آشکارسازی اختلال در بخش حلقه ردیابی گیرنده GPS

نیلوفر دباغی داریان[۱]، سمیرا توحیدی [۲]، سید محمد رضا موسوی میرکلایی [*,۳].

۱- کارشناسی، دانشکده مهندسی برق، دانشگاه علم و صنعت ایران، تهران

۲- دانشجوی دکتری، دانشکده مهندسی برق، دانشگاه علم و صنعت ایران، تهران

۳- استاد، نوسنده مسئول، دانشکده مهندسی برق، دانشگاه علم و صنعت ایران، تهران

چکیده

سامانه‌ی موقعیت یابی جهانی[†] (GPS) ابزاری مناسب برای اندازه‌گیری ساعت دقیق، ارتفاع، طول و عرض جغرافیایی هر نقطه می‌باشد. این سامانه با استفاده از ماهواره‌هایی که سطح زمین را پوشش می‌دهند، قادر به تشخیص موقعیت دقیق گیرنده است. اختلال‌های عمدی و غیرعمدی به وجود آمده، موجب کاهش دقت و امنیت گیرنده‌های سامانه GPS می‌گردد. این مقاله با استفاده از گیرنده‌ی رادیو نرم افزاری[‡] (SDR) و بررسی معیار دلتا در حلقه ردیابی، روشی کارا برای آشکارسازی حمله فریب مبتنی بر همبستگی سیگنال خروجی، ارائه می‌دهد.

.

کلمات کلیدی: کلیدی: GPS، حمله فریب، همبستگی، معیار دلتا، ردیابی، گیرنده نرم‌افزاری.

۱. مقدمه

سامانه‌ی GPS، یک سامانه‌ی مسیریابی ماهواره‌ای است که از دهه ۱۹۵۰ توسط وزارت دفاع آمریکا و ابتدا با اهداف نظامی شروع به کار نموده است. در سال‌های اخیر به علت کاربرد بسیار و نیاز روزمره، با روی کار آمدن گیرنده‌های تجاری، استفاده از GPS در زمینه‌های مختلفی فزونی یافته و استفاده از آن برای عموم آزاد شده است. این سامانه با استفاده از ماهواره‌هایی که سطح زمین را پوشش می‌دهند، قادر به تشخیص موقعیت دقیق گیرنده است. هر ماهواره دو موج حامل L1 (1575.42MHz) و L2 (1227.6MHz) (که از فرکانس مبنا f0=10.3MHz بدست می‌آید) را جهت موقعیت‌یابی ارسال می‌کند. این فرکانس‌ها توسط کدهای شبه تصادفی[§] (PRN) و پیام ناوبری مدوله می‌شوند.

فاصله‌ی بسیار زیاد ماهواره‌ها از سطح زمین، پایین بودن سطح توان سیگنال، نرخ به‌روز رسانی ضعیف و سامانه ناوبری رادیویی، امنیت سیگنال‌های GPS رسیده به سطح زمین را تهدید می‌کند. با توجه به آسیب‌پذیری سیگنال‌های GPS،

* **Corresponding Author (Email: m_mosavi@iust.ac.ir)**

† **Global Positioning System**
‡ **Software-Defined Radios**
§ **Pseudo Random Noise**

اختلال‌های عمدی و غیرعمدی وجود دارند که امنیت و دقت این سامانه را محدود می‌کند. از اختلال‌های غیرعمدی می‌توان به خطاهای ماهواره، گیرنده، مشاهده، یونسفر، تروپسفر، انحراف ساعت و چندمسیری اشاره کرد [۱].

در رابطه با اختلال‌های عمدی می‌توان از بلاکینگ، جمینگ و فریب نام برد. در حمله جمینگ، سیگنال جعلی با سطح توان بالایی بر سیگنال اصلی غلبه می‌کند و گیرنده را از دریافت سیگنال اصلی باز می‌دارد. حمله بلاکینگ، مانع رسیدن سیگنال اصلی به گیرنده می‌شود.

حمله فریب می‌تواند در سه نوع ۱- ساده، ۲- متوسط و ۳- پیچیده صورت گیرد که در این حالت سیگنال‌های معتبر GPS با سیگنال‌های نامعتبر ترکیب شده و با هدف گمراهی گیرنده در ردیابی، وارد این بخش می‌گردند. به دلیل تشابه سیگنال‌های اصلی و جعلی در حمله فریب، گیرنده ممکن است متوجه وقوع این اختلال نشود و در نتیجه راه حل ناوبری نادرستی را دنبال کند، در حالی که به درستی آن باور دارد. لذا آشکارسازی حمله‌ی فریب پیچیده‌تر است. به همین دلیل امروزه، بسیاری از روش‌های ضدفریب گسترش یافته است. در راستای حفظ امنیت این سامانه، استفاده از روش‌های نظارت و تشخیص تداخل امری حیاتی است. بدین منظور می‌توان از معیار نظارت بر کیفیت سیگنال [*] (SQM)، استفاده کرد.

در این روش، می‌توان از مقایسه‌ی خروجی همبسته‌سازها با مقدار آستانه از پیش تعیین شده برای تصمیم‌گیری در مورد حضور یا عدم حضور حمله‌ی فریب بهره برد. درواقع می‌توان قله‌های غیرطبیعی یا افزایش تعداد قله‌ها در تابع همبستگی را تشخیص داد و هرگونه اعوجاج را به وقوع حمله فریب نسبت داد. با فرض اینکه گیرنده ابتدا روی پیک‌های معتبر قفل شده، فریبنده سعی می‌کند این پیک‌ها را گمراه نماید. تشخیص وجود یا عدم وجود فریب با استفاده از آزمون‌های فرضیه‌ی آماری انجام می‌شود. برای پردازش سیگنال رشته داده خروجی RF از تابع ابهام متقابل [†] (CAF) که حاصل تخمین تابع همبستگی دو بعدی است، استفاده می‌شود. بررسی این تابع، تغییرات ناشی از وجود فریب در حلقه‌های ردیابی و خروجی حلقه قفل تاخیر [‡] (DLL) و حلقه قفل فاز [§] (PLL) را آشکار می‌کند [۲].

اگرچه درصورتی که فریبنده بتواند بدون تغییر شکل بیشینه همبستگی، سیگنال فریب را تولید کند، این روش کارآیی خود را از دست می‌دهد. برای بهبود آن باید از چندین راه حل برپایه‌ی همین روش بهره گرفت که از جمله می‌توان به دفاع سیگنال باقی‌مانده [**] (VSD)، بردار پایه [††] (VB) و روش ترکیبی اشاره کرد.

در روش VSD، گیرنده‌ها همبستگی بیشتری برای افزایش دقت پیش بینی‌ها ایجاد می‌کنند. برای این کار چند معیار تعریف می‌شود. ایده اصلی در روش ردیابی VB، ترکیب راه حل ناوبری و سیگنال ردیابی است. این یک روش تحلیلی برای بررسی تعامل بین قله‌های همبستگی معتبر و تقلبی در طول حملات است. اگر این توزیع به طور قابل ملاحظه‌ای از شکل استاندارد منحرف باشد، حمله جعلی تشخیص داده می‌شود. روش ترکیبی به بررسی فریب‌دهنده‌ای که بتواند هم زمان هر دو مشخصه‌ی توان و توزیع همبستگی سیگنال فریب را منطبق با سیگنال اصلی نگه دارد، می‌پردازد [۳].

