A Two-Way Time of Flight Ranging Scheme for Wireless Sensor Networks

Evangelos B. Mazomenos, Dirk De Jager, Jeffrey S. Reeve, and Neil M. White

Electronic Systems and Devices Group,
School of Electronics and Computer Science,
University of Southampton,SO17 1BJ, U.K.
{ebm07r,ddj07r,jsr,nmw}@ecs.soton.ac.uk

Abstract. Relative ranging between Wireless Sensor Network (WSN) nodes is considered to be an important requirement for a number of distributed applications. This paper focuses on a two-way, time of flight (ToF) technique which achieves good accuracy in estimating the point-to-point distance between two wireless nodes. The underlying idea is to utilize a two-way time transfer approach in order to avoid the need for clock synchronization between the participating wireless nodes. Moreover, by employing multiple ToF measurements, sub-clock resolution is achieved. A calibration stage is used to estimate the various delays that occur during a message exchange and require subtraction from the initial timed value. The calculation of the range between the nodes takes place on-node making the proposed scheme suitable for distributed systems. Care has been taken to exclude the erroneous readings from the set of measurements that are used in the estimation of the desired range. The two-way ToF technique has been implemented on commercial off-the-self (COTS) devices without the need for additional hardware. The system has been deployed in various experimental locations both indoors and outdoors and the obtained results reveal that accuracy between 1m RMS and 2.5m RMS in line-of-sight conditions over a 42m range can be achieved.

1 Introduction

The ability to estimate the relative distance between low-power wireless embedded nodes is paramount for a number of applications which require location-awareness [1, 2]. In the general case, two or more nodes will engage in some kind of interaction, typically transmit and/or receive signals, and will be tasked with measuring a property of the signal that can be appropriately processed in order to extract the relative distance between the two interacting nodes. For example, by measuring the Received Signal Strength (RSS) value of a signal, the range between the two nodes can be derived [3]. Another well-known approach is based on calculating the transit time of a signal and use it to estimate the point-to-point range of two nodes. These methods are known as Time of Flight (ToF) or Time of Arrival (ToA). The amount of time that a signal requires to reach the receiver is measured with the use of on-node clocks. The a-priori knowledge of the signal's velocity enables the approximation of the desired distance.

Important advancements in microelectronics technology over the past decade, resulted in the production of very accurate clocks (ns accuracy) in electronic devices. As

a result a variety of ToF methods has been utilized in a number of established navigational and positioning systems (e.g. GPS). Consequently, as node localization became a necessity in WSNs, ToF techniques for low-power sensor nodes have been investigated. One major area of concern, has been the fact that low-power embedded devices are not equipped with high frequency clocks and time synchronization in these devices is an inherently difficult task, which also has attracted significant research interest [4, 5].

In this paper a two-way ToF ranging technique for WSNs is proposed. Our approach is to employ a two-way ToF method in order to avoid the need for synchronization between the participating nodes. This method targets low-power embedded devices, thus the clocks that are considered, operate at relatively low-frequencies (up to 32MHz). Multiple two-way ToF measurements are obtained which allows the system to achieve sub-clock resolution. The final ToF value is extracted after averaging the accumulated timing values. A simple, yet practical procedure is employed to eliminate any erroneous data which are caused because of surrounding noise or sampling artifacts. A calibration step is also carried out to exclude the delays that are included in the two-way path of the signal. Accuracy and latency are important in a ranging system for low-power embedded nodes capable of operating in real-time. Different to a number of approaches in this research area where the accumulated data require significant post-processing, the proposed system completes all the necessary processing on the nodes that participate in the ranging operation. Hence the proposed ranging system can support distributed applications and can act as an auxiliary network service. The estimation of the range can then be exploited according to application needs. The key contributions of this paper are the implementation of a two-way ToF ranging method on COTS hardware and the evaluation of its performance on real-world experiments

The remainder of this paper is organized as follows. The following section performs a review of previously proposed ToF systems in WSNs with some background information regarding ToF ranging. In sequel, the specific details of the two-way ToF ranging that is proposed, are provided in Section 3 alongside an investigation of the error sources. A thorough analysis, of the implementation on hardware follows in Section 4. Section 5 presents the experiments that were carried out in indoors and outdoors locations and the analysis of the results obtained. Finally, Section 6 summarizes the key points and concludes the paper.

2 Related Work

ToF ranging systems attempt to estimate the point-to-point distance between two communicating devices by capturing the time that a signal requires to travel from one device to the other. Since the speed of the signal is known and constant (e.g., the speed of light for electromagnetic signals), the distance can then be calculated. McCrady *et.al* are among the first to propose a ToF ranging system for WSNs [6]. However their work lacks implementation. The RSSI and ToF methods have been combined in a locationing system [7]. Ultra Wideband (UWB) transceivers have the ability to yield fine-grained resolution in measuring the ToF due to the high bandwidth occupancy. Thus, a handful of ToF ranging systems are based on Ultra Wideband (UWB) technology [8–10]. However, low-power WSNs nodes are normally not equipped with UWB transceivers

and their incorporation on embedded nodes presents a number of challenges. Lanzisera *et. al.* propose a ToA locationing scheme for low-power ASIC WSN nodes [11]. In the prototype an FPGA board is attached to the WSN node to carry out the necessary calculations. FPGA boards alongside WSN nodes are also used in [12], where a RF-ToF ranging system is presented and the ToF is extracted by the channel impulse which is produced after converting the received signal from the time to the frequency domain by applying FFT. For this procedure, both FPGA and DAC are used. The approach we propose, differentiates from the previous approaches since it does not require any additional per-node hardware.

