods. The phase measurement principle can be seen from the Vernier delay line [13], where in this implementation, the function of the two buffer delay lines is generated through the frequency difference Δt. The transmission time and period of the transmitter clocks are required at the receiver in order to recover the TOF period; this is achieved through synchronization detailed in the next section.

2.3. Synchronization

There are two constraints relevant to the evaluation of TOF measurements: (1) the transmitting (Tx) and receiving (Rx) devices must be precisely synchronized to a common system clock (ck) and (2) the receiving device must be provided with the transmission time of the ranging signal. From this perspective, a signal is transmitted from some device A at a known time $(t_{A\text{-transmit}})$ and is detected at a measured time $(t_{A\to B})$ with reference to a common system time. There are two methods of synchronizing the devices A and B categorized as one-way transaction and two-way-time transfer (TWTT).

2.3.1. One-way ranging. With a one-way ranging transaction, synchronization between the transmitter and receiver devices is achieved by the use of different signal frequencies. An electromagnetic signal is used to synchronize the devices and a slower acoustic signal is used to measure the TOF [14].

2.3.2. Two-way time transfer. The two-way-time-transfer technique [15] is illustrated in figure 3 where devices A and B incorporate transceivers as opposed to a single transmitter and receiver. The method is used to compare two clocks or oscillators in order to reduce the phase offset (in clock cycles) and hence synchronize the devices. A and B operate from independent system times which are unsynchronized and have some phase offset where the resolution of the technique is bound by the period of the clock at device A. The phase offset and signal TOF between A and B are derived from equations (4)–(7), where $(t_{A\text{-transmit}})$ and $(t_{B\text{-transmit}})$ are the transmit times, $(t_{A\to B})$ and $(t_{B\to A})$ are the received times, (t_{tof}) is the time-of-flight period and $(t_{B\text{-offset}})$ is the phase offset

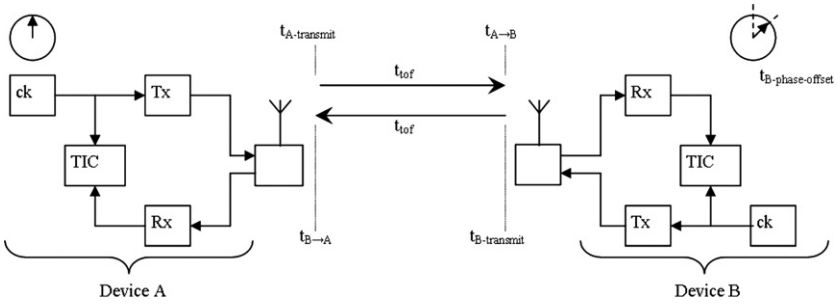

Figure 3. Two-way time transfer method for synchronization [15].

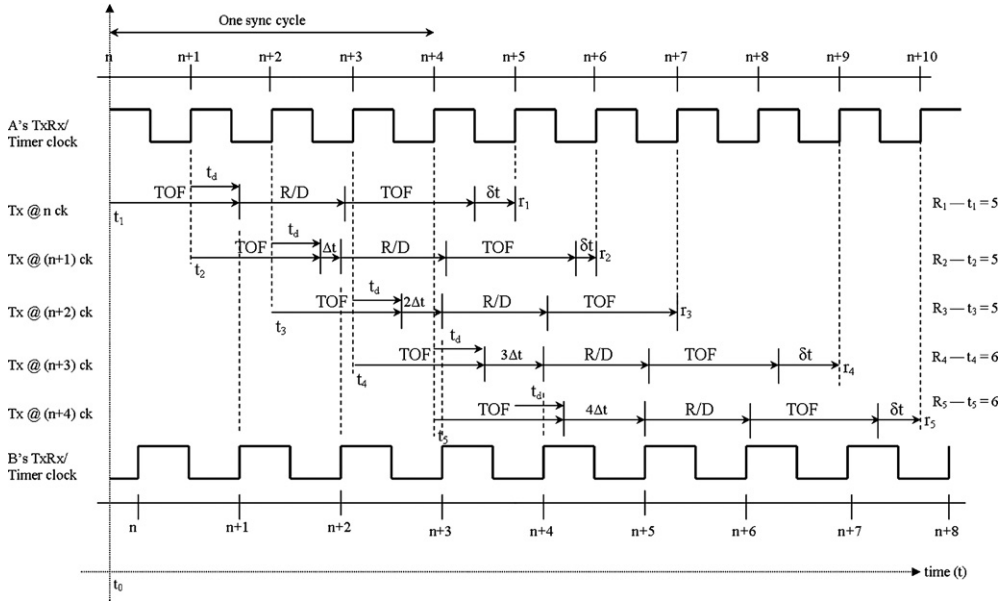

Figure 4. Timing diagram of two-way time-of-flight ranging with phase measurement.

of device B's clock with respect to device A's clock. The unsynchronized two-way time transfer measurements include the phase offset as an additive term in the forward transfer and a subtractive term in the reverse transfer with respect to A's clock. The additive phase offset can be removed by averaging multiple two-way transfers and hence an accurate TOF period is obtained. The TOF period is extracted from the time interval counter (TIC) or free-running timer. This is then calibrated to correspond to the true distance d[AB] by using d[m] $= \tau c$, where c is the speed of light (3×10^8 m s^{-1}):

$$t_{A\to B} = t_{A\text{-transmit}} + t_{\text{TOF}} + t_{B\text{-offset}}, \quad (4)$$

$$t_{B\to A} = t_{B\text{-transmit}} + t_{\text{TOF}} - t_{B\text{-offset}}, \quad (5)$$

$$t_{\text{TOF}} = \tfrac{1}{2}[(t_{A\to B} + t_{B\to A}) - (t_{A\text{-transmit}} + t_{B\text{-transmit}})], \quad (6)$$

$$t_{\text{offset}} = \tfrac{1}{2}[(t_{A\to B} - t_{B\to A}) - (t_{A\text{-transmit}} - t_{B\text{-transmit}})]. \quad (7)$$

