Filtering Noisy 802.11 Time-of-Flight Ranging Measurements

Andreas Marcaletti  
ETH Zurich  
Zurich, Switzerland

Maurizio Rea  
ETH Zurich  
Zurich, Switzerland

Domenico Giustiniano  
IMDEA Networks Institute  
Madrid, Spain

Vincent Lenders  
Armasuisse  
Thun, Switzerland

Aymen Fakhreddine  
IMDEA Networks Institute & UC3M  
Madrid, Spain

ABSTRACT

Time-of-Flight (ToF) echo techniques have been proposed as a way to estimate the range between regular Wi-Fi stations. Recent works either did not address practical questions for deployability, or made evaluations in basic setups, or used advanced 802.11 hardware designs. We build an approach solely deployed using ToF measurements and relying on software access point (AP) upgrades of simple commercial off-the-shelf 802.11 chipsets. Our solution filters noisy measurements collected by WiFi chipsets of six dollars each, it has been tested across different and heterogeneous setups and testbeds, and has the potential to enable ToF ranging in every Wi-Fi chipsets.

Categories and Subject Descriptors

C.2.1 [Computer-Communication Networks]: Network Architecture and Design—Wireless Communication

Keywords

Indoor Localization; 802.11; Time of Flight; Design; Implementation; Evaluation

1. INTRODUCTION

In the attempt to find an alternative to error-prone signal-strength based ranging measurements [3, 5, 10, 13, 16], Time-of-Flight (ToF) echo techniques have recently received attention by the research community. The underlying principle of ToF is that the distance between two devices is estimated using the time that the signal travels between two devices, with the advantage of being less susceptible to the diversity of the obstacles between the devices [8, 14]. The intuition is that electromagnetic waves travel at a speed that is close to the speed of light for most propagation media in typical indoor environments, and thus the signal propagation speed is fairly independent on the environment, obstacles, etc.

Despite of these advantages, ToF measurements are very sensitive to noise since, at the speed of light, a measurement error of 1 μs already results in a distance estimation error of 300 meters. This noise is further exacerbated when using Commercial Off-The-Shelf (COTS) WiFi devices for a cost-effective and wide-spread implementation. Recent efforts could increase the accuracy of ToF at the cost of leveraging advanced hardware designs available in more recent WiFi chipsets [14]. However, most of the Access Points (APs) in the world are still deployed with older hardware, and it is economically not possible to change all the APs with newer hardware in the near future (and also not appealing in terms of electronic garbage).

We leverage the existing 802.11 protocol timing specification (and nothing more than that) to build a system that runs on COTS APs to estimate the distance to target stations. We rely on a customized firmware operating in the core of the 802.11 MAC state machine of a low-cost WiFi chipset (cost per unit of less than six dollars). To deal with the intrinsic challenges of noisy ToF measurements, we develop an adaptive filter which manages to predict the distance despite the large noise introduced by the devices and the multipath reflections in indoor environments.

Our approach has been tested across various setups and testbeds. We show that our filtering technique needs just a few samples to estimate the distance range with a median error of $1.7 \pm 2.4$ m and a 80-percentile error of $3.7 \pm 5.8$ m, comparable to [14] (median error of $\approx 1$ m and 80-percentile error of $\approx 5$ m) that required advanced inputs from the hardware such as channel state information per antenna. Our solution further outperforms recent works such as [8].

Given its simplicity, the principles discussed in our work can be applied to any old and new 802.11 AP already deployed, just with software upgrades.

2. BACKGROUND AND CHALLENGES

This section describes the basics of WiFi ToF ranging and highlights various real-world challenges that arise when applying this technique with simple off-the-shelf devices.

2.1 WiFi ToF Ranging Technique

While traditional ToF-based echo techniques as employed in radar systems rely on uncoded RF signals and their reflections, WiFi echo techniques use regular frames of communication. In WiFi communication, every DATA frame is acknowledged by the receiver with an ACK frame.
The distance to the target device is then inferred as \( \delta_t \) where \( t \) is the time offset may be also generated at the target device.

