مجله علمی - پژوهشی "پدافند الکترونیکی و سایبری"

سال سوم، شماره ۴، زمستان ۱۳۹۴، ص ۲۲- ۱۱

مقابله با فریب در گیرنده GPS با استفاده از همبستگی و روش حداقل میانگین مربعات بر مبنای الگوریتم Sign-Data

زهرا شخم‌زن[۱] و سید محمدرضا موسوی میرکلایی[۲*]

۱-کارشناسی‌ارشد، دانشکده مهندسی برق، دانشگاه علم و صنعت ایران

۲-استاد، دانشکده مهندسی برق، دانشگاه علم و صنعت ایران

(دریافت:۹۳/۱۲/۲۸، پذیرش: ۹۴/۱۰/۲۲)

چکیده

در میان انواع تداخل سیگنال ماهواره‌های سامانه موقعیت‌یاب جهانی GPS، فریب به‌عنوان خطرناک‌ترین دخالت عمدی درنظر گرفته شده است. با حضور فریب در سیگنال دریافتی GPS اطلاعات نادرست به گیرنده می‌رسد که مشکلاتی در محاسبات زمانی و مکانی گیرنده ایجاد می‌کند. مقابله با فریب در دو بخش آشکارسازی و کاهش فریب انجام می‌پذیرد. در این مقاله به‌منظور آشکارسازی سیگنال فریب از ویژگی‌های تابع همبستگی بهره گرفته‌ایم. در فرآیند کاهش فریب، روش فیلتر وفقی LMS بر مبنای الگوریتم Sign-Data مورد استفاده قرار می‌گیرد. این روش اثر تداخل فریب را در سیگنال دریافتی GPS کاهش می‌دهد و در برابر تداخلی از نوع فریب تأخیری دفاع می‌کند. روش پیشنهادی بر روی داده‌های واقعی و در مرحله اکتساب از فرآیند پردازش گیرنده GPS اعمال می‌گردد. نتایج نشان می‌دهند که روش وفقی مبتنی بر الگوریتم Sign-Data به‌طور متوسط اثربخشی فریب را ۸۹ درصد محدود می‌کند. علاوه‌بر کاهش فریب، پارامتر PDOP نیز که نمایانگر موقعیت فضایی ماهواره‌های شناسایی‌شده است، در همه نتایج بهبود یافته است. به‌طور میانگین مقدار PDOP از ۴۷ به ۲/۶۶ کاهش یافته است.

واژه‌های کلیدی: GPS، آشکارسازی، کاهش فریب، همبستگی، LMS و الگوریتم Sign-Data

۱- مقدمه

ماهواره‌های GPS[۱] به انتشار سیگنال‌های رادیویی می‌پردازند تا این امکان را برای گیرنده‌های GPS فراهم نمایند که به تعیین موقعیت و زمان همگام‌شده بپردازند. گیرنده GPS براساس اختلاف زمان ارسال و دریافت سیگنال توسط یک ماهواره مشخص می‌کند که گیرنده GPS چقدر از ماهواره فاصله دارد. سپس گیرنده با استفاده از فاصله تا چهار ماهواره مجزا GPS، موقعیت را محاسبه می‌نماید [۳-۱]. امروزه GPS کاربردهای بسیار وسیعی در زمینه‌های مختلف صنعتی، نظامی، غیرنظامی، کشاورزی، حمل و نقل و نقشه‌برداری پیدا کرده است [۴].

سیگنال GPS ممکن است در بین مسیر توسط فریبنده دچار اختلال شود. درنتیجه این عمل گیرنده در پیداکردن موقعیت خود دچار مشکل می‌شود. در میان انواع تداخل سیگنال GPS، فریب به‌عنوان خطرناک‌ترین دخالت عمدی درنظر گرفته‌شده است [۵]. تهدید حملات فریب به سه بخشِ اصلی تقسیم می‌شود.

نخستین فریب، حمله ساده از طریق شبیه‌ساز سیگنال GPS است. یکی از راه‌های ساده فریب اضافه‌کردن یک تقویت‌کننده قدرت و یک آنتن به شبیه‌ساز سیگنال GPS و تابش سیگنال RF[۲] به‌سمت گیرنده موردنظر است. البته مشکلاتی نیز برای این نوع فریب وجود دارد. اولین مسئله، هزینه و مشکل دیگر آن، فضای اشغالی است. حمله فریب مبتنی بر شبیه‌ساز سیگنال به‌سادگی آشکار می‌گردد. دومین فریب، حمله متوسط از طریق گیرنده- فریبنده قابل‌حمل است. گیرنده- فریبنده می‌تواند به اندازه‌ای کوچک ساخته شود که به‌طور نامعلوم در کنار آنتن گیرنده اصلی قرار گیرد. گیرنده- فریبنده، سیگنال اصلی GPS را برای تخمین مکان، سرعت و زمان خودش دریافت می‌کند که به‌دلیل نزدیکی به گیرنده اصلی تقریباً با آن برابر است. سپس برطبق این تخمین سیگنال‌های جعلی را تولید می‌کند و حمله فریب را به‌وجود می‌آورد. اگر گیرنده اصلی ساکن باشد و مکان آن نسبت به گیرنده- فریبنده مشخص باشد، گیرنده- فریبنده می‌تواند تا حدودی دورتر از گیرنده اصلی قرار بگیرد.

سومین فریب به حمله‌های پیچیده از طریق چند حلقه قفل فاز توسط گیرنده- فریبنده قابل حمل معروف هستند. در واقع این حمله همان حمله با یک گیرنده- فریبنده است که در آن از

*رایانامه نویسنده پاسخگو: m_mosavi@iust.ac.ir

1- Global Positioning System

2- Radio Frequency

تعداد بیش‌تری از این دستگاه استفاده شده است و پیچیدگی بیش‌تری دارد. یکی از قوی‌ترین راه‌های دفاعی در برابر این حمله روش‌های رمزنگاری است [۶].

وقتی سیگنال GPS دچار فریب می‌گردد، گیرنده قادر به تفکیک سیگنال‌های معتبر و جعلی نیست و باتوجه به توان بزرگ‌تر سیگنال فریب، آن را به‌جای سیگنال اصلی ردیابی و پردازش می‌کند [۷]. مقابله با فریب می‌تواند در هریک از سطوح گیرنده از جمله بخش پردازش سیگنال، بخش بیت داده، معادلات موقعیت‌یابی و بخش موقعیت‌یابی (اکتساب، ردیابی و استخراج شبه‌فاصله) انجام پذیرد. در روش‌های مقابله با فریب تمرکز بر روی وجوه تمایز سیگنال‌های معتبر و جعلی است. برای حل مشکل فریب مطالعات گسترده‌ای در حال انجام است و روش‌های متنوعی برای مقابله با فریب ارائه و نمونه‌های عملی آن ساخته شده است [۸ و ۹].

در این مقاله اقدام مقابل برای کاهش فریب اعمال‌شده به سیگنال GPS صورت می‌پذیرد. به‌منظور آشکارسازی سیگنال فریب از راه‌کاری با استفاده از تابع همبستگی و برای کاهش اثر فریب از راه‌کار فیلتر وفقی بهره می‌بریم. در فرآیند کاهش فریب، روش وفقی LMS بر مبنای الگوریتم Sign-Data مورد استفاده قرار می‌گیرد.

مراحل تدوین مقاله به‌شرح زیر صورت گرفته است. بخش دوم برخی روش‌های مرتبط با موضوع آشکارسازی و کاهش فریب را اشاره می‌کند. در بخش سوم، توضیح مختصری از نحوه تولید سیگنال فریب معرفی می‌گردد. راه‌کار آشکارسازی فریب براساس ویژگی‌های تابع همبستگی در بخش چهارم ارائه می‌گردد. بخش پنجم روش وفقی LMS مبتنی بر الگوریتم را برای کاهش اثر سیگنال فریب دریافتی تشریح می‌نماید. در بخش ششم نتایج حاصل از روش ارائه‌شده با داده‌های واقعی گزارش می‌شود. در پایان نیز نتیجه‌گیری از کل مباحث بیان‌شده انجام می‌پذیرد.

۲- مروری بر روش‌های مقابله با فریب در GPS

چند نمونه روش تشخیص و کاهش فریب که در مقالات معتبر ذکر گردیده‌اند، در ادامه آمده است. برای مقابله با فریب باید بین دفاع رمزنگاری و غیررمزنگاری تمایز قائل شد. ابتدا چند روش غیررمزنگاری معرفی می‌شود. در پایان نیز روش‌های رمزنگاری بیان می‌گردند.

یکی از قویترین روش‌های غیررمزنگاری مقابله با فریب دفاع چندآنتنه است. این دفاع به فضای دو یا چندآنتنه‌ای نیاز دارد که به‌وسیله بخش قابل ملاحظه‌ای، تقریباً ۲۰ سانتی‌متر، از طول موج سیگنال GPS تأمین می‌شود. این عمل با افزایش هزینه، وزن و اندازه گیرنده همراه است. درنتیجه دفاع چندآنتنه به‌طور گسترده توسط تولیدکنندگان تجاری GPS مورد استفاده قرار نمی‌گیرد [۱۰].

