مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
سال ششم، شماره ۳، پاییز ۱۳۹۷، ص ۸۰-۶۵

کاهش خطای فریب GPS با استفاده از تخمین‌گر تطبیقی در حلقه ردیابی

مریم معاضدی[۱]، سید محمدرضاموسوی میرکلایی[۲*]، زهرا نصرپویا[۳]، علی صدر[٤]

۱- دانشجوی دکتری، ۲- استاد، ۳- دانشجوی کارشناسی‌ارشد، ٤- دانشیار، دانشکده مهندسی برق، دانشگاه علم و صنعت ایران

(دریافت: ۹۶/۰۵/۲۷، پذیرش: ۹۶/۱۲/۰٤)

چکیده

یکی از عوامل ایجاد خطا در ردیابی گیرنده‌های GPS حملاتی نظیر فریب است. هدف از این حملات، محاسبه نادرست مکان و زمان است. فریبنده با ارسال سیگنال جعلی باعث ایجاد فریب می‌شود که به شکل‌های مختلفی تولید می‌گردد. در این مقاله، تداخل مورد بررسی از نوع فریب تأخیری است. در واقع، هدف ارائه روشی جدید در قسمت ردیابی سیگنال GPS است که به‌واسطه آن بتوان تأثیر فریب ایجادشده را کاهش داد. الگوریتم پیشنهادی دو بخش اصلی دارد. بخش نخست شامل تخمین میزان تأخیر فریب است. پس از آن با یک روش ابتکاری تأثیر سیگنال فریب در بخش همبسته‌ساز حلقه ردیابی استخراج و از کل سیگنال ورودی کاسته می‌گردد. بدین ترتیب که ابتدا میزان تأثیر فریب تخمین زده شود و سیگنال فریب تخمینی به‌دست آید. برای این منظور، دو تخمین‌گر برپایه همبسته‌ساز چندگانه و تطبیقی ارائه شده است. همبستگی این سیگنال و سیگنال دیجیتالی IF محاسبه شده و وارد بخش کاهش فریب می‌گردند. در بخش کاهش فریب، همبستگی سیگنال به‌دست‌آمده با خودهمبستگی سیگنال دریافتی جمع شده و همبستگی سیگنال GPS معتبر استخراج می‌گردد. این روش پیاده‌سازی راحتی داشته و در عین حال ابزاری مطمئن برای مقابله با فریب است. پس از اعمال الگوریتم پیشنهادی، خطای ردیابی سیگنال به‌طور میانگین حدود ۸۸ ٪ کاهش می‌یابد.

واژگان کلیدی: گیرنده GPS، حمله فریب، حلقه قفل تأخیر، همبسته‌ساز باند باریک

۱- مقدمه

امروزه تعداد کاربردهای بی‌سیم براساس سیگنال‌های GPS برای همزمان‌سازی، ناوبری و موقعیت‌یابی افزایش یافته است؛ متأسفانه سیگنال‌های GPS غیرنظامی مستعد پذیرش تداخل هستند. به‌طورکلی، تداخل عمدی سیگنال‌های GPS به دو بخش جمینگ و فریب تقسیم‌بندی می‌شود [۱]. فریب GPS براساس فرستادن یک سیگنال جعلی GPS که توسط شبیه‌سازی از روی سیگنال اصلی است، ایجاد می‌گردد. فریبنده‌های GPS برای ساختن سیگنال‌های غلط GPS ساخته می‌شوند تا گیرنده‌ها را فریب داده، خطای مکانی و زمانی ایجاد کرده و سیستم‌های مخابراتی و ناوبری را مختل نمایند [۲].

GPS ابزاری عمومی برای مکان‌یابی فضایی است که دقت کافی و اطلاعات پیوسته برای استفاده در کاربردهای مهم ناوبری مانند سیستم توزیع برق، حمل و نقل کامیون‌ها، کشتی‌ها و هواپیماها فراهم می‌کند. در سال ۲۰۰۱ میلادی، وزارت حمل و نقل ایالات متحده، آسیب‌پذیری زیرساخت‌های حمل‌ونقل خود را نسبت به اختلال در سیگنال‌های GPS غیرنظامی تشخیص داد. در گزارش آن‌ها که به‌عنوان گزارش Volpe شناخته می‌شود، هشدار داده شد از آن‌جایی‌که GPS در زیرساخت‌های غیرنظامی نفوذ پیدا کرده است، بنابراین، تبدیل به یک هدف وسوسه‌انگیز شده و می‌تواند توسط افراد، گروه‌ها یا کشورها مورد سوءاستفاده قرار گیرد. در دهه اخیر، حمله فریب به‌عنوان خطرناک‌ترین دخالت عمدی در GPS شناخته شده است. همه گیرنده‌های GPS شهری که در دسترس عموم هستند، نسبت به فریب بی‌توجه می‌باشند. در سطح زمین یک اختلال کم‌توان نیز می‌تواند به‌راحتی یک گیرنده GPS تجاری را در شعاع چندکیلومتری فریب دهد. در سال‌های اخیر، با توجه به پیشرفت‌های سریع در فناوری SDR، نرم‌افزار گیرنده- فریبنده بسیار عملی‌تر و کم‌هزینه‌تر پیاده‌سازی می‌شود. بنابراین، فریب و اقدامات متقابل مربوط به آن بسیار مورد توجه قرار گرفت و چندین مقاله در روش‌های آشکارسازی و کاهش فریب در مقالات اخیر منتشر شد.

* رایانامه نویسنده مسئول: M_Mosavi@iust.ac.ir

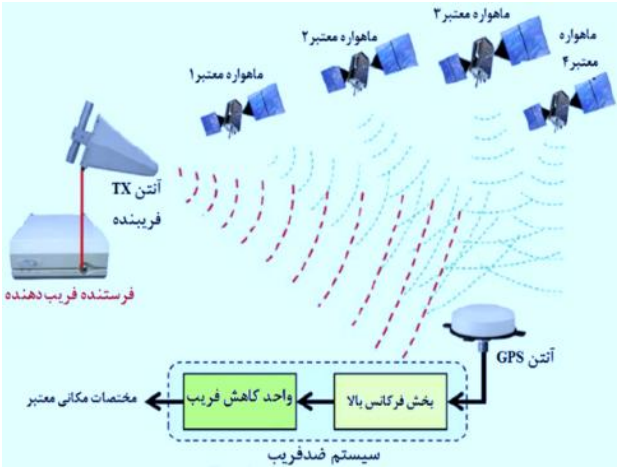
حمله فریب به سه دسته عمده ساده، متوسط و پیچیده تقسیم می‌شود که در این‌جا حمله متوسط مورد بررسی قرار می‌گیرد. در این نوع حمله سیگنال اصلی GPS تأخیر یافته و ذخیره شده و با سیگنال اصلی جمع و سپس برای گیرنده هدف ارسال می‌گردد [۲]. این نوع حمله باعث گمراهی گیرنده شده و آن‌را در ردیابی سیگنال اصلی GPS دچار خطا می‌کند. بنابراین، نیازمند روشی برای کاهش خطای ناشی از این حمله هستیم. قدم نخست در این مسیر شناسایی فریب و به عبارتی تشخیص وجود سیگنال فریب است. مرحله بعد که قدم اصلی نیز است، جبران‌سازی یا کاهش آن است. شکل (۱) یک سیستم ضدفریب را در حالت کلی نشان می‌دهد.

در ادامه این مقاله ابتدا به بررسی روش‌های کاهش فریب می‌پردازیم. در این بخش تا حد ممکن سعی شده است که ترتیب ارائه مطالب متناسب با ترتیب مطرح‌شدن روش‌ها باشد تا روند بهبود و تکامل روش‌های کاهش فریب توسط خواننده به‌طور مشهودی درک گردد. در بخش سوم آثار حمله فریب در حلقه ردیابی مورد بررسی قرار می‌گیرد. بخش چهارم به راه‌کار پیشنهادی که استفاده از همبسته‌ساز باند باریک است اختصاص دارد. در نهایت، نتایج بر روی داده‌های آزمایشگاهی و داده‌های واقعی در بخش ردیابی سیگنال GPS بیان می‌گردند.

۲- مروری بر روش‌های مقابله با فریب

برای کاهش فریب، مطالعات گسترده‌ای در حال انجام بوده و روش‌های متنوعی برای مقابله با آن ارائه و نمونه‌های عملی آن ساخته شده است [۳-۹]. بخشی از روش‌های موجود برای مقابله با فریب که در ابتدای تحقیقات مورد توجه واقع شدند، بر مبنای مقایسه و بررسی مداوم اطلاعات داخلی و خارجی و تخمین سیگنال معتبر در صورت تشخیص وجود حمله، عمل می‌کنند [۱۰]. اطلاعات داخلی مربوط به داده‌هایی است که از GPS دریافت می‌شود و اطلاعات خارجی داده‌هایی هستند که از دیگر سیستم‌های ناوبری حاصل می‌شوند. استفاده از این روش نیاز به وسایل اندازه‌گیری اضافه بر گیرنده GPS دارد.

روش دیگر، پردازش فضایی سیگنال‌های ورودی است. به‌دلیل محدودیت‌های عملی، معمولاً فرستنده‌های فریب (به‌جز فریبنده‌های ماهر) چندین سیگنال جعلی را از یک آنتن می‌فرستند، درحالی‌که سیگنال‌های معتبر GPS از ماهواره‌های مختلف در مسیرهای گوناگون فرستاده می‌شوند.



شکل (۱): شمای کلی یک سیستم ضدفریب [۲].

ازاین‌رو، می‌توان روش پردازش فضایی را برای تخمین اثر سه‌بعدی سیگنال‌های دریافتی و تفکیک این سیگنال‌ها که رابطه فضایی مشخصی دارند، به‌کار گرفت [۱۱-۱۵]. این روش پیچیدگی سخت‌افزاری بالایی دارد، درحالی‌که برای فریب‌های پیچیده جواب‌گو نیست.

شپارد[۱] نشان داد که تداخل بین پیک همبستگی سیگنال اصلی و سیگنال فریب بسیار شبیه به تداخل چندمسیری و مسیر مستقیم است [۱۶]. بنابراین، روش‌های آشکارسازی و کاهش چندمسیری می‌تواند برای فریب نیز مورد استفاده قرار گیرد. نظارت بر کیفیت سیگنال (SQM[۲]) یک روش آشکارسازی چندمسیری است که برای آشکارسازی حملات فریب بر روی گیرنده‌های ردیابی به‌کار برده شده است [۱۷]. لدوینیا[۳] در سال ۲۰۱۰ میلادی، نرخ و اختلاف آزمون‌های SQM برای آشکارسازی فریب را به‌کار گرفت. سپس، روش بررسی صحت استقلال گیرنده (RAIM)[۴] را برای آشکارسازی و کاهش فریب در سطح ناوبری و مسائل مکان‌یابی را ارایه داد [۱۸]. این روش‌ها توانایی تفکیک چندمسیری و فریب را ندارند.

آشکارسازی و کاهش حملات فریب بر روی گیرنده‌های GPS ردیابی یکی از مهم‌ترین روش‌های ضدفریب محسوب می‌شود که برای گیرنده‌های ردیابی بردار پایه GPS طراحی شده است [۱۹]. یک گیرنده VB زنجیره‌ای می‌تواند سطح ناوبری و اندازه‌گیری‌های حلقه‌های ردیابی را برای راه‌اندازی NCO هر PRN جمع کند. ساختار کاهش فریب باید اندازه‌گیری‌های محلی را که از

۱- Shepard
2- Signal Quality Monitoring
۳- Ledvina
4- Receiver Autonomous Integrity Monitoring

فیلترهای حلقه ردیابی می‌آید، نادیده بگیرد و از اندازه‌گیری‌های سطح ناوبری برای راه‌اندازی NCOها استفاده کند. این حالت باقی می‌ماند تا زمانی‌که بیشینه همبستگی فریب دور شود و همبسته‌ساز به فرآیند ردیابی سیگنال اصلی بازگردد. این گیرنده علاوه‌بر پیچیدگی بالا نیاز به تغییر سخت‌افزار گیرنده دارد که هزینه بالایی دارد.