3. Ranging system

To satisfy the synchronization requirement between two devices involved with TOF ranging, we use two-way ranging transaction in order to perform unsynchronized TOF measurements as illustrated from a time perspective in figure 4. Devices A and B operate from clocks with known periods t_1, t_2 where Δt is the difference in the period. We define the synchronization period as the number of cycles of clock A for which A and B are out of phase as shown in figure 2. Two-way ranging transactions are exchanged between the devices for each incremented period of clock A to obtain sub-clock period phase measurements over the synchronization period. The scheme operates by devices A and B first committing to perform TOF ranging and agreeing a common channel. Following this stage, two-way ranging transactions are made between A and B. Device A transmits a ranging message to device B. During transmission, A reads and stores the value of a free-running timer. After a TOF propagation period corresponding to the distance AB, the message arrives at B, which receives this message on its next clock edge after $n\Delta t$, where n is the phase measurement number. After a fixed period response delay (R/D), B transmits a ranging transaction back to A. Following the return TOF period, A receives the ranging message after a period δt and again stores the value of the free-running timer. The two-way period is determined by subtracting the final stored value from the initial stored value. This process is repeated with each two-way measurement shifted in time by one clock period over the synchronization cycle to obtain the round-trip estimates including a phase offset term. The period δt does

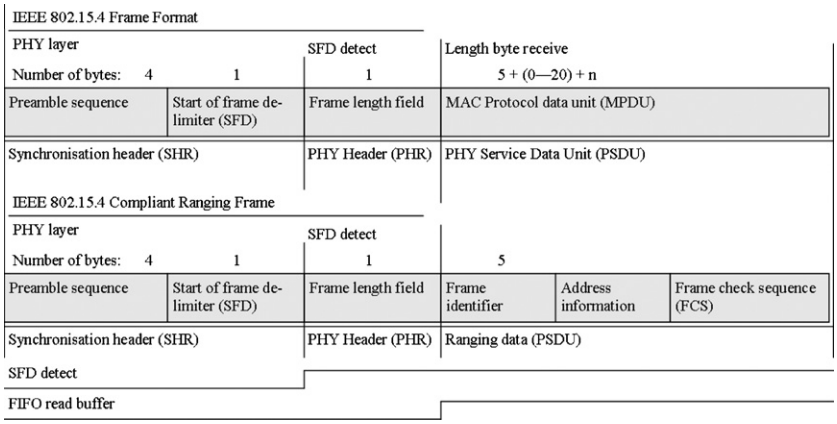

Figure 5. Schematic illustration of the IEEE 802.15.4 compliant ranging frame.

not affect phase measurements since its period is always less than one cycle of A's clock. Phase measurement resolution Δt is decided by the frequency difference between A and B where Δt is incremented for each measurement by transmitting on the next successive clock edge.

The TOF period with phase offset measurement t_d is then computed by equation (3) for n measurements over the synchronization period. This estimate is then converted to a distance estimate by executing three steps: (1) obtaining the calibrated round-trip period by subtracting the minimum round-trip period (when the distance A–B is zero) from the mean estimate round-trip period; (2) obtaining a single TOF period by dividing the calibrated estimate round-trip period by 2; (3) using the relationship $\Delta s = v\Delta t$ to convert from time to distance.

4. System implementation

4.1. Prototyping platform

A Texas Instruments TI CC2430 development kit [16] was selected to prototype the two-way TOF ranging system. The TI CC2430 is a fully integrated 2.4 GHz RF transceiver and Intel 8051 MCU particularly suited for personal area network (PAN) applications compliant with the Zigbee and IEEE 802.15.4 protocol. The RF radio module operates with direct sequence spread spectrum (DSSS) modulation with a 2 Mb s^{-1} chip-rate to produce a 250 kb s^{-1} data rate in the 2.4 GHz ISM frequency band [17]. To extract round-trip timing for TOF measurements, we use the TI CC2430s high-frequency 32 MHz crystal oscillator and medium access control (MAC) capture timer.

4.2. Frame format and timing extraction

The TI CC2430 supports the IEEE 802.15.4 frame format described fully in [17] consisting of a synchronization header (SHR), physical (PHY) header and PHY service data unit (PSDU). Its compliant adaption for TOF ranging is shown in figure 5 as transmitted by the PHY layer from left to right.

The synchronization header consists of a preamble sequence followed by a start-of-frame delimiter (SFD). During receive mode, the synchronization header is used by the transceiver signal demodulator to identify and synchronize to the incoming data frame. On reception, the transceiver frequency adjusts and synchronizes to the received preamble sequence. Compliant packets are identified by a continuous search and correlating the received preamble sequence with a local copy. The physical header also known as the frame length field defines the number of bytes in the MAC protocol data unit (MPDU) or PSDU. This field is implemented to make data frames compliant with IEEE 802.15.4 but is not essential for TOA ranging packets. To make the IEEE 802.15.4 frame efficient and suitable for TOF ranging measurements, only the synchronization header, PHY header and a PSDU consisting of an identifier, address information and check sequence are used. This corresponds to ranging packets which are 11 bytes in length.

Timing extraction for TOF estimation is provided through the SFD byte. On reception and synchronization of compliant packets, the SFD byte triggers timing extraction via a free-running timer. The TI CC2430 incorporates a 16-bit MAC timer which is configurable to capture the rising edge of the SFD on transmission and reception of ranging frames. This is configured to free-run and the round-trip period is extracted by subtracting the final timer value from the initial timer value. Switching between transmit and receive mode of the transceiver is performed through software for each two-way measurement.

4.3. Time-of-arrival estimation algorithm

Two-way TOF ranging is performed between two TI CC2430 development platforms which are flash programmed independently as an 'initiator' and 'responder'. For the purpose of testing, the address of the responder and the number of ranging transactions to be executed are pre-programmed on to the initiator prior to the ranging process. A ranging packet identifier is also predefined as a single byte. High level software flow diagrams for the initiator and responder are shown in figures 6 and 7.