An intriguing approach for ToF ranging in WSNs is the one that employs acoustic signals instead of electromagnetic ones. It is known that acoustic signals travel in a much slower speed than electromagnetic signals thus making them easier to utilize in ToF scenarios. Both ultrasonic and audible sound signals have been utilized in ToF ranging systems. Occasionally, acoustic and RF signals can be combined in a time difference of arrival method (TDoA). The two signals are emitted simultaneously and the RF signal is used to synchronize the receiver. The TDoA value is considered to be the ToF of the acoustic signal. A ranging system based on this approach is implemented on the Mica2 mote in [13]. A simple tone which is produced by the mote's sounder is the acoustic signal that it is timed. The "Calamari" localization system follows a similar approach but employs the tone detector of the Mica mote instead of the sounder and requires all participating nodes to be pre-calibrated to achieve good accuracy [14]. Another example where acoustic and RF signals are used on the same system is the "Cricket" locationing system developed at MIT [15]. One disadvantage of acoustic ranging, is the limited effective range of acoustic-based ranging systems. The systems presented previously are capable of producing accurate ranging but within a limited range. Radio interferometric geolocation is another method to estimate the range in wireless embedded nodes, by using the radio interferometry principle. According to the authors in [16] very good accuracy ($< 10cm$) can be achieved. The major drawback of this system, which makes it unsuitable for real-time ranging, is that a significant amount of time is required for the ranging algorithm to run to completion.

The proposed ranging method for low-power embedded nodes is inspired by the work presented by Thorbjornsen *et. al.* in [17]. Our intention is to evaluate the two-way ToF ranging technique and ultimately incorporate it in the range-only tracking system presented in [18]. The approach presented here, attempts to achieve better resolution in timing the value of the two-way message exchange by employing a different method on how the timer's value is captured. Instead of detecting a received message by sampling the receiver with a constant sampling rate, the receiver is programmed to signal an interrupt whenever a ranging message has completed a two-way path. The interrupt routine is then used to capture the value of the running timer. This approach results in better resolution of the two-way timing values, thus achieves better resolution in the resulting distance by processing multiple two-way transactions between the participating nodes.

3 Overview of the Proposed System

The basic concept of the proposed two-way ToF ranging system is illustrated in Figure 1. The objective is to estimate the distance between node A and node B.Initially node A sends the first ranging signal and captures the time of its timer ($\mathbf{t}_{tAB}$). Node B receives the signal and after a period of time, that corresponds to node B swapping its state, from receiver to transmitter (as well as a number of other delays) node B sends a ranging signal back to node A. Following, node A receives the reply signal and stores the time of reception ($\mathbf{t}_{rBA}$). The timer in node A measures $\mathbf{t}_A = \mathbf{t}_{rBA} - \mathbf{t}_{tAB}$ multiple times. Instead of using a clock at node B to measure the time that the signal spends in the node, our approach is to measure all the delays that occur during this two-way signal exchange process. This is accomplished by placing the transceivers at a minimum distance ($< 0.2m$) and executing multiple transactions that are averaged to produce the minimum time($\mathbf{t}_{min}$) that is required in order to complete a message exchange. This time corresponds to a minimal ToF period and reveals all the hardware and software delays that occur during a two-way ranging transaction. We make the assumption that the these delays remain constant and are independent of the distance between the nodes. Subsequently only the propagation delay will increase the two-way time transfer value as the nodes are placed at greater distance.

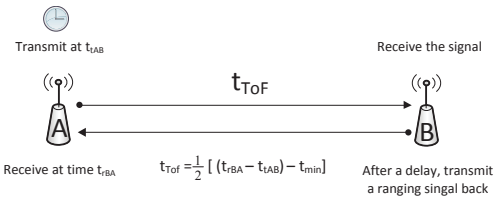


Fig. 1: Proposed Two-way ToF Ranging

Figure 2 illustrates a timing diagram of a message exchange between the two nodes. Send and receive occurs on the rising edge of the nodes clocks. Assuming that for a set distance the t_{ToF} will be the same and the delay T_{B_proc} that node B requires to process the ranging signal and submit the reply is constant, then the only ambiguity will be inserted by the delays associated to the clocks phase shift and frequency drift. Given that the two clocks are unsynchronized and have a small difference in frequency the phase offset between the devices will oscillate, thus the delays T_{d1} and T_{d2} will follow a similar varying pattern. By oversampling, we capture a normally distributed set of multiple timing transactions centered around the mean ToF value. Subsequently, capturing a sufficiently large number of timing values will allow us to extract the mean ToF value from the Gaussian distribution which can be, linearly associated to the distance between the nodes.

The calculation phase involves the extraction of the ToF out of the multiple stored timer values. In the event that one, or in general a small fraction of these n transactions has produced erroneous timing, including them in the average calculation will result in

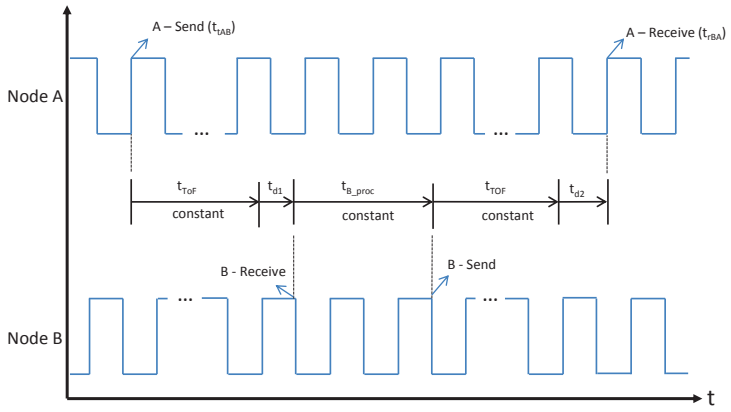


Fig. 2: Timing Diagram of a two-way message exchange

a distortion of the correct mean value. To avoid this, and to assure that the ToF calculation is based on the most accurate and "true" transactions the following procedure is followed. Let us assume that we obtain n two-way ToF values $\mathbf{t}_n$. The initial average mean $\widetilde{\mathbf{t}}_{ToF}$ and the standard deviation of the n values is given from the following:

$$\widetilde{\mathbf{t}}_{ToF} = \frac{1}{n}\sum_{i=1}^{n}\mathbf{t}_n \qquad \sigma_{ToF} = \frac{1}{n}\sum_{i=1}^{n}(\mathbf{t_n} - \widetilde{\mathbf{t}}_{ToF}) \tag{1}$$