قاعده ابتکاری انتخاب پیک معتبر بر پایه اندازه‌گیری CNR نیز در رابطه با کاهش فریب به‌کار گرفته شده است [۲۰]. در این روش بررسی C/No با یک قاعده تصمیم‌گیری ادغام شده است. فریبنده آفست داپلر سیگنال‌های جعلی را تطبیق می‌دهد و فاز کد را به‌نحوی تنظیم می‌نماید که بر ناحیه هدف منطبق باشد. مرز ناحیه هدف دقیقاً مشخص نیست، اما تأثیر فریب خارج از آن به شدت افت می‌کند. این روش علاوه‌بر پیچیدگی بالا برای دیگر أنواع فریب پاسخ مناسب ندارد.

ملاحظه می‌شود که با روش‌های موجود امکان مقابله مطمئن و کم هزینه با حمله فریب وجود ندارد. از این‌رو نیاز به یک روش ساده و در عین حال هزینه پایین به‌شدت احساس می‌شود. روش پیشنهادی در این مقاله با الگوریتم تطبیقی و بدون تغییر در ساختار گیرنده GPS و صرفاً ارتقاء نرم‌افزاری در حلقه ردیابی توانسته تا حدی زیادی اثر حمله فریب را کاهش دهد. پس از معرفی کامل‌تر راه‌کار پیشنهادی در بخش بعدی، مقایسه جامعی با روش‌های پیشین در بخش ۵ انجام خواهد شد.

۳- مدل‌سازی تداخل در حلقه ردیابی

مطالعه روش‌های چندمسیری و روش‌های کاهش این آثار در ارتباطات و سیستم‌های ناوبری، به‌طور خاص سیستم‌های دسترسی چندگانه تقسیم کد، یک راه طبیعی برای مدل کردن تداخل‌های GPS فراهم می‌کند. چندمسیری معمولاً در ناحیه تابع همبستگی مختلط مدل می‌شود که این ناحیه مناسب مدل کردن فریب نیز است. اگر کل سیگنال ورودی در گیرنده همبسته شود، یک تابع همبستگی مختلط x در زمان t و تأخیر آفست مانند معادله (۱) ایجاد می‌گردد که درآن $x(t,\zeta)$ برهم نهی ۴ جزء همبستگی مختلط، x_d مسیر مستقیم GPS، x_m جزء چندمسیری، x_s جزء فریب و n نویز سفید گوسی اضافه شده است. در واقع جزء مسیر مستقیم تابع همبستگی مختلط نظیر سیگنال GPS اصلی است. این تابع در هنگام حضور چندمسیری به سیگنال مسیر مستقیم و در هنگام حضور فریب به سیگنال اصلی مربوط است. در این‌جا مسیر مستقیم و اصلی معادل درنظر گرفته شده‌اند. تابع همبستگی مختلط $x(t,\zeta)$ با زمان t و تأخیر آفست ζ، وقتی تولید می‌شود که گیرنده کپی کد منتشرشده شبه‌تصادفی را با سیگنال منتشرشده ورودی همبسته نماید. حلقه قفل تأخیر با سه جزء همبستگی مختلط (اولیه، میانی و نهایی) برای تعقیب سیگنال بر روی این تابع اجرا می‌شود، اگرچه بعضی گیرنده‌ها جزءهای همبستگی بیشتری تولید می‌کنند. تعداد بیشتر این جزءهای همبستگی پیش‌بینی بهتری بر روی میزان خرابی ناحیه تابع همبستگی مختلط نسبت به اولیه، میانی و نهایی به‌تنهایی عرضه می‌کنند. وقتی‌که زنجیره‌ای از تأخیر جزءهای همبستگی موجود است، ناحیه تابع همبستگی مختلط می‌تواند به‌عنوان سیگنال پیوسته زمان درنظر گرفته شود. جزء همبستگی مختلط مسیر مستقیم $x_d(t,\zeta)$ می‌تواند به‌صورت معادله (۲) مدل گردد.

$$x(t,\zeta)=x_d(t,\zeta)+x_m(t,\zeta)+x_s(t,\zeta)+n(t,\zeta) \quad (۱)$$

$$x_d(t,\zeta) = \alpha_d(t)R(\zeta - \zeta_d(t))e^{j\theta_d(t)} \quad (۲)$$

این معادله نشان می‌دهد $x_d(t,\zeta)$ یک انتقال‌یافته زمانی، مقیاس‌بندی‌شده ناحیه و اصلاح‌شده فاز تابع همبستگی مختلط $R(\zeta)$ است که در آن، $0\le \alpha_d(t)\le 1$ فاکتور مقیاس‌بندی، $\zeta_d(t)$ تأخیر ثانیه‌ها و فاز برحسب رادیان است که همگی متغیر با زمان هستند. اگر گیرنده فقط یک سیگنال مسیر مستقیم را تعقیب کند، حلقه قفل تأخیر و حلقه قفل فاز به ترتیب سعی کرده‌اند $\theta_d(t)$ و $\zeta_d(t)$ را مساوی صفر قرار دهند که در این مورد مناسب‌تر است $\alpha_d(t)=1$ باشد. تابع خودهمبسته $R(\zeta)$ به‌صورت معادله (۳) مدل می‌شود:

$$R(\zeta)\approx\begin{cases}1-\dfrac{|\zeta|}{T_C} & ;|\zeta|<T_C\\ 0 & ;\text{otherwise}\end{cases} \quad (۳)$$

که در آن، $T_c \approx 1\ \mu s$ است و سرعت تراشه سیگنال GPS L1 C/A را تخمین می‌زند. در عمل $R(\zeta)$ برای هر کد منتشرشده شبه‌تصادفی در هر ماهواره کمی تغییر می‌کند. این تغییر تأثیری بر مدل ندارد و بنابراین، معادله (۳) یک تقریب منطقی است. چندمسیری در ناحیه همبستگی مختلط $x_m(t,\zeta)$ می‌تواند به‌عنوان انطباق تأخیر بعضی سیگنال‌های مسیر مستقیم مدل شود.

$$x_m(t,\zeta)=\sum_{k=1}^{N}\alpha_{m,k}(t)\,R(\zeta-\zeta_{m,k}(t))e^{j\theta_{m,k}(t)} \quad (۴)$$

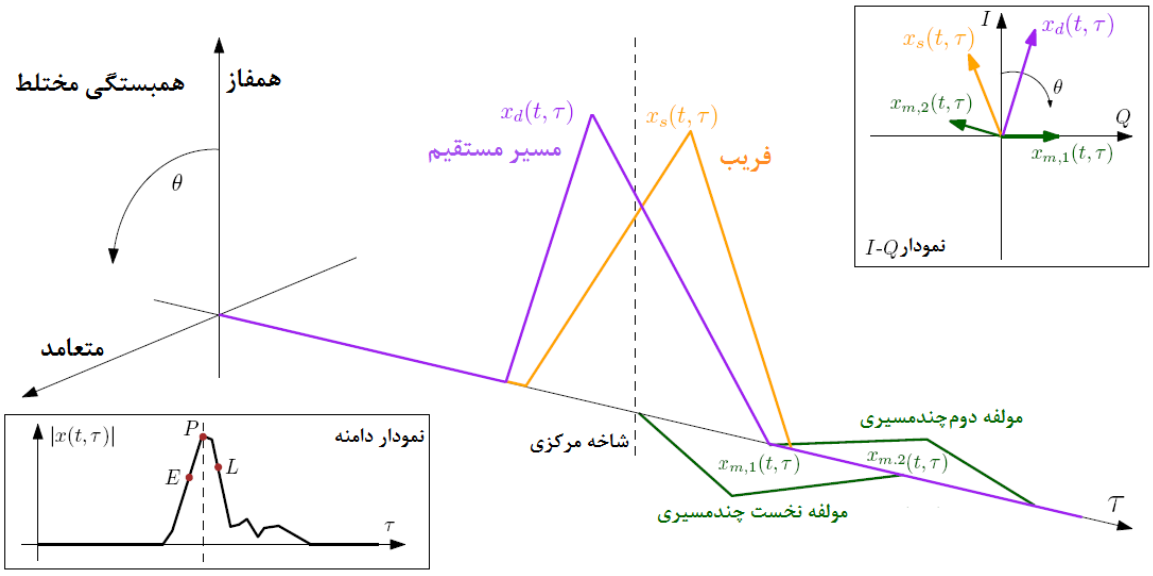
اگر سیگنال چندمسیری وجود نداشته باشد، N=0 است. چون سیگنال‌های چندمسیری، کپی سیگنال‌های مسیر مستقیم با تأخیر هستند، بنابراین $\zeta_{m,k}(t)>0$ است. به این ترتیب می‌توان نتیجه گرفت که به‌دلیل $0\le \alpha_{m,k}(t)\le \alpha_d(t)$ سیگنال چندمسیری نسبت به سیگنال مسیر مستقیم تضعیف می‌شود. هرچند در

برخی موارد سیگنال مسیر مستقیم می‌تواند بیشتر از سیگنال‌های بازگشتی چندمسیری تضعیف شوند. مدل سیگنال فریب $x_s(t,\zeta)$ در ناحیه تابع همبستگی مختلط به‌صورت معادله (۵) است:

$$x_s(t,\zeta)=(\alpha_s(t)R(\zeta-\zeta(t))e^{j\theta_s(t)})\times I_{spoofing} \quad (۵)$$

معادله فوق یک احساس شهودی ایجاد می‌کند، چون اگر فریبنده سعی کند گیرنده قربانی را با سیگنال جعلی که یک کپی خیلی نزدیک سیگنال GPS است، فریب دهد، باید $x_s(t,\zeta)$ تقریباً با $x_d(t,\zeta)$ برابر باشد. این تنها تفاوت قابل توجه در این مدل شاخص $1_{spoofing}$ است که مشخص می‌نماید فریب اتفاق افتاده است یا خیر؟ قابل توجه است که در این حالت، مورد چندفریبی درنظر گرفته نشده است [۲۰].

شکل (۲) یک مثال بدون نویز را که یک حمله فریب در حضور چندمسیری است، نشان می‌دهد. اگرچه شکل، حملات فریب پیچیده یا محیط چالش‌برانگیز چندمسیری نشان داده نشده، ولی یک مثال محتمل است.



شکل (۲): ناحیه همبستگی مختلط یک حمله فریب، نمودار I-Q نظیر و اندازه.

فریبنده یک سیگنال جعلی $x_s(t,\zeta)$ با یک دامنه کاهش یافته و کمی تأخیر در $x_d(t,\zeta)$ را ارسال می‌کند. تطبیق فاز حامل سیگنال فریب و اصلی برای فریبنده دشوار است. بنابراین، شکل (۲) موردی را نشان می‌دهد که $\theta_d(t)\neq\theta_s(t)$ است و در قسمت سمت راست بالا (شکل I-Q) نشان داده شده است. با وجود اینکه دو جزء چندمسیری وجود دارد، اندازه آن‌ها به‌طور قابل توجهی نسبت به $a_d(t)$ کاهش یافته و تأخیرشان زیاد است. در این شکل، فاز چندمسیری تقریباً عمود بر فاز $x_d(t,\zeta)$ است.

