Scalable Wi-Fi Client Self-Positioning Using Cooperative FTM-Sensors

Leor Banin, Ofer Bar-Shalom, Nir Dvorecki, and Yuval Amizur

***Abstract*— This paper presents a protocol that enables an *unlimited* number of Wi-Fi users to position themselves within a meter-level accuracy and navigate indoors using time-delay-based Wi-Fi measurements. The proposed protocol, called collaborative time of arrival, is broadcast-based and relies on cooperation between the network sensors that support IEEE 802.11 fine-timing measurements (FTMs) capabilities, which are enabled in state-of-the-art Wi-Fi chipsets. The clients can estimate and track their position by passively listening to timing measurements that are exchanged between the FTM-sensors. The passive nature of the clients' operation enables them to maintain their privacy by not exposing their presence to the network. This paper outlines the principles of the protocol and the mathematical background of the position estimation algorithms. Both theoretical analysis of the expected positioning accuracy, as well as real-life system performance examples, are provided. The protocol's performance analysis is based on a publicly available database of real network measurements.**

***Index Terms*— IEEE 802.11 standard, indoor navigation, Kalman filters, maximum-likelihood estimation, multisensor systems, position measurement, time-difference-of-arrival (TDoA), time measurement.**

I. Introduction

RANGING based on time-delay measurements for wireless local area network (WLAN) [1] mobile devices has evolved significantly during the past decade. The bandwidth increases from 20 MHz up to 160 MHz, combined with the multiple-input-multiple-output (MIMO) technology, has ignited a rapid standardization effort of a fine-timing measurement (FTM) protocol [1], [2]. This has facilitated the development of accurate, time-delay-based Wi-Fi indoor positioning and navigation systems [5]–[14]. FTM is a point-to-point (P2P) single-user protocol, which includes an exchange of multiple message frames between an initiating Wi-Fi station (ISTA) and a responding station (RSTA). The ISTA (which is typically a mobile Wi-Fi client such as a mobile phone) attempts to measure its range with respect to the RSTA (e.g., Wi-Fi access point (AP) or a dedicated FTM "responder"). Obtaining an accurate time-delay estimate in a dense-multipath environment is challenging and requires an accurate detection of the first signal path, which is associated with the line of sight (LoS) between the two stations and estimation of its arrival time. This is implemented using either superresolution methods [7], [8], or maximum-likelihood methods [9], applied to the estimated channel response. The channel response is estimated using training sequences of orthogonal frequency-division multiplexing (OFDM) symbols with known subcarrier modulation included in the exchanged messages [3]. A schematic description of the message exchange of the FTM protocol is illustrated in Fig. 1.

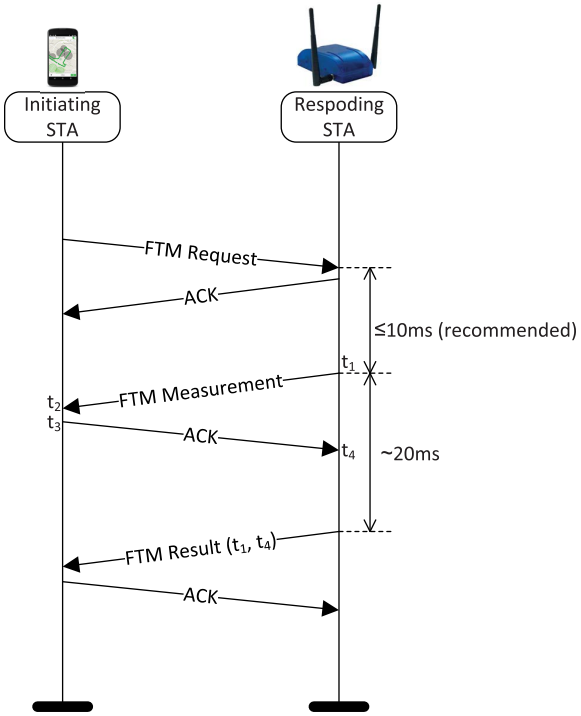

Fig. 1. FTM protocol message flow example.

The time of flight (ToF) between the two stations is calculated using the following equation:

$$\text{ToF} = \frac{(t_4 - t_1) - (t_3 - t_2)}{2} \tag{1}$$

where t_1 denotes the time of departure (ToD) measured by the RSTA, and t_4 denotes the time of arrival (ToA), which is estimated by the RSTA. The values of t_1 and t_4 are reported back to the ISTA after the completion of the FTM

Manuscript received August 1, 2018; revised October 21, 2018; accepted October 22, 2018. Date of publication December 17, 2018; date of current version September 13, 2019. This work was supported by Intel Communication & Devices Group (iCDG), Intel Corporation. The Associate Editor coordinating the review process was Jesús Ureña. *(Corresponding author: Ofer Bar-Shalom.)*

The authors are with the Intel's Location Core Division, Petah Tikva 49527, Israel (e-mail: ofer.bar-shalom@intel.com).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIM.2018.2880887

[1]Commonly referenced using the synonym "Wi-Fi," which is the Wi-Fi alliance owned trademark for WLAN technology.

measurement phase. The values of t_1 and t_4 are reported at picosecond granularity using a 48-bit counter that wraps around approximately every 281.5 s ($= 2^{48} \cdot 10^{-12}$). The 48-bit format was defined mainly to enable a unified timing measurement report format for both "millimeter-wave" 802.11 systems (e.g., 60 GHz) and Wi-Fi systems operating in the <7-GHz band. Yet, the achievable timing accuracy for the latter type is in the order of 1 ns (∼30 cm) [13]. The ISTA combines the values of t_1 and t_4 along with its own estimated ToA (t_2) and measured ToD (t_3) values, to obtain a range estimate with respect to the RSTA.[2]

Being a P2P, single-user protocol, the FTM protocol is limited in scenarios where a large number of users are requesting positioning services simultaneously. Given that obtaining a single range measurement takes roughly 30-ms per client station (cSTA) [16], each AP may only be able to service approximately 30 cSTAs per second (while exhausting its capacity, leaving it with no bandwidth to provide any data services). Moreover, with more and more navigating users attempting to execute FTM sessions, the likelihood of frame collision increases. This decreases the likelihood of successful range measurement, thereby reducing the number of cSTAs that can be serviced. This is likely to happen in large stadiums hosting rock concerts or major sports events, large airport terminals, central public transportation terminals, and so on. Providing an adequate level of positioning and data services to a user capacity of such magnitude would require the deployment of a network that consists of thousands of FTM responders. The collaborative ToA (CToA) protocol is aimed to provide a cost-effective solution for such use cases.

CToA is a geolocation protocol designed to provide positioning and navigation services to a large scale of users. This can be achieved using a broadcast approach rather than a P2P or a point to multipoint ranging approach. The protocol operates over an unmanaged network of *unsynchronized* and independent units called "broadcasting stations" (bSTA), which together form a high-precision geolocation network. The bSTAs, deployed at known locations, are implemented using either standard Wi-Fi APs capable of measuring accurate ToA or network detached, responderlike units with FTM capabilities. According to the protocol [16], the bSTA units serve several purposes. Every bSTA:

1) periodically broadcasts CToA "beacons," which consist of a packet used for timing measurements and some data information elements;
2) measures the ToD of its own beacons and announces it within the beacon;
3) listens for CToA beacons broadcast by its neighbor bSTAs, and measures their ToA;
4) maintains a log of its current ToD and ToA measurements and publishes its most recent measurements log as part of its next CToA beacon broadcast; and
5) periodically announces its location as part of its CToA beacon broadcasts.

[2]The exchange of the FTM measurement message and its acknowledgment (ACK) frame, which has to be sent out after exactly a short interframe spacing (SIFS) of 16μs, is assumed to finish within a short period, during which the clocks of the two stations do not drift appreciably.

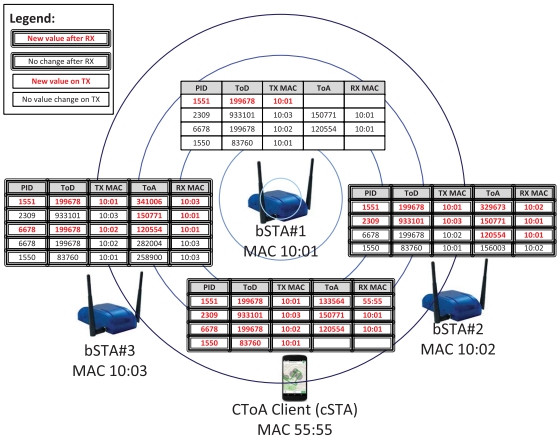

Fig. 2. CToA beacon broadcast example.

The protocol may be visioned as the indoor counterpart of the global navigation satellite systems (GNSSs). It is designed for enabling an *unlimited* number of clients to estimate their location and navigate while maintaining their privacy. The cSTAs only passively listen to the bSTA broadcasts. Once a cSTA receives a broadcast, it measures its ToA and combines it with the ToD/ToA measurements log published by the bSTA in their beacons, to determine its current position. Since the cSTAs do not transmit, their presence is unexposed and their privacy is maintained.