این مقاله با استفاده از معیار دلتا و مقایسه‌ی توابع همبسته‌ساز خروجی در مرحله حلقه ردیابی گیرنده، وقوع حمله‌ی احتمالی فریب را آشکار می‌کند.

در بخش دوم، پس از معرفی حمله‌ی فریب به روش‌های آشکارسازی آن می‌پردازیم. در بخش سوم، کاربرد و نحوه‌ی استفاده از گیرنده نرم‌افزاری شرح داده می‌شود و ضمن تعریف معماری آن، چگونگی آشکارسازی حمله فریب در حلقه ردیابی شرح داده می‌شود. در بخش چهارم به شبیه‌سازی و ارزیابی روش استفاده شده، پرداخته می‌شود. در نهایت، نتیجه‌گیری در قسمت پنجم ارائه می‌شود.

---

[*] **Signal Quality Monitoring**
[†] **Cross Ambiguity Function**
[‡] **Delay Lock Loop**
[§] **Phase Lock Loop**
[**] **Vestigial Signal Defense**
[††] **Vector Base Tracking**

۲. معرفی حمله‌ی فریب و آشکارساز ی آن

فریب به عنوان خطرناک‌ترین نوع حمله در سامانه GPS شناخته شده است و هنگامی رخ می‌دهد که سیگنال تداخلی باعث محاسبه‌ی نادرست مکان گیرنده شود. به بیانی دیگر فریبنده، گیرنده GPS را به سمت راه‌حل ناوبری غلط پیش می‌برد. در این حالت سیگنال تداخلی، از حامل و مدلاسیون مشابه سیگنال اصلی برخوردار است، اما سطح توان آن به گونه‌ای است که حلقه‌ی ردیابی گیرنده را تحت اختیار خود قرار می‌دهد و موجب مکان‌یابی غلط می‌شود. گیرنده GPS در معرض حمله، مجموع سیگنال‌های اصلی و جعلی را دریافت می‌کند. به گونه‌ای که سیگنال جعلی با غلبه بر سیگنال اصلی به صورت نامحسوس کنترل گیرنده را بر عهده می‌گیرد. حمله‌ی فریب و مقابله با آن می‌تواند در هریک از سطوح گیرنده از جمله بخش بیت داده، اکتساب، ردیابی، استخراج شبه فاصله و معادلات ناوبری صورت پذیرد [۴]. در این مقاله، هدف آشکارسازی حمله‌ی فریب در مرحله ردیابی می‌باشد.

برای عملکرد بهتر روش‌های ضدفریب، لازم است ابتدا شناخت جامعی از روش‌ها و انواع فریب‌دهنده‌ها داشته باشیم. به منظور تسهیل در تجزیه و تحلیل، می‌توان حملات فریب را به سه دسته ساده، متوسط و پیچیده تقسیم بندی کنیم. در فریب‌دهنده ساده، از تقویت‌کننده توان، آنتن و شبیه‌ساز برای تولید سیگنال جعلی استفاده می‌شود. فریب‌دهنده متوسط، یک گیرنده GPS را (به جای شبیه‌ساز) در فریبنده تعبیه می‌کند تا با دریافت سیگنال و دست کاری آن سیگنال جعلی را تولید نماید. امروزه با استفاده از فناوری SDR نرم‌افزار گیرنده - فریبنده بسیار پرکاربردتر و عملی‌تر می‌باشد. حمله فریب پیچیده، با کمک چند گیرنده - فریب‌دهنده به صورت هماهنگ رخ می‌دهد.

میزان تخریب سیگنال معتبر GPS، فرصتی برای تشخیص محسوب می‌شود. لذا با بررسی مشخصه‌های مختلف سیگنال GPS رسیده به گیرنده‌ی هدف، می‌توان به وجود سیگنال فریب پی‌برد. نظارت بر تابع همبستگی سیگنال با استفاده از معیارهایی که به بررسی ویژگی‌های خروجی همبسته‌سازها می‌پردازند، انجام می‌شود؛ تا وقوع هرگونه ناهنجاری، حمل بر رخ دادن فریب اتلاق شود. در ادامه به بررسی چند معیار شناخته شده، جهت شناسایی حمله فریب می‌پردازیم [۵].

✓ معیار دلتا

$$\Delta_\tau(t) = \frac{I_{E,\tau}(t) - I_{l,\tau}(t)}{2I_p(t)} \qquad (۱)$$

که در آن، $I_{L,\tau}(t)$ و $I_{E,\tau}(t)$ به اندازه τ ثانیه از $I_p(t)$ عقب‌تر و جلوتر هستند.

به دلیل تقارن، در شرایط عدم وجود فریب، داریم:

$$E\left[\Delta_\tau(t)\right] = 0 \qquad (۲)$$

که در آن، $I_{L,\tau}(t)$ و $I_{E,\tau}(t)$ به اندازه τ ثانیه از $I_p(t)$ عقب‌تر و جلوتر هستند. این معیار، معیاری است که به عنوان تشخیص فریب در سامانه شناخته می‌شود. با این وجود، برخی از انواع حملات هم زمان می‌توانند سیگنال‌های نامعتبر را بدون اعوجاج آشکار در $I(t,\tau)$ جعل کنند و فقط سبب تغییر شکل $Q(t,\tau)$ بشوند. از آنجا که این معیار شامل مقیاس چهارگانه نیست، تشخیص این نوع حملات با آزمایش دلتا غیرممکن است.

✓ معیار ضریب

$$RT_{\tau}(t) = \frac{I_{E,\tau}(t)+I_{l,\tau}(t)}{2I_{P}(t)} \quad (۳)$$

این معیار نه تنها شامل نقص‌های آزمایش دلتا است، بلکه ممکن است حملاتی که روی $I_P(t)$ تاثیر دارد را به غلط تشخیص دهد. تغییرات متریک بستگی به تفاوت نسبی همبسته‌سازهای اولیه و دیرهنگام و سریع دارد. با این حال، در بیشتر موارد، I_E و I_L تقریباً به یک اندازه اما در جهت مخالف تغییر می‌کنند. به عنوان مثال، I_E کاهش می‌یابد، در حالی که I_L نسبت به حالت طبیعی افزایش می‌یابد. در این حالت، مجموع همبستگی اندازه‌گیری شده در شاخه همبسته‌های اولیه و دیرهنگام که باعث ایجاد معیار نسبت شده‌اند تقریباً ثابت خواهد بود. در نتیجه، این معیار نمی‌تواند این نوع حملات را به درستی تشخیص دهد.

✓ معیار تفاوت اندازه

$$MD_{\tau} = \frac{|X_{E,\tau}(t)|-|X_{l,\tau}(t)|}{|X_{p}(t)|} \quad (۴)$$

که در آن، $X_{L,\tau}(t)$ و $X_{E,\tau}(t)$ به‌ترتیب به اندازه τ ثانیه از $X_P(t)$ عقب‌تر و جلوتر هستند و با بهره گیری از اندازه‌ی مقدار همبستگی در نقاط مختلف محاسبه می‌شود. البته باید توجه داشت تفکیک اختلال‌های فریب و چندمسیری از چالش‌های پیش روی این روش است. این معیار شبیه به آزمایش دلتا است.

