Nanosecond-precision Time-of-Arrival Estimation for Aircraft Signals with low-cost SDR Receivers

Roberto Calvo-Palomino  
IMDEA Networks Institute, Spain  
University Carlos III of Madrid  
roberto.calvo@imdea.org

Fabio Ricciato  
University of Ljubljana, Slovenia  
fabio.ricciato@fri.uni-lj.si

Domenico Giustiniano  
IMDEA Networks Institute, Spain  
domenico.giustiniano@imdea.org

Blaz Repas  
University of Ljubljana, Slovenia  
br9404@student.uni-lj.si

Vincent Lenders  
armasuisse, Switzerland  
vincent.lenders@armasuisse.ch

ABSTRACT
Precise Time-of-Arrival (TOA) estimations of aircraft and drone signals are important for a wide set of applications including aircraft/drone tracking, air traffic data verification, or self-localization. Our focus in this work is on TOA estimation methods that can run on low-cost software-defined radio (SDR) receivers, as widely deployed in Mode S / ADS-B crowdsourced sensor networks such as the OpenSky Network. We evaluate experimentally classical TOA estimation methods which are based on a cross-correlation with a reconstructed message template and find that these methods are not optimal for such signals. We propose two alternative methods that provide superior results for real-world Mode S / ADS-B signals captured with low-cost SDR receivers. The best method achieves a standard deviation error of 1.5 ns.

1 INTRODUCTION
Aircraft and unmanned aerial vehicles continuously transmit wireless signals for air traffic control and collision avoidance purposes. These signals are either sent as responses to interrogations by secondary surveillance radars (SSR) or automatically on a periodic basis (ADS-B). Both types of signals are transmitted over the so-called Mode S data link [12] on the 1090 MHz radio frequency.

Over the last few years, sensor network projects have emerged which collect those signals using a crowd of low-cost software-defined radio (SDR) receivers such as e.g. the OpenSky Network [20], FlightAware [3], Flightradar24 [6] and many others. These sensor networks can leverage the time-of-arrival (TOA) of Mode S signals for various kinds of applications, including aircraft localization [20, 22], air traffic data verification [13, 16, 17, 19, 21], and self-localization [15]. In those applications, a set of cooperating receivers measure locally the TOA of the arriving signals and then send these data to a central computation server. By joint processing the TOA of the same signal arriving at different receivers, the central server is able to estimate the location of the transmitter, the location of the receivers, or the exact time when the signal was transmitted.

The accuracy of these applications heavily depends on the precision of the TOA estimation, and in order to estimate positions up to a few meters it is necessary to estimate the TOA with nanosecond precision. The goal of this work is to provide a method for the TOA estimation of Mode S signals that delivers nanosecond-level precision even with low-cost SDR receivers, such as the widespread RTL-SDR dongle [3]. We show that existing TOA estimation approaches based on a cross-correlation with a reconstructed signal template are sub-optimal in the particular context of Mode S signals. In fact, the loose tolerance margins allowed by the specifications on the shape and position of each individual symbol within the packet (up to ± 50 ns) adds uncertainty to the reconstruction of the whole packet waveform at the receiver.

We propose two alternative methods that improve the precision and at the same time reduce the computational load. We test different variants of TOA estimation on real-world signal traces captured with RTL-SDR, which is currently the cheapest SDR device on the market and widely used by crowdsourced sensor networks. Our results show that the best proposed method delivers TOA estimates with a standard deviation error of 1.5 ns. We further identify the limited dynamic range of the RTL-SDR device (less than 50 dB with 8-bit analog-to-digital converter (ADC) and fixed automatic-gain controller (AGC)) as the main performance bottleneck, and show that sub-nanosecond precision is achievable for signals that are not clipped due the limited dynamic range of the device.

2 BACKGROUND
This section provides background on aircraft signals which we rely on to estimate the TOA, and the limitations of classical TOA estimation methods.

