

کاهش خطای فریب GPS با استفاده از تخمین گر تطبیقی در حلقه ردیابی

مریم معاضدی^۱، سید محمدرضاموسوی میرکلایی^{۲*}، زهرا نصرپویا^۳، علی صدر^۴

۱- دانشجوی دکتری، ۲- استاد، ۳- دانشجوی کارشناسی ارشد، ۴- دانشیار، دانشکده مهندسی برق، دانشگاه علم و صنعت ایران

(دریافت: ۹۶/۰۵/۲۷، پذیرش: ۹۶/۱۲/۰۴)

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 به واسطه آن بتوان تأثیر فریب ایجاد شده 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 به دست آید. برای این منظور، دو تخمین گر 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 به دست آمده 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.

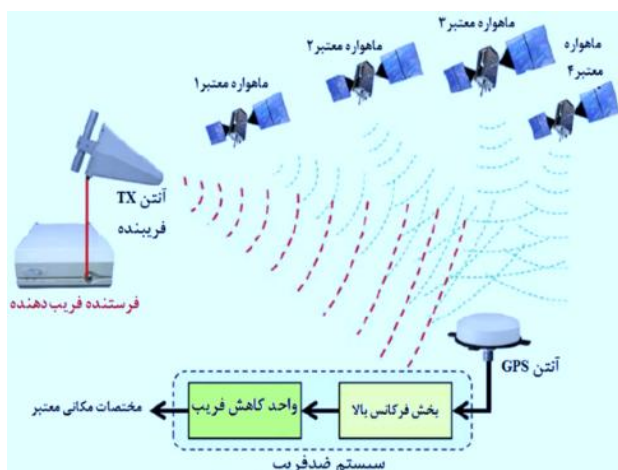
واژگان کلیدی: گیرنده GPS، حمله فریب، حلقه قفل تأخیر، همبسته‌ساز باند باریک

هوایماها 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 آنجایی که 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 به راحتی 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.

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. فریب‌دهنده‌های 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



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

از این رو، می‌توان روش پردازش فضایی را برای تخمین اثر سه بعدی سیگنال‌های دریافتی و تفکیک این سیگنال‌ها که رابطه فضایی مشخصی دارند، به کار گرفت [۱۱-۱۵]. این روش پیچیدگی سخت‌افزاری بالایی دارد، در حالی که 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 به کار برده شده است [۱۷]. لدوینیا^۳ در سال ۲۰۱۰ میلادی، نرخ و اختلاف آزمون‌های SQM برای آشکارسازی فریب را به کار گرفت. سپس، روش بررسی صحت استقلال گیرنده (RAIM)^۴ را برای آشکارسازی و کاهش فریب در سطح ناوبری و مسائل مکان‌یابی را ارائه 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 ضد فریب 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

حمله فریب به سه دسته عمده ساده، متوسط و پیچیده تقسیم می‌شود که در این جا 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 ضد فریب 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. به دلیل محدودیت‌های عملی، معمولاً فرستنده‌های فریب (به‌جز فریب‌دهنده‌های ماهر) چندین سیگنال جعلی را از یک آنتن می‌فرستند، در حالی که سیگنال‌های معتبر GPS از ماهواره‌های مختلف در مسیرهای گوناگون فرستاده می‌شوند.

۱- Shepard

۲- Signal Quality Monitoring

۳- Ledvina

۴- Receiver Autonomous Integrity Monitoring

می شود که گیرنده کپی کد منتشر شده شبه تصادفی را با سیگنال منتشر شده ورودی همبسته نماید. حلقه قفل تأخیر با سه جزء همبستگی مختلط (اولیه، میانی و نهایی) برای تعقیب سیگنال بر روی این تابع اجرا می شود، اگر چه بعضی گیرنده ها جزء های همبستگی بیشتری تولید می کنند. تعداد بیشتر این جزء های همبستگی پیش بینی بهتری بر روی میزان خرابی ناحیه تابع همبستگی مختلط نسبت به اولیه، میانی و نهایی به تنهایی عرضه می کنند. وقتی که زنجیره ای از تأخیر جزء های همبستگی موجود است، ناحیه تابع همبستگی مختلط می تواند به عنوان سیگنال پیوسته زمان در نظر گرفته شود. جزء همبستگی مختلط مسیر مستقیم $x_d(t, \zeta)$ می تواند به صورت معادله (۲) مدل گردد.

