WiFi Localization Based on IEEE 802.11 RTS/CTS Mechanism

Zhe Cui
Department of Electrical and Computer Engineering
University of Maryland, College Park
College Park, MD 20742, USA
zcui@umd.edu

Ashok Agrawala
Department of Computer Science
University of Maryland, College Park
College Park, MD 20742, USA
agrawala@cs.umd.edu

ABSTRACT

Location Based Services are providing one of the fastest growing market segments today. While the most common technique for location determination is GPS, several alternative approaches have been proposed for Wi-Fi environments, based on time of flight, signal strength, etc. Time based techniques not only require accurate timestamping mechanisms, but also precise and synchronized clocks, which is quite difficult and expensive in industry. On the other hand, signal strength based methods need a lot of ground truth data. These method also require time consuming work and efforts before the system comes into use. In considerations of costs and time consumption, we present in this paper an approach for determining the location of a general Wi-Fi device combining RTS/CTS and TDoA techniques. The proposed model is deployable in various environments and contains two different methods, with clock mapping functions and asynchronized clocks. We also explain limitations of current round trip time (RTT) based RTS/CTS systems. Extensive experiments have been conducted and demonstrated how an accuracy of about one foot can be obtained and also the assumption of RTT measurements have been verified.

Categories and Subject Descriptors

C.3 [**Special-Purpose and Application-Based Systems**]: Real-time and embedded systems

General Terms

Design, Algorithms, Measurement.

Keywords

Location Determination, RTS/CTS, Time Difference of Arrival, Round-Trip-Time Measurements

1. INTRODUCTION

One of the fastest growing market segments for computer and smart-phone based application are location based services. Knowing the place of a device can be used for a variety of purposes including navigation of a car on the road, locally relevant advertising, social networking, geo-tagging of pictures, asset tracking, shopping mall guidance, etc. Additional applications continuously appear as new technology gives higher accuracy, flexibility and compatibility. Even though nowdays, GPS is the most commonly used technique for Location Determination and becoming more popular with steadily decreasing cost of this approach, there are still many instances in which GPS does not work properly. Therefore a continuing interest in non-GPS based techniques is still active.

With ever increasing availability and deployment of Wi-Fi coverage, several approaches for non-GPS based location determination have been proposed which use time of flight or signal strength measurements. In the noisy Wi-Fi environment, signal strength based approach has limitations in accuracy as well as high set-up cost as it often requires a development of signal strength fingerprinting for the area which may have to be repeated at regular intervals of time [3, 17]. Time-based techniques determine the distance by measuring time of flight of the packets transmitted between nodes [13]. With radio signal traveling at the speed of light, achieving high accuracy(below one foot) requires time measurements within 100 ps range.

In order to obtain timestamps with this degree of accuracy, it is not only required to have high resolution for timestamping, but also accurate clocks which should also be synchronized. High precision of synchronization across multiple clocks in distributed environments is recognized to be a rather difficult problem and costs much. While slight drift in one clock may not impact measurements significantly, when multiple clocks have drifts, localization results can be dominated by the clock characteristics.

The goal of our work is to develop techniques which permit localization of ordinary Wi-Fi enabled devices including smart phones and Access Points without the need for clock characteristics. With this kind of technique, it is easy to estimate location among different independent clocks.

Several researchers have proposed time-based location methods that do not require perfect synchronization among different clocks. Youssef [23] presented a distributed algorithm which determines propagation delays among a set of n nodes.

MOBIQUITOUS 2015, July 22-24, Coimbra, Portugal

DOI 10.4108/eai.22-7-2015.2260052

It deals with general crystal oscillator clocks which does not require an infrastructure of accurate clocks. Mah [19] improved precision of timestamps using off-the-shelf wireless network cards. Generally, synchronization can be achieved relatively to a master clock or the average of clocks. Network Time Protocol [21] and IEEE 1588 [18] physically adjust offsets and frequencies to a master clock. Consensus clock synchronization [19] and joint distributed synchronization [7] adjust local clock to an average.

There are also some papers that have focused on RTS/CTS based localization. Most of them measured Round-Trip-Time (RTT) of RTS/CTS in order to determine the pairwise propagation delay between sending node and Access Point. Hoene [16] presented a software-based trilateration algorithm with the measurement of RTT of a sequence of wireless MAC packets (e.g., RTS/CTS, DATA/ACK, etc). It overcomes the low clock resolution constraints of off-the-shelf IEEE 802.11 cards and achieves an accuracy of four meters. Prieto and Bahillo [2,22] added a low-cost hardware to the existing system and applied statistical linear regression estimates to ToA computation. An external time counter for measuring RTT is used and in line-of-sight (LOS) scenarios it can achieve one meter accuracy. All of the above mentioned methods have utilized RTT measurements for ToA or TDoA computation, in which high accuracy cannot be achieved due to uncertainty of characteristics on wireless devices. In addition, complete scheme including RTS, CTS, DATA and ACK has been used, which increases wireless network traffic and costs much energy.

The steps which convert ToA and TDoA measurements to location have been studied as two optimization problems for a long time, i.e., trilateration [20] and hyperbolic location [6, 11]. These two types of determination are bases of almost all modern time-based localization systems, in which trilateration uses ToA and hyperbolic location uses TDoA measurements. Also, many efficient algorithms that solve optimization problems have been proposed, such as iterative gradient descent method for least squares [5]. One important extension is stated in [4] and [8] for sensor network localization.

