2011 American Control Conference
on O'Farrell Street, San Francisco, CA, USA
June 29 - July 01, 2011

Novel Multiplexing Technique in Anti-Jamming GNSS Receiver

Chung-Liang Chang, *Member, IEEE*

Abstract—**This paper proposes the multiplexing technique that combines signal detector, decision logic, and anti-J modules to counteract narrowband continuous wave interference and spoofing signal in global navigation satellite system (GNSS) receivers. The signal detector is to detect the presence of different types of jammers. The decision logic is utilized to select different anti-jam strategies against jammers. Effective carrier to noise ratio (C/No) is employed to assess the performance of proposed scheme. Through the establishment of mathematical model and simulation results, the proposed scheme can effectively detect and mitigate jammers so that the positioning performance of GNSS receivers will not be contaminated.**

I. INTRODUCTION

AN eye-catching statement in BBC News Report states that "Technology that depends on satellite-navigation signals is increasingly threatened by attack from widely available equipment, experts say [1]." How to effectively counteract these attacks and defend global navigation satellite system (GNSS) from the effect of interference is the current concern of scholars and experts. The internal code design of civilian GNSS receiver is coarse/acquire-code (C/A-code) instead of precise-code (P-code) of military type. Thus, the global positioning system (GPS) receiver is vulnerable to the spoof attack of hackers, extortionists, etc. To scope with intentional and unintentional interferences, the current techniques used to mitigate interferences consist of three types: antenna array techniques, pre-correlation, and post-correlation techniques. Though these techniques can efficiently mitigate many types of interference such as narrowband, wideband and pulse, deeper thoughts and strategies are required to deal with counterfeited GPS signal [2, 3]. It is declared in Volpe Report that ***"A spoofer also can defeat nearly all anti-jamming equipment*** [4]***."*** Spoofing is more hazardous than jamming because jamming causes the service to deteriorate in performance while spoofing takes command of the receiver and then injects misleading information. Such an impact can not be ignored. For instance, the local area augmentation system (LAAS) developed in America often utilizes pseudolite satellites set up by the ground stations to obtain high position dilution of precision (PDOP) during navigation. However, the effect on aviation is hazardous once the pseudolite (pseudo satellite) are abused to broadcast misleading navigation information.

In 1995, several concepts for countering spoofing had been proposed by Edwin L. key, such as amplitude discrimination, time-of-arrival discrimination, polarization discrimination, and cryptographic authentication, etc. [5]. The author considers that the adoption of multiple element antenna may be the best anti-spoofing technique to measure the angle of arrival (AOA) of all received signals. The spoofer are easily rejected because it is very difficult for a spoofer to match the AOA of satellite signals. In recent year, this technique has been implemented and often applied to interference mitigation of GNSS military navigation. The mitigation methods regarding near-field pseudolite and co-channel interference have been subsequently proposed. These methods can effectively mitigate pseudolite signals with stronger power to avoid its effect on navigation positioning. The cooperation of this method with effective interference detection and early warning mechanism, it will be rather helpful for future navigation system.

This paper utilizes adaptive antenna array technique in combination with signal acquisition and decision logic to constitute spoofing signal (SPS) detection and mitigation (or cancellation) system in order to safeguard the current GNSS receivers against spoof attack and secure GNSS-based positioning. Besides, this system also incorporates narrowband continuous wave interference (CWI) detection and mitigation technique to consolidate the reliability of interference mitigation performance for this system.

II. METHODOLOGY

This paper combines signal detection, decision logic and mitigation technique to counteract CWI and spoofing signal. A block diagram of the proposed algorithm is shown in Fig. 1, and it consists of three mechanisms, which are anti-J module, signal detector and decision logic module. The decision logic module can conduct different processing mode based on the "flag" sent by signal detector.

Without spoofing signal or CWI, the receiver remains in initial mode to conduct signal acquisition and tracking. Under the situation of no interference, the internal signal processing of receiver performs three modes. Mode 1 is termed "Hold Mode", where the receiver remains the same operation as it did. Mode 2 is called "Anti-CWI Mode", where the received signals are processed by a CWI excisor. Mode 3 is termed "Anti-SPS Mode", where the received samples of multi-channel are processed through anti-SPS module. After the operation of mode 2 and mode 3, the output of module is ultimately processed through signal correlation.

In addition, knowledge database provides the useful information to enhance the performance of anti-J module and

Manuscript received September 22, 2010. This work was supported in part by the National Science Council under Grant NSC 99-2221-E-020 -036.