$$x(t, \zeta) = x_d(t, \zeta) + x_m(t, \zeta) + x_s(t, \zeta) + n(t, \zeta) \quad (1)$$

$$x_d(t, \zeta) = \alpha_d(t) R(\zeta - \zeta_d(t)) e^{j\theta_d(t)} \quad (2)$$

این معادله نشان می دهد $x_d(t, \zeta)$ یک انتقال یافته زمانی، مقیاس بندی شده ناحیه و اصلاح شده فاز تابع همبستگی مختلط $R(\zeta)$ است که در آن، $0 \leq \alpha_d(t) \leq 1$ فاکتور مقیاس بندی، $\zeta_d(t)$ تأخیر ثانیه ها و فاز بر حسب 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 کرده اند $\zeta_d(t)$ و $\theta_d(t)$ را مساوی صفر قرار دهند که در این مورد مناسب تر است $\alpha_d(t) = 1$ باشد. تابع خود همبسته $R(\zeta)$ به صورت معادله (۳) مدل می شود:

$$R(\zeta) \approx \begin{cases} 1 - \frac{|\zeta|}{T_c} & ; |\zeta| < T_c \\ 0 & ; \text{otherwise} \end{cases} \quad (3)$$

که در آن، $T_c \approx 1 \mu s$ است و سرعت تراشه سیگنال GPS L1 C/A را تخمین می زند. در عمل $R(\zeta)$ برای هر کد منتشر شده شبه تصادفی در هر ماهواره کمی تغییر می کند. این تغییر تأثیری بر مدل ندارد و بنابراین، معادله (۳) یک تقریب منطقی است. چندمسیری در ناحیه همبستگی مختلط $x_m(t, \zeta)$ می تواند به عنوان انطباق تأخیر بعضی سیگنال های مسیر مستقیم مدل شود.

$$x_m(t, \zeta) = \sum_{k=1}^N \alpha_{m,k}(t) R(\zeta - \zeta_{m,k}(t)) e^{j\theta_{m,k}(t)} \quad (4)$$

اگر سیگنال چندمسیری وجود نداشته باشد، $N=0$ است. چون سیگنال های چندمسیری، کپی سیگنال های مسیر مستقیم با تأخیر هستند، بنابراین $0 < \zeta_{m,k}(t)$ است. به این ترتیب می توان نتیجه گرفت که به دلیل $0 \leq \alpha_{m,k}(t) \leq \alpha_d(t)$ سیگنال چندمسیری نسبت به سیگنال مسیر مستقیم تضعیف می شود. هر چند در

فیلترهای حلقه ردیابی می آید، نادیده بگیرد و از اندازه گیری های سطح ناوبری برای راه اندازی NCOها استفاده کند. این حالت باقی می ماند تا زمانی که بیشینه همبستگی فریب دور شود و همبسته ساز به فرآیند ردیابی سیگنال اصلی بازگردد. این گیرنده علاوه بر پیچیدگی بالا نیاز به تغییر سخت افزار گیرنده دارد که هزینه بالایی دارد.

قاعده ابتکاری انتخاب پیک معتبر بر پایه اندازه گیری CNR نیز در رابطه با کاهش فریب به کار گرفته شده است [۲۰]. در این روش بررسی C/No با یک قاعده تصمیم گیری ادغام شده است. فریبند آفست داپلر سیگنال های جعلی را تطبیق می دهد و فاز کد را به نحوی تنظیم می نماید که بر ناحیه هدف منطبق باشد. مرز ناحیه هدف دقیقاً مشخص نیست، اما تأثیر فریب خارج از آن به شدت افت می کند. این روش علاوه بر پیچیدگی بالا برای دیگر انواع فریب پاسخ مناسب ندارد.