In this paper, two TDoA based methods for localization in IEEE 802.11 wireless networks are presented. These two methods use RTS/CTS handshake without RTT measurements. With the help of three customized digital transceivers (which are also called SMart Integrated Localisation Extension (SMiLE board)) [10] from Austrian Academy of Sciences, one can locate arbitrary AP that is within transmitting range of the boards as long as we know the MAC address of the AP. Specifically, we keep transmitting RTS packets from one SMiLE board to AP and get CTS reponded by AP. At the same time, receiving timestamps of RTS and CTS at the second and third boards are recorded. Based on only receiving time differences, we can compute the TDoA difference for AP and listening nodes. As stated above, DATA packets have lengths much larger than RTS/CTS. Thus it costs more energy and time to send but only a small part of the packets is useful for localization, i.e., timestamps. On the other hand, RTS/CTS mechanism reduces frame collisions won't cause a lot of traffic load increases. So it is a better idea that we only use RTS/CTS packets, which are shorter in length and can be sent automatically.

The remainder of this paper is as follows. New time-based location system design using only RTS/CTS is described in Section II, where mathematical formulations and assumptions will also be given. It turns out that in one method we can neglect the effects of drift ratio in some sense which will be shown in experiments, while in the other method we do not need scheduling of sending RTS. Current use of RTT measurements are explained in Section III. Then we implement the theoretical model described. Experimental results are discussed in Section V, where RTT verifications are described first, as well as statistical distributions and explanations. Then location estimation performances for both indoor and outdoor are explained while error distributions are also discussed. Finally, we conclude our work and give an overview of current and future steps in related research.

2. OUR APPROACH

Originally, RTS/CTS is an optional mechanism used to reduce frame collisions introduced by hidden node problem, as well as virtual carrier sensing in CSMA/CA. Our approach is to make use of the RTS/CTS scheme to build up a TDoA based localization model which relies on timestamping exchanging wireless RTS/CTS packets. In this section, we first describe the model analytically and then explain the mathematical formulations of the system, which verifies the feasibility of this model.

2.1 Model Description

As discussed earlier, we aim to obtain TDoA values for localization. This requires one packets received by multiple nodes that can be timestamped. The infrastructure setup consists of at least three anchor nodes and one unknown node, all of which are within transmitting range of each other in the same coordinate system. Generally in ideal WiFi environment, this range is at most 40 to 50 meters. Specifically, anchor nodes are in the known locations and unknown node(UN) can be any wireless devices, such as APs, Smartphones. UN can respond to RTS automatically if its status is idle according to 802.11 protocol. Packets exchanging scheme is stated in details below.

In the beginning, one of the anchor nodes sends RTS packets at a certain time of interval and gets CTS back from UN, and all other anchor nodes are in listening mode, i.e, they both receive RTS and CTS from that anchor and UN. In a single round of exchanging RTS/CTS messages, there are $2n$ timestamps on the anchor side, where n is the number of anchors. One anchor has RTS sending and CTS receiving timestamps, and each of the other anchor nodes has timestamps received for both RTS and CTS. The explicit 3-node example illustration is shown in Fig.1.

Based on these timestamps, as well as pairwise distances between anchor nodes, TDoA values can be computed related to UN. There are two slightly different methods that we aim to propose according to the mechanism stated above. One method is based on one single round of RTS/CTS and the other is related to each anchor taking turns sending RTS/CTS. For ease of notation and explanation, we summarize notations in Table.1. In the next, we will look for more details in three anchor node case, which is the small-

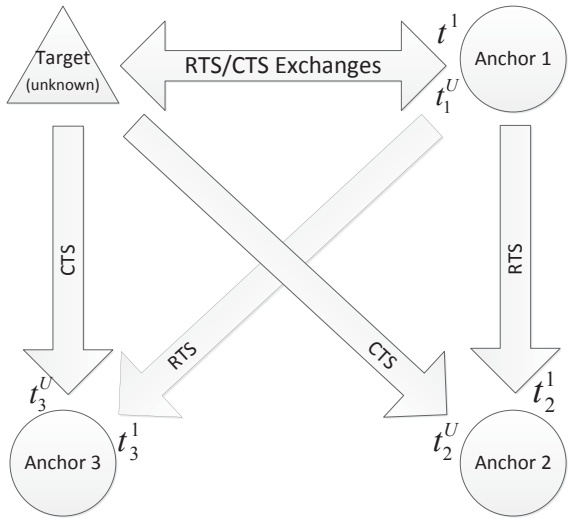


Figure 1: 3-node RTS/CTS messaging example

est number of anchors for localization if we do not use RTT measurements.

Definition	Notation	Remarks
global clock	t	same among device
local clock	τ	varies across devices
drift ratio	β	-
offset	α	-
ToA between a,b	$d(a,b)$	or $ToA(a,b)$
TDoA between a&b,c	-	$TDoA(a,b,c)$

Table 1: Notations Representation

2.2 Mathematical Formulations

In this part, mathematical formulations are derived and explained separately for two methods. We first define some common representations in ease of understanding: Unknown Node(UN) is any wireless device we aim to locate and anchors are devices that can timestamp and their locations are known to us. t^1 through t_3^U in figure 1 are defined as sending or receiving time. And τ^1 through τ_3^U are corresponding timestamps read from local clocks. Specifically, superscript stands for sending node and subscript is receiving node. U represents UN. β stands for clock drift and α is offset.

2.2.1 Anchors Taking Turns Sending RTS

In this scheme all anchors send RTS and get CTS back consecutively. This method provides more timestamps and thus does not necessarily require synchronization across multiple clocks.