ToF ranging can be formulated as follows. If \( d \) is the distance between a local station and a target, the measured time-of-flight \( t_{\text{MEAS}}(d) \) between a sent DATA frame and a received ACK frame is expressed as

\[
t_{\text{MEAS}}(d) = 2 \cdot t_r(d) + t_{\text{ACK}} + \delta,
\]

where \( t_r(d) \) is the signal propagation time between the transmitter of the DATA frame and the target (channel reciprocity is assumed), \( t_{\text{ACK}} \) is the time needed to transmit the ACK, \( \delta \) is an offset depending on the target and local sender. The distance to the target device is then inferred as

\[
d_n = \frac{c}{2} \cdot (t_{\text{MEAS}}(d) - t_{\text{ACK}} - \delta),
\]

where \( c \) is the speed of signal propagation which is close to the speed of light in air. Assuming that \( N \) consecutive samples \( \{d_n\} \) are collected, the distance between the local station and the mobile device is finally estimated as:

\[
d = f(d_n),
\]

where \( f \) is either the expected value on the input data or any other estimator.

**Firmware integration.** To alleviate any unnecessary source of noise or instability, the time measurements \( t_{\text{MEAS}}(d) \) have to work as close as possible to the radio hardware. The best location to fully control the measurement is therefore in the firmware of the WiFi radio chipset, rather than in the driver as proposed in [8]. To measure \( t_{\text{MEAS}}(d) \) in the firmware, we have customized the open-source 802.11 openFWWF firmware\(^1\). This firmware is written in assembler and runs on off-the-shelf 802.11 Broadcom chipsets, such as the ones widely used in Linksys APs. Our customized firmware reports \( t_{\text{MEAS}}(d) \) for each successful transmission of an 802.11 DATA frame. The timing is regulated by the general purpose timer, running on the wireless card’s internal clock at a rate of \( 88 \text{ MHz} \). The timer starts to count clock cycles just after the 802.11 processor sets up a register to indicate that a frame has been sent. Once the ACK frame has been received, the timer gets stopped. Every time a measurement is made, the firmware writes \( t_{\text{MEAS}}(d) \) into a defined address of the shared memory (SHM). The measurement architecture is shown in Fig. 2. Since the driver has also access to the shared memory block, it can retrieve the measurement every time an ACK is received\(^2\). In the driver, we gather additional data about the incoming ACK such as the data rate, MAC addresses, etc, and store them all in a buffer. Once this buffer is full or a timeout elapsed, the data is transferred to the user space with the help of UDP sockets.

### 2.2 Real-world Challenges

In the real-world, ToF measurements are affected by large noise coming from the timing imprecision of off-the-shelf WiFi devices. The offset \( \delta \) is given by:

\[
\delta = \delta_T + \delta_L,
\]

where \( \delta_T \) and \( \delta_L \) are the offsets of target station and local sender, respectively. In addition, the multipath signal propagation characteristics of complex indoor environments play an important role to ToF measurements. In the following, we describe the main sources of noise and how they affect the accuracy of ToF ranging.

**Target and measuring noise.** The 802.11 standard specifies the SIFS time between the reception of a DATA and the transmission of an ACK at the receiver as a fixed interval. In 802.11b, for example, this time is specified as \( 10 \mu s \) [2]. However a relatively high tolerance of \( 1 \mu s \) is tolerated which can result in significant noise and distance estimation errors up to 300 meters if the target is effectively exploited this specified tolerance level. While most chipsets may not fully exploit this tolerance, the dispersion is still quite significant.

To illustrate this, Fig. 3 on the left represents the resulting dispersion of a typical Broadcom WiFi chipset as target device. The shown histogram was obtained by estimating the distance \( d_n \) according to Eq. (2) for 10000 packets.

\(^1\)http://www.ing.unibs.it/openfw wf/

\(^2\)We operate in promiscuous mode which allows us to know in the driver when an ACK has been received and thus a new data is available in the SHM.
avoid any dispersion from environmental effects, the measurements were performed over a coaxial cable of 13.5 meters length. As we can see, there is heavy noise in the measurement setup that leads to distance estimations ranging from 0 to 25 meters.

**Environmental noise.** It is well known that signal propagation in complex indoor environments is subject to multipath effects in which multiple copies of the transmitted signal arrive at the receiver over different reflected paths. It is even possible that the direct component is entirely attenuated and the signal is received only over indirect paths. Since signals that travel over indirect paths will take longer to arrive at the receiver, they introduce an error in the distance estimation when considering the time-of-flight. This situation is shown in Fig. 3 in the middle and on the right where the same experiment as on the left was repeated but for a line-of-sight (LOS) and non-line-of-sight (NLOS) signal propagation link over omnidirectional antennas. The dispersion spans a range of 40 and 60 meters for the LOS and NLOS links respectively. In addition, the NLOS link shows a skewed distribution, suggesting that the signals are received from different propagation paths over the duration of the experiment. Multipath effects must therefore be taken into consideration in order not to overestimate the distance when dealing with reflected signal propagation paths. Finally, multipath may also happen in LOS links, and thus a method robust to the propagation conditions must be designed.

