Cognitive Interference Avoidance in 4th Generation GPS

Brian Kelley
Department of ECE
University of Texas at San Antonio
San Antonio, TX, U.S.A.
Brian.Kelley@utsa.edu

Gonzalo De La Torre Parra
Department of ECE
University of Texas at San Antonio
San Antonio, TX, U.S.A.
Gonzalo_delatorre@live.com

David Akopian
Department of ECE
University of Texas at San Antonio
San Antonio, TX, U.S.A.
David.Akopian@utsa.edu

Abstract - *GPS systems have revolutionized the way people and social networks in society interact. As GPS becomes more ubiquitous in road transportation, energy, or autonomous delivery drones, there is increasing opportunity for adversaries and malicious attackers to exploit GPS infrastructure so as to hijack or damage position-sensitive systems. We propose the development of a precise positioning system that can be implemented in terrestrial metropolitan networks that is also capable of interference avoidance, hi-jack prevention, and operational in GPS denied environments. The significant contribution of this work is the development of cognitive GPS system that utilizes a novel anti-jamming algorithm to dynamically allocate signal power so as to avoid interference. We also propose a resource elements encryption algorithm to prevent hi-jacking and GPS spoofing.*

Keywords: positioning, 4G, 5G, GPS, interference avoidance, cyber security, spoofing, jamming, cognitive

1 Introduction

The emergence of wireless systems as inexpensive, ubiquitous connectivity devices generates an opportunity to leverage pervasive wireless communications in new ways. The efficiency of delivering information is directly related to the spectral efficiency of the communication network. In many planned cellular networks, fixed geometry constraints allow relatively easy analysis of spectral efficiency. The incorporation of newer, more spectrally efficient communication devices and protocols has become commonplace. Hence the advent of future 4G Wireless networks (e.g. LTE-Advanced [1-4]) is directly traceable to the improved network capacity of the multi-user OFDMMIMO networks. As new communication networks emerge, an increasingly important application category involves proximity-based spatial location information. In this paper, we hypothesize that future unplanned wireless networks, harnessing the wide-scale availability of ubiquitous wireless connectivity, will increasingly benefit by integrating location position systems to aid with multi-hop routing protocols [5,6]. Independently, since many emerging communication protocols have convergently evolved towards multi-carrier orthogonal frequency division multiplexing (MC-OFDM) [5], we describe new hybrid concepts involving a conjoining of cooperative position system estimation and next generation MC-OFDM wireless air interfaces. Frequency domain positioning demonstrate clear advantage capability in anti-jamming avoidance, MIMO positioning, privacy transmission, and bandwidth adaptable positioning.

2 Securing GPS Against Adversaries

The terrestrial model illustrated in Figure 1is based upon a metropolitan area configuration that avoids the use of satellites. In the case of an adversarial jammers, the signal power is much less than the interference. The well known $SNIR$ in dB is presumed negative.

Figure 2 illustrates the three principle innovations for secure GPS system signaling. Firstly, timing delay estimation is based upon frequency domain timing using OFDM Zadoff-Chu sequences. Secondly, the frequency domain timing signal are optimally allocated in power and spectral frequency band to avoid interference. We maximize signal to noise plus inteference (SNIR) as a means of optimum interference avoidance in the presence of noise and fading channels. The interference avoidance algorithm utlizes a waterfilling algorithm that we discus in the next section. The interference avoidance in the TX system locates nulls in adversary jamming signal. The feedback channel from the receiver system enables the transmitter to allocate maximum transmit power in the interference nulls. Thirdly, we propose encrypting a message authentication signal at the source using RSA encryption or other suitable methods. The encrypted authentication message is a BPSK modulate signal with amplitude combined with the Zadaoff-Chu sequence. The purpose of authentication is to thwart well known GPS-spoofing. In spoofing, the adversary transmits network style GPS signals that are capable of creating artificial range and locations estimation in the Rx system. This secure GPS system is illustrated in Figure 2.

3 System Model for GPS Interference Avoidance in Ricean Fading

The baseband indicator signal for range estimation is defined as $s(t)$. The operation framework adopts a Rician fading channel model, $h(t)$. We communicate with a target receiver at an unknown Euclidian distance between the source a and receiver b, r_{ab}. It is noted that the family of Constant Amplitude Zero Auto-Correlation (CAZAC) sequences forms an important class of signals useful for

978-1-4799-7611-9/15/$31.00 ©2015 IEEE

correlation metrics in ranging. The Zadoff-Chu poly phase sequence of length N (without loss of generality, N even) [7]-[11] is applied. For p relatively prime to N, the frequency domain Zadoff-Chu sequence of length N is given by

$$\mathrm{S[k]} \triangleq \exp\left(-\frac{\mathrm{j}\left(\frac{2\pi}{\mathrm{N}}\right)\mathrm{pk}^2}{2}\right)\ \mathrm{k} \in \left\{-\frac{\mathrm{N}}{2} \ldots \frac{\mathrm{N}}{2} - 1\right\} \quad (1)$$