Let's first recall general linear clock model with drifts and offsets, which is stated in Pinpoint [23] system. Here we use the representation that global time is t, then local clock reading related to drift rate and offset is

$$\tau = \beta(t + \alpha) \tag{1}$$

Note that for a typical crystal oscillator clock, value for clock drift is in the order of 10^{-7}. And t^1 is RTS sending time from anchor 1 and t^U is CTS sending time from UN. If three anchors take turns sending RTS, we get $6 \times 3 = 18$ timestamps. Assume $D(i,j)$ is pairwise distance between node i and j, and c is speed of light in the air, we have

$$d(i,j) = \frac{D(i,j)}{c} \tag{2}$$

Eq.(2) gives us the relationship between actual distances and measurements through packet exchanging with timestamps. This is also the foundation of many synchronization and location methods, since generally speed of light is assumed to be constant. When we get $d(i,j)$, pairwise distance is known to us. Suppose ToA values among anchor nodes are known. Apply Eq.(1) to τ^1 through τ_3^U separately and substitute different t terms:

$$\tau_2^1 = \beta_2(t^1 + d(1,2) + \alpha_2) \tag{1.1}$$

$$\tau_2^U = \beta_2(t^U + d(U,2) + \alpha_2) \tag{1.2}$$

$$\tau_3^1 = \beta_3(t^1 + d(1,3) + \alpha_3) \tag{1.3}$$

$$\tau_3^U = \beta_3(t^U + d(U,3) + \alpha_3) \tag{1.4}$$

Here $l.h.s$ are clock readings from independent clocks, and they tend to be thousands of millions ($10^9 \sim 10^{10}$) per second when nano- or sub-nanosecond readings are used. Such resolution of clock is required if we want to achieve distance measurement accuracy of one foot or lower. However, with a typical clock drift of one part in 10^{-7}, an error of 100 ns may be introduced, resulting in a distance error of about 100 feet. When we subtract Eq.(1.2) from Eq.(1.1) and Eq.(1.4) from Eq.(1.3), to get

$$\tau_2^U - \tau_2^1 = \beta_2(t^U - t^1 + d(U,2) - d(1,2)) \tag{3}$$

$$\tau_3^U - \tau_3^1 = \beta_3(t^U - t^1 + d(U,3) - d(1,3)) \tag{4}$$

From our empirical experiments with various access points, iPhones and Android smartphones, $r.h.s$ in Eq.3 and 4 without drift rate term of β_3 and β_4 are around (400 ± 1) μs. When multiply this by drift ratio (typically 1 ± 10^{-7}), error is within a few inches. So we take out drift ratio terms in the equations and make the approximation

$$\tau_2^U - \tau_2^1 \approx t^U - t^1 + d(U,2) - d(1,2) \tag{5}$$

$$\tau_3^U - \tau_3^1 \approx t^U - t^1 + d(U,3) - d(1,3) \quad (6)$$

Subtract Eq.(5) from (6) and eliminate common terms to have

$$\tau_3^U - \tau_3^1 - (\tau_2^U - \tau_2^1) \approx (d(U,3) - d(U,2)) - (d(1,3) - d(1,2)) \quad (7)$$

$l.h.s$ of Eq.(7) are timestamps that can be obtained easily from reading local clocks. And $r.h.s$ has the following expression: $TDoA(U,3,2) - TDoA(1,3,2)$. Terms in the first parenthesis of Eq.(7) can be explained as $TDoA(U,3,2)$, which stands for TDoA value between AP, 3 and 2. Similarly, second term is $TDoA(1,3,2)$. If TDoA values among anchor nodes can be either estimated through time-based method, such as parts of trilateration and hyperbolic location stated in [13], or computed from physical measurements, TDoA values of UN can be derived without difficulty.

As stated above, in this method without drift compensation, one hyperbola can be generated from RTS sent by one anchor without synchronization. That's the reason why anchors need to take turns to send RTS, which will provide three hyperbolas among 3 nodes.

2.2.2 Single Round RTS/CTS Method

While only one anchor is sending RTS instantly, we have one single round of 6 timestamps. In order to utilize only these timestamps, clocks have to be synchronized first. We aim to synchronize all anchors with respect to the one sending RTS, with the help of timestamps related to RTS, and determine TDoA with CTS timestamps. Here we use linear mapping functions described in [15]. The idea is to convey timestamps for events taking place at one node to the other node(s). It is a function between two clocks that maps timestamps from one local clock to timestamps at the other node at the same global time.

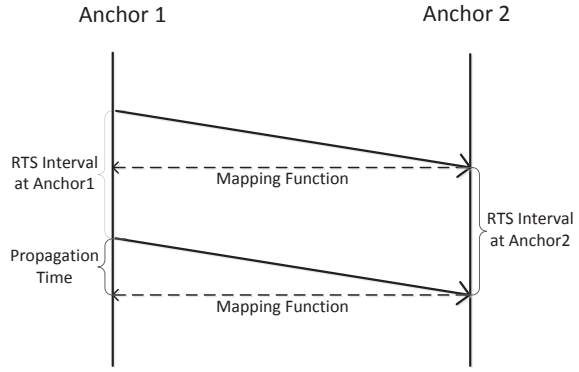


Figure 2: Synchronization Using Two Consecutive Rounds

We suppose anchor 1 is sending and synchronize anchor 2 and 3 with respect to 1. Here for ease of explanation, we take anchor 2 for example. Anchor 3 works in the same way. For ith round of RTS, we denote timestamps as $\tau^1(i)$. We use two consecutive rounds of sending and receiving timestamps to estimate relative drift ratio (Fig.2). So we have

$$\widehat{\frac{\beta_2}{\beta_1}}(i) = \frac{\tau_2^1(i+1) - \tau_2^1(i)}{\tau^1(i+1) - \tau^1(i)} \quad (8)$$

Once we have obtained relative drift, we can calculate offset difference by

$$(\alpha_1 - \frac{\beta_1}{\beta_2}\alpha_2) = \tau^1(i) - \widehat{\frac{\beta_1}{\beta_2}}(i)(\tau_2^1(i) - d(1,2)) \quad (9)$$