از آن‌جا که $\theta_{m,k}(t)$ می‌چرخد، وقتی ماهواره‌ها به دور مدار خود در گردش هستند، سرعت چندمسیری نسبت به مسیر مستقیم تغییر می‌کند. قسمت پایین سمت چپ شکل دامنه، نشان می‌دهد که $|x(t,\zeta)|$ بزرگتر از تابع خود همبسته ایده‌آل $R(\zeta)$ نیست. سه نقطه در شکل اندازه جزءهای همبستگی اولیه، میانی و نهایی هستند که معمولاً گیرنده برای دنبال‌کردن سیگنال به‌کار می‌برد. با این سه جزء همبستگی، گیرنده GPS نمی‌تواند به‌اندازه کافی خرابی در دامنه نشان داده‌شده در شکل را درست کند. برای VSD[1] قوی‌تر جزءهای همبستگی بیشتری نیاز است.

تخریب ناحیه تابع همبستگی مختلط همچنین می‌تواند در مولفه در فاز $I(t,\zeta)=\Re[x(t,\zeta)]$ و مربع $Q(t,\zeta)=\Im[x(t,\zeta)]$ از اجزاء $x(t,\zeta)$ مشاهده شود. وقتی که فریب، چندمسیری و نویز نداریم $I(t,\zeta)=R(\zeta)$ و $Q(t,\zeta)=0$، اما وقتی فریب، چندمسیری و نویز درنظر گرفته می‌شوند، $I(t,\zeta)$ و $Q(t,\zeta)$ تغییر می‌کنند.

شکل (۳) همان سناریو شکل (۲) است با این تفاوت که اجزاء چندمسیری حذف شده‌اند و فقط اجزاء مسیر مستقیم و فریب درنظر گرفته شده‌اند که در این‌جا $I(t,\zeta)$ با $R(\zeta)$ برابر نیست و نیز $Q(t,\zeta)\neq0$ است. تخریب وابسته به تأخیر به‌دلیل تخریب فاز وابسته به تأخیر است که توسط سیگنال فریب با فاز غیرحامل تطبیق داده‌شده، ایجاد گردیده است. برای مثال، در جزء همبستگی $\pm T_c/2$، $x_s(t,\zeta)$ اضافه‌شده در شکل‌دهی $Q(t,\zeta)$ نقش دارد. اما چون سیگنال فریب فاز حامل آن منطبق نشده است، تخریب در $Q(t,\zeta)$

1-Vestigal Signal Detection

ثابت نیست (به این معنا که انحراف آن با $R(\zeta)$ تغییر می‌کند). به‌علت $\theta_s(t)\neq\theta_d(t)$ و $\zeta_s(t)\neq\zeta_d(t)$، تابع همبستگی مختلط $R(\zeta)$، خطا در جزء توان ۲ تابع $\zeta_s(t)$ را افزایش یا کاهش می‌دهد. تخریب در $I(t,\zeta)$ به هر دو دلیل اتفاق می‌افتد.

از آن‌جایی‌که شکل (۳) یک حمله فریب را نشان می‌دهد، می‌توان چنین درنظر گرفت که در آن، $x_s(t,\zeta)$ با یک جزء قوی چندمسیری $x_{m,1}(t,\zeta)$ جایگزین شده است. در این مورد، تخریب یکسانی در $I(t,\zeta)$ و $Q(t,\zeta)$ وجود دارد. بنابراین، نوع تخریب نشان داده شده در شکل (۳)، یک فریب منحصربه‌فرد نیست. برای مخابره موفقیت‌آمیز داده‌های ناوبری باید نسخه‌های محلی کد و فاز به‌صورت دقیق تولید شوند که این امر وابسته به حلقه قفل تأخیر[1] (DLL) است.

هدف DLL، ردیابی فاز کد از یک کد خاص در سیگنال است. خروجی این حلقه کاملاً بر نسخه محلی کد C/A تطبیق دارد. حلقه ردیابی کد در گیرنده GPS برعهده DLL است که حلقه ردیابی اولیه- نهایی نامیده می‌شود. سیگنال ورودی با سه عدد تکرار محلی کد میانی، اولیه و نهایی با فاصله چیپ‌های دقیق از هم تفکیک شده‌اند. ایده این حلقه آن است که پاسخ عبور از صفر تفکیک‌کننده را ردیابی کند. در حضور حمله فریب (فرض‌شده فقط یک سیگنال فریب داریم)، سیگنال دریافتی به‌صورت معادله (۶) است:

$$s(t)=A_0.d(t-\zeta_0).cf(t-\zeta_0)cos(2\pi ft-\theta_0)+A_1.d(t-\zeta_1).cf(t-\zeta_1)cos(2\pi ft-\theta_1)+b(t) \quad (۶)$$

با دریافت پاسخ تفکیک‌گر سیگنال ترکیبی خطای ردیابی خروجی تفکیک‌گر اولیه- نهایی ناشی از فریب در DLL را نشان می‌دهد (مطابق شکل (۴)) [۲۱]. مشاهده می‌شود که مقدار عبور از صفر تفکیک‌کننده، انتقال پیدا کرده است که موجب ایجاد خطا در تخمین تأخیر کد می‌شود.

۴- الگوریتم پیشنهادی تخمین و حذف فریب در حلقه ردیابی

شکل (۵) بلوک دیاگرام راه‌کار نوین پیشنهادی به‌منظور کاهش فریب را نشان می‌دهد. ابتدا سیگنال اصلی و فریب از طریق آنتن گیرنده دریافت و در قسمت گیرنده RF پردازش شده و سپس وارد بلوک A/D می‌گردد. در این مرحله سیگنال آنالوگ ورودی به حوزه دیجیتال تبدیل و وارد قسمت ردیابی می‌شود. از طرف دیگر، خروجی PLL و DLL در هم ضرب و وارد بلوک تخمین‌گر فریب می‌گردند. در این بلوک پس از تخمین میزان تأخیر ζ، سیگنال فریب تخمین زده شده به‌دست می‌آید. سپس همبستگی این سیگنال و سیگنال ورودی دیجیتالی IF محاسبه شده و در نهایت به بخش کاهش فریب می‌رود. در این بخش سیگنال به‌دست آمده با خودهمبستگی سیگنال دریافتی جمع می‌گردد.

درحضور سیگنال اصلی و فریب می‌توان سیگنال دریافتی را مدل کرد [۲۲]. اگر سیگنال IF دریافتی را به‌صورت معادله (۷) نشان دهیم، معادله (۸) به‌ترتیب قسمت هم‌فاز و متعامد این سیگنال را نشان می‌دهد.

$$S_r(t)=\sum_{k=1}^{N_{Sat}}\sum_{m=1}^{N_k}\alpha_{km}.c(t-\tau_k-\Delta\tau_{km}).e^{j(\varepsilon_{\theta\lambda m}+\theta_{\lambda m})}+n(t) \quad (۷)$$

$$I(j)=\sum_{m=0}^{N}\alpha_m K_c(\varepsilon_r-\Delta\tau_m+d\tau_j)\cos(\varepsilon_\theta+\Delta\theta_m)+n_I,$$
$$Q(j)=\sum_{m=0}^{N}\alpha_m K_c(\varepsilon_r-\Delta\tau_m+d\tau_j)\sin(\varepsilon_\theta+\Delta\theta_m)+n_q \quad (۸)$$

اشکال (۶) و (۷) مقایسه نتایج حاصل از ردیابی سیگنال اصلی و فریب را نشان می‌دهد. همان‌طور که مشاهده می‌شود پس از ایجاد فریب، دامنه نمودار بخش هم‌فاز سیگنال افزایش و دامنه نمودار بخش متعامد کاهش یافته است. خطای ایجادشده در I و Q باعث ایجاد خطای کد و فاز و در نتیجه خطای ردیابی شده و گیرنده را در موقعیت‌یابی صحیح فریب می‌دهد.

سیگنال دریافتی در قسمت RF فیلتر می‌شود و پس از تبدیل به باند پایه، سیگنال IF حاصل می‌گردد. سپس نمونه‌برداری و کوانتیزه می‌شود. سیگنال IF دیجیتالی برابر مجموع سیگنال اصلی GPS سیگنال فریب و نویز است. مدل سیگنال اصلی GPS در خروجی تبدیل‌کننده A/D به‌صورت معادله (۹) درمی‌آید که در آن، A_0 دامنه سیگنال اصلی GPS، $P(n-\zeta 0)$ کد طیف گسترده با تأخیر ζ_0، w_0 فرکانس زاویه‌ای و ϕ_0 فاز حامل است. بنابراین، مجموع سیگنال اصلی GPS و سیگنال فریب به‌صورت معادله (۱۰) بیان می‌گردد.

$$y_0(n)=A_0P(n-\zeta_0)\cos(w_0n+\phi_0) \quad (۹)$$

$$y(n)=\sum_{i=0}^{m}A_mP(n-\zeta_i)\cos(w_in+\phi_i) \quad (۱۰)$$

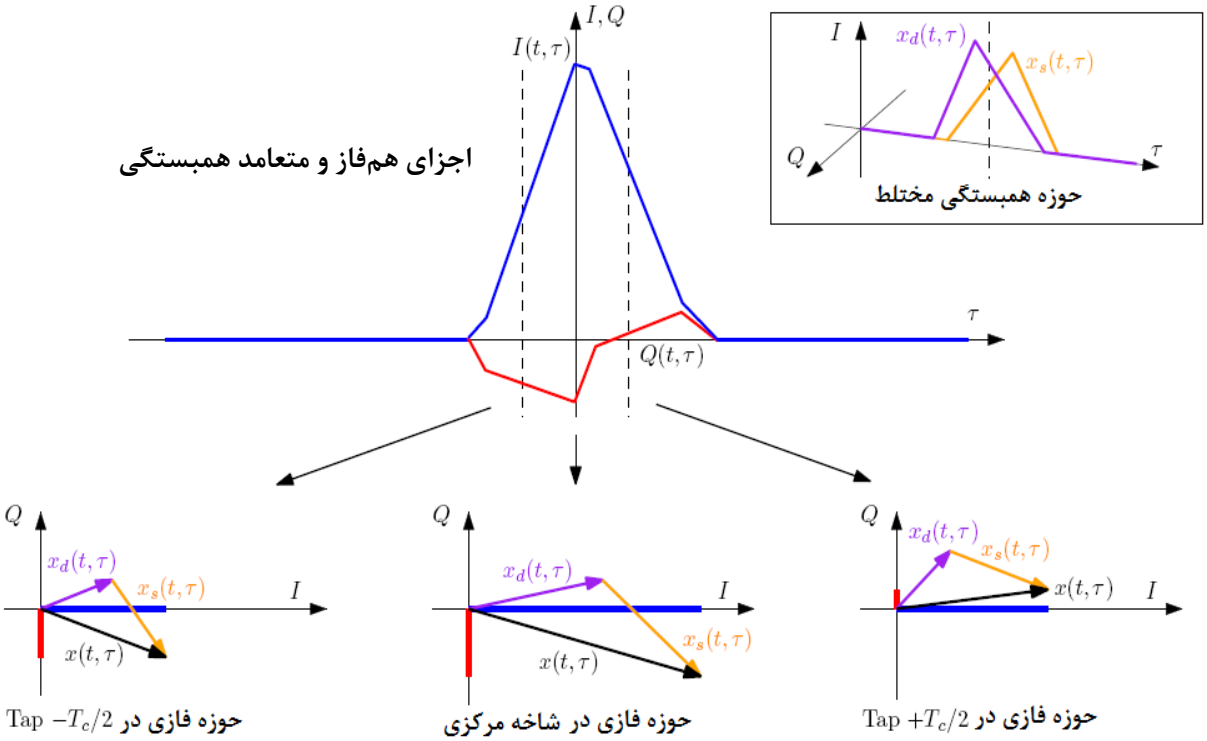
در این معادله، M=۱ بیان‌گر سیگنال فریب است. A_1، ϕ_1 و ζ_1 بیان‌گر دامنه، فاز حامل و تأخیر کد سیگنال فریب است. بنابراین، به‌عنوان سیگنال دریافتی واقعی GPS بعد از اضافه کردن نویز در تبدیل‌کننده A/D داریم:

$$y(n)=\sum_{i=0}^{m}A_mP(n-\zeta_i)\cos(w_in+\phi_i)+\eta(n) \quad (۱۱)$$

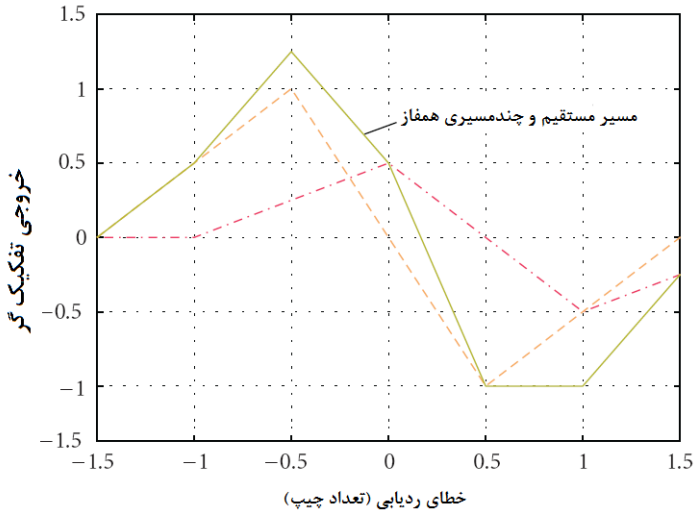
که در آن، $\eta(n)$ نویز سفید با میانگین صفر است. شکل (۸) تابع همبستگی نرمال‌شده با حضور فریب تأخیری را نشان می‌دهد.

