SYNCHRONIZATION OF LOW-COST DISTRIBUTED SPECTRUM SENSING NODES FOR MULTILATERATION-BASED GEOLOCATION

Stefan Grönroos (stefan.gronroos@abo.fi)[1,2], Kristian Nybom (kristian.nybom@abo.fi)[2], and Jerker Björkqvist (jerker.bjorkqvist@abo.fi)[2]

[1]Turku Centre for Computer Science (TUCS), Turku, Finland
[2]Åbo Akademi University, Turku, Finland

ABSTRACT

In this work, we show how a distributed sensing network consisting of very low-cost nodes can also be used to locate radio transmitters without prior knowledge of which waveform is used. This information can aid in increasing location awareness among cognitive radios, as well as provide assistance in locating offending transmitters. The low accuracy of the internal clocks of these low-cost receivers as well as the geographical distribution of the nodes result in significant challenges regarding the synchronization of the receivers in order to position the source with adequate accuracy. In this paper, we synchronize the nodes to an arbitrary modulated RF signal, after which we calculate estimated time differences of arrival (TDOAs) to an unknown transmitter. We describe the implementation as well as give results on measurement accuracy in various scenarios using a prototype network of nodes spread out in the city of Turku, Finland.

1. INTRODUCTION

Previously, the authors of this work evaluated and proposed a spectrum sensing system in the form of a distributed network of very low-cost nodes[1]. These nodes consist of Raspberry Pi mini-computers coupled with USB dongles with software defined radio (SDR) reception capabilities. While the receivers themselves are inferior to dedicated spectrum sensing equipment, it was argued that the very low cost of each node (roughly 50 USD) enables a large and dense network of sensing nodes to be built. This, together with suitable software for fusion of the sensing information received from each node, could compensate for the deficiencies of the individual nodes, while providing much more local measurements than a less dense network of more costly nodes.

In this paper, we explore a complementary use case for such a network of geographically distributed sensing nodes. Through the well established procedure of multilateration, the network could be utilized to determine the source of detected RF transmissions. Multilateration using time differences of arrival (TDOAs), however, requires fine-grained synchronization of the receivers in time in order to be able to determine TDOAs to each node from an unknown transmitter. Wishing to keep each node simple and thus low-cost, we explore a technique where we use a signal from a known source location to synchronize the I/Q sample streams from each node, after which we utilize this synchronization to determine the difference in arrival times from the unknown source to pairs of sensing nodes.

The capability of locating unknown transmitters can aid in generating more detailed spectrum usage data in cognitive radio (CR) environments. This may also be useful for instance in order to track non-compliant transmitters interfering with communications.

In [2], the authors set up a system of low-cost sensors using Ettus Research USRP hardware in each node. TDOA measurements are used to calculate the location of unknown transmitters. The USRP hardware is however significantly more expensive than the hardware setup used in this work. The authors of [2] also used GPS synchronization, while in this work, we synchronize to arbitrary known signals. Navigation using non-GPS signals of opportunity such as TV and radio broadcasts has also been discussed in, among others, [3], [4] and [5]. The system presented in [3] uses timing information obtained from ATSC (Advanced Television Systems Committee) digital television signals for geolocation both indoors and outdoors. Field measurements showed promising results also in locations with poor GPS coverage.

In [4], a system where receivers do not know their position beforehand, and cooperatively locate themselves using signals of opportunity such as television and AM radio signals, is explored. The differential TDOA approach described is designed to eliminate the need for synchronous receiver clocks, and takes into account clock drift between receivers. The paper only presents simulations, and not field measurements, however. The idea of a large network of cooperating nodes for navigation is also discussed in [5]. Through simulations, the suitability of WCDMA (Wideband Code Division Multiple Access), digital television and GSM (Global System for Mobile Communications) signals for navigation were investigated.

The paper is structured as follows. In section 2, we describe multilateration, and the requirements for performing it. In section 3, we describe the components of the sensing network, while section 4 describes the algorithm used to synchronize

samples from each node, and the implementation of these algorithms. In section 5 we present initial results, as well as some discussion. We conclude the paper in section 6.