Here $d(1,2)$ is ToA between anchor 1 and 2 and drift ratio is determined in Eq.8. Generally, drift rate and offsets are not constant as time goes by, so we utilize two consecutive rounds of timestamps to determine drift and offset in between. CTS is sent during two RTS, and in this way, receiving time of CTS packets at anchor 2 can be mapped to anchor 1 with linear function of appropriate parameters

$$\phi_{12}(\tau_2^U) = \frac{\beta_1}{\beta_2}\tau_2^U + (\alpha_1 - \frac{\beta_1}{\beta_2}\alpha_2) \quad (10)$$

$l.h.s$ is the timestamp τ_2^U after mapped to anchor 1. We map all timestamps to anchor 1 to make them in a single clock scale. Thus CTS sent from UN and received at all anchors can be used for TDoA determination

$$TDoA(U,2,1) = \phi_{12}(\tau_2^U) - \tau_1^U \quad (11)$$

$$TDoA(U,3,1) = \phi_{13}(\tau_3^U) - \tau_1^U \quad (12)$$

While only one anchor is sending, two TDoA values are obtained and UN can be located with two hyperbolas. The main point we make here is to map timestamps from multiple anchors to one, in the sense that they are synchronized. Thus no more turns of RTS are needed.

2.2.3 Error Discussion

In the method that anchors taking turns sending RTS, assumption that drift ratio is equal to 1 has been made. Actually, drift rate fluctuates within $1 \pm 10^(-7)$ range most of the time. This assumption will give us an error of several inches in the TDoA measurements, which is reasonable. Drift rate terms can be eliminated in some sense that we differentiate TDoA values between anchor and UN.

In single round case, mapping independent clocks to one anchor makes all timestamps synchronized into one clock

scale. It frees anchors from sending RTS in turn, but every clock has its own drift and offset. Since it is not possible to get accurate global clock, we cannot get rid of the effects of drift and offset. It is interesting to us that errors caused by clock characteristics can be reduced through averaging of multiple measurements. More details will be discussed in experiments.

3. USING RTS/CTS FOR RTT MEASUREMENTS

Round-trip time (RTT) are classical measurements that have been well studied and applied tremendously in clock synchronization and location systems. Definitions of RTT is length of time it takes for a signal to go from some node A to another node B and come back. Clearly node B takes a finite time to receive the signal from A and then sends a response back to A. If both nodes timestamp sending and receiving time of the signals and clocks are synchronized to real time, RTT can be calculated easily and accurately. After knowing RTT values, we can then calculate the distance between two nodes and use such measurements for determining locations of a set of nodes. If, on the other hand, node B is not timestamping, then node A can only determine actual RTT plus "turnaround" time at node B. In IEEE 802.11 protocol, RTS/CTS mechanism may be used to estimate RTT by measuring the time from RTS sending from A to receiving of CTS at node A.

While RTT measurements make computation easier, it is not always possible that both sides can be timestamped precisely. According to the specifications of 802.11 protocol [1], a node must respond to an RTS with a CTS within SIFS (Short Inter Frame Space) which is specified to be 10 or 16 μs. When we are interested in measuring the distance with accuracies below one foot we need the time measurements with accuracy in sub nanoseconds. The variability in SIFS does not lend itself to yielding such precision. Other than that, many delays from UN side are supposed to exist, i.e., delay between receiving packets and recording clocks, delay between time-stamping and sending CTS, delay between starting to send CTS and recording clocks, etc.

In the scheme proposed here we do not rely on the time delay between RTS and CTS at one node but utilize this mechanism to get UN to send a CTS which is received at multiple other nodes. We can then utilize the Time Difference of Arrival techniques to determine the location of UN, both with and without synchronization.

4. IMPLEMENTATIONS

Our proposed RTS/CTS location system contains multiple anchor nodes and one unknown node(UN). Here for implementation, we use three customized SMiLE boards from *Oregano Systems* which are designed by researchers in Austria Academy of Sciences [9] as stated in the introduction as anchor nodes. Each of these boards contains one Altera Cyclone3 FPGA chip that acts as Central Processing Unit, tranceivers which can transmit WiFi signals in different channels within 2.4 GHz band frequency in 802.11b protocol and multiple clock sources. These boards use a 25 MHz local oscillator to generate independent clocks. The board can also timestamp ingress and egress frames at a resolution of 88.78 ps (this is the unit of one clock tick). Other experiments have been conducted on these boards and the noise term is shown to have a standard deviation of 60 ps [15]. The software used is ANSI C code based on Altera NIOSII platform, where we can define sending time interval, power level, clock sources, frequency channels, as well as managing messages exchanging schemes of the boards in the system.

In order to estimate locations using different proposed methods and characterize RTT measurements, a series of tests were carried out both inside the office building and outside. We tested RTT empirical distribution with one SMiLE board and other general APs. And for location estimation, three boards and one Cisco LinkSys AP (model WRT54GL) were used for both indoor and outdoor experiments.

5. EXPERIMENTAL RESULTS

There are two series of experiments conducted, RTS/CTS based RTT measurements and TDoA location estimation based on model in section II. We first give the configurations of the experimental setup and then discuss results for different experiments, respectively.

5.1 Configurations

Since SMiLE boards do not have MAC layer, packet formats have to be generated manually. We tested communications between anchor nodes and UN before experiments every time. Channel 6 with $freq = 2437MHz$ is used and verified to have the most responding ratio. This channel is also typically non-overlapping within 802.11b DSSS channels. RTS sending time interval was chosen to be 9 ms, which is large enough compared with RTT of single RTS/CTS round. All readings of local clocks are made after processing. Therefore, RTT measurements will contain the interval of transmission and reception. The default sending speed is 1 Mbit/s and length of standard RTS and CTS packets [1] are 20 and 14 bytes, respectively. So RTS interval is $1Mbit/s \times (20 \times 8)bits/packet = 160$ μs and CTS interval is 112 μs. Compared with the microsecond processing time, propagation delay is within 1%. Detailed structure of RTT is shown in Figure.3. So the total RTT is approximately $160 + 2 \times 112 + SIFS = 394$ μs, where SIFS is 10 μs in 802.11b protocol and we have receiving interval for RTS and both sending and receiving intervals for CTS.