Fig. 2 illustrates an example of CToA beacon broadcast and its reception. It assumes a CToA network, which consists of three unsynchronized bSTA units and a single cSTA. These units are assigned with (simplified) medium access control (MAC) addresses: "10:01," "10:02," and "10:03," while the cSTA has a MAC address of "55:55." As illustrated in Fig. 2, at a time indicated by ToD time-stamp of "199678" (measured in picoseconds and referenced to the time base of bSTA#1), bSTA#1 broadcasts a CToA beacon associated with packet identification (PID) "1551." The ToD and the PID are logged in a "CToA location measurement report" (CLMR) log-file maintained by bSTA#1, which also includes the MAC address of the bSTA. The CLMR broadcast by bSTA1 also includes the time-stamps it has measured for previous broadcasts it received from bSTA#2 and #3. The beacon propagates through the channel, and as illustrated in Fig. 2, is received by bSTA #2 & #3, and the cSTA, which update their measurement logs accordingly: bSTA#2 measured the beacon's ToA as "329673" (referenced to its own time base) and updates that value in its CLMR log, along with its own MAC address as the receiving unit. Similarly, bSTA#3 and the cSTA estimate and log the ToAs of that same beacon as "341006," and "133564," respectively. The bSTAs also update their CLMR logs with the additional time-stamps measured by bSTA#1 as reported in its broadcast CLMR. The CLMR is managed as a "sliding-window" of the time-stamps measured during the past X seconds. The size of that window may be tuned for optimizing the overall system performance. The entries of the CLMR log table undergo a time-stamp matching phase, during

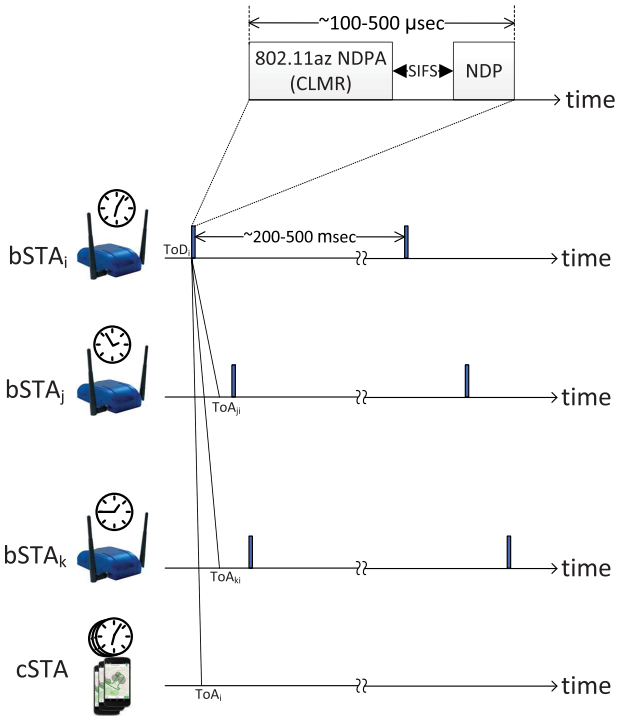

Fig. 3. CToA beacon broadcast timing.

which the ToA measurements are matched with their corresponding ToD value. As will be discussed in Section III-B, the client feeds this timing information, along with the position information of the bSTAs, (also broadcast periodically as part of their beacons), into a Kalman filter that produces an updated estimate of its current position. The messaging sequence of the protocol is described in Fig. 3. The broadcast consists of two transmitted frames separated by a standard, SIFS of 16 μs [2]. The first frame is called "null-data packet (NDP) announcement" and has a twofold role: it announces the arrival of the NDP, used by the receiver for measuring the broadcast's ToA, and it conveys the information elements that carry the CLMR and the bSTA location information. A similar broadcast messaging concept has been discussed in [15], for enabling angular information for the navigating clients. The CToA beacon duration varies between 100 and 500 μs (depending on the amount of data contained in the CLMR). Every bSTA broadcasts a CToA beacon once every 200 to 500 ms. Every bSTA announces its CToA beacon broadcasting schedule to facilitate the optimization of the cSTAs reception duration. Once the cSTA is tracking its location, it may only wake up for less than 500 μs every time it wishes to receive a new timing measurement. The rate, at which the cSTA needs to wake up, depends on its required location accuracy and the accuracy of its crystal oscillator (XO).

A. Related Work and Paper Contributions

The concept of time synchronization for wireless sensor networks (WSN) using two-way time-stamps exchanges has been addressed in [4] (and its referenced sources). The problem of joint synchronization and ranging in a WSN between pairs of nodes exchanging time-stamps has been considered in [12]. The localization of a blind node using time-difference-of-arrival (TDoA) measurements enabled by time-stamps exchange has been proposed in [10]. In [11], this solution was extended for a network-centric architecture, enabling TDoA-based localization and velocity determination of a noncooperative node (namely, a node that does not announce the ToD of the packets it transmits), using time-stamps exchanged between sensor nodes in an asynchronous network. There, the node localization was based on a discrete, least-squares-based fixing, rather than continuous tracking of its position and network clock parameters. It may be worth noticing that the solution in [11] is nonscalable in the sense that the number of nonoverlapping transmissions, which may be sent by the noncooperative nodes within a given time window, is finite. Furthermore, as the noncooperative nodes transmit, their privacy is compromised.

The contributions of this paper are given in the following.

1) A novel scalable, time-delay-based, client positioning protocol for unsynchronized Wi-Fi networks.
2) A Kalman filter-based, client positioning engine (PE).
3) A theoretical analysis of the PE's asymptotic accuracy.
4) Performance evaluation based on a *real* indoor network, for which a measurement database is provided, along with the MATLAB source code of the PE (see [17]).

B. Paper Organization

The remainder of this paper is organized as follows. Section II formulates the client position estimation problem. The position estimation algorithms are derived in Section III. This section is divided into two parts; first, Section III-A outlines the measurement models and the maximum-likelihood position estimators for client mode in the absence of clock drifts. Then, Section III-B introduces the effect of the clock drifts on the measurement models and details the Kalman filter algorithm executed by the client device and used for estimating and tracking all the time-varying parameters in the system. The measurement models derived in Section III-A are used in Section IV for obtaining bounds on the expected positioning accuracy. System-level simulation and real-life system performance are described in Section V. Further insights and design aspects are discussed in Section VI, while the final conclusions are summarized in Section VII. Finally, in the Appendix, the Cramér-Rao lower bounds (CRLBs) for the positioning problem are derived. These are used for illustrating the theoretical system performance discussed in Section IV.

Notation: We use lowercase letters to indicate scalars, lowercase boldface letters to denote vectors, and uppercase boldface letters to express matrices. Other notations are described next to their first appearance.

II. Problem Formulation

In Section II, the mathematical background of the client position estimation is established. Section II-A outlines general definitions that are used in Section II-B for defining

the client position estimation problem.[3] Finally, Section II-C provides an analysis of problem solvability and the minimal configuration that is required for enabling the position estimation.

A. Preliminary Definitions

A "measurement" is defined as the ToF of a broadcast transmission between the two endpoints, A and B. The transmitting endpoint, A, measures the ToD of its broadcast, while the receiving endpoint, B, measures its ToA. Both timing measurements are referenced to the client's clock, and thus have offsets marked by ν_A and ν_B, respectively. The clock offsets also account for any timing biases that may exist due to some obstruction in the propagation medium, resulting in a non-LoS (NLoS) link between the two endpoints. Mathematically, this may be expressed as

$$z \triangleq \mathrm{ToF}_{AB} = (\mathrm{ToA}_B + \nu_B) - (\mathrm{ToD}_A + \nu_A). \tag{2}$$

By denoting the coordinates vectors of the endpoints as $\mathbf{q}_A$ and $\mathbf{q}_B$, respectively, the ToF between the two endpoints may be expressed as

$$\begin{aligned} z &\triangleq \mathrm{ToF}_{AB} \equiv \mathrm{ToA}_B - \mathrm{ToD}_A \\ &= \frac{1}{c}\|\mathbf{q}_B - \mathbf{q}_A\| + \nu_B - \nu_A \end{aligned} \tag{3}$$

where the notation, $\|\mathbf{x}\|$, designates the Euclidean norm of the vector $\mathbf{x}$, and c denotes the speed of light.

If the client acts as the receiving endpoint, then $\nu_B \equiv 0$ and the noiseless ToF measurement is defined as

$$z \triangleq \frac{1}{c}\|\mathbf{q}_B - \mathbf{q}_A\| - \nu_A. \tag{4}$$

B. CToA Problem Definition

Assume that a single cSTA, located at: $\mathbf{p} = [x, y, 0]^T$, attempts to estimate its position using time-delay measurements it gathers from M bSTAs, whose locations are known to the cSTA, where the mth bSTA is located at $\mathbf{q}_m = [x_m, y_m, z_m]^T$.

The cSTA collects two types of time-delay measurements.

1) $\mathrm{bSTA}_i \rightarrow \mathrm{bSTA}_j$ measurements, where $i, j \in 1 \ldots M$, $\forall i \neq j$. These time delays are measured by the bSTAs and published in their beacon broadcast. The cSTA collects L measurements of this type, where the lth measurement is denoted by $\tilde{z}_l$. Each measurement is subjected to additive Gaussian-distributed measurement error with zero-mean and standard deviation of $\tilde{\sigma}$, denoted by $\tilde{n}_l \sim \mathcal{N}(0, \tilde{\sigma}^2)$.
2) $\mathrm{bSTA}_i \rightarrow \mathrm{cSTA}$, where $i \in 1 \ldots M$. These time-delays are measured by the cSTA itself, and the cSTA collects $\mathcal{L}$ measurements of this type, where the ℓth measurement is denoted by $\bar{z}_\ell$. Each measurement is subjected to additive Gaussian measurement error distributed as $\bar{n}_\ell \sim \mathcal{N}(0, \bar{\sigma}^2)$. Typically, $\bar{\sigma} > \tilde{\sigma}$.

Let ν_i denote the (unknown) offset between the cSTA and bSTA_i clocks. Assuming a single $\mathrm{bSTA}_i \rightarrow \mathrm{cSTA}$ ToA measurement of the ℓth broadcast made by the ith bSTA, is unbiased, then it may be modeled as

$$\bar{z}_\ell = \frac{1}{c}\|\mathbf{p} - \mathbf{q}_i\| - \nu_i + \bar{n}_\ell, \quad \ell = 1, \ldots, \mathcal{L}. \tag{5}$$

Similarly, the measurement of the lth broadcast transmitted by the ith bSTA and received by the jth bSTA, may be modeled as

$$\begin{aligned} \tilde{z}_l &= \mathrm{ToA}_j - \mathrm{ToD}_i - \nu_i + \nu_j + \tilde{n}_l \\ &= \frac{1}{c}\|\mathbf{q}_j - \mathbf{q}_i\| - \nu_i + \nu_j + \tilde{n}_l, \quad l = 1, \ldots, L. \end{aligned} \tag{6}$$

C. Minimal System Configuration Analysis

In the following section, we analyze what the minimal network configuration that enables positioning is. Assume that the venue is covered by M bSTA units capable of receiving each other's broadcasts. Under the assumption that the clock offsets are time-invariant, and ignoring any initial system transients, a broadcast sent by the mth bSTA and received by other $(M-1)$ bSTAs and the client, contains the $(M-1)$ "inter-bSTA" previous measurements collected by that bSTA. Hence, the client collects $M(M-1)$ "indirect" measurements (which depend only on the unknown clock offsets). However, it is easy to verify that only $(M-1)$ of them are linearly independent. In addition, the client collects M "direct" measurements, which depend both on its position and the clock offsets. The number of unknowns is $(M+2)$ for the 2-D positioning case, and $(M+3)$ for the 3-D case. As there are a total of $(M-1)+M$ linearly independent measurements, we require that

$$2M - 1 \geq M + 2 \tag{7}$$

for solving the 2-D positioning problem. It is easy to see that three bSTA would be sufficient for solving the 2-D, whereas four bSTAs would be required for 3-D case. Notice that this result is equivalent to the GNSS positioning problem, in which the entire satellite network is synchronized, but its clock offset is unknown to the receiving client. Clearly, if the clock offsets are time-varying then more ("historic") measurements are needed in order to estimate the statistics of these variables. As explained in Section I, such measurements are included in the broadcasts of every bSTA.