1- Delay Locked Loop

همان‌گونه که مشاهده می‌گردد تقارن بخش‌های هم‌فاز و متعامد از بین رفته و تخمین تأخیر زمانی مشکل است. همین تـأخیر زمـانی خطای حلقه DLL و در نتیجه موقعیت‌یابی را موجب می‌گردد.



شکل (۳): شکل تخریبی که می‌تواند در I و Q تابع x(t,ζ) در حین یک حمله فریب وجود داشته باشد.



شکل (۴): خطای ردیابی خروجی تفکیک‌کننده اولیه- نهایی ناشی از فریب در DLL.

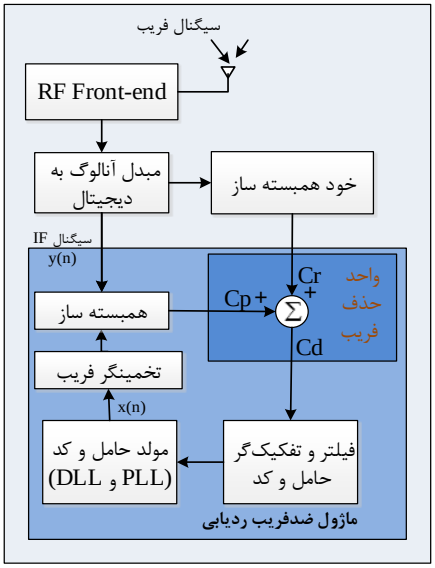
برای بررسی صحت راه‌کار پیشنهادی دو نوع سیگنال ایسـتا و دینامیک استفاده می‌شود که داده ایستا برای کاربردهـای زمـانی و گیرنده‌های تفاضلی کاربرد دارد و داده دینامیک برای وسایل نقلیه استفاده می‌شود.

واحد تفکیک‌گر همبسته‌سازها را به دو دسـته معتبـر و فریـب تقسیم می‌کند. به این ترتیب که فـرض مـی‌کنـد نخسـتین پیـک مربوطه به سیگنال فریب و باقی سـیگنال‌هـا ناشـی حملـه فریـب هستند. در این مرحله خود همبستگی سیگنال فریب را از سیگنال IF ورودی کم می‌شود.

در قسـمت کـاهش فریـب ، میـزان همبسـتگی توابـع جمـع می‌گردند که در آن، Cr(ζ) تابع خودهمبستگی سیگنال دریافتی و Cp(ζ) تـابع همبسـتگی سـیگنال فریـب تخمینـی اسـت. معادلـه همبستگی سیگنال فریب تاخیری با دامنـه $\tilde{A}_i$ ، تـأخیر $\tilde{\tau}_i$ و فـاز

حامل $\tilde{\varphi}_i$ به شکل زیر حاصل می‌شود:

$$C_i(\tau)=\tilde{A}_i C(\tau-\tilde{\tau}_i)\cos(\tilde{\varphi}_l-\tilde{\varphi}_i) \quad (۱۲)$$



شکل (۵): بلوک دیاگرام راه‌کار پیشنهادی برای کاهش فریب.

که در آن، $C(\tau)$ تابع خودهمبستگی سیگنال کد ماهواره مربوطه است. درنتیجه، کل مقدار همبستگی سیگنال فریب تخمینی $C_i(\tau)$ با رابطه زیر قابل بیان است:

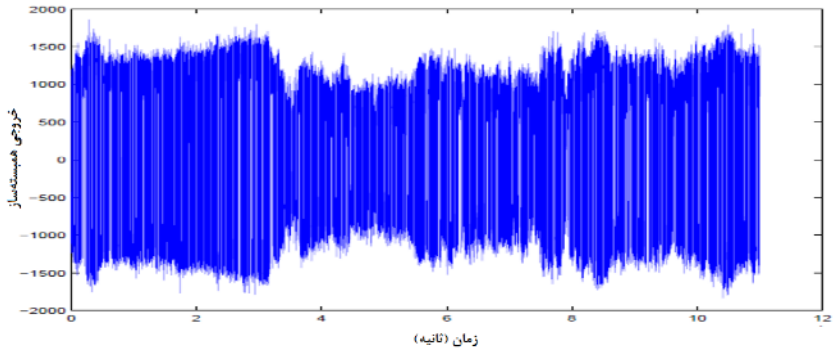
$$C_p(\tau)=C_{l+1}(\tau)+C_{l+2}(\tau)+\ldots+C_K(\tau)$$
$$=\sum_{i=l+1}^{k}C_i(\tau) \quad (۱۳)$$

کل مقادیر همبستگی سیگنال فریب Cp از مقدار همبستگی سیگنال ورودی C_r کم می‌شود. در نهایت همبستگی خروجی طبق رابطه (۱۴) حاصل می‌شود.

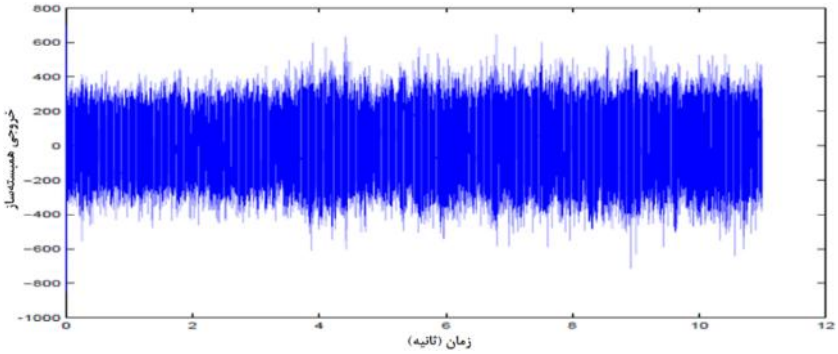
$$C_d(\zeta)=C_r(\zeta)-C_p(\zeta) \quad (۱۴)$$

از آن‌جایی که خطای ردیابی ناشی از فریب در DLL و PLL به‌دلیل تخریب همبستگی سیگنال دریافتی است، تفاضل همبستگی‌ها یعنی C_d کاهش فریب در حلقه ردیابی را فراهم می‌کند. به بیان دیگر، استفاده از C_d حلقه ردیابی را قادر می‌سازد تا سیگنال اصلی را با دقت بیشتری ردیابی نماید. برای کاهش فریب در بخش ردیابی باید روشی ارایه گردد تا اثر این خطای ایجادشده، تعدیل یابد.

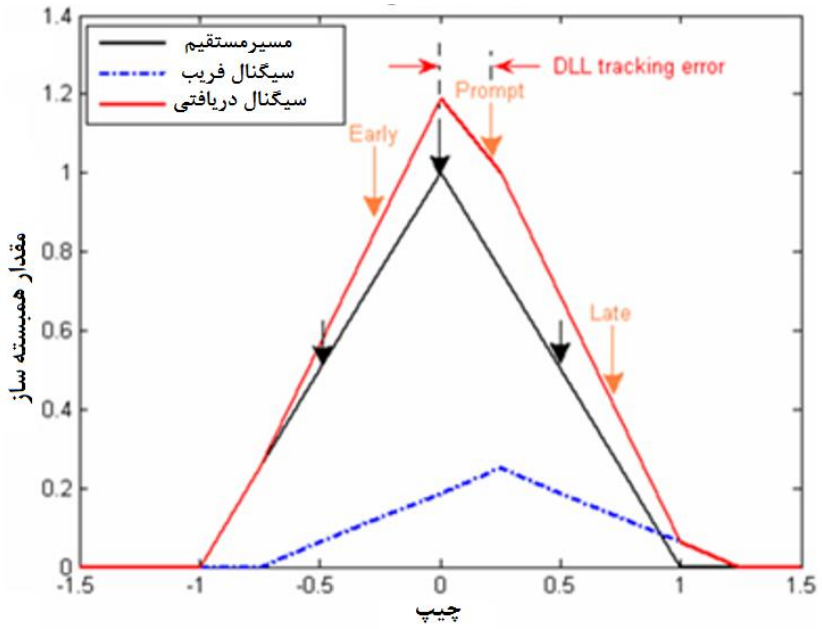
در الگوریتم پیشنهادی، خروجی سیگنال پردازش‌شده در ماژول ضدفریب با مقدار خودهمبستگی سیگنال دریافتی جمع می‌گردد. اگرچه با این روش می‌توان خطای فریب بر روی تابع همبستگی سیگنال دریافتی را کاهش داد، ولی نمی‌توان آن‌را به‌طور کلی حذف کرد. زیرا سیگنال مرجع استفاده‌شده برای تخمین فریب خود شامل خطای فریب است و فریب به‌طور دقیق تخمین‌زده نمی‌شود.



شکل(۶): خروجی همبسته‌ساز در بخش ردیابی برای سیگنال فریب.



شکل(۷): خروجی همبسته‌ساز در بخش ردیابی برای سیگنال معتبر.



شکل (۸): توابع همبستگی DLL با فریب و بدون فریب.