C. L. Chang is with the Department of Biomechatronics Engineering, National Pingtung University of Science and Technology, Neipu, Pingtung County 91201 Taiwan (e-mail: chungliang@mail.npust.edu.tw).

978-1-4577-0079-8/11/$26.00 ©2011 AACC

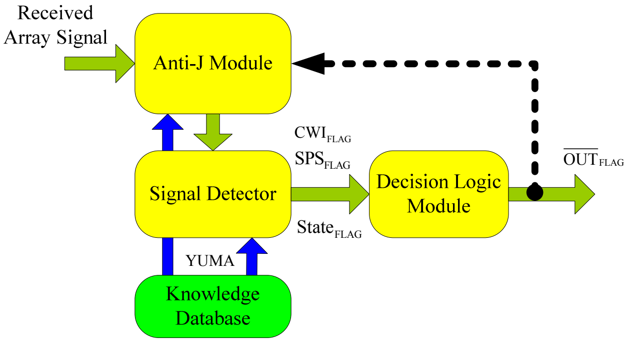

Fig. 1 Anti-jamming System

such information consists of YUMA data and coarse signal parameters [6]. The following first illustrates the mathematical description of received signal to lay foundation for subsequent discussion.

A. Spatial Signal Model

The array signal received by GNSS receiver can be modeled as

$$\mathbf{r}[k]=\mathbf{a}_{\mathrm{d}}s_{\mathrm{d}}[k]+\sum_{l=1}^{L}\tilde{\mathbf{a}}_l\tilde{s}_l[k]+\sum_{i=1}^{J}\mathbf{b}_i u_i[k]+\boldsymbol{\eta}[k] \qquad (1)$$

The input array signal with N antenna has been already down-converted and digitized by the receiver front-end in (1). $\mathbf{r}[k]=[r_1 \quad r_2 \quad \cdots \quad r_n \quad \cdots \quad r_N]^{\mathrm{H}}$ is $N\times 1$ vector of input signal. The notation $\mathbf{r}[k]=\mathbf{r}(kT_s)$ is used to denote a digital sequence sampled at the frequency $f_s=1/T_s$. T_s is period of sampling. k is the discrete time index. $\mathbf{a}_{\mathrm{d}}$, $\tilde{\mathbf{a}}_l$, and $\mathbf{b}_j$ are $N\times 1$ steering vector of the desired satellite signal s_{d}, $l-$th co-channel satellite signal $\tilde{s}_l$, and $i-$th continue wave interferences u_i, respectively. Steering vector represents the relative phases at each antenna in correspondence to azimuth θ and elevation φ, where the steering vector varies based on different array configuration [7]. L and J stand for the number of visual satellite and CWI, where SPS is included within L satellites. $\boldsymbol{\eta}[k]$ is noise vector with zero mean and Gaussian distribution. It is assumed that GPS signal, interferences, and noise are uncorrelated to each other. The in-band interference u_i in (1) is defined as

$$u_i[k]=\sqrt{P_i}\exp\{-j2\pi f_i kT_s+\theta_i\} \qquad (2)$$

where f_i and θ_i are digitalized carrier frequency and phase, respectively. The signal structure of SPS and GPS discussed here is the same and is classified in co-channel navigation signals. The signal model described above will be conducted in its corresponding processing algorithm on the basis of different decision mode. The following will demonstrate the signal processing method of each module: signal detector, anti-J module, and decision logic module.

B. Signal Detector

1) GPS Signal Detection

This signal detection process is a two dimensional signal search, which aims to acquire coarse code phase and Doppler frequency. It generates initial signal parameter for subsequent signal tracking. The typical acquisition methods are sequence search method and block fast Fourier transform (FFT) search method [8]. Each has its pros and cons. For common signal processing method, the process terminates once the coarse signal parameter is acquired. However, the search of whole area is required in consideration of whether spoofing signal exists.