2. MULTILATERATION

Multilateration is a technique which can be used for locating the source of signals using geographically distributed sensing nodes. Typically this is done through measuring the time of arrival (TOA) of the signal at each node, or through measuring the time difference of arrival (TDOA) between pairs of nodes (see figure 1). Let τ_i and τ_j be the times of arrival at nodes i and j. Then $\tau_{i,j} = \tau_i - \tau_j$ is the TDOA between nodes i and j. An estimate, $\hat{\tau}_{i,j}$, of the TDOA can be determined, for example, by cross-correlation of the received signal at both nodes. The location of the cross-correlation peak will be correspond to the TDOA. The distance difference to the source can be calculated as $c\tau_{i,j}$, with c being the speed of light.

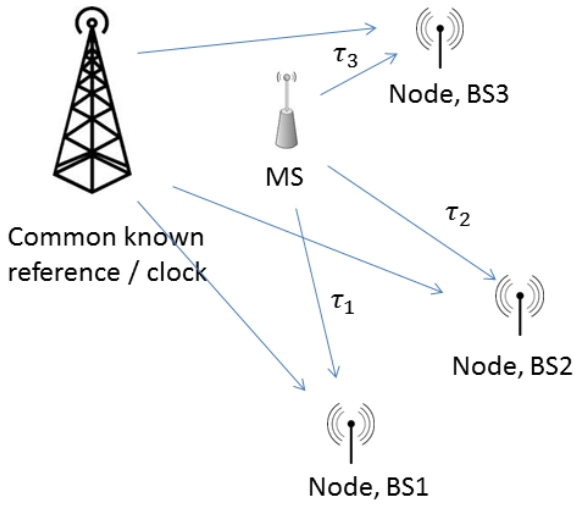

Figure 1: System overview for multilateration

Each TDOA measurement gives an infinite number of possible source locations located on a hyperboloid in 3D space, or on a hyperbola on a plane. From K sensors, we can calculate $\big((K-1)K\big)/2$ unique TDOAs (noting that $\tau_{i,j} = -\tau_{j,i}$). In the noise-free case, the intersection point of all hyperboloids or hyperbolas yields the source location. Given well distributed nodes, we may need 3 and 4 TDOA measurements to locate the source in 2D and 3D space respectively. When noise is present in the TDOA measurements, we use optimization algorithms to try to minimize the error caused by noise.

In the work of [6] the authors explore positioning algorithms for cellular networks using TDOA. In their work, the position of the Mobile Stations (MS) is analyzed in the perspective of observed TDOA (OTDoA), part of the 3GPP standard, as mentioned in [7]. In most analyses, however, the assumption is that the MS is using information received from Base Stations (BS) for determining their *own* position. This information could be TDOAs, when using well time synchronized BS (i.e. a μs synchronization error leads to a distance offset of 300 m). In more coarse systems, information on typical signal strengths or signal characteristics patterns can be used, when BSs are ordinary FM radio transmitters or TV transmitters. In our case, we do it the other way around, and measure the TDOA observed in the spectrum observers, for which their own locations are known.

The theory for TDOA based MS positioning is described in [6]. We use their notation, but use our system, meaning that the base stations correspond to our receivers numbered from 1 to the total number of receivers, N_{BS}. The MS is our transmitter to be localized at position $\mathbf{x} = [x, y]^T$. The BS are at positions $\mathbf{x}_\nu, \nu \in 1, 2, \ldots, N_{BS}$. The distance between a BS and and the MS is given by

$$r_\nu(\mathbf{x}) = \|\mathbf{x}_\nu - \mathbf{x}\| = \sqrt{(x_\nu - x)^2 + (y_\nu - y)^2} \tag{1}$$

We can treat distances and propagation times as equal, hence TDOAs for BS ν vs BS 1 can be given by

$$d_{\nu,1}(\mathbf{x}) = r_\nu(\mathbf{x}) - r_1(\mathbf{x}) \tag{2}$$

where BS1 is one of the receivers used as a reference. Now, with N_{BS} independent base stations (in our case receivers), we get $N_{BS} - 1$ measurements given by

$$\mathbf{d} = [d_{2,1}, d_{3,1}, \ldots, d_{N_{BS},1}] \tag{3}$$

based on the measurement model

$$\mathbf{d} = d(\mathbf{x}) + \mathbf{n} \tag{4}$$

where $\mathbf{n} = [n_{2,1}, n_{3,1}, \ldots, d_{N_{BS},1}]$ is zero mean Additive White Gaussian Noise (AWGN). When this is set into the context of our measurement systems giving OTDOA $\tau_{i,j}$ we get

$$\mathbf{d} = c[\hat{\tau}_{2,1}, \hat{\tau}_{3,1}, \ldots, \hat{\tau}_{N_{BS},1}] \tag{5}$$

Introducing the cost function, based on Nonlinear Least Squares (for reference [8]),

$$\xi(\mathbf{x}) = (\mathbf{d} - d(\mathbf{x}))(\mathbf{d} - d(\mathbf{x}))^T \tag{6}$$

and minimizing the cost function over the unknown MS position,

$$\hat{\mathbf{x}} = \arg\min_x \xi(\mathbf{x}) \tag{7}$$

we can find an estimate $\hat{\mathbf{x}}$ for the position.