۴-۱- تخمین‌گر فریب بر پایه همبسته‌ساز چندگانه

در کاهش فریب در مرحله پردازش سیگنال از راه‌کار همبسته‌ساز چندگانه مطابق شکل (۹) استفاده شده است [۲۳]. پس از تبدیل سیگنال RF به IF و حذف حامل از آن، سیگنال پردازش‌شده وارد بخش همبسته‌سازها می‌شود. تعداد بیشتر همبسته‌ساز کنترل حلقه ردیابی را آسان‌تر و دقیق‌تر میسر می‌سازد. در برخی موقعیت‌ها تعدادی از این همبسته‌سازها می‌توانند غیرفعال نگه داشته شوند. همان‌طور که در شکل (۹) نشان داده شده است، مولد NCO و PRN بانکی از نسخه‌های شاخه‌های ابتدایی- انتهایی از کد محلی بر مبنای سیگنال معتبر تأخیریافته تولید می‌کند. فاصله همبسته‌سازها Δ و تعداد آن‌ها N است. از این همبسته‌سازها برای تخمین ویژگی‌های کانال استفاده می‌شود. پایه تئوری این روش تئوری تخمین بیشینه احتمال است. تابع هدف برای کمینه کردن متوسط مربع خطا (MSE) با رابطه زیر معرفی می‌گردد:

$$MSE(\hat{a},\hat{\tau},\hat{\theta}) = \int_{t-\tau}^{\tau}[r(t)-s(t)]^2 dt \qquad (۱۵)$$

که در آن، s(t) و r(t) به‌ترتیب سیگنال‌های فریب و معتبر هستند. ساده‌ترین راه‌حل برای این مشکل با تنظیم انحرافات جزیی MSE مطابق رابطه زیر حاصل می‌شود:

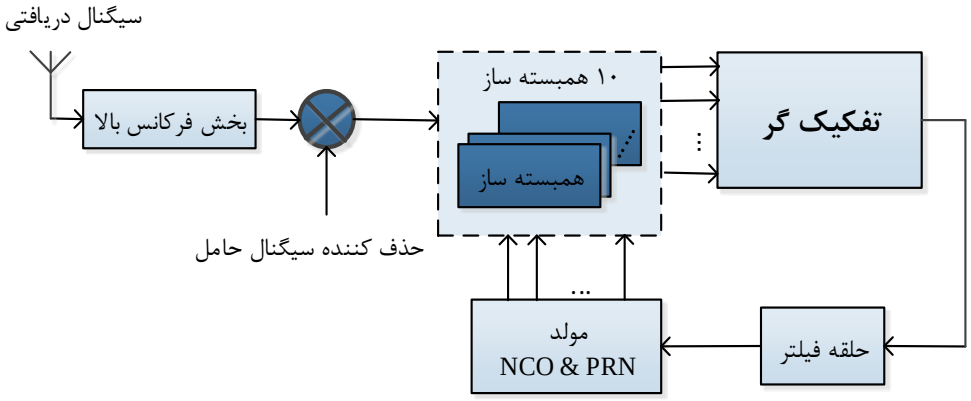
$$\hat{\tau}_i = \max_{\tau}\left[\mathrm{Re}\left(\left(R_{XX}-\sum_{x=i}^{M}\hat{a}_x R(\tau_i-\hat{\tau}_x)\exp(j\hat{\theta}_x)\right)\exp(-j\hat{\theta}_i)\right)\right] \qquad (۱۶)$$

$$\hat{\theta}_i = \arg\left[R_{XX}(\hat{\tau}_i)-\sum_{x=i}^{M}\hat{a}_x R(\tau_i-\hat{\tau}_x)\exp(j\hat{\theta}_x)\right]$$

که در آن، Rxx تابع همبسته‌ساز فرکانس پایین هم‌فاز/متعامد و $R(\Delta\tau)$ تابع همبستگی مرجع است. ایده اصلی فرآیند همبسته‌ساز چندگانه اجرای برازش منحنی به روش غیرخطی است که با M+1 سیگنال انجام می‌شود. ارزیابی این روش با بررسی سیگنال‌های کد و فاز باندهای پایین‌تر انجام می‌شود.

$$\Delta\tau = \frac{c}{T_c}\sqrt{\frac{N_{TLoop}d}{2C/No}};\Delta\theta = \frac{\lambda}{2\pi}\sqrt{\frac{N_{TLoop}d}{2C/No}} \qquad (۱۷)$$

که در آن، c سرعت نور، C/N0 نسبت حامل به نویز، N_{TLoop} پهنای باند نویز معادل حلقه ردیابی و d فاصله شاخه‌های ابتدایی و انتهایی است که این‌جا 2Δ درنظر گرفته شده است. همبستگی سیگنال دریافتی با هر کد محلی در بانک همبسته‌ساز محاسبه می‌شود. تفکیک‌گر در شکل (۹) مقادیر همبستگی را به عنوان ورودی استفاده می‌کند و تأخیر LOS را به‌عنوان خروجی تخمین می‌زند، سپس، با فیلتر حلقه هموار می‌شود. درنهایت، متوسط نقاط ابتدایی و انتهایی به عنوان ورودی تفکیک‌گر استفاده می‌شود. به این ترتیب نیازی به تغییر در ساختار تفکیک‌گر در حلقه ردیابی نیست. این مساله پیاده‌سازی عملی این راه‌کار را در کاربردهای تجاری آسان‌تر می‌کند. در ادامه دو راه‌کار پیشنهادی بر این اساس شرح داده می‌شوند.



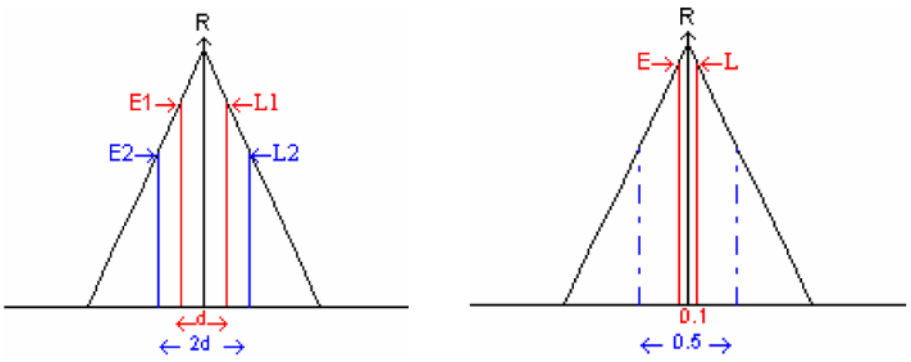
شکل (۹): بلوک دیاگرام حلقه DLL برپایه چند همبسته‌سازی.

۴-۱-۱- همبسته‌ساز باند باریک

استفاده از فاصله چیپ ۰/۱ در حلقه قفل فاز به GPSهای اولیه برمی‌گردد، زیراکه برای به‌حداقل رساندن سخت‌افزار یک راه مناسب بود. در این تحقیق، ایده همبسته‌ساز باند باریک گسترش داده شده است. به‌جای استفاده از همبسته‌ساز استاندارد با فاصله چیپ یک بین شاخه‌های اولیه و نهایی، یک همبسته‌ساز باند باریک با فاصله کمتر از ۱ چیپ استفاده گردیده است تا تابع تفکیک‌کننده ساخته شود. بعد از بررسی‌های متعدد مقدار ۰/۱ چیپ برای این الگوریتم انتخاب شد. به این ترتیب تغییرات جزئی تابع همبستگی نیز قابل شناسایی است. این قاعده در شکل (۱۰- الف) نشان داده شده است.

۴-۱-۲- همبسته‌ساز با کیفیت بالا

این نوع همبسته‌ساز از نوع همبسته‌ساز با تفاضل دوگانه است که برای کاهش فریب، دو همبسته‌ساز را به‌صورت موازی به‌کار می‌گیرد که در شکل (۱۰- ب) نشان داده شده است. این نوع از همبسته‌ساز در گروه همبسته‌سازها با خطای دو برابرشده قرار دارد که در توابع تفکیک‌کننده به‌جای یکی از دو همبسته‌ساز استفاده می‌کنند. همان‌طورکه در شکل نیز مشاهده می‌شود، فاصله جفت دورتر دقیقاً دو برابر جفت نزدیک‌تر است. جفت همبسته‌ساز نزدیک دارای فاصله چیپ ۰/۱ چیپ و همبسته‌ساز دورتر، فاصله چیپ ۰/۲ دارد. لازم به ذکر است که تفکیک‌کننده‌های کد براساس یک ترکیب خطی از همبسته‌سازها هستند.



(الف) (ب)

شکل (۱۰): الف) همبسته‌ساز باند باریک و ب) همبسته‌ساز با کیفیت بالا.

۴-۲- الگوریتم تطبیقی

در کاربردهایی که گیرنده متحرک است مانند کشتی و کامیون‌ها، همبسته‌ساز چندگانه پاسخ مناسبی ندارد و با گذشت زمان خطای مکان‌یابی افزایش می‌یابد. برای به‌روزرسانی مداوم مکان‌یابی از الگوریتم تطبیقی استفاده گردید. بلوک دیاگرام الگوریتم تطبیقی در شکل (۱۱) قابل مشاهده است. خروجی فیلتر با اعمال وزن‌های مناسب تخمین‌زده می‌شود. به منظور کمینه‌کردن تابع هزینه، وزن‌های فیلتر با رابطه زیر بهینه می‌شوند:

$$L(n) = \|y(n) - \tilde{y}(n)\|^2 \qquad (۱۸)$$

بهینه‌سازی از نقطه نظر آماری به تئوری فیلتر وینر منجر می‌شود که یک نقطه کمینه قابل محاسبه با رابطه زیر را دارد:

$$\zeta = E[|e(n)|^2] \qquad (۱۹)$$

دسترسی به کمینه تابع MSE نیاز به متوسط‌گیری از کل نمونه‌ها دارد که در نمونه‌های عملی امکان‌پذیر نیست. برای حل این مشکل، سیگنال را ارگودیک فرض می‌شود. در نتیجه، می‌توان از متوسط‌گیری آنی سیگنال خطا استفاده کرد. روش‌های جستجو برای یافتن ضرایب بهینه فیلتر وینر در واقع تابع تطبیقی است. به منظور رسیدن به این هدف، الگوریتم LMS به‌دلیل سادگی مهمترین گزینه در این زمینه است. رابطه (۲۰) سیگنال خطا یا تابع هدف را بیان می‌کند. تغییرات سیگنال مطلوب طبق رابطه (۲۱) تخمین زده می‌شود.

$$e(n) = y(n) - \hat{y}(n) \quad (۲۰)$$

$$\hat{y}(n) = w^T(n) * x(n) \quad (۲۱)$$

که در آن، w(n) و x(n) به‌ترتیب از روابط (۲۲) و (۲۳) به‌دست می‌آید:

$$w_n = [w_0, w_1, w_2, ..., w_k] \quad (۲۲)$$

$$x(n) = [x(n), x(n-1), ..., x(n-N+1)]^T \quad (۲۳)$$

در هر تکرار ضرایب فیلتر طبق رابطه (۲۴) تغییر می‌کند. طبق معادله (۲۴)، مقدار لحظه‌ای سیگنال خطا به‌عنوان تخمین MSE به کار می‌رود.

$$w(n+1) = w(n) + 2\mu e(n)x(n) \quad (۲۴)$$

این الگوریتم بعد از همگرایی می‌تواند خطای فریب را کاهش دهد. به‌منظور بهبود کارآیی الگوریتم LMS، نمونه‌های ارتقاء یافته‌های آن معرفی شده‌اند. با توجه به این‌که گام پیشرفت LMS در همه تکرارها ثابت است، در مقایسه با دیگر الگوریتم‌ها توانایی کمتری در کاهش خطا دارد. زیرا که نمی‌تواند کمینه مطلق را بیابد، هرچند که سرعت همگرایی بالایی دارد. الگوریتم SLMS[1] گام پیشرفت متغیری دارد. با نزدیک‌شدن به نقطه همگرایی، گام پیشرفت کوچکتر می‌شود تا کمینه مطلق با دقت بالاتری محاسبه شود. به این ترتیب، توازن بهتری بین دقت و سرعت فراهم می‌شود. این الگوریتم طبق معادله (۲۵) از معادله بازگشتی (۲۴) با جایگزینی خطای تخمین با علامتش حاصل می‌شود. پیاده‌سازی این الگوریتم ارزان‌تر از LMS است.

$$w(n+1) = w(n) + \mu sign(e(n))x(n)$$
$$= w(n) + \left(\frac{\mu}{|e(n)|}\right)e(n)x(n) \quad (۲۵)$$

پس از همگرایی الگوریتم یادگیری پارامترهای تخمین‌زده شده، قابل حصول است. بعد از پردازش فیلتر تطبیقی خروجی همبستگی را به دو بخش معتبر و فریب تفکیک می‌کند. درنهایت، پارامترهای تخمینی برای محاسبه همبستگی سیگنال معتبر به‌دست می‌آید.