In the complete RTS/CTS mechanism, four-way handshaking also includes DATA and ACK packets. In our setup only RTS/CTS is used in our experiment for the packets have fixed lengths and formats. Also time-stamping process takes less time.

5.2 RTT Measurements

We set one anchor sending RTS continuously every 9 ms whether it gets CTS from UN or not. The measurements took place along the corridor out of an office after 8:00 pm, when there was less network traffic and no movement of humans. The corridor has about 10 feet in width and 10 feet in height. When anchors received CTS, it read clocks and reported the packets along with corresponding RTS timestamps to a laptop via wire connection through a switch. Anchors and UN were put on top of 4-feet boxes to eliminate floor reflection. In Fig.4, histograms and distributions

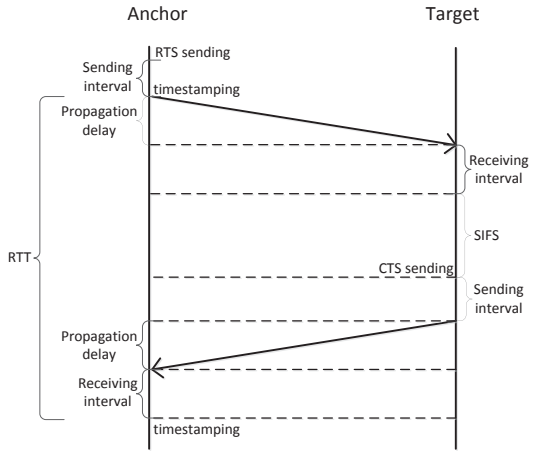
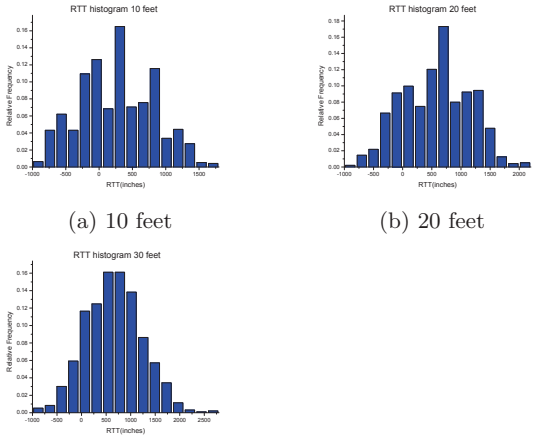


Figure 3: RTT detailed Structures

of RTT (computed from $\tau_1^U - \tau^1$) clock readings measured by designed system are shown in (a), (b) and (c) respectively, with actual distances of 10, 20 and 30 feet. The offset has been eliminated according to the explanation above. All the nodes were in Line of Sight (LOS) to each other and pairwise distances were measured by a tape. 1000 consecutive readings for each single experiment were collected. It shows how RTT in inches grew with distance increases, as similar results in [22], in which a nonparametric method was used and tested. Gaussian distribution error was also assumed in [12], which matches our experimental results.



(a) 10 feet (b) 20 feet

(c) 30 feet

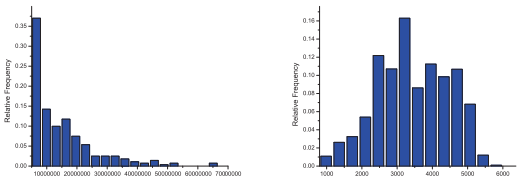
Figure 4: Round Trip Time (RTT) Histograms (inches)

The mean and standard deviation results of RTTs are given in Table 2. Here one clock tick is 88.78 ps, and the corresponding distance is approximately one inch. We compensated for transmission and reception time and all the units have been changed to inches. The first two columns show that average of RTTs are within 10 feet of true distances. Actually in 20 feet test, the estimate result suddenly jumped, which should be mainly caused by multipath effects. The last column shows us RTT measurements based on RTS/CTS mechanism are not that stable to use, with standard deviation over 40 feet. In typical IEEE 802.11 WLAN protocol, APs are not more than 50 meters(164 feet) apart, thus 50 feet deviation will affect location estimation results significantly. Also, RTT differences between 10, 20 and 30 feet have relative errors about 20% as actual distance changes. This is not surprising considering such a large variance.

RTT Actual	estimate	error	deviation
240	256	14	602
480	595	115	609
720	687	33	611

Table 2: RTT statistics comparison (inches)

Similar tests have been conducted with respect to different kinds of UNs. Fig.5(a) plots RTT of a standard Access Point, one deployment of general WLAN network in the building. We note that most of values are within 400 μs but there are also some large terms over 700 μs. These sudden jumps were caused by scheduling of physical AP, which generates several virtual APs. Specifically, the physical AP takes turns to act as various standard APs at different short time intervals. This is good for saving WLAN resources but will cause longer delays than expected in experimental measurements. Fig.5(b) shows RTT histograms of a hot spot enabled iPhone5. Compared with our own general AP, this graph appears to have similar characteristics as Cisco AP test above with no sudden jumps. It confirms our assumption and also gives us visual explanations of the limitations of RTT measurements when AP's timestamps are not known.