In the following step we calculate the absolute difference of each one of the n values from the initial mean. Ultimately, out of the n collected ToF values we exclude the ones that their absolute difference to the initial mean is greater than the standard deviation. The final $\widehat{\mathbf{t}}_{ToF}$ value is calculated by averaging the remaining m values.

$$\widehat{\mathbf{t}}_{ToF} = \frac{1}{m}\sum_{i=1}^{n}\mathbf{t}_m \tag{2}$$

Obtaining the two-way ToF is the main step in estimating the range between the two nodes. That value is converted to distance by executing the following.

1. Calibrate the $\widehat{\mathbf{t}}_{ToF}$ value by subtracting it from the minimum two-way ToF. The minimum two-way ToF ($\mathbf{t}_{min}$) is obtained by placing the nodes at a minimum distance and averaging n transactions in a similar way as mentioned previously.
2. Divide the calibrated value by two, to get a single-way ToF time. $\mathbf{t}_{ToF_{final}} = \frac{1}{2}(\widehat{\mathbf{t}}_{ToF} - \mathbf{t}_{min})$.
3. Multiply the above with the speed of light to convert time to distance

3.1 Sources of Ranging Error

The achievable accuracy of any RF-ToF ranging system is primarily limited by the following four factors which introduce temporally and spatially random errors [19].

Corrupting Noise Noise as well as interference, are two major factors that can cause the accuracy to degrade. In RF-ranging systems for example, noise can cause the receiver to detect signals in the wrong time leading to faulty measurements. The effect of noise in a ranging method can be quantified with the use of the Signal-To-Noise Ration (SNR) in the receiver's side and the occupied bandwidth (B). These measures are linked via the Cramér-Rao Lower bound (CRB). For two-way ToF ranging systems and n measurements averaged, the CRB of variance σ^2_{ToF} is given by the following relationship [20].

$$\sigma^2_{ToF} \geq \frac{c^2}{2(2\pi B)^2 \cdot SNR \cdot n} \tag{3}$$

Clock Synchronization Clock synchronization is a key aspect in every ToA system. The times of transmission and reception of wireless signals must be known using a common time base in order to deduce accurate measurements. Clock synchronization is of particular importance in one-way ToA methods. Two-way methods exhibit an advantage over the one-way method since each node operates its own clock, hence its own timing system. Nevertheless, in order to extract the ToF value in a two-way ranging method, the delay time in the replying node as well as the offset between the node clocks must be approximated and then taken into account in the calculation of the ToF value.

Multipath Channel Effects Multipath propagation results in significant measurements errors in ToF systems. Multipath interference typically occurs, because the transmitted signal bounces off objects in the environment, and then adds to the LoS signal. Consequently, the LoS signal can be severely attenuated which may result in the signal being incorrectly received or lost completely. The error caused by multipath interference is difficult to be quantified as it depends upon the deployment environment.

Timing Uncertainties Apart from the sources of ranging error that were analysed previously a number of additional uncertainties may add non-deterministic delays that will result in distorted timing of the two-way round trip timing value. A thorough analysis of these uncertainties is performed by Maróti *et. al* [5] in their work on synchronization techniques. One must also consider that an additional factor of uncertainty will be the drift over time that the clock oscillator on the embedded node will demonstrate. The output frequency of the node's clock is susceptible to drift and is affected by the surrounding temperature and the node's supply voltage. It is therefore, not uncommon to observe different latencies even on the same hardware. Additional timing uncertainties may incur from the node's radio operation during the submission and reception of packets. These uncertainties are influenced by factors such as the message length, the interrupt handling and channel availability. It is imperative to ensure that the effect of these errors will remain constant as possible in the implementation of the proposed ToF system in order to avoid erroneous timing of the two-way message transmission that will result in diminishing ranging accuracy.

Due to the previously mentioned reasons, we expect the ToF values to vary for a set distance. During the calibration stage the additional delays introduced by these

factors must be sufficiently captured in order to be excluded from the ToF values. To achieve this, the combined delays which are introduced by these factors must remain as constant as possible during any experimental set-up. By oversampling the ToF values sufficiently the errors that are associate to the timing uncertainties are averaged out and do not affect the mean calculated averaged measurements given that the calibration values is removed.

4 Implementation

The Texas Instruments (T.I.) EZ430-RF2500 is a complete wireless development platform which combines the MSP430 microcontroller (MCU) and the CC2500 low-power radio module. The EZ430-RF2500 target board connects to a standard USB port for programming, debugging and communications purposes. The MCU is a 16-bit microcontroller with a clock speed up to 16MHz. It employs 32kB of flash memory and 1 kB of RAM. The MCU contains the following clock sources. A low-power 12KHz crystal oscillator (VLO) and a more accurate and energy demanding digital controlled oscillator(DCO) which can be set to a range of frequencies (1-16Mhz). The DCO operates on factory calibrated settings that demonstrate improved tolerance against temperature and voltage supply compared to previous versions of the MSP430 family of microcontrollers. Two timers/counters (named Timer A (16bit) and Timer B (variable bit-length)) are present and can be linked to any of the available clock sources. The timers have multiple capture/compare registers that are triggered via interrupts [21].