To initiate the ranging process, the initiator device A requests to perform ranging with the responder device B by transmitting a 'request to range' (RTR) packet. Assuming

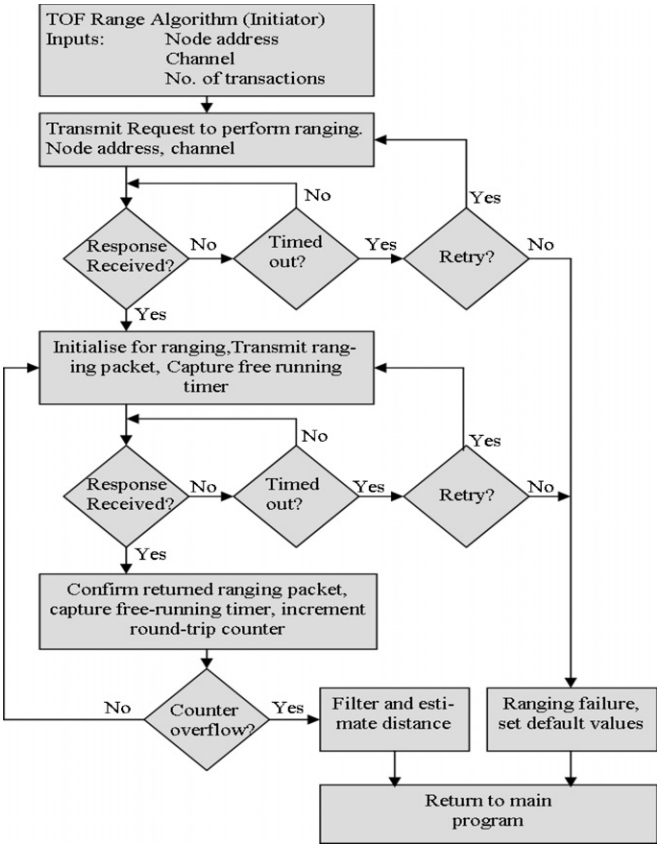

Figure 6. High level ranging algorithm flow diagram for an 'initiator' device.

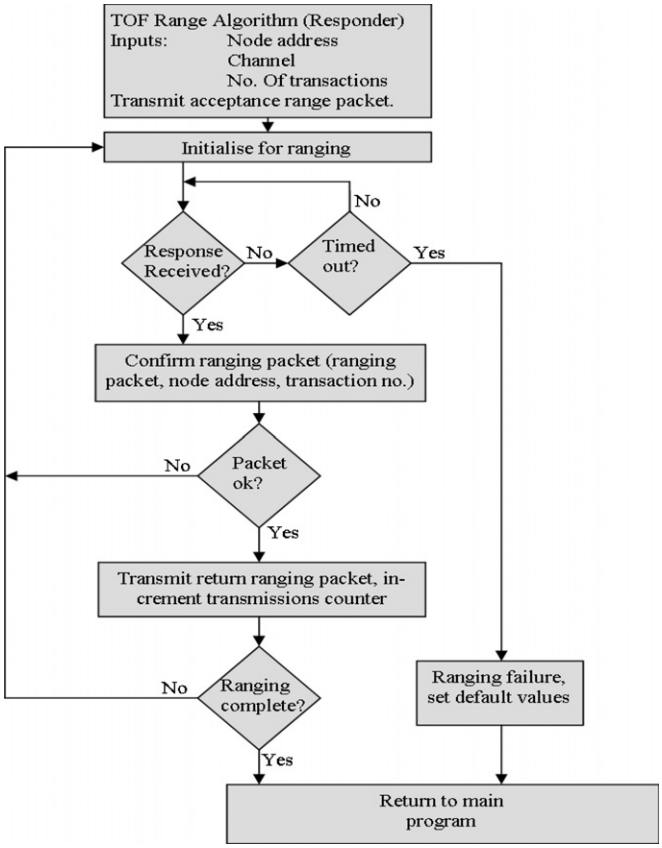

Figure 7. High level ranging algorithm flow diagram for a 'responder' device.

that device B is within a radio range of A and the packet is not lost, B receives and acknowledges the 'request to range' message by transmitting an 'acceptance to range' (ATR) packet back to A. Assuming arrival of the ATR packet at A within an appropriate time period, A initializes itself to perform ranging. The RF radio is configured and the agreed channel for ranging is selected. The round-trip timer is configured to operate as a free-running capture timer with capture activated by the rising edge of the SFD detect. A ranging packet is then transmitted to B with the value of the free-running timer captured on transmission. Device A switches to receive mode and waits for a return ranging packet from B. If the return ranging packet is not received within a time-out period, the ranging transaction is presumed 'lost' and the ranging packet is re-transmitted. Three re-transmission attempts are made before the ranging process is regarded as a 'failure'.

On reception of a packet at device A following previous transmission of a ranging packet, the packet preamble sequence and SFD trigger the capture of the free-running capture timer. Device A checks the identity of the packet and if as expected (i.e. a ranging packet), the round-trip measurement is calculated by subtracting the transmit time from the receive time. This value is stored and the ranging transaction counter is incremented to indicate the number of successfully completed ranging transactions. If a corrupted or incorrect packet is received, the round-trip measurement is disregarded. The process is repeated until the required number of ranging transactions have been achieved. The distance estimate with phase offset measurement is then computed and filtered as required. Ranging is complete and the estimated distance is returned to the main program.

From the perspective of the responder B, a 'request to range' (RTR) packet is received from device A. This packet contains the address of device A which is requesting to range with B, the channel on which ranging should be executed and the number of ranging transactions to be performed. Assuming that device B has the corresponding packet address, the ranging process can be executed. B acknowledges the RTR by transmitting an 'acceptance to range' (ATR) packet back to A and then enters a waiting loop ready for a ranging packet to be received from device A. If no ranging messages are received within the waiting loop, the loop times-out and the ranging process is regarded as a failure. The radio module and round-trip timer are returned to their default values before the ranging algorithm is exited. The main program receives a set of standard values in the case of a ranging failure. Alternatively, when a packet is received, B confirms the packet type, checks its validity and stores the transaction number. If the parameters are as expected, B transmits a return ranging packet back to A. This process is always executed over the same number of system clock cycles in order that the phase offset can be obtained. Alternatively, if the received packet is corrupt or of an incorrect type or format, B returns to its waiting loop ready to receive the next ranging packet. Following completion of all ranging transactions, B returns all hardware device values to their defaults and jumps back to the main program.

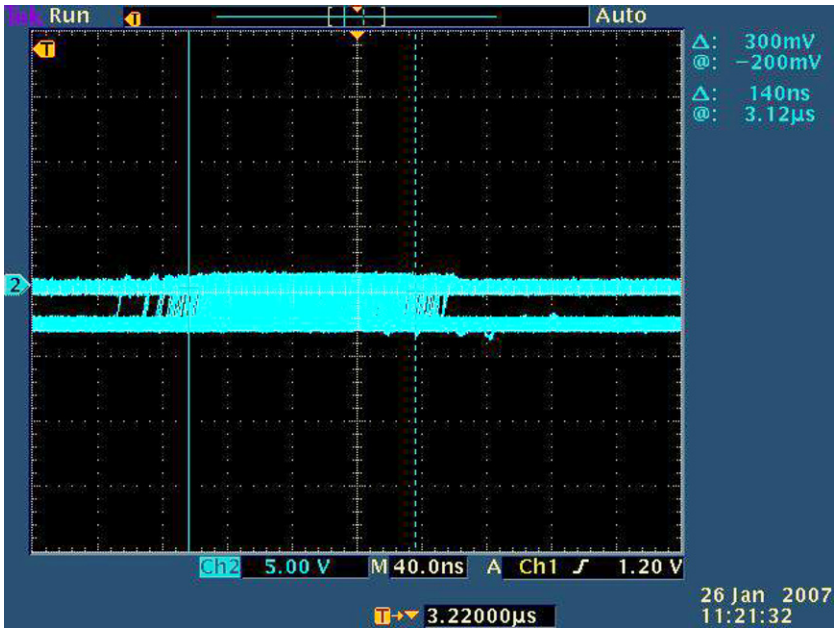

Figure 8. Digital storage oscilloscope capture of the TI CC2420 correlator drift over the 140 ns period.