(a) standard AP (b)hot spot enabled phone

Figure 5: RTT histogram for standard AP and phone hot spots (inches)

As already mentioned in Section II, variances in SIFS, sending and receiving process time all contribute to the instability of RTT values. Resolutions in 802.11 WLAN techniques are in microseconds, which cannot be enough for distance estimates if we aim to achieve precision of several feet.

5.3 Location Estimation

The purpose of developing a time-based system for TDoA determination is to use it for location. Hyperbolic location techniques manage distances to survey planar coordinates of unknown positions. In our experiments, three SMiLE boards were deployed as anchors. The same Cisco Linksys AP in RTT measurement was used here as UN for location estimation. As explained in Section II, TDoA values can be

generated either through sending RTS from only one anchor or in turns by anchors.

Also, TDoA values among anchor nodes are used for location in both methods, and it is easy to measure by either making physical measurements or exchanging packets to obtain ToA values in the same way that was mentioned in [13]. Here for accuracy purposes, physical measurements were applied. In a set of experiments, three similar tests only differed in sending nodes, the reason why we manually made three independent experiments not schedule anchors taking turns sending RTS is that the packet loss ratio of RTS/CTS are much higher than normal data packets, and it always occurs that there is no CTS respond to RTS. So it is more difficult to get all the packets of a single round in scheduling scheme than only one anchor sending. Two sets of localizations for indoor and outdoor environments were conducted and results of two methods will be discussed and compared in the following part. For synchronized method, only one anchor sending data was used.

5.3.1 Outdoor

The outdoor experiments were conducted on a Saturday morning outside a building on the campus. The environment was quite clean and there were no obstacles around. In modern WLAN networks, APs were distributed typically within 50 meters apart, so geometry of nodes in our experiments were between 10 and 20 feet apart in line of sight to each other.

The topology is a convex quadrilateral which is almost a rectangle, except that UN is a little out of the rectangle. Angles between 1, 2 and 2, 3 are 90 degree. Nodes are distributed in 2-D plane to apply Euclidean distance in location estimation. One anchor was organized so that only one of them sent RTS with an interval of 9 ms, and as long as it received CTS from UN, the timestamps were reported to the laptop through switch, which is the same process as in RTT measurements. The other two anchors were only listening to both RTS and CTS packets, and as stated in Section II, six timestamps were collected for a single round. Table 3 contains actual pairwise distance measured by tape. We first give the plot of relative clock drift and offset for the synchronized RTS/CTS method in Fig.6.

Node Pair	Actual Distance (inches)
1,2	122
1,3	170
2,3	129
1,AP	152
2,AP	190
3,AP	123

Table 3: Outdoor Pairwise distance by physical measurements

Most of the time, drift and offset are quite stable within a small range. When there are adjustments or deviations in the clock, they will jump a lot. This is shown in Fig.6. That's the reason why we need to determine drifts and offsets in different rounds, but not a single constant across time.

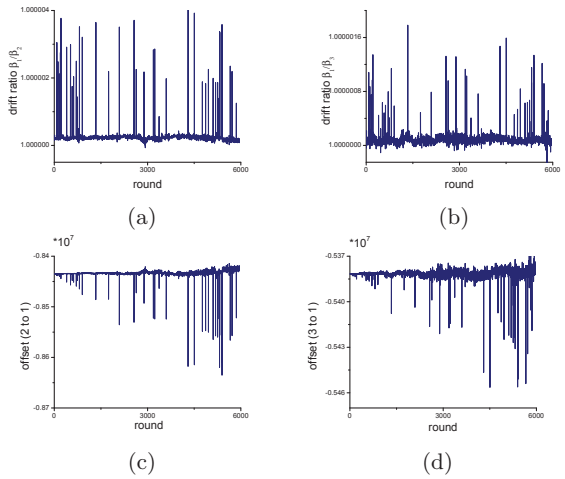


Figure 6: Relative Clock Drift and Offset

Table 4 compares experimental results of TDoA values from two methods with corresponding ground truth in Table 3. The first row of Table 4 is node pairs where first node is the one that generated TDoA, i.e., node pair(1,2,3) stands for $TDoA(1,2,3) = d(1,2) - d(1,3)$. Method 1 is single round of RTS/CTS with synchronization and method 2 is the one taking turns sending. Here anchors are synchronized with respect to 1. So we do not have TDoA of node pair AP, 2 and 3. Both methods have mean errors and variances of TDoA around one foot(12 inches).

Note that six thousand rounds of timestamps were collected for one single experiment, which takes about 60 seconds because of packet loss during the process. The standard deviation approximately one foot in length has been achieved, which will be used for localization.

TDoA Pair	AP,1,2	AP,1,3	AP,2,3
Ground Truth	-38	29	67
Mean Error(1)	10.3	13.4	-
Std Dev.(1)	10.9	8.9	-
Mean Error(2)	10.0	13.7	10.6
Std Dev.(2)	14.2	8.4	11.1

Table 4: Outdoor TDoA comparison results in inches

After getting TDoA value from the experiments, steepest gradient descent method in [5] which minimizes the squared error for all pair of nodes with TDoA information was applied here to do the nonlinear optimization. Mah [19] used techniques by Fang [11] if TDoA measurements are assumed to have significant error. It is not necessary here because results are rather descent without more error reduction. Localization estimates are provided in Table 5. Our proposed methods give us an average error of 6.36 and 6.60 inches. Note that all timestamp readings are according to independent local oscillators and we have not done further processing except mapping functions in method 1. Actually, location determination provides rather small error. For multiple experiments conducted with nodes in different locations, al-

most all of them have an error between 6 and 9 inches.

node	x(inches)	y(inches)
anchor 1	-2.0	129.0
anchor 2	120.0	129.0
anchor 3	120.0	0
AP(actual)	30.9	-21.2
AP(method 1)	35.5	-16.8
AP(method 2)	36.3	-17.4
Mean Error(method 1)	6.36	
Mean Error(method 2)	6.60	

Table 5: Outdoor Location Estimation Performances

The experiment took place on a windy day when there were winds blowing around. Flow of air caused changes in the surrounding environment, which may cause instability of temperature and pressure. These factors may result in differences in speed of light and in turn introduce errors in timestamps and TDoA measurements. This is another error term besides wireless channel noise during transmission, which cannot be eliminated.