In general, there is no closed form solution to this optimization problem, hence iterative approaches have to be used, such as Gauss-Newton, Steepest Descent or Levenberg-Marquardt.

When sampling the signal from each location, the signal needs to be precisely synchronized in time, in order to distinguish between delays resulting from unsynchronized receivers

and delays resulting from TDOA. A common technique for keeping the receivers precisely synchronized is through the use of GPS. Using GPS disciplined clocks is however an additional cost to the system, and also makes the system dependent on the availability of a GPS signal.

3. SETUP

In this section, we describe the various components, both hardware and software, of our experimental spectrum sensing network.

3.1. Sensor nodes

The sensor nodes consist of a Raspberry Pi mini-computer, which is equipped with a single-core 700 MHz ARM11 CPU and 512 MB of RAM. The SDR receiver is a USB dongle intended for the reception of DVB-T, DAB, and FM radio broadcasts. The dongle contains a Realtek RTL2832U demodulation chip and a Rafael Micro R820T tuner chip. It has been discovered that the demodulation chip is capable of outputting raw 8-bit I/Q samples in addition to decoding DVB-T on-chip. This capability was originally used to decode DAB and FM radio, but has lately made these dongles highly popular as low-cost SDR receivers [9]. The dongles are capable of streaming samples at approximately 2.5 MS/s reliably. A sample sensor node is shown in figure 2. The Raspberry Pi model used for the sensor nodes costs roughly 35 USD, while the DVB-T dongle costs less than 15 USD, yielding a total cost of roughly 50 USD for the bare hardware and a low-quality antenna. Peripherals such as storage media (a Secure Digital card is required for the Raspberry Pi), power supplies, enclosures and perhaps higher quality antennas add to this price.

3.2. SDR dongle oscillator

The main 28.8 MHz crystal oscillator — which is used both for the tuner chip, and for the ADC clock — used in the dongle is quite inaccurate, on the order of 100 ppm. This makes it problematic to use in applications requiring accurate synchronization of the sampled data from several dongles. The frequency offset caused by the crystal can be partially compensated for, for example using the frequency correction channel (FCCH) of GSM networks to calibrate the dongle.

It is important to let the dongle reach operating temperature before measurements, in order to minimize crystal frequency drift. Using a temperature controlled crystal oscillator (TCXO) could improve the stability of the clock significantly. The goal of this work is however to keep modifications, and thus cost, to a minimum.

3.3. Distribution of receivers

For our experiments, we distributed three RPi-based sensor nodes across the city of Turku, Finland. Figure 3 shows the locations of the three RPi nodes, as well as the Kuusisto and Metsämäki transmitters used for the experiments described in section 5. The distance from RPi 3 to RPi 1 was approximately 1.2 km, and to RPi 2 approximately 4.3 km. Table 1 shows further information on the antenna type and placement of the various measurement nodes. Note that RPi 2 was only equipped with a low quality antenna, and placed inside of a concrete apartment building, while RPi 1 and 3 were connected to superior antennas, with better placement. Figure 4 shows node RPi 3 mounted in an enclosure on the roof of an office building.