The CC2500 is a low-cost radio transceiver operating in the 2.4GHz RF band, designed for low-power embedded applications. Various modulation formats (OOK, 2-FSK, MSK) and data rates (2.4 - 500 kBaud) are supported. The configuration of CC2500 is done by programming 8-bit registers. Three registers are associated to general purpose output digital pins (GDO0-2) that can be used in various ways. The CC2500 radio does not directly support the IEEE 802.15.4 frame format. It uses a proprietary format, similar to the one described in the 802.15.4 protocol. The CC2500 consists of a variable length preamble sequence (PRE), a synchronization word (SYNC WORD), a length byte (LEN), an address byte (ADD), the data payload (PAY) and finally an optional two-byte cycle redundancy check field (CRC). The packet's maximum length is 256 bytes [22]. For the purposes of the proposed ranging system the following configuration settings were made for the CC2500 transceiver. Two datarate settings were used at 250kbps and at 500kbps. The transmission power was set to the highest value possible, that is +1dBm. The modulation used is minimum-shift keying (MSK), the preamble length was set to 2 bytes and the SYNC WORD to 4 bytes. Finally SYNC WORD detection was set to 30/32 bits.

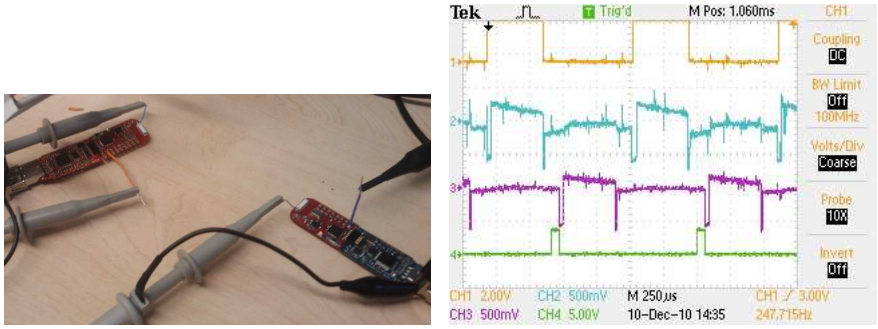
To achieve the maximum possible resolution in timing the two-way ToF value, Timer A is set to continuously count-up mode and is sourced to the DCO which is set at the maximum possible clock frequency at 16 MHz. In order to capture the ToF a GDO pin is configured to change state to "high" whenever a SYNC WORD is transmitted or received. The GDO pin returns in low "state" when the entire packet is transmitted/received. In the developed software, the GDO pin is programmed to trigger an interrupt in the event that it changes state from low-to-high. Using that interrupt, Timer

A resets whenever a SYNC WORD of a ranging message is transmitted and its value, which correspond to the two-way ToF, is captured directly from the hardware register only when a SYNC WORD is received (assuming that the incoming message is transmitted from the other device that takes place in the ranging procedure) through the same interrupt routine. A binary variable acts as a lock in order to avoid unwanted capturing of the timer's value. This method avoids the need for sampling the pin with a predefined rate, since the GDO pin itself triggers the interrupt and offers better resolution.

As mentioned earlier, the two-way ToF ranging is performed between a pair of EZ430-RF2500 devices programmed independently with different software. One of them is termed as the *requester* and the other one as the *responder*. The *requester* is the device that initiates the sequence in order for the two devices to engage in exchanging the necessary ranging messages. Practically, the *requester* device controls the initiation and termination of the ranging process. The software that we developed was designed with the following in mind. Both the *requester* as well as the *responder* code must be as simple as possible. No additional interrupts or unnecessary operation should intervene during the transmission of the ranging packets. The packets to be sent, should be in terms of size, as minimum as possible to eliminate any delays on the MCU and radio load. Our major goal is to maintain a constant delay primarily in the *responder* node during the relay of the ranging packets. Of all the sources of delay mentioned analyzed by Maróti *et. al* we try to keep the propagation delay as the primary source of variability in the timing of the two-way ToF value. In conclusion, the developed software targeted at maintaining the hardware delays as constant as possible.

Additional precautions were taken to minimize the effect of uncertainty sources during a single two-way transaction. As pointed out in [5], various factors affect the uncertainties in a message transmission. Through our implementation we tried to maintain these uncertainties as constant as possible. Constant packet length was used to avoid varying transmission/reception times. The clear channel assessment option was not used as we assumed that there was no contention in accessing the channel during the experiments. An important source of delay that we had to tackle, is the amount of time the *responder* needs to acknowledge a correct ranging signal and reply accordingly. To guarantee a constant response time on the *responder's* side, we used a minimal static code routine specifically for this application. All other interrupts were disabled apart from the one associated to message detection. To evaluate the *responder's* reply delay, we used the same 16MHz clock to capture the time from the moment a packet is detected at the *responder* until the reply message is transmitted back. This delay, which includes the $9.6\mu s$ that is required for the transceiver to change state from Rx to Tx, was found to be constant during the exchange of ranging signals. Nevertheless one of the latencies that we were not able to address pertains to the interrupt handling. In essence, we assume that the moment an interrupt flag is raised, from the radio to signal the reception of a ranging packet, the MCU starts responding to that interrupt accordingly. However in reality there might be a sub-clock delay between the signalling of the interrupt by the radio and the MCU's response, due to the fact that the two components operate on different clocks. An approach that could mitigate these effects is to drive both the MCU and Radio from the same clock source. To evaluate the delays associated with the timing between the nodes, the code on the *requester* node was altered to

set a pin high immediately after the Send Packet command was strobed to the CC2500 Radio, and the code on the *responder* was altered to set a pin "high" immediately when a packet was received. Two small connections where then soldered to the transmitting and receiving antennas of the devices, and a Teltronix TDS2014 Four Channel Oscilloscope was then connected to the transmitting and receiving nodes. This is visualised in Figure 3(a).