**Additional sources of noise.** Off-the-shelf WiFi chipsets have not been designed to provide accurate ToF measurements. Additional noise therefore comes from the coarse clock resolution of the radios. For example, the Broadcom chipset operates with a reference clock of 88 MHz, corresponding to a maximal distance resolution of 1.7 meters. In addition to this quantization noise, off-the-shelf chipsets introduce all sorts of considerable additional noise. As we could see in the histograms of Fig. 3, the shape of the distribution is far from being smooth despite using 10000 samples to create the histograms, suggesting that the radios must have some bias when measuring the time. The measurement noise must therefore also be factored in to estimate the distance.

### 3. TARGET AND MEASURING NOISE

To dissect the relative importance of the noise of the target station with respect to the local noise, we use a wideband oscilloscope (Infinium 90000A Oscilloscope) with a fast sampling rate of 10 GS/s to measure the target offset $\delta_t$. A horn antenna is connected to the oscilloscope which serves as a passband filter for the 2.4 GHz band. The target device is in close proximity to the horn antenna, so that radio signals of received 802.11 DATA and transmitted 802.11 ACK are immediately captured by the oscilloscope, and effects of signal reflections are minimized. The noise of our high-end oscilloscope can be regarded as low such that reported measurements are not affected by any measuring noise but dominated by the target noise [4].

We use above setup to statistically compare the effective ToF to the measured time $t_{\text{MEAS}}(d)$ as being locally reported by our firmware on the Broadcom chipset. To compare both distributions, we use the method of the quantile-quantile (QQ) plot. We collect samples in LOS settings at $d = \{1, 15, 60\}$ m. Results are summarized in Fig. 4. We observe a linear pattern, which indicates that the noise of the target station and the data measured locally by the 802.11 firmware have very similar distributions. Hence, the dispersion of the local offset has a negligible impact on the noise of $t_{\text{MEAS}}(d)$, and most of the dispersion comes from the target device. This further demonstrates that our approach to implement the ToF measurement in the firmware allows to minimize the impact of the local dispersion of the noise for LOS links with limited multipath. In the next section, we look at the impact of richer multipath.

### 4. ENVIRONMENTAL NOISE

Environmental noise is tricky to deal with. The reasons are the following:

- multipath reflections introduce a skewness of the sample distribution which cannot be easily smoothed out by averaging over a set of biased samples,
- the target noise introduces large offset noise which adds to the noise created by multipath,
- environmental noise is highly unpredictable as the reflected paths are location-specific.
We therefore need an adaptive filter that is calibrated to the actual multipath characteristics of the experienced location-specific environment.

Our goal is to design a filter that takes a series of $N$ consecutive measurements $\{\hat{d}_1, \hat{d}_2, \ldots, \hat{d}_N\}$, and selects the $p$-percentile $\hat{d}(p)$ of the series that minimizes the estimation error. Intuitively, in absence of multipath, the median $p = 50$ could fairly represents the distance, while taking the median in presence of multipath reflections will cause an over-estimation of the distance due to the added traveled distance of the signals. By selecting a percentile $p < 50$ to estimate the distance, we can therefore counterbalance those biased values in the estimation process.

### 4.1 Data Integrity

First, to guarantee data integrity in our evaluation, we removed sequences of samples which experienced undesired side effects for a systematic evaluation. In particular, for statistical relevance of the results, consecutive ToF measurements are supposed to be independent and identically distributed (i.i.d.). While this assumption holds in most tests, this condition does not hold in general. We perform cable tests and they show that the autocorrelation is very low for lag greater than zero. We observe however that there are links with high autocorrelation when DATA is transmitted over the air. This could be explained with the presence of more than one path between transmitter and receiver, which may imply that the circuitry continuously jumps between two states in an attempt to tune the frame synchronization. We therefore discard those sequences which were subject to a high absolute lag-one autocorrelation (above 0.2) for the analysis. Removing measurements with a high autocorrelation is a valid assumption in the real-world as this kind of test can easily be performed by the AP.

