A wireless TDOA estimation architecture using software-defined radios

F. Quitin, C. Cheng, M. Leng and W.P. Tay

***Abstract*—Localization of non-cooperative wireless sources can be achieved by using time-difference-of-arrival (TDOA) estimation. The difficulty of implementing wireless TDOA estimation architectures is due to the stringent synchronization requirements, where the clocks of the different sensor nodes must be synchronized within a few tens of nanoseconds to achieve reasonable accuracy. In this paper, we propose an all-wireless relaying architecture for TDOA estimation. We show that, with our architecture, non-zero time offsets between the different nodes are canceled out, provided the clock skews are reasonably low. Implementation results suggest that our architecture is able to achieve the expected accuracies, both in controlled and outdoor environments.**

I. Introduction

In localizing a non-cooperative RF target emitter, the sensors need to rely on angle-of-arrival information (in the case of multi-antenna sensors) or time-difference-of-arrival (TDOA) information, where the difference in propagation times between the transmiting target and two sensor nodes is estimated. TDOA localization has attracted a lot of attention in prior works, yet very few practical implementation can be found in literature. This is mostly due to the stringent requirement for very accurate synchronization between the different nodes: to achieve accuracies around 10 m, the clocks of the different sensor nodes need to be synchronized within a few tens of nanoseconds. Conventional wisdom suggests to use the Global Positioning System (GPS) to synchronize the different local oscillators (LOs). At its best, the accuracy of GPS synchronization is as low as 30 ns, but in GPS-degraded environments this error can be as high as 100 ns, which leads to TDOA estimation errors that result in localization errors up to 60 m. In this paper, we propose an architecture for TDOA estimation that does not require GPS synchronization, and that offers accuracy better than what can be obtained with GPS synchronization. We validate our architecture with a software-defined radio implementation, and provide test results for an outdoor experiment.

Related work: Localization techniques based on TDOA have been extensively investigated, ranging from a few decades back [1]–[3] to the present [4]–[9]. Several TDOA-based prototypes have been implemented for acoustic networks [10]–[14], however, very few papers discuss practical implementations for wireless networks. This is due to the stringent synchronization requirements: acoustic signals have a propagation speed of approximately 340 m/s, hence one can use wireless signals to synchronize the different oscillators. For wireless signals, the propagation speed requires the clocks to be synchronized within a few tens of nanoseconds, which makes implementation much more challenging. In [15], [16], the authors synchronize the oscillators and clocks of the different nodes using external GPS units (in [15] the external GPS unit is implemented with a software-defined radio). The obtained accuracy is highly dependent on the GPS availability and amount of GPS obstruction, but can be as good as 50 ns. In both papers, the data needs to be transferred and processed offline for TDOA recovery and localization.

Contributions: In this paper, we propose a practical system design for the localization of a non-cooperating RF source using TDOA between different sensor nodes. Our architecture allows for non-zero clock offset and (limited) clock skew between the different sensor nodes. The sensors are not explicitly synchronized, and the TDOA estimation instead relies on a relaying technique that does not require GPS, but achieves time accuracy better than synchronization using GPS. We investigate the estimation error of the proposed architecture, and provide practical bounds and limits for our design. The proposed architecture is implemented and validated on a software-defined radio testbed. Unlike most TDOA implementations, our implementation does not require any off-line data collection and processing, and allows for real-time operation and localization. Implementation issues are discussed, and experimental results are presented and analyzed.

II. System architecture

A. TDOA estimation architecture

Suppose that we have $N+1$ sensor nodes that want to measure the TDOA of signals from a non-cooperative RF source transmitting an unknown signal $x(t)$. Consider the scenario in which one of the nodes, which we assume without loss of generality to be node $N+1$ and which we designate as the receiver node, wants to compute the TDOA of the received signals at all nodes with respect to (w.r.t.) each other. We call the other N nodes the relay nodes. At some commonly agreed upon time T_0, all $N+1$ nodes sampling the signal received from the RF source over the frequency band f_1 for a predefined duration. This can be done by using a beacon message from one of the sensor nodes to trigger all the nodes, or can be preprogrammed into the sensor nodes. However because of the difference in distances of the beacon to each

F. Quitin, C. Cheng, M. Leng and W.P. Tay are with the School of Electrical and Electronic Engineering, Nanyang Technological Unviersity, Singapore (fquitin@ntu.edu.sg)

node or because of clock offsets in the local clocks of the nodes, the times T_{0i} at which each node i start recording the message from the RF source may be different for different nodes. Even when synchronized with GPS, the time offset between nodes can still be as large as 100 ns, depending on the quality of the GPS satellite constellation. In the following section we will see how our architecture compensates for the time offset between the different nodes. Once the nodes are finished sampling the signal from the RF source, each relay node will forward its recorded samples to the receiver node after a predefined time T_{Di} over the frequency band f_2. To avoid packet collisions, we devise a TDMA scheme where each relay forwards its recorded message to the receiver in its allocated timeslot. Finally, the receiver uses the samples from the different relays along with its own recorded samples to perform cross-correlation and estimate the TDOA between the different sensor nodes.