4.4. Interference issues

The two-way TOA ranging system is prototyped using the TI CC2430 which uses an IEEE 802.15.4 compliant communications protocol and operates in the 2.4 GHz ISM band. It is expected that other wireless systems will interfere in this band including 802.11 b/g WLAN. To avoid interference, a clear-to-send channel check is made before transmission of ranging packets. If a ranging packet becomes corrupt or is lost, the two-way transaction is disregarded and an additional transaction is made to complete the data set. To further avoid interference issues with the prototype system, testing is carried out in remote locations where interference sources are minimal.

During the process of ranging in a network of an arbitrary number of nodes, the collision of ranging and data packets may be avoided by either performing ranging on a different RF channel to that of data transfer, using allocated time slots or by random delay between transmission of packets.

4.5. Time-of-flight error margin

MacCrady *et al* [18] define the error margin as the sum of all the variances of each time delay period of the transceiver components as a TOA ranging signal passes through them. The total time delay (T_{delay}) is a Gaussian random variable formed by summing each of the independent components and is defined by equation (8) where its variance is reduced by N two-way transactions $\left(\text{i.e. } \sigma_T^2 = \sigma_{t_r}^2/N\right)$:

$$T_{\text{delay}} = \frac{1}{N}\sum_{i=1}^{N}(t_i), \qquad \text{where} \quad i = 1, 2, \ldots, N. \tag{8}$$

For a single two-way ranging transaction, the total time delay consists of a transmission and reception at the initiator and responder (with antenna delays), a relative phase offset term between device clocks and a response delay period. This is defined by equation (9), where t_{1T}, t_{2T}, t_{1R}, t_{2R} are the transmission and reception times at the initiator and responder, Δt_2 is the relative phase offset and t_{2RES} is the response period:

$$T_{\text{delay}} = t_{1T} + t_{2R} + \Delta t_2 + t_{2RES} + t_{2T} + t_{1R}. \tag{9}$$

If multiple two-way transactions are performed, then the variance in TOA estimates is expected to reduce by a root function of the number of transactions. The corresponding error margin of equation (9) is expressed by equation (10). It is clear from (10) that the error in TOA estimates can be reduced either by multiple two-way transactions or by reducing the variance in individual time components:

$$\sigma_{\text{TOA}} = \frac{1}{\sqrt{N}}[\sigma_T + \sigma_{R2} + \sigma_{\Delta t2} + \sigma_{t2RES} + \sigma_{T2} + \sigma_{1R}]. \tag{10}$$

Considering that the TI CC2430 components cannot be independently accessed to measure individual time delays, we therefore draw several assumptions based on equation (10) before proceeding: (1) the time variance from the transceiver's analogue front end for both the receiver and transmitter including antenna delays is expected to be less than 1 ns, as reported in [18]; (2) the relative phase offset between the initiator and responder will contribute to the greatest error; (3) the error contribution from the response delay will also be less than 1 ns given that the crystal oscillator accuracy is typically 40 ppm of the crystal frequency for the TI CC2430.

To verify those assumptions, figure 8 shows the capture of the SFD over successive receptions of data packets using the TI CC2420. We use the TI CC2420 in place of the TI CC2430 because of the readily available hardware and direct access to the SFD through hardware. The transmitting TI CC2420 is used as a trigger for the digital storage oscilloscope (DSO), and the SFD rising edge of the receiving TI CC2420 is captured

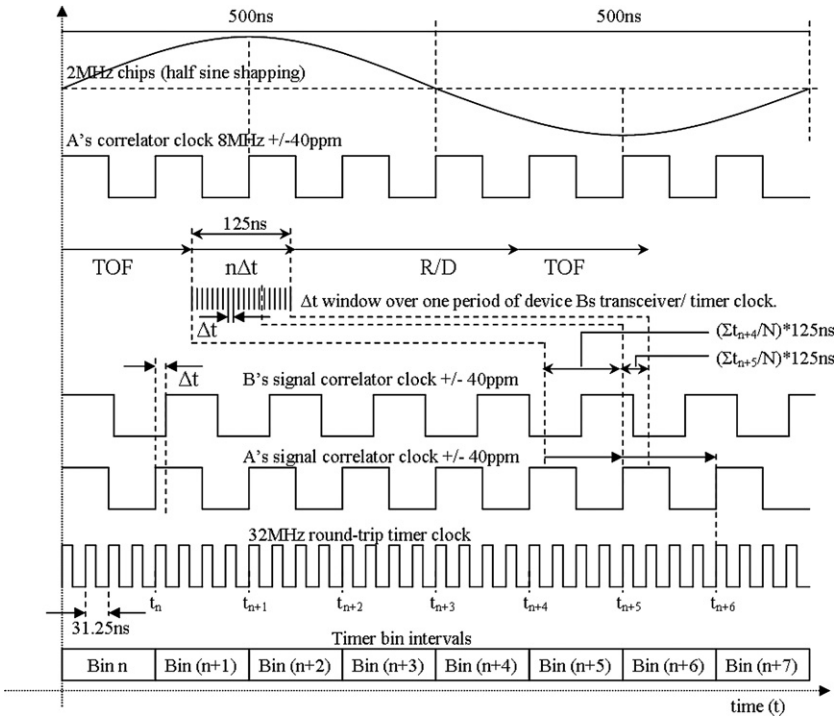

Figure 9. Two-way ranging with phase offset measurement using the TI CC2430.

by the DSO on reception of data packets; hence, figure 8 shows the variance contribution of $t_{1T} + t_{1R} + \Delta t_2$. Since t_{1T} and t_{1R} are expected to be small (i.e. < 2–3 ns), figure 8 confirms that the TI CC2420 correlates incoming chip sequences at 8 MHz (1/125 ns) given the approximate 125 ns drift period. The 140 ns period of drift is expected from t_{1T}, t_{1R} and early and late arrivals through multipath propagation during the testing in the laboratory.