2.1 Mode S signal format
Hereafter we briefly review the physical-layer format of SSR Mode S [18] reply and ADS-B messages transmitted by aircrafts on the 1090 MHz channel. Both packet formats consist of a preamble of 8 µs plus a payload of 112 or 56 bits (only for other SSR Mode S replies) sent at 1 Mbps rate, for a total duration of 120 µs or 64 µs, respectively. The information bits are modulated with a simple Binary Pulse Position Modulation (BPPM) scheme as illustrated in Fig. 1: the symbol period of 1 µs is divided into two “chips” of 0.5 µs, and the high-to-low and low-to-high transitions encode bits “1” and “0”, respectively. It is clear from Fig. 1 that the BPPM modulation produces two types of pulses of different duration, denoted hereafter as “Type-I” and “Type-II”. Type-I pulses have a nominal duration of one chip period and are produced by the bit sequences ”00”, ”11” and ”10”. The preamble consists of four Type-I pulses. On the other hand, Type-II pulses have a nominal duration of two chip periods and are produced exclusively by the ”01” sequence. On average, we
Additive White Gaussian Noise (AWGN) channel is a correlation shape. As to the pulse of each pulse, tolerance values of 50 ns are allowed. The standard "course book" approach to TOA estimation in the presence of additive noise. Consequently, the correlation-based approach with high SNR, such an uncertainty might well prevail over the effect of the signal. Considering that Mode S signals are typically received with prediction of the shape and position of the pulses in the source, such loose tolerance margins introduce uncertainty in the time, while pulse amplitude may vary up to 2 dB (approximately 60%). Such loose tolerance margins introduce uncertainty in the prediction of the shape and position of the pulses in the source signal. Considering that Mode S signals are typically received with high SNR, such an uncertainty might well prevail over the effect of additive noise. Consequently, the correlation-based approach with a known packet template is no longer guaranteed to be optimal, motivating the quest for alternative, more precise methods.

2.2 Limitation of standard TOA methods

The standard "course book" approach to TOA estimation in the Additive White Gaussian Noise (AWGN) channel is a correlation filter [14]: the received signal is cross-correlated with a known template corresponding to the source signal, and the point in time maximizing the cross-correlation module is taken as TOA estimate. The correlation method relies on the assumption that the source signal can be reconstructed very precisely at the receiver, based on the signal specifications and knowledge of the payload bits $p_m$. Under this assumption, the correlation method represents the Maximum Likelihood Estimator (MLE) [14]. However, this assumption is problematic in the particular case of real-world Mode S signals. In fact, the standard specifications tolerate up to ±50 ns jitter in the position of each individual pulse within the packet: such high tolerance value is practically negligible for the decoding process, but not for the task of determining the TOA with nanosecond precision. As to the shape of each pulse, tolerance values of 50 ns are allowed for the pulse duration and rise time and up to 150 ns for the decay time, while pulse amplitude may vary up to 2 dB (approximately 60%). Such loose tolerance margins introduce uncertainty in the prediction of the shape and position of the pulses in the source signal. Considering that Mode S signals are typically received with high SNR, such an uncertainty might well prevail over the effect of additive noise. Consequently, the correlation-based approach with a known packet template is no longer guaranteed to be optimal, motivating the quest for alternative, more precise methods.

2.3 Proposed methods: CorrPulse and PeakPulse

Hereafter we describe two novel TOA estimation algorithms specifically developed for Mode S signals. For a generic packet $m$ we shall denote by $K_m$ the total number of pulses in the whole packet (preamble and payload). The input vector of complex samples $(s_m)$ is preliminarily upsampled by a factor $N$ and transformed into vector $s'_m$ (for a review of upsampling process see e.g. [10]). To illustrate, Fig. 3 plots an excerpt of the amplitude of both vectors, namely $|s_m|$ (top plot) and $|s'_m|$ (bottom plot), for a generic packet found in a real-world trace.

The key aspect of the proposed algorithms is that the actual temporal position $t_k$ of the generic $k$th pulse within the packet is estimated independently from other pulses, with no need to reconstruct a template for the whole packet. For each pulse $k \geq 2$,
we compute the individual shift \( \Delta \tau_k = \hat{\tau}_k - \tau_k \), i.e., the difference between the estimated and nominal pulse position relative to the (estimated) position of the first pulse. Finally, the pulse shifts are averaged in order to obtain the final TOA estimate:

\[
\hat{\tau} = \hat{\tau}_1 + \frac{1}{K_m - 1} \sum_{k=2}^{K_m} \Delta \tau_k
\]

The two proposed variants differ in the way individual pulse position estimates are obtained, and which type(s) of pulses are considered. In the first variant, labeled CorrPulse, each pulse position is determined through pulse-level cross-correlation of the upsampled vector \( s_m \) with the corresponding nominal pulse shape. Both Type-I and Type-II pulses are considered in the final averaging.