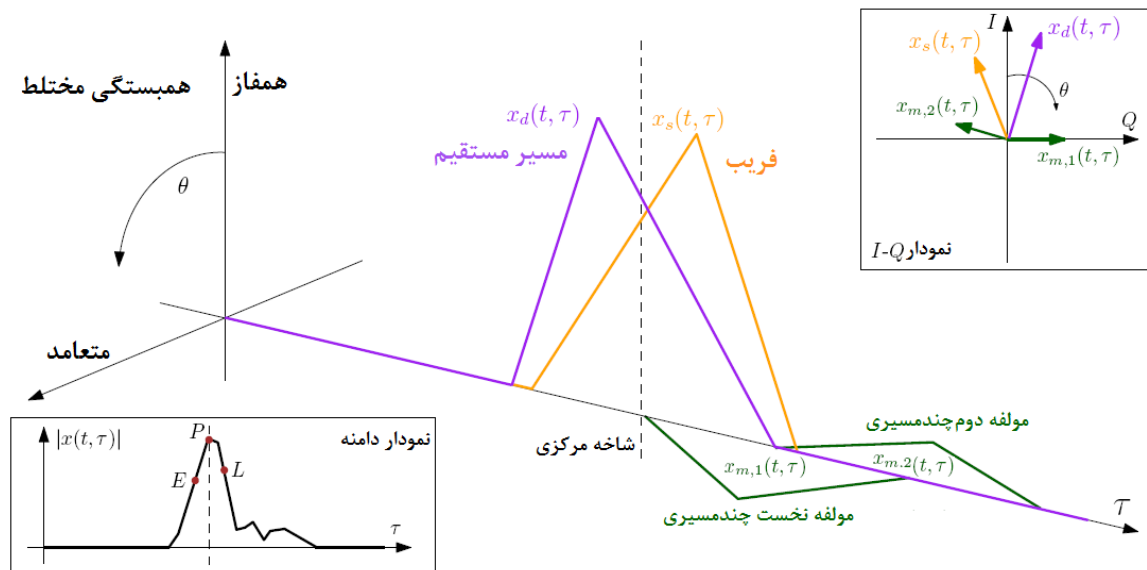
ملاحظه می شود که با روش های موجود امکان مقابله مطمئن و کم هزینه با حمله فریب وجود ندارد. از این رو نیاز به یک روش ساده و در عین حال هزینه پایین به شدت احساس می شود. روش پیشنهادی در این مقاله با الگوریتم تطبیقی و بدون تغییر در ساختار گیرنده GPS و صرفاً ارتقاء نرم افزار در حلقه ردیابی توانسته تا حدی زیادی اثر حمله فریب را کاهش دهد. پس از معرفی کامل تر راه کار پیشنهادی در بخش بعدی، مقایسه جامعی با روش های پیشین در بخش ۵ انجام خواهد شد.

۳- مدل سازی تداخل در حلقه ردیابی

مطالعه روش های چندمسیری و روش های کاهش این آثار در ارتباطات و سیستم های ناوبری، به طور خاص سیستم های دسترسی چندگانه تقسیم کد، یک راه طبیعی برای مدل کردن تداخل های GPS فراهم می کند. چندمسیری معمولاً در ناحیه تابع همبستگی مختلط مدل می شود 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 می گردد که در آن $x(t, \zeta)$ 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 این جا مسیر مستقیم و اصلی معادل در نظر گرفته شده اند. تابع همبستگی مختلط $x(t, \zeta)$ با زمان t و تأخیر آفست ζ ، وقتی تولید

شاخص $I_{spoofing}$ است که مشخص می‌نماید فریب اتفاق افتاده است یا خیر؟ قابل توجه است که در این حالت، مورد چندفریبی در نظر 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.

^۱VSD قوی‌تر جزء‌های همبستگی بیشتری نیاز است.