Defining $\Delta_f \triangleq \frac{f_S}{N}$, the cyclic prefix is CP, an FFT of size N bins, $L \triangleq (N + CP)$, and the cyclic prefix time duration $T_{cp} = LT_s$, the time domain sequence with cyclic prefix is

$$\mathrm{s[n]} = \frac{1}{\mathrm{N}} \sum_{\mathrm{k}=-\frac{\mathrm{N}}{2}}^{\frac{\mathrm{N}}{2}-1} \mathrm{S[k]} \exp\left(\mathrm{j}2\pi \mathrm{f_k}[\mathrm{n} - \mathrm{CP}]\right), \mathrm{n} = 0 \ldots \mathrm{L} - 1$$

3.1 Interference Avoidance in Jamming

To properly take full advantage of the correlation properties of the Zadoff-Chu sequence [12]-[19], so as to transmit it in the most efficient manner, we allocate signal power optimally across bins using water filling [20]. Total transmit power will imply the total number of bins used for transmit. The frequency response of the Rician fading channel is defined as $H[k\Delta_f]$, where Δ_f is set as the spacing between the resource elements in the frequency domain. In our scenarios $\Delta_f = 15\ KHz$.

With a lost of generality OFDM symbol transmit power is fixed and the noise and interference are varied to achieve signal to noise plus interference ratios. We have selected waterfilling thresholds as a control signal for allocation of power across the band. We define the received signal power as $S_{rx}[k\Delta_f]$. This leads us to express the signal power gain at the receiver $\gamma_k[k\Delta_f]$ with amplitude dependent upon the Rician fading channel gain, the noise variance and the path loss dependent receiver signal power.

$$\gamma_k[k\Delta_f] \triangleq \frac{(H[k\Delta_f] \times H[k\Delta_f]^*) \times \sum S_{rx}[K\Delta_f]}{V[k\Delta_f] + I[k\Delta_f]} \quad (2)$$

The spectral resource elements in γ_k greater than one standard deviation, σ_{γ_k}, from $E[\gamma_k]$ correspond to joint nulls in interference and high channel gain. With this finding, γ_k in dB is

$$\gamma_{kdB}[k\Delta_f] = 10log_{10}(\gamma_k[k\Delta_f]) \quad (3)$$

$$\sigma^2_{\gamma_{dB}} = 10log_{10}\left(E(\gamma^2_{kdB}) - \left(\mu_{\gamma_{kdB}}\right)^2\right)$$

$$\mu_{\gamma_{kdB}} \triangleq \frac{1}{K_0} \sum_{k=-\frac{K_0}{2}}^{\frac{K_0}{2}-1} \gamma_{kdB}[k\Delta_f] \quad (4)$$

$$E[\gamma_{kdB}] = \frac{\sum \gamma_{kdB}[k\Delta_f]}{n} \quad (5)$$

The selected resource elements of $\gamma_{klog}[k\Delta_f]$ are defined as $S\gamma_{klog}[k\Delta_f]$. This corresponds to the nulls in the adversary jamming signal and indicates the resource elements with the highest gain. The information is conveyed via the feedback channel from the receiver to the transmit system

$$S\gamma_{kdB}[k\Delta_f] \triangleq \gamma_{kdB}[k\Delta_f], \quad \text{if} \quad \gamma_{kdB}[k\Delta_f] > \sigma^2_{\gamma_{kdB}} + E[\gamma_{kdB}] \quad (6)$$

We set a threshold to γ_0, for the power allocation based upon an optimum water filling gain for each resource element such that

$$P_\gamma[k\Delta_f] = \left(\frac{1}{\gamma_0} - \frac{1}{\gamma_k[k\Delta_f]}\right) \times Pt, \quad \gamma \geq \gamma_0 \quad (7)$$

This appropriately allocates an optimum number of resource elements for use, per symbol. The optimum resource elements to use are selected opportunistically according to the Ricean channel, the interferer signal, and noise level. The power allocated per selected resource element occurs dynamically. The number of available bins per symbol is defined by the water filling procedure. The constructed Zadoff-Chu sequence must be segmented into N_s epochs (# of OFDM Symbols) to fit this sequence into multiple transmitted OFDM symbols. Thus,

$$S[k]_{n_s} \triangleq \exp\left(-\frac{\mathrm{j}\left(\frac{2\pi}{\mathrm{N_1}}\right)\mathrm{pk}^2}{2}\right), \ \mathrm{k} \in ([0,1, \ldots \mathrm{N_0} - 1] + \mathrm{n_s} \times \mathrm{N_0}), \ n_s \in \{0,1, \ldots \mathrm{N_s} - 1\}, \ \mathrm{N_s} \triangleq \mathrm{N_1/N_0} \quad (8)$$

This permits us to transmit a Zadoff-Chu transmit signal with a large sequence of elements. This provides, at the receiver, a peak amplitude during the correlation calculation proportional to the number of elements of the sequence. Large sequences provide greater advantage in low SNR and SNIR than short sequences.