Here, block FFT search method is utilized to conduct signal acquisition. This method performs circular correlation through Fourier transforms and the correlation result is given by

$$z(w,v)=F^{-1}\left\{F(y(w))F^{*}(g(kT_s-v))\right\} \qquad (3)$$

where $y[w]=r_n[k]\exp\{-j(f_{IF}+w)kT_s\}$ represents the demodulated signal multiplied through input signal and locally generated intermediate frequency. F, F^{-1}, and "$*$" depict the FFT, inverse FFT, and complex conjugated operator. $g(\cdot)$ is local replica code with estimated delay τ. The w and v depicts the code and Doppler trial point in two-dimensional grid. When w and v equal the actual code phase and Doppler frequency, (3) yield the maximum correlation. Thus, without the impact of CWI, (3) is the sum of in-phase I and quadrature Q component. After the I and Q is squared and then summed and operated through non-coherent integration, it will yield correlator output and lead to the decision variable.

$$\bar{z}=\sum_{m=1}^{M}\{\mathrm{I}_m^2+\mathrm{Q}_m^2\} \qquad (4)$$

where M is the non-coherent integration. The correlator output ($\bar{z}$) is compared with a threshold which corresponds to the probability of detection $\mathrm{P_D}$ and probability of false alarm $\mathrm{P_{FA}}$. $\mathrm{H_d}$ and $\mathrm{H_0}$ represent whether the desired signal is present or absent and is correctly aligned or not with the local replica; In order to determine the receiver operating characteristic (ROC), the following $\mathrm{P_{FA}}$ and $\mathrm{P_D}$ have to be evaluated:

$$\mathrm{P_{FA}}(\gamma)=\rho(\bar{z}>\gamma|\mathrm{H_0}) \qquad (5)$$

$$\mathrm{P_{D}}(\gamma)=\rho(\bar{z}>\gamma|\mathrm{H_d}) \qquad (6)$$

where γ is the detection threshold and $\rho(\cdot)$ is probability function. Given $\mathrm{P_{FA}}$, the detection threshold γ can be easily determined by inverting the function $\mathrm{P_{FA}}(\gamma)$. In (4), assume desired signal is not present under hypothesis $\mathrm{H_0}$ and co-channel interference component is not taken into account, (4) is given by

$$\bar{z}_{\mathrm{n}}=\sum_{m=1}^{M}\{[\bar{\eta}_{\mathrm{I}}^2]_m+[\bar{\eta}_{\mathrm{Q}}^2]_m\} \qquad (7)$$

When the signal is not present or not correctly aligned it is possible to assume that both $\bar{\eta}_I$ and $\bar{\eta}_Q$ are zero mean. The normalized detection criterion, $\bar{z}_{\mathrm{n}}/\sigma^2$, has a central chi-square distribution with $2M$ degrees of freedom. $\sigma^2=N_0/2KT_s$ is power of centred Gaussian noise, N_0 is the noise power spectral density (PSD) in unit of Watt/Hz. It is possible to derive the false alarm probability in (5) rewritten as follows:

$$\mathrm{P_{FA}}(\gamma)=(1+(\gamma/2\sigma^2))\exp\{-\gamma/2\sigma^2\} \qquad (8)$$

Assume that the desired signal is not present and a minor cross-correlation peak is taken into consideration. Thus, the correlation output in (4) can be rewritten by

$$\overline{z}_c = \sum_{m=1}^{M} \left\{ \begin{array}{l} \{\sum_{l=1}^{L} \sqrt{P_l} b_0[k] T_c R_{l0}(\tau) \mathrm{sinc}(\Delta f_{l0} T_c) \cos\phi_l + \overline{\eta}_I[k]\}_m^2 + \\ \{\sum_{l=1}^{L} \sqrt{P_l} b_0[k] T_c R_{l0}(\tau) \mathrm{sinc}(\Delta f_{l0} T_c) \sin\phi_l + \overline{\eta}_Q[k]\}_m^2 \end{array} \right\} \tag{9}$$

where R_{l0} represents the Fourier series coefficients of the cross correlation function between 0 and $l-$th satellite signal, respectively. $T_c = KT_s$ is the integration time interval. K is the number of samples used for signal parameter estimation. The normalized detection criterion $\overline{z}_c / \sigma^2$ in (9), respectively, conforms to a non-central chi-square distribution with $2M$ degrees of freedom, and the expected value of non-centrality parameter

$$\Lambda_L = (\frac{2MT_c}{LN_0}) \sum_{l=1}^{L} P_l R_{l0}^2(\tau)(\mathrm{sinc}(\Delta f_{l0} T_c))^2 \tag{10}$$

where $\{\sum_{l=1}^{L} P_l R_{l0}^2(\tau)\} / LN_0$ is the cross-correlation term that can impact the detection performance because the false alarm probability is determined from the precise cross-correlation term. Similarly, the expected value of non-centrality parameter Λ can be obtained and shown in (11) if the desired signal is present (under hypothesis $\mathrm{H_d}$).