In the next subsection that we show that, if the relay delay time T_{Di} is accurate, the recording starting time T_{0i} of each relay node does not matter and is compensated for in our architecture. We will also show, both theoretically and experimentally, that limited clock skews does not affect the TDOA estimation of our architecture.

B. Timing of received signals

Let $x(t)$ be the signal transmitted from the non-cooperating RF source. The received signal at the i-th relay is then given by $r_i(t) = x(t-\tau_{i1})$ where τ_{i1} is the propagation delay between the RF source and the i-th relay, and we have omitted noise and channel gains for readability. The relay will start sampling the received signal at time T_{0i} (which differs slightly for each relay) to obtain as the lth sample,

$$r_i[l] = x(T_{0i} + \beta_i l T_s - \tau_{i1})$$

where T_s is the sample rate, and β_i is the clock skew of the i-th relay. Each relay will wait for its alloted time slot before forwarding the message to the final receiver. The transmitted message from each relay is then given by

$$t_i(t) = \sum_{l=-\infty}^{\infty} x(T_{0i} + \beta_i l T_s - \tau_{i1}) \cdot u(t - \beta_i l T_s - T_{0i} - \beta_i T_{Di})$$

where T_{Di} is the retransmission delay of the i-th relay, and $u(t)$ is the pulse shaping filter of the relay. The receiver will start sampling the message from relay i at time $T_{0R} + \beta_R T_{Di}$, where β_R is the clock skew of the final receiver. The nth sample of the signal received from relay i at the final receiver can be written as

$$r_R^{(i)}[n] = \sum_{l=-\infty}^{\infty} x(T_{0i} + \beta_i l T_s - \tau_{i1}) \cdot g(T_{0R} + \beta_R T_{Di} + \beta_R n T_s - \beta_i l T_s - T_{0i} - \beta_i T_{Di} - \tau_{i2}) \quad (1)$$

where τ_{i2} is the propagation delay between the i-th relay and the final receiver, and $g(t) = u(t) * u'(t)$ with $u'(t)$ being the pulse shaping filter at the receiver. If the pulse shaping filters are chosen appropriately and inter-symbol interference is canceled, we have $g(t) = \delta(t)$ where $\delta(t)$ is the Dirac function. In that case, (1) can be simplified to

$$r_R^{(i)}[n] = x(T_{0R} + (\beta_R - \beta_i) T_{Di} + \beta_R n T_s - \tau_{i2} - \tau_{i1}) \quad (2)$$

If the clock skew equals one, i.e., $\beta_R = \beta_i = 1$, then (2) simplifies to

$$r_R^{(i)}[n] = x(T_{0R} + n T_s - \tau_{i2} - \tau_{i1})$$

which is independent of the relay measurement time T_{0i}. For different nodes (which forward their samples with different delays), the received samples at the receiver node will have identical offset T_{0R}. The proposed architecture can thus successfully cancel out differences in node measurement time offsets if all clock skews are unity. The receiver then computes the ambiguity functions between the received messages $r_R^{(i)}[n]$ and $r_R^{(j)}[n]$ from nodes i and j. The index of the peak of the ambiguity function is equal to $\tau_{i2} + \tau_{i1} - \tau_{j2} - \tau_{j1}$. If τ_{i2} and τ_{j2} are known, the receiver can recover the original TDOA $\tau_{i1} - \tau_{j1}$.

C. TDOA estimation error

As seen from (2), clock skew induces a relay-dependent time offset. The clock skew is a slowly varying parameter, and the TDOA errors of successive measurements will be highly correlated. For a given relay, the TDOA error due to clock skews is given by

$$\varepsilon_\tau = (\beta_R - \beta_i)\, T_{Di} \quad (3)$$

For oven-controlled crystal oscillators (OCXO), the typical accuracy is several tens of parts-per-billion (ppb). The relay delay is typically in the order of tens to hundreds of milliseconds. For a clock accuracy of 25 ppb and a relay delay time of 100 ms, the resulting time error is only 5 ns (corresponding 1.5 m accuracy). In this case, clock skew can be ignored for all practical purposes. For lower quality oscillators, such as temperature-compensated crystal oscillators (TCXO), the clock skew can deviate from unity by as high as several parts-per-million (ppm), leading to errors as large as a few hundred nanoseconds.

