An over-the-air CFO-assisted synchronization algorithm for TDOA-based localization systems

Zohreh Ebadi*, Cédric Hannotier*, Heidi Steendam†, François Horlin* and François Quitin*
* Brussels School of Engineering, Université libre de Bruxelles (ULB), Brussels, Belgium
† TELIN/IMEC, Ghent University, Ghent, Belgium
Email: zohreh.ebadi@ulb.ac.be

Abstract—Time-difference-of-arrival (TDOA) localization systems estimate the difference in propagation delay between a target transmitter and pairs of receivers in order to locate the target. One important requirement is that the receiver nodes should be accurately time-synchronized, which is hard to achieve in practice without relying on cable-connected receivers. Over-the-air synchronization algorithms often rely on periodic messages from a master node, but due to clock drift, the rate of these messages needs to be high. In this paper, we propose a new synchronization algorithm that additionally exploits the carrier frequency offset (CFO) between the target node and the receiver nodes to reduce the rate of messages from the master node while maintaining good synchronization accuracy. Simulation results show the good performance of the proposed method, and preliminary experimental results show its feasibility on a hardware platform.

Index Terms—Localization, TDOA, synchronization, CFO

I. Introduction

Localization of radio-frequency transmitters is an increasingly important topic in wireless communications [1]. TDOA-based localization is based on estimating the difference in propagation delay between a transmitter and a pair of receivers, which creates a hyperbole of possible transmitter locations. TDOA-based localization offers several advantages: the transmitter does not need to be cooperative (i.e. its exact waveform does not need to be known), and the transmitter does not need to be synchronized to the receivers [1], [2]. The major drawback of TDOA localization systems is that the different receivers need to be accurately time-synchronized, which is hard to achieve in practice. Transceivers derive their internal time from their internal local oscillator (LO), which have non-zero offsets w.r.t. one another (mainly due to manufacturing tolerances and slight temperature variations) [2]. These LO offsets result in clock offset and clock skew, which represent the offset and the rate of variation of a receiver clock w.r.t. a reference clock.

Receiver node synchronization can broadly be classified into wired and wireless methods. Wired synchronization methods (such as [3]) rely on distributing a central clock signal to all the receiver nodes through cables, which is expensive and impractical in wireless systems [3], [4]. One attractive wireless synchronization method is global navigation satellite system (GNSS) based synchronization. GNSS systems provide access to a precise universal time coordinated (UTC) time reference, which can be used for disciplining a LO. However, such a synchronization is highly dependent on GNSS availability, with accuracies going from 50 nanoseconds to hundreds of nanoseconds depending on satellite visibility [4]. Other wireless synchronization methods are based on master-slave architectures, in which a master node distributes an over-the-air reference signal to the slave nodes (i.e. the receiver nodes for a TDOA localization system) [5]–[8]. The basic idea of master-slave synchronization is to frame the time-of-arrival (TOA) of the messages from the target node in the master clock reference by using the messages from the master node. For this method to work, the master needs to send out messages at a high rate to achieve sufficient accuracy [9].

In this paper, we propose a new method to 1) synchronize the receiver nodes of a TDOA localization system using transmissions from a master node, and 2) estimate the TDOA of a target node. Our synchronization method is based on the realization that the time skew that occurs between a transmitter and receiver is directly proportional to the carrier frequency offset (CFO) between this transmitter and receiver [10]. By estimating the CFO between the target node and the receivers and using it appropriately, we can get a more tightly synchronized network of receivers for a TDOA-based localization system, thereby allowing a much reduced rate of messaging from the master node.

Contributions: The contributions of this paper are summarized as follows:

- we propose a CFO-assisted synchronization algorithm to estimate the TDOA of a target node;
- the proposed algorithm is evaluated and validated through simulations;
- a preliminary experiment is performed to validate the proposed method on a software-defined radio platform.

The significance of our work lies in the fact that our synchronization algorithm requires no hardware modification of existing transceiver integrated circuits (ICs). It relies on information that is readily available in such ICs (such as the TOA and the CFO of a packet), thus allowing for tight synchronization of a TDOA-based localization system without expensive hardware or low-level software modifications.