شپارد[1] [۱۱] نشان داد که تداخل بین پیک همبستگی سیگنال اصلی و سیگنال فریب بسیار شبیه به تداخل چندمسیری و مسیر مستقیم است. بنابراین روش‌های آشکارسازی و کاهش چندمسیری می‌تواند برای فریب نیز مورد استفاده قرار گیرد. نظارت بر کیفیت سیگنال[2] (SQM) یک روش آشکارسازی چندمسیری است که برای آشکارسازی حملات فریب بر روی گیرنده‌های ردیابی به‌کار برده شده است. لدوینیا[3] [۱۲] نرخ و اختلاف آزمون‌های SQM برای آشکارسازی فریب و سپس روش RAIM[4] را برای آشکارسازی و کاهش فریب در سطح ناوبری و مسائل مکان‌یابی به‌کار گرفت. روش RAIM، یک دفاع عملی در مقابل خطای اندازه‌گیری شبه‌فاصله در گیرنده GPS است. این روش از طریق فرضیه آماری، خطای اندازه‌گیری شبه‌فاصله را آشکار می‌کند و خطای اندازه‌گیری را از مسئله ناوبری حذف می‌نماید. آزمون فرضیه آماری استفاده شده در RAIM متکی بر روش استاندارد تنظیم احتمال هشدار اشتباه و محاسبه آستانه براساس احتمال تشخیص است. این دقت زیربنای RAIM و تأکید آن بر آزمون فرضیه آماری، آزمون‌های مشابه RAIM را برای آشکارسازی و کاهش فریب گسترش داده است [۱۳].

مشخصه CNR[5] و شبه فاصله از جمله معیارهایی هستند که در مقابله با فریب به‌طور معمول مورد استفاده قرار می‌گیرند. در مرجع [۱۴] بررسی CNR با یک قاعده تصمیم‌گیری ادغام شده است. عملکرد این روش بر پایه تخمین CNR پیک همبستگی سیگنال‌های GPS دریافتی قرار دارد. مسئله اصلی در این روش تعیین حدآستانه بهینه برای مقایسه CNR است. درصورتی‌که توان سیگنال فریب شناخته‌شده باشد، انتخاب حد آستانه بهینه مشکل نیست. اما در ازای مقدار CNR نامعلوم سیگنال فریب، حد آستانه بهینه با بهینه‌سازی تعیین می‌شود. فرض می‌شود که در اثر وجود فریب دو پیک همبستگی در سیگنال وجود دارد و از احتمال وجود پیک دیگر در اثر چندمسیری و طراحی ضعیف گیرنده صرف‌نظر شده است. قاعده‌ای برای تشخیص سیگنال فریب وجود دارد. به این نحو که با مقایسه CNR سیگنال واقعی و فریب نسبت به حد آستانه بهینه پیک بزرگ‌تر به سیگنال واقعی یا سیگنال فریب نسبت داده می‌شود. باتوجه به این قاعده و اندازه احتمال خطای کلی میزان موثربودن فریبنده مشخص

1- Shepard
2- Signal Quality Monitoring
3- Ladonia
4- Receiver Autonomous Integrity Monitoring
5- Carrier to Noise Ratio

می‌گردد. مرجع [۱۵] نیز از بررسی مداوم شبه‌فاصله برای تشخیص تغییرات غیرمعمول آن در اثر حمله فریب استفاده کرده است.

روش‌های رمزنگاری گیرنده را قادر می‌سازند تا سیگنال‌های معتبر GPS را از سیگنال‌های جعلی با احتمال زیاد تشخیص دهد. لوگان اسکات[1] [۱۶] یک روش رمزنگاری ضدفریب براساس کدهای امنیتی طیف گسترده[2] (SSSC) پیشنهاد داد. آخرین نسخه ارائه‌شده این روش که هدف آن سیگنال L1C است بر روی ماهواره‌های بلوک۳ GPS منتقل خواهد شد، زیرا شکل موج L1C هنوز نهایی نشده‌است. در همان مقاله ION-GNSS 2003، لوگان اسکات NMA را نیز پیشنهاد داد. اگر اجرای L1C بر روی SSSC غیرعملی باشد، طرح اعتبارسنجی پیام ناوبری[3] (NMA)، یک مورد با پس‌زمینه قوی را در اختیار قرار می‌دهد. روش NMA یک امضای دیجیتالی عمومی در ساختار انعطاف‌پذیر سیگنال ناوبری[4] (CNAV) تعبیه می‌کند [۱۷].

به‌طورکلی روش چندآنتنه درکنار کارآیی مناسب، پیچیدگی پردازشی و سخت‌افزاری گیرنده را به‌طور قابل ملاحظه‌ای افزایش می‌دهد. RIAM هم با جود دقت بالا، پیچیدگی محاسباتی بالایی به‌همراه دارد. همچنین، در حضور پدیده چندمسیری عملکرد خوبی از خود نشان نمی‌دهد. روش انتخاب پیک معتبر از لحاظ پیاده‌سازی ساده است، اما در مقابله با حمله تأخیری بازدهی خوبی ندارد. روش‌های رمزنگاری از نظر امنیتی و کارآیی دقت بسیار خوبی دارند، ولی به تغییر در ساختار سیگنال GPS نیاز دارند.

۳- تحلیل سیگنال فریب در GPS

اجزای تشکیل‌دهنده سیگنال GPS به‌صورت رابطه (۱) می‌باشد:

$$s_Z = \sqrt{2P_c}\left(c^Z(t) \oplus D^Z(t)\right)\cos(2\pi f_{L1} t) + N_Z \qquad (۱)$$

در این رابطه، P_C توان سیگنال GPS، C^Z و D^Z به‌ترتیب بیانگر کد C/A و داده ناوبری می‌باشند. Z نمایانگر شماره ماهواره است. f_{L1} هم فرکانس حامل و N_Z نیز دنباله نویز گوسی با میانگین صفر و واریانس σ^2 می‌باشد [۱۷]. در فرآیند فریب برای گمراه‌کردن گیرنده هدف، سیگنال دریافتی گیرنده اصلی، ترکیبی از سیگنال فریب و سیگنال معتبر است. در این مقاله شبیه‌سازی این سیگنال ترکیبی مورد استفاده قرارمی‌گیرد و به‌صورتی‌که در ادامه بیان می‌گردد، به‌دست می‌آید. در سازوکار ترکیب سیگنال معتبر و فریب دو عامل مؤثر تأخیر و دامنه اهمیت دارد. در عمل برای تولید سیگنال فریب، گیرنده فریبنده سیگنال اصلی را تأخیر می‌دهد. برای ایجاد حمله موفق، نسبت توان سیگنال فریب را بزرگ‌تر از سیگنال معتبر درنظر می‌گیرند. بنابراین سیگنال تأخیریافته را در یک عدد بزرگ‌تر از یک (α) ضرب می‌کند تا توان سیگنال تأخیر یافته بیش‌تر از توان سیگنال اصلی باشد. بدین ترتیب سیگنال فریب s_{spoof} توسط رابطه (۲) شناخته می‌گردد. سپس سیگنال معتبر و فریب به‌طور همزمان به گیرنده GPS می‌رسند. در واقع سیگنالی که دریافت می‌شود به‌صورت ترکیب سیگنال اصلی و فریب می‌باشد. درنتیجه دو سیگنال از یک جنس دریافت می‌شود، اما یکی تأخیر یافته و توان بیش‌تری نسبت به دیگری دارد. سیگنال دریافتی در گیرنده اصلی GPS پس از ترکیب سیگنال اصلی و فریب توسط رابطه (۳) مشخص می‌گردد.

$$s_{spoof} = \alpha s_{Z-d} \qquad (۲)$$

$$x_Z = s_Z + s_{spoof} \qquad (۳)$$

که در این دو عبارت، s_Z نشان‌دهنده سیگنال معتبر دریافتی از ماهواره شماره Z است و s_{Z-d} سیگنال تأخیریافته توسط گیرنده فریبنده می‌باشد. مشخصه α که مقدار ۲+ دارد، ضریب سیگنال تأخیر یافته را نشان می‌دهد. x_Z سیگنالی است که به‌عنوان سیگنال ترکیبی معتبر و فریب به گیرنده هدف می‌رسد. سیگنال ماهواره‌های GPS که دچار فریب شدند، پس از دریافت توسط آنتن گیرنده تقویت می‌شود. سپس این سیگنال دریافتی از بخش Front End عبور کرده و تبدیل به فرکانس باند میانی می‌شود. سیگنال مربوطه نمونه‌برداری شده و وارد قسمت‌های اکتساب و ردگیری گیرنده نرم‌افزاری GPS می‌گردد. در ادامه راه‌کار آشکارسازی فریب مبتنی بر تابع همبستگی و روش وفقی LMS[5] مبتنی بر الگوریتم sign-data برای جبران اثر سیگنال فریب ارائه گردیده است. با اعمال این روش‌ها در بخش اکتساب گیرنده بر سیگنال دیجیتال ورودی با فرکانس میانی IF[6] که همراه با فریب است، اقدام متقابل برای کاهش فریب صورت می‌گیرد. در بخش اکتساب گیرنده ماهواره‌های در دسترس ظاهر می‌شوند و گیرنده از داده‌های ۵ تا از این ماهواره‌ها در حل معادلات ناوبری برای مکان‌یابی استفاده می‌نماید. حسن انتخاب بخش اکتساب برای اعمال روش مورد نظر مقاله این است که گیرنده بتواند به‌صورت بلادرنگ عمل نماید.