III. Positioning Algorithms

In the following section,[4] the CToA positioning algorithms are derived. To facilitate the explanation, the derivation is split into two parts; first, in Section III-A, we address the client position estimation problem under the assumption that the bSTA clocks do not drift over time, such that their offsets with respect to the client's clock are time-invariant. Under this assumption, we derive the position estimators for two cases.

1) "First-Fix"—corresponds to the scenario, in which the client first attempts to sync and estimate its position.
2) "Tracking"—corresponds to the scenario where the client already has an estimate of its position including

[3] Section II-A and Section II-B are excerpted from [16].

[4] This section is excerpted from [16].

the bSTA timing-related parameters and continues tracking them using a Kalman filter.

Then, in Section III-B, we outline the Kalman filter that enables the client to simultaneously estimate and track its own location coordinates, as well as the clock parameters of the bSTAs.

A. Position Estimation in the Absence of Clock Drifts

In the following section, we derive the maximum-likelihood estimates (MLEs) of the client position under the assumption that the clocks of the client and the bSTA do not drift over time, so that the clock offsets remain constant. For simplicity, the derivation assumes a horizontal position only (which is of most interest in indoor positioning scenarios). The extension to 3-D positioning is straightforward.

1) MLE Solution for Client's First-Fix: Let $\mathbf{e}_i$ denote an $M\times 1$ vector of zeros, whose ith entry is 1. Using this notation

$$\nu_i = \mathbf{e}_i^T \boldsymbol{\nu} \tag{8}$$

$$\nu_j - \nu_i = \left(\mathbf{e}_j^T - \mathbf{e}_i^T\right)\boldsymbol{\nu} \tag{9}$$

where $\boldsymbol{\nu} \triangleq [\nu_1, \ldots, \nu_M]^T$, and $\mathbf{x}^T$ denotes the transposition of the vector $\mathbf{x}$. Now, the timing measurements may be recast as

$$\bar{z}_\ell = \frac{1}{c}\|\mathbf{p} - \mathbf{q}_i\| - \mathbf{e}_i^T\boldsymbol{\nu} + \bar{n}_\ell \tag{10}$$

$$\tilde{z}_l = \frac{1}{c}\|\mathbf{q}_j - \mathbf{q}_i\| + \left(\mathbf{e}_j^T - \mathbf{e}_i^T\right)\boldsymbol{\nu} + \tilde{n}_l. \tag{11}$$

We may further define the following vectors and matrices:

$$\begin{aligned}
\bar{\mathbf{z}} &\triangleq [\bar{z}_1, \ldots, \bar{z}_{\mathcal{L}}]^T \\
\tilde{\mathbf{z}} &\triangleq [\tilde{z}_1, \ldots, \tilde{z}_L]^T \\
\mathbf{z} &\triangleq \begin{bmatrix} \bar{\mathbf{z}} \\ \tilde{\mathbf{z}} \end{bmatrix}
\end{aligned} \tag{12}$$

$$\begin{aligned}
\bar{d}_\ell(\mathbf{p}) &\triangleq \|\mathbf{p} - \mathbf{q}_i\| \\
\tilde{d}_l &\triangleq \|\mathbf{q}_i - \mathbf{q}_j\| \\
\bar{\mathbf{d}}(\mathbf{p}) &\triangleq [\bar{d}_1(\mathbf{p}), \ldots, \bar{d}_{\mathcal{L}}(\mathbf{p})]^T \\
\tilde{\mathbf{d}} &\triangleq [\tilde{d}_1, \ldots, \tilde{d}_L]^T \\
\mathbf{d}(\mathbf{p}) &\triangleq \begin{bmatrix} \bar{\mathbf{d}} \\ \tilde{\mathbf{d}} \end{bmatrix}
\end{aligned} \tag{13}$$

$$\begin{aligned}
\bar{\mathbf{E}} &\triangleq [-\mathbf{e}_{i,1}, \ldots, -\mathbf{e}_{i,\mathcal{L}}]^T \\
\tilde{\mathbf{E}} &\triangleq [(\mathbf{e}_{j,1} - \mathbf{e}_{i,1}), \ldots, (\mathbf{e}_{j,L} - \mathbf{e}_{i,L})]^T \\
\mathbf{E} &\triangleq \begin{bmatrix} \bar{\mathbf{E}} \\ \tilde{\mathbf{E}} \end{bmatrix}
\end{aligned} \tag{14}$$

$$\begin{aligned}
\bar{\mathbf{n}} &\triangleq [\bar{n}_1, \ldots, \bar{n}_{\mathcal{L}}]^T \\
\tilde{\mathbf{n}} &\triangleq [\tilde{n}_1, \ldots, \tilde{n}_L]^T \\
\mathbf{n} &\triangleq \begin{bmatrix} \bar{\mathbf{n}} \\ \tilde{\mathbf{n}} \end{bmatrix}.
\end{aligned} \tag{15}$$

Using the definitions of (12)–(15), we may recast (10) and (11) as

$$\mathbf{z} = c^{-1}\mathbf{d}(\mathbf{p}) + \mathbf{E}\boldsymbol{\nu} + \mathbf{n}. \tag{16}$$

The measurement noise is assumed to be Gaussian-distributed with the mean and covariance as follows:

$$\begin{aligned}
E\{\mathbf{n}\} &= \mathbf{0} \\
E\{\mathbf{n}\mathbf{n}^T\} &= \begin{bmatrix} \bar{\sigma}^2\mathbf{I}_{\mathcal{L}} & \mathbf{0} \\ \mathbf{0} & \tilde{\sigma}^2\mathbf{I}_L \end{bmatrix} \triangleq \mathbf{W}
\end{aligned} \tag{17}$$

where $E\{.\}$ denotes the expectation operator and $\mathbf{I}_N$ denotes an $N \times N$ identity matrix.

Under these assumptions, the MLE of the cSTA position vector, $\hat{\mathbf{p}}$, may be obtained as

$$\hat{\mathbf{p}} = \underset{\mathbf{p},\boldsymbol{\nu}}{\operatorname{argmin}} (\mathbf{z} - c^{-1}\mathbf{d} - \mathbf{E}\boldsymbol{\nu})^T \mathbf{W}^{-1} (\mathbf{z} - c^{-1}\mathbf{d} - \mathbf{E}\boldsymbol{\nu}) \tag{18}$$

where $\mathbf{X}^{-1}$ denotes the inverse of the matrix $\mathbf{X}$.

The estimate of the clock offsets vector may be found using weighted least-squares (WLS) criteria

$$\hat{\boldsymbol{\nu}} = (\mathbf{E}^T\mathbf{W}^{-1}\mathbf{E})^{-1}\mathbf{E}^T\mathbf{W}^{-1}(\mathbf{z} - c^{-1}\mathbf{d}). \tag{19}$$

Define

$$\mathbf{B} \triangleq [\mathbf{W}^{-1} - \mathbf{W}^{-1}\mathbf{E}(\mathbf{E}^T\mathbf{W}^{-1}\mathbf{E})^{-1}\mathbf{E}^T\mathbf{W}^{-1}]. \tag{20}$$

Then, by substituting (19) back in (18) we get

$$\hat{\mathbf{p}} = \underset{\mathbf{p}}{\operatorname{argmin}} (\mathbf{z} - c^{-1}\mathbf{d})^T \mathbf{B} (\mathbf{z} - c^{-1}\mathbf{d}). \tag{21}$$

The nonlinear minimization problem in (21) can be solved via 2-D grid search (or 3-D search, in case of three-positioning), over all the possible locations.

2) MLE Solution for a Client in "Tracking Mode": Once the client receiver has converged to the true values of the bSTA clock offsets and continuously tracks them, these clock offsets may be considered as "known" (up to some estimation error). In such case, it would be reasonable to assume that $\mathbf{z} \simeq \bar{\mathbf{z}}$, $\mathbf{d} \simeq \bar{\mathbf{d}}$. Define

$$\boldsymbol{\zeta} \triangleq \bar{\mathbf{z}} - \bar{\mathbf{E}}\hat{\boldsymbol{\nu}}. \tag{22}$$

The resulting measurement model in this case may be recast as

$$\boldsymbol{\zeta} = c^{-1}\bar{\mathbf{d}}(\mathbf{p}) + \check{\mathbf{n}}. \tag{23}$$

The additive noise vector, $\check{\mathbf{n}}$, is assumed to be Gaussian-distributed with the following properties:

$$\begin{aligned}
E\{\check{\mathbf{n}}\} &= \mathbf{0} \\
E\{\check{\mathbf{n}}\check{\mathbf{n}}^T\} &\triangleq \left(\bar{\sigma}^2 + \sigma_r^2\right)\cdot\mathbf{I}_{\mathcal{L}}
\end{aligned} \tag{24}$$

where σ_r corresponds to the standard deviation of the residual estimation error of the clock offsets. The client position MLE, in this case, is obtained by minimizing the following cost function:

$$\hat{\mathbf{p}} = \underset{\mathbf{p}}{\operatorname{argmin}} |\boldsymbol{\zeta} - c^{-1}\bar{\mathbf{d}}(\mathbf{p})|^2 \tag{25}$$

where again, the nonlinear minimization problem in (25) can be solved via grid search over the position coordinates space.

B. Position Estimation Under Clock Drifts

The analysis outlined in the former section ignored any clock drifts, which result from the XO frequency deviations. Such deviations may be caused by multiple effects such as ambient temperature changes, phase noise, thermal noise, crystal aging, and so on. Each bSTA measures the timing related to the broadcast events (ToD or ToA). This timing is referenced to its native time base. Once the measurements are conveyed to the cSTA for enabling it to compute its location, the cSTA needs to resolve the instantaneous clock offset of the bSTA associated with that measurements and is a function of the offset drift rate. Assuming the first-order clock drift model, the instantaneous value of the clock offset of the nth bSTA is calculated using

$$\nu_n(t_i) = \nu_n(t_{i-1}) + \dot{\nu}_n \cdot \Delta t \tag{26}$$

where $\nu_n(t_{i-1})$ corresponds to the previous estimated value of the clock offset, (where $\nu_n(t_0)$ denotes its initial value), $\dot{\nu}_n$ denotes the clock skew (or the change rate of the clock offset), and $\Delta t = t_i - t_{i-1}$. In the following section, we outline the algorithm, which enables the cSTA to estimate and track its location under clock drifts. The Kalman Filter is the optimal estimate for linear system models with additive-independent white noise in both the transition and the measurement system models. Yet, in many systems, including navigation systems, the measurement model is not linearly dependent in the parameters of interest. In such cases, the extended Kalman filter (EKF), which is the nonlinear version of the Kalman filter, is widely used [21]. In the EKF, the state transition and observation models are not required to be linear functions of the states, but instead, may only be differentiable functions. The EKF is executed by the client, enabling it to estimate and track its own position coordinates, as well as the timing parameters of the stray bSTA units, from which it receives the measurement broadcasts. An EKF is described by two equations, which define the system and the observation (measurement) models. These models are described next.