تخریب ناحیه تابع همبستگی مختلط همچین 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 در نظر 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 در نظر گرفته شده‌اند که در این جا $I(t, \zeta)$ یا $R(\zeta)$ برابر نیست و نیز $Q(t, \zeta) \neq 0$ است. تخریب وابسته به تأخیر به دلیل تخریب فاز وابسته به تأخیر است که توسط سیگنال فریب با فاز غیرحامل تطبیق داده شده، ایجاد گردیده است. برای مثال، در جزء همبستگی $\pm T/2$ $x_s(t, \zeta)$ اضافه شده در شکل دهی $Q(t, \zeta)$ نقش دارد. اما چون سیگنال فریب فاز حامل آن منطبق نشده است، تخریب در $Q(t, \zeta)$

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 به صورت معادله (۵) است:

$$x_s(t, \zeta) = (\alpha_s(t) R(\zeta - \zeta(t)) e^{j\theta_s(t)}) \times I_{spoofing} \quad (5)$$

معادله فوق یک احساس شهودی ایجاد می‌کند، چون اگر فریب‌دهنده 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 توجهه در این مدل

فریب‌دهنده 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 فریب‌دهنده دشوار است. بنابراین، شکل (۲) موردی را نشان می‌دهد که $\theta_d(t) \neq 0$ است و در قسمت سمت راست بالا (شکل I-Q) نشان داده شده است. با وجود اینکه دو جزء چندمسیری وجود دارد، اندازه آن‌ها به طور 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 آن جا 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 دنبال کردن سیگنال به کار می‌برد. با این سه جزء همبستگی، گیرنده GPS نمی‌تواند به اندازه کافی خرابی در دامنه نشان داده شده در شکل را درست کند. برای

خروجی PLL و DLL در هم ضرب و وارد بلوک تخمین گر فریب می گردند. در این بلوک پس از تخمین میزان تأخیر ζ ، سیگنال فریب تخمین زده شده به دست می آید. سپس همبستگی این سیگنال و سیگنال ورودی دیجیتال IF محاسبه شده و در نهایت به بخش کاهش فریب می رود. در این بخش سیگنال به دست آمده با خودهمبستگی سیگنال دریافتی جمع می گردد.

در حضور سیگنال اصلی و فریب می توان سیگنال دریافتی را مدل کرد [۲۲]. اگر سیگنال IF دریافتی را به صورت معادله (۷) نشان دهیم، معادله (۸) به ترتیب قسمت هم فاز و متعامد این سیگنال را نشان می دهد.

$$S_r(t) = \sum_{k=1}^{N_{\text{Sat}}} \sum_{m=1}^{N_k} \alpha_{km} \cdot c(t - \tau_k - \Delta\tau_{km}) \cdot e^{j(\varepsilon_{\theta_{km}} + \theta_{\lambda m})} + n(t) \quad (7)$$

$$I(j) = \sum_{m=0}^N \alpha_m K_c(\varepsilon_r - \Delta\tau_m + d\tau_j) \cos(\varepsilon_\theta + \Delta\theta_m) + n_1, \\ Q(j) = \sum_{m=0}^N \alpha_m K_c(\varepsilon_r - \Delta\tau_m + d\tau_j) \sin(\varepsilon_\theta + \Delta\theta_m) + n_q \quad (8)$$

اشکال (۶) و (۷) مقایسه نتایج حاصل از ردیابی سیگنال اصلی و فریب را نشان می دهد. همان طور که مشاهده می شود پس از ایجاد فریب، دامنه نمودار بخش هم فاز سیگنال افزایش و دامنه نمودار بخش متعامد کاهش یافته است. خطای ایجاد شده در I و Q باعث ایجاد خطای کد و فاز و در نتیجه خطای ردیابی شده و گیرنده را در موقعیت یابی صحیح فریب می دهد.