تفاوت این است که از مقدار مطلق همبستگی‌ها استفاده می‌شود. معمولاً در حملات جعل، شاخه‌های هم فاز افزایش می‌یابد، درحالی که جزء متعامد کاهش می‌یابد. با توجه به این حقیقت که این معیار، اندازه تابع همبستگی را در نظر می‌گیرد، تغییرات هم فاز و متعامد ممکن است تا حدی یکدیگر را جبران کنند. بنابراین، انتظار می‌رود که این معیار حساسیت کمی نسبت به سیگنال‌های جعل شده، داشته باشد.

✓ معیار فاز ابتدایی – نهایی

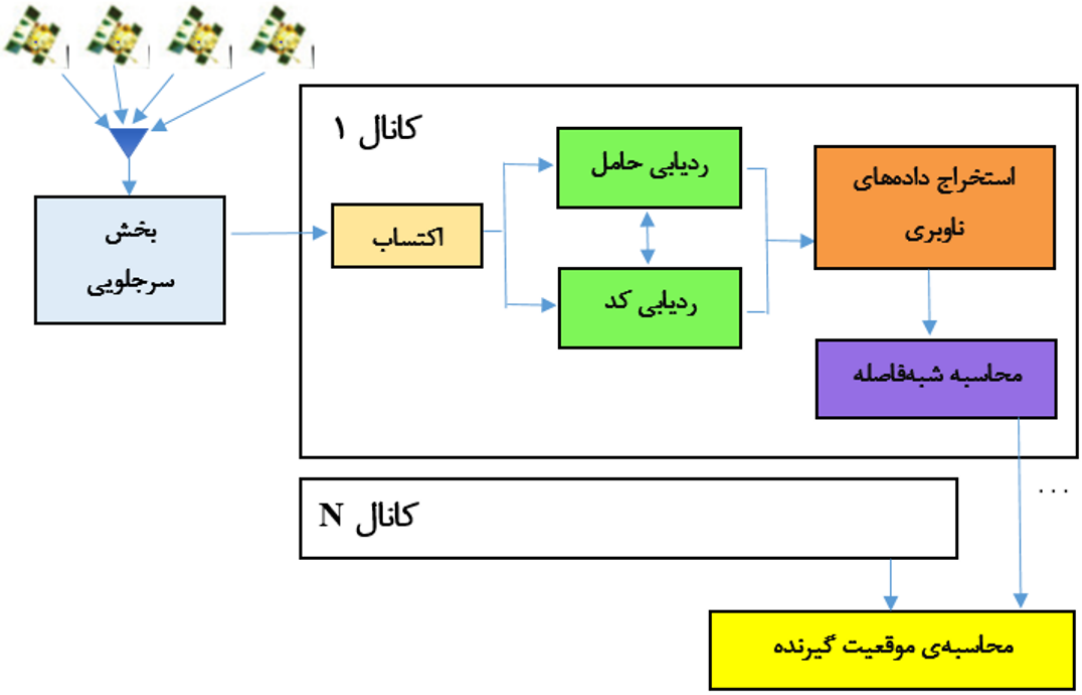
این معیار اخیرا به عنوان یک روش نظارت به صورت زیر در نظر گرفته می‌شود.

$$ELP_{\tau}(t) = tan^{-1}\left(\frac{Q_{L,\tau}(t)}{I_{L,\tau}(t)} - \frac{Q_{E,\tau}(t)}{I_{E,\tau}(t)}\right) \quad (۵)$$

که در آن، $Q_{E,\tau}(t)$ و $Q_{L,\tau}(t)$ به ترتیب به اندازه τ ثانیه جلوتر و عقب‌تر از $Q_P(t)$ هستند و $Q_P(t)$ جزء متعامد شاخه همبستگی همزمان می‌باشد. $ELP_{\tau}(t)$ اختلاف فاز بین نقاط ابتدایی و نهایی همبستگی را محاسبه می‌کند. این معیار برای آشکارسازی چندمسیری برای سیگنال‌های L1 و L2C بکار رفته است. این تنها معیاری است که جزء متعامد همبستگی را در محاسبات در نظر می‌گیرد [۶].

۳. گیرنده نرم‌افزاری

گیرنده نرم‌افزاری GPS، گیرنده‌ای است که پردازش سیگنال آن به استثنای قسمت‌های مربوط به دریافت سیگنال آنالوگ تا تبدیل به یک رشته بیت خام دیجیتال روی عناصر برنامه‌پذیر پیاده‌سازی می‌شود. ساختار این گیرنده مطابق شکل ۱ قابل نمایش است.



شکل ۱ – معماری گیرنده نرم‌افزاری.

پس از عبور از بخش سر جلویی با هدف فیلتر و تقویت سیگنال، در مرحله اکتساب به منظور تعیین ماهواره‌های قابل رویت، پارامترهای فاز کد و فرکانس حامل به صورت تقریبی محاسبه می‌گردند. هدف اصلی از ردیابی پالایش مقادیر تقریبی بخش اکتساب، اصلاح این مقادیر، پی‌گیری و تغییر شکل داده‌های ناوبری برای ماهواره خاص است، درحالی که ویژگی‌های سیگنال با زمان تغییر می‌کند. واحد ردیابی باید دو نسخه سیگنال محلی تولید کند. یکی برای حامل و دیگری برای کد، تا سیگنال یک ماهواره کاملا ردیابی شود. برای ردیابی سیگنال موج حامل اغلب از PLL یا حلقه‌های قفل فرکانس* (FLL) استفاده می‌شود. حلقه ردیابی کد در گیرنده GPS یک DLL است [۷].

اهمیت حلقه ردیابی در این است که وقوع حمله فریب، این حلقه را مختل می‌کند. واحد ردیابی میزان همبستگی را در PLL و DLL محاسبه می‌نماید. در صورت وجود تداخل، تابع همبستگی کد تحریف شده و ممکن است منجر به ایجاد خطای ناوبری شود [۸].

هدف این مقاله نیز در همین راستا است که در صورت وجود فریب، با استفاده از معیارهایی در مرحله ردیابی گیرنده نرم‌افزاری GPS، انحرافات سیگنال را شناسایی کند و وجود سیگنال جعلی را تشخیص دهد.

با فرض اینکه کد PRN تولیدی به طور کامل با کد ورودی هم فاز باشد، سیگنال I به صورت زیر تعریف می‌شود:

$$I^K = D^k(n)\cos(w_{IF}n)\cos(w_{IF}n+\varphi) = \frac{1}{2}D^k(n)\cos(\varphi) + \frac{1}{2}D^k(n)\cos(2w_{IF}n+\varphi) \quad (۶)$$

که در آن، φ مبین اختلاف فاز بین سیگنال ورودی و نسخه فاز حامل محلی است.