Figure 9 illustrates a simplified timing diagram for the two-way ranging scheme using the TI CC2430. TOA ranging packets are transmitted using half-sine-shaped chips with frequency 2 Mchips s^{-1}. The drift period measured in figure 8 confirms the receiver's signal correlation period as 125 ns (8 MHz) in order to detect the half-sine-shaped chip sequences. To carry out round-trip timing using the TI CC2430, the MAC capture timer is used which has a frequency of 32 MHz. This is a factor of four times the correlation frequency and hence we expect the histogram bars to be separated by four clock periods for each round-trip time measurement. Although this does not affect the performance of the two-way ranging system, we expect a quantization error which will increase the number of transactions necessary to obtain a specified ranging accuracy.

Based on the result from figure 8 and the relative frequency difference between two TI CC2430 development boards, Δt is too small to measure using an oscilloscope. We make the assumption that relative phase offset between the initiator and responder is sufficiently random in order that the drift distribution can be considered normal. This corresponds to the initiator and responder having a random offset phase difference Δt. Under this assumption, ranging accuracy, in the absence of noise, is expected to be $\sigma_x^2 = 18.75/\sqrt{N}$, where N is the number of transactions (i.e. $d = vt \Rightarrow (3 \times 10^8) \cdot (125 \times 10^{-9}) = 37.5$ m, two-way $\Rightarrow 37.5/2 = 18.75$ m/clock period).

5. Preliminary experimental results

Ranging results have been obtained for LOS, NLOS and indoor environments using the standard TI CC2430 development kit operating on a single 2435 MHz channel and a transmission power of −1.5 dBm (700 mW). The LOS environment was a level grass field with no obstacles within 100.0 m of the test area. In contrast, the NLOS environment was on the University of Southampton Campus where buildings and foliage provided multipath, obstruction and signal blockage. Indoor testing was carried out in a residential flat constructed of brick work and stud-partition internal walls. Ranging was carried out over ranges of 250.0 m LOS, 120.0 m NLOS and 8.0 m indoors where the distances were restricted by boundaries of each test location.

In order to extract a valid set of ranging data, a simple program was written in Python software to interface one of the TI CC2430 development boards to a laptop computer via its RS232 port and record the ranging data. To provide initiator–responder distance referencing for the LOS and NLOS tests, an XE1610-OEMPVT GPS receiver evaluation module was also interfaced to the laptop computer via USB. The ranging measurement and GPS position estimates were then thread-read and recorded once per second each time a GPS position estimate became valid. Any corrupt samples (i.e. corrupt or lost ranging packets) were disregarded. The GPS receiver has an expected position accuracy of <5.0 m circular error probable (CEP) and resolution of >2.0 m by conversion of the

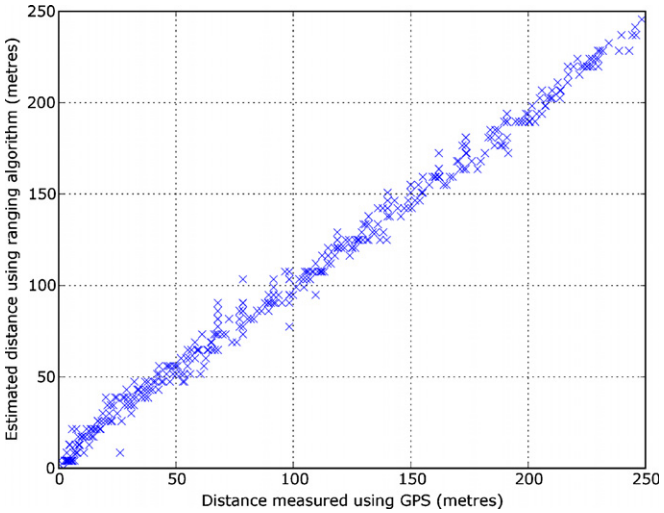

Figure 10. Performance of the ranging algorithm for the LOS condition, TI CC2430 ranging estimate versus GPS measured distance, 100 two-way samples. RMS error = 7.0 m, max error = 24.9 m, min error = 0.0 m.

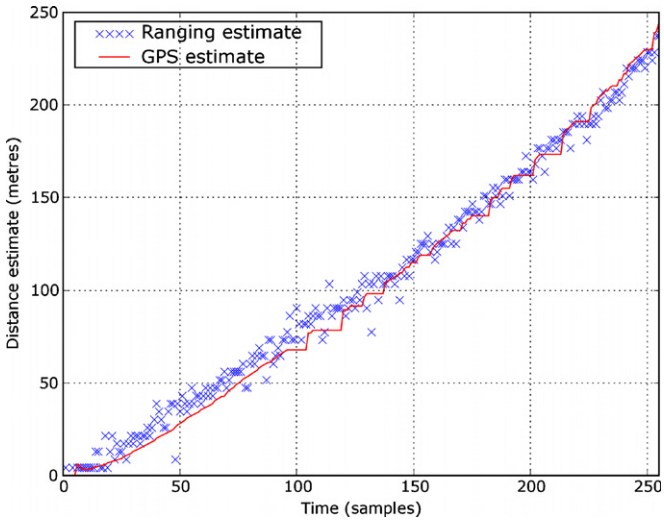

Figure 11. Performance of the ranging algorithm for the LOS condition, TI CC2430 ranging estimate and GPS measured distance versus time (samples), 100 two-way samples.