Our model of spatial positioning in fading from the transmitter (Tx) perspective can be written as

$$\mathrm{Y[k\Delta_f]} = \mathcal{F}\left(\mathrm{s[n]}_{n_s} * \delta(\mathrm{n} - \tau_0) * \mathrm{h[n]} + \mathrm{v[n]} + \mathrm{i[n]}\right) \quad (9)$$

$$Y[k\Delta_f] = S[k\Delta_f] exp(-j2\pi k\Delta_f \tau_0) H[k\Delta_f] + V[k\Delta_f] + I[k\Delta_f] \quad (10)$$

The channel $h(t)$ is modeled as a Rician fading channel. The explicit propagation delay, encapsulated explicitly by $\delta(t - \tau_0)$, represents the source line of site (LOS) separation from the observed signal. To properly receive the signal and make a proper use of the Ricean Model, the LOS is assumed to be 8dB greater than the fading component. The Rician baseband equivalent signal is:

$$h(t) = \underbrace{\sqrt{\frac{K_f}{K_f+1}}}_{L} \underbrace{exp(j(2\pi f cos(\theta_l)t) + \propto_m)}_{\mathrm{h_0}} + \underbrace{\sqrt{\frac{1}{K_f+1}}}_{S} \mathrm{h_s(t)} \quad (11)$$

Therefore, from Eq (11):

$$H[k\Delta_f] = \underbrace{H_0 \Pi(k\Delta_f)}_{LOS} + \underbrace{\sqrt{\frac{1}{K_f+1}} H_s[k\Delta_f]\Pi(k\Delta_f)}_{NLOS} \quad (12)$$

At the receiver, we receive a delayed Tx signal. In the frequency domain the expectation would be the following:

$$Y[k\Delta_f] = S[k\Delta_f]exp(-j2\pi k\Delta_f\tau_0)H_0 + \underbrace{S[k\Delta_f]exp(-j2\pi k\Delta_f\tau_0)\sqrt{\frac{1}{K_f+1}}H_s[k\Delta_f]}_{ICI} + V[k\Delta_f] + I[k\Delta_f] \quad (13)$$

We note that the baseband OFDM signal $Y[k\Delta_f]$ is corrupted by an inter-carrier interference (ICI) signal due to the non-line of site self-interference. We desire to cancel this.

It can also be noted that Eq. (13) does not account for finite bandwidth effect. For the following results we approximate the channel by a discrete time process, $\beta(t) \triangleq \sum_{d=0}^{D-1} h_d\, \delta(t - \tau_d\,(t))$ band limited to bandwidth W and $\mathcal{F}(\mathrm{sinc}(Wt)) \Longrightarrow \Pi(f) \xrightarrow{DFT} \Pi(k\Delta_f)$.

Therefore, $y(t) = (\beta(t) * s(t) + N_0(t)) * sinc(Wt)$. Inserting $\beta(t)$, we arrive at:

$$y(t) = \sum_{d=0}^{D-1} h_d \sum_\tau s(\tau)\mathrm{sinc}\left(\frac{t}{T_s} - \tau/T_s - \tau_d^l(t)/T_s\right) + v(t) \quad (14)$$

Converting Eq. (14) from time to discrete frequency, we arrive at the frequency channel $(k\Delta_f)$. Separating into line of site (LOS) and non-line of site (NLOS) components:

$$H[k\Delta_f] = \underbrace{H_o[k\Delta_f]\Pi(k\Delta_f)}_{LOS} + \underbrace{\sqrt{\frac{1}{K_f+1}} H_s[k\Delta_f]\Pi(k\Delta_f)}_{NLOS} \quad (15)$$

Defining the LOS component via $H_0 \triangleq H - \mathbb{I}$, The ICI interference parameter is therefore

$$\mathbb{I}[k\Delta_f] = \sqrt{\frac{1}{K_f+1}} H_s[k\Delta_f]\Pi(k\Delta_f) \quad (16)$$