$$\begin{aligned} \Lambda &= \Lambda_0 + \Lambda_L \\ &= \underbrace{(\frac{2MP_0T_c}{N_0}) R_{00}^2(\tau)(\mathrm{sinc}(\Delta f_{00} T_c))^2}_{\Lambda_0} \\ &+ (\frac{2MT_c}{LN_0}) \sum_{l=1}^{L} P_l R_{l0}^2(\tau)(\mathrm{sinc}(\Delta f_{l0} T_c))^2 \end{aligned} \tag{11}$$

where Λ_0 is the expected value of non-centrality parameter without the impact of co-channel interference. The probability of detection is determined by the detection threshold and the non-central chi-square distribution. It is associated with the carrier noise density ratio through the non-centrality parameter. Thus, from these considerations, it is possible to evaluate the detection probability with non-coherent integration in (6) shown as follows [9]:

$$\mathrm{P_D}(\gamma) = Q(\sqrt{\frac{\Lambda_0}{\sigma^2}}, \sqrt{\frac{\gamma}{\sigma^2}}) \cong Q(\sqrt{\frac{2MP_0KT_s}{N_0}}, \sqrt{\frac{4\gamma KT_s}{N_0}}) \tag{12}$$

where $Q(\cdot,\cdot)$ is the Generalized Marcum Q function of order two [9, 10], defined as

$$Q(\mathrm{a},\mathrm{b}) = \frac{1}{\mathrm{a}} \int_{\mathrm{b}}^{+\infty} x^2 \exp\{-\frac{x^2+\mathrm{a}^2}{2}\} B_1(\mathrm{a}x) dx \tag{13}$$

where $B_1(\cdot)$ is the modified Bessel function of first kind and order two [11]. In (10), it is assumed that the Doppler frequency and the delay of the local replica match those of the received signal, and the loss $R_{00}^2(\tau)(\mathrm{sinc}(\Delta f_{00} T_c))^2$ is negligible. In the following, the contribution of the CWI $u_i[k]$ in the correlator output is also analyzed. The CWI is first multiplied by the reference carrier, and then is spread in the first correlation stage, where it is multiplied by the receiver generated code. The resulting signal is

$$\begin{aligned} &\Phi[k] \\ &= u_i[k] g(kT_s - \tau) \exp\{j2\pi(\tilde{f}_{IF} + \tilde{f}_d) kT_s\} \\ &= \sqrt{P_i} g(kT_s - \tau) \exp\{-j2\pi f_i kT_s + \theta_i\} \exp\{j2\pi(\tilde{f}_{IF} + \tilde{f}_d) kT_s\} \\ &= \sum_{\beta=-\infty}^{\infty} P_\alpha C_\beta \exp\{j2\pi(\alpha + \beta + \Delta f_i) kT_s\} \exp\{-j2\pi\beta\tau kT_s\} \end{aligned} \tag{14}$$

where $g(\cdot)$ is spread code which is also written as

$$g(kT_s) = \sum_{\beta=-\infty}^{\infty} C_\beta \exp\{j2\pi\beta kT_s\} \tag{15}$$

C_β is the Fourier series coefficients of the periodic g function. "$\sim$" is estimated value. In (14), assume that the interference frequency f_i is α KHz away from the sum of IF, Doppler frequency, and a residual term $\Delta f_i = f_i - \tilde{f}_{IF} - \tilde{f}_d$. After the integration, the equation in (14) becomes as follows:

$$\begin{aligned} \overline{\Phi} &= \sum_{k=1}^{K} \Phi[k] \\ &= \sum_{\beta=-\infty}^{\infty} T_c P_\alpha C_\beta \mathrm{sinc}((\alpha + \beta + \Delta f_i) T_c) \exp\{-j2\pi\beta\tau kT_s\} \end{aligned} \tag{16}$$

By definition, the residual term Δf_i is lower than $1/2T_s$; then for $\alpha \neq -\beta$, $\mathrm{sinc}((\alpha + \beta + \Delta f_i)T_c) \cong 0$. Otherwise, $\mathrm{sinc}((\alpha + \beta + \Delta f_i)T_c) \equiv \mathrm{sinc}(\Delta f_i T_c)$. Therefore, (16) is rewritten as

$$\overline{\Phi} = KT_s P_\alpha C_\alpha^* \mathrm{sinc}(\Delta f_i T_c) \exp\{-j2\pi\alpha\tau kT_s\} \tag{17}$$

"*" is conjugate operator. If the received signal includes the co-channel interference and CWI, the effective carrier-to-noise density ratio (C/N_0) calculated by (9) and (17) may be expressed as

$$C/N_0 = \frac{(2MP_0T_c)R_{00}^2(\tau)(\mathrm{sinc}(\Delta f_{00}T_c))^2}{\frac{N_0}{L}\sum_{l=1}^{L}(2MP_lT_c)R_{l0}^2(\tau)(\mathrm{sinc}(\Delta f_{l0}T_c))^2 + \frac{1}{J}\sum_{i=1}^{J}[KT_sP_\alpha C_\alpha^*\mathrm{sinc}(\Delta f_iT_c)]_i^2} \tag{18}$$

The above equation can evaluate the performance of interference mitigation.