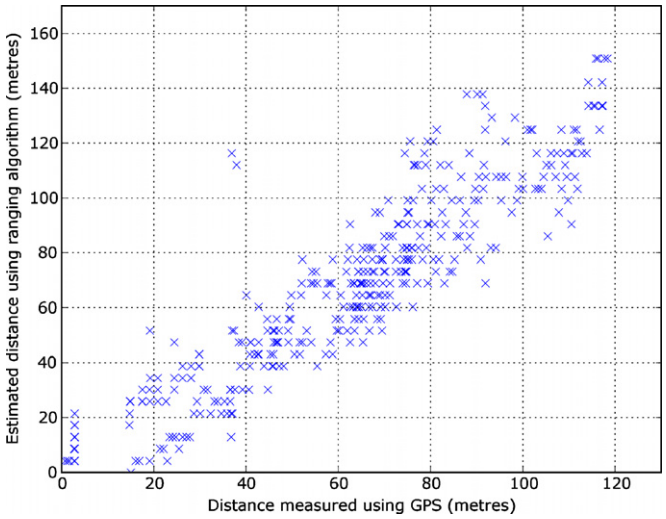

Figure 12. Performance of the ranging algorithm for the NLOS condition, TI CC2430 ranging estimate versus GPS measured distance, 100 two-way samples. RMS error = 15.8 m, max error = 79.5 m, min error = 0.0 m.

latitude and longitude coordinates to metres. To confirm our conversion calculations, a measuring wheel was also used to measure the 250.0 m for the LOS condition. The accuracy of those techniques was considered satisfactory to reference the RF two-way TOA ranging with the phase offset measurement algorithm. A 100 sample average was chosen arbitrarily per TOF measurement. This corresponds to an expected variance in ranging measurements of 1.9 m under ideal assumptions (i.e. random clock offset and in the absence of noise). Since GPS cannot obtain signal lock indoors, ranging estimates were measured in 1 m increments relative to a tape measure. A high sample set of 1000 samples were used per measurement in order to achieve an expected variance in estimates of less than 0.6 m. To calibrate the ranging measurements, the minimum round-trip period was estimated over an average of ten ranging transactions when the transceivers were in close proximity (<1.0 m). This average value was then subtracted from each ranging measurement before conversion to the distance estimate.

The linear ranging performance for the LOS condition over 250.0 m is shown in figures 10 and 11. The results confirm a typical improvement in ranging performance through averaging with an RMS error of 6.7 m. Resolution is typically 4.6 m because of the quantization introduced by averaging samples on the TI CC2430. Performance was consistent over the 250.0 m distance performance only significantly degrading on reaching the limit of the TI CC2430 radio range which is as expected. The step-response of the GPS referencing in figure 11 typically shows that the distance referencing (GPS receiver) lost signal lock during the test which introduces a small error in the measured performance. One alternative frequency-dependent RF TOA ranging method [5] reports TOA ranging estimates with the RMS error of 0.9 m_{rms} and the peak error of 2.5 m for the LOS condition using an FPGA and similar 2.4 GHz RF radio module. In comparison, our time-dependent TOA ranging results inherit greater RMS error which we expect is due to both the low averaged sample number and the inaccurately generated period Δt and unknown synchronization period using our prototype system implemented on off-the-shelf hardware.

Performance for the NLOS condition over 120.0 m is shown in figures 12 and 13 by moving the responder through different LOS, NLOS and complete signal blocked positions. The increased spread in ranging estimates illustrated in figure 12 confirms that the ranging system suffers more significantly in those conditions as expected. The RMS error is 15.8 m which is over twice the error reported for the LOS condition. This is expected not only for the aforementioned reason, but also due to the loss of GPS signal lock and the contoured landscape which was not accounted for with reference to GPS. NLOS ranging in [5] reports ranging results through a wall for fixed distance up to 10 m. The ranging error is 1.8 m_{rms} with a peak error of 3.4 m. We expect that the

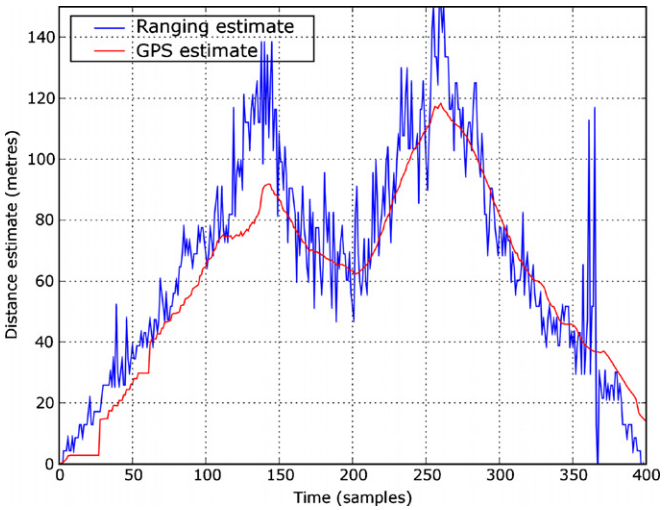

Figure 13. Performance of the ranging algorithm for the NLOS condition, TI CC2430 ranging estimate and GPS measured distance versus time (samples), 100 two-way samples.

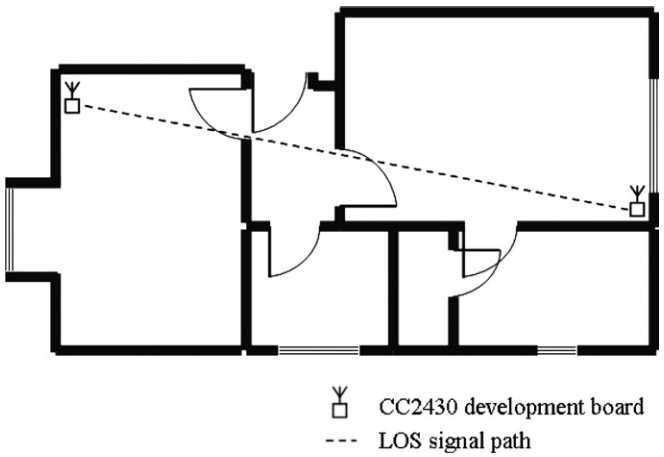

Figure 14. Scale diagram of the residential flat used for indoor testing of the two-way TOA ranging algorithm. External walls constructed using brickwork; internal walls are stud-partition. Ranging experiments conducted for the LOS condition over 8 m with internal doors open.

significantly larger range error in this result is due to the larger transceiver–transceiver separation distance and NLOS signal propagation over the NLOS test environment.