1) CToA EKF System Model: The system model is defined by the following recursive equation:

$$\mathbf{x}_k = \mathbf{F}_k \mathbf{x}_{k-1} + \mathbf{w}_k, \quad k \geq 0 \tag{27}$$

where the index k denotes the discrete time-step. The vector $\mathbf{x}_k$ denotes an $N \times 1$ states vector, which describes the parameters being estimated and tracked by the filter. The states vector for the client mode consists of the client's position coordinates and per-bSTA clock parameters [clock offset and clock offset change rate (or skew)]. The size of the EKF state vector is thus $N = 3 + 2\ M$, where M denotes the number of bSTAs being received by the cSTA (both directly and indirectly)

$$\begin{aligned} \mathbf{p}_k &\triangleq [x_k, y_k, z_k]^T \\ \boldsymbol{\nu}_k &\triangleq [\nu_{1,k}, \ldots, \nu_{M,k}]^T \\ \dot{\boldsymbol{\nu}}_k &\triangleq [\dot{\nu}_{1,k}, \ldots, \dot{\nu}_{M,k}]^T \\ \mathbf{x}_k &\triangleq \left[\mathbf{p}_k^T, \boldsymbol{\nu}_k^T, \dot{\boldsymbol{\nu}}_k^T\right]^T. \end{aligned} \tag{28}$$

The state vector $\mathbf{x}_k$ is associated with a covariance matrix

$$\mathbf{P}_k = E\{(\mathbf{x}_k - \bar{\mathbf{x}}_k)(\mathbf{x}_k - \bar{\mathbf{x}}_k)^T\} \tag{29}$$

where $\bar{\mathbf{x}}_k \triangleq E\{\mathbf{x}_k\}$. When the filter initialized the state-covariance matrix is assumed to be

$$\mathbf{P}_0 = \begin{bmatrix} \tilde{\mathbf{P}}_{\mathbf{p},0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \sigma_{\nu,0}^2 \mathbf{I}_M & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \sigma_{\dot{\nu},0}^2 \mathbf{I}_M \end{bmatrix} \tag{30}$$

where $\sigma_{\nu,0}$, $\sigma_{\dot{\nu},0}$ denote the initial values for the standard deviations of the clock offsets and drifts, and $\tilde{\mathbf{P}}_{\mathbf{p},0}$ denotes the initial value of states covariance matrix, given by

$$\tilde{\mathbf{P}}_{\mathbf{p},0} \triangleq \begin{bmatrix} \sigma_{x,0}^2 & 0 & 0 \\ 0 & \sigma_{y,0}^2 & 0 \\ 0 & 0 & \sigma_{z,0}^2 \end{bmatrix}. \tag{31}$$

The initial values of the standard deviations constructing the initial states covariance matrix are commonly determined empirically.

The dynamic system model linear transfer function is denoted by $\mathbf{F}_k$, an $N \times N$ block-diagonal matrix defined as follows:

$$\mathbf{F}_k \triangleq \begin{bmatrix} \mathbf{I}_3 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_M & \Delta t \mathbf{I}_M \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_M \end{bmatrix} \tag{32}$$

where Δt corresponds to the elapsed time between the two consecutive discrete time-steps.

The vector $\mathbf{w}_k$ denotes a random $N \times 1$ model noise vector, which described the uncertainties in the system model and has the following statistical properties:

$$\begin{aligned} E\{\mathbf{w}_k\} &= \mathbf{0} \\ E\left\{\mathbf{w}_k \mathbf{w}_k^T\right\} &= \mathbf{Q}_k \\ E\left\{\mathbf{w}_k \mathbf{w}_j^T\right\} &= \mathbf{0}, \quad \forall k \neq j \\ E\left\{\mathbf{w}_k \mathbf{x}_k^T\right\} &= \mathbf{0}, \quad \forall k. \end{aligned} \tag{33}$$

In the EKF system model, the process noise, $\mathbf{w}_k$ is assumed to be Gaussian-distributed with zero-mean and a covariance matrix, $\mathbf{Q}_k$, which is block-diagonal and given by

$$\mathbf{Q}_k = \Delta t \cdot \begin{bmatrix} \mathbf{Q}_{\mathbf{p},k} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \tilde{\sigma}_{\nu}^2 \mathbf{I}_M & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \tilde{\sigma}_{\dot{\nu}}^2 \mathbf{I}_M \end{bmatrix} \tag{34}$$

where

$$\mathbf{Q}_{\mathbf{p},k} \triangleq \begin{bmatrix} \tilde{\sigma}_x^2 & 0 & 0 \\ 0 & \tilde{\sigma}_y^2 & 0 \\ 0 & 0 & \tilde{\sigma}_z^2 \end{bmatrix}. \tag{35}$$

In general, the determination of the noise variance values of $\mathbf{Q}_k$, is challenging, and is often obtained by some heuristic methods. Commonly, it is assumed that most of the clock deviation is dictated by the clock skew, rather than clock measurement noise. The values of $\{\tilde{\sigma}_x^2,\ \tilde{\sigma}_y^2,\ \tilde{\sigma}_z^2\}$ are determined according to the motion assumptions of the cSTA device (e.g., pedestrian, vehicle/drone etc.).

2) EKF Measurement Model: The measurement model is defined as

$$\mathbf{z}_k = \mathbf{h}(\mathbf{x}_k) + \mathbf{v}_k \tag{36}$$

where $\mathbf{z}_k$ is a $J \times 1$ vector of measurements, in which each entry corresponds to a ToF measurement that follows the definition of (2). The vector $\mathbf{h}(\mathbf{x}) \triangleq [h_1(\mathbf{x}), h_2(\mathbf{x}), \ldots, h_J(\mathbf{x})]^T$, denoting the nonlinear measurement model vector transfer function, and $\mathbf{v}_k$ denotes the additive measurement noise that has the following statistical properties:

$$\begin{aligned} E\{\mathbf{v}_k\} &= \mathbf{0} \\ E\{\mathbf{v}_k \mathbf{v}_k^T\} &= \mathbf{R}_k = \sigma_m^2 \mathbf{I} \delta_{kj} \\ E\{\mathbf{v}_k \mathbf{x}_k^T\} &= \mathbf{0}, \quad \forall k \\ E\{\mathbf{w}_k \mathbf{v}_j^T\} &= \mathbf{0}, \quad \forall k, j \end{aligned} \tag{37}$$

where δ_{kj} denotes the Kronecker delta. As discussed in Section III-A, there are two types of transfer functions, which depend on the type of the measurement (bSTA$_i$ $\rightarrow$ cSTA or bSTA$_i$ $\rightarrow$ bSTA$_j$). From (10) and (11), it is easy to see that the corresponding measurement transfer functions are given by

$$h_\ell(\mathbf{x}_k) = \frac{1}{c}\|\mathbf{p}_k - \mathbf{q}_i\| - \mathbf{e}_i^T \boldsymbol{\nu}_k \tag{38}$$

$$h_l(\mathbf{x}_k) = \frac{1}{c}\|\mathbf{q}_j - \mathbf{q}_i\| + (\mathbf{e}_j - \mathbf{e}_i)^T \boldsymbol{\nu}_k. \tag{39}$$

Since the measurement transfer function, $\mathbf{h}(\cdot)$ is nonlinear, it cannot be applied to estimate the measurements covariance matrix directly. Instead, we linearize $\mathbf{h}(\cdot)$ by replacing it with its first-order Taylor series expansion, calculated around $\hat{\mathbf{x}}_{k|k-1}$

$$\mathbf{h}(\mathbf{x}_k) \cong \mathbf{h}(\hat{\mathbf{x}}_{k|k-1}) + \mathbf{H}_k \cdot (\mathbf{x}_k - \hat{\mathbf{x}}_{k|k-1}) \tag{40}$$

where the notation $\hat{\mathbf{x}}_{n|m}$ represents the estimate of $\mathbf{x}$ at time n given observations up to and including time $m \leq n$. The matrix $\mathbf{H}_k$ denotes the Jacobian of the measurement model function vector $\mathbf{h}(\cdot)$, which is a $J \times N$ matrix defined as

$$\begin{aligned} \mathbf{H}_k &\triangleq \begin{bmatrix} \frac{\partial h_1}{\partial x_1} & \frac{\partial h_1}{\partial x_2} & \cdots & \frac{\partial h_1}{\partial x_N} \\ \vdots & & \ddots & \vdots \\ \frac{\partial h_J}{\partial x_1} & \frac{\partial h_J}{\partial x_2} & \cdots & \frac{\partial h_J}{\partial x_N} \end{bmatrix} \\ [\mathbf{H}_k]_{ij} &\equiv \left.\frac{\partial h_i}{\partial x_j}\right|_{\mathbf{x}=\hat{\mathbf{x}}_{k|k-1}}. \end{aligned} \tag{41}$$

The Jacobian is obtained by calculating the partial derivatives of (38) and (39). Equations (42) and (43) define the corresponding lines of the matrix $\mathbf{H}_k$

$$[\mathbf{H}_k]_\ell = \left[\frac{(\mathbf{p}_k - \mathbf{q}_n)^T}{c\|\mathbf{p}_k - \mathbf{q}_n\|}, -\mathbf{e}_i^T, \mathbf{0}_M^T\right] \tag{42}$$

$$[\mathbf{H}_k]_l = \left[\mathbf{0}_3^T, (\mathbf{e}_j - \mathbf{e}_i)^T, \mathbf{0}_M^T\right]. \tag{43}$$

To accelerate the EKF convergence, the initial values for the clock offset and the position states, $\hat{\mathbf{v}}_0$, $\hat{\mathbf{p}}_0$, may be obtained using (19) and (21), respectively. An implementation of the EKF algorithm was presented in [16] and a possible MATLAB realization of this code is described [17].