In the second variant, labeled PeakPulse, individual pulse positions are determined by simply picking the local maximum point value within the pulse interval, with no cross-correlation operation. In this variant only Type-I pulses are considered, while Type-II pulses are ignored. This is motivated by the fact that Type-II pulses have lower curvature, hence their local peaks cannot be identified as reliably as for Type-I pulses.

4 EVALUATION METHODOLOGY

This section describes how we evaluate our new methods. First, we introduce the other competing methods taken as reference for the comparison. Then, we present the testbed setup with commercial low-cost hardware. Finally, we provide details on the procedure adopted to empirically assess the precision of the TOA measurement methods in the given setup.

4.1 Other methods for comparison

4.1.1 Correlation with whole-packet template: CorrPacket. This is the canonical cross-correlation method with a known signal template. For every packet \( m \), the whole packet template is reconstructed from the decoded bits \( p_m \) and then cross-correlated with the amplitude of the incoming signal. Here also, upsampling by a factor \( N \) is adopted to achieve sub-sample precision. Within the template, the \( k \)th pulse is positioned at the nominal time \( \tau_k \). As to the pulse shapes, we have tested two different variants: "Rectangular" (R), and "Smoothed" (S). The two versions will be denoted by CorrPacket/R and CorrPacket/S. The rectangular pulses have a nominal duration of 0.5 \( \mu \)s and 1 \( \mu \)s for Type-I and Type-II pulses, respectively, and zero rise/decay times. The rectangular pulse mask is represented exclusively by "0" and "1" values, hence multiplications with another vector reduce to element selection, which saves on computation load. The "Smoothed" shape corresponds to the output of a low-pass filter with passband of 2.4 MHz—matched to the bandwidth of the RTL-SDR receiver—when the input signal is a nominal Type-I/Type-II pulse with the minimum decay/raise time of 50 ns as per specifications [11].

4.1.2 Existing dump1090 based implementations. We also evaluate the precision of the timestamp reported by the mutability fork of the open-source tool dump1090 [1]. Furthermore, we test on our traces also the method adopted by Eichelberger et al. in a recent ACM SenSys'17 paper [15] which is also based on dump1090. Code inspection revealed that this method is based on a cross-correlation (implemented in frequency domain) with a partial packet template consisting of the preamble plus one quarter of the payload, with rectangular pulses and upsampling factor \( N = 25 \).

4.2 Testbed setup

The experimental setup consists of two identical sensors connected to a single antenna through a power splitter and cables of identical length. The sensors are located on the roof of a building as Figure 4 shows. Every sensor consists of one RTL-SDRv3 “Silver” model [4] attached to a Raspberry Pi-3 [2]. The AGC gain is set to a fixed value, manually tuned to maximize the packet decoding rate. The sampling rate was set to \( f_s = 2.4 \) MHz; the maximum value that our setup is able to acquire with sample losses. Every I and Q sample is represented with 8 bit. The full stream of IQ samples are recorded one and processed multiple times offline. Our results are based on a sample trace of 5 minutes collected in Thun (Switzerland) on 02-Aug-2017 at time 09:41. The number of ADS-B packets that are correctly decoded at both sensors by the dump1090 open-source tool [1] amount to 26445 from 59 different aircraft.

4.3 Evaluation Metrics

In this section, we briefly describe the methodology adopted to assess the precision of the different TOA estimation methods. The problem is not trivial, since our receivers are not synchronized and the “true” TOA is unknown. Therefore, we developed an evaluation method which allows us to quantify the TOA precision without a ground truth.

Denote by \( t_{m,i} \) the true absolute arrival time of packet \( m \) to receiver \( i \) and by \( \hat{t}_{m,i} \) the corresponding measured TOA (by the
method under test). In general, the measured value \( \hat{t}_{m,i} \) is affected by two distinct sources of error, namely clock error and measurement noise:

\[
\hat{t}_{m,i} = t_{m,i} + \xi_i(t_m) + \epsilon_{m,i}.
\]

The term \( \xi_i(t_m) \) models the clock error between the receiver clock and the absolute time reference, and can be modeled by a slowly-varying function of time. Its magnitude depends on the hardware characteristics of the device, and specifically on the stability of the local oscillator.