2) CWI Detection

According to the lower power of GNSS signal which is below the noise floor, it is greatly helpful to detect CWI. In general, the power of CWI is higher than the noise. Thus, if the input signal is converted to frequency domain, it can monitor whether CWI exists. To avoid extra FFT computation load, we can meanwhile monitor whether CWI exists during signal acquisition. The CWI alarm flag ($\mathrm{CWI_{FLAG}}$) is set to one. Otherwise, it is set to zero. The rule of detection is shown as follows:

$$\mathrm{CWI_{FLAG}} = \Gamma\{\frac{\max\{10\log_{10}|F(y(w))|\}}{E\{10\log_{10}|F(y(w))|\}} > \mathrm{D}\} \tag{19}$$

where $E\{\}$ and $\max\{\}$ are expectation operator and peak value, respectively. $\Gamma\{\}$ denotes the indicator variable such that $\Gamma\{\mathrm{TRUE}\} = 1$ and $\Gamma\{\mathrm{FALSE}\} = 0$. D is the interference detection margin in dB.

3) *Spoofing Signal Detection*

This section describes how to differentiate the existence of spoofing signal. The typical spoofer can adjust time offset and navigation data bit. Moreever, the user position and satellite information in the sky are known a priori for a spoofer. Assume the power of spoofer is not strong enough to invalidate the positioning of receiver, it can be informed of the available satellite in the sky through YUMA data. If the PRN number of counterfeited satellite matches that of the available satellite at that time, signal correlation is utilized to observe the search result. It is shown that two correlation peaks appear on the search dimension, where the higher correlation peak represents spoofing signal whereas the lower one stands for authentic signal. Fig. 2 demonstrates two correlation peaks. However, it is not necessarily true due to the peak caused by multipath. It is for certain that the peak caused by multipath corresponding to Doppler frequency aligns with that of line of sight (LOS), but different in code delay. Such a difference renders it easier to differentiate whether the correlation peak belongs to multipath. Otherwise, the spoofing signal exists.

The $\mathrm{SPS}_{\mathrm{FLAG}}$ is then set as 1. Suppose the received signal contains spoofing signal ($l=1$), the expected value of the noncentrality parameter Λ in (11) can be decomposed through correlation as follows:

$$\begin{aligned}\Lambda = & (\frac{2MP_0T_c}{N_0})R_{00}^2(\tau)(\mathrm{sinc}(\Delta f_{00}T_c))^2 \\ & \underbrace{+(\frac{2MP_1T_c}{N_0})R_{10}^2(\tau)(\mathrm{sinc}(\Delta f_{10}T_c))^2}_{\Lambda_{\mathrm{spoof}}} \\ & +(\frac{2MT_c}{(L-1)N_0})\sum_{l=2}^{L}P_lR_{l0}^2(\tau)(\mathrm{sinc}(\Delta f_{l0}T_c))^2\end{aligned} \qquad (20)$$

In (20), the symbol Λ_{spoof} is a power of cross-correlation term generated by the spoofing signal. As a result, the expected value of the noncentrality parameter is shown as follows:

$$\begin{aligned}\Lambda_{\mathrm{spoof}} = & (\frac{2MP_0T_c}{N_0})R_{01}^2(\tau^{\mathrm{spoof}})(\mathrm{sinc}(\Delta f_{01}T_c))^2 \\ & +(\frac{2MP_1T_c}{N_0})R_{11}^2(\tau^{\mathrm{spoof}})(\mathrm{sinc}(\Delta f_{11}^{\mathrm{spoof}}T_c))^2 \\ & +(\frac{2MT_c}{(L-1)N_0})\sum_{l=2}^{L}P_lR_{l1}^2(\tau^{\mathrm{spoof}})(\mathrm{sinc}(\Delta f_{l1}T_c))^2\end{aligned} \qquad (21)$$