IV. Approximate Performance Analysis

For obtaining theoretical performance bounds, the driftless measurement models derived in Section III-A were used for calculating the respective CRLB. The derived bounds are affected mainly by the geometrical properties of the network deployment, as well as the additive noise levels. Yet, these bounds ignore propagation models that may account for the type of materials through which the signals propagate. Under the assumption that the additive measurement noise is Gaussian-distributed, for each location on a given grid, one can calculate the circular error probable (CEP) that defines the radius of the circle centered around the estimator's mean estimate (or the true receiver location in our case), in which the receiver is contained with a probability, P_{in} [23, eqs. (63) and (64)]

$$P_{\text{in}} = \frac{1}{2\pi\sqrt{\lambda_1\lambda_2}} \iint_R \exp\left(-\frac{\zeta_1^2}{2\lambda_1} - \frac{\zeta_2^2}{2\lambda_2}\right) d\zeta_1 d\zeta_2 \tag{44}$$

where R is a circle defined as

$$R \triangleq \left\{(\zeta_1, \zeta_2) : \sqrt{\zeta_1^2 + \zeta_2^2} \leq \text{CEP}\right\} \tag{45}$$

and λ_1, λ_2 ($\lambda_1 \geq \lambda_2$) denote the eigenvalues of the 2-D positioning error covariance matrix for position $\mathbf{p}$, which is predicted by the CRLB derived in the Appendix. The CEP for probability, P_{in}, may be calculated using [23, eq. (72)]

$$P_{\text{in}} \cdot \frac{1+\gamma^2}{2\gamma} = \int_0^{UL} e^{-x} I_0\left(\frac{1-\gamma^2}{1+\gamma^2} \cdot x\right) dx \tag{46}$$

where I_0 denotes the modified Bessel function of the first kind and

$$\gamma^2 \triangleq \frac{\lambda_2}{\lambda_1}; \quad UL \triangleq \frac{(1+\gamma^2)}{4\lambda_2} \cdot \text{CEP}^2 \tag{47}$$

with

$$\text{CEP}(P_{\text{in}}) = \int_{\mathbf{p}} f_{\text{CEP}}(P_{\text{in}}|\mathbf{p}) f(\mathbf{p}) d\mathbf{p} \tag{48}$$

where $f_{\text{CEP}}(P_{\text{in}}|\mathbf{p})$ is given by (46).

Fig. 4 depicts curves of the expected probabilities of different CEP values for "First-Fix" and "Tracking mode" scenarios. These curves were obtained for a typical office network deployment depicted in Fig. 5, where the red rings denote the position of the bSTAs. The CEP values were evaluated numerically as follows. On each of the 10^4 sampling points along the client's trajectory denoted by the red dots as shown in Fig. 5, the respective CRLB error covariance matrices were calculated. These calculations were done assuming the client receives broadcasts from only the four nearest bSTAs. At each point, a position-dependent CEP curve was calculated using (46) for 100, equally spaced, probability values between 0 and 1-ϵ. The final curves in Fig. 4 are position-independent and obtained by averaging the CEP curves over the entire trajectory, assuming equal probability of the client's position.

Mathematically, (48) may be approximated as

$$\text{CEP}(P_{\text{in}}) \simeq \frac{1}{N_{\text{Loc}}} \sum_{n=1}^{N_{\text{Loc}}} \text{CEP}_n(P_{\text{in}}) \tag{49}$$

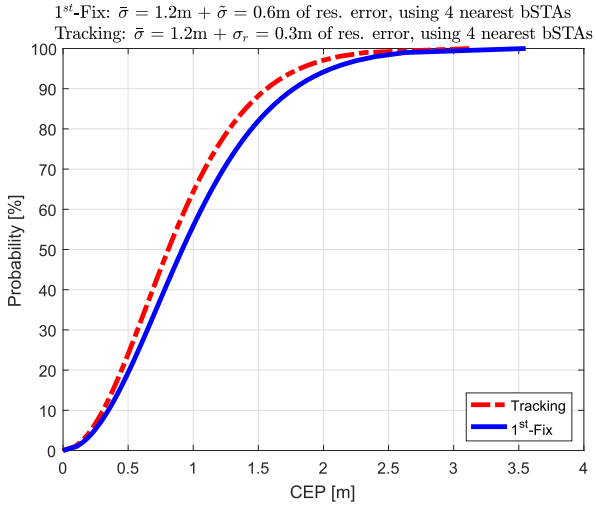

Fig. 4. Theoretical errors bounds along the client trajectory.

Fig. 5. Indoor office system simulation.

where $\mathrm{CEP}_n(P_{\mathrm{in}})$ denotes the CEP value corresponding to probability P_{in} at the nth location sampling point, and N_{Loc} is the total number of location sampling points. The noise level assumed were $\bar{\sigma} = 0.6$ m, $\tilde{\sigma} = 1.2$ m, and $\sigma_r = 0.3$ m.

The following proposition proves that given enough samples, the asymptotic accuracy of the client position in "First-Fix" is equivalent to the one that can be attained with the position tracking filter converged.

Proposition 1 (Asymptotic Performance): The asymptotic positioning accuracy for a client in "First-Fix" mode, approaches the accuracy attained in "Tracking mode," given $\tilde{N} \to \infty$ replicas of the bSTA→bSTA timing measurements.

Proof: See Appendix. ■

V. Performance in an Indoor Network

To validate the concept, the CToA system was tested using both system-level simulations and an actual deployed network. In the following section, we outline examples of the positioning accuracy of a mobile client in an indoor network. These results were obtained for both a simulated network environment and a real-life network, deployed over the same indoor venue. To analyze its accuracy, the position estimates were compared against a "ground-truth" (reference) the trajectory of the mobile client. This reference trajectory was generated using a robotic ground-truth tool based on "light detection and ranging" (LiDAR) [14]. The LiDAR system used integrates a 270° laser scanner, which uses a dedicated map and laser measurements to estimate its position. Its output is a series of position reports generated at a rate of 20 Hz with an accuracy of 10–30 cm. The map was obtained in advance through a survey of the venue using the LiDAR system, during which a structure map was created using a simultaneous localization and mapping algorithm (see [19]). The reference trajectory of the mobile client was used for both the system-level simulations, as well as for the real-life system measurements. The remainder of this section outlines the simulation methodology and system implementation. This section is concluded with a comparative analysis of the simulation and the real system results.

A. Simulation Methodology

At its lower level, a typical geolocation system architecture consists of a measurement engine (ME) and a PE. The ME receives raw signal samples (e.g., the OFDM channel estimation) and outputs raw timing measurements. The PE receives the raw timing measurements from the ME and outputs an estimate of the current position, where the PE implements the EKF described in Section III-B. The system-level simulation described here is focused on the PE while assuming an "ideal" ME. It relies on a modeling of skewed bSTA clocks, as described next. The ToA time-stamps fed into the PE are referenced to the signal's propagation distance, while the channel impairments effect is simulated via Gaussian-distributed errors added to the measured clock time-stamps, which are fed to the PE.

1) Station Clock Modeling: The modeling of the bSTA and client (cSTA) clocks' behavior is at the heart of the system simulation and is used for realizing the time-stamps fed into the PE. The STA clock is modeled as a recursive random process defined as follows (see [22]):

$$\tilde{\mathbf{c}}_k = \tilde{\mathbf{F}}_k \tilde{\mathbf{c}}_{k-1} + \tilde{\mathbf{n}}_k \tag{50}$$

where $\tilde{\mathbf{c}}_k$ denotes the clock system states vector that contains the following states: clock offset, clock skew (drift), and skew rate, $\tilde{\mathbf{F}}_k$ denotes the states-transition model matrix, and $\tilde{\mathbf{n}}_k$ denotes process noise, all of which are defined as follows:

$$\tilde{\mathbf{c}}_k \triangleq \begin{bmatrix} \nu_k \\ \dot{\nu}_k \\ \ddot{\nu}_k \end{bmatrix} \tag{51}$$

$$\tilde{\mathbf{F}}_k \triangleq \begin{bmatrix} 1 & \Delta t & \frac{1}{2}\Delta t^2 \\ 0 & 1 & \Delta t \\ 0 & 0 & 1 \end{bmatrix} \tag{52}$$

$$\tilde{\mathbf{n}}_k \triangleq \sqrt{\Delta t} \cdot \tilde{\mathbf{Q}}\tilde{\mathbf{n}} \tag{53}$$

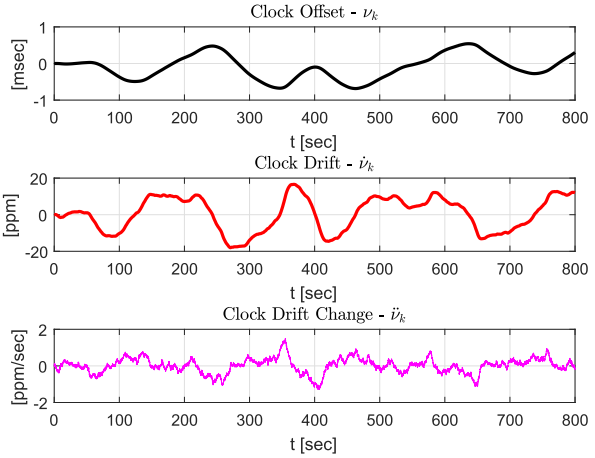

Fig. 6. Skewed clock realization example.

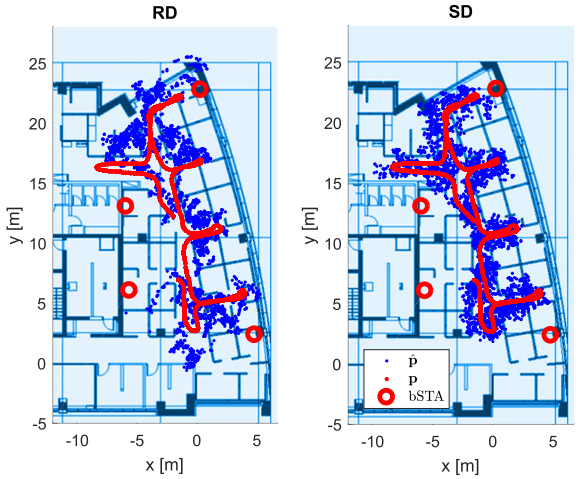

Fig. 7. Real data versus simulated data position estimates.

with

$$\tilde{\mathbf{Q}} \triangleq \begin{bmatrix} \sigma_\nu & 0 & 0 \\ 0 & \sigma_{\dot{\nu}} & 0 \\ 0 & 0 & \sigma_{\ddot{\nu}} \end{bmatrix} \tag{54}$$

$$\tilde{\mathbf{n}} \triangleq \begin{bmatrix} \mathcal{N}(0,1) \\ \mathcal{N}(0,1) \\ \mathcal{N}(0,1) \end{bmatrix} \tag{55}$$

where for $\sigma_\nu = \sigma_{\dot{\nu}} = 10^{-10}$ and $\sigma_{\ddot{\nu}} = 10^{-7}$. Fig. 6 depicts an example realization of the clock states. The clock model also implements a mechanism to maintain the drift within the specified boundaries of ± 25 ppm.