۵- نتایج پیاده‌سازی الگوریتم

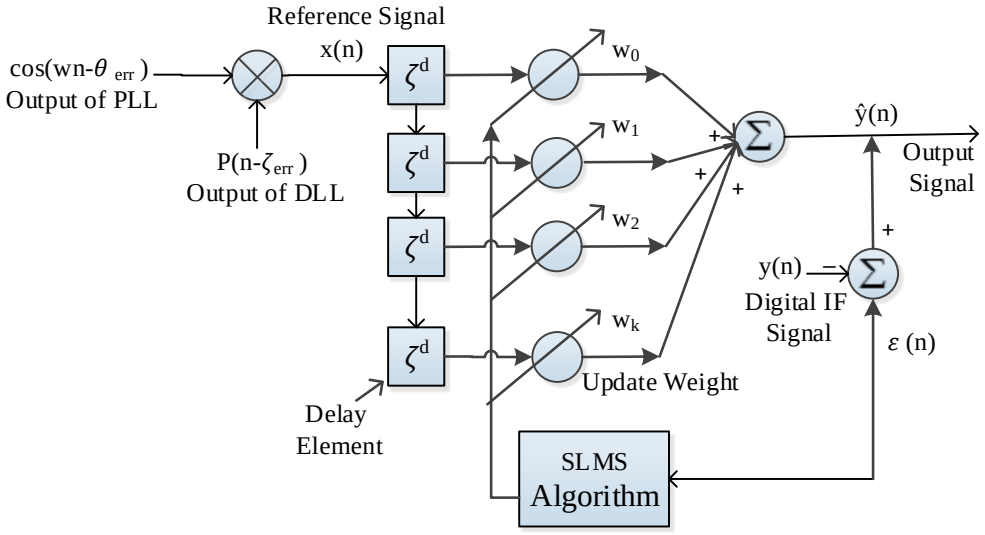
برای آزمودن رویکرد پیشنهادی، نیاز به داده‌های فریب مورد استفاده در کاربردهای عملی است. برای این منظور، ابتدا نمونه آزمایشگاهی داده فریب تأخیری تهیه شد. پس از ایجاد فریب، دامنه بخش هم‌فاز سیگنال افزایش و دامنه بخش متعامد کاهش می‌یابد. خطای ایجادشده در I و Q باعث ایجاد خطای کد و فاز و درنتیجه، خطای ردیابی می‌شود. این خطا گیرنده را در روند موقعیت‌یابی فریب می‌دهد. ذخیره‌سازی و تأخیر در سیگنال حقیقی GPS به‌منظور تولید فریب در گذشته بررسی شده است [۲].

می‌دانیم درصورت داشتن گیرنده واقعی و وجود سیگنال واقعی GPS در محیط، پس از انتشار سیگنال تأخیریافته در ورودی گیرنده واقعی، مجموع دو سیگنال جعلی و معتبر دریافت می‌شود. با توجه به این نکته، برای تولید سیگنال جعلی از سیگنال‌های واقعی جمع‌آوری‌شده، ابتدا از سیگنال معتبر دریافتی به‌مدت کافی نمونه‌برداری و سپس در فضای حافظه در دسترس ذخیره‌سازی کردیم و پس از ایجاد تأخیر مناسب، آن‌را برای ترکیب با سیگنال‌های حقیقی GPS منتشر نمودیم. شمای کلی سیستم پیاده‌شده در شکل (۱۲- الف) قابل مشاهده است. برای جلوگیری از تشخیص سریع سیگنال فریب در ورودی فریبنده یک واحد تخمین توان قرار داده شده است تا درنهایت، سیگنال منتشرشده را متناسب با توان سیگنال GPS در محل تنظیم نماید.

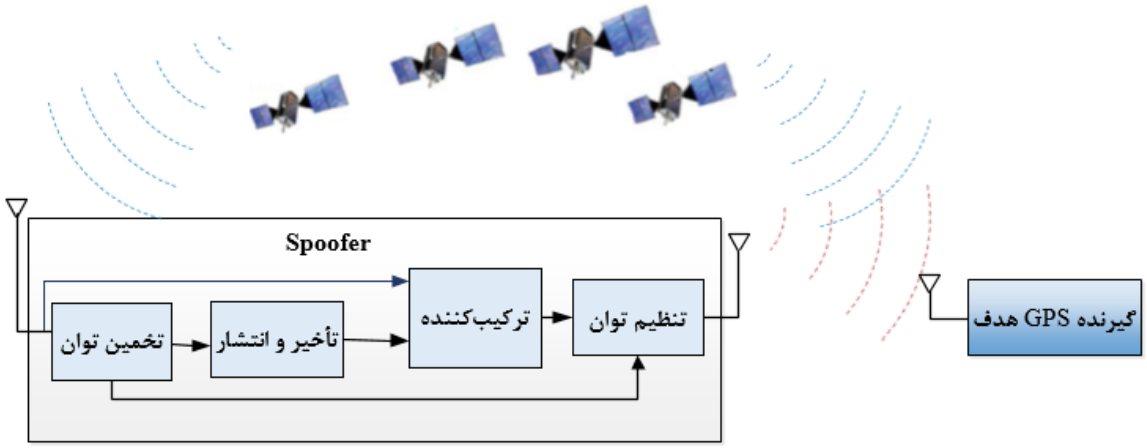
برای پیاده‌سازی عملی سناریو فریب تأخیری نیاز به تجهیزاتی است که بتواند سیگنال RF دریافتی از آنتن گیرنده GPS را ذخیره نموده و با سرعت بالا پیش‌پردازش‌های لازم را اعمال و سیگنال جدید را پس از بازگرداندن به حوزه RF به سمت گیرنده هدف ارسال نماید. به این ترتیب، خطای کوانتیزاسیون سیگنال IF در تولید سیگنال فریب مشکل‌ساز نمی‌شود. با توجه به امکانات موجود، این‌کار تنها با استفاده از شبیه‌ساز سیگنال GPS امکان‌پذیر است. شکل (۱۲- ب) سیستم آزمایشگاهی

1- Sign Least Mean Square

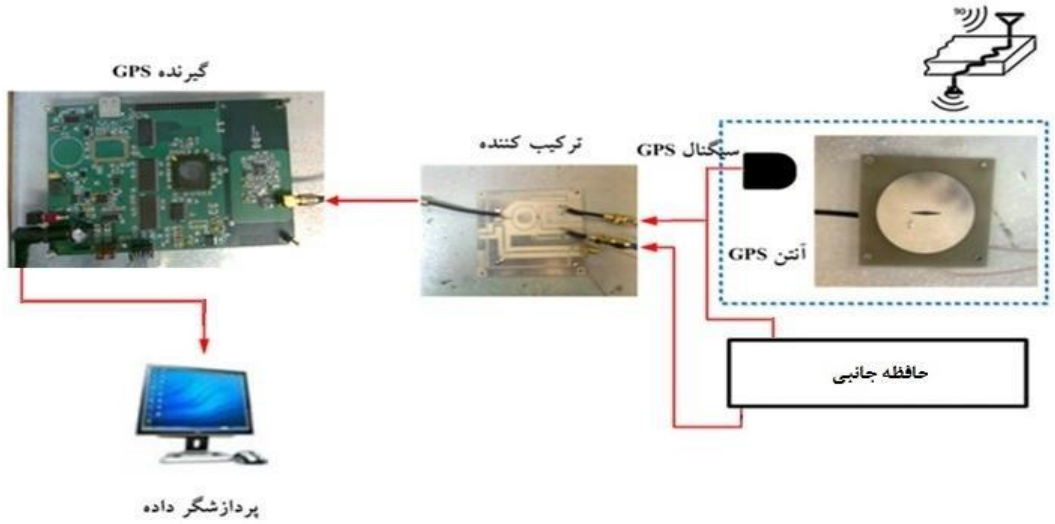
مورد استفاده را نشان می‌دهد.



شکل (۱۱): بلوک دیاگرام الگوریتم تطبیقی بر پایه الگوریتم SLMS.



(الف)



(ب)

شکل (۱۲): شمای کلی سیستم تولید فریب. الف) نرم‌افزاری و ب) اندازه‌گیری.

شکل (۱۳) خروجی نمونه حلقه DLL قبل و بعد از اعمال الگوریتم ضدفریب بر روی داده فریب نمونه را نشان می‌دهد. همان‌طورکه ملاحظه می‌شود خطای خروجی همبسته‌سازها بعد از اعمال الگوریتم در باز ۰/۱ محدود شده است. درحالی‌که برای داده فریب بازه تغییرات در سیگنال فریب در بازه ۰/۸ است. متوسط قدر مطلق داده معتبر ۰/۳ با انحراف معیار ۰/۰۹ به‌دست آمد که بعد از اعمال الگوریتم مقدار متوسط به ۰/۰۷ و انحراف معیار به ۰/۰۴ کاهش یافته است. همچنین، مشخص است که الگوریتم عملکرد بلادرنگ دارد، زیراکه مقدار خروجی حلقه در عرض ۲ ثانیه به تعادل رسیده است.

اشکال (۱۵-۱۴) یک نمونه پاسخ ناوبری را به‌ترتیب قبل و بعد از اعمال الگوریتم ضدفریب نشان می‌دهند. نمودار بالایی در شکل‌ها مربوط به تغییرات مختصات جغرافیایی در هر سه بعد است. نمودار پایین سمت چپ تغییرات مختصات به‌دست‌آمده در سطح افق را نشان می‌دهد و نمودار سمت راست پایین در رابطه با ماهواره‌های در دید می‌باشد. همان‌طورکه از شکل (۱۴) مشخص است، تغییرات مکان‌یابی در بازه حدود ۸۰۰ متر می‌باشد که بعد از اعمال الگوریتم ضدفریب، مطابق شکل (۱۵) این مقدار به ۱۰۰ متر کاهش یافته است. در سطح افق نیز سیگنال فریب موجب شده که گیرنده هدف متحرک به‌نظر برسد، درحالی‌که بعد از اعمال روش پیشنهادی مشابه سیگنال معتبر اصلی داده ساکن استخراج شده است.

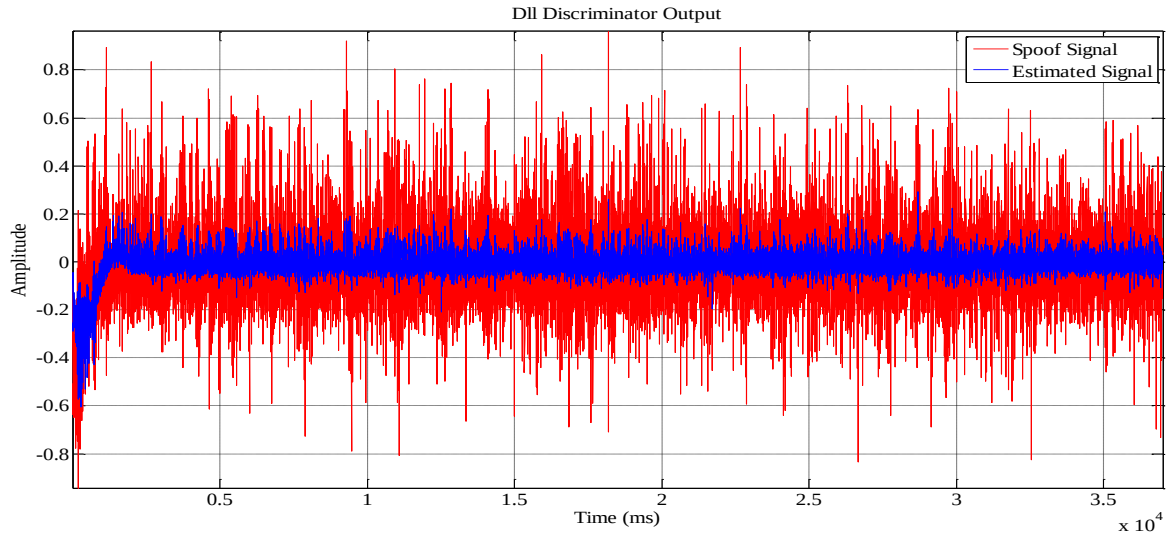
مجموعه داده آزمایشگاهی شامل پنج داده فریب و مجموعه داده اندازه‌گیری شامل سه داده فریب هستند. جداول (۴-۱) نتایج اعمال الگوریتم بر پایه دو تخمین‌گر متفاوت را بر روی هر دو مجموعه داده اندازه‌گیری و نرم‌افزاری نشان می‌دهند. برای بررسی دقیق‌تر مقدار خطا قبل و بعد از اعمال الگوریتم در دو بعد افق و ارتفاع نیز گزارش شده است. جداول (۲-۱) نتایج اعمال الگوریتم ضدفریب با تخمین‌گر کیفیت بالا را به‌ترتیب برای داده‌های آزمایشگاهی و اندازه‌گیری گزارش می‌کنند. متوسط کاهش خطا برای داده‌های آزمایشگاهی ۹۰ ٪ و برای داده‌های اندازه‌گیری ۸۳/۵ ٪ حاصل شده است. نویز بیشتر در داده‌های اندازه‌گیری دقت الگوریتم را کاهش داده است. جداول (۴-۳) نتایج اعمال الگوریتم ضدفریب با تخمین‌گر باند باریک برای داده‌های آزمایشگاهی و اندازه‌گیری را نشان می‌دهند. متوسط کاهش خطا برای داده‌های آزمایشگاهی ۹۲ ٪ و برای داده‌های اندازه‌گیری ۸۸ ٪ حاصل شده است.