1- Logan Scott
2- Spread Spectrum Security Codes
3- Navigation Message Authentication
4- Civil Navigation Message

5- Least Mean Squares
6- Intermediate Frequency

۴ - آشکارسازی فریب در GPS

از تابع همبستگی، اغلب در پردازش سیگنال برای تحلیل توابع یا مجموعه داده‌ها از جمله حوزه زمان سیگنال‌ها استفاده می‌گردد. همبستگی گرفتن از دو سیگنال ویژگی‌هایی از دو سیگنال را در اختیار قرار می‌دهد. در یک تعریف عام، همبستگی گرفتن میزان شباهت بین دو سیگنال را مشخص می‌کند. در این مقاله با به‌کارگیری تابع همبستگی و درنظرگرفتن ویژگی‌های آن، سیگنال فریب را در سیگنال دریافتی گیرنده GPS آشکار می‌نماییم. در بخش اکتساب گیرنده معتبر با همبستگی گرفتن از سیگنال دیجیتال ورودی IF که همراه با فریب است، می‌توان به تأخیر موجود در سیگنال فریب دست یابیم. برای این هدف دو نوع همبستگی مورد استفاده قرار گرفت. یکی خود همبستگی و دیگری همبستگی متقابل است. در خود همبستگی از دو سیگنال یکسان و در همبستگی متقابل از دو سیگنال متفاوت همبستگی گرفته می‌شود. روابط مربوط به خود همبستگی و همبستگی متقابل به‌ترتیب در روابط (۴) و (۵) آمده است.

$$r_s(k) = \sum_{n=-\infty}^{\infty} s_Z^*(n) s_Z(n+k) \qquad (۴)$$

$$r_{sx}(k) = \sum_{n=-\infty}^{\infty} s_Z^*(n) x_Z(n+k) \qquad (۵)$$

رابطه (۴) خود همبستگی از سیگنال معتبر را نشان می‌دهد. دو ویژگی که از همبستگی گرفتن بین دو سیگنال می‌توان استخراج کرد، تأخیر و توان سیگنال است. در این تحقیق به‌دنبال یافتن تأخیر سیگنال فریب درون سیگنال دریافتی GPS هستیم. به این معنی که اگر تأخیری در سیگنال یافتیم از حضور سیگنال فریب در سیگنال ورودی گیرنده GPS مطلع می‌شویم. واضح است که برای به‌دست آوردن تأخیر (d) در رابطه (۲) و آشکارسازی سیگنال فریب موجود در سیگنال ترکیبی می‌توان از تابع همبستگی متقابل رابطه (۵) استفاده نمود. بدین معنی که بین سیگنال معتبر رابطه (۱) و سیگنال ترکیبی رابطه (۳)، همبستگی متقابل گرفته شود. اما در این تحقیق چون نوع گیرنده هدف تک‌فرکانسه است، فقط می‌توان یک سیگنال را در فرآیند همبستگی شرکت داد. بدین ترتیب در حضور فریب، سیگنال ترکیبی همانند رابطه (۳) به گیرنده می‌رسد. بنابراین برای آشکارسازی فریب در این حالت رابطه‌ای مشابه رابطه (۴) به‌کار برده می‌گردد. ولی در این حالت به‌جای سیگنال معتبر از سیگنال ترکیبی ذکرشده در رابطه (۳) بهره می‌گیریم. پس با به‌کارگیری سیگنال ترکیبی در رابطه (۴)، رابطه (۶) به‌دست می‌آید.

$$r_x(k) = \sum_{n=-\infty}^{\infty} x_Z^*(n) x_Z(n+k) \qquad (۶)$$

بنابراین باتوجه به ماهیت سیگنال فریب و سیگنال ترکیبی x_Z این امکان وجود دارد که با خودهمبستگی‌گرفتن از سیگنال دریافتی در بخش اکتساب گیرنده به آشکارسازی تأخیر موجود در سیگنال فریب دست یابیم [۱۸].

۵- راه‌کار پیشنهادی کاهش فریب در GPS

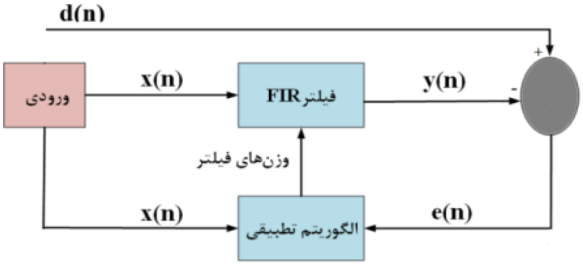
پس از آشکارسازی فریب نیاز به روشی است که اثر سیگنال فریب در گیرنده GPS کاهش یابد. ارتباط بین بخش آشکارسازی و بخش کاهش فریب در این است که میزان تأخیر کمک می‌کند در گیرنده نرم‌افزاری چه مقدار از سیگنال IF ورودی در روش کاهش فریب شرکت نماید، زیرا در بخش اکتساب نیازی نیست کل سیگنال ورودی مورد پردازش قرار گیرد. با دانستن میزان تأخیر و تنظیمات مناسب گیرنده نرم‌افزاری می‌توان به اندازه‌ای سیگنال مورد استفاده قرار داد که هم ماهواره‌های در دسترس شناسایی گردند و هم بخشی از سیگنال در فرآیند کاهش فریب شرکت کند که شامل سیگنال تأخیری است.

یکی از روش‌های حذف تداخل استفاده از فیلترهای وفقی می‌باشد. وقتی سیگنالی در معرض تداخل قرار می‌گیرد، با استفاده از فیلتر وفقی می‌توان سیگنال معتبر را از مزاحم جدا نمود [۱۹]. بنابراین با استفاده از فیلتر وفقی می‌توان تداخل فریب را از سیگنال معتبر حذف نمود. فریبی که در این مقاله بکار می‌گیریم از نوع فریب تأخیری است. سازوکار این نوع فریب در بخش ۳ شرح داده شد. در ادامه این بخش از راه‌کار فیلتر وفقی برای کاهش فریب بهره می‌گیریم. همانند بخش آشکارسازی، اعمال فیلتر وفقی در بخش اکتساب گیرنده بر سیگنال ورودی IF صورت می‌پذیرد تا ماهواره‌های معتبر شناسایی گردند. با شناسایی ماهواره‌های معتبر خطای گیرنده در فرآیند مکان‌یابی کاهش پیدا می‌کند. سیگنال IF دیجیتال به صورت داده‌های چهارسطحی با سطح‌های ۱± و ۳± می‌باشد.

روش‌های گوناگونی برای پیاده‌سازی الگوریتم به‌روزرسانی ضرایب فیلتر وفقی وجود دارد. باتوجه به هدف این تحقیق، بهترین انتخاب فیلتری با روش حداقل میانگین مربعات خواهد بود، زیرا برای پیاده‌سازی روش و خروجی محاسبات به‌صورت بلادرنگ، لازم است محاسبات تا حد امکان ساده و حجم محاسباتی نیز متناسب با توان پردازشی موجود باشد. بنابراین در ادامه با انتخاب روش LMS مبتنی بر الگوریتم Sign-Data به ذکر توضیحات و معرفی این روش می‌پردازیم.

این نوع از فیلترهای وفقی طوری ضرایب فیلتر را تغییر می‌دهند که میانگین مربعات خطا را به حداقل برساند. این راه‌کار از روش نزول شیب تصادفی[1] برای تطبیق استفاده می‌کند، به‌طوری‌که تنها با اطلاع از مقدار خطای فعلی ضرایب را تغییر می‌دهد.