A scale drawing of the indoor test environment is illustrated in figure 14. The initiator–responder separation distances are increased in 1 m increments over a total distance of 8 m with each estimate being computed for 1000 averaged samples. The sample number is increased to reduce the variance in estimates due to the short testing distance. Internal doors were left open during the test and testing was carried out for the LOS condition through three rooms including a living room, hall and bedroom with full furnishings including tables, bookshelves, chairs, glass units and many other surfaces which contribute to signal distortion and scattering. Figure 15 illustrates ranging performance for the condition where the responder is placed at each known distance between 0.0 and 8.0 m. The ranging RMS error was measured as 1.7 m

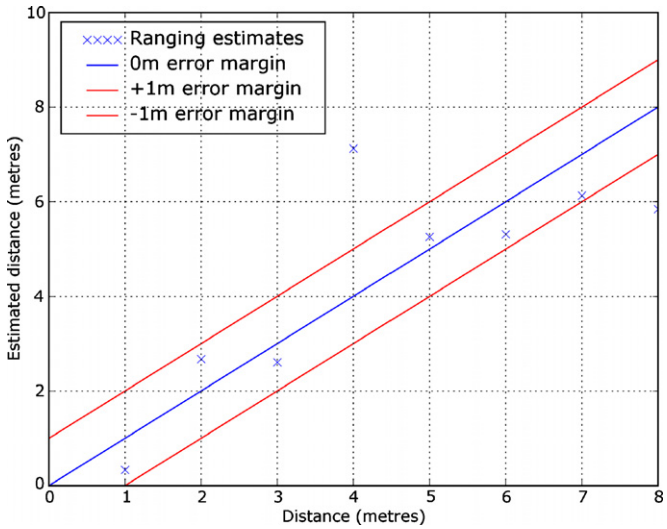

Figure 15. Performance of the ranging algorithm for the indoor condition, TI CC2430 ranging estimate versus measured distance, 1000 two-way samples. RMS error = 1.7 m, max error = 3.2 m, min error = 0.3 m.

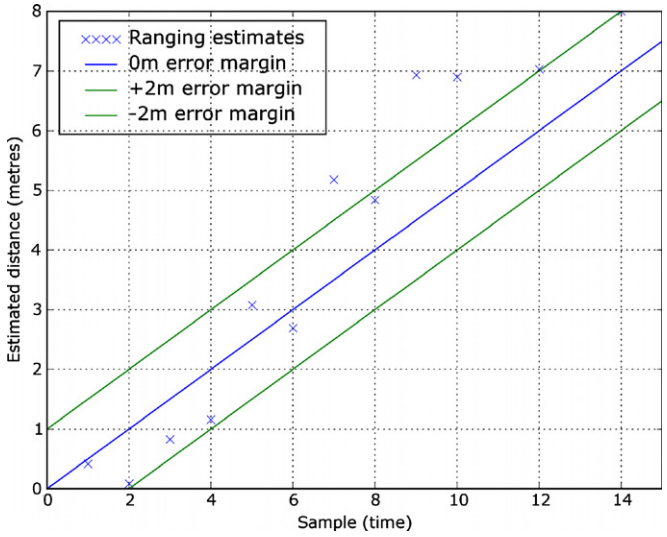

Figure 16. Real-time motion performance of the ranging algorithm for indoor condition, TI CC2430 ranging estimate versus measured distance, 1000 two-way samples. RMS error = 3.2 m, max error = 6.0 m, min error = 0.0 m.

with a maximum error of 3.2 m. This compares well to the indoor LOS results reported in [5] where the ranging error was measured as 2.6 m_{rms} with a peak error of 5.5 m over similar transceiver–transceiver test distances. Our results confirm that averaging greater sample numbers reduces TOA range estimates as expected. Figure 16 shows the performance of the algorithm for real-time motion when the responder is linearly moved over an initiator–responder distance of 8.0 m. The RMS error was measured as 3.2 m with a maximum error of 6.0 m. The larger error was expected under velocity because of the time-variant channel.

The results are summarized in table 1. Ranging accuracy is constrained by noise, quantization in the round-trip timing measurements and averaged sample number. Assuming a

Table 1. Prototype ranging system estimation errors (m) measured relative to the GPS range estimate.

	Sample no	σ expected	RMS error (m)	Max. error (m)
LOS	100	$\approx 1.9 + \sigma_n$	7.0	24.9
NLOS	100	$\approx 1.9 + \sigma_n$	15.8	79.5
Indoor	1000	$\approx 0.6 + \sigma_n$	1.7	3.2

normally distributed clock offset (figure 8), the expected accuracies in the absence of noise, transceiver AFE and signal lock delays are 1.9 m for the LOS and NLOS conditions using a 100 sample average ($\sigma_x^2 = 18.75/\sqrt{N}$, where $N = 100$). Under the same assumptions, indoor accuracy was expected within 0.6 m using 1000 averaged samples ($\sigma_x^2 = 18.75/\sqrt{N}$, where $N = 1000$). The addition of noise, signal multipath, AFE and transceiver signal lock delays increased this variance for each condition. Figure 8 confirms a 140 ns relative drift period; hence, we expect the variance in time delay from all additional contributions to be in the region 0–10 ns (140 ns − 125 ns → 15 ns, minus multipath delay from test environment), hence limiting the performance of this ranging technique. We expect those time variance contributions to be reduced by increasing the number of two-way ranging transactions.

6. Conclusion

We have successfully implemented and demonstrated a novel narrow-band two-way TOA ranging method with phase offset measurement using low-frequency clocks to determine range measurements with accuracies better than 7.0 m LOS, 15.8 m NLOS and 1.7 m indoor using low-cost, low-power hardware. In addition, our algorithm operates fully on a single-chip solution. To the best of the authors' knowledge, this is the first time-dependent RF TOA ranging scheme to exploit the relative offset in frequency between two radio transceivers involved with TOA ranging in order to improve ranging resolution. The technique therefore has substantial benefits in WSNs where sensor nodes are required to operate with low-power consumption and thus a low system clock frequency. In addition, the use of conventional RF as opposed to UWB allows the operating range of the WSN within regulation to be over a much greater range (>50 m).

The resolution of this technique is bound by three fundamental factors: (1) variance in time delays of the transceiver analogue front end; (2) the distribution of the relative clock offset between the transceivers herein assumed to be normally distributed; (3) the signal-to-noise-ratio (SNR). The time taken to achieve a specified degree of accuracy is limited by the bandwidth of the signal correlator.