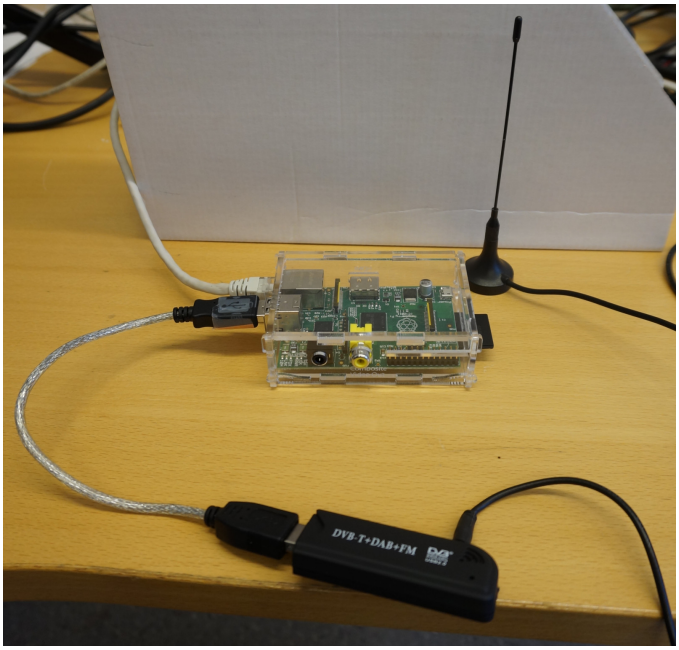

Figure 2: A Raspberry Pi-based sensor node, with SDR capable USB dongle attached.

Table 1: Description of the various nodes seen in fig. 3

Node	Antenna	Placement
RPi 1	Wideband double discone	On balcony
RPi 2	Simple wire antenna	Inside apartment
RPi 3	Wideband antenna	Roof of office bldg.

4. IMPLEMENTATION

The RPi nodes described in section 3 are connected to the Internet, and raw I/Q samples can be sent to a central computer for processing. The implementation relies on the observation that if the SDR dongle is tuned to a new frequency, the sample stream remains uninterrupted (i.e. no samples are seemingly lost during tuning). This feature allows us to tune between a known reference signal, and the signal of interest, while maintaining a constant sample rate, which allows us to synchronize the sample

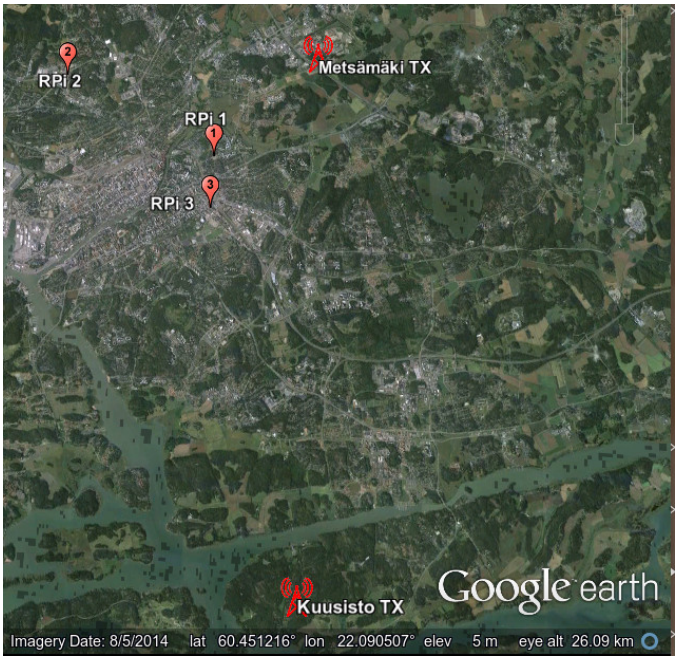

Figure 3: Placement of the RPi-based sensor nodes (RPi 1 to 3 in figure), as well as transmitters used in experiments, in Turku, Finland.

streams from different receivers using the reference signal.

In the following, we assume a sampling frequency of F_s, a correlation window length of T_c seconds, and a guard interval length of T_g seconds. Let $\mathbf{p}_i$ be the position of measurement node i, and $\mathbf{q}_c$ and $\mathbf{q}_t$ be the positions of the reference (known) and target (unknown) transmitters respectively. The algorithm run on the receiving computer to acquire the samples from each node is roughly the following:

1. Tune each node to known receiver's frequency f_c, and start receiving samples over the network connection.
2. Wait for $T_c + 2T_g$ s.
3. Tune each receiver to f_t, the frequency of interest.
4. Wait for $T_c + 2T_g$ s.
5. Send command to tune back to f_c.
6. Wait for $T_c + T_g$ s.
7. Stop receiving when a total of $(3T_c + 5T_g) * F_s$ samples have been collected from each node.

This timing and sampling order is also illustrated in figure 5. The commands to tune to a new frequency were transmitted over the network, and were thus subject to various network delays. The guard intervals were used as unsafe zones, where the node might be tuned to any frequency due to various latencies.