5.3.2 Indoor

In the indoor environment, we deploy the nodes so that pairwise distances were within 10 feet. This is mainly because higher precision requirements for indoor location. All the other settings were the same as outdoor experiments. Drift and offset measurements have similar distributions, which have not been shown here. Actual distance in one experiment is listed in Table 6, as well as TDoA comparisons in 7.

Node Pair	Actual Distance (inches)
1,2	36
1,3	60
2,3	48
1,AP	50
2,AP	68
3,AP	48

Table 6: Indoor Pairwise distance by physical measurements

Variances of 12.7 inches and estimation error of around one foot are also achieved in the test. It is worth noting that pairwise distances are not always within one foot error as long as indoor environment becomes complicated, such as people moving around, non-line of sight situations, multipath effects. Actually, even if people are not moving across the direct path of node pair and are several feet away from the system, it will cause sudden errors. In the consideration of that, it may not be practical to use the current proposed method directly to localize without any other compensation in indoor environment. Though complexities of environment increase possibilities of error, similar results have been obtained in restricted environment and are summarized in Table 8.

5.3.3 Discussions

From Table 4 to 8, performances between physical measurements, TDoA and two proposed location methods are shown

TDoA Pair	AP,1,2	AP,1,3	AP,2,3
Ground Truth	-18	2	20
Mean Error(1)	12	2.1	3.6
Std Dev.(1)	12.7	8.4	9.1
Mean Error(2)	8.9	6.5	-
Std Dev.(2)	4.3	7.4	-

Table 7: Indoor TDoA comparison results in inches

node	x(inches)	y(inches)
anchor 1	120.2	0
anchor 2	120.2	36
anchor 3	72.2	36
AP(actual)	72.2	-12.1
AP(method 1)	68.3	-13.8
AP(method 2)	69.6	-14.2
Mean Error(method 1)	4.25	
Mean Error(method 2)	3.34	

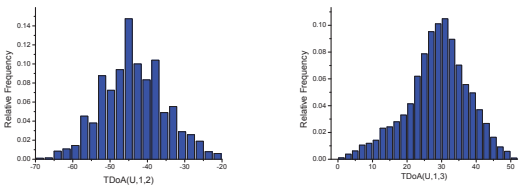
Table 8: Indoor Location Estimation Performances

for both indoor and outdoor environments. Generally, single round method needs more post-processing including clock mapping function while does not require multiple anchors sending RTS. The other method gets rid of synchronization but have to take turns for RTS/CTS exchanging. Estimation errors of two methods are similar. Both have mean error about one foot. One thing to note is that number of rounds we collected for experiments does not contribute much to the estimate performance. We tested with 10, 100, 200, 500, 1000, 2000, 3000 and 6000 samples. The results showed that as long as sample size is larger than 100, location estimate error remain almost the same. This eases us from the fact that collecting as many samples as possible. Through the restricted environment, there are still some sources of errors, which are stated below.

Noise through wireless transmission process is one major error term in 802.11 WLAN. The error can be greatly mitigated through wired transmission but it will decrease the mobility of the system.

Here we compared TDoA values generated by proposed methods with measurements by tape for both methods. The distribution in Fig.7 shows that errors for TDoA estimation are like Gaussian distributions. It is also not surprising if the error follows independent identically distribution(i.i.d). This matches our assumption but we have to confirm it with more verifications. If so, the distributions of TDoA are i.i.d, then we can minimize variances by averaging over repeated rounds of measurements, which is also shown to be a significant improvement since we can get 100 rounds within one second and lower the variance by 10.

Another error comes from physical measurements by tape for pairwise distances. Differences between measured and actual distances contribute to that error. We make approximation in Eq. (7) such that clock drift does not make much difference. In fact, clock drift may change according to temperature because oscillators used in SMiLE board are Temperature-Control-Oscillator (TXCO). Anchor geometry is also related to the final location error of the UN, which is



(a) (b)

Figure 7: TDoA Histograms (inches)

discussed both in [19] and [14]. Results in this paper have rather small errors for indoor localization. Actually, normal indoor environment can be much more complicated due to walls all around, reflections, refractions and movement of human bodies. So we may get such results with error around one foot in only restricted environments.

6. CONCLUDING REMARKS

In this paper a novel TDoA location model based on RTS/CTS mechanism in IEEE 802.11 is introduced. In section V we have shown that the precision of location estimation of about 1 foot has been achieved with both synchronized and asynchronized methods. Taking advantage of customized FPGA extension boards which has sub-nanosecond accuracy is an key part for our experiments. Furthermore, short packets sending intervals may allow easily implementation of real time location determination.

Instead of traditional four-way message exchanges, we propose to use only RTS/CTS. This makes it easy for our processing of timestamps because RTS and CTS both have fixed lengths. The first method only needs timestamps that one anchor sends RTS, and uses linear mapping functions to synchronize clocks. In the second method, it does not necessarily require clock synchronization or drift compensation. We make the assumption that approximation of drift ratio to be 1, which is shown to be reasonable in our system according to our experimental results.

We also evaluate RTS/CTS based RTT characteristics for different mobile devices. RTT measurement is widely used in time-based location systems and services. Its simpleness and popularity prompt many ToA methods, as well as research topics. While people benefit a lot from this point of view, strict requirements may not be always satisfied. That's why the new methods based on TDoA come to appear. Also we give some considerations and limitations of traditional RTT measurements in different situations.