At this point it can be noted that at the receiver we do not have any information about the Ricean channel through which the OFDM Symbols containing the Zadoff-Chu sequence were transmitted. Due to this constraint, the *Ricean channel must be estimated* at the receiver. We now account for this. The sampled, estimated Ricean channel at the receiver is modeled as:

$$h_{estdel}[n] = (h[n] + \sigma_{\hat{H}}[n]) * \delta(\mathrm{n} - \tau) \quad (17)$$

where $\sigma_{\hat{H}}[n] = h[n] - h_{estdel}[n] * \delta(\mathrm{n} + \tau)$

Note that we define $\sigma_{\hat{H}}$ as the error between the actual Ricean channel and the estimated channel. It is expected that a lower $\sigma_{\hat{H}}$ permits us to more accurately eliminate the ICI component from $Y[k\Delta_f]$ in the discrete frequency domain. Error in the estimated channel $\sigma_{\hat{H}}$ has the following properties:

- The expected value of the error mean can be defined as: $E[\sigma_{\hat{H}}[n]] = 0\ for\ all\ n$
- The unit variance of the error can be defined as: $E[\sigma_{\hat{H}}[n]\sigma_{\hat{H}}[n]^*] = 1\ for\ all\ n$

From the statement in Eq. (15) we can separate the line of site (LOS) and non-line of site (NLOS) components in the time domain as:

$$h_{estdel}[n] = h_{los}[n] * \delta(\mathrm{n} - \tau) + h_{scat}[n] * \delta(\mathrm{n} - \tau) + \sigma_{\hat{H}los}[n] * \delta(\mathrm{n} - \tau) + \sigma_{\hat{H}scat}[n] * \delta(\mathrm{n} - \tau) \quad (18)$$

To properly use this estimated Ricean channel, we need to proceed to convert this estimated channel from the time domain to the frequency domain:

$$H_{estdel}[k\Delta_f] = \mathcal{F}(h_{estdel}[n]) \quad (19)$$

The time domain Rician channel at the receiver is modeled with a delay corresponding to $\delta(\mathrm{n} - \tau)$, the frequency Rician channel needs to be inversely phase shifted where at τ_0 is the ideal to reach the closest estimate to H:

The actual Rician channel is

$$H[k\Delta_f] \approx H_{estdel}[k\Delta_f]exp(j2\pi k\Delta_f\tau_0) \quad (20)$$

The estimated Rician channel at the receiver is

$$\hat{H}[k\Delta_f, \hat{\tau}_0] = H_{estdel}[k\Delta_f]exp(j2\pi k\Delta_f\hat{\tau}_0) \quad (21)$$

From Eq. (15) and Eq. (21) we can define:

$$\hat{H}[k\Delta_f, \hat{\tau}_0] = \underbrace{\widehat{H_o}[k\Delta_f, \hat{\tau}_0]\Pi(k\Delta_f)}_{LOS} + \underbrace{\sqrt{\frac{1}{K_f+1}}\hat{H}_s[k\Delta_f, \hat{\tau}_0]\Pi(k\Delta_f)}_{NLOS} \quad (22)$$

$$\underbrace{\hat{H}_0[k\Delta_f, \tau_0]\Pi(k\Delta_f)}_{LOS} \approx \underbrace{H_o[k\Delta_f]\Pi(k\Delta_f)}_{LOS} \quad (23)$$

$$\underbrace{\sqrt{\frac{1}{K_f+1}}\hat{H}_s[k\Delta_f, \tau_0]\Pi(k\Delta_f)}_{NLOS} \approx \underbrace{\sqrt{\frac{1}{K_f+1}}H_s[k\Delta_f]\Pi(k\Delta_f)}_{NLOS} \quad (24)$$

The prior equation implies that at τ_0, $\widehat{H}_0$ and $\widehat{H}_s$ are the closest approximate to H_o and H_s respectably. Therefore by the definition of Eq. (16) the ICI component $\mathbb{I}[k\Delta_f]$ is maximally approached when $\widehat{H}_s$ approaches to τ_0.

From Eq. (16) and Eq. (24) we can define:

$$\hat{\mathbb{I}}[k\Delta_f, \tau_0] \approx \mathbb{I}[k\Delta_f] \tag{25}$$

$$\hat{\mathbb{I}}[k\Delta_f, \hat{\tau}_0] = \underbrace{\sqrt{\frac{1}{K_f+1}}\widehat{H}_s[k\Delta_f, \hat{\tau}_0]\Pi(k\Delta_f)}_{\widehat{NLOS}} \tag{26}$$

One constraint that can affect the estimation performance $\widehat{H} \approx H$ is our lack of information about timing. To properly define the estimate, $\hat{\tau}_0$, we define the line of site (LOS) signal nominally as k=8dB greater than non-line of site (NLOS) scattering components of the Ricean Channel.