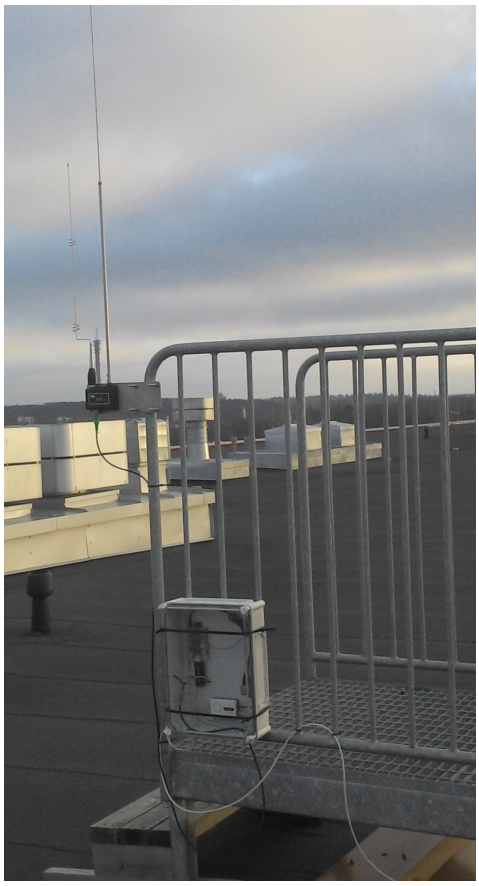

Figure 4: Node RPi 3 in a weatherproof enclosure beside the antenna on the roof of an office building.

Now, let $r_i[n], n \in [1, (3T_c + 5T_g) * F_s]$ be the raw samples from node i.

Then for each $n \in [1, T_c F_s]$, let

$$
\begin{aligned}
v_i[n] &= r_i[n + T_g F_s] \\
u_i[n] &= r_i[n + (T_c + 3T_g) F_s] \\
w_i[n] &= r_i[n + (2T_c + 5T_g) F_s]
\end{aligned}
$$

$\mathbf{v}_i$ and $\mathbf{w}_i$ thus correspond to the signal from two measurements on the reference frequency f_c, while $\mathbf{u}_i$ corresponds to the signal of interest as measured from node i.

For each unique pair of nodes (i, j), let

$$\tau_{v_i,v_j} = \arg\max_k \left(\max_\Delta \mathcal{F}_D^{-1}(\mathcal{F}_D\{v_i[n]\}^* \cdot s_\Delta \circ \mathcal{F}_D\{v_j[n]\})[k] \right)$$

, where $\mathcal{F}_D$ is the discrete Fourier transform using FFT, and $s_\Delta(\mathbf{x})$ is a discrete circular shift of Δ samples on $\mathbf{x}$. τ_{u_i,u_j} and τ_{w_i,w_j} are defined in the same way.

I.e. using FFT-based cross-correlation, we maximize the correlation peak between the measured signal from nodes i and j over a set of frequency shifts applied to the measurement from

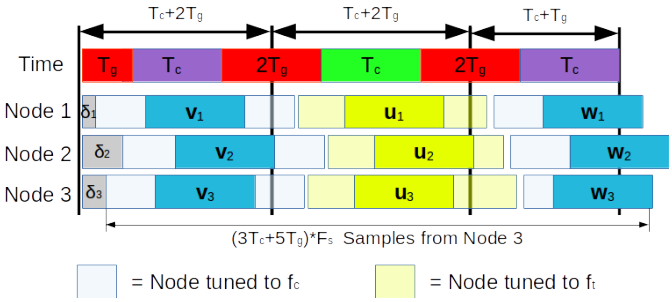

Figure 5: Diagram illustrating the order and timing of sampling using three example nodes.

node j. The index of the maximum peak gives us a delay in an integer number of samples. The frequency shifts are performed to compensate for tuning and sampling frequency deviations between the nodes due to unsynchronized oscillators.

τ_{v_i,v_j} and τ_{w_i,w_j} thus correspond to the delay between the sample streams received from nodes i and j when tuned to f_c the first and second time respectively. Likewise, τ_{u_i,u_j} corresponds to the same delay when tuned to f_t. These delays are the result of several factors. In addition to the delay of interest resulting from the TDOA between the transmitter and the two receivers, there is also a (typically much larger) delay caused by the jitter in measurement start times between nodes caused by network latencies and internal hardware and software delays. This initial delay δ_i for node i is illustrated in figure 5.