جدول (۵) مقایسه کمی بین دو تخمین‌گر پیاده‌سازی‌شده را نشان می‌دهد. مشاهده می‌گردد که راه‌کار پیشنهادی برپایه تخمین‌گر تطبیقی توانسته است به‌طور میانگین ۹۳ ٪ خطای فریب آزمایشگاهی و ۸۷ ٪ خطای اندازه‌گیری را کاهش دهد. درحالی‌که راه‌کار پیشنهادی برپایه تخمین‌گر باند باریک خطای مکان‌یابی داده آزمایشگاهی را بطور میانگین ۹۵ ٪ و خطای فریب داده اندازه‌گیری را ۸۹ ٪ کاهش داده است. به این ترتیب، می‌توان نتیجه گرفت که الگوریتم پیشنهادی برپایه تخمین‌گر تطبیقی کارآیی بهتری دارد.

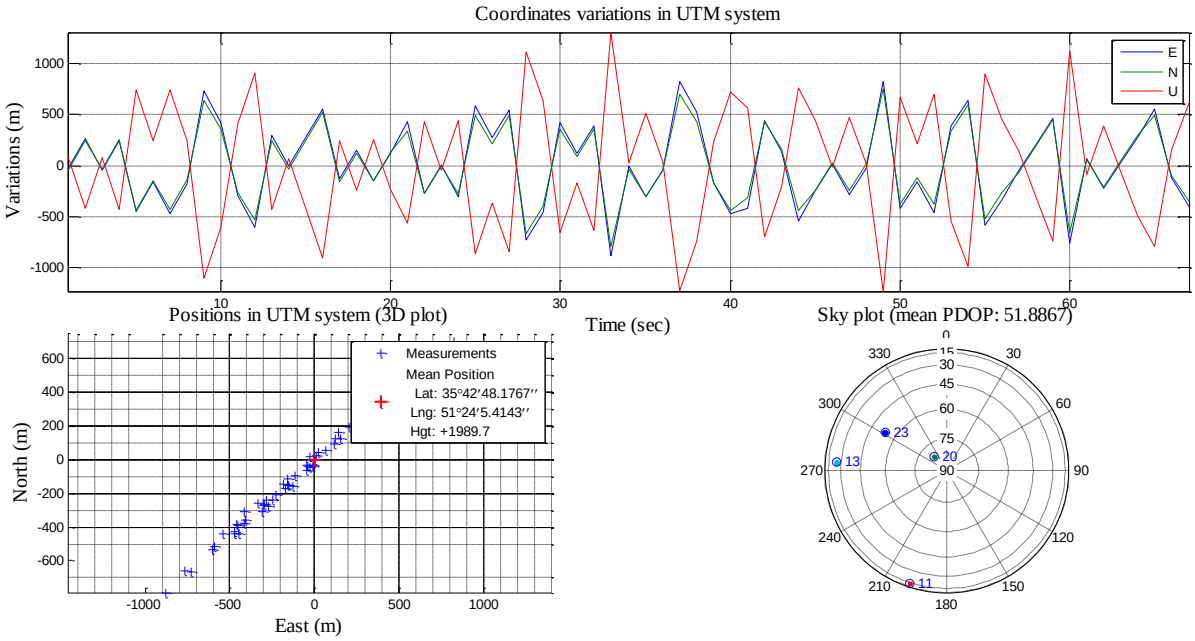
۶- مقایسه روش پیشنهادی با روش‌های موجود

با توجه به این‌که مقالات موجود در حوزه فریب نتایج کمی از نتیجه کار خود ارائه نداده‌اند، امکان مقایسه درصدی روش پیشنهادی با نمونه‌های موجود وجود ندارد. جدول (۷) مقایسه‌ای تحلیلی بین روش‌های پیشین و الگوریتم پیشنهادی برپایه تجهیزات مورد استفاده، مزایا و محدودیت‌ها ارایه می‌نماید. به منظور مقایسه و قضاوت صحیح بین روش‌های موجود امتیازدهی انجام می‌دهیم. به این ترتیب که برای هر ویژگی بهترین و بدترین حالت درنظر می‌گیریم. بسته به این‌که وضعیت الگوریتم در رابطه با آن ویژگی به چه شکلی باشد، به این ویژگی در الگوریتم از ۰ تا ۱۰ امتیاز تعلق می‌گیرد. به‌عنوان مثال، برای ویژگی تجهیزات لازم، اگر روشی هیچ سخت‌افزار اضافی لازم نداشته باشد، امتیاز ۱۰ و اگر نیاز به تغییر اساسی در ساختار گیرنده باشد، امتیاز صفر تعلق می‌گیرد. معیار امتیازدهی مقادیر ارایه‌شده در [۲۴] می‌باشد که در آن نیز مقایسه به همین نحو انجام شده است. ملاحظه می‌شود که روش پیشنهادی با ۲۵ امتیاز بهترین کارآیی را از خود نشان می‌دهد.

در روش الگوریتم تطبیقی، از لحاظ پیچیدگی زمانی، مدتی که حلقه ردیابی پردازش انجام می‌دهد، ۱ ٪ افزایش می‌یابد. فیلترهای تطبیقی برای کاهش پیچیدگی محاسباتی از تبدیل فوریه استفاده می‌کنند. پیچیدگی محاسباتی الگوریتم تطبیقی پیشنهادی از درجه N است که برابر با طول فیلتر مورد استفاده تعریف می‌گردد و در این‌جا، ۱۰ درنظرگرفته شده است. ملاحظه می‌گردد که روش پیشنهادی از کارآیی مطلوبی در مقایسه با دیگر روش‌ها برخوردار است. محدودیت بارز آن، عدم پاسخ مناسب در برابر فریب هماهنگ است.



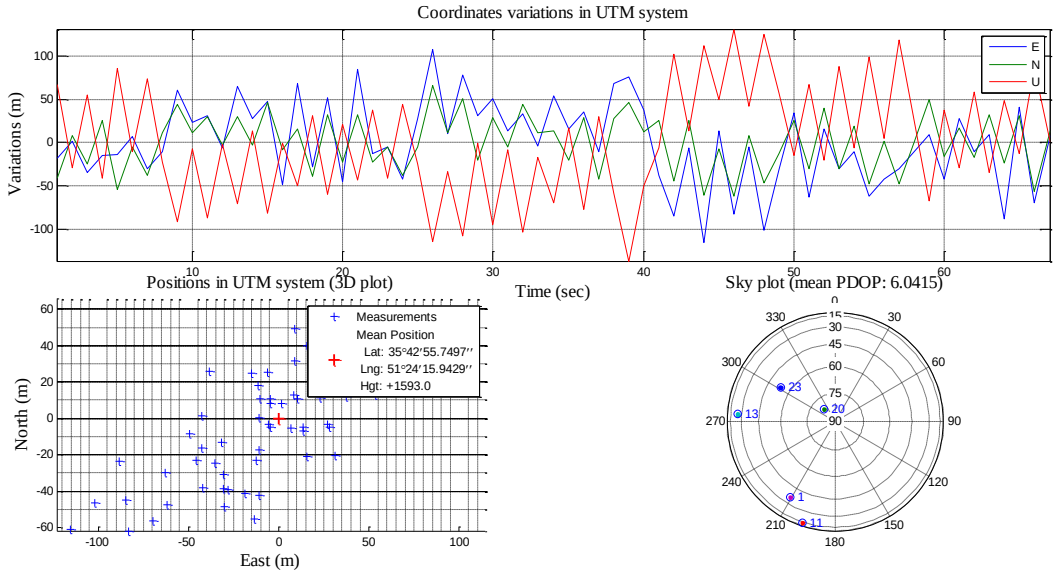
شکل (۱۳): خروجی حلقه DLL قبل و بعد از اعمال الگوریتم ضدفریب.



شکل (۱۴): نتایج ناوبری داده‌های دارای فریب.

جدول (۱): نتایج اعمال الگوریتم ضدفریب با تخمین‌گر همبسته‌ساز چندگانه برای داده‌های آزمایشگاهی.

میزان فریب	خطای فریب قبل از اعمال الگوریتم (متر)	خطای فریب بعد از اعمال الگوریتم (متر)	درصد بهبود
مجموعه داده اول	۷۱	۷	۸۹
مجموعه داده دوم	۸۴	۶	۹۴
مجموعه داده سوم	۱۷۲	۹	۹۵
مجموعه داده چهارم	۲۸۰	۹	۹۸
مجموعه داده پنجم	۹۷۰	۱۹۹	۷۹



شکل (۱۵): نتایج ناوبری داده پس از اعمال الگوریتم ضدفریب.

جدول (۲): نتایج اعمال الگوریتم ضدفریب با تخمین‌گر همبسته‌ساز چندگانه برای داده‌های اندازه‌گیری.

داده‌ها	مقدار فریب در سطح افق (متر)		مقدار فریب در ارتفاع (متر)		مقدار فریب در کل (متر)		درصد کاهش فریب
	قبل از اعمال الگوریتم	بعد از اعمال الگوریتم	قبل از اعمال الگوریتم	بعد از اعمال الگوریتم	قبل از اعمال الگوریتم	بعد از اعمال الگوریتم	
مجموعه داده اول	۳۴۳	۲۷	۲۹۸	۶۶	۴۵۴	۶۹	۸۵
مجموعه داده دوم	۱۷	۴۱	۲۵۸	۴۳	۲۵۹	۶۴	۷۷
مجموعه داده سوم	۳۷۰	۳۱	۴۱۵	۲۲	۵۵۷	۴۱	۹۵

جدول(۳): نتایج اعمال الگوریتم ضدفریب با تخمین‌گر تطبیقی برای داده‌های آزمایشگاهی.

میزان فریب	خطای فریب قبل از اعمال الگوریتم (متر)	خطای فریب بعد از اعمال الگوریتم (متر)	درصد بهبود
مجموعه داده اول	۷۱	۷	۹۰
مجموعه داده دوم	۸۴	۹	۹۱
مجموعه داده سوم	۱۷۲	۸	۹۵
مجموعه داده چهارم	۲۸۰	۱۳	۹۶
مجموعه داده پنجم	۹۷۰	۱۰۴	۸۹

جدول (۴): نتایج اعمال الگوریتم ضدفریب با تخمین‌گر تطبیقی برای داده‌های اندازه‌گیری.