خروجی Q بدین صورت تعریف می‌گردد:

$$Q^K = D^k(n)\cos(w_{IF}n)\,sin(w_{IF}n+\varphi) = \frac{1}{2}D^k(n)\sin(\varphi) + \frac{1}{2}D^k(n)\sin(2w_{IF}n+\varphi) \quad (۷)$$

با عبور این دو سیگنال از فیلتر پایین‌گذر قسمت‌هایی که فرکانس دو برابر فرکانسی میانی دارند حذف شده و سیگنالی

* **Frequency Lock Loop**

به صورت زیر خواهیم داشت:

$$I^K = \frac{1}{2} D^k(n) \cos(\varphi) \quad (۸)$$

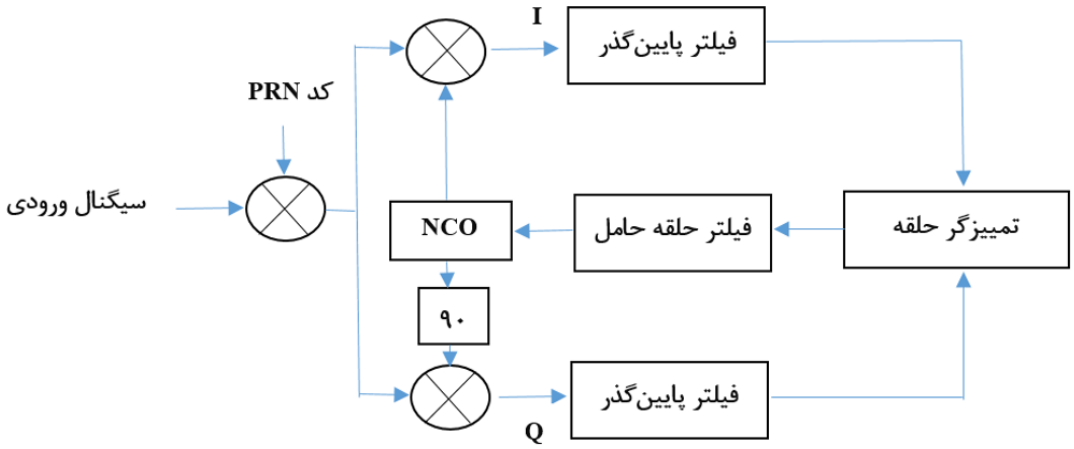
$$Q^K = \frac{1}{2} D^k(n) \sin(\varphi) \quad (۹)$$

خطای فاز نسخه حامل محلی تولیدی را می‌توان به صورت رابطه (۱۰) نوشت:

$$\frac{Q^K}{I^K} = \frac{\frac{1}{2} D^k(n) \sin(\varphi)}{\frac{1}{2} D^k(n) \cos(\varphi)} \rightarrow \varphi = \tan^{-1}\left(\frac{Q^K}{I^K}\right) \quad (۱۰)$$

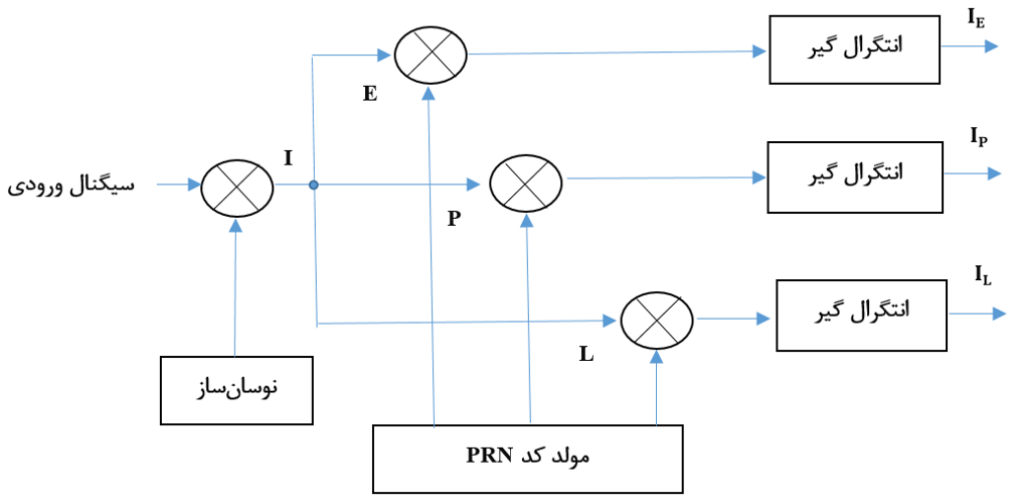
درنتیجه خطای فاز همبستگی زمانی کمینه می‌شود که میزان همبستگی بازوی Q صفر باشد و مقدار همبستگی تابع I بیشینه باشد.

ردیابی حامل به کمک حلقه کاستاس با هدف انتقال تمام انرژی روی بخش هم فاز و کمینه کردن بخش متعامد به منظور کاهش خطا، مطابق شکل ۲ انجام می‌شود [۹].



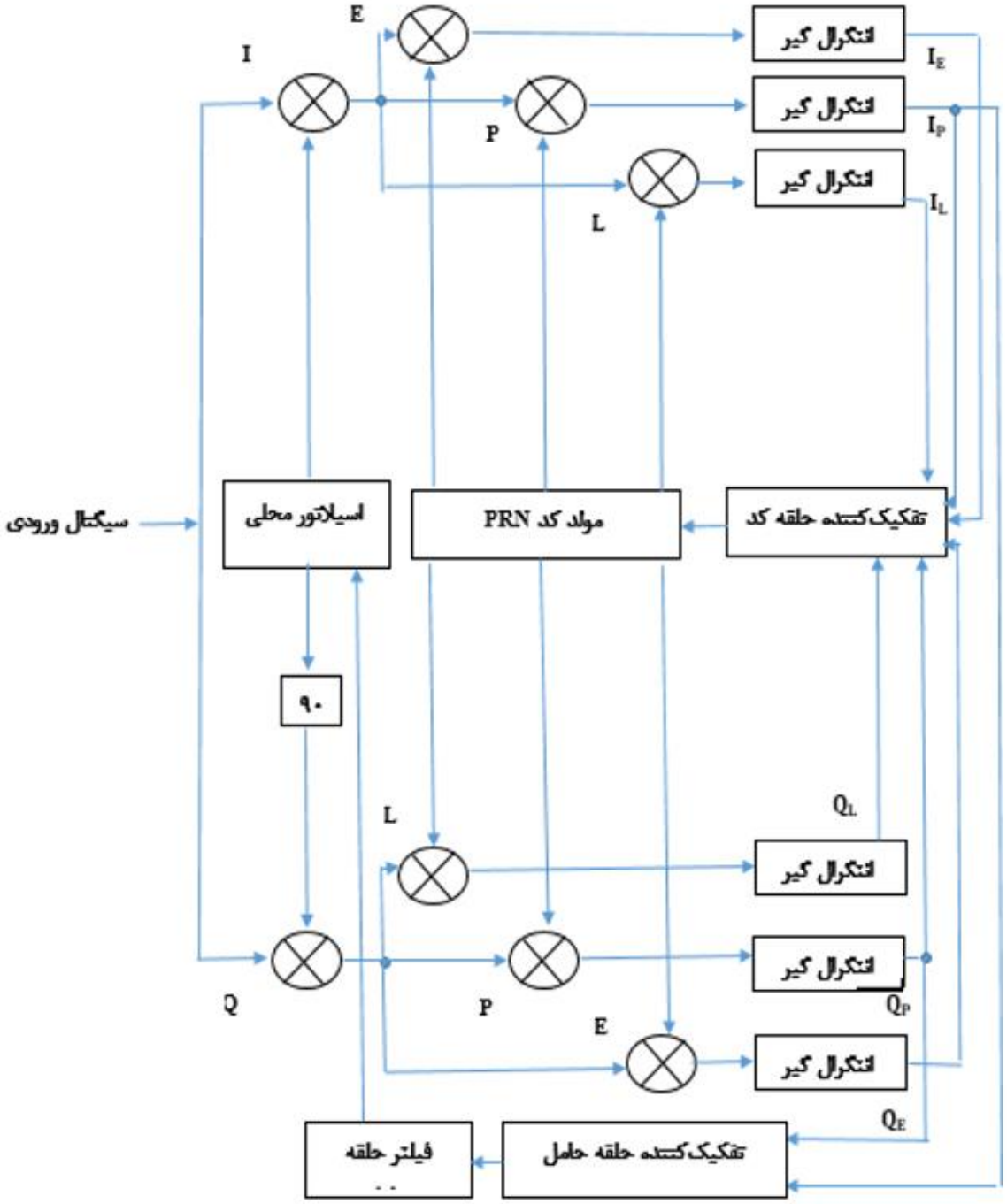
شکل ۲ – حلقه کاستاس.