Ideally,

$$\begin{aligned}\tau_{v_i,v_j} &\equiv \tau_{w_i,w_j} \\ &\equiv (\frac{F_s}{c}(\|\mathbf{p}_i - \mathbf{q}_c\|) + \delta_i) - (\frac{F_s}{c}(\|\mathbf{p}_j - \mathbf{q}_c\|) + \delta_j) \\ &= \frac{F_s}{c}(\|\mathbf{p}_i - \mathbf{q}_c\| - \|\mathbf{p}_j - \mathbf{q}_c\|) + (\delta_i - \delta_j)\end{aligned}$$

and similarly,

$$\tau_{u_i,u_j} \equiv \frac{F_s}{c}(\|\mathbf{p}_i - \mathbf{q}_t\| - \|\mathbf{p}_j - \mathbf{q}_t\|) + (\delta_i - \delta_j)$$

Thus, again in the ideal case, we can eliminate the unknown $(\delta_i - \delta_j)$ term, and get an estimation on the difference in TDOA between a pair of nodes and the two transmitters as follows:

$$\begin{aligned}&\tau_{v_i,v_j} - \tau_{u_i,u_j} \\ &= \frac{F_s}{c}\Big((\|\mathbf{p}_i - \mathbf{q}_c\| - \|\mathbf{p}_j - \mathbf{q}_c\|) - (\|\mathbf{p}_i - \mathbf{q}_t\| - \|\mathbf{p}_j - \mathbf{q}_t\|)\Big)\end{aligned}$$

, or equivalently

$$\begin{aligned}&\|\mathbf{p}_i - \mathbf{q}_t\| - \|\mathbf{p}_j - \mathbf{q}_t\| = \\ &\|\mathbf{p}_i - \mathbf{q}_c\| - \|\mathbf{p}_j - \mathbf{q}_c\| - \frac{c}{F_s}(\tau_{v_i,v_j} - \tau_{u_i,u_j})\end{aligned} \tag{8}$$

where the TDOA of interest is the left hand side of the equation. The right hand side can be calculated, as we know the distances between our measurement nodes and the reference transmitters.

As $\tau_{v_i,v_j} = \tau_{w_i,w_j}$ in the ideal case, the second measurement of f_c should not be necessary. However, the measured delay will often "drift", likely due to sampling rate mismatch. Since the signal of interest, u_i was sampled between v_i and w_i, we attempt to correct for this drift by assuming the delay excluding the TDOA difference to be $\tau'_{i,j} = (\tau_{v_i,v_j} + \tau_{w_i,w_j})/2$. Thus equation 8 becomes

$$\begin{aligned}&\|\mathbf{p}_i - \mathbf{q}_t\| - \|\mathbf{p}_j - \mathbf{q}_t\| = \\ &\|\mathbf{p}_i - \mathbf{q}_c\| - \|\mathbf{p}_j - \mathbf{q}_c\| - \frac{c}{F_s}(\tau'_{i,j} - \tau_{u_i,u_j})\end{aligned} \tag{9}$$

5. RESULTS AND DISCUSSION

In this section we will present initial results from measurements using the three RPi nodes described in section 3. The transmitters were located at Metsämäki and Kuusisto, as shown in figure 3. The Kuusisto site broadcasts many different FM and DVB-T channels to the Turku area. The Metsämäki site broadcasts only FM radio channels.

To measure the accuracy of the algorithm and see the impact of two very different types of signals on the accuracy, the first experiment was to estimate the distance differences according to equation 9 when both the reference and target transmitters were either two DVB-T channels, or two FM stations transmitted from the Kuusisto site. In this case $\tau'_{i,j} - \tau_{u_i,u_j}$ should ideally be zero.

A sampling frequency F_s of 1.8MS/s, and a correlation window length of 262144 samples were used. The selected F_s implies that one sample corresponds to 165.5 meters. As the 1.8 MHz bandwidth is smaller than the 8 MHz bandwidth of the DVB-T signal, no filter was used when measuring against a DVB-T signal. For FM radio, a 120 kHz low-pass filter was used in order to measure only the FM signal of interest and not neighboring FM channels as well.

The results of this experiment are shown in table 2, where the average error and the standard deviation are shown for both the FM and DVB measurements. We can see that when FM transmitters were used, the errors and standard deviations were generally significantly higher than when DVB signals were used. This is expected, as broadband signals tend to correlate better, when measured during the same time period. It's also worth noting that FM radio measurements might be severely affected by the type of content being broadcast during the sampling window. For example, if there is only silence during the 150 ms sampling window, we will mostly correlate against a pure carrier wave, which does not yield a good delay estimate.