روش LMS به روشی تکرارشونده، پی‌درپی اطلاعاتی را در جهت منفی بردار شیب[2] بر وزن‌های فیلتر اعمال می‌کند که در نهایت به حداقل شدن خطای میانگین مربعات می‌انجامد [۲۰]. در این مقاله از فیلتری با پاسخ ضربه محدود[3] (FIR) به‌دلیل انطباق‌پذیری بالا و سادگی در پیاده‌سازی الگوریتم LMS بهره می‌بریم. این فیلتر FIR وزن‌های متغیری دارد که مشخصه آن باتوجه به شرایط سیگنال ورودی تغییر پیدا می‌کند. همانند فیلتر FIR، فیلترهای با پاسخ ضربه نامحدود[4] IIR نیز می‌توانند در هسته روش وفقی استفاده گردند، اما ممکن است در حین به‌روزرسانی به‌سمت ناپایداری پیش روند. اگرچه انواع گوناگونی از روش LMS ارائه گردیده است، به‌دلیل سادگی در محاسبات، الگوریتم Sign-Data مورد استفاده قرار گرفته است. در این الگوریتم به‌جای استفاده از سیگنال ورودی در روش اصلی LMS، از تابع علامت آن استفاده می‌شود. نمای کلی فیلتر وفقی ذکر شده در شکل (۱) نمایش داده شده است. باتوجه به این شکل ورودی‌های روش وفقی، سیگنال‌های d(n) و x(n) دارای نمونه‌هایی با اندازه N می‌باشند. طبق رابطه (۷)، ورودی x(n) ترکیبی از سیگنال معتبر و فریب می‌باشد. مطابق با رابطه (۸)، سیگنال d(n) شامل سیگنال مطلوب $s'_Z(n)$ است که بخشی از سیگنال دیجیتال معتبر GPS است. به‌منظور حذف فریب از سیگنال x(n) و دست‌یابی به سیگنال معتبر در خروجی فیلتر تطبیقی بخش سیگنال معتبر در x(n) و سیگنال مطلوب d(n) نباید با بخش سیگنال فریب همبستگی داشته باشند، اما ورودی d(n) و بخش سیگنال معتبر باید همبستگی داشته باشند.



شکل (۱). نمای بلوکی فیلتر وفقی ارائه‌شده به‌منظور مقابله با فریب در GPS

$$x(n) = s_N(n) + s_{spoof}(n) \quad (۷)$$

$$d(n) = \acute{s}_N(n) \quad (۸)$$

باتوجه به این‌که سیگنال d(n) شامل سیگنال مطلوبی از جنس سیگنال معتبر است، پس سیگنال d(n) با بخش سیگنال معتبر x(n) همبستگی دارد. به‌دلیل این‌که سیگنال معتبر ماهواره‌ها و سیگنال فریب نیز از دو منبع مختلف تولید می‌گردند، این دو سیگنال مستقل هستند و سیگنال معتبر و فریب با هم همبستگی ندارند. پس جزء فریب سیگنال x(n) در فرآیند فیلترینگ حذف می‌گردد و باتوجه به شکل (۱)، جزء سیگنال فریب در خروجی y(n) ظاهر نمی‌گردد. بنابراین آنچه در خروجی y(n) فیلتر وفقی باقی می‌ماند، تخمینی از بخش سیگنال معتبر خواهد بود که با کسر آن از d(n) آنچه در خروجی باقی می‌ماند (یعنی e(n))، جزئی از سیگنال مزاحم فریب است. باتوجه به این ویژگی‌ها، روش فیلتر وفقی LMS مبتنی بر الگوریتم sign-data گزینه مناسبی برای حذف تداخل فریب از سیگنال دریافتی GPS است. در ادامه مراحل مختلف این روش بیان می‌گردد. خروجی فیلتر وفقی توسط رابطه (۹) مشخص می‌شود. این خروجی تخمینی از سیگنال دیجیتال معتبر است.

$$y(n) = \sum_{m=0}^{M-1} w_m(n) x(n-m) \quad (۹)$$

در این رابطه، $w_m(n)$ معرف تعداد M ضریب فیلتر در زمان معین n است. معیاری برای تعیین چگونگی عملکرد فیلتر لازم است که از تفاضل خروجی فیلتر و خروجی مطلوب بدست می‌آید. هرقدر d(n) با $s_N(n)$ هم‌پوشانی بیش‌تری داشته باشد، مقدار e(n) به صفر نزدیک‌تر خواهد بود و فیلتر عملکرد بهتری را از خود نشان خواهد داد.

$$e(n) = d(n) - y(n) \quad (۱۰)$$

همان‌طورکه اشاره شد، ضرایب فیلتر طوری تنظیم می‌شوند که میانگین مربعات خطا e(n) به حداقل برسد. از آنجایی‌که تعداد m ضریب برای فیلتر موجود است، الگوریتم به‌روزرسانی به‌صورت زیر معرفی می‌گردد:

$$w_m(n+1) = w_{km}(n) + 2\mu e(n) sgn x(n-m) \quad m = 0,1,\dots M-1 \quad (۱۱)$$

رابطه (۱۱) روشی ساده و در عین حال بهینه و قدرتمند را جهت به‌روزرسانی ضرایب فیلتر بدون میانگین‌گیری و یا مشتق‌گیری برای پیاده‌سازی فیلترهای تطبیقی معرفی می‌کند. در معادله فوق، x(n) ورودی فیلتر در زمان n می‌باشد. باتوجه به

1- Stochastic Gradient Descent
2- Gradient Vector
3- Finite Impulse Response
4- Infinite Impulse Response

این عبارت به‌جای استفاده از سیگنال ورودی، از تابع علامت آن استفاده می‌نماید. پارامتر μ که اندازه گام[1] نامیده می‌گردد، نرخ همگرایی[2] و دقت فرآیند انطباق[3] را نشان می‌دهد. انتخاب مقادیر بزرگ برای μ سبب همگرایی سریع می‌گردد، اما در مواردی ناپایداری سیستم را به‌دنبال خواهد داشت [۱۹]. برای اطمینان از این‌که سیستم پایدار خواهد ماند، μ در بازه زیر انتخاب می‌گردد:

$$0 < \mu < \frac{2}{\lambda_{max}} \qquad (۱۲)$$

در این رابطه، λ_{max} بزرگ‌ترین مقدار ویژه ماتریس خود همبستگی ورودی x(n) می‌باشد. پس از این‌که خروجی فیلتر، سیگنال خطا و ضرایب جدید محاسبه گردیدند، باتوجه به ورودی جدید و خطا، به‌روزرسانی جدید صورت می‌پذیرد.

۶- نتایج شبیه‌سازی مجموعه داده‌های اندازه‌گیری

داده‌های مورد نیاز برای شبیه‌سازی به‌وسیله یک گیرنده نرم‌افزاری GPS تک‌فرکانسه جمع‌آوری شد. همچنین، راه‌کارهای پیشنهادی برای آشکارسازی و کاهش فریب در بخش اکتساب یک گیرنده نرم‌افزاری اعمال گردید. به‌منظور آشکارسازی فریب توسط روابط همبستگی (۴ و ۶) به‌ترتیب از سیگنال دیجیتال معتبر GPS و سیگنال دیجیتال ترکیبی x_N شبیه‌سازی به‌عمل آمده است. در ابتدا از سیگنال معتبر خودهمبستگی گرفته شده است تا تفاوت خروجی خودهمبستگی در دو سیگنال بدون فریب GPS و سیگنال شامل فریب مشخص گردد و به ویژگی‌های خودهمبستگی سیگنال بدون فریب پی برده شود. درنهایت عملکرد تابع خودهمبستگی بر سیگنال فریب مورد بررسی قرار گرفته شد. همان‌طورکه در شکل (۲) نشان داده شده است، در خروجی حاصل از تابع خود همبستگی سیگنال بدون فریب یک پیک بزرگ و پیک‌هایی کوچک مشاهده می‌گردد. هرکدام از این پیک‌ها ویژگی‌هایی دارند که اطلاعاتی از سیگنال معتبر مورد بررسی را در اختیار قرار می‌دهند. پیک بزرگی که در مقدار صفر ایجاد می‌گردد، بدین مفهوم است که در مقدار صفر بیش‌ترین شباهت سیگنال رخ می‌دهد. این نتیجه‌ای منطقی است، زیرا دو سیگنال مشابه هستند. لازم به‌ذکر است که کد شبه‌تصادفی ماهواره‌ها هر ۱میلی‌ثانیه تکرار می‌شود. بنابراین پیک‌های کوچک‌تر در بازه‌های ۱میلی‌ثانیه آشکار می‌گردند. از آنجایی‌که در هر ۱میلی‌ثانیه ۵۷۱۴ نمونه داده قرار دارند، باتوجه به شکل (۲) در ضرایب صحیحی از عدد ۵۷۱۴ این پیک‌های کوچک ظهور پیدا می‌کنند.