The term \( \epsilon_{m,i} \) represents the measurement noise in the TOA estimation process and is modeled by a random variable with zero mean and variance \( \sigma^2_{\text{TOA}} \). The precision of the TOA estimate, defined as the reciprocal of the noise variance, is independent of the clock error. The goal of the present study is to reduce \( \sigma^2_{\text{TOA}} \). The problem of counteracting the clock error component remains outside the scope of the present contribution. Here it suffices to mention that the clock error can be mitigated by adopting receivers with GPS Disciplined Oscillators (GPSDO), or it can be estimated and compensated in post-processing [7–9].

Hereafter we illustrate the methodology to experimentally quantify the empirical TOA standard deviation \( \sigma_{\text{TOA}} \), notwithstanding the presence of a non-zero clock error component. First, we need to get rid of the unknown true absolute arrival time \( t_{m,i} \) in Equation (2). Since we use two identical receivers attached to the same antenna, we can set \( t_{m,1} = t_{m,2} = t_m \) and subtract the TOA measurements at the two sensors to obtain the corresponding time difference:

\[
\Delta t_m = \hat{t}_{m,2} - \hat{t}_{m,1} = \Delta \xi(t_m) + \Delta \epsilon_m
\]

wherein \( \Delta \xi(t) \equiv \xi_2(t) - \xi_1(t) \) denotes the compound clock error, and \( \Delta \epsilon_m \equiv \epsilon_{m,2} - \epsilon_{m,1} \) the compound measurement error with variance \( \sigma^2_{\Delta \epsilon} = 2 \sigma^2_{\text{TOA}} \). At short time-scales, within the coherence time of the process \( \Delta \xi(t) \), the clock error represents a systematic error, i.e. a bias term that can be estimated and removed in order to estimate the error variance \( \sigma^2_{\Delta \epsilon} \). We do so by modeling the slowly-varying function \( \Delta \xi(t) \) by a polynomial whose coefficients are estimated by standard order-recursive Least Squares (refer to [14, Chapter 8] for details). After removing the estimated clock error component, we obtain a set of residuals \( \{\Delta \epsilon\} \). Their Mean Square Error (MSE) represents an empirical estimate of twice the TOA variance \( \text{MSE}_{\Delta \epsilon} = 2 \cdot \sigma^2_{\text{TOA}} \). Accordingly, their Root Mean Square Error (RMSE) provides a direct empirical estimate of the TOA error standard deviation, formally:

\[
\hat{\sigma}_{\text{TOA}} = \frac{\sqrt{2}}{N_{\text{points}}} \text{RMSE}_{\Delta \epsilon} \approx 0.7 \cdot \text{RMSE}_{\Delta \epsilon}.
\]

5 NUMERICAL RESULTS

We now present the results on the precision of the different TOA estimation methods as evaluated in our testbed.
The latter matches more closely the pulse shape passed through the ECDF of the residuals 
values of the TOA error standard deviation \( \hat{\sigma}_{\text{TOA}} \) indicate that should be preferred when computation load is not of concern. For these, it is convenient to consider the rectangular pulse shape with binary 0/1 values, due to lower computation load. Referring to Fig. 5(a), we observe that the proposed PeakPulse algorithm achieves a \( \text{RMSE}_{\Delta \epsilon} \) of 3.15 ns, less than half the value of the canonical CorrPacket/R method. It is remarkable that such good result was obtained with no cross-correlation operation. Fig. 6 shows \( \hat{\sigma}_{\text{TOA}} \) for different values of the upsampling factor \( N \). We observe that the precision of the proposed methods PeakPulse and CorrPacket/R improves faster than CorrPacket/R with increasing \( N \). These results indicate that PeakPulse should be preferred when computation load is at premium.

Next we consider applications that enjoy abundant computation power, for which the main goal is to maximize precision and computation load is not of concern. For these, it is convenient to consider higher upsampling factors (\( N = 83 \) in our case) and, for the cross-correlation methods, the more elaborated "Smoothed" pulse shape. The latter matches more closely the pulse shape passed through the RTL-SDR front-end, leading to slightly higher precision than the simpler "Rectangular" shape, as can be verified from Table 1. The ECDF of the residuals \( \Delta \epsilon \)'s for these methods are plotted in Fig. 5(b). It can be seen that the proposed CorrPulse/S method is more precise than the classical CorrPacket/S method, and achieves \( \text{RMSE}_{\Delta \epsilon} = 2.16 \) ns corresponding to \( \hat{\sigma}_{\text{TOA}} = 1.51 \) ns.