As a follow-up experiment, we chose to attempt to locate the Metsämäki site using one of its FM radio broadcasts, using a DVB-T transmission at Kuusisto as a reference transmitter. The same sampling rate and correlation window size were used. The results of this experiment can be found in table 3. A map showing geographic points that are less than 170 m from at least one hyperbola defined by the average distance differences generated by this experiment is shown in figure 6. The map is rendered as a

Table 2: Distance error measurements with FM and DVB-T signals, where both reference and target transmitter are at the Kuusisto site. Measurements were taken for each pair of RPi nodes, and averaged over 6 measurements per pair.

Measure	RPi (1,2)	RPi (1,3)	RPi (2,3)
f_c = 103.9 MHz (FM Radio) and f_t = 89.8 MHz (FM Radio)			
Average error (m)	513	291	416
Standard deviation (m)	479	907	96
f_c = 698 MHz (DVB-T) and f_t = 714 MHz (DVB-T)			
Average error (m)	42	125	97
Standard deviation (m)	267	142	217

Table 3: Distance error measurements when using the Kuusisto DVB-T transmitter at 698 MHz as a reference, and the FM radio channel at 105.5 MHz at Metsämäki as the target. Measurements were taken for each pair of RPi nodes, and averaged over 10 measurements per pair.

Measure	RPi (1,2)	RPi (1,3)	RPi (2,3)
Average error (m)	733	230	806
Standard deviation (m)	144	221	144

heatmap, where the red areas are areas where several hyperbolas intersect.

From the map in figure 6, one "hotspot" is located roughly 1-1.5 km from the target Metsämäki transmitter. The explanation for this error can be seen in table 3, where the pairs (1,2) and (2,3) give an average error of 700-800 m, despite quite a low standard deviation. RPi node 2 was equipped with a very simple antenna, with the antenna inside an apartment building. This error is thus quite likely due to the non line-of-sight (NLOS) placement of the antenna. The pair (1,3) gives a much smaller average error, which is likely due to these nodes being connected to better antennas, and mounted higher up on their respective buildings.

Based on these initial results, it seems clear that further emphasis should be placed on mitigating the effect of NLOS receivers on the system. This issue was also identified in [2]. In [10], a mitigation strategy in a TOA scenario where measurements are weighed according to their reliability is discussed. The method assumes no knowledge of which signals suffer from NLOS effects, but requires that the number of range measurements (i.e. the number of sensor nodes) are larger than the bare minimum. The authors of [11], propose a method for NLOS node identification using TDOA residuals (difference between measured and estimated distances). Lower bounds on range errors in TDOA positioning systems affected by NLOS effects are discussed in e.g. [12, 13].

The effect that the unsynchronized, drifting, oscillators have on accuracy should also be further investigated. It is also worth noting that the cross correlation step in equation 4 becomes very computationally complex if the receiver clocks have not been calibrated quite well to some reference beforehand. This is due to the fact that the set of frequency shifts Δ to search through

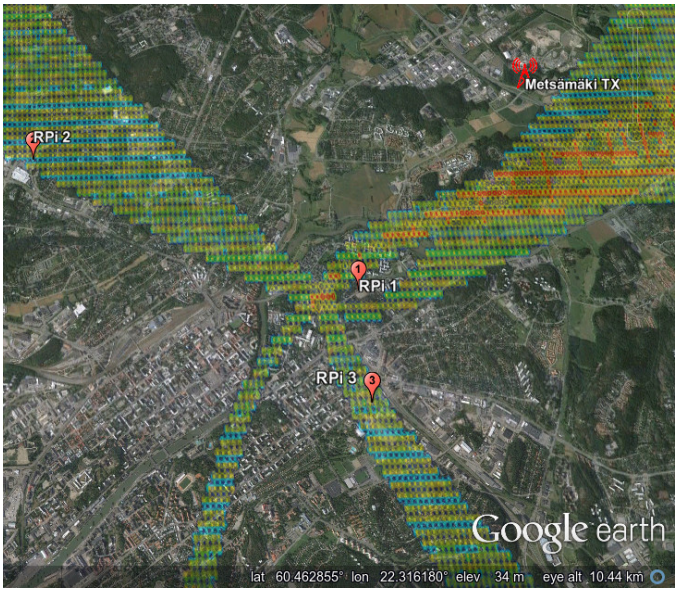

Figure 6: Map showing the three hyperbolic curves resulting from the average distance differences calculated when using the Kuusisto DVB-T transmitter at 698 MHz as a reference, and the FM radio channel at 105.5 MHz at Metsämäki as the target. The hyperbolas have been rendered as a heatmap of geographic points that are less than 170 m from a hyperbola. The red areas show points where several hyperbolas roughly intersect.

needs to be larger if the sampling and tuner frequencies between nodes are further apart.