(a) (b)

Fig. 3: Investigation of the timing uncertainties

In Figure 3(b), Channel 1 and 2 of the Oscilloscope represent the MCU pin set "high" immediately after the transmit packet command was strobed; and the signal transmitted on the Antenna respectively. Channel 3 and 4 of the Oscilloscope represent the *responder's* antenna signal and the pin set high on successful reception of a packet. From the timing analysis it can be seen that the transmit to receive signal on the microcontroller takes 488μs which corresponds to 7708 counts of an accurate 16MHz clock. This means that our timing values on the *requester* node correspond well to the total time measured by the oscilloscope. We thus assume that the radio operation does not add any significant uncertainty to our measurements and the timing values distrbution is associated to the phase offset and clock drift (see section 5.2).

To begin with, in the *requester* device a slow clock (12 KHz) sourced at Timer B, triggers the initiation of the entire process. The slow clock is set to have a period which is longer than the time that is required to complete a ranging operation, meaning the exchange of the nominal number of ranging packets between the two nodes and the extraction of the average time. When Timer B fires, the *requester* device sends a "request to send" packet and waits for the *responder* to reply . This procedure is repeated twice to ensure that the communication link between requester-responder is established successfully. Following, the requester begins the transmission of the first ranging packet (a simple packet with minimum payload) and also resets the value of the 16 MHz timer as explained previously (after the transmission of the SYNC WORD). Immediately after the transmission is completed, the requester switches its status to receiver and waits for a return packet from the *responder*. Upon, a successful reception of a ranging packet by the *responder*, the *responder* device checks to verify that the received packet is a

correct ranging packet and then (while also swaps status from receiver to transmitter) transmits back a ranging packet at the *requester*.

On reception of a ranging packet at the *requester* following previous transmission of a ranging packet, the GDO pin triggers an interrupt (when the SYNC WORD of the incoming packet is correctly detected) which captures Timer's A value which corresponds to the two-way ToF and the additional delays. This implementation with the use of an interrupt will yield better resolution than sampling the GDO pin with a constant sampling rate as in [17]. When the full packet is received, it is checked for correctness and if it is found to be correct the captured value is stored. The ranging transaction counter is incremented and the next cycle of ranging transmissions begins. This two-way packet exchange process is repeated until the nominal ranging transactions number is reached. The *requester* device then enters the calculation phase. In the event that a false packet has triggered the interrupt the captured value is considered erroneous and disregarded. The calculation phase was described in the previous section and pertains to the extraction of the ToF value. With this method the ToF averaged value is refined from all the values that might be erroneous. After the final ToF estimate is produced, the program resets all the variables and waits for Timer B to fire the next time in order for the same procedure to be repeated.

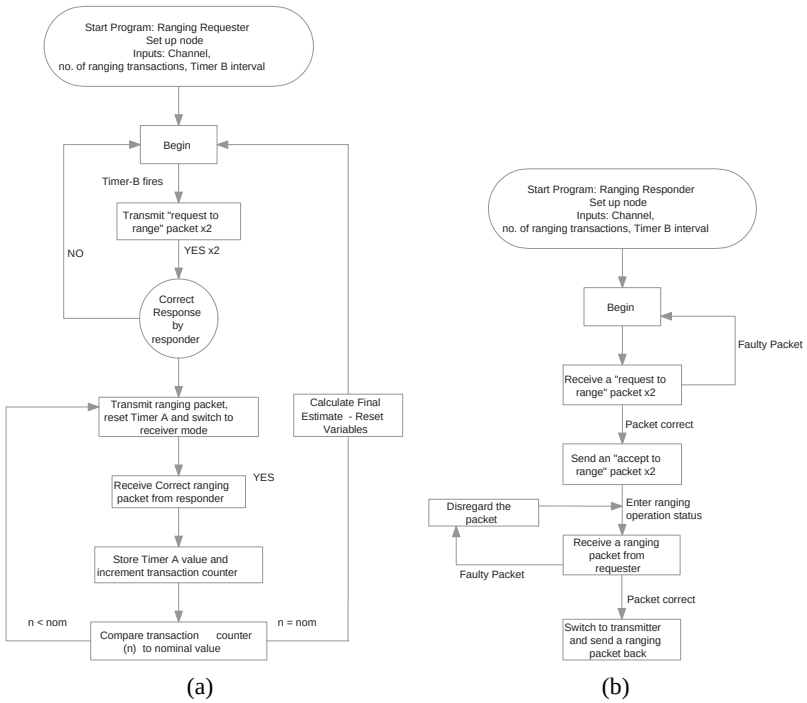


Fig. 4: Flow Diagrams of the *requester* and *responder* software

5 Deployment and Results

The two-way ToF method was tested on field experiments in order to evaluate the ranging precision and overall performance of the method. The experimental setup consisted of a pair of EZ430-RF2500 wireless nodes programmed with the *requester* and *responder* code respectively. The ideal environment for this type of experiment is an obstacle free area with good line-of-sight (LoS) for the two nodes. In addition, the interference from other wireless systems must be as low as possible. Since the CC2500 radio transceiver operates on the 2.4GHz band, it is expected that a number of other wireless networks, like WLAN, will cause significant interference if the deployment takes place in areas where such networks are present. Experiments were carried out on three different locations.

The first site (Location 1) is a level grass field at the University of Southampton campus where surrounding buildings could be a reason for multipath propagation and a number of WLAN university networks might cause interference. In this site the maximum communication range between the two nodes was limited due to space restrictions to 42m in LoS. In the second site (Location 2), nodes were deployed on a grass field with no obstacles being close to the experimental set-up. The maximum range between the two nodes that allowed the ranging system to run adequately was 70m in good LoS conditions. A number of experiments took place indoors in a narrow building corridor at the University of Southampton, School of Electronics and Computer Science (Location 3). The hallway is 42m long and had a maximum width of approximately 2m and minimum of 1.7m. In such an environment distortions in the measurements are expected due to multipath effects.