5.2 Error vs. signal strength
In the following, we investigate the impact of signal strength on the TOA error obtained with the most precise method, namely CorrPulse/S with \( N = 83 \). For a generic packet \( m \) and sensor \( i \), we denote by \( \gamma_m \), the average of the squared pulse height over all pulses – an indicator of the arriving packet strength. Furthermore, we denote by \( \beta_{m,i} \) the number of pulses that are clipped in the receiver due to one or more of the corresponding IQ samples saturating the ADC.

\[
\gamma_m = \frac{1}{N_{\text{packets}}} \sum_{i} \sum_{m} \gamma_{m,i}, \quad \beta_{m,i} = \text{number of clipped pulses}, \quad \hat{\sigma}_{\text{TOA}}(m) = \text{TOA error for packet } m.
\]

Table 1: Empirical estimates of TOA error standard deviation \( \hat{\sigma}_{\text{TOA}} \).

<table>
<thead>
<tr>
<th>estimation method</th>
<th>( \hat{\sigma}_{\text{TOA}} )</th>
<th>nanoseconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>legacy dump1090</td>
<td>all packets</td>
<td>L</td>
</tr>
<tr>
<td>45.20</td>
<td>44.94</td>
<td>45.19</td>
</tr>
<tr>
<td>SenSys'17, ( N = 25 )</td>
<td>5.90</td>
<td>6.11</td>
</tr>
<tr>
<td>CorrPacket/R, ( N = 25 )</td>
<td>4.98</td>
<td>5.48</td>
</tr>
<tr>
<td>CorrPacket/R, ( N = 83 )</td>
<td>2.14</td>
<td>3.04</td>
</tr>
<tr>
<td>CorrPacket/S, ( N = 83 )</td>
<td>2.07</td>
<td>3.00</td>
</tr>
<tr>
<td>CorrPacket/R, ( N = 25 )</td>
<td>1.89</td>
<td>2.75</td>
</tr>
<tr>
<td>CorrPacket/R, ( N = 83 )</td>
<td>1.63</td>
<td>2.72</td>
</tr>
<tr>
<td>CorrPacket/S, ( N = 83 )</td>
<td>1.51</td>
<td>2.60</td>
</tr>
<tr>
<td>PeakPulse, ( N = 25 )</td>
<td>2.20</td>
<td>3.36</td>
</tr>
<tr>
<td>PeakPulse, ( N = 83 )</td>
<td>2.12</td>
<td>3.44</td>
</tr>
</tbody>
</table>

In Fig. 7, we plot for each individual packet \( m \) the absolute value of the residual error \( |\Delta \epsilon_m| \) obtained with CorrPulse/S (\( N = 83 \)) against the mean signal strength between the two sensors \( \gamma_m \). Each packet is classified into one of three classes: packets with \( \gamma_m \leq 0.04 \) are labeled by "L", packets with \( \min(\gamma_{m,i}, \beta_{m,i} \geq 10 \) are labeled with "H", and all remaining packets are labeled with "M". The three classes are marked respectively with black, red and blue markers in Fig. 7. The estimated TOA error standard deviation obtained by each method for each class are reported in Table 1. On one extreme, timing estimates for "L" packets with lower strength are impaired by quantization noise. On the other extreme, packets received with high strength are subject to ADC clipping, a form of distortion that clearly degrades timing precision. As expected, these two classes yield higher error with all methods. Between the two extremes, the strength of "M" packets fits well the dynamic range: for these, the proposed method achieves \( \hat{\sigma}_{\text{TOA}} = 0.79 \) ns.

In our traces, less than 60% of all packets fall into class "M". With better hardware, and specifically with more ADC bits and larger dynamic range, it would be possible to tune the AGC gain so as to increase the fraction of packets falling in this class, thus improving the overall precision.

The above results indicate that the received packet metrics \( \gamma_{m,i} \) and \( \beta_{m,i} \) can be used to provide, for each individual TOA measurement \( t_{m,i} \), an indicator of the expected precision, i.e., of...
We have presented two variants of a novel TOA estimation method within the dynamic range of the receiver, the PeakPulse method has been implemented in C, integrated in the dump1090 receiver and is released as open-source.

ACKNOWLEDGMENTS
This work has been funded in part by the Madrid Regional Government through the TIGRES-CM program (S2013/ICE-2919). We would like to thank Manuel Eichelberger from ETH Zurich for sharing the code we used in our evaluation for comparison purposes.

REFERENCES