We evaluate the TDOA estimation error experimentally with our software-defined radio testbed (described in Section III) when using different types of local oscillators, with only one relay and one receiver. The transmitter is connected with short cables to the relay and the receiver, and the relay forwards its message to the receiver over a short wireless link. The relay and the receiver are placed next to one another, such that the measured TDOA should be zero. The settings of relay and receiver are given in Table I. The setup is ran with various values for the relay delay time T_D, and with two different types of oscillators for both relay and receiver (TCXO and OCXO). Figure 1 shows the TDOA error for various values of T_D. The presented values are averaged over 10 successive measurements. The blue and red line correspond to the first-order best fit of the measured data. It can be seen that, for the OCXO, the error due to clock skew cannot be observed, and is below the resolution accuracy of our setup (which is indicated

TABLE I
EXPERIMENTAL SETUP SYSTEM PARAMETERS

Parameter	Value
RF source frequency	795 MHz
RF source signal bandwidth	1 MHz
Relay/Rx sample rate	10 MHz
Relaying channel frequency	755 MHz
Relay delay T_{Di}	$\{25, 50, 75\}$ ms
Recorded packet length	10 ms

by the black line). In the case of the TCXO, the error due to clock skew is larger than the resolution accuracy, and the TDOA error increases linearly with T_D, as predicted by (3). The term $(\beta_R - \beta_i)$ is equal to $2.79 \cdot 10^{-7}$, which is within the TCXO manufacturing tolerance of 2.5 ppm.

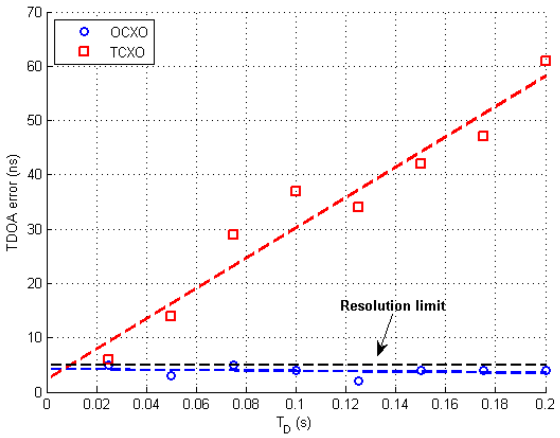

Fig. 1. TDOA error as a function of T_D for two different types of oscillators. For an OCXO, the TDOA error is below the resolution accuracy, but for the TCXO the effect of clock skew can clearly be seen.

III. IMPLEMENTATION ON SOFTWARE-DEFINED RADIO TESTBED

A. Architecture implementation

The architecture of Section II was implemented on a software-defined radio testbed. We used an Agilent signal generator for the non-cooperative transmitter, which transmits a random QPSK-modulated message. The relay nodes consist of USRP-N210 SDRs with WBX daughterboards. The WBX daughterboard permits to receive and transmit on two different frequency bands simultaneously, and the USRP drivers allow for precise timing commands that permit to set the relay delay time T_{Di} with accuracy down to one sample. The receiver node is an USRP-N210 SDR with a TVRX2 daughterboard, which allows the receiver to receive on two different frequency bands simultaneously. The different parameters of the setup are described in Table I.

To trigger the recording at all the relays and receiver more or less simultaneously, all nodes are first connected to GPS such that their internal clocks are set to UTC time. Note that even with the GPS receiver, the time error of the nodes is still as large as ± 100 ns (which for a TDOA measurement correspond to an error of 60 m). Once the node time is aligned to UTC time, the GPS antennas can be disconnected, such that the nodes use their internal clocks to increment time. A measurement is then triggered automatically every 20 seconds. Since the nodes are using their internal clocks, small time offsets will appear between the different nodes. Note that the triggering mechanism is not very critical, as the nodes need not start measuring simultaneously. Another possibility would be to have the receiver broadcast a message to all relays to trigger the measurement. In that case, different propagation delays will cause the relays to start measuring with slight offsets with respect to one another.

The relays and receiver operate at a sample rate of 10 MHz, which allows for a resolution of 100 ns. The messages at the receiver (both from the RF source and from the relays) are oversampled and low-pass filtered to increase the resolution. Since we assume that the waveform of the RF source signal is unknown, it is impossible to create a matched filter at the receiver. Instead, we use a simple low-pass filter to increase the signal resolution, with the filter bandwidth set to match the transmitter signal bandwidth. Our setup must be calibrated to allow for small hardware-specific time offsets when using different T_{Di}. These offsets, however, are fixed and can be calibrated once and for all with a cabled setup.