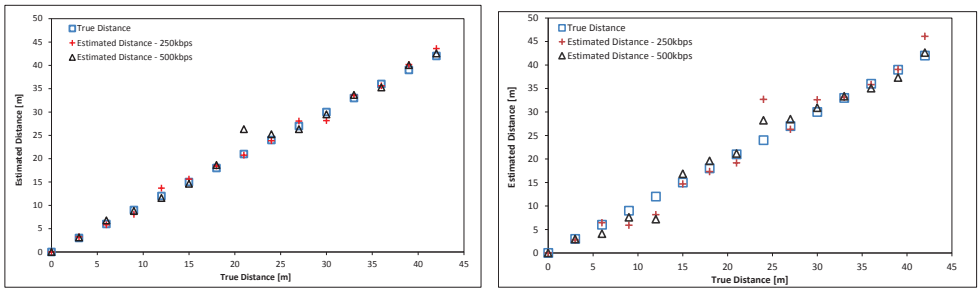
5.1 Experimental Setup

The EZ430-RF2500 devices were strapped on two wooden chairs to avoid the signal bouncing off the ground. The elevation was 90 cm off the ground. Both nodes were powered on from laptops (using the USB dongles) to ensure that they operated with full power supply. The laptop on the *requester* was also used in order to log the ranging data via its USB port. It must be clarified at this point, that the two laptops did not participate in any way in the extraction or calculation of the range between the nodes. Their only purpose was to log the results from the nodes. The transmission power of the CC2500 radio was set at the maximum possible value of +1dBm. Two datarate settings were used for the node's radio in these experiments at 250kbps and at 500kbps.

Due to the EZ430-RF2500 design, the antenna orientation plays a significant role on the maximum communication range. We concluded that the best antenna orientation was with the two antennas facing each other and being slightly inclined at an angle from the vertical position, towards the ground. Of the two nodes the calculation *responder* was positioned at the beginning of the experiment, while the *requester* was moved to the various positions. Ranging data were collected from the *requester* node in steps of 3m until the maximum communication range where the experiment was adequately running was reached. A tape measure was used as reference and in order to measure the "true" distance between the two nodes. Initially the reference two-way ToF was estimated by placing the two nodes at a minimum distance ($< 0.3m$) and averaging 100 two-way

transactions. In these experiments 1000 two-way transactions were used to estimate the distance between the two nodes. The calculation phase was executed every 100 transactions, thus 10 times in every location to reach the nominal 1000 values. The *requester* nodes was then moved to the next position. The metric used to evaluate the system's accuracy is mainly the RMS error which is defined as follows. Assuming we estimate n positions: $d_{rms} = \sqrt{\frac{1}{n}(\mathbf{d}_{real} - \mathbf{d}_{esti})^2}$. At this point, it must be highlighted that within the purposes of this work we focused on the point-to-point range between two embedded nodes only. If multiple pair of nodes are to be engaged in ranging, the calibration stage must be executed for each individual pair of ranging nodes.

Results from two different days of experiments and for both datarate values are provided for Location 1 and Location 3. In Location 2 only the 250kbps was used as we tried to reach the maximum communication range and the slowest datarate facilitated our attempt. The collective results are illustrated in Figures 5 - 6 and in Table 1.



(a) (b)

Fig. 5: Ranging results from experiments in Location 1-(a) and Location 3-(b)

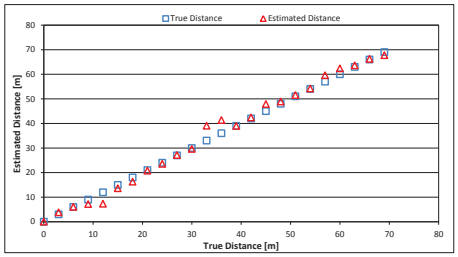


Fig. 6: Ranging results from Location 2

Ranging Results			
Location	Datarate	RMS error	Maximum Error
Location 1	250kbps	0.75m	1.79m
	250kbps	0.94m	1.84m
	500kbps	1.51m	5.32m
Location 2	250kbps	2.23m	6m
Location 3	250kbps	2.51m	5.32m
	500kbps	1.99m	4.82m

Table 1: Results from experiments for the proposed ToF method

5.2 Performance Analysis

First of all, the timer that was used in the timing process is a 16MHz timer (maximum allowed value for the MCU). This value provides a resolution of $1/16MHz \times c = 18.75m$ In section 3.1 the CRB for a two-way ToF ranging method was formulated. At 250kbps the CC2500 transceiver occupies 540KHz of bandwidth while at 500kbps 812KHz. Considering the radio setting (output power +1dBm) and a typical environment where our experiments are conducted, a -5db SNR is an expected value. Hence from Equation 3 the lower bound of the variance of the proposed system, given that 1000 measurements are used, is $\sigma^2_{ToF} = 137.3ns$ for the 250kbps and $60.7ns$ for the 500kbps respectively. These values correspond to a minimum ranging error standard deviation of 3.5159m and 2.33m for each datarate respectively (calculated from $\sigma_{ToF} \cdot c$). It must be noted that the -5db SNR is a typical value and in general the SNR varies in different deployments.

To get a notion of the way the clock on the MCU variates over time we proceed to the following experiment. To measure the drift in clock frequency, we used a Hameg HM8123 frequency counter connected to a 10MHz SRS FS725 Rubidium Frequency Standard clock reference, and measured the clock frequency approximately every second over a period of 3 hours under room temperature and constant power supply. The HM8123 gating time was set to 100ms. We recorded the frequency from the HM8123 via a laptop's USB port. The results reveal that the DCO clock frequency is normally distributed with a standard deviation of 1.63KHz. The clock's accuracy is therefore in the area of 1% and the drift exhibits a standard deviation of 0.01% around the mean value. Due to this behavior, an additional error of around 17cm per clock cycle will be inserted because of the clock's instability. This frequency distribution yields a distribution of the time values similar as the one illustrated in Figure8.