ایده پشت DLL این است که میزان همبستگی سیگنال ورودی را با سه تکرار کد، متقدم، همزمان و متاخر محاسبه می‌نماید. این سه نسخه اغلب با فاصله تراشه نیم چیپ تولید می‌شوند. سپس سه خروجی در کل دوره کد C/A ادغام شده و ذخیره می‌شوند. خروجی این ادغام‌ها معیاری است که میزان همبستگی کد خاص ساخته شده با کد موجود را نشان می‌دهد. خروجی‌های هم‌فاز همبسته ساز یعنی I_E، I_P و I_L برای انتخاب بهترین جواب باهم مقایسه می‌شوند. در حالتی که کد اصلی دارای بیشترین مقدار همبستگی باشد و نسخه‌های تقدم و تاخر دارای همبستگی برابر باشند، فاز کد به صورت صحیح ردیابی شده است. شکل ۳ بلوک دیگرام حلقه ردیابی را نمایش می‌دهد [۱۰].



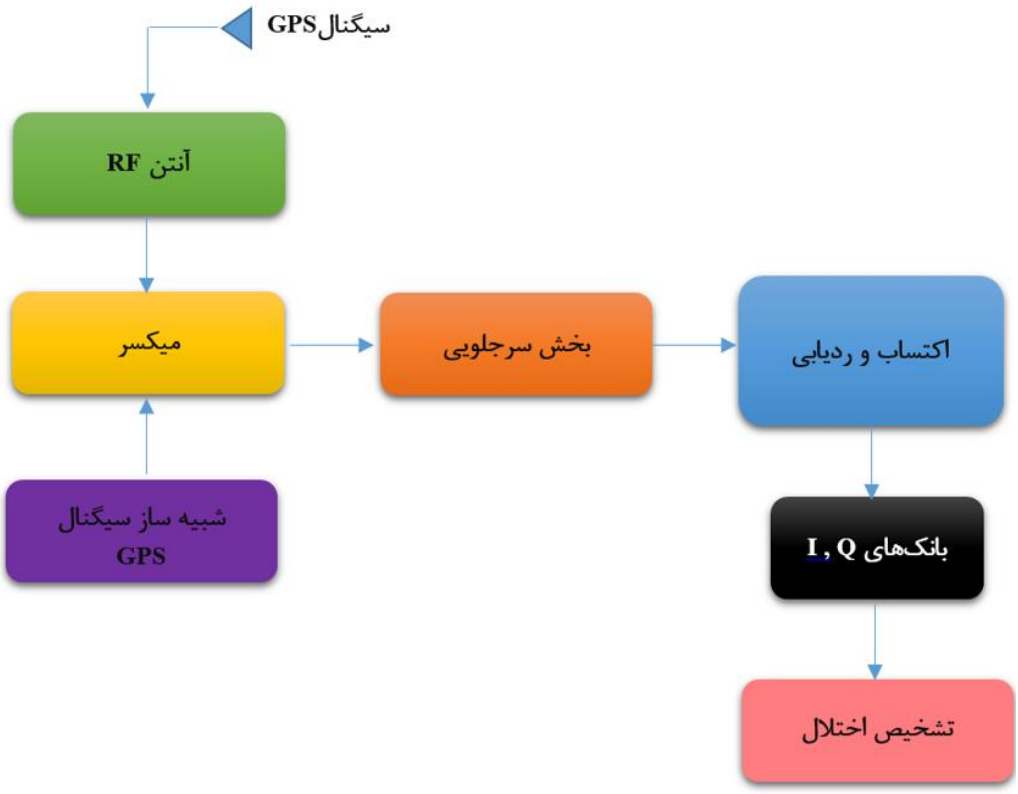
شکل ۳ – بلوک دیاگرام DLL.

شکل ۴ بلوک دیاگرام ترکیب حلقه‌های ردیابی حامل و کد را نشان می‌دهد. در حلقه ترکیبی حامل و کد، خروجی‌های تاخر و تقدم شاخه‌های متعامد و هم‌فاز برای تفکیک‌گر حلقه کد و خروجی‌های اصلی در تفکیک‌گر حلقه حامل استفاده می‌شوند [۱۱].



شکل ۴ – ترکیب DLL و PLL برای ردیابی کد و حامل.

شکل ۵ بلوک دیاگرام گیرنده نرم‌افزاری را نشان می‌دهد؛ که با استفاده از معیار دلتا که توسط خروجی همبسته‌سازها تعریف می‌شود می‌توانیم در مرحله ردیابی، حمله‌ی فریب را آشکار کنیم. بدین منظور از دو مجموعه داده اصلی و جعلی استفاده می‌شود؛ به طوری که داده جعلی با اعمال تاخیر در داده اصلی توسط شبیه‌ساز تولید می‌گردد [۱۲].

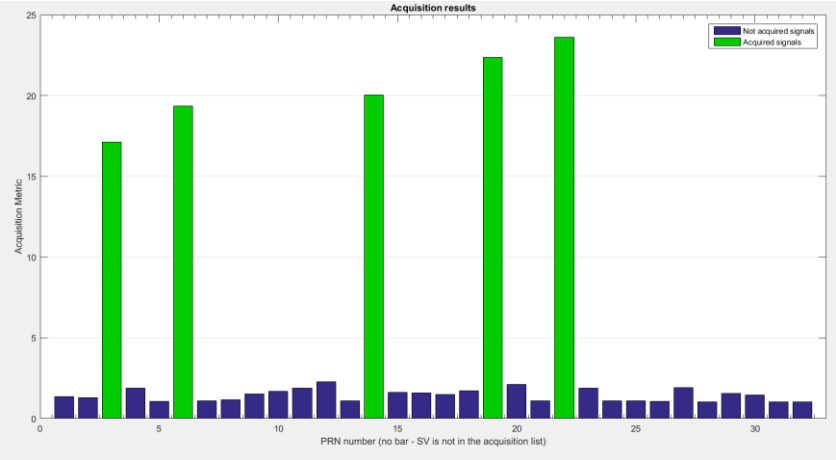


شکل ۵ – بلوک دیاگرام تشخیص فریب در حلقه ردیابی گیرنده نرم‌افزاری GPS.