B. Experimental results

The TDOA estimation setup is first ran in a controlled environment. We use only one relay and one receiver, and the relay-to-receiver link is a short wireless link that accounts for zero-TDOA. The link between the transmitter and the relay uses a short cable, and cables of various lengths are used for the transmitter-to-receiver link. By using cables to connect the transmitter with the relay/receiver, we avoid the problem of multipath (the relay and receiver are placed close to one another, such that the relay-to-receiver link has a very dominant line-of-sight and no multipath either). Figure 2 shows the estimated TDOA for different cable lengths. For each cable length, ten measurements were taken, and the results in Figure 2 shows the mean and 2σ-spread of the measurements. The measured TDOA is compared with the TDOA that is obtained by measuring the cable delays with a vector network analyzer (VNA), which serves as a reference. It can be seen that all measurements are within 10 ns of the reference measurement, which is the resolution limit of our setup. It can be concluded that, in a controlled environment without multipath, a TDOA accuracy as low as 10 ns can be achieved with our architecture.

Figure 3 show an experimental result for a full-wireless setup with three relay nodes and one receiver. For each transmitter location, ten successive TDOA measurements were taken, separated by 10 seconds. The nodes are placed such that there is a dominant LOS between the transmitter and each relay node, and between the relay nodes and the receiver nodes. However, the LOS is sometimes obstructed by the foliage of a tree or by people passing by during the experiment. With four nodes we have a total of six TDOAs between nodes, and each TDOA describes a hyperbole between the

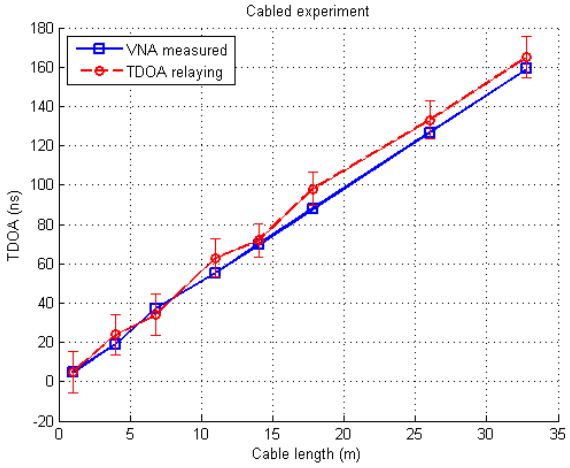

Fig. 2. Measured TDOA for a cabled setup with different cable lengths. The real TDOA, measured with a VNA, is shown for reference.

two corresponding nodes. The hyperboles corresponding to one transmitter location (and 10 successive measurements) are shown in Figure 3, where each color corresponds to a different pair of nodes. It can be seen that successive measurements might yield slightly different results, and the different hyperboles intersect close to the transmitter's location. The

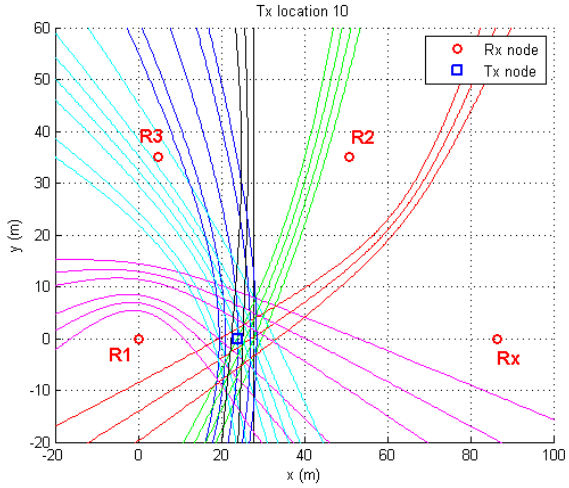

Fig. 3. Hyperboles corresponding to the TDOAs measured with three relay nodes and one receiver. The blue lines correspond to the TDOA between Rx and R1, the red lines between RX and R2, the green lines between Rx and R3, the cyan lines between R1 and R2, the magenta lines between R1 and R3, and the black lines between R2 and R3.

transmitter was moved to 9 different locations, on a line between Rx and R1. The transmitter locations are separated by 5 m. At each location, ten TDOA measurements were taken, each separated by 10 s. The overall TDOA error has a mean of -2 ns and a standard deviation of 28 ns. This error is attributed mostly to multipath-induced errors: when the LOS is obstructed by foliage or people, the multipath components have a larger influence on the TDOA estimation and can easily induce errors in the TDOA estimation. However, in over two thirds of the measurement, the error is below 30 ns (which corresponds to an error of 10 m).