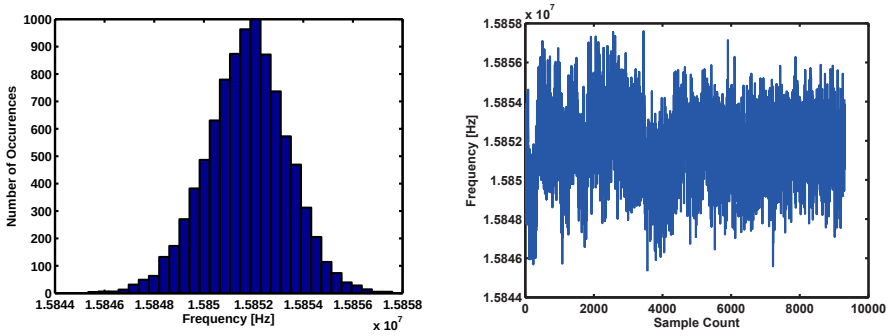


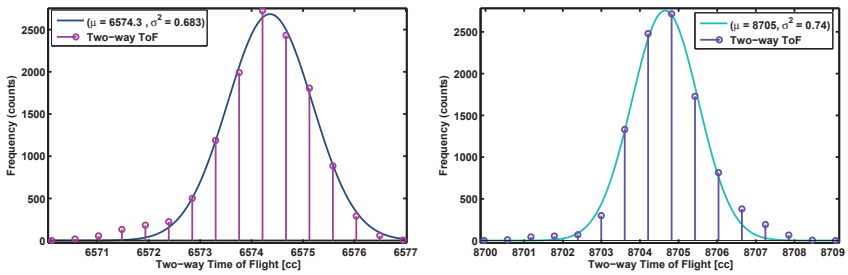
Fig. 7: Investigation of the 16Mhz clock inaccuracy. Frequency Histogram (a); Frequency vs Time (b)

As stated previously the node performed the necessary calculations whenever 100 two-way transactions were completed. Part of the process is the calculation of the standard deviation for these 100 transaction in order to exclude the timing values that fall

outside the single deviant boundary. This procedure was repeated for 10 times in order to reach 1000 transactions. From all the experiments carried out the standard deviation of the timing values before averaging, was in the range of $1.4cc - 1.8cc$ for the 500kbps setting and $2.4cc - 3cc$ for the 250kbps. After averaging the 100 values the deviation was reduced to $0.4cc - 0.8cc$ for both the 500kbps and the 250kbps. Assuming a value of $0.6cc$ and dividing this by two we get $\sigma_{ToF} = 0.3cc$.

This value is expressed in clock cycles (cc) and a single clock cycle of the 16MHz timer is $(1/16MHz = 62.5ns)$. Thus the standard deviation of the proposed system can be approximated as $\sigma_{ToF} = 18.75ns$. This translates to a maximum standard deviation of 5.62m. To sum up, given the theoretical derived lower bound, we presented a ToF ranging technique which exhibits a maximum standard deviation at the same order of magnitude as the theoretical calculated using the CRB lower bound.

To also verify the distribution of the measurements that the proposed ToF ranging system yields, an experiment is designed where two nodes are placed in a short distance ($\tilde{2}m$) and a vast number of ToF estimates is logged over a period of time. This experiment was executed with both datarate values. Approximately 10000 two-way ToF values were logged in each execution. The values are plotted according to 15 equally spaced bins. From Figure 8 it is clear that the values can be considered as normally distributed and exhibit a standard deviation which is very close to the one observed in the previous experiments.



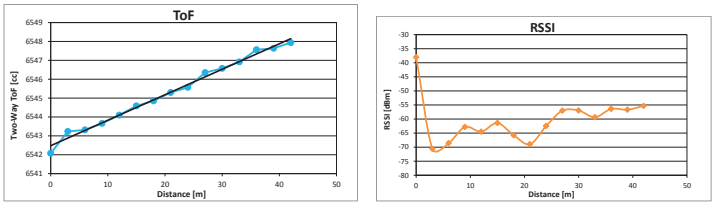
(a) Histogram of 500kbps datarate (b) Histogram of 250kbps datarate

Fig. 8: Timing Histogram of 10000 two-way values

5.3 Comparison between ToF and RSSI

This section provides a comparison between ToF and RSSI, two of the most well established techniques for estimating the range between two nodes in RF systems. The CC2500 radio offers the option of capturing the RSSI value of an incoming packet upon reception. That option was used in one of the outdoor experiments and the RSSI value of the reply ToF messages sent by the“responder” to the “requester” was captured. The calculation of the mean RSSI value took place in a similar way like the ToF by averaging 1000 RSSI values. The RSSI values are then converted to dBm. Figure 9 illustrates the ToF and RSSI values against the distance of the two nodes. Typically

the RSSI values decay proportionally to d^{-n} where n is the path-loss exponent, normally between and four [23]. From Figure 9, it is clear that the this relationship is not confirmed and thus the equivalent distance estimation will be faulty. On the other hand the proposed ToF system, demonstrates the expected linearity. Although the approach that is followed for the RSSI does not take into account various factors which cause the attenuation of the signal, like shadowing effects, we provide it here as a comparison to the proposed ToF method.