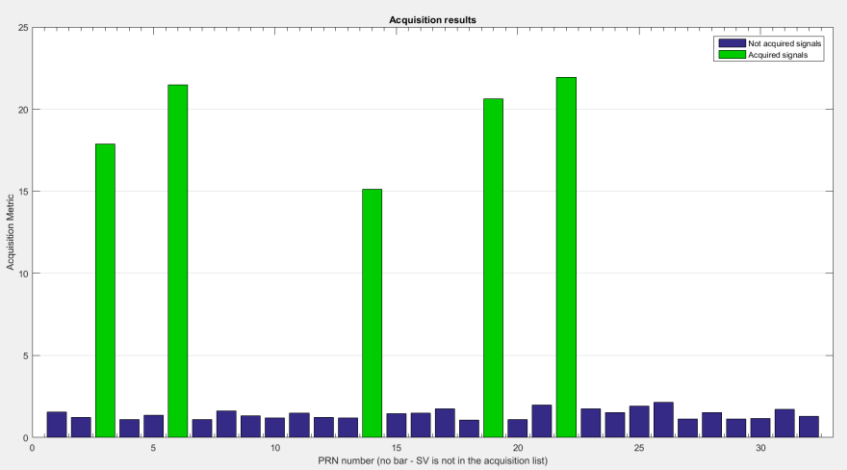
۴. شبیه‌سازی

در این قسمت به تشخیص و آشکارسازی حمله فریب در حلقه‌ی ردیابی با استفاده از معیار دلتا می‌پردازیم تا هرگونه ناهنجاری در سیگنال آشکار شود. به این منظور از نرم‌افزار منبع باز SoftGNSS که به زبان برنامه‌ریزی متلب* است، بهره می‌گیریم. ابتدا اکتساب داده‌ها با روش جست‌وجو موازی در فضای فاز کد آغاز می‌شود تا کانال‌های در دید شناسایی گردد. با توجه به شکل ۶ برای هر دو سناریو بدون فریب که حاوی داده اصلی است و سناریو فریب که حاوی سیگنال معتبر و سیگنال جعلی است، ۵ کانال PRN3، PRN6، PRN14، PRN19 و PRN22 قابل شناسایی است.

* **MATLAB**



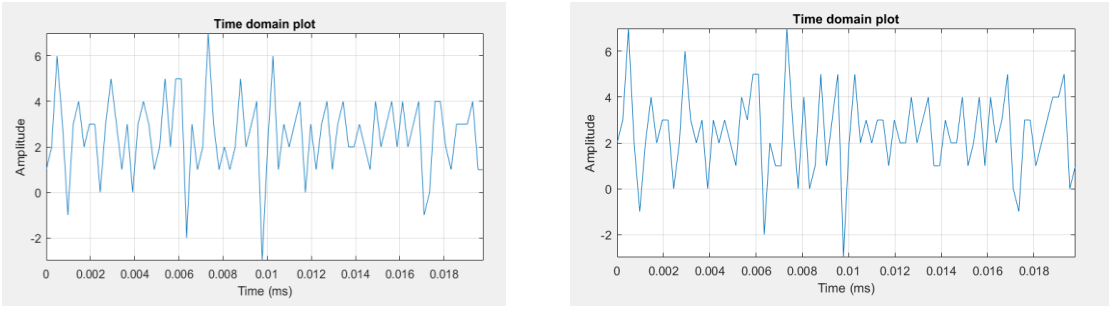
(الف)



(ب)

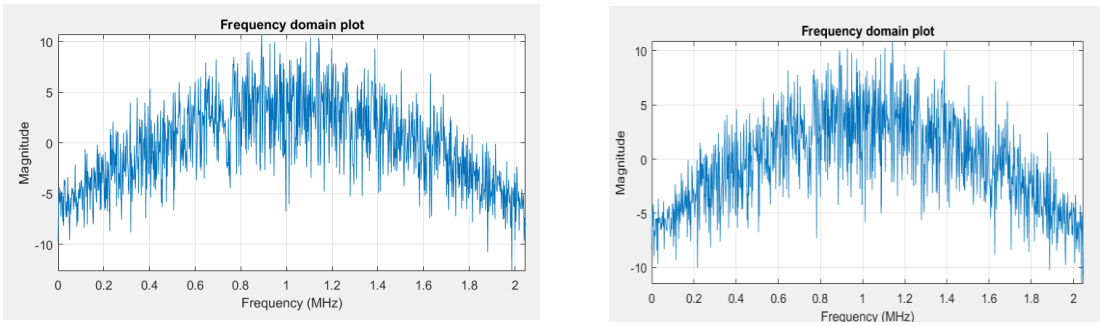
شکل ۶ – نتایج مرحله اکتساب داده‌های: (الف) معتبر و (ب) جعلی.

با بررسی نمودار حوزه زمان، فرکانس و هیستوگرام این دو داده که در شکل‌های ۷، ۸ و ۹ رسم شده است، تفاوت محسوسی که بتوان داده جعلی را از اصلی تمییز داد، قابل مشاهده نیست. لذا از معیار دلتا و بررسی ویژگی همبسته‌سازهای خروجی در حلقه ردیابی به منظور تشخیص حمله فریب استفاده می‌کنیم. با توجه به تعریف معیار دلتا، این معیار قادر به شناسایی ناهنجاری‌های موجود در بخش هم فازسیگنال است. مقایسه‌ی معیار دلتا در سناریو بدون فریب و با فریب نشان می‌دهد که نمودار مثلثی شکل مربوط به بخش هم‌فاز و متعامد در حالت بدون اختلال، به صورت تقریباً متقارن است به طوری که سطح هم فاز نیز نسبت به حالت فریب یافته سیگنال، بزرگ‌تر است. همچنین، این تقارن در حالت فریب ممکن است دچار اختلال شود و بخش هم‌فاز سیگنال، حالت مثلثی شکلش را از دست بدهد. لازم به ذکر است که این معیار قادر به شناسایی اختلالاتی است که روی بخش هم فاز سیگنال اثر می‌گذارند.



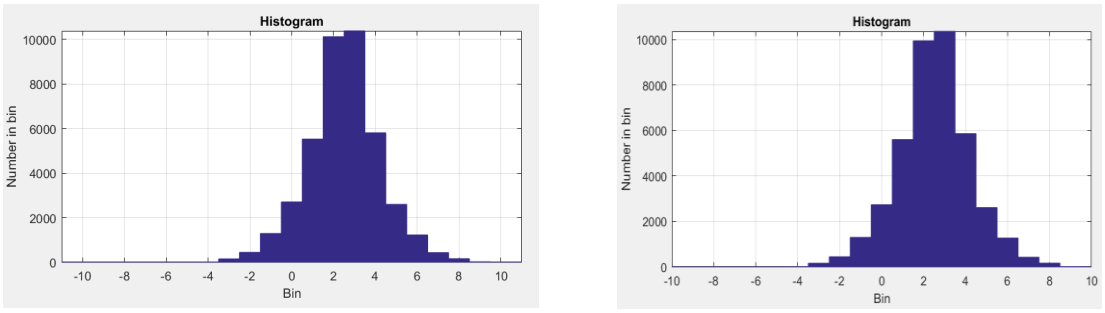
(ب) (الف)

شکل ۷ – نمایش حوزه زمان سیگنال: (الف) معتبر و (ب) جعلی.



(ب) (الف)

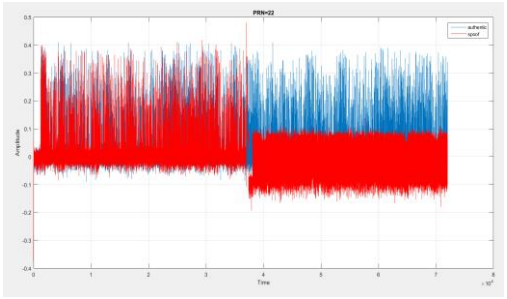
شکل ۸ – نمایش حوزه فرکانس سیگنال: (الف) معتبر و (ب) جعلی.