سیگنال دریافتی در قسمت RF فیلتر می شود و پس از تبدیل به باند پایه، سیگنال IF حاصل می گردد. سپس نمونه برداری و کوانتیزه می شود. سیگنال IF دیجیتال برابر مجموع سیگنال اصلی GPS سیگنال فریب و نویز است. مدل سیگنال اصلی GPS خروجی تبدیل کننده A/D به صورت معادله (۹) در می آید که در آن، A_0 دامنه سیگنال اصلی GPS، $P(n-\zeta_0)$ کد طیف گسترده با تأخیر ζ_0 ، w_0 فرکانس زاویه ای و ϕ_0 فاز حامل است. بنابراین، مجموع سیگنال اصلی GPS و سیگنال فریب به صورت معادله (۱۰) بیان می گردد.

$$y_0(n) = A_0 P(n-\zeta_0) \cos(w_0 n + \phi_0) \quad (9)$$

$$y(n) = \sum_{i=0}^m A_m P(n-\zeta_i) \cos(w_i n + \phi_i) \quad (10)$$

در این معادله، $M=1$ بیان گر سیگنال فریب است. A_1 ، ϕ_1 و ζ_1 بیان گر دامنه، فاز حامل و تأخیر کد سیگنال فریب است. بنابراین، به عنوان سیگنال دریافتی واقعی GPS بعد از اضافه کردن نویز در تبدیل کننده A/D داریم:

$$y(n) = \sum_{i=0}^m A_m P(n-\zeta_i) \cos(w_i n + \phi_i) + \eta(n) \quad (11)$$

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

ثابت نیست (به این معنا که انحراف آن با $R(\zeta)$ تغییر می کند). به علت $\theta_s(t) \neq \theta_d(t)$ 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 می دهد. تخریب در $I(t, \zeta)$ به هر دو دلیل اتفاق می افتد.

از آن جایی که شکل (۳) یک حمله فریب را نشان می دهد، می توان چنین در نظر 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 منحصربه فرد نیست. برای مخاברה موفقیت آمیز داده های ناوبری باید نسخه های محلی کد و فاز به صورت دقیق تولید شوند که این امر وابسته به حلقه قفل تأخیر (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 می شود. سیگنال ورودی با سه عدد تکرار محلی کد میانی، اولیه و نهایی با فاصله چسپ های دقیق از هم تفکیک شده اند. ایده این حلقه آن است که پاسخ عبور از صفر تفکیک کننده را ردیابی کند. در حضور حمله فریب (فرض شده فقط یک سیگنال فریب داریم)، سیگنال دریافتی به صورت معادله (۶) است:

$$s(t) = A_0 \cdot d(t-\zeta_0) \cdot cf(t-\zeta_0) \cos(2\pi ft - \theta_0) + A_1 \cdot d(t-\zeta_1) \cdot cf(t-\zeta_1) \cos(2\pi ft - \theta_1) + b(t) \quad (6)$$