2) Measurement Modeling: The ToD and ToA measurements are realized as clock time-stamps of the bSTAs and the client and rely on the clock model described in Section V-A1. Although the modeled ToD time-stamps are fed into the PE as-is, the ToA time-stamps also account for the geometrical propagation distance between the transmitter and the receiver, as well as a random bias to model the NLoS channel propagation effect.

B. Real-Life System Performance

To study the actual system performance in an indoor environment, a network of bSTA units was set up. The bSTA units were implemented using Intel Wireless-AC8260 Wi-Fi 802.11ac, 2×2 dual-band chipsets [25], mounted in mini personal computers. The position estimates were obtained for a client device, built using the same Wi-Fi module mounted on the robotic "ground-truth" vehicle. The OFDM channel estimation and the ME (including the LoS detection and ToA estimation mechanism) were implemented on the Wi-Fi chipset in a combination of hardware and firmware that was executed on the AC8260 processing cores.

The PE was executed on the client processor, where the EKF also implemented several heuristic, range-based mechanisms for outlier measurement rejection. A description of these mechanisms can be found in [21, Ch. 15.3]. Both the real-life as well as the simulated network measurements used for generating the results presented in this paper, along with the MATLAB code of the PE, are available in [17].

The test venue selected is a populated open space, cubical office floor. This is a highly congested Wi-Fi environment, which is also heavily multipath dense due to the 1.5 m high, metal-framed cubical offices that generate multiple reflections of the transmitted signals. Moreover, the center of the venue contains a structure of thick concrete walls forming the floor shelter (notice the thick, black rectangle in Fig. 7). These walls generate a constant NLoS propagation channel between some of the bSTAs, as well as between the client and the bSTAs in certain sections of the venue.

C. Performance Results

Fig. 7 depicts the reference and estimated client trajectories used for both the simulation data and the real data (RD) measurements. These estimates correspond to measurement frames broadcast at a 40 MHz channel bandwidth. The true positions of the client along the reference trajectory are denoted by $\mathbf{p}$ and marked by red dots. The estimated client positions are denoted by $\hat{\mathbf{p}}$ and marked by blue dots. The location of the bSTAs in the network is marked by the red rings. The bSTAs were placed on shelves at a height of 2.2 m. The simulation was defined such that each bSTA exchanges measurements with its four nearest neighbor bSTAs. In addition, in every point along the trajectory, the client used measurements from the four nearest bSTAs. This restriction was applied to the simulation environment to imitate the expected channel conditions, in which not all the bSTAs are visible from every point along the trajectory. This restriction does not apply to the real system, such that the bSTAs attempt to measure transmissions coming from any neighbor bSTA (even if there is no LoS between them). Consequently, the client attempts to use any of the bSTA broadcasts it receives. In both cases, the bSTAs were set to broadcast CToA beacons at 2 Hz. The real-life system was set to broadcast the beacons with a bandwidth of 40 MHz. Since the PE has no notion of signal bandwidth, the additive error levels in the system simulation were set to match the typical ranging errors expected for 40 MHz OFDM transmissions. The positioning accuracy is described by means of the cumulative distribution function (CDF) of the client's

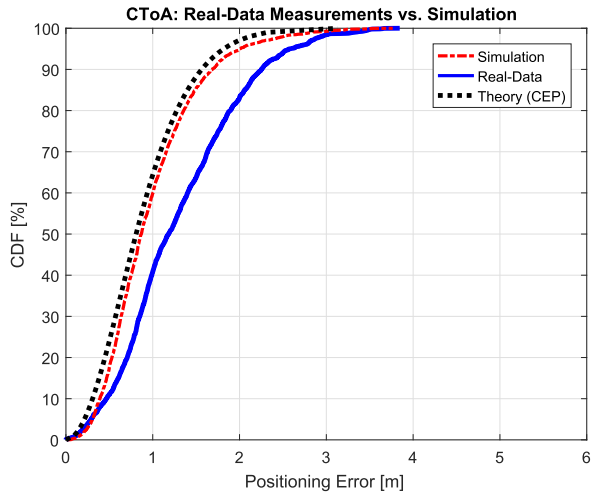

Fig. 8. Theoretical and empirical client positioning error CDF.

positioning errors, which are defined as

$$\varepsilon = \|\hat{\mathbf{p}} - \mathbf{p}\|. \tag{56}$$

Fig. 8, which depicts the CDF, contains three curves: the blue curve describes the CDF of the client's positioning error measured during a real-life recordings of the system. The real-life recording is compared against the positioning accuracy predicted by the simulation (dashed-dotted red curve) and against the theoretical accuracy predicted by the CRLB (black dotted curve). The latter curve was obtained for the "tracking mode" as explained in Section V.

As can be seen from this analysis, the system achieves an accuracy better than 1.5 m in 67% of the cases and about 2 m in 95% of the cases. The deviation between the error distributions of the real system and the theoretical/simulated system may be attributed to the outliers and range biases, which are introduced, by nature, in real network measured data, but do not exist in the model generating the simulated data. The outliers may be filtered-out using outlier rejection mechanisms that can be applied to the EKF code.

VI. Discussion

Although client mode CToA[5] may be perceived as the indoor counterpart of GNSS, it imposes different implementation challenges. GNSS networks implement a similar time-stamped broadcast approach to enable an unlimited number of client receivers to navigate simultaneously worldwide. Yet, two fundamental differences distinct the time tracking of receivers in a GNSS network compared to CToA network: first, a GNSS network is synchronized, whereas the CToA network is not. Second, due to its multiple-access nature, the broadcasts sent by the network satellite vehicles (SVs) are received at the client simultaneously, while in a CToA network, the broadcasts are staggered in time. Let us delve into these two differences and explore them in detail.

[5]Portions of the following discussion are excerpted from the Discussion Section in [16].

In GNSS networks the SVs are synchronized using onboard atomic clocks, which have a frequency stability of approximately 10^{-14}. This frequency stability translates into a clock drift of roughly 1 ns per day [20] (equivalent to a ranging error of about 35 cm - an error that is further corrected by the GNSS system). Since GNSS networks are fully synchronized in terms of timing parameters, the GNSS client receiver needs to estimate only the offset and the drift between its internal clock, and the network clock. The client receiver's clock is typically generated using an XO with a frequency stability in the order of 10^{-6} (commonly expressed in units of parts-per-million). Tracking these parameters (along with additional system states such as position and velocity)[6] is done using a Kalman filter algorithm [21].

In the CToA network, since the bSTAs are unsynchronized, each bSTA contributes a clock offset and drift that need to be estimated and tracked. Furthermore, different MAC methods used by GNSS and CToA impose an additional challenge. In GNSS networks, the multiplexing at the code space (code division multiple access) or the frequency space (frequency-division multiple access) ensures that broadcast transmissions from all SVs are received simultaneously at the client. Conversely, CToA relies on the "listen-before-talk" MAC of the IEEE 802.11, which effectively results in timing measurements being staggered in time. Given that a typical Wi-Fi XO has an accuracy of ± 25 ppm, consecutive timing measurements taken from the same broadcasting source may accumulate significant time drift [18]. This implies that while one bSTA clock offset is measured, other bSTAs clock offsets keep on drifting apart.

The Kalman filtering combined with the broadcasting nature of the protocol enables several levels of system robustness. For instance, the filter's state-covariance matrix enables tracking of interconnections between hidden nodes, which are received indirectly via other bSTAs. These indirect measurements enable the client to synchronize with those bSTAs even before receiving them directly. Additional immunity against frame losses enabled as the beacons can be received by multiple neighbor bSTAs near the bSTA so their measurements can be relayed using the broadcasting mechanism.

The protocol enables multiple degrees of freedom that can be tuned for optimizing the overall network performance. For example, the amount of data included in the beacon that defines the minimal subrate, at which the clients may wake up, and the beacon broadcasting rate. Consider, for instance, a broadcasting rate of 2 Hz, where each beacon contains the last second of timing measurements (both ToA and ToD) captured by that bSTA. Such rate enables the cSTAs to wake up only once a second to update their position and clock estimates. Furthermore, the timing measurements history-window length affects the "First-Fix" scenario as the accuracy of the position and clock offsets initial estimates is proportional to the amount of data included. On the other

[6]The SVs orbital motion generates a substantial Doppler offset on the GNSS carrier frequency, which enables to estimate the GNSS receiver's 3-D speed. Thus, the EKF state vector in GNSS receivers typically includes a total of 6+2N states: three states for the receiver position, three states for the 3-D receiver speed, and two additional states for the clock model, which are tracked per satellite constellation (i.e., GLONASS, Galileo etc.).

hand, the broadcasting rate and amount of data each broadcast contain affect the Wi-Fi network traffic and its level of congestion. For a typical Wi-Fi network, which relies on a ±25 ppm XO stability, a 2–5 Hz bSTA beacon broadcasting rate and 600 ms of history-window are sufficient for cSTAs to track the clock behavior of the bSTAs in the network.

Being an unmanaged and unidirectional protocol (without any REQUEST-ACK scheme between the network nodes), CToA facilitates a rather simple interoperability between AP/bSTA and cSTA units produced by different vendors. Furthermore, as the bSTAs may be network detached units, which implies they do not require any wired "backbone" network infrastructure and thus may be easily moved around the venue. This gives yet another degree of flexibility during the network deployment and performance tuning phase for achieving optimal performance.

VII. Conclusion

A novel protocol for scalable Wi-Fi client self-positioning using cooperative FTM-sensors was presented. The CToA protocol is designed to enable scalability of existing IEEE 802.11/Wi-Fi FTM-based, geolocation systems. It relies on a periodic broadcast of time-delay measurement frames transmitted by an unmanaged network of bSTAs placed at known locations called bSTA. These measurements, which may be collected independently by an unlimited number of receiving clients, are combined with similar time-delay measurements reported by the bSTAs and enable passive clients to estimate their location within the network and navigate indoors while maintaining their privacy. The network can also be used simultaneously for tracking thousands of broadcasting clients, which enables the support of a variety of applications, such as asset tracking, data analytics, and so on. Due to the infrequent nature of the broadcasts and the clock source quality of both the client and bSTAs, the clocks tend to drift appreciably between the measurement events. To solve this, the client uses a Kalman filter for estimating and tracking the clock-related system parameters, as well as its instantaneous position coordinates.