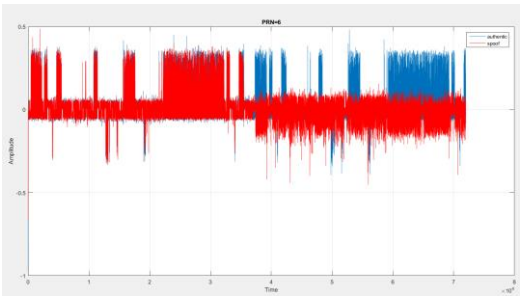
(ب) (الف)

شکل ۹ – نمایش هیستوگرام سیگنال: (الف) معتبر و (ب) جعلی.

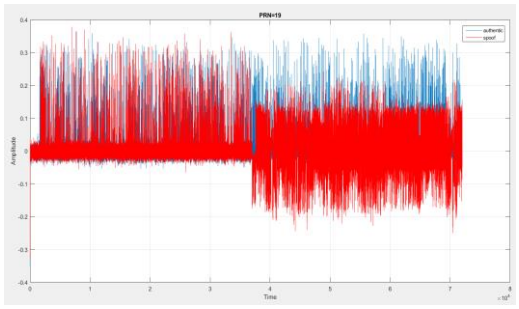
در ادامه نمودار دلتا را برای کانال‌های ردیابی شده در حالت سیگنال معتبر و جعلی در شکل‌های ۱۰، ۱۱، ۱۲، ۱۳ و ۱۴ رسم می‌کنیم. نمودار آبی رنگ معیار دلتا محاسبه شده را برای داده اصلی و نمودار قرمز رنگ معیار دلتا به ازای داده فریب می‌باشد. در سناریو فریب سیگنال جعلی در لحظه‌ی ۳۶ ثانیه اعمال شده است. همان‌طور که در شکل‌های مربوطه ملاحظه می‌شود نمودار دلتا داده‌های اصلی و داده‌های فریب تا لحظه‌ی ۳۶ ثانیه کاملاً منطبق هستند؛ در حالی که بعد از لحظه اعمال سیگنال فریب، نمودار معیار دلتا محاسبه شده در سناریو فریب کاملا متمایز از نمودار مربوط به سناریو بدون فریب می‌باشد که این تمایز، حاکی از وجود فریب در داده‌های جعلی است.



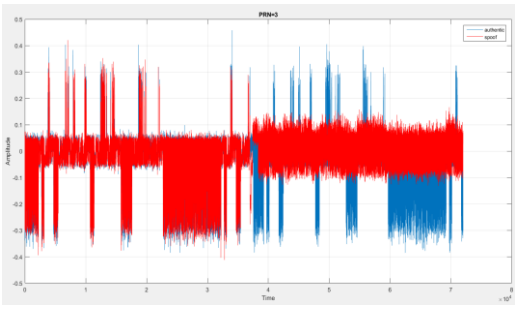
شکل ۱۰ – نمودار دلتا مرحله ردیابی PRN=22.



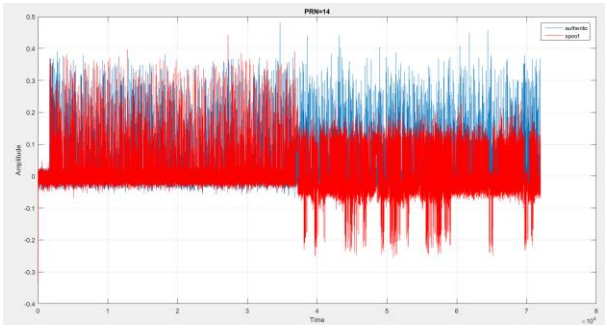
شکل ۱۱ – نمودار دلتا مرحله ردیابی PRN=6.



شکل ۱۲ – نمودار دلتا مرحله ردیابی PRN=19.

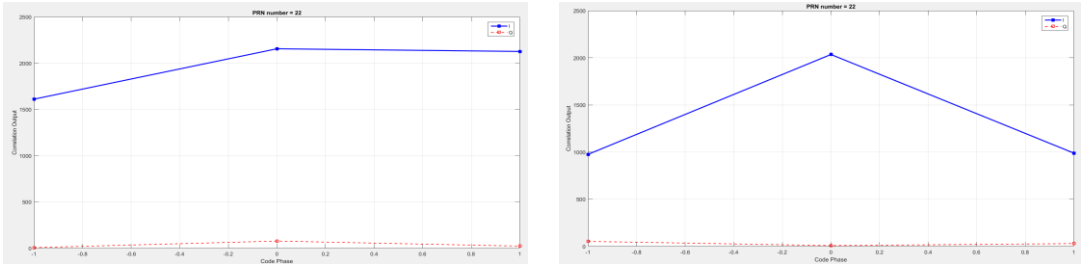


شکل ۱۳ – نمودار دلتا مرحله ردیابی PRN=3.



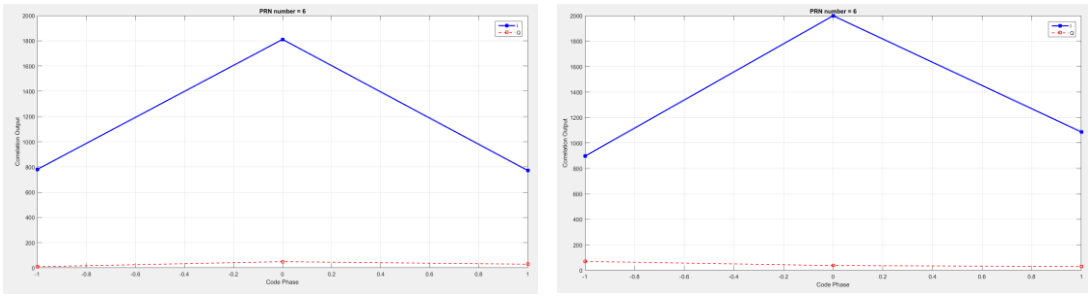
شکل ۱۴ – نمودار دلتا مرحله ردیابی PRN=14.

برای آشکارسازی بهتر حمله فریب نمودار همبسته‌سازهای خروجی داده‌های اصلی و جعلی را در شکل‌های ۱۸،۱۷،۱۶،۱۵ و ۱۹ رسم و مقایسه می‌کنیم. مطابق تعریف، بخش هم‌فاز داده‌های اصلی به صورت مثلثی و متقارن می‌باشد. در حالی که؛ این تقارن در داده‌های فریب وجود ندارد و از این طریق می‌توان داده اصلی را از داده جعل شده توسط حمله‌ی فریب شناسایی کرد.



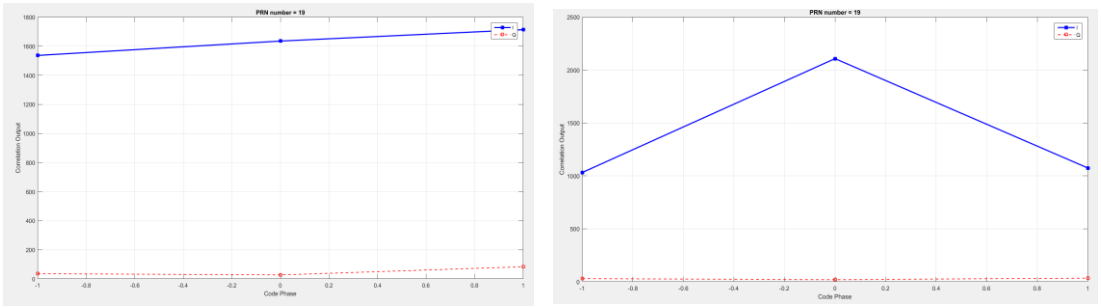
(الف) (ب)

شکل ۱۵ – خروجی همبسته‌ساز PRN=22: (الف) معتبر و (ب) جعلی.