Therefore $H \approx \widehat{H}$ when:

$$\widehat{H}_0 \approx \widehat{H}_s \times 10^{(8/10)} \tag{27}$$

We now recover the baseband signal by eliminating the non-line of site (NLOS) component from the received signal:

$$X(k\Delta_f, \hat{\tau}_0) \triangleq (H[k\Delta_f]S[k\Delta_f]exp(-j2\pi k\Delta_f\tau_0)\Pi(k\Delta_f) - \hat{\mathbb{I}}[k\Delta_f]exp(-j2\pi k\Delta_f\hat{\tau}_0)\hat{S}[k\Delta_f]\Pi(k\Delta_f) + V[k\Delta_f] + I[k\Delta_f]) \tag{28}$$

After eliminating the non-line of site (NLOS) component from the baseband signal we are left with the LOS component left:

$$X(k\Delta_f) \triangleq (H_0[k\Delta_f]S[k\Delta_f]exp(-j2\pi k\Delta_f\tau_0)\Pi(k\Delta_f) + V[k\Delta_f] + I[k\Delta_f]) \tag{29}$$

To eliminate the delay from the baseband signal we can inverse phase shift Eq. (29) to determine $\hat{\tau}_0$:

$$X(k\Delta_f, \hat{\tau}_0) \triangleq (H_0[k\Delta_f]S[k\Delta_f]exp(-j2\pi k\Delta_f\tau_0)\Pi(k\Delta_f) + V[k\Delta_f] + I[k\Delta_f])exp(j2\pi k\Delta_f\hat{\tau}_0) \tag{30}$$

$$X(k\Delta_f, \hat{\tau}_0) \triangleq (H_0[k\Delta_f]S[k\Delta_f]\Pi(k\Delta_f) + V[k\Delta_f] + I[k\Delta_f]) \tag{31}$$

$$\tau_{opt} = \underset{\hat{\tau}_0}{max}\left(\sum_{k=-\frac{N}{2}}^{\frac{N}{2}-1} S[\langle k\rangle_N\Delta_f]\, X(k\Delta_f, \hat{\tau}_0)\right) \tag{32}$$

Eq. (31) represents the maximum likelihood delay estimate of the MC-OFDM baseband signal. The residual error between the optimum signal and the ideal LOS signal is $\tau_e \triangleq \tau_0 - \hat{\tau}_{opt}$. Therefore, the result of the OFDM correlation statistic at $\hat{\tau}_0$is the LOS channel coefficient.

3.2 Rician Multipath Fading Versus Cramer Rao Bound Performance Analysis

The previously stated method allows us to optimally define the delay $\hat{\tau}_0$ between one reference or AdHoc node to the target. In simulation we observed that a minimum of 7 nodes provides us with an acceptable estimate when using the Cramer Rao Bound, but more reference nodes can be used. Figure 1 illustrates a 5-node (eNB) system. Once all the delay estimates $\hat{\tau}_0$ have been calculated, we can proceed to (X,Y) location of the target . *The conversion from range estimate to (X,Y) position is outlined in the Appendix.* The Euclidian error in meters between the target $\tilde{u}$ and the target guess $\tilde{v}$ is defined by:

$$\varepsilon_d = |\tilde{u} - \tilde{v}|$$

We now describe the Cramer Rao bound and (X,Y) positioning. From [21], for the OFDM positional reference symbol (PRS) γ, delay τ_0 AWGN noise $v(t)$, the receive signal $y(t)$ can be written as

$$\mathrm{y(t)} = \mathrm{s}_\gamma(\mathrm{t} - \tau_0) + \mathrm{v(t)} \tag{33}$$

We note that

$$s_\gamma(t) = \sum_{\gamma=0}^{\Gamma-1}\sum_{k=-N/2}^{N/2-1} \tag{34}$$

$$H[k]x_\gamma[k]\mathrm{p(t} - \gamma\mathrm{LT}_s)\mathrm{exp}(j2\pi f_k[t - \gamma\mathrm{LT}_s]) \tag{35}$$

The subcarrier frequency bin is k and sampling frequency f_s. The system estimates τ_0 from observations $y(t)$. Let us define the Fourier transform of the noiseless received signal as:

$$S_y(f, \boldsymbol{\eta}) = \sum_{\gamma=0}^{\Gamma-1}\sum_{k=-\frac{N}{2}}^{\frac{N}{2}-1} \tag{36}$$

$$H[k]x_\gamma[k]\mathrm{p(f} - \mathrm{f}_k)\,\mathrm{exp}(-j2\pi f\gamma\mathrm{LT}_s)\,\mathrm{exp}(-j2\pi f\tau_0) \tag{37}$$

The Cramer Rao Bound is $[\boldsymbol{J}^{-1}]_{1,1}$ where $\boldsymbol{J}$ is the Fisher information matrix, and $\boldsymbol{\eta} = [\tau_0, x_\gamma[k], H[k]]$ from [21]:

$$[\boldsymbol{J}]_{ro,co} = Re\left\{\int_{-\infty}^{\infty}\frac{\delta S_r^*(f,\boldsymbol{\eta})}{\delta\eta_{ro}}\frac{1}{S_w(f)}\frac{\delta S_r(f,\boldsymbol{\eta})}{\delta\eta_{co}}df\right\} \tag{38}$$

The parameter $S_w(f) = N_o$ is the power spectral density of the noise at each k.