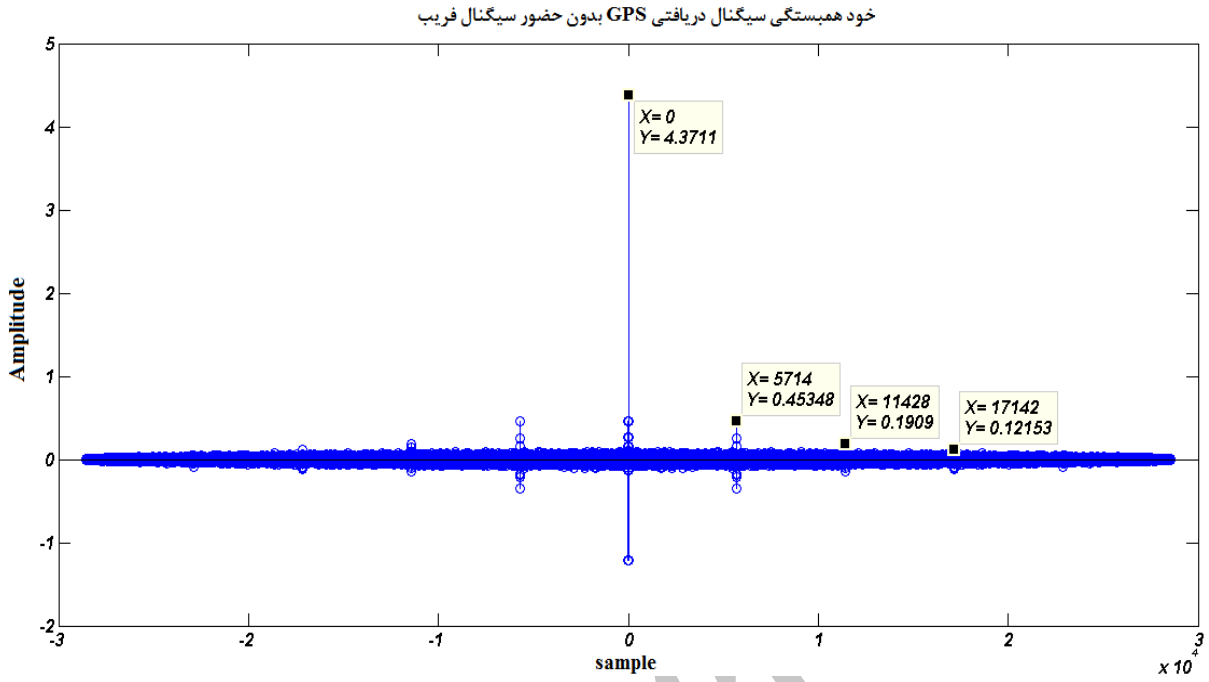
در شکل (۳)، سیگنال ترکیبی x_N که میزان تأخیر در سیگنال فریب آن ۳۵ میلی‌ثانیه است، در فرآیند خودهمبستگی شرکت می‌نماید. همان‌طورکه ملاحظه می‌نماییم، این شکل نسبت به شکل (۲) دچار تغییر شده است. در این شکل سه پیک قابل مشاهده است. پیک بزرگ در صفر رخ می‌دهد که نشان‌دهنده بیش‌ترین شباهت سیگنال در صفر می‌باشد. اما دو پیک کوچک‌تر حضور یک سیگنال فریب در سیگنال دریافتی گیرنده GPS را آشکار می‌نمایند. اگر مقداری که محور افقی در این دو پیک نشان می‌دهد بر عدد ۵۷۱۴ تقسیم نماییم، مقدار تأخیر موجود در سیگنال فریب به‌دست می‌آید. در این شکل دو پیک کوچک مقادیر ۲۰۰۰۰۰± را روی محور افقی نشان می‌دهند. با تقسیم ۲۰۰۰۰۰± بر عدد ۵۷۱۴ مقادیر ۳۵± حاصل می‌گردد که این عدد نشان‌دهنده تأخیر ۳۵ میلی‌ثانیه در سیگنال فریب است. بنابراین دو پیک هم حضور یک سیگنال فریب در سیگنال ورودی گیرنده هدف را آشکار می‌کنند و هم مقدار تأخیر را نشان می‌دهند. سیگنال‌های ترکیبی دیگر با تأخیرهای متفاوت مورد آزمایش قرار گرفت. با این راه‌کار فریب موجود در آنها نیز شناسایی شد. به‌دلیل تشابه نتایج این بخش به بررسی نمودار یک سیگنال ترکیبی اکتفا شده است.

در ادامه این بخش نتایج روش کاهش فریب را مورد بررسی قرار می‌دهیم. همان‌طورکه ذکر شد، به‌منظور کاهش فریب روش فیلتر وفقی LMS مبتنی بر الگوریتم sign-data در بخش اکتساب گیرنده نرم‌افزاری GPS اعمال می‌گردد. برای شبیه‌سازی این روش از فیلتر FIR با طول ۳۱ و گام پیشرفت ۰,۰۰۰۱ بهره گرفته‌ایم.

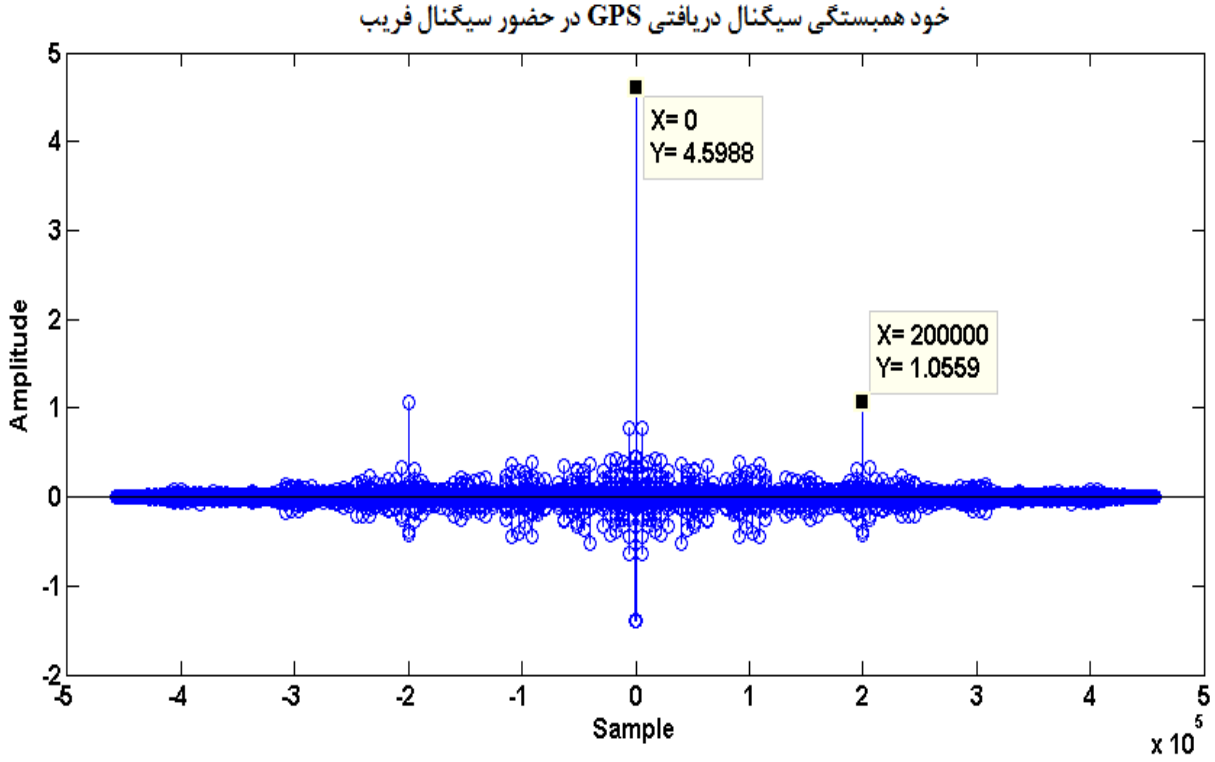
برای مقایسه بین حالت فریب و کاهش فریب شکل‌های خروجی مربوط به یک نمونه داده فریب تأخیری را مورد بررسی قرار می‌دهیم. تأثیر داده فریب مورد آزمایش در گیرنده GPS به‌گونه‌ای است که در حالت معمولی و بدون اعمال روش کاهش فریب، موقعیت گیرنده ۴۵۴ متر نسبت به موقعیت واقعی اختلاف دارد. راه‌کار کاهش فریب، موقعیت گیرنده در حالت فریب را به موقعیت واقعی نزدیک می‌نماید. شکل‌هایی که در ادامه آورده شده‌اند مربوط به نتایج حاصل از تعداد ماهواره‌های رؤیت‌شده در بخش اکتساب و تعیین موقعیت پس از حل معادلات ناوبری است. برای این‌که تفاوت بین نتایج حاصل از فریب و اعمال روش LMS مبتنی بر الگوریتم sign-data مشخص شود، شکل‌های مربوط به هر دو نتیجه پشت سر هم و به‌ترتیب آمده‌اند. در شکل‌های مربوط به اکتساب ماهواره، رنگ سبز نشان‌دهنده ماهواره‌های شناسایی‌شده است. شبیه‌سازی طوری تنظیم شده است که هر ماهواره سبزی به‌عنوان ماهواره معتبر شناخته نمی‌گردد، بلکه در بخش اکتساب باتوجه به

1- Step Size
2- Convergence Rate
3- Accuracy of Adaptation Process

تنظیمات مربوط به تعداد ماهواره‌های در دسترس، ۵ ماهواره‌ای که سطح بیش‌تری دارند، مورد انتخاب قرار می‌گیرند. قابل‌ذکر است ماهواره‌هایی توانایی رؤیت‌شدن دارند که سطح آن‌ها از ۵/۸ بیش‌تر باشد.