Assume that the 1-th satellite is spoofing signal in (20) and disguises as desired signal s_0. Under the same false alarm rate in (5), the detection probability of spoofing signal is as follows:

$$\mathrm{P}_{\mathrm{D}}^{\mathrm{spf}}(\gamma) = \rho(\overline{z} > \gamma \mid \mathrm{H}_{\mathrm{spf}}) \qquad (22)$$

It is worth noting that the fault can occur if the value of τ^{spoof} is between $\tau-(KT_s/1023)/2$ and $\tau+(KT_s/1023)/2$ (The Doppler uncertainties are neglected). Thus, (6) and (22) reveal that the detection of authentic signal can be a simultaneous detection of counterfeited signal. The false alarm rate of the detection of fake signal is as follows:

$$\mathrm{P}_{\mathrm{FA}}^{\mathrm{spf}}(\gamma) = \rho(\overline{z} > \gamma \mid \mathrm{H}_{\mathrm{d}}) \cap \rho(\overline{z} > \gamma \mid \mathrm{H}_{\mathrm{spf}}) \qquad (23)$$

Under hypothesis $\mathrm{H}_{\mathrm{spf}}$, the procedure depicted in section 2-2-1 can be employed to calculate the effective C/No of spoofing signal. Assume the spoofing signal has been detected and cancelled, $\mathrm{SPI}_{\mathrm{FLAG}} = 0$.

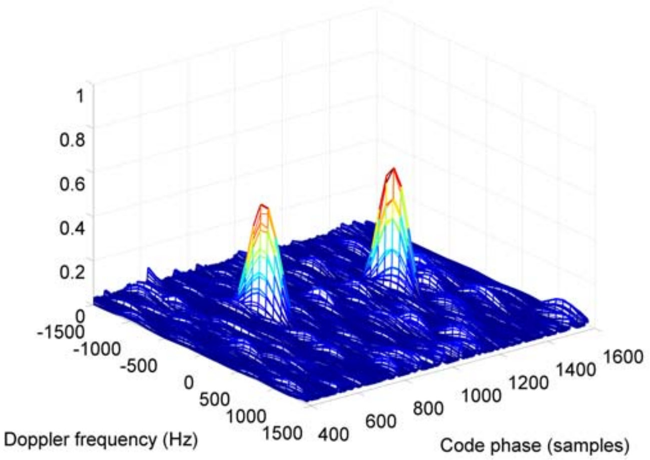

Fig. 2 Monitor of spoofing signal

4) *C/N$_0$ Estimator*

The C/N_0 compares the received signal carrier power of post-correlation with the noise density (or equivalently noise in a 1 Hz bandwidth). The mathematics evaluation is demonstrated in section 2. This estimation of C/N_0 is important because it helps verify whether the carrier and code tracking loops are in lock, control the response of the receiver to low signal in noise environment and determine the signal to noise ratio to assess or predict receiver performance. In this paper, the power ratio method [Parkinson, 1996a] is used in simulation.

C. Decision Logic

This section demonstrates how to select the signal process mode with regards to the signal detection results under varied environments. The flag $\mathrm{OUT}_{\mathrm{FLAG}}$ determines the mode selection results which as shown in Table 1. $\overline{\mathrm{OUT}}_{\mathrm{FLAG}}$ depicts to hold the previous state. It is worth that both $\mathrm{CWI}_{\mathrm{FLAG}}$ and $\mathrm{SPS}_{\mathrm{FLAG}}$ equal to one, the mode 2 (anti-CWI module) is performed. After the $\mathrm{CWI}_{\mathrm{FLAG}}$ switches to zero, mode 3 (anti-SPS module) is started. Meanwhile, mode 2 remains the same. In addition, the flag $\mathrm{State}_{\mathrm{FLAG}} = 1$ indicates the environment is jammed, otherwise, on behalf of unjammed environment. In $\mathrm{CWI}_{\mathrm{FLAG}} = 0$ and $\mathrm{SPS}_{\mathrm{FLAG}} = 0$, the output $\overline{\mathrm{OUT}}_{\mathrm{FLAG}}$ maintain the original mode until the SPS and CWI disappear and the decision logic module switch to initial mode (mode 1).

D. Anti-J Modules

This section describes the method of mitigating or eliminating the interference. The anti-J module is performed while the decision logic module switch to anti-CWI or anti-SPS mode. The procedure of anti-CWI module is firstly demonstrated in the following.