داده‌ها	مقدار فریب در سطح افق (متر)		مقدار فریب در ارتفاع (متر)		مقدار فریب در کل (متر)		درصد کاهش فریب
	قبل از اعمال الگوریتم	بعد از اعمال الگوریتم	قبل از اعمال الگوریتم	بعد از اعمال الگوریتم	قبل از اعمال الگوریتم	بعد از اعمال الگوریتم	
مجموعه داده اول	۳۴۳	۲۸	۲۹۸	۴۳	۴۵۴	۵۲	۸۹
مجموعه داده دوم	۱۷	۲۹	۲۵۸	۳۶	۲۵۹	۴۷	۸۳
مجموعه داده سوم	۳۷۰	۱۶	۴۱۵	۱۷	۵۵۷	۲۶	۹۷

جدول (۵): مقایسه دو تخمین‌گر پیشنهادی در الگوریتم ارایه‌شده.

	داده اندازه‌گیری (٪)		داده آزمایشگاهی (٪)	
روش ها	متوسط کاهش	بازه تغییرات	متوسط کاهش	بازه تغییرات
همبسته‌ساز چندگانه	۸۷	۱۸	۹۳	۱۷
تطبیقی	۸۹	۱۲	۹۵	۸

جدول (۶) جمع‌بندی ویژگی‌های راه‌کار پیشنهادی.

پارامتر	ویژگی مربوطه
محل اعمال الگوریتم	حلقه ردیابی
متغیر مورد بررسی	خروجی همبسته سازها
پیچیدگی زمانی الگوریتم تطبیقی	۱٪ زمان شبیه‌سازی حلقه ردیابی
نوع فریب	فریب تاخیری
سیگنال GPS ورودی بخش ضدفریب	دوبیتی (۴ سطحی)
تخمینگرها	۱- همبسته ساز چندگانه و ۲- الگوریتم تطبیقی
تعداد همبسته‌ساز چندگانه	۱۰
فاصله همبسته‌سازها	۰/۱ چیپ
الگوریتم تطبیقی	SLMS
متغیر استفاده شده برای ارزیابی	RMS خطای مکانی فریب برحسب متر

جدول (۷): مقایسه روش‌های موجود کاهش فریب با راه‌کار پیشنهادی.

روش‌های تشخیص	محدودیت‌ها	مزیت‌ها	تجهزات مورد نیاز	معیارهای بررسی‌شده	نمره نهایی
SQM	نیاز به داده قبلی، عدم کارآیی در حملات هماهنگ (۲)	تشخیص آسان (۵)	ارتقا نرم‌افزاری (۶)	شاخه همبسته‌ساز (۵)	۱۸
VSD	ناکارآمد در حملات هماهنگ، نیاز به داده‌های قبلی (۵)	توانایی تفکیک چندمسیری (۷)	ارتقاء سخت افزاری و نرم افزاری (۳)	شاخه همبسته‌ساز (۴)	۱۹
گیرنده برداری	هزینه و پیچیدگی بالا (۳)	دقت تشخیص بالا (۸)	حلقه ردیابی اضافی (۲)	شاخه همبسته‌ساز (۳)	۱۶
ترکیبی	غیرقابل اطمینان در چندمسیری و بلادرنگ نبودن (۴)	امنیت بالا (۷)	ارتقاء نرم‌افزاری و سخت‌افزار اضافی (۲)	همبسته‌ساز و توان (۳)	۱۶
RAIM	غیرقابل اطمینان در شرایط بیش از دو ماهواره جعلی (۲)	پیاده‌سازی آسان (۵)	ارتقاء نرم‌افزاری (۶)	شبه فاصله (۳)	۱۶
پردازش فضایی	غیرقابل اطمینان در حملات فریب پیچیده (۶)	قابلیت اطمینان بالا (۷)	ارتقاء نرم‌افزاری و سخت‌افزار اضافی (۰)	سیگنال IF (۵)	۱۸
کار پیشنهادی	نیاز به داده‌های قبلی (۵)	پیاده‌سازی آسان، سریع و قابل اطمینان (۹)	ارتقاء نرم‌افزاری (۶)	همبسته‌ساز (۵)	۲۵

با توجه به امکانات موجود، در ارزیابی الگوریتم پیشنهادی تنها فریب تأخیری مورد استفاده قرار گرفت، اما به‌نظر می‌رسد در برابر انواع مختلف حمله فریب، روش پیشنهادی بتواند کارآیی قابل قبولی داشته باشد.

۷- نتیجه‌گیری

در این مقاله پس از مرور مختصری بر روش‌های ضدفریب موجود برای کاهش خطای مکانی ناشی از حمله فریب در ردیابی سیگنال‌های GPS، راه‌کاری نوین ارایه گردید. به این ترتیب که ابتدا میزان تأثیر فریب در حلقه ردیابی، تخمین زده می‌شود تا سیگنال فریب تخمینی به‌دست آید. همبستگی این سیگنال و سیگنال دیجیتالی IF محاسبه می‌گردند.

در بخش کاهش فریب همبستگی سیگنال به‌دست‌آمده با خودهمبستگی سیگنال دریافتی جمع می‌شود تا همبستگی سیگنال GPS معتبر استخراج گردد. با استفاده از همبسته‌ساز باند باریک با فاصله چیپ ۰،۱ بین ۰ تا ۱ در قسمت ردیابی نرم‌افزار GPS، مشاهده شد که میزان خطای ناشی از فریب به‌میزان چشمگیری کاهش می‌یابد. متوسط میزان کاهش خطا برای داده‌های آزمایشگاهی ۹۵٪ و برای داده‌های اندازه‌گیری ۸۹٪ حاصل شد.

۸- منابع

[1] A. Broumandan, A. Jafarnia-Jahromi, and G. Lachapelle, "Spoofing Detection, Classification and Cancelation (SDCC) Receiver Architecture for a Moving GNSS Receiver," GPS Solution, vol. 19, pp. 475-487, 2015.

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

[3] M. R. Mosavi, and Z. Shokhmzan, "Spoofing Mitigation of GPS Receivers using Normalized Least Mean Squares," Iranian Journal of Electrical and Electronic Engineering, vol.11, no.3, pp. 1-11, 2015.

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

[5] N. Shafiee, M. R. Mosavi, and M. Moazedi, "Detection of Delay Spoofing Attack base on Multi-Layer Neural Network in Single-Frequency GPS Receiver," Journal of Electronics and Cyber Defense, vol.3, no.1, pp. 69-80, 2015. (in Persian)

[6] Z. Shokhmzan and M. R. Mosavi, "Defense Against Spoofing in GPS Receiver using Correlation and Least Mean Squares Method Based on Sign-Data Algorithm," Journal of Electronics and Cyber Defense, vol. 3, no. 4, pp. 11-22, 2016. (in Persian)

[7] M. R. Mosavi, M. J. Rezaei, N. Hosseinzadeh, and R. A. Kiaamiri, "New Intelligent 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)

[8] M. R. Mosavi and F. Shafiee, "Narrowband Interference Suppression for GPS Navigation using Neural Networks," Journal of GPS Solutions, vol. 20, no. 3, pp. 341-351, 2016.

[9] K. C. Kwon, C. K. Yang and D. S. Shim, "Spoofing Signal Detection using Accelerometers in IMU and GPS Information," The Transactions of the Korean Institute of Electrical Engineers, vol. 63, no. 9, pp. 1273-1280, Sep. 2014.

[10] A. Farhadi, M. Moazedi, M. R. Mosavi, and A. Sadr, "A Novel Ratio-Phase Metric of Signal Quality Monitoring for Real-Time Detection of GPS Interference," Journal of Wireless Personal Communications, 2017.

[11] A. Javaid, F. Jahan, and W. Sun, "Analysis of Global Positioning System-based Attacks and a Novel Global Positioning System Spoofing Detection/Mitigation Algorithm for Unmanned Aerial Vehicle Simulation," Simulation: Transactions of the Society for Modeling and Simulation International, vol. 93, no. 5, pp. 427-441, 2017.

[12] J. Nielsen, A. Broumandan, and G. Lachapelle, "Spoofing Detection and Mitigation with a Moving Handheld Receiver," GPS World Magazine, vol. 21, no. 9, pp. 27-33, Sep. 2010.

[13] S. Daneshmand, "GNSS Interference Mitigation using Antenna Array Processing," Ph.D. Thesis, Department of Geometrics Engineering, University of Calgary, Alberta, April 2013.

[14] J. Nielsen, A. Broumandan, and G. Lachapelle, "GNSS Spoofing Detection for Single Antenna Handheld Receivers," Journal of the Institute of Navigation, vol. 58, no. 4, pp. 335-344, Sep.2011.

[15] J. Magiera and R. Katulski, "Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing," Journal of Applied Research and Technology, vol. 13, pp. 45-57, 2015.

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

[17] Y. Yang and J. Xu, "GNSS Receiver Autonomous Integrity Monitoring (RAIM) Algorithm based on Robust Estimation," Geodesy and Geodynamics, vol. 7, no. 2, pp. 117-123, March 2016.

[18] D. J. Jwo and Z. M. Wen, "Neural Network Assisted Vector Tracking Loop for Bridging GPS Signal Outages," Applied Mechanics and Materials, vols. 764-765, pp. 560-564, 2015.

[19] L. Baoa, R. Wub, W. Wangb, and D. Lub, "Spoofing Mitigation in Global Positioning System Based on C/A Code Self-coherence with Array Signal Processing," Journal of Communications Technology and Electronics, vol. 62, no. 1, pp. 66-73, 2017.

[20] A. Cavaleri, B. Motella, M. Pini, and M. Fantino, "Detection of Spoofed GPS Signals at Code and Carrier Tracking Level," The 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing, pp. 1-6, Dec. 2010.

[21] J. Huanga, L. L. Prestia, B. Motella, and M. Pini, "GNSS Spoofing Detection: Theoretical Analysis and Performance of the Ratio Test Metric in Open Sky," vol. 2, pp. 37-40, 2016.

[22] C. L. Chang and J. C. Juang, "An Adaptive Multipath Mitigation Filter for GNSS Application," CACS Automatic Control Conference, pp. 1-6, Nov. 2005.

[23] X. Fan, Li. Du, and D. Duan, "Synchrophasor Data Correction under GPS Spoofing Attack: A State Estimation based Approach," IEEE Transactions on Smart Grid, pp. 1-11, 2017.

[24] E. Shafiee, M. R. Mosavi, and M. Moazedi, "Detection of Spoofing Attack using Machine Learning based on Multi-Layer Neural Network in Single-Frequency GPS Receivers," Journal of Navigation, pp. 1-20, 2017.

Journal of Electronical & Cyber Defence
Vol. 6, No. 3, 2018, Serial No. 23

GPS Spoofing Mitigation using Adaptive Estimator in Tracking Loop

M. Moazedi, M. R. Mosavi*, Z. Nasrpooya, A. Sadr

*Imam Hossein University

(Received: 18/08/2017, Accepted: 23/02/2018)

ABSTRACT

The attacks such as spoofing is one of the main sources of error in tracking of Global Positioning System (GPS) receivers. The aim of these attacks is to calculate fake time and position. The spoofer sends the counterfeit signal and causes to spoof. This counterfeit signal is generated in different ways. In this paper, the studied interference is the delay spoof. Indeed, the aim is introducing a new approach in tracking loop of the GPS receiver in order to decrease the generated delay by spoof attack. The suggested algorithm has two main steps. The first step estimates the amount of delay spoof. Subsequently, through an innovative approach, the effect of spoofing signal is extracted and then subtracted from the total measured correlation function. To achieve that, the effect of spoofing signal is estimated and the estimated spoofing signal is generated separately. For this purpose, two estimator based on multi-correlator and adaptive approach is introduced. Correlation of this signal with the digital IF signal is calculated and entered into the spoof mitigation part. In this part, correlation of this signal is added to auto-correlation of received signal and correlation of authentic signal is achieved. These techniques provide easy-to-implement and quality assurance tools for anti-spoofing. Applying the proposed algorithm decreases the average spoofing error by 88%.

Keywords: GPS Receiver, Spoofing Attack, Delay Lock Loop, Narrow Band Correlator

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