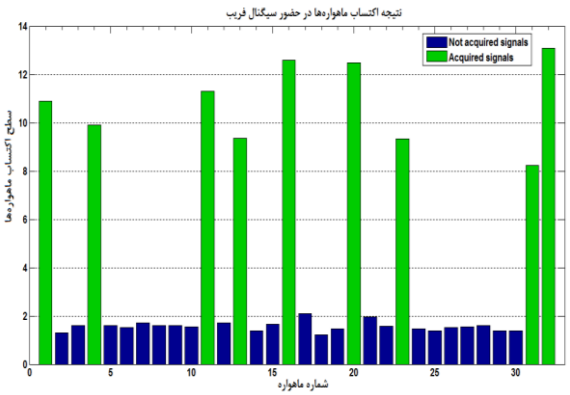
شکل (۲). خروجی خود همبستگی سیگنال GPS بدون حضور سیگنال فریب



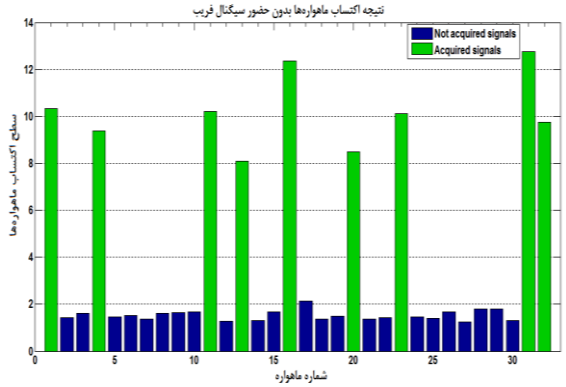
شکل (۳). خروجی خودهمبستگی سیگنال دریافتی GPS همراه با فریب تأخیری ۳۵ میلی‌ثانیه.

به‌ترتیب آمده‌اند. در شکل‌های مربوط به اکتساب ماهواره، رنگ سبز نشان‌دهنده ماهواره‌های شناسایی‌شده است. شبیه‌سازی طوری تنظیم شده است که هر ماهواره سبزی به‌عنوان ماهواره معتبر شناخته نمی‌گردد، بلکه در بخش اکتساب باتوجه به تنظیمات مربوط به تعداد ماهواره‌های در دسترس، ۵ ماهواره‌ای که سطح بیش‌تری دارند، مورد انتخاب قرار می‌گیرند. قابل‌ذکر است ماهواره‌هایی توانایی رؤیت‌شدن دارند که سطح آن‌ها از ۵/۸ بیش‌تر باشد.

شکل‌های (۴ و ۵) نتایج مربوط به تعداد ماهواره‌های رؤیت‌شده در بخش اکتساب، به‌ترتیب در حالت فریب و اعمال الگوریتم Sign-Data را نشان می‌دهند. همان‌طورکه از شکل‌ها مشخص است، در هر دو حالت ۹ ماهواره سبز رؤیت شده است. اما از بین این ۹ ماهواره، ۵ ماهواره‌ای که سطح بالاتری دارند، انتخاب می‌شوند. شکل (۴) مشخص می‌نماید که در حالت فریب ماهواره‌های شماره ۱، ۱۱، ۱۶، ۲۰ و ۳۲ به‌عنوان ۵ ماهواره با سطح بالاتر در فرآیند محاسبه موقعیت گیرنده شرکت می‌نمایند. اما بعد از اعمال الگوریتم کاهش فریب و باتوجه به شکل (۵) ماهواره‌های شماره ۱، ۱۱، ۱۶، ۲۳ و ۳۱ به‌عنوان ۵ ماهواره مفید انتخاب می‌گردند. با مقایسه دو حالت فریب و بعد از اعمال روش کاهش فریب درمی‌یابیم که ماهواره‌های ۲۰ و ۳۲ در حالت فریب جز ۵ ماهواره با سطح بالا بودند، اما پس از اعمال الگوریتم کاهش فریب این دو ماهواره به‌عنوان ماهواره مفید انتخاب نمی‌گردند. همچنین، پس از کاهش فریب ماهواره‌های ۲۳ و ۳۱ به ماهواره‌های معتبر تبدیل شدند. علاوه‌بر تفاوت‌های ذکرشده سطح بقیه ماهواره‌ها هم دچار تغییر شدند.



شکل (۴). نتایج اکتساب ماهواره برای داده فریب ۴۵۴ متری قبل از الگوریتم کاهش فریب



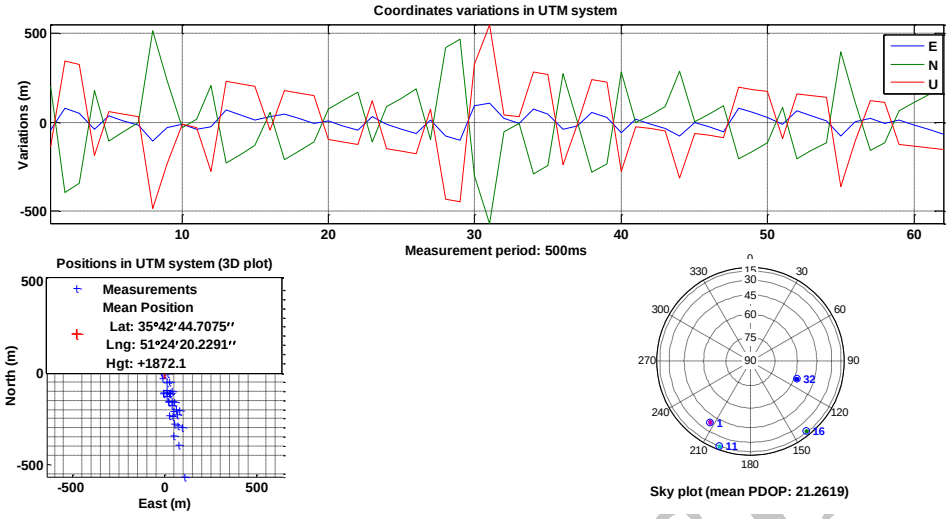
شکل (۵). نتایج اکتساب ماهواره برای داده فریب ۴۵۴ متری بعد از اعمال الگوریتم sign-data

پس از حل معادلات ناوبری در هر دو حالت فریب و کاهش فریب، نتایج موقعیت‌یابی گیرنده GPS در شکل‌های (۶ و ۷) ظهور می‌نمایند. هرکدام از این شکل‌ها شامل سه بخش است. یک قسمت اندازه طول، عرض و ارتفاع در طول حدود ۶۶ بار اندازه‌گیری با گام ۵۰۰ میلی‌ثانیه را نمایش می‌دهد. در قسمت دیگر مقدار متوسط طول، عرض و ارتفاع موقعیت جغرافیایی مشخص می‌گردد. بخش سوم نیز موقعیت فضایی ماهواره‌های در دسترس را نشان می‌دهند. باتوجه به نحوه قرارگیری ماهواره‌ها در فضا، مشخصه PDOP[1] را تعریف می‌کنند. این مشخصه نشان‌دهنده صورت فلکی ماهواره‌های شناسایی شده است. هرچه مقدار این مشخصه کم‌تر باشد، بدین معنی است که ماهواره‌ها به‌طور مطلوبی در فضا قرارگرفته‌اند. با اعمال الگوریتم Sign-Data به‌منظور کاهش فریب و با مقایسه شکل‌های (۶ و ۷) این مشخصه به‌طور چشم‌گیری کاهش یافته است، به‌طوری‌که مقدار PDOP از مقدار حدودی ۲۱ به ۳ تقلیل یافته است. در کل پس از اعمال روش کاهش فریب در بخش اکتساب گیرنده GPS، مقدار مؤثر فریب از ۴۵۴ متر به ۶۱ متر کاهش یافت. درنتیجه به‌کارگیری این روش به کاهش مقدار مؤثر خطای فریب ۸۷ درصدی منجر گردید.

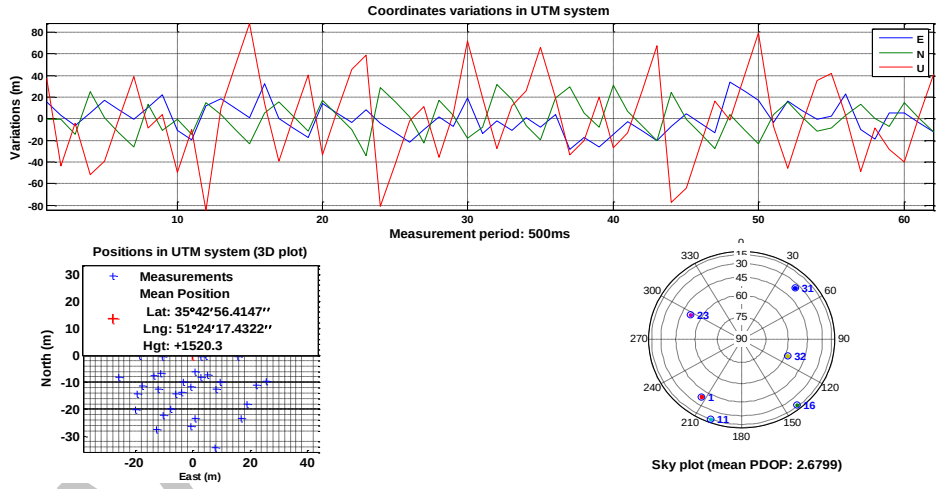
در جدول (۱) جزئیات نتایج شبیه‌سازی مربوط به شش مجموعه داده فریب اندازه‌گیری با تأخیرهای مختلف جمع‌بندی شده‌اند. روش فیلتر وفقی LMS براساس الگوریتم sign-data در هر شش مجموعه داده به کاهش فریب منجر گردید. بهترین نتیجه بر مجموعه داده پنجم رخ داد که درصد کاهش خطای RMS[2] در حدود ۹۵ درصد به‌دست آمد. به‌طورکلی این روش متوسط کاهش خطای RMS حدود ۸۹ درصد را نتیجه می‌دهد. پارامتر PDOP نیز در همه مجموعه داده‌ها کاهش یافته است (به‌طور میانگین از مقدار ۴۷ به ۲/۶۶). پارامتر ΔEN و ΔH

1- Position Dilution of Precision
2- Root Mean Square

به‌ترتیب تغییرات در سطح افق و ارتفاع را نشان می‌دهد.