The remainder of the paper is organized as follows. Section II explains the system model considered in this paper. Section III presents the CFO-assisted synchronization algorithm and resulting TDOA estimation algorithm. The simulation
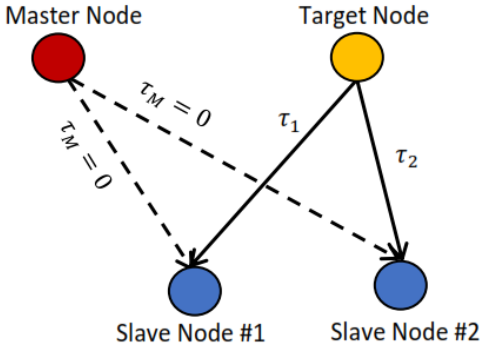
Fig. 1. System model architecture. The propagation delay between the master and the slaves are assumed to be compensated.

Fig. 2. Receiver architecture.

results are discussed in Section IV. Finally, the preliminary experiments are presented and evaluated in Section V.

II. SYSTEM MODEL

In this section, we first describe the master-slave architecture that is used in this paper, and then we discuss the LO clock model.

A. System Architecture

Let us consider the following simplified system model (as shown in Figure 1) where two receiver nodes try to estimate the TDOA of a target transmitter. The receivers are called slave nodes and the target transmitter is referred to as the target node. A master transmitter node sends out periodic synchronization messages. In practice, the slave nodes and the master node can be the base stations. Also, the target node can be the cell phone. Although this paper will focus on two slave nodes, the results of this work can easily be extended to an arbitrary number of slaves. Without loss of generality, we assume that the propagation delay between the master and the slave nodes is zero[1]. The propagation delay between target node and the i-th slave node is referred to as τ_i. In the following, we will assume that there is a collision avoidance mechanism implemented such that packets of the target node and the master node do not collide.

B. LO Model

Let us assume the i-th slave node with a receiver architecture as depicted in Figure 2. The slave is equipped with a non-ideal LO that has a normalized frequency $1 + \varepsilon_i$, with ε_i the normalized frequency offset. A transceiver "counts" time by counting the internal ADC ticks. Since the ADC is driven by the non-ideal LO, it's sampling frequency will be $f'_{si} = f_s + \Delta f_{si} = (1 + \varepsilon_i) f_s$, where f_s is the nominal sampling frequency. Therefore, the time as seen by the i-th slave node is given by

$$t_i = \theta_i + \beta_i t \qquad (1)$$

[1]Since the master and the slave nodes are part of the infrastructure, we assume that the propagation delay between the master and the slaves can be estimated or is known a priori. As a consequence, it can easily be compensated in our algorithm.
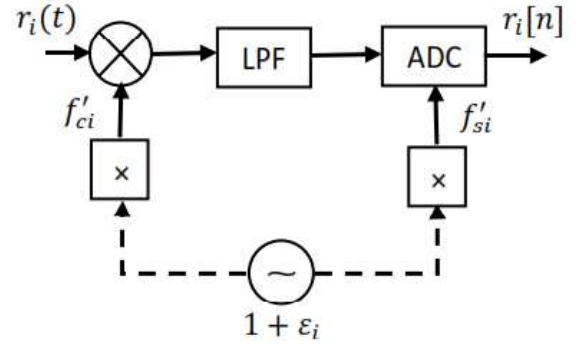
where θ_i, the absolute clock offset of slave node i, corresponds to the time that the slave node is turned on, and β_i is the clock skew of slave node i, defined as:

$$\beta_i = \frac{1}{1 + \varepsilon_i} \approx 1 - \varepsilon_i \qquad (2)$$

Without loss of generality, we will assume in this paper that the master node has "reference" time, so that equation (1) contains the clock drift of the i-th slave w.r.t. the master node.