4 Simulation Results

A model of the work described on this paper was developed using Matlab. Three scenarios were tested to use for comparison (1) AWGN, (2) AWGN and fading, and (3) AWGN, fading and interference.

On all tests, a Zadoff-Chu sequence composed of 2048 elements was constructed. In tests b and c it is

assumed that we can identify the Ricean's channel LOS component from the NLOS component. Also, the variance of the channel estimate $(\sigma_{\hat{H}})^2$ was varied for performance comparison. A total of 35 target estimates were calculated per test in Figures 4-8. All tests assumed single antenna performance. Even at -15 dB SNIR (i.e. high interference), Figure 8 indicates 1 meter accuracy in realistic channel estimation.

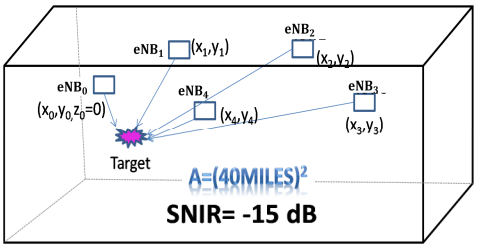

Figure 1. Metropolitan Area System Framework

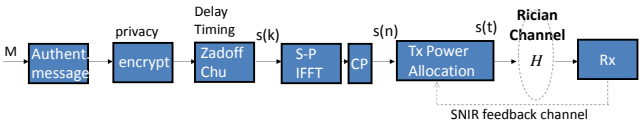

Figure 2. GPS Secure Model

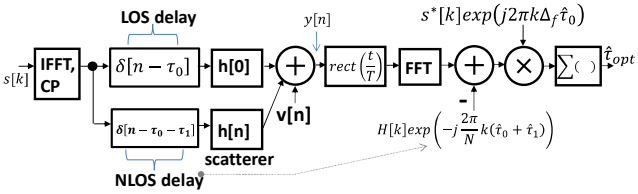

Figure 3. Timing model in fading

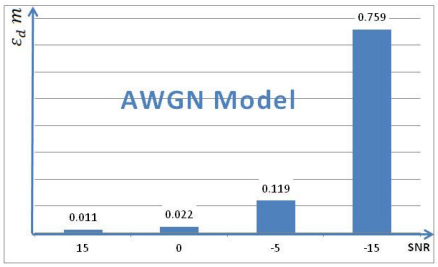

Figure 4. (X,Y) position error in AWGN

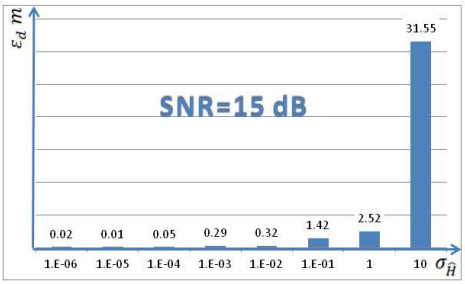

Figure 5. (X,Y) position error in Fading at 15dB SNR as a function of channel estimation error standard deviation.

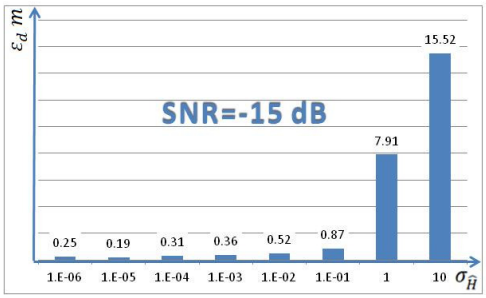

Figure 6. (X,Y) position error in Fading at -15dB SNR as a function of channel estimation error standard deviation.

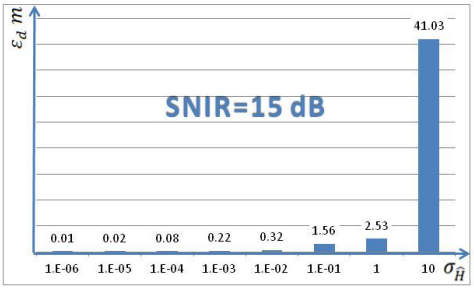

Figure 7. (X,Y) position error in Fading and interference at at 15dB SNIR as a function of channel estimation error standard deviation.

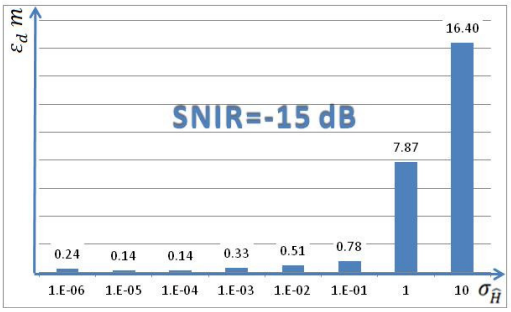

Figure 8. (X,Y) position error in Fading and interference at at -15dB SNIR as a function of channel estimation error standard deviation.