(a) Distance vs ToF (b) Distance vs RSSI

Fig. 9: ToF vs RSSI

6 Conclusions

In this paper, we presented a two-way RF-ToF method for ranging estimation in wireless embedded nodes. The multiple two-way transaction approach, achieves two major objectives. Firstly, it does not require the difficult task of synchronization among the participating nodes and secondly, amends the lack of fine resolution due to the low-frequency clocks that most WSNs are equipped with. In our opinion the calibration method we follow is effective since it caters for a number of delays difficult to be measured by using only a clock at the "reply" device. Sub-clock resolution is achieved by averaging the obtained time values. In addition, a simple yet effective procedure disposes any erroneous values that are present in the set of measurements. Experimental results demonstrate an average accuracy of about 1m in outdoors deployments and about 2.25m indoors. Accuracy can be further reduced if additional two-way measurements are used. The proposed ranging system is implemented on COTS hardware. It is therefore our belief that it can be implemented on different hardware platforms. Unlike other ToF ranging methods, our system does not require any additional hardware. The entire procedure of obtaining and filtering the values as well as the calculation of the final ToF is completed on the nodes.

One future direction of this work is to employ the proposed ranging method in scenarios that include mobile nodes. Mobility poses strict latency demands, and this system was designed with this in mind. Although, we have not experimented with tracking of mobile targets yet, we plan this to be one of the application domains of the work presented in this paper.

Acknowledgements. The authors wish to thank Kay Römer for his valuable comments during the review of this paper and the anonymous reviewers for their constructive feedback.

References

1. Patwari, N., Ash, J., Kyperountas, S., Hero, A.O., I., Moses, R., Correal, N.: Locating the nodes: cooperative localization in wireless sensor networks. IEEE Signal Process. Mag. **22**(4) (Jul 2005) 54 – 69
2. Hightower, J., Borriello, G.: Location systems for ubiquitous computing. IEEE Computer **34**(8) (Aug 2001) 57 –66
3. Bahl, P., Padmanabhan, V.N.: Radar: an in-building rf-based user location and tracking system. In: IEEE INFOCOM. (Mar 2000)
4. Sivrikaya, F., Yener, B.: Time synchronization in sensor networks: a survey. IEEE Network **18**(4) (Jul 2004) 45 – 50
5. Maróti, M., Kusy, B., Simon, G., Lédeczi, A.: The flooding time synchronization protocol. In: ACM SenSys. (Nov 2004)
6. McCrady, D., Doyle, L., Forstrom, H., Dempsey, T., Martorana, M.: Mobile ranging using low-accuracy clocks. IEEE Trans. Microw. Theory Techn. **48**(6) (Jun 2000) 951 –958
7. Patwari, N., Hero, A.O., I., Perkins, M., Correal, N., O'Dea, R.: Relative location estimation in wireless sensor networks. IEEE Trans. Signal. Process. **51**(8) (Aug 2003) 2137 – 2148
8. Chung, W.C., Ha, D.: An accurate ultra wideband (uwb) ranging for precision asset location. In: IEEE Conference Ultra Wideband Systems and Technologies. (Nov 2003)
9. Lee, J.Y., Scholtz, R.: Ranging in a dense multipath environment using an uwb radio link. IEEE J Sel. Areas Commun. **20**(9) (Dec. 2002) 1677 – 1683
10. Fontana, R., Gunderson, S.: Ultra-wideband precision asset location system. In: IEEE Conference on Ultra Wideband Systems and Technologies. (May 2002)
11. Lanzisera, S., Lin, D., Pister, K.: Rf time of flight ranging for wireless sensor network localization. In: Intl. Workshop on Intelligent Solutions in Embedded Systems. (Jun 2006)
12. Karalar, T., Rabaey, J.: An rf tof based ranging implementation for sensor networks. In: IEEE Intl. Conference in Communications. (Jun 2006)
13. Sallai, J., Balogh, G., Maróti, M., Lédeczi, Á., Kusy, B.: Acoustic ranging in resource-constrained sensor networks. In: Intl. Conference on Wireless Networks. (Jun 2004)
14. Whitehouse, K., Culler, D.: Calibration as parameter estimation in sensor networks. In: 1st ACM Workshop on Wireless Sensor Networks and Applications. (Sep 2002)
15. Priyantha, N.B., Chakraborty, A., Balakrishnan, H.: The cricket location-support system. In: Sixth Intl. Conference on Computing and Networking (MobiCom). (Aug 2000)
16. Maróti, M., Völgyesi, P., Dóra, S., Kusý, B., Nádas, A., Lédeczi, A., Balogh, G., Molnár, K.: Radio interferometric geolocation. In: ACM SenSys. (Nov 2005)
17. Thorbjornsen, B., White, N., Brown, A., Reeve, J.: Radio frequency (rf) time-of-flight ranging for wireless sensor networks. Measurement Science and Technology **21**(3) (Mar 2010) 1–12
18. Mazomenos, E., Reeve, J., White, N.: Tracking manoeuvring mobile nodes in wireless sensor networks. In: 7th IEEE Intl. Conference on Networking, Sensing and Control. (Jan 2010)
19. Gustafsson, F., Gunnarsson, F.: Mobile positioning using wireless networks: possibilities and fundamental limitations based on available wireless network measurements. IEEE Signal Process. Mag. **22**(4) (Jul 2005) 41–53
20. Stüber, G.L.: Principles of Mobile Communication (2nd ed.). Kluwer Academic Publishers, Norwell, MA, USA (2001)
21. Texas Instruments: Ez430-rf2500 development tool user guide.
Available online: http://focus.ti.com/lit/ug/slau227e/slau227e.pdf (2008)
22. Texas Instruments: Cc2500 2.4 ghz low-cost low-power transceiver datasheet.
Available online: http://focus.ti.com/lit/ds/symlink/cc2500.pdf (2009)
23. Srinivasan, K., Levis, P.: Rssi is under appreciated. In: 3rd Workshop on Embedded Networked Systems (EmNets). (May 2006)