In a practical receiver, the same LO is used to generate carrier frequency and sampling frequency [10]. Since the LO also drives the down-converter, the carrier frequency generated at the mixer is not equal to the nominal carrier frequency f_c, but rather to $f'_{ci} = f_c + \Delta f_{ci} = (1 + \varepsilon_i) f_c$, where Δf_{ci} is denoted the CFO. The CFO of a receiver is expressed w.r.t. a reference node, which is in the situation at hand the master node. Since the ADC and the down-converter are both driven by the same LO, we can state that

$$\varepsilon_i = \frac{\Delta f_{ci}}{f_c} = \frac{\Delta f_{si}}{f_s} \qquad (3)$$

This link between the CFO and the time skew of a receiver will be further exploited in our CFO-assisted synchronization algorithm in Section III.

III. CFO-ASSISTED SYNCHRONIZATION

A. TDOA estimation without synchronization

Let us start by considering what happens if two receiver nodes are not synchronized. If the target sends a message at time t^T, the TOA of this message at slave i is given by

$$t_i^T = \theta_i + \beta_i t^T + \tau_i \qquad (4)$$

The TDOA τ_{ij} between slave nodes i and j is given by

$$\tau_{ij} = t_i^T - t_j^T \qquad (5)$$
$$= \tau_i - \tau_j + (\theta_i - \theta_j) + (\beta_i - \beta_j) t^T \qquad (6)$$

We can see that the TDOA error is composed of a constant term $(\theta_i - \theta_j)$, as well as a term $(\beta_i - \beta_j) t^T$ that increases with time. Messages sent out by the target at later time instants t^T will have higher error, as the synchronization mismatch between the different receivers increases due to the clock skews of the slave nodes.

B. Conventional master-slave synchronization

In this section, we describe conventional master-slave synchronization algorithms, on which we will build our CFO-assisted synchronization. Let us assume that the master node and target send messages at times t^M and t^T, respectively. The TOA of the target message is given by (4), while the master message is received by slave i at time

$$t_i^M = \theta_i + \beta_i t^M \qquad (7)$$

Conventional synchronization is performed by putting the TOA of the target node at slave i in the master's reference frame as follows:

$$\tilde{t}_i^T = t_i^T - t_i^M \qquad (8)$$
$$= \tau_i + \beta_i \left(t^T - t^M \right) \qquad (9)$$

The TDOA τ_{ij} between two slave nodes i and j is then given by

$$\tilde{\tau}_{ij} = \tilde{t}_i^T - \tilde{t}_j^T \qquad (10)$$
$$= \tau_i - \tau_j + (\beta_i - \beta_j) \left(t^T - t^M \right) \qquad (11)$$

It can be seen that the time offsets θ_i and θ_j were canceled out, but that the term due to the clock skews is still present. As a consequence, in conventional synchronization, the TDOA will only be accurate if $\left(t^T - t^M \right)$ is small. In other words, the TDOA error will be negligible only if the time between the target message and the last master message is small.

C. CFO-assisted synchronization algorithm

In this section, we propose a method to get rid of the remaining drift term in equation (11), so that synchronization accuracy will hold even if the time elapsed since the last message from the master node increases. This will allow to greatly reduce the amount of master messages, thereby reducing the communication bandwidth required for synchronization. To apply CFO-assisted synchronization, we use a compensated TOA at each slave node i:

$$\hat{t}_i^T = \left[t_i^T - t_i^M \right] \left(1 + \frac{\Delta f_{ci}^T}{f_c} \right) \qquad (12)$$

where Δf_{ci}^T is the CFO of received signal at slave i w.r.t. the target node. By using (4), (7) and (3), this can be rewritten as

$$\hat{t}_i^T = \left[\tau_i + \beta_i \left(t^T - t^M \right) \right] \left(1 + \varepsilon_i^T \right) \qquad (13)$$

where ε_i^T is the normalized LO offset of slave i w.r.t. the target node, i.e. $\varepsilon_i^T = \varepsilon_i - \varepsilon_T$, with ε_T the normalized frequency offset of the target node w.r.t the reference. By using (2), this can be rewritten as

$$\hat{t}_i^T \approx \left[\tau_i + (1 - \varepsilon_i) \left(t^T - t^M \right) \right] \left(1 + \varepsilon_i^T \right) \qquad (14)$$

The previous expression can be simplified by observing that the terms ε_i and ε_i^T are in the order of parts-per-million (ppm), while the terms τ_i are at most in the order of microseconds.