شکل (۶). نتایج ناوبری برای داده فریب ۴۵۴ متری قبل از الگوریتم کاهش فریب



شکل (۷). نتایج ناوبری برای داده فریب ۴۵۴ متری بعد از اعمال الگوریتم Sign-Data

جدول (۱). نتایج اعمال فیلتر بر روی شش مجموعه داده اندازه‌گیری با فریب حدود ۴۴۰ تا ۶۷۰ متر

داده فریب	قبل از اعمال الگوریتم				بعد از اعمال الگوریتم				درصد کاهش
	PDOP	RMS (متر)	ΔH (متر)	ΔEN (متر)	PDOP	RMS (متر)	ΔH (متر)	ΔEN (متر)	
مجموعه داده اول	۲۱	۴۵۴	۲۹۷	۳۴۳	۳	۶۱	۵۴	۲۹	۸۷
مجموعه داده دوم	۵۱	۵۵۷	۴۱۵	۳۷۰	۲	۶۴	۴۲	۴۹	۸۹
مجموعه داده سوم	۴۳	۴۳۹	۲۰۹	۳۸۷	۳	۴۷	۳۳	۳۶	۸۹
مجموعه داده چهارم	۲۱	۴۷۹	۳۱۳	۳۶۳	۲	۷۳	۶۵	۳۵	۸۵
مجموعه داده پنجم	۱۰۳	۶۶۶	۳۴۶	۵۶۹	۳	۳۷	۱۹	۳۲	۹۵
مجموعه داده ششم	۴۳	۴۹۲	۳۰۱	۳۸۹	۳	۵۳	۴۴	۲۹	۸۹

پیچیدگی روش فیلتر وفقی LMS مبتنی بر الگوریتم Sign-Data به طول فیلتر آن بستگی دارد. همان‌طورکه در ابتدای این بخش بیان شد، برای این تحقیق از فیلتری با طول ۳۱ بهره گرفته‌ایم. باتوجه به طول فیلتر، پیچیدگی روش پیشنهادی از رابطه (۱۳) محاسبه می‌شود:

$$order = 2M + 1 = 2 * 31 + 1 = 63 \qquad (۱۳)$$

در این رابطه، M طول فیلتر مورد استفاده در روش فیلتر وفقی LMS مبتنی بر الگوریتم Sign-Data است. روش LMS پیچیدگی کم‌تری نسبت به روش RLS و فیلتر کالمن در مبحث فیلترهای وفقی دارد. روش RLS[1] پیچیدگی از درجه ۲ دارد. بنابراین یکی از دلایل انتخاب روش LMS برای این تحقیق پیچیدگی کم‌تر این روش است. در این مقاله به علت عدم دسترسی به داده‌ها و پارامترهای نرم‌افزاری الگوریتم‌های مربوطه در مقالات مرتبط با روش‌های دیگر، فقط پیچیدگی روش پیشنهادی محاسبه گردید.

باتوجه به پژوهش‌های اخیر مشخص گردید که گیرنده‌های GPS در برابر انواع حملات فریب کاملا آسیب‌پذیر هستند. با این حال، با پیاده‌سازی روش‌های ضدفریب برای افزایش قدرت گیرنده‌های تجاری GPS می‌توان با فریب مقابله کرد. این مقابله می‌تواند در هر سطحی از بخش‌های پردازش گیرنده اجرا گردد. در جدول (۲)، مقایسه‌ای بین روش‌های پیشین مقابله با فریب و روش پیشنهادی به‌طور کیفی صورت گرفته است. همان‌طورکه از این جدول مشخص است، روش وفقی مبتنی بر الگوریتم Sign-Data نسبت به سه روش دیگر با درصد بیش‌تری اثر فریب را جبران نموده است.

جدول (۲). مقایسه کمی بین روش‌های مقابله با فریب

روش‌های کاهش فریب	محل اعمال روش در گیرنده	متوسط درصد کاهش فریب
فیلتر کالمن [۲۲]	مرحله ناوبری	۴۵
تبدیل موجک [۲۳]	مرحله ناوبری	۶۲/۵
شبکه عصبی بازگشتی [۲۲]	مرحله ناوبری	۶۵
روش ارائه شده در این مقاله	مرحله اکتساب	۸۹

در ادامه این بخش، مقایسه‌ای بین روش‌های دیگر مقابله با فریب و روش پیشنهادی به‌طور کیفی صورت گرفته است. روش RAIM، یک روش ضدفریب در مقابل خطای اندازه‌گیری شبه‌فاصله در گیرنده GPS است. این روش از طریق فرضیه آماری، خطای اندازه‌گیری شبه‌فاصله را آشکار می‌کند و خطای اندازه‌گیری را از مسئله ناوبری حذف می‌نماید. این روش به‌دلیل استفاده از آزمون‌های فرضیه آماری دقت و پیچیدگی بالایی دارد. بنابراین حجم محاسبات بالا از ایرادهای این روش است. درصورتی‌که در رویکرد روش پیشنهادی حجم محاسبات پایین و سرعت اجرا بالا می‌باشد.

روش پردازش فضایی از کارآیی قابل اطمینانی در حذف فریب برخوردار است. این روش به فضای دو یا چندآنتنه‌ای نیاز دارد. به‌طور کلی ایراد این روش افزایش تعداد آنتن‌ها است که با افزایش هزینه، وزن و اندازه گیرنده همراه است. همچنین، مشکل روشی که از پردازش فضایی استفاده می‌کند، الگوریتم زمان‌بر آن است. اما روش پیشنهادی نیاز به هزینه اضافی و افزایش ابعاد ندارد و سرعت اجرای خوبی نسبت به پردازش فضایی دارد.

در روش انتخاب پیک معتبر، عملکرد روش بر پایه تخمین CNR پیک همبستگی سیگنال‌های GPS دریافتی قرار دارد. در اثر وجود فریب، دو پیک همبستگی در سیگنال وجود دارد و از احتمال وجود پیک دیگر در اثر چندمسیری و طراحی ضعیف گیرنده صرف‌نظر شده است. این روش با تعیین حدآستانه و مقایسه CNR سیگنال واقعی و فریب نسبت به حد آستانه قادر به تشخیص پیک معتبر سیگنال واقعی یا سیگنال فریب می‌باشد. پیاده‌سازی این روش ساده است، ولی به علت خطا در انتخاب پیک معتبر باتوجه به حد آستانه در حمله‌های تأخیری کارآیی مطلوبی ندارد. کارآیی روش پیشنهادی این مقاله در برابر حمله‌های تأخیری موفقیت آمیز است و باتوجه به مشخصه همبستگی توانایی تشخیص پیک سیگنال فریب و واقعی را دارد. روش‌های رمزنگاری گیرنده را قادر می‌سازند تا سیگنال‌های معتبر GPS را از سیگنال‌های جعلی با احتمال زیاد تشخیص دهند. روش رمزنگاری NMA یک امضای دیجیتالی عمومی در ساختار انعطاف‌پذیر سیگنال ناوبری تعبیه می‌کند. بنابراین از نظر امنیتی و کارآیی دقت بسیار خوبی دارند. مشکل این روش این است که برای تعبیه امضای دیجیتال به تغییر اساسی در ساختار سیگنال ارسالی از ماهواره نیاز دارند و این عمل فعلا امکان‌پذیر نیست. روش پیشنهادی مبتنی بر LMS نیاز به هیچ‌گونه تغییر ساختاری در سیگنال ندارد و قابلیت اجرای آن وجود دارد. مقایسه کیفی این روش‌ها و روش پیشنهادی در جدول (۳) دسته بندی شده‌است. هر روش در بخش خاصی از گیرنده اعمال می‌گردد که در جدول (۳) برای هر روش مکان اعمال در گیرنده مشخص شده‌است. همان‌طورکه از این جدول ملاحظه می‌شود، کارآیی روش وفقی مبتنی بر الگوریتم Sign-Data باتوجه به پیاده‌سازی آسان، اطمینان و سرعت اجرای بالا نسبت به دیگر روش‌ها برتری قابل توجه دارد.