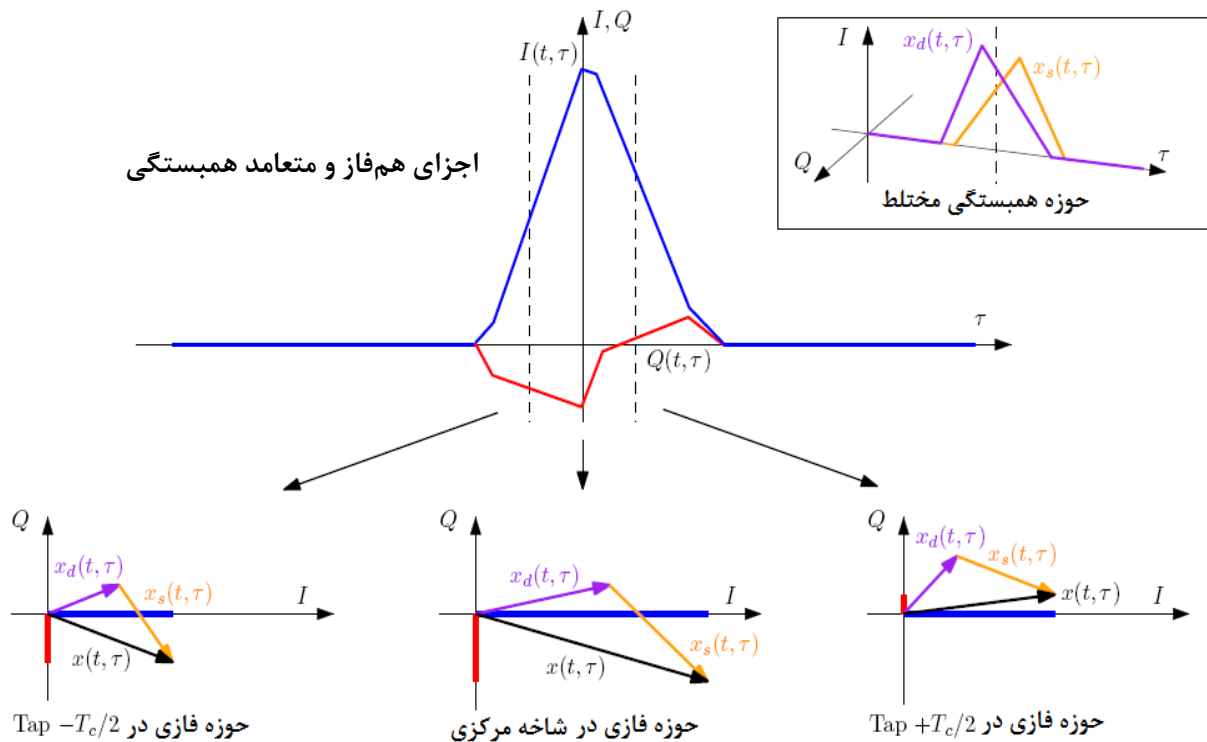
با دریافت پاسخ تفکیک گر سیگنال ترکیبی خطای ردیابی خروجی تفکیک گر اولیه- نهایی ناشی از فریب در DLL را نشان می دهد (مطابق شکل (۴)) [۲۱]. مشاهده می شود که مقدار عبور از صفر تفکیک کننده، انتقال پیدا کرده است که موجب ایجاد خطا در تخمین تأخیر کد می شود.

۴- الگوریتم پیشنهادی تخمین و حذف فریب در حلقه ردیابی

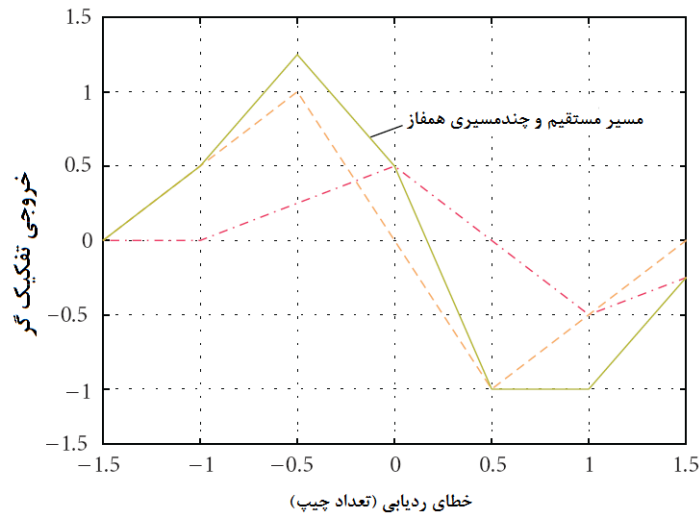
شکل (۵) بلوک دیاگرام راه کار نوین پیشنهادی به منظور کاهش فریب را نشان می دهد. ابتدا سیگنال اصلی و فریب از طریق آنتن گیرنده دریافت و در قسمت گیرنده RF پردازش شده و سپس وارد بلوک A/D می گردد. در این مرحله سیگنال آنالوگ ورودی به حوزه دیجیتال تبدیل و وارد قسمت ردیابی می شود. از طرف دیگر،

خطای حلقه DLL و در نتیجه موقعیت‌یابی را موجب می‌گردد.