Therefore, the terms $\varepsilon_i^T \tau_i$ and $\varepsilon_i \varepsilon_i^T \left(t^T - t^M \right)$ can be neglected w.r.t. the other terms. The previous expression can then be simplified as

$$\hat{t}_i^T \approx \tau_i + (1 - \varepsilon_i) \left(t^T - t^M \right) + \varepsilon_i^T \left(t^T - t^M \right) \qquad (15)$$

Since $\varepsilon_i^T = \varepsilon_i - \varepsilon_T$, this can be further simplified to

$$\hat{t}_i^T \approx \tau_i + (1 - \varepsilon_T) \left(t^T - t^M \right) \qquad (16)$$

The TDOA $\hat{\tau}_{ij}$ between two slave nodes i and j can then be obtained as

$$\hat{\tau}_{ij} = \hat{t}_i^T - \hat{t}_j^T = \tau_i - \tau_j , \qquad (17)$$

which no longer depends on the LO offset or the LO skews. The CFO-assisted TDOA estimation is thus able to obtain accurate TDOAs based on a master-slave architecture, even if some time has elapsed since the last master message. Intuitively, it can be understood that the master message is used to cancel the time offset between the different slave nodes (i.e. θ_i and θ_j in (7)), while the CFO term in (12) (i.e. the term $\frac{\Delta f_{ci}^T}{f_c}$) is used to predict and cancel out the clock skew that occurs between the slave nodes.

Note that in order to use (12), t_i^T, t_i^M, and Δf_{ci}^T should be estimated. So, in practice (12) is affected by the estimator error. Also, the proposed method also works if the CFO-compensated TOA in (12) uses the CFO of the slave w.r.t. the master node, i.e. Δf_{ci} instead of Δf_{ci}^T.

IV. SIMULATION RESULTS

A. Simulation setup

Simulations were conducted to evaluate the performance of the CFO-assisted synchronization algorithm. The simulated setup is based on the master-slave architecture of Figure 1, with two slave nodes. The propagation delays between the target and both slave nodes are equal to $\tau_1 = 1$ μs and $\tau_2 = 3$ μs, respectively (yielding a theoretical TDOA of $\tau_{12} = 2$ μs). The block-diagram of a transmitter and receiver is shown in Figure 3. We consider a communication system that operates at a carrier frequency of 2.6 GHz with a bandwidth of 1.08 MHz, which is up-sampled to 20 MHz. The target and master node periodically transmit long term evolution primary synchronization code (LTE PSC) signals (i.e. a Zadoff-Chu sequence [11]). The receiver estimates the TOA of the received packets before down-sampling, and estimates the CFO using
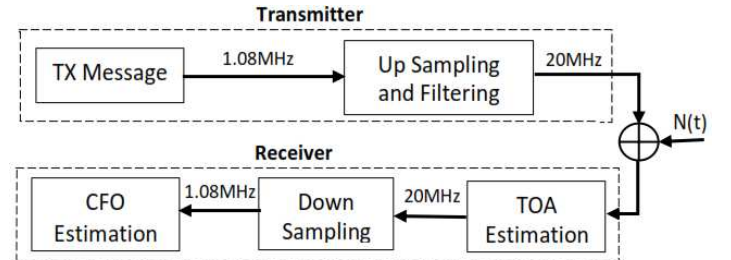

Fig. 3. Block-diagram of our simulation setup.