Though we presented good location estimate results for both indoor and outdoor environments, it is common that in the indoor environment we may encounter multipath dominated effects, as well as other unpredictable matters. This may be another step forward towards indoor localization. In the test environment that experiments were conducted, we assume all nodes are within range of each other. Generally this is always the case unless long distance estimation, which has to exploit other messages other than typical WiFi signals. Other extensions may include characterization of different Access Points, indoor multipath propagation model and statistical models to the process of timestamps, which may increase the accuracy furthermore.

7. REFERENCES

[1] I. S. Association et al. 802.11-2012-ieee standard for information technology–telecommunications and information exchange between systems local and metropolitan area networks–specific requirements part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications, 2012.

[2] A. Bahillo, J. Prieto, S. Mazuelas, R. M. Lorenzo, J. Blas, and P. Fernandez. Ieee 802.11 distance estimation based on rts/cts two-frame exchange mechanism. In *Vehicular Technology Conference, 2009. VTC Spring 2009. IEEE 69th*, pages 1–5. IEEE, 2009.

[3] P. Bhargava, S. Krishnamoorthy, A. K. Nakshathri, M. Mah, and A. Agrawala. Locus: An indoor localization, tracking and navigation system for multi-story buildings using heuristics derived from wi-fi signal strength. In *Mobile and Ubiquitous Systems: Computing, Networking, and Services*, pages 212–223. Springer, 2013.

[4] P. Biswas, T.-C. Lian, T.-C. Wang, and Y. Ye. Semidefinite programming based algorithms for sensor network localization. *ACM Transactions on Sensor Networks (TOSN)*, 2(2):188–220, 2006.

[5] J. Caffery and G. L. Stuber. Subscriber location in cdma cellular networks. *Vehicular Technology, IEEE Transactions on*, 47(2):406–416, 1998.

[6] Y. Chan and K. Ho. A simple and efficient estimator for hyperbolic location. *Signal Processing, IEEE Transactions on*, 42(8):1905–1915, 1994.

[7] B. Denis, J.-B. Pierrot, and C. Abou-Rjeily. Joint distributed synchronization and positioning in uwb ad hoc networks using toa. *Microwave Theory and Techniques, IEEE Transactions on*, 54(4):1896–1911, 2006.

[8] T. Eren, O. Goldenberg, W. Whiteley, Y. R. Yang, A. S. Morse, B. D. Anderson, and P. N. Belhumeur. Rigidity, computation, and randomization in network localization. In *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, volume 4, pages 2673–2684. IEEE, 2004.

[9] R. Exel, G. Gaderer, and P. Loschmidt. Localisation of wireless lan nodes using accurate tdoa measurements. In *Wireless Communications and Networking Conference (WCNC), 2010 IEEE*, pages 1–6. IEEE, 2010.

[10] R. Exel, J. Mad, G. Gaderer, and P. Loschmidt. A novel, high-precision timestamping platform for wireless networks. In *Emerging Technologies & Factory Automation, 2009. ETFA 2009. IEEE Conference on*, pages 1–8. IEEE, 2009.

[11] B. T. Fang. Simple solutions for hyperbolic and related position fixes. *Aerospace and Electronic Systems, IEEE Transactions on*, 26(5):748–753, 1990.

[12] A. Günther and C. Hoene. Measuring round trip times to determine the distance between wlan nodes. In *NETWORKING 2005. Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless*

Communications Systems, pages 768–779. Springer, 2005.

[13] I. Guvenc and C.-C. Chong. A survey on toa based wireless localization and nlos mitigation techniques. *Communications Surveys & Tutorials, IEEE*, 11(3):107–124, 2009.

[14] S. Han. *CLOCK SYNCHRONIZATION AND TARGET LOCATION DETERMINATION IN WIRELESS NETWORKS*. PhD thesis, 2014.

[15] S. Han, A. Agrawala, M. Mah, R. Exel, and T. Bigler. Clock synchronization-an approach using mapping functions. In *European Wireless 2014; 20th European Wireless Conference; Proceedings of*, pages 1–7. VDE, 2014.

[16] C. Hoene and J. Willmann. Four-way toa and software-based trilateration of ieee 802.11 devices. In *Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on*, pages 1–6. IEEE, 2008.

[17] K. Kaemarungsi and P. Krishnamurthy. Properties of indoor received signal strength for wlan location fingerprinting. In *Mobile and Ubiquitous Systems: Networking and Services, 2004. MOBIQUITOUS 2004. The First Annual International Conference on*, pages 14–23. IEEE, 2004.

[18] K. Lee, J. C. Eidson, H. Weibel, and D. Mohl. Ieee 1588-standard for a precision clock synchronization protocol for networked measurement and control systems. In *Conference on IEEE*, volume 1588, 2005.

[19] M. Y. M. Mah. Time-based location techniques using inexpensive, unsynchronized clocks in wireless networks. 2011.

[20] D. E. Manolakis. Efficient solution and performance analysis of 3-d position estimation by trilateration. *Aerospace and Electronic Systems, IEEE Transactions on*, 32(4):1239–1248, 1996.

[21] D. L. Mills. Simple network time protocol (sntp) version 4 for ipv4, ipv6 and osi. 2006.

[22] J. Prieto, A. Bahillo, S. Mazuelas, J. Blas, P. Fernández, and R. Lorenzo. Rts/cts mechanism with 802.11 for indoor location.

[23] M. Youssef, A. Youssef, C. Rieger, U. Shankar, and A. Agrawala. Pinpoint: An asynchronous time-based location determination system. In *Proceedings of the 4th international conference on Mobile systems, applications and services*, pages 165–176. ACM, 2006.