5 Conclusions

The proposed GPS system introduces the concept of using interference avoidance as a tool for dynamic adaptation to adversarial jamming. The results are for single antenna systems, but point to tremendous potential gain for future multi-antenna configurations. We offer innovative resource elements and power allocation in the frequency domain at the transmitter using waterfilling. The Zadoff-Chu sequence provides excellent correlation properties even under low SNR/SNIR. The tests demonstrated a distance error close to 1 cm at a SNR/SNIR of 15dB. Furthermore, it can be observed that as the estimated channel error $\sigma_{\hat{H}}$ decreases, distance error from the target ε_d in meters, reduces even at a SNR/SNIR of -15dB. The wide range of applications of this system includes the capability to thwart GPS spoofing and GPS jamming.

6 Appendix: 4G-PS: (X,Y) Spatial Position Estimation Via 4G Mobiles

Let us define, c, as the speed of light and f as the frequency of the specific (multi-carrier) OFDM symbol. The derivation proceeds as follows:

Define $\tilde{u} = x + jy$ as the target and $\tilde{v} = x_m + jy_m$ as the target guess, leveraging the notation of ([49],[50]) we find that

$|r_m|^2 = |\tilde{v}_m - u|^2 = (x_m - x)^2 + (y_m - y)^2 \rightarrow$

$|r_m|^2 = |\tilde{v}_m|^2 - 2x_m x - 2y_m y + x^2 + y^2$ (39)

$r^0_{a,b} \triangleq |r_a| - |r_b|,\ r_{a,b} \triangleq |r_a| - |r_b| + n_{a,b}$

$r_{m,0} = |\tilde{v}_m - \tilde{u}| - |\tilde{v}_0 - \tilde{u}|\ .$ (40)

$\therefore\ |r_m|^2 = \left(r^0_{m,0} + |r_0| + n_{m,0}\right)^2$ and (41)

$\left(r_{m,0}\right)^2 + 2r_{m,0}|r_0| + |r_0|^2 +$

$\underbrace{\left(n_{m,0}\right)^2 + 2\, n_{m,0}\left(r_{m,0} + |r_0|\right)}_{n_T} = |\tilde{v}_m|^2 - 2x_m x - 2y_m y +$

$x^2 + y^2$ (42)

Where n_T is an (x,y) position noise that is induced from observation range noise.

$x^2 + y^2 - 2x_m x - 2y_m y = \left(r_{m,0}\right)^2 +$

$2r_{m,0}|r_0| + |r_0|^2 - |\tilde{v}_m|^2 + n_T$ (43)

$|\tilde{v}_m|^2 - 2x_m x - 2y_m y + x^2 + y^2 = \left(r_{m,0}\right)^2 +$

$2r_{m,0}|r_0| + |r_0|^2 + n_T$ (44)

Let us define

$f(x, y, x_m, y_m) \triangleq |\tilde{v}_m|^2 - 2x_m x - 2y_m y + x^2 + y^2$ (45)

$f(x, y, x_m, y_m) = \underbrace{\left(r_{m,0}\right)^2 + 2r_{m,0}}_{TDOA}\ \underbrace{|r_0| + |r_0|^2 - |\tilde{v}_m|^2}_{\substack{Anchor\ Reference \\ Locations}} +$

$\underbrace{n_T}_{noise}$ (46)

We can now formally define the receiver measurement metric plus noise as:

$\Gamma_{\mathrm{m}}(\mathrm{r}) \triangleq \left(r_{m,0}\right)^2 + 2r_{m,0}|r_0| + |r_0|^2 - |\tilde{v}_m|^2 + n_T$ (47)

Noting that the time difference of arrival, is $\Delta t_{m,\tilde{u}} - \Delta t_{0,\tilde{u}}$, we can relate to distance via

$r^0_{m,0} = |\tilde{v}_m - u| - |\tilde{v}_0 - u| = c\left(\Delta t_{m,\tilde{u}} - \Delta t_{0,\tilde{u}}\right)$ (48)

Noting the delay relationship

$x(t - \Delta t) \overset{\mathcal{F}}{\leftrightarrow} |X(f)| exp(j[2\pi f \Delta t + \angle X(f)]),$

$r^0_{m,0} = \frac{c}{2\pi f}\left\{atan\left(\frac{Im[exp(j[2\pi f \Delta t_{m,\tilde{u}} + \angle X(f)])]}{Re[exp(j[2\pi f \Delta t_{m,\tilde{u}} + \angle X(f)])]}\right) -\right.$