the received message after down-sampling. The primary synchronization signals (PSS) correlation based method in [11] is used to estimate the CFO. The LO of the different nodes is simulated using the discrete time model from [12], described as follows:

$$\left[\begin{array}{c} \phi[k] \\ \omega[k] \end{array} \right] = \left[\begin{array}{cc} 1 & T_0 \\ 0 & 1 \end{array} \right] \left[\begin{array}{c} \phi[k-1] \\ \omega[k-1] \end{array} \right] + \zeta[k] \qquad (18)$$

where $\phi[k]$ and $\omega[k] = 2\pi\Delta f_c[k]$ are phase and angular frequency offsets at time slot k, respectively. Further, T_0 and $\zeta[k]$ denote the transmit period and process noise, respectively. The covariance matrix $Q = E[\zeta[k]\zeta[k+T_0]]$ of the process noise can be written as

$$Q(T_0) = \omega_c^2 q_1^2 \left[\begin{array}{cc} T_0 & 0 \\ 0 & 0 \end{array} \right] + \omega_c^2 q_2^2 \left[\begin{array}{cc} \frac{T_0^3}{3} & \frac{T_0^2}{2} \\ \frac{T_0^2}{2} & T_0 \end{array} \right] \qquad (19)$$

where $\omega_c = 2\pi f_c$ is the angular carrier frequency. Taking into account [12], the values of process noise parameters q_1^2 and q_2^2 of the temperature compensated crystal oscillator (TCXO) are 8.47×10^{-22} s and 5.51×10^{-18} Hz, respectively.

B. Simulated synchronization results

In the first simulation, we assume that both the target and the master node send a message every 5 ms, i.e. the master messages are sent at a high rate. Figure 4 shows the estimated TDOA value when the nodes are not synchronized (Section III-A) and when they are synchronized using conventional master-slave synchronization (Section III-B). In the case without synchronization, we can see the TDOA error increases over time, as predicted by (6). The conventional synchronization seems to work very well (with a maximum error of plus or minus one sample of the upsampled signal) since the rate of master messages is quite high, thereby annulling the term in (11) containing the effect of time skew.

In the second simulation, the rate of master messages is reduced to one message every 500 ms (while the target still transmits a message every 5 ms). Unlike the previous simulation, it can be seen that the error of conventional synchronization increases over time between two master messages, reaching errors of several hundreds of nanoseconds. The CFO-assisted synchronization, however, is able to keep the TDOA error small, and the estimated TDOA stays close to the real TDOA of 2 μs, even when the time between two master messages is large.

V. Experimental results

A. Experiment setup

The CFO-assisted synchronization was also evaluated on a preliminary experimental setup. The setup is shown in Figure 6. It consists of four USRP-X310 software-defined radios (SDRs), i.e. a master node, a target node and two slave nodes. The target node and master send a 802.11 preamble every 1 ms and 100 ms, respectively. Each transmitting SDR is cable-connected to both slave SDRs (by using RF splitters). The cables are short enough for their delay to be negligible. The LO of the USRPs is a TCXO, with an accuracy of 1
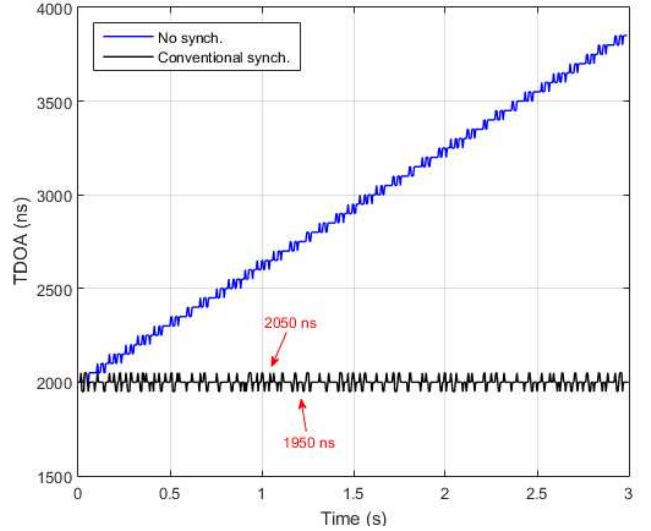