همان‌گونه که مشاهده می‌گردد تقارن بخش‌های هم‌فاز و متعامد از بین رفته و تخمین تأخیر زمانی مشکل است. همین تأخیر زمانی



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



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

هستند. در این مرحله همبستگی سیگنال فریب را از سیگنال IF ورودی کم می‌شود.

در قسمت کاهش فریب، میزان همبستگی توابع جمع می‌گردند که در آن، $Cr(\zeta)$ تابع خودهمبستگی سیگنال دریافتی و $Cp(\zeta)$ تابع همبستگی سیگنال فریب تخمینی است. معادله همبستگی سیگنال فریب تاخیری با دامنه \tilde{A}_i ، تأخیر $\tilde{\tau}_i$ و فاز

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

واحد تفکیک‌گر همبسته‌سازها را به دو دسته معتبر و فریب تقسیم می‌کند. به این ترتیب که فرض می‌کند نخستین پیک مربوطه به سیگنال فریب و باقی سیگنال‌ها ناشی حمله فریب

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

$$C_p(\tau) = C_{l+1}(\tau) + C_{l+2}(\tau) + \dots + C_K(\tau) \quad (13)$$

$$= \sum_{i=l+1}^k C_i(\tau)$$

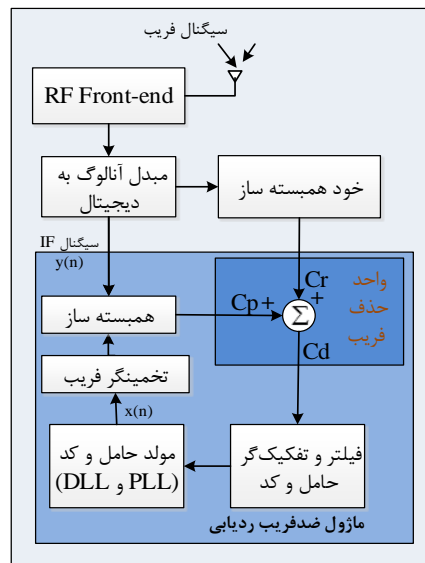
کل مقادیر همبستگی سیگنال فریب C_p از مقدار همبستگی سیگنال ورودی C_r کم می شود. در نهایت همبستگی خروجی طبق رابطه (۱۴) حاصل می شود.

$$C_d(\zeta) = C_r(\zeta) - C_p(\zeta) \quad (14)$$

از آن جایی که خطای ردیابی ناشی از فریب در DLL و PLL به دلیل تخریب همبستگی سیگنال دریافتی است، تفاضل همبستگی ها یعنی C_d کاهش فریب در حلقه ردیابی را فراهم می کند. به بیان دیگر، استفاده از C_d حلقه ردیابی را قادر می سازد تا سیگنال اصلی را با دقت بیشتری ردیابی نماید. برای کاهش فریب در بخش ردیابی باید روشی ارائه گردد تا اثر این خطای ایجاد شده، تعدیل یابد.

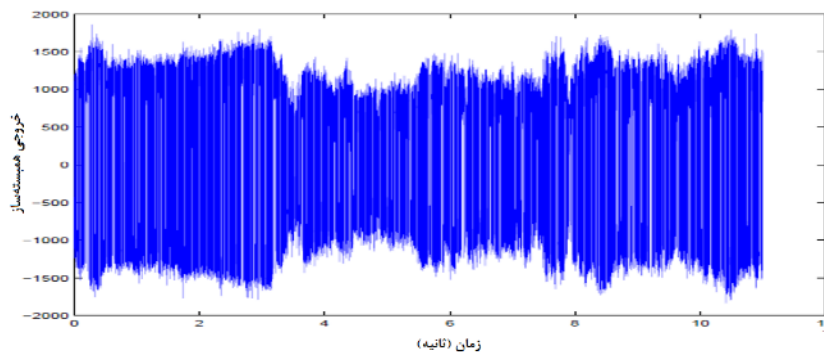
در الگوریتم پیشنهادی، خروجی سیگنال پردازش شده در مازول ضد فریب با مقدار خود همبستگی سیگنال دریافتی جمع می گردد. اگرچه با این روش می توان خطای فریب بر روی تابع همبستگی سیگنال دریافتی را کاهش داد، ولی نمی توان آنرا به طور کلی حذف کرد. زیرا سیگنال مرجع استفاده شده برای تخمین فریب خود شامل خطای فریب است و فریب به طور دقیق تخمین زده نمی شود.