1) *Anti-CWI Module*

The anti-CWI module is performed while the decision logic module switch to mode 2. The function of this module is firstly to demodulate the carrier component and then transform to frequency domain by performing the FFT operator. Finally, the excision method is utilized to remove the partial interference component. Each frequency cell is compared to the threshold and if that exceeds the threshold, its value is held at the threshold [12].

2) *Anti-SPS Module*

The incoming signals are received through the antenna arrays. The optimal adaptive weights are computed using the block adaptive spatial beamforming algorithm. The measurement data are multiplied by the adaptive weights and summed up to give the output for acquisition/tracking applications [13].

III. Simulation Result

Consider the 2x2 uniform rectangular array (URA) where the antenna locations are distributed uniform on the XY plane with a radius of half-wavelength spacing. The proposed technique conduct the Matlab software and YUMA data to construct the real environment of GNSS signal reception. The raw data length is 600 ms with the sampling frequency is 16.368 MHz and digital IF as 4.092 MHz. The navigation data bit is removed from the record data. Fig. 3 demonstrates the signal detection probability versus a function of effective C/N_0 with the power of cross-correlation term $\{\sum_{l=1}^{L} P_l R_{l0}^2(\tau)\}/LN_0 =$ 20 dB-Hz and power of spoofing term $(P_1/N_0)R_{10}^2(\tau^{\text{spoof}}) = 38.2$ dB-Hz.

Assume that the direction of SPS and CWI are unknown to the system. Fig. 4 demonstrates the relation between different I/No and signal detection probability under fixed frequency of CWI. The false alarm rate is set as 0.005. Note that the value of signal detection probability decreases rapidly when the I/N_0 is above 25 dB and CWI is present.

After the anti-CWI processing, the probability of signal detection maintains between 0.78 and 0.82. Fig. 5 shows that the adoption of proposed technique with anti-SPS and anti-CWI process ensures the effective C/No to keep 42.8 dB (authentic PRN 13). In addition, due to the presence of CWI, the C/N_0 decreases rapidly at 70 ms. The CWI_{FLAG} changes form zero to one. The decision logic module switches to anti-CWI module in mode 2. The module utilizes frequency excision method to remove the peak of interference in frequency domain.

After this process, the CWI_{FLAG} changes to zero at 100 ms. Then, the decision logic starts the anti-SPS module in mode 3. At 110 ms, the signal detector can identify the SPS and then the beamforming algorithm is performed. Thus, the C/N_0 of real navigation signal increases up to 42.8 dB and $\text{SPS}_{\text{FLAG}} = 0$ at 210 ms. It is worth note the the anti-CWI and anti-SPS module performs the anti-jam function normally until $\text{State}_{\text{FLAG}} = 0$.

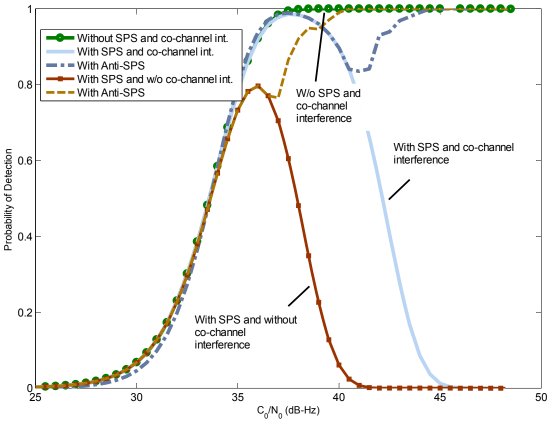

Fig. 3 Signal detection probability versus C/N_0 (PRN 6)

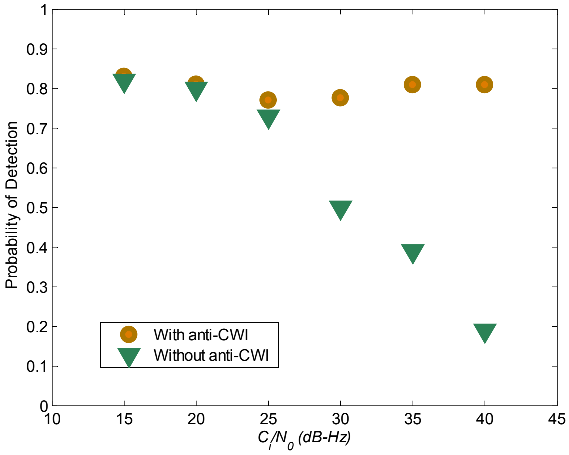

Fig. 4 Probability of detection versus I/N_0 ($T_c = 1$ ms , $K = 5$, $\text{P}_{\text{FA}} = 0.005$)