Fig. 4. TDOA without and with (conventional) synchronization, for a high rate of master messages. The real TDOA is 2000 ns.
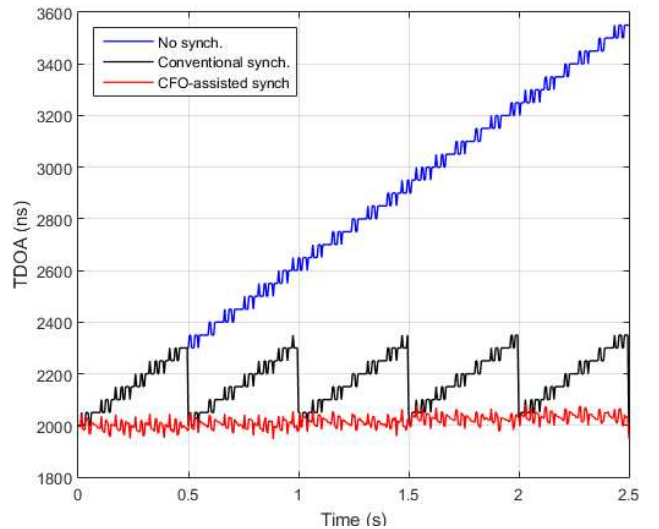

Fig. 5. TDOA without, with conventional and with CFO-assisted synchronization for a low rate of master messages. The real TDOA is 2000 ns.

ppm. The carrier frequency of the USRPs is set to 2.45 GHz, and they all operate at a bandwidth of 20 MHz. The received baseband samples are stored and post-processed offline to extract the TOA and CFO of the received packets.

B. Synchronization results on the hardware testbed

The TOAs and CFOs are estimated using the (known) preamble of the transmitted packets. The TOA resolution is increased by using the parabolic interpolation method described in [13], which allows to have a time resolution beyond the sample rate. Since the cable length is very short, the TDOA should approximately be equal to zero. Similarly to
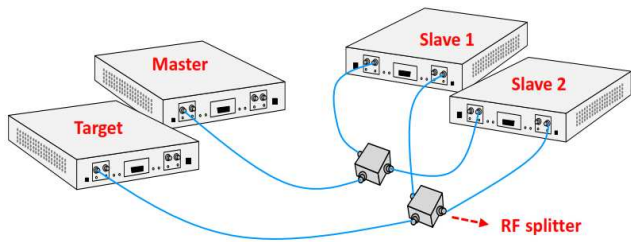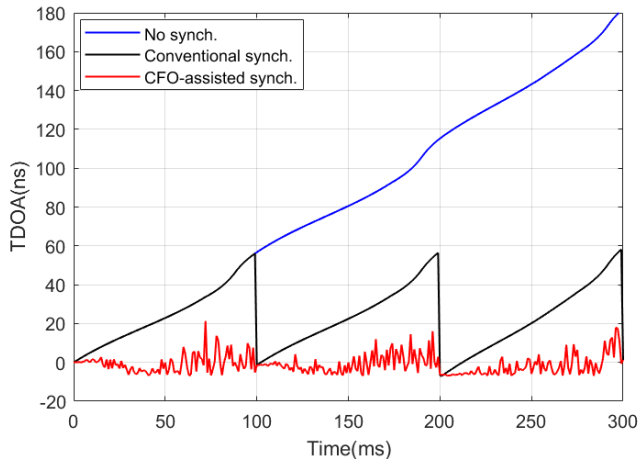
Fig. 6. Experimental setup.

Fig. 7. TDOA without, with conventional and with CFO-assisted synchronization on the hardware testbed.

the simulated results, in the case without synchronization, the TDOA increases to several hundreds of nanoseconds (in just a few hundreds of milliseconds). For conventional master-slave synchronization, we can see in Figure 7 that the TDOA is close to zero right after a message was received from the master, but quickly drifts to tens of nanoseconds after tens of milliseconds. When using the CFO-assisted synchronization, the TDOA remains below 20 ns even after several tens of milliseconds, showing the efficiency of our proposed method.

The error of our synchronization scheme is affected by two terms in (12): the TOA terms t_i^T and t_i^M, and the CFO term Δf_{ci}^T. A deeper analysis of the different error terms on the synchronization accuracy will be left for future work.