System-level simulations and real-life system experiments indicate that the network is capable of reaching a positioning accuracy roughly 2 m in 95% of the cases in congested, multipath-dense Wi-Fi indoor environments.

Appendix

The following Appendix is excerpted from [16].

A. CToA Cramér Rao Lower Bound

We shall now derive the CRLB for the method in the absence of clock drifts. The CRLB provides a lower bound on the covariance matrix of any unbiased estimator.

1) CRLB Client in "First Fix" Mode: Since the observations vector, $\mathbf{z}$, is distributed as, $\mathbf{z} \sim \mathcal{N}(\boldsymbol{\mu}, \mathbf{W})$, the ijth entry of the Fisher information matrix (FIM) may be obtained as [25, Ch. 8, eq. (8.36)]

$$\mathbf{J}_{ij} = \mathrm{tr}\left\{\mathbf{W}^{-1}\frac{\partial \mathbf{W}}{\partial \psi_i}\mathbf{W}^{-1}\frac{\partial \mathbf{W}}{\partial \psi_j}\right\} + 2\left\{\frac{\partial \boldsymbol{\mu}^T}{\partial \psi_i}\mathbf{W}^{-1}\frac{\partial \boldsymbol{\mu}}{\partial \psi_j}\right\} \quad (57)$$

where ψ_i is the ith element of the parameters vector, $\boldsymbol{\psi} \triangleq [\mathbf{p}^T, \boldsymbol{\nu}^T]^T$. Since the noise covariance matrix, $\mathbf{W}$, is free of any unknown parameters, (57) becomes

$$\mathbf{J}_{ij} = 2\left\{\frac{\partial \boldsymbol{\mu}^T}{\partial \psi_i}\mathbf{W}^{-1}\frac{\partial \boldsymbol{\mu}}{\partial \psi_j}\right\}. \quad (58)$$

For $\boldsymbol{\mu} \triangleq c^{-1}\mathbf{d} + \mathbf{E}\boldsymbol{\nu}$, the partial derivatives with respect to the client's position coordinates are given by

$$\begin{aligned}\frac{\partial \boldsymbol{\mu}}{\partial x} &= c^{-1}\dot{\mathbf{d}}_x \equiv c^{-1}\left[\dot{\tilde{\mathbf{d}}}_x^T, \mathbf{0}_L^T\right]^T \\ \frac{\partial \boldsymbol{\mu}}{\partial y} &= c^{-1}\dot{\mathbf{d}}_y \equiv c^{-1}\left[\dot{\tilde{\mathbf{d}}}_y^T, \mathbf{0}_L^T\right]^T \\ \frac{\partial \boldsymbol{\mu}}{\partial \nu_i} &= \mathbf{E}\mathbf{e}_i\end{aligned} \quad (59)$$

where $\dot{\tilde{\mathbf{d}}}_x, \dot{\tilde{\mathbf{d}}}_y$ denote the vectors containing the partial derivatives with respect to the client's position coordinates, which are given by

$$\frac{\partial \bar{d}_i}{\partial x} = -\frac{(x_i - x)}{\sqrt{(x_i - x)^2 + (y_i - y)^2}} \quad (60)$$

$$\frac{\partial \bar{d}_i}{\partial y} = -\frac{(y_i - y)}{\sqrt{(x_i - x)^2 + (y_i - y)^2}}. \quad (61)$$

Using (59), the FIM elements can be found as

$$\begin{aligned}J_{xx} &= 2c^{-2}\dot{\mathbf{d}}_x^T\mathbf{W}^{-1}\dot{\mathbf{d}}_x = \frac{2}{c^2\bar{\sigma}^2}\dot{\tilde{\mathbf{d}}}_x^T\dot{\tilde{\mathbf{d}}}_x \\ J_{xy} &= J_{yx} = 2c^{-2}\dot{\mathbf{d}}_x^T\mathbf{W}^{-1}\dot{\mathbf{d}}_y = \frac{2}{c^2\bar{\sigma}^2}\dot{\tilde{\mathbf{d}}}_x^T\dot{\tilde{\mathbf{d}}}_y \\ J_{yy} &= 2c^{-2}\dot{\mathbf{d}}_y^T\mathbf{W}^{-1}\dot{\mathbf{d}}_y = \frac{2}{c^2\bar{\sigma}^2}\dot{\tilde{\mathbf{d}}}_y^T\dot{\tilde{\mathbf{d}}}_y \\ J_{x\nu_i} &= 2c^{-1}\dot{\mathbf{d}}_x^T\mathbf{W}^{-1}\mathbf{E}\mathbf{e}_i \\ J_{y\nu_i} &= 2c^{-1}\dot{\mathbf{d}}_y^T\mathbf{W}^{-1}\mathbf{E}\mathbf{e}_i \\ J_{\nu_i\nu_j} &= 2\mathbf{e}_i^T\mathbf{E}^T\mathbf{W}^{-1}\mathbf{E}\mathbf{e}_j.\end{aligned} \quad (62)$$

Define

$$\mathbf{J}_{\mathbf{pp}} \triangleq \begin{bmatrix} J_{xx} & J_{xy} \\ J_{yx} & J_{yy}\end{bmatrix} \quad (63)$$

$$\mathbf{J}_{\mathbf{p}\boldsymbol{\nu}} \triangleq \begin{bmatrix} \mathbf{J}_{x\boldsymbol{\nu}} \\ \mathbf{J}_{y\boldsymbol{\nu}}\end{bmatrix}. \quad (64)$$

The FIM is given by

$$\mathbf{J} = \begin{bmatrix} \mathbf{J}_{\mathbf{pp}} & \mathbf{J}_{\mathbf{p}\boldsymbol{\nu}} \\ \mathbf{J}_{\mathbf{p}\boldsymbol{\nu}}^T & \mathbf{J}_{\boldsymbol{\nu}\boldsymbol{\nu}}\end{bmatrix}. \quad (65)$$

The CRLB is obtained by inverting the complete FIM (see [25, Ch.8, eq. (8.166)])

$$\mathbf{J}^{-1} = \left[\begin{array}{c|c} \left(\mathbf{J}_{\mathbf{pp}} - \mathbf{J}_{\mathbf{p}\boldsymbol{\nu}}\mathbf{J}_{\boldsymbol{\nu}\boldsymbol{\nu}}^{-1}\mathbf{J}_{\mathbf{p}\boldsymbol{\nu}}^T\right)^{-1} & () \\ \hline () & ()\end{array}\right]. \quad (66)$$

The bound on the position coordinates is given by the top-left block of $\mathbf{J}^{-1}$

$$\mathbf{C}_{\mathbf{pp}}^{1^{\mathrm{st}}\mathrm{Fix}} = \left[\mathbf{J}_{\mathbf{pp}} - \mathbf{J}_{\mathbf{p}\boldsymbol{\nu}}\mathbf{J}_{\boldsymbol{\nu}\boldsymbol{\nu}}^{-1}\mathbf{J}_{\mathbf{p}\boldsymbol{\nu}}^T\right]^{-1}. \quad (67)$$

2) Approximate CRLB for a Client in "Tracking Mode": When the EKF is converged and the bSTA clock offsets are known (up to some residual error), and are being continuously tracked, then $\boldsymbol{\mu} \simeq c^{-1}\mathbf{d}$, and $\boldsymbol{\psi} \triangleq \mathbf{p}$.

Consequently

$$\mathbf{J}_{ij} \simeq \frac{2}{c^2(\bar{\sigma}^2+\sigma_r^2)}\left\{\frac{\partial \boldsymbol{\mu}^T}{\partial \psi_i}\frac{\partial \boldsymbol{\mu}}{\partial \psi_j}\right\}. \tag{68}$$

The partial derivatives are obtained using (59), and the CRLB on the position coordinates estimation error is obtained by

$$\begin{aligned}\mathbf{C}_{\mathbf{pp}}^{\text{Tracking}} &\simeq \frac{1}{J_{xx}J_{yy}-J_{xy}^2}\begin{bmatrix} J_{yy} & -J_{xy} \\ -J_{xy} & J_{xx}\end{bmatrix} \\ &= \begin{bmatrix}\sigma_{xx}^2 & \sigma_{xy} \\ \sigma_{xy} & \sigma_{yy}^2\end{bmatrix}. \end{aligned}\tag{69}$$

B. Proof of Proposition 1

Assume that every broadcast includes $\tilde{N}$ replicas of the timing measurements collected by the bSTA. Recall that $\mathcal{L}$ denotes the number of broadcast timing measurements that were measured by the client itself, then if the clock offsets were time-invariant then one could define

$$\check{\mathbf{E}} \triangleq \begin{bmatrix}\bar{\mathbf{E}} \\ \hdashline \mathbf{1}_{\tilde{N}} \otimes \tilde{\mathbf{E}}\end{bmatrix}, \quad \check{\mathbf{W}} \triangleq \begin{bmatrix}\bar{\sigma}^2\mathbf{I}_{\mathcal{L}} & \mathbf{0} \\ \mathbf{0} & \tilde{\sigma}^2\mathbf{I}_{\tilde{N}\times L}\end{bmatrix}. \tag{70}$$

Next, from (62), we have

$$J_{v_i v_j} = 2\mathbf{e}_i^T\mathbf{E}^T\mathbf{W}^{-1}\mathbf{E}\mathbf{e}_j. \tag{71}$$

Then, under (70), $J_{v_i v_j}$ becomes

$$\begin{aligned}\check{J}_{v_i v_j} &= 2\mathbf{e}_i^T\check{\mathbf{E}}^T\check{\mathbf{W}}^{-1}\check{\mathbf{E}}\mathbf{e}_j \\ &= 2\mathbf{e}_i^T\left[\bar{\sigma}^{-2}\bar{\mathbf{E}}^T \,\vdots\, \tilde{\sigma}^{-2}\mathbf{1}_{\tilde{N}}^T\otimes\tilde{\mathbf{E}}^T\right]\begin{bmatrix}\bar{\mathbf{E}} \\ \hdashline \mathbf{1}_{\tilde{N}}\otimes\tilde{\mathbf{E}}\end{bmatrix}\mathbf{E}\mathbf{e}_j \\ &= 2\mathbf{e}_i^T(\bar{\sigma}^{-2}\bar{\mathbf{E}}^T\bar{\mathbf{E}} + \tilde{N}\cdot\tilde{\sigma}^{-2}\tilde{\mathbf{E}}^T\tilde{\mathbf{E}})\mathbf{e}_j \\ &\underset{\tilde{N}\to\infty}{\approx} 2\tilde{N}\tilde{\sigma}^{-2}\mathbf{e}_i^T\tilde{\mathbf{E}}\tilde{\mathbf{E}}^T\mathbf{e}_j. \end{aligned}\tag{72}$$

Recall that from (67), we have

$$\mathbf{C}_{\mathbf{pp}}^{1^{\text{st}}\text{Fix}} = \left[\mathbf{J}_{\mathbf{pp}} - \mathbf{J}_{\mathbf{p}\boldsymbol{\nu}}\mathbf{J}_{\boldsymbol{\nu}\boldsymbol{\nu}}^{-1}\mathbf{J}_{\mathbf{p}\boldsymbol{\nu}}^T\right]^{-1}. \tag{73}$$

Hence, under $\tilde{N}\to\infty$, $\check{\mathbf{J}}_{\mathbf{p}\boldsymbol{\nu}}\check{\mathbf{J}}_{\boldsymbol{\nu}\boldsymbol{\nu}}^{-1}\check{\mathbf{J}}_{\mathbf{p}\boldsymbol{\nu}}^T \to 0$.