$\left. atan\left(\frac{Im[exp(j[2\pi f \Delta t_{0,\tilde{u}} + \angle X(f)])]}{Re[exp(j[2\pi f \Delta t_{0,\tilde{u}} + \angle X(f)])]}\right)\right\}$ (49)

From this, let us further define

$A \triangleq$ (50)

$$\begin{bmatrix} \vdots & \vdots \\ \frac{\partial}{\partial x}\left[f(x, y, x_m, y_m)|_{(x_m, y_m)}\right] & \frac{\partial}{\partial y}\left[f(x, y, x_m, y_m)|_{(x_m, y_m)}\right] \\ \vdots & \vdots \end{bmatrix}$$

$\hat{\tilde{u}} = (A^T A)^{-1} A^T [f(x, y, x_m, y_m) - \Gamma_{\mathrm{m}}(\mathrm{r})] + \begin{bmatrix} x_m \\ y_m \end{bmatrix}$ (51)

From (22), we can define the key recursion equation

$\begin{bmatrix} x_m \\ y_m \end{bmatrix} = (A^T A)^{-1} A^T [f(x, y, x_m, y_m) - \Gamma_{\mathrm{m}}(\mathrm{r})] + \begin{bmatrix} x_{m-1} \\ y_{m-1} \end{bmatrix}$ (52)

References

[1] K. Takeda, S. Nagata, Y. Kishiyama, M. Tanno, K. Higuchi, M. Sawahashi, "Investigation on Optimum Radio Parameter Design in Layered OFDMA for LTE-Advanced," 2009 IEEE 69th Vehicular Technology Conference.

[2] A. Ibing, D. Kuhling, H. Boche, "Software Defined Hybrid MMSE/QRD-M Turbo Receiver for LTE Advanced Uplink on a Cell Processor," 2009 IEEE International Conference on Communications: ICC Communication Workshop.

[3] 3GPP TR-36.913 E-UTRA Requirements for Further Advancement for E-UTRA, LTE-Advanced, Release 10, April, 2011.

[4] 3GPP TS-36.201 E-UTRA TSPG RAN E-UTRA, LTE-Physical Layer, Release 10, Dec., 2010.

[5] Ha Duyen Trung, W. Benjapolakul, "Location-aided multipath routing method for mobile ad hoc wireless networks," Proc. of First Intl Conf. on Communications and Electronics (ICCE), October 2006, pp. 7-12.

[6] L. Blazevic, J.Y. Boudec, S. Giordano, "A location-based routing method for mobile ad hoc networks," IEEE Transactions on Mobile Computing, Vol. 4, No. 2, pp. 97-110, 2005.

[7] Brian Kelley, "Massively Parallel Cooperative Localization in Scalable Sensor Networks," Int. J. of Communication Networks and Distributed System (IJCNDS), 2010.

[8] Brian Kelley and Ed Rivas, "OFDM Location-Based Routing Protocols in Ad-Hoc Networks," IEEE Wireless Hive Conference, Austin, TX, 2008.

[9] M. Cohn and A. Lempel, "On Fast M-Sequence Transforms", IEEE Transactions on Information Theory, pp135-137, January 1977

[10] A. Lempel, M. Cohn, W. Eastman, "A Class of Balanced Binary Sequences with Optimal Autocorrelation Properties," IEEE Transactions on Information Theory," Vol. 23 Jan. 1977

[11] Branislav M. Popovic, "Generalized Chip-Like Polyphase Sequences with Optimum Correlation Properties," IEEE Transactions on Information Theory, Vo. 38, No. 4, 1992.

[12] Yilin Zhao, "Standardization of Mobile Phone Positioning for 3G Systems," IEEE Communications Magazine, July 2002, pp. 109-116

[13] Spirent. An overview of LTE positioning. White Paper. Feb. 2012.

[14] ERICSSON. Positioning with LTE. Maximizing performance through integrated solutions. White Paper. Sept. 2011.

[15] Open Mobile Alliance, SUPL 1.0 Requirement document, OMA-RD-SUPL-V10

[16] E.D. Kaplan. Understanding GPS: Principles and Applications. Boston: Artech House, 1996.

[17] P. Misra, P. Enge. Global Positioning System, Signals, Measurements, and Performance. Ganga-Jamuna Press, Lincoln, MA. 2001.

[18] US Global Positioning System. http://www.gps.gov/

[19] Russian Federal Space Agency. Information-analytical Centre. GLONASS. http://www.glonass-center.ru/en/

[20] A. Goldsmith, Wireless Communications, pp. 78-79, 374-401, Cambridge Univ. Press, 2005.

[21] M. Panchetti, "Design and analysis of a time-delay estimator for positioning of LTE wireless terminals",http://etd.adm.unipi.it/theses/available/etd-06272012-150833/unrestricted/Chapter5.pdf, Master Thesis, University of Pisa.