VI. CONCLUSION

In this paper, we studied the problem of TDOA estimation while focusing on the synchronization aspect. Conventional master-slave synchronization suffers from the time skew that affects the TDOA accuracy *in between* master messages. We proposed a novel synchronization algorithm, based on the observation that time skew is proportional to CFO, as both the RF mixer and the ADC of a transceiver are driven by the same LO. Our CFO-assisted synchronization allows, through some very basic mathematical operations, to obtain a tight synchronization for TDOA-based localization systems. The advantage and significance of our synchronization algorithm

is that it requires no additional hardware, since it relies on information that is already available in most transceiver ICs. Our future work will focus on the error characterization of the proposed synchronization algorithm. While both TOA and CFO errors affect the quality of our synchronization, their effect will ultimately define the minimum delay between two master messages that is required to maintain a certain synchronization level. The proposed algorithm will also be tested on an ultra-wideband ranging system, since the proposed method can benefit from much less messaging overhead than conventional two-way ranging algorithms.

REFERENCES

[1] S. Gezici, "A survey on wireless position estimation," Wireless Personal Communications, vol. 44, no. 3, pp. 263--282, Feb. 2008.

[2] M. R. Gholami, S. Gezici and E. G. Strom, "TDOA Based Positioning in the Presence of Unknown Clock Skew," IEEE Trans. Communications, vol. 61, pp.2522–2534, June 2013.

[3] S. Leugner, M. Pelka and H. Hellbrück, "Comparison of wired and wireless synchronization with clock drift compensation suited for U-TDoA localization," 13th Workshop on Positioning, Navigation and Communications (WPNC), Bremen, pp. 1–4, 2016.

[4] A. Luong et al., "A Stitch in Time and Frequency Synchronization Saves Bandwidth," 2018 17th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN), Porto, pp. 96–107, 2018.

[5] S. Dwivedi, A. De Angelis, D. Zachariah and P. Händel, "Joint Ranging and Clock Parameter Estimation by Wireless Round Trip Time Measurements," in IEEE Journal on Selected Areas in Communications, vol. 33, pp. 2379–2390, Nov. 2015.

[6] I. Skog and P. Handel, "Synchronization by Two-Way Message Exchanges: Cramér-Rao Bounds, Approximate Maximum Likelihood, and Offshore Submarine Positioning," in IEEE Transactions on Signal Processing, vol. 58, pp. 2351–2362, April 2010.

[7] R. M. Vaghefi and R. M. Buehrer, "Joint TOA-based sensor synchronization and localization using semidefinite programming," 2014 IEEE International Conference on Communications (ICC), Sydney, NSW, pp. 520–525, 2014.

[8] A. Mahmood, M. I. Ashraf, M. Gidlund, and J. Torsner, "Over-the-air time synchronization for urllc: Requirements, challenges and possible enablers," arXiv preprint arXiv:1807.00078, 2018.

[9] H. Wang, L. Shao, M. Li and P. Wang, "Estimation of Frequency Offset for Time Synchronization With Immediate Clock Adjustment in Multihop Wireless Sensor Networks," in IEEE Internet of Things Journal, vol. 4, no. 6, pp. 2239–2246, Dec. 2017.

[10] I. Dotlic, A. Connell and M. McLaughlin, "Ranging Methods Utilizing Carrier Frequency Offset Estimation," 2018 15th Workshop on Positioning, Navigation and Communications (WPNC), Bremen, pp. 1–6, 2018.

[11] F. Wang and Y. Zhu, "An efficient CFO estimation algorithm for the downlink of 3GPP-LTE," 2011 International Conference on Wireless Communications and Signal Processing (WCSP), Nanjing, pp. 1–6, 2011.

[12] F. Quitin, M. M. U. Rahman, R. Mudumbai and U. Madhow, "A Scalable Architecture for Distributed Transmit Beamforming with Commodity Radios: Design and Proof of Concept," in IEEE Transactions on Wireless Communications, vol. 12, no. 3, pp. 1418–1428, March 2013.

[13] F. Quitin, Z. Madadi and W. P. Tay, "RF transmitter geolocation based on signal periodicity: Concept and implementation," 2015 IEEE International Conference on Communications (ICC), London, 2015, pp. 4593-4598.