### 4.2 Estimating Multipath Noise

The second step is to estimate the noise caused by multipath reflections on a link. Since we cannot directly measure the individual multipath components at the signal-level on off-the-shelf WiFi radios, we propose to use a higher-level estimator $f$ for this. We explored various options in an extensive evaluation in one of our testbeds (Testbed I, Fig. 7) with all links with low lag-one autocorrelation (83% of the links). As estimators, we considered the first three moments (median, standard deviation, and skewness) for the ToF as well as for the Received Signal Strength Indicator (RSSI). For each of these six estimators, we evaluate two variants, leading to a total of twelve candidate estimators. In the first variant, we determine the moments directly on the raw samples. In the second variant, we attempt to pre-filter obvious outliers that arise from the device-related measurement noise prior determining the moments. These outliers are filtered out applying the Thompson Tau technique, a statistical method for deciding whether to keep or discard samples based on the expected value and the expected deviation of the sequence of samples.

We evaluate the precision of these estimators by determining their correlation to the optimal percentile $p_{opt}$, defined as the percentile that provides the minimum absolute distance estimation error as:

$$p_{opt} = \arg \min_{0 < p < 0.5} |d - \hat{d}(p)| \quad (5)$$

Table 1: Absolute value of Pearson correlation coefficient between different moments of the RSSI and ToF versus the optimal percentile $p_{opt}$ ($0$=no correlation, $1$=maximum correlation).

<table>
<thead>
<tr>
<th></th>
<th>unfiltered</th>
<th>pre-filtered</th>
</tr>
</thead>
<tbody>
<tr>
<td>median of RSSI</td>
<td>0.62</td>
<td>0.63</td>
</tr>
<tr>
<td>standard deviation of RSSI</td>
<td>0.04</td>
<td>0.05</td>
</tr>
<tr>
<td>skewness of RSSI</td>
<td>0.23</td>
<td>0.24</td>
</tr>
<tr>
<td>median of ToF</td>
<td>0.76</td>
<td>0.76</td>
</tr>
<tr>
<td>standard deviation of ToF</td>
<td>0.19</td>
<td>0.21</td>
</tr>
<tr>
<td>skewness of ToF</td>
<td>0.20</td>
<td>0.51</td>
</tr>
</tbody>
</table>

that is, the a-posteriori optimal percentile for each link given the true distance of each link in our experiments.

To quantify the correlation between the different moments and $p_{opt}$, we use the Pearson correlation coefficient on the entire set of links of Testbed I. The Pearson correlation coefficient is an indicator of the linear correlation of the variables, where absolute values close to zero indicate a low correlation and absolute values close to one represent a high linear dependence of two variables. A value close to one thus indicates that a moment is a good estimator to predict a percentile that will filter out the multipath noise effectively.

Table 1 shows the resulting correlation coefficient for all twelve variants. The best correlation is provided by the median of the ToF, followed by the median of the RSSI and the skewness of the ToF. All other moments have a correlation coefficient below 0.5 which indicates a low correlation. Most of the moments profit from pre-filtering to remove the outliers. In particular, the skewness of the ToF increases from 0.20 to 0.51 and is therefore considerably better when pre-filtering the outliers.

One may wonder why the skewness of the ToF has a worse correlation than the median ToF. Intuitively, the skewness of the distribution should be a good indicator of the multipath, given that links with strong reflected (delayed) components are left-skewed, with $p_{opt}$ smaller than for right-skewed link. Our results suggest that the combined device-related noise of the receiver and the measuring station have a strong negative effect on the correlation on the skewness. This is reflected in the pre-filtered version of the skewness which has a considerably better correlation than the unfiltered version. In contrast, the median of the ToF is much more robust to this device-related noise and therefore outperforms the skewness. In addition, it reflects the tendency of having more links affected by multipath for longer distances.

### 4.3 Filter Design

Motivated by the good correlation of the median ToF and the optimal percentile, we designed a filter that relies on this correlation to select an appropriate percentile of the sample ToF measurements when estimating the distance. The filter relies on a linear model which is derived from the empirical distribution of the median ToF versus $p_{opt}$. We call it offline calibration, since it would be usually performed before actual tests. This distribution on all the 207 links of Testbed I is shown in the top of Fig. 5. We note that the value of the optimal percentile is widely distributed between $0 \leq p_{opt} \leq 50\%$. Therefore, it does not exist one value of percentile
5. EVALUATION METHODOLOGY

This section presents the system and environmental setup we used to evaluate the performance of our filter.