For this technique to operate as expected, the assumption was made that the distribution of the relative clock offset between transceivers is normally distributed. Figure 17 illustrates the quantized distribution of the relative clock offset. This test was performed for 1000 round-trip TOA measurements where the initiator and responder were placed with antennas separated by 0.1 m. The signal correlator

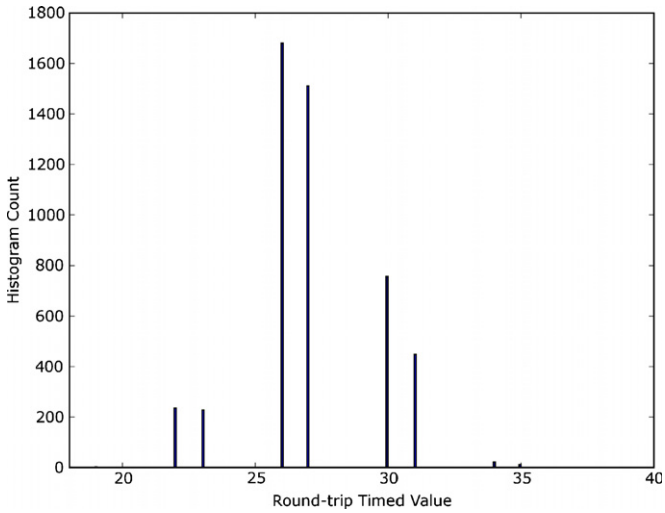

Figure 17. Histogram count of round-trip timed values for 5000 two-way TOA measurements using the TI CC2430.

frequency was determined as 8 MHz, four times lower than the 32 MHz MAC timer used for round-trip timing; hence, we expect histogram bars to be spaced by four clock periods (i.e. at 22, 26, 30 and 34). The additional bars at 23, 27, 31 and 35 we expect are caused by late triggering of the capture timer. In the ideal case (i.e. in the absence of noise and no time delays in AFE) only two histogram bars exist; however, the additional bars are expected due to the 140 ns drift period shown in figure 8. It is expected that error is also caused by the non-ideal receiver lock on chip-sequences during reception as the receiver tries to synchronize to the packet preamble chip sequence.

We suspect that the recorded variances are greater than expected because of the error contribution caused by referencing the system to GPS during the test. In addition, we expect the error to exist in the calibration because the relative phase offset between the device clocks will not be the ideal normal distribution that we assume.

One previous RF TOF ranging system (frequency-dependent) prototyped by Karalar and Rabaey [4] reports an RF TOA ranging scheme with estimation accuracy within −0.5 to 2.0 m using an FPGA with a 100 Msps ADC sample rate. Ranging accuracy in this scheme is improved by increasing the sample rates of the signal ADC and DAC. We use a TI CC2430 with determined signal sampling of 8 Msps and a TOA phase offset scheme to achieve ranging accuracy below 7.0 m RMS under LOS conditions using 100 averaged samples. Ranging accuracy is improved by increasing the sample number making this scheme suitable for WSN applications where low-frequency system clocks are ideal.

Our further work will involve improving the accuracy and resolution of this TOA-based ranging technique and implementing the method into fixed infrastructure and relative locationing systems. We intend to improve the performance by using a known frequency difference between the transceivers in order to obtain Δt more accurately. This will enable us to achieve our desired accuracy with significantly less round-trip samples. We also intend to replace the arbitrary chosen sample number N by considering the variance in the

round-trip time measurement distribution to automatically perform the required number of ranging transactions N for a specified ranging accuracy. Further development will involve the implementation of filtering to reduce the variance of round-trip measurements under NLOS conditions. We also intend to investigate further the transceiver signal lock to reduce the error in round-trip measurements.

References

[1] Mainwaring A, Polastre J, Szewczyk R, Culler D and Anderson J 2002 Wireless sensor networks for habitat monitoring *WSNA'02: Proc. 1st ACM Int. Workshop on Wireless Sensor Networks and Applications*

[2] Tian J, Wu H and Gao M 2008 Measurement and control system of sewage treatment based on wireless sensor networks *IEEE Int. Conf. on Industrial Technology, 2008: ICIT 2008 (April 2008)* pp 1–4

[3] Fontana R J, Richley E and Barney J 2003 Commercialization of an ultra wideband precision asset location system *IEEE Conf. on Ultra Wideband Systems and Technologies, 2003 (16–19 November 2003)* pp 369–73

[4] Karalar T C and Rabaey J 2006 An RF ToF based ranging implementation for sensor networks *IEEE Int. Communications Conf. (University of California, Berkeley, June 2006)* vol 7, pp 3347–52

[5] Lanzisera S, Lin D T and Pister K S J 2006 RF time of flight ranging for wireless sensor network localization *Int. Workshop on Intelligent Solutions in Embedded Systems, 2006 (30 June 2006)* pp 1–12

[6] Fontana R J and Gunderson S J 2002 Ultra-wideband precision asset location system *IEEE Conf. on Ultra Wideband Systems and Technologies (May 2002)* pp 147–50

[7] Li X 2005 Performance study of RSS-based location estimation techniques for wireless sensor networks *Military Communications Conf., 2005: MILCOM 2005 (IEEE, 17–20 October 2005)* vol 2, pp 1064–8

[8] Schantz H G 2007 A real-time location system using near-field electromagnetic ranging *Antennas and Propagation Society Int. Symp., 2007 (IEEE, 9–15 June 2007)* pp 3792–5

[9] Peng R and Sichitiu M L 2006 Angle of arrival localization for wireless sensor networks *IEEE Communications Society on Sensor and Ad Hoc Communications and Networks (28 September 2006)* pp 374–82

[10] Texas Instruments TI CC2430 datasheet, www.ti.com

[11] Urkowitz H 1983 *Signal Theory and Random Processes* (Boston, MA: Artech House)

[12] Chung W C and Ha D S 2003 An accurate ultra wideband (UWB) ranging for precision asset locationing *IEEE Conf. on Ultra Wideband Systems and Technologies (16–19 November 2003)* pp 389–93

[13] Xia T, Zheng H, Li J and Ginawi A 2005 Self-refereed on-chip jitter measurement circuit using Vernier oscillators *IEEE Computer Society Annual Symp. on VLSI (May 2005)* pp 218–23

[14] Sallai J, Balogh G, Maróti M, Lédeczi A and Kusy B 2004 Acoustic ranging in resource-constrained sensor networks *Int. Conf. on Wireless Networks (Nov. 2004)* p 467

[15] Xia T, Zheng H, Li J and Ginawi A 1989 Fundamentals of two-way time transfers by satellite *Proc. 43rd Ann. Symp. on Frequency Control (May–June 1989)* pp 174–8

[16] TI/Chipcon CC2430DK Development Kit, www.ti.com

[17] IEEE 2003 802.15.4 Standard for Information Technology (London: IEEE)

[18] McCrady D D, Doyle L, Forstrom H, Dempsey T and Martorana M 2000 Mobile ranging using low-accuracy clocks *IEEE Trans. Microwave Theory Techn.* **48** 951–8