IV. Conclusion

In this paper we have presented a novel wireless TDOA estimation architecture. By having each node forward its samples to a receiver node, the time offset between different nodes is canceled out. Such an architecture permits to have a TDOA error that is lower than when using GPS-synchronized nodes, especially in GPS-degraded environments. Our implementation on a software-defined radio testbed showed that such an architecture can achieve errors below 10 ns in controlled environments, and errors with zero-mean and a standard deviation of 30 ns in outdoor environments.

References

[1] C. Knapp and G. C. Carter, "The generalized correlation method for estimation of time delay," *Acoustics, Speech and Signal Processing, IEEE Transactions on*, vol. 24, no. 4, pp. 320–327, Aug 1976.

[2] G. Jacovitti and G. Scarano, "Discrete time techniques for time delay estimation," *Signal Processing, IEEE Transactions on*, vol. 41, no. 2, pp. 525–533, Feb 1993.

[3] Y. Chan and K. Ho, "A simple and efficient estimator for hyperbolic location," *Signal Processing, IEEE Transactions on*, vol. 42, no. 8, pp. 1905–1915, Aug 1994.

[4] T. Sathyan, A. Sinha, and T. Kirubarajan, "Passive geolocation and tracking of an unknown number of emitters," *Aerospace and Electronic Systems, IEEE Transactions on*, vol. 42, no. 2, pp. 740–750, April 2006.

[5] K. Ho, X. Lu, and L. Kovavisaruch, "Source localization using tdoa and fdoa measurements in the presence of receiver location errors: Analysis and solution," *Signal Processing, IEEE Transactions on*, vol. 55, no. 2, pp. 684–696, Feb 2007.

[6] G. Mao, B. Fidan, and B. D. O. Anderson, "Wireless Sensor Network Localization Techniques," *Comput. Netw.*, vol. 51, no. 10, pp. 2529–2553, Jul. 2007. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2006.11.018

[7] G. Wang and H. Chen, "An Importance Sampling Method for TDOA-Based Source Localization," *Wireless Communications, IEEE Transactions on*, vol. 10, no. 5, pp. 1560–1568, May 2011.

[8] G. Wang, Y. Li, and N. Ansari, "A semidefinite relaxation method for source localization using tdoa and fdoa measurements," *Vehicular Technology, IEEE Transactions on*, vol. 62, no. 2, pp. 853–862, Feb 2013.

[9] K. H. Choi, W.-S. Ra, J. B. Park, and T. S. Yoon, "Compensated robust least-squares estimator for target localisation in sensor network using time difference of arrival measurements," *Signal Processing, IET*, vol. 7, no. 8, pp. 664–673, October 2013.

[10] K. Frampton, "Acoustic self-localization in a distributed sensor network," *Sensors Journal, IEEE*, vol. 6, no. 1, pp. 166–172, Feb 2006.

[11] T. Damarla, L. Kaplan, and G. Whipps, "Sniper Localization Using Acoustic Asynchronous Sensors," *Sensors Journal, IEEE*, vol. 10, no. 9, pp. 1469–1478, Sept 2010.

[12] J. Isaacs, S. Venkateswaran, J. Hespanha, U. Madhow, J. Burman, and T. Pham, "Multiple event localization in a sparse acoustic sensor network using UAVs as data mules," in *Globecom Workshops (GC Wkshps), 2012 IEEE*, Dec 2012, pp. 1562–1567.

[13] C. Steffes and L. Meyer, "Evaluation of a tdoa based acoustic localization system," in *Sensor Data Fusion: Trends, Solutions, Applications (SDF), 2013 Workshop on*, Oct 2013, pp. 1–4.

[14] X. Zhong, A. Mohammadi, W. Wang, A. Premkumar, and A. Asif, "Acoustic source tracking in a reverberant environment using a pairwise synchronous microphone network," in *Information Fusion (FUSION), 2013 16th International Conference on*, July 2013, pp. 953–960.

[15] J. Bhatti, T. Humphreys, and B. Ledvina, "Development and demonstration of a TDOA-based GNSS interference signal localization system," in *Position Location and Navigation Symposium (PLANS), 2012 IEEE/ION*, April 2012, pp. 455–469.

[16] N. El Gemayel, S. Koslowski, F. Jondral, and J. Tschan, "A low cost TDOA localization system: Setup, challenges and results," in *Positioning Navigation and Communication (WPNC), 2013 10th Workshop on*, March 2013, pp. 1–4.