Thus, given enough bSTA→bSTA measurements (equivalent to an EKF in "Tracking mode"), $\mathbf{C}_{\mathbf{pp}}^{1^{\text{st}}\text{Fix}} \approx \mathbf{C}_{\mathbf{pp}}^{\text{Tracking}}$ (up to additive noise level scaling).

This concludes the proof.

ACKNOWLEDGMENT

An earlier version of this paper has been presented as a whitepaper during the September 2017 meeting of IEEE 802.11 TGaz in Waikoloa, HI (see [16]). Specifically, Sections II-A and II-B, the great majority of Section III, most of the discussion in Section VI, and the Appendix have been reused from that whitepaper.

REFERENCES

[1] E. Au, "The latest progress on IEEE 802.11mc and IEEE 802.11ai [standards]," *IEEE Veh. Technol. Mag.*, vol. 11, no. 3, pp. 19–21, Sep. 2016.

[2] *IEEE Standard for Information Technology–Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks–Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Standard 802.11-2016, 2016.

[3] E. Perahia and R. Stacey, *Next Generation Wireless LANs: 802.11n and 802.11ac*, 2nd Ed. Cambridge, U.K.: Cambridge Univ. Press, 2013.

[4] B. Sundararaman, U. Buy, and A. D. Kshemkalyani, "Clock synchronization for wireless sensor networks: A survey," *Ad Hoc Netw.*, vol. 3, no. 3, pp. 281–323, 2005.

[5] A. Makki, A. Siddig, and C. J. Bleakley, "Robust high resolution time of arrival estimation for indoor WLAN ranging," *IEEE Trans. Instrum. Meas.*, vol. 66, no. 10, pp. 2703–2710, Oct. 2017.

[6] P. Serrano, P. Salvador, V. Mancuso, and Y. Grunenberger, "Experimenting with commodity 802.11 hardware: Overview and future directions," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 671–699, 2nd Quart., 2015.

[7] X. Li and K. Pahlavan, "Super-resolution TOA estimation with diversity for indoor geolocation," *IEEE Trans. Wireless Commun.*, vol. 3, no. 1, pp. 224–234, Jan. 2004.

[8] F. X. Ge, D. Shen, Y. Peng, and V. O. K. Li, "Super-resolution time delay estimation in multipath environments," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 54, no. 9, pp. 1977–1986, Sep. 2007.

[9] P. J. Voltz and D. Hernandez, "Maximum likelihood time of arrival estimation for real-time physical location tracking of 802.11a/g mobile stations in indoor environments," in *Proc. IEEE Position Location Navigat. Symp. (PLANS)*, Apr. 2004, pp. 585–591.

[10] F. Bandiera, A. Coluccia, G. Ricci, F. Ricciato, and D. Spano, "TDOA localization in asynchronous WSNs," in *Proc. 12th IEEE Int. Conf. Embedded Ubiquitous Comput.*, Milano, Italy, Aug. 2014, pp. 193–196.

[11] F. Ricciato, S. Sciancalepore, F. Gringoli, N. Facchi, and G. Boggia, "Position and velocity estimation of a non-cooperative source from asynchronous packet arrival time measurements," *IEEE Trans. Mobile Comput.*, vol. 17, no. 9, pp. 2166–2179, Sep. 2018.

[12] R. T. Rajan and A. J. V. D. Veen, "Joint ranging and synchronization for an anchorless network of mobile nodes," *IEEE Trans. Signal Process.*, vol. 63, no. 8, pp. 1925–1940, Apr. 2015.

[13] L. Banin, U. Schatzberg, and Y. Amizur, "Next generation indoor positioning system based on WiFi time of flight," in *Proc. 26th Int. Tech. Meeting Satellite Division Inst. Navigat.*, Nashville TN, USA, Sep. 2013, pp. 975–982.

[14] L. Banin, U. Schatzberg, and Y. Amizur, "WiFi FTM and map information fusion for accurate positioning," in *Proc. Int. Conf. Indoor Positioning Indoor Navigat. (IPIN)*, Alcalá de Henares, Spain, Oct. 2016. [Online]. Available: http://www3.uah.es/ipin2016/usb/app/descargas/215_WIP.pdf

[15] N. Dvorecki, O. Bar-Shalom, and Y. Amizur, "AoD-based positioning for Wi-Fi OFDM receivers," in *Proc. 30th Int. Tech. Meeting Satellite Division Inst. Navigat. (ION GNSS)*, Portland, OR, USA, Sep. 2017, pp. 2883–2893.

[16] L. Banin, O. Bar-Shalom, N. Dvorecki, and Y. Amizur, *High-Accuracy Indoor Geolocation Using Collaborative Time of Arrival(CToA)—Whitepaper*, document IEEE 802.11-17/1387R0, Sep. 2017. [Online]. Available: https://mentor.ieee.org/802.11/dcn/17/11-17-1387-00-00az-high-accuracy-indoor-geolocation-using-collaborative-time-of-arrival-ctoa-whitepaper.pdf

[17] L. Banin, O. Bar-Shalom, N. Dvorecki, and Y. Amizur. *Reference-PE-and-Measurements-DB-for-WiFi-Time-Based-Scalable-Location*. Accessed: Apr. 2018. [Online]. Available: https://github.com/intel/Reference-PE-and-Measurements-DB-for-WiFi-Time-based-Scalable-Location

[18] H. Kim, X. Ma, and B. R. Hamilton, "Tracking low-precision clocks with time-varying drifts using Kalman filtering," *IEEE/ACM Trans. Netw.*, vol. 20, no. 1, pp. 257–270, Feb. 2012.

[19] J. J. Leonard, H. F. Durrant-Whyte, and I. J. Cox, "Dynamic map building for an autonomous mobile robot," *Int. J. Robot. Res.*, vol. 11, no. 4, pp. 286–298, Aug. 1992.

[20] M. A. Lombardi, T. P. Heavner, and S. R. Jefferts, "NIST primary frequency standards and the realization of the SI second," *NCSLI Meas.*, vol. 2, no. 4, pp. 74–89, 2007.

[21] P. D. Groves, *Principles of GNSS, Inertial, and Multisensor Integrated Navigation Systems*, 1st ed. Boston MA, USA: Artech House, 2008.

[22] A. Pásztor and D. Veitch, "PC based precision timing without GPS," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 30, no. 1, pp. 1–10, Jun. 2002.
[23] D. J. Torrieri, "Statistical theory of passive location systems," *IEEE Trans. Aerosp. Electron. Syst.*, vol. AES-20, no. 2, pp. 183–198, Mar. 1984.
[24] H. L. Van Trees, *Optimum Array Processing: Part IV of Detection, Estimation, and Modulation Theory*. New York, NY, USA: Wiley, 2002.
[25] *Intel Dual Band Wireless-AC 8260: Product Brief*. Accessed: 2015. [Online]. Available: https://www.intel.com/content/www/us/en/wireless-products/dual-band-wireless-ac-8260-brief.html

Leor Banin received the B.Sc. degree *(magna cum laude)* in electrical engineering from Tel-Aviv University, Tel Aviv, Israel, in 2001, with a focus on digital signal processing and communications.

He has been involved in very large scale integration chip design, DSP firmware, and algorithms development for wireless communications systems. Since 2010, he has been a Researcher with Intel's Location Core Division, Petah Tikva, Israel. He has co-authored several conference papers. He holds over 30 patents in the field of wireless communications and geolocation applications. His current research interests include signal processing, geolocation and inertial navigation systems, and machine learning applications.

Ofer Bar-Shalom received the B.Sc. degree in mechanical engineering and the M.Sc. and Ph.D. degrees in electrical engineering from Tel-Aviv University, Tel Aviv, Israel, in 1997, 2001, and 2015, respectively.

He has been involved in cellular and wireless connectivity systems development for over 20 years. He is currently a Researcher with Intel's Location Core Division, Petah Tikva, Israel. He has authored multiple journal and conference papers. He holds over 15 patents in the fields of wireless communications, real-time systems, multimedia, and geolocation applications. His current research interests include signal processing, geolocation, navigation and radar systems, and machine learning applications.

Nir Dvorecki received the B.Sc. degree in electrical engineering, and the B.Sc. degree in physics in 2012, and the M.Sc. degree in electrical engineering in 2015, all from Tel-Aviv University, Tel Aviv, Israel.

Since 2015, he has been a Researcher with the Intel's Location Core Division, Petah Tikva, Israel. His current research interests include geolocation, inertial navigation systems, and machine learning applications.

Yuval Amizur received the B.Sc. degree *(summa cum laude)* in electrical engineering from the Technion—Israel Institute of Technology, in 1996, and the MBA degree *(magna cum laude)* and the M.Sc. degree *(summa cum laude)* in electrical engineering from Tel-Aviv University, Tel Aviv, Israel, in 2002 and 2008, respectively.

He has been involved in cellular and wireless connectivity systems development for over 20 years. He has been leading Intel's Location Core Division Algorithms Group in Petah Tikva, Israel. He has co-authored several conference papers, and holds over 30 patents in the field of wireless communications and geolocation applications. His current research interests include signal processing, geolocation, inertial navigation systems, and machine learning applications.