In the implementation described in this work, the commands to begin sampling, and to tune between f_c and f_t were sent to nodes across the network. A more reliable approach would be to send the sampling schedule ahead of time, and make sure that the local computer clocks are synchronized reasonably well (to roughly 10-100 ms) using for example the NTP (network time protocol). This would reduce the required guard interval length.

6. CONCLUSION

In this paper, we described a method for synchronizing low-cost spectrum sensing nodes using RF signals with a known origin in order to estimate TDOAs to an unknown transmitter for later use in multilateration-based geolocation.

Initial measurements show that the method works, and could certainly contribute some rough location information on transmitters in a cognitive radio environment. The initial measurements showed some weaknesses of the system when targeting narrowband signals, and conversely quite promising results when targeting wideband signals. As some measurements might have been seriously affected by multipath propagation due to poor receiver placement, methods for mitigating these effects should be investigated. This could be achieved by the use of a larger number of more widely distributed nodes in combination

with methods for ranking measurements according to their apparent reliability.

Furthermore, the multilateration algorithm should be implemented to complete the system. The location algorithm could also be tightly coupled with the spectrum sensing software, in order to enable efficient positioning of new signals as they show up in the spectrum sensing sweeps.

REFERENCES

[1] S. Grönroos, K. Nybom, J. Björkqvist, J. Hallio, J. Auranen, and R. Ekman, "Distributed Spectrum Sensing Using Low Cost Hardware," in *Proceedings of the 2014 Wireless Innovation Forum European Conference on Communications Technologies and Software Defined Radio (WInnComm-Europe 2014)*, Nov 2014.

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

[3] M. Rabinowitz and J. Spilker, J.J., "A new positioning system using television synchronization signals," *Broadcasting, IEEE Transactions on*, vol. 51, no. 1, pp. 51–61, March 2005.

[4] C. Yan and H. Fan, "Asynchronous differential TDOA for non-GPS navigation using signals of opportunity," in *Acoustics, Speech and Signal Processing, 2008. ICASSP 2008. IEEE International Conference on*, March 2008, pp. 5312–5315.

[5] M. Enright and C. Kurby, "A signals of opportunity based cooperative navigation network," in *Aerospace Electronics Conference (NAECON), Proceedings of the IEEE 2009 National*, July 2009, pp. 213–218.

[6] C. Mensing and S. Plass, "Positioning Algorithms for Cellular Networks Using TDOA," in *Acoustics, Speech and Signal Processing, 2006. ICASSP 2006 Proceedings. 2006 IEEE International Conference on*, vol. 4, May 2006, pp. IV–IV.

[7] Y. Zhao, "Standardization of mobile phone positioning for 3G systems," *Communications Magazine, IEEE*, vol. 40, no. 7, pp. 108–116, Jul 2002.

[8] F. Gustafsson and F. Gunnarsson, "Mobile positioning using wireless networks: possibilities and fundamental limitations based on available wireless network measurements," *Signal Processing Magazine, IEEE*, vol. 22, no. 4, pp. 41–53, July 2005.

[9] Osmocom, "OsmocomSDR (Wiki)," http://sdr.osmocom.org/trac/wiki/rtl-sdr (Accessed 13.06.14), 2014.

[10] P.-C. Chen, "A non-line-of-sight error mitigation algorithm in location estimation," in *Wireless Communications and Networking Conference, 1999. WCNC. 1999 IEEE*, 1999, pp. 316–320 vol.1.

[11] L. Cong and W. Zhuang, "Non-line-of-sight error mitigation in TDOA mobile location," in *Global Telecommunications Conference, 2001. GLOBECOM '01. IEEE*, vol. 1, 2001, pp. 680–684 vol.1.

[12] Y. Qi and H. Kobayashi, "Cramer-Rao Lower bound for geolocation in non-line-of-sight environment," in *Acoustics, Speech, and Signal Processing (ICASSP), 2002 IEEE International Conference on*, vol. 3, May 2002, pp. III–2473–III–2476.

[13] J. Xu, M. Ma, and C. Law, "Theoretical Lower Bound for UWB TDOA Positioning," in *Global Telecommunications Conference, 2007. GLOBECOM '07. IEEE*, Nov 2007, pp. 4101–4105.