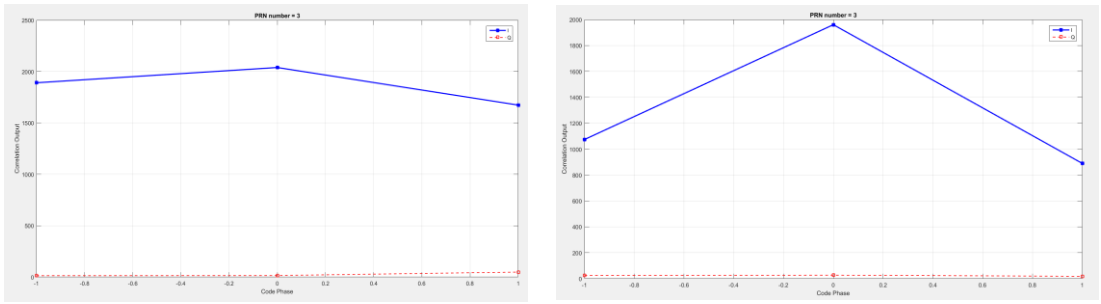
(ب) (الف)

شکل ۱۶ – خروجی همبسته‌ساز PRN=6: (الف) معتبر و (ب) جعلی.



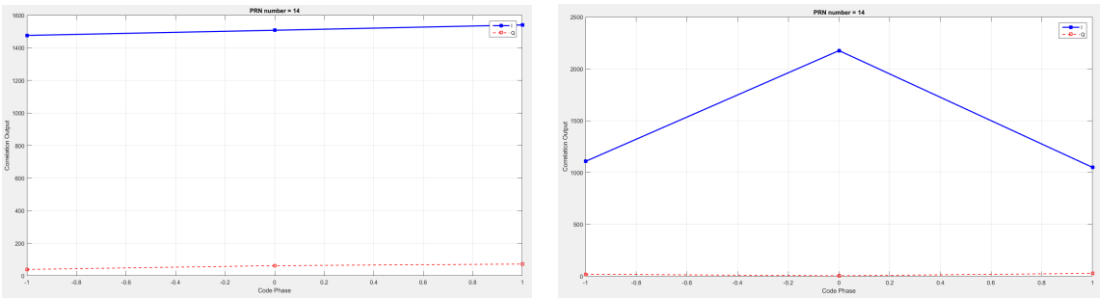
(ب) (الف)

شکل ۱۷ – خروجی همبسته‌ساز PRN=19: (الف) معتبر و (ب) جعلی.



(ب) (الف)

شکل ۱۸ – خروجی همبسته‌ساز PRN=3: (الف) معتبر و (ب) جعلی.



(ب) (الف)

شکل ۱۹ – خروجی همبسته‌ساز PRN=14: (الف) معتبر و (ب) جعلی.

۵. نتیجه‌گیری

در این مقاله، ضمن معرفی فریب به عنوان یکی از مخرب‌ترین حملات سامانه GPS به بررسی و آشکارسازی آن در حلقه ردیابی گیرنده نرم‌افزاری، با استفاده از معیار دلتا در مبحث ارزیابی دفاع سیگنال باقی‌مانده پرداخته شد که قادر به آشکارسازی ناهنجاری به وجود آمده، در سیگنال است. در نهایت، با استفاده از تفاوت‌های نمودار خروجی همبسته‌ساز سیگنال اصلی و جعلی، می‌توان به وجود فریب در سیگنال جعلی پی برد.

از مزایای استفاده از روش گیرنده نرم‌افزاری، می‌توان به انعطاف پذیری و عدم نیاز به تجهیزات سخت‌افزاری اشاره کرد که البته دارای دقت بسیاری می‌باشد و از نظر حافظه، نیازی به اطلاعات قبلی ندارد. چالش این روش، بار محاسباتی زیاد آن است. از معایب روش دلتا، می‌توان به این موضوع اشاره کرد که ممکن است حمله فقط روی بخش همبسته‌ساز Q تاثیر بگذارد و تغییری در بخش I نداشته باشد، لذا در این حالت آشکارسازی مختل می‌گردد. بنابراین، برای بهبود آشکارسازی، لازم است از معیارهایی استفاده شود که بتوان تاثیر فریب را در هر دو عامل I و Q بررسی نمود. همچنین، در این مقاله از سه همبسته‌ساز برای ردیابی و نظارت سیگنال استفاده شد. با افزایش تعداد همبسته‌سازها می‌توان دقت این روش را افزایش داد.

مراجع

[۱] سید محمد رضا موسوی میرکلایی، "پردازش داده‌ها در گیرنده‌های تک فرکانسه GPS"، انتشارات دانشگاه علم و صنعت ایران، ۱۳۸۹.

[۲] سید محمد رضا موسوی میرکلایی، مریم معاضدی، محمد جواد رضایی و امیر طباطبایی، "مقابله با اختلال در گیرنده‌های GPS"، انتشارات دانشگاه علم و صنعت ایران، ۱۳۹۴.

[3] M. Moazedi, M. R. Mosavi and A. Sadr, "Real-Time Interference Detection in Tracking Loop of GPS Receiver", Iranian Journal of Electrical & Electronic Engineering, Vol. 13, No. 2, pp. 194-204, 2017.

[4] A. Sadr, M. R. Mosavi, and M. Moazedi, "High-Sensitivity GPS Data Classification Based on Fuzzy Logic", Journal of Marine Science, Vol. 8, No. 1, pp. 115-126, 2021.

[5] P. Melin, F. Olivas, O. Castillo, F. Valdez, J. Soria and M. Valdez, "Optimal Design of Fuzzy Classification Systems using PSO with Dynamic Parameter Adaptation through Fuzzy Logic", Tijuana Institute of Technology, Vol. 40, No. 8, pp. 3196-3206, 2013.

[6] S. Tohidi and M. R. Mosavi, "Effective Detection of GNSS Spoofing Attack using a Multi-Layer Perceptron Neural Network Classifier Trained by PSO", Iran University of Science and Technology Tehran, Iran, 25th International Computer Conference (CSICC 2020), 1-2 January 2020.

[7] A. J. Jahromi, A. Broumandan, J. Nielsen and G. Lachapelle, “GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques”, International Journal of Navigation and Observation, pp.1-16, 2012.

[8] K. Borrea and I. Kudryavtsev, "Software Defined GNSS Receiver", Scientific and Technological Experiments on Automatic Space Vehicles and Small Satellites, Vol. 104, pp. 9-14, 2015.

[9] Y. Hu, "GNSS SDR Signal Generator Implementation Based on USRP N210", International School Beijing University of Posts and Telecommunications, Beijing, 100878, China, 2019.

[10] W. Feng, J. M. Friedt, G. Goavec-Merou and F. o. Meyer, "Software Defined Radio Implemented GPS Spoofing and Its Computationally Efficient Detection and Suppression", IEEE Aerospace and Electronic Systems Magazine, Vol. 36, No. 3, pp. 36-52, 2021.

[11] K. Borre, D. M. Akos, N. Bertelsen, P. Rinder and S. H. Jensen, “A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach”, Birkhäuser Boston, 2007.

[12] O. V. Korniyenko and M. S. Sharawi, “GPS software Receiver Implementations”, IEEE Potentials, Vol. 26, No. 3, pp. 42-46, 2007.