1 -Recursive Least Squares

جدول (۳). مقایسه کیفی بین روش‌های پیشین و روش پیشنهادی

روش‌های مقابله با فریب	عملکرد روش	محل اعمال روش	مزایا	محدودیت‌ها
RAIM	استخراج شبه‌فاصله	ناوبری	دقت بالا	پیچیدگی محاسباتی و عدم کارآیی در حضور چندمسیری
پردازش فضایی	حذف سیگنال فریب	سیگنال IF ورودی	اطمینان بالا	هزینه بالا و عدم کارآیی در حضور چندمسیری
انتخاب پیک معتبر	ردیابی پیک سیگنال معتبر	اکتساب و ردیابی	پیاده‌سازی آسان	عدم کارآیی در حمله تأخیری
رمزنگاری NMA	امضای دیجیتال پیام ناوبری	داده ناوبری	اطمینان بالا	تغییر در ساختار شکل موج سیگنال GPS
روش ارائه شده در این مقاله	آشکارسازی و حذف سیگنال فریب	اکتساب	اطمینان بالا، سرعت بالای تشخیص و پیاده‌سازی آسان	کارآیی بدون حضور چندمسیری

۷- نتیجه‌گیری

در راه‌کار پیشنهادی برای آشکارسازی فریب در سیگنال دریافتی گیرنده GPS از ویژگی تابع همبستگی بهره گرفتیم. پس از آشکارسازی به‌منظور کاهش اثر فریب در سیگنال دریافتی گیرنده GPS روش فیلتر وفقی LMS براساس الگوریتم Sign-Data مورداستفاده قرارگرفته شده است. شبیه‌سازی بر روی شش مجموعه داده فریب اندازه‌گیری صورت گرفت. روش مورداستفاده به کاهش فریب در هر مجموعه داده منجر گردید. بهترین نتیجه بر مجموعه داده پنجم رخ داد که درصد کاهش خطای RMS در حدود ۹۵ درصد به‌دست آمد. نتایج حاصل نشان می‌دهند که به‌کارگیری روش وفقی براساس الگوریتم Sign-Data به‌طور متوسط مقدار موثر فریب را ۸۹ درصد کاهش می‌دهد. لازم به‌ذکر است علاوه‌بر کاهش فریب، پارامتر PDOP نیز در همه نتایج به‌طور قابل‌توجهی بهبودیافته است که به معنی بهبود صورت فلکی ماهواره‌های شناسایی‌شده است. مقدار PDOP به‌طور میانگین از ۴۷ به ۲/۶۶ کاهش یافته است.

۸- مراجع

[1] F. Shafiee and M. R. Mosavi, "Narrow band Interference Suppression for GPS Navigation using Neural Networks," Journal of GPS Solutions, pp. 1-11, 2015.

[2] H. Azami, M. R. Mosavi, and S. Sanei, "Classification of GPS Satellites using Improved Back Propagation Training Algorithms," International Journal of Wireless Personal Communications, vol. 71, no. 2, pp. 789-803, 2013.

[3] A. Jovanovic, C. Botteron, and P. A. Farine, "Multi-Test Detection and Protection Algorithm against Spoofing Attacks on GNSS Receivers," IEEE Pos., Loc. and Nav. Symp. (PLANS), pp. 1258-1271, 2014.

[4] K. Wesson, M. Rothlisberger, and T. Humphreys, "Practical Cryptographic Civil GPS Signal Authentication," Journal of the Institute of Navigation (JIN), vol. 59, no. 3, pp. 177-193, 2012.

[5] M. R. Azarbad and M. R. Mosavi, "A New Method to Mitigate Multipath Error in Single-Frequency GPS Receiver with Wavelet Transform," Journal of GPS Solutions, vol. 18, no. 2, pp. 189-198, 2014.

[6] M. R. Mosavi, "Comparing DGPS Corrections Prediction using Neural Network, Fuzzy Neural Network and Kalman Filter," Journal of GPS Solutions, vol. 10, no. 2, pp. 97-107, 2006.

[7] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS Spoofer Countermeasure Effectiveness Based on Signal Strength, Noise Power and C/N_0 Observables," International Journal of Satellite Communications and Networking, vol. 30, no. 4, pp. 181-191, 2012.

[8] T. Humphreys, "Detection Strategy for Cryptographic GNSS Anti-Spoofing," IEEE Transactions on Aerospace and Electronic Systems, vol. 49, pp. 1073-1090, 2013.

[9] A. R. Baziar, M. Moazedi, and M. R. Mosavi, "Analysis of Single Frequency GPS Receiver under Delay and Combinig Spoofing Algorithm," Journal of Wireless Personal Communications, vol. 83, no. 3, pp. 1955-1970, 2015.

[10] C. Bonebrake and L. R. O'Neil, "Attacks on GPS Time Reliability," IEEE Transactions on Security & Privacy, vol. 12, no. 3, pp. 82-85, 2014.

[11] 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 (IJNO), pp. 1-16, 2012.

[12] A. M. Mitelman, "Signal Quality Monitoring for GPS Augmentation Systems," Ph.D. Thesis, Department of Electrical Engineering, Stanford University, California, 2004.

[13] A. Cavaleri, M. Pini, L. Lo Presti, and M. Fantino, "Signal Quality Monitoring Applied to Spoofing Detection," the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS), pp. 1-9, 2011.

[14] D. P. Shepard and T. E. Humphreys, "Characterization of Receiver Response to Spoofing Attacks," GPS World, vol. 21, no. 9, pp. 27-33, 2010.

[15] J. Nielsen, V. Dehghanian, and G. Lachapelle, "Effectiveness of GNSS Spoofing Countermeasure based on Receiver CNR Measurements," International Journal of Navigation and Observation (IJNO), pp. 1-9, 2012.

[16] A. R. Bazyar, M. Moazedi, M. R. Mosavi, and S. Z. Ghaffari, "A Novel Technique for GPS Spoofing Detection based on Pseudo-range Measurements in order to Protection of Marine Navigation Systems," Iranian Journal of Marine Technologies, vol. 1, no.2, pp. 1-13, 2013. (in Persian)

[17] L. Scott, "Anti-Spoofing and Authenticated Signal Architectures for Civil Navigation Systems," 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS), 2003.

[18] A. J. Jahromi, T. Lin, A. Broumandan, J. Nielsen, and G. Lachapelle, "Detection and Mitigation of Spoofing Attacks on a Vector-Based Tracking GPS Receiver," International Technical Meeting of the Institute of Navigation (ION GNSS), pp. 3-8, 2012.

[19] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandan, and G. Lachapelle, "A Low Complexity GNSS Spoofing Mitigation Technique using a Double Antenna Array," GPS World Magazine, vol. 22, no. 12, pp. 44-46, 2011.

[20] L. Ge, Sh. Han, and Ch. Rizos, "Multipath Mitigation of Continuous GPS Measurements using an Adaptive Filter," Journal of GPS Solutions, vol. 4, no. 2, pp. 19-30, 2000.

[21] B. Farhang Boroujeny, "Adaptive Filters Theory and Applications," University of Utah USA, 2013.

[22] M. R. Mosavi, M. J. Rezaei, N. Hosseinzadeh, and R. A. Kiaamiri, "New Intellogent Methods for Detection and Mitigation of Spoofing Signal in GPS Receivers," Journal of Electronics and Cyber Defense, vol. 2, no. 1, pp. 71-81, 2014. (in Persian)

[23] M. R. Mosavi, A. Bazyar, and M. Moazedi, "A New Wavelet based Method for Reduction of Spoofing Effect on Single-Frequency GPS Receivers," Journal of Soft Computing and Information Technology, vol. 3, no. 3, pp. 59-68, 2014. (in Persian)

Journal Of Electronical & Cyber Defence
Vol. 3, No. 4, 2016, Serial No.12

Defense Against Spoofing in GPS Receiver using Correlation and Least Mean Squares Method Based on Sign-Data Algorithm

Z. Shokhmzan, M. R. Mosavi*

*Iran University of Science and Technology

(Received: 19/03/2015, Accepted: 12/01/2016)

ABSTRACT

Among the variety of GPS signal interference, spoofing is considered as the most dangerous intentional interference. If spoofing signal would have existed in the received signal GPS, wrong information reaches the receiver which causes problems in time and location computation of the receiver. Defense against spoofing includes the spoofing detection and reduction. In this paper, we use the properties of correlation function for spoofing detection. In order to mitigate spoofing, we apply the method of Least Mean Squares (LMS) based on sign-data algorithm. This approach reduces effect of the spoofing interference in the received signal GPS and defends against interference of kind of delay spoofing. The proposed approach have been implemented on real dataset and in the acquisition stage from GPS receiver processing. The results show that the adaptive method based on sign-data algorithm decrease effectiveness of spoofing on average 89 percent. In addition to spoofing reduction, the Position Dilution of Precision (PDOP) parameter improves at all of results. PDOP parameter indicates the spatial position of identified satellites. The PDOP value mitigated from 47 to 2.66 on average.

Keywords: GPS Spoofing, Detection, Mitigation, Correlation, LMS and Sign-Data Algorithm.

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