Table 1: Mode selection of decision logic module

$\text{State}_{\text{FLAG}}$	CWI_{FLAG}	SPI_{FLAG}	OUT_{FLAG}
0	0	0	1 (Initial Mode)
1	0	0	$\overline{\text{OUT}}_{\text{FLAG}}$ (Hold mode)
1	1	0	2 (Anti-CWI Mode)
1	0	1	3 (Anti-SPS Mode)
1	1	1	2 (Anti-CWI Mode)

IV. Conclusion

In this paper, a simple multiplex technique has been applied to anti-jam system to deal with the simultaneous presence of various types of interference. The simulation results illustrate that with the application of this technique, the SPS and CWI are effectively removed. Moreover, regarding detection and processing of SPS, the proposed technique can safeguard the receiver form receiving spoofing signal and avoid positioning error. This technique can be applied to future GNSS receiver design.

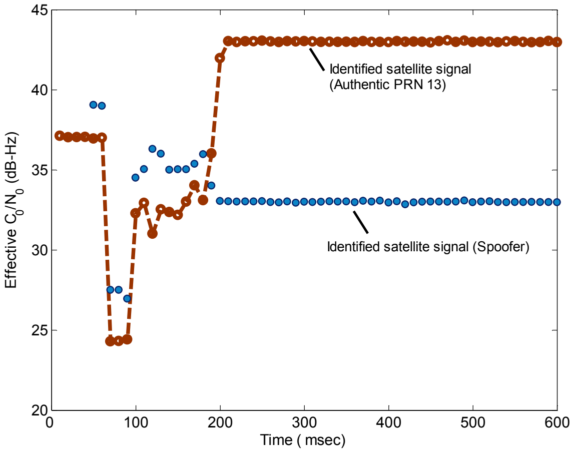

Fig. 5 Time versus C/N_0

Acknowledgment

The author would like to thank the National Science Council of Taiwan (R.O.C.) for their support of this project under grant NSC 99-2221-E-020-036.

References

[1] J. Palmer, Sat-nav systems under growing threat from 'jammers'. Science and technology reporter, *BBC News*, Feb. 2010. Available: http://news.bbc.co.uk/2/hi/science/nature/8533157.stm

[2] L. Scott, "Anti-spoofing & authenticated signal architectures for civil navigation systems," *Proc. ION GPS/GNSS*, pp. 1543–1552, Portland, Oregon, USA, Sept. 2003.

[3] G. Hein, F. Kneissi, J.-A. Avila-Rodriguez, and S. Wallner, "Authenticating GNSS: proofs against spoofs," Part 2. *Inside GNSS*, September/October, pp. 71–78, 2007.

[4] John A. Volpe National Transportation Systems Center, "Vulnerability assessment of the transportation infrastructure relying on the Global Positioning System," Tech. Rep., Aug. 2001.

[5] E. L. Key, "Techniques to counter GPS spoofing" Internal memorandum, MITRE Corporation, Feb. 1995.

[6] Navigation Center, http://www.navcen.uscg.gov/?pageName=gpsAlmanacs.

[7] C. L. Chang and J. C. Juang, "Effect of array configurations on the performance of GNSS interference suppression," *International Journal of Control, Automation and Systems*, vol.6, no. 6, pp. 884–893, Dec. 2008.

[8] D. Akopian, "Fast FFT based GPS satellite acquisition methods," *Proc. IEE Radar Sonar and Navig.*, vol. 152, no. 4, pp. 277–286, Aug. 2005.

[9] D. A. Shnidman, "The calculation of the probability of detection and the generalized Marcum Q-function," *IEEE Transactions on Information Theory*, vol. 35, no. 2, pp. 389–400, Mar. 1989.

[10] D. A. Marcum, "A statistical theory of target detection by pulsed radar," *IEEE Transactions on Information Theory*, 6, pp. 59–144, Apr. 1960.

[11] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions: with Formulas, Graphs, and Mathematical Tables*. Dover, NY, USA, 1965.

[12] C. L. Chang and J. C. Juang, "Performance analysis of narrowband interference mitigation and near-far resistance scheme for GNSS receivers," *Signal Processing*, vol. 90, no. 9, pp. 2676–2685, Mar. 2010.

[13] J. C. Juang and C. L. Chang, "Performance analysis of GPS pseudolite interference mitigation using adaptive spatial beamforming," *ION 61st Annual Meeting,* Cambridge, Massachusett, USA, June 2005, pp. 1171–1180.