5.1 System Setup

AP infrastructure. We have build a prototype ToF system to evaluate its performance in real-world conditions. Our system is based on COTS APs from Soekris (net5501 embedded machine with a 500 MHz AMD Geode LX single chip processor). The APs are equipped with Broadcom AirForce54G 4318 mini PCI type III cards which we operate with our customized firmware and b43 driver presented in Section 2.1. As operating system on the APs we use Ubuntu server 10.04 with a Linux kernel version 2.6.32-60. In order to operate the embedded device as WLAN AP, we use the software suite hostapd. The APs are connected to the central localization unit over Gigabit Ethernet.

Target devices. As target devices we use Dell Inspiron 5150 laptops equipped with Broadcom AirForce54G 4318 mini PCI type III cards. The operating system on the laptops is Ubuntu 10.04 with its original Linux kernel version 2.6.32-21.32. The wireless cards are operated in client mode.

5.2 Deployment Scenarios

Testbed deployment. We perform experiments in three indoor testbeds deployed in different environments. We deploy 10 APs in Testbed I and III and 9 APs in Testbed II. Testbed I and Testbed II are office environments. The environment of Testbed I is shown in Fig. 7 and it covers a surface of almost 1000 m². We use 25 randomly selected locations (marked with a cross) to test our algorithms. We conducted tests over two different days, with some position repeated again with different location of some furniture, and collected a total of 207 wireless links. Testbed II features 180 links and it covers a smaller space of around 200 m². The target station is in 20 different positions. Testbed III has been deployed at the facilities of the IEEE/ACM IPSN Microsoft Indoor Localization Competition [1]. The testbed features 200 links and it covers 320 m². The target device is placed at 20 different positions across two rooms and a hallway. In all the testbeds there exists a mixture of line-of-sight and non-line-of-sight wireless links. The testbeds also contain several propagation obstructions, including concrete walls, tables and glasses. All experiments are conducted with other active WLAN networks. We operate the three testbeds on a fixed frequency channel of the 2.4 GHz ISM band. The PHY automatic selection rate is active, such that the measurements include probes sent at different rates.

6. EVALUATION RESULTS

This section evaluates the performance of different ranging estimators in our testbeds.

6.1 Filter Performance

Distance Ranging Accuracy. To test our filter, we have evaluated its performance on all the links of Testbed I. For each link, we first compute the distance estimation error with 20 samples, and then calculate the average error...
ToF (similar results are achieved with our other filters). As reported in Fig. 8, the online calibration achieves similar results with respect to the offline tests, with median error of 2.6 m and a 80-percentile error of 5.4 m. Thus, the environmental calibration can be executed online without significant performance loss.

Robustness to different environments/testbeds. Fig. 9 shows the median and 80-percentile of the distance error for the three different testbeds using sequences of 20 samples. As shown in the x-label of the figure, we measure a high Pearson correlation coefficient between the median of ToF and the optimal percentile (0.76 – 0.89). The median distance error is in the range 1.7 – 2.4 m and the 80-percentile error is in the range 3.7 – 5.8 m. Concluding, the estimator is robust across different environments.

Impact of Number of ToF Samples. A further parameter we evaluate with regard to our filter is the number of ToF measurement samples N that are used for the estimation of the distance. Figure 10 shows the error for our filter that relies on the median of the ToF as a function of the number of samples. It is remarkable that the error is stable with five or more samples for the median of the distance error, and with ten or more samples for the 80-percentile of the distance error.

7. CONCLUSION
We have designed a cost-effective ranging technique such that it does not require any special hardware, special antennas, or software-defined radio architectures. Our solution can be deployed as a software upgrade to current WLAN infrastructures. While our best performing estimator may be a bit counter-intuitive, we have shown its robust performance in a variety of different setups and testbeds. Since ToF-based WLAN localization is still at its infancy, we believe that further research in this area might help to even further improve the accuracy of our results in the future.

Acknowledgments
We are grateful to Francesco Gringoli for sharing the open-FWWF code and supporting the project with his enlightening comments. The work was supported by Armasuisse. The research leading to these results has received funding from the European Research Council under the EU’s Seventh Framework Programme, ERC Grant Agreement no. 617721.
8. REFERENCES