$$C_i(\tau) = \tilde{A}_i C(\tau - \tilde{\tau}_i) \cos(\tilde{\varphi}_l - \tilde{\varphi}_i) \quad (12)$$

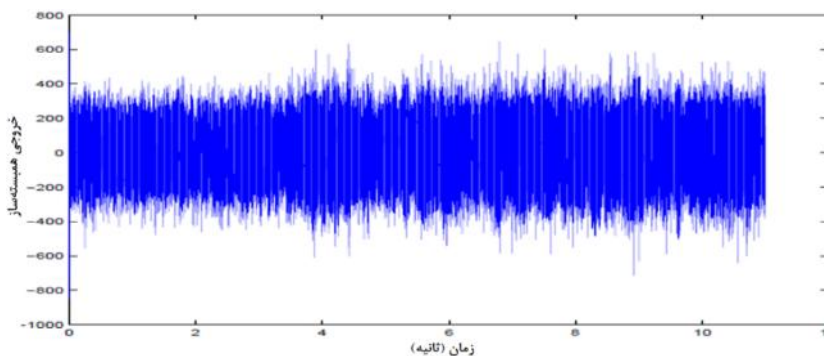


شکل (۵): بلوک دیاگرام راه کار پیشنهادی برای کاهش فریب.

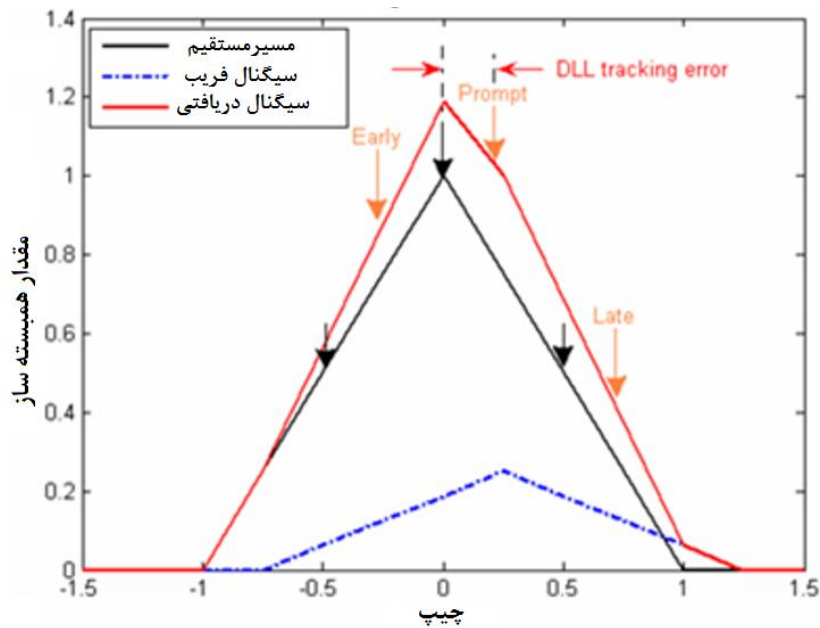
که در آن، $C(\tau)$ تابع خود همبستگی سیگنال کد ماهواره مربوطه است. در نتیجه، کل مقدار همبستگی سیگنال فریب تخمینی $C_i(\tau)$ با رابطه زیر قابل بیان است:



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



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



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

۴-۱- تخمین گر فریب بر پایه همبسته‌ساز چندگانه

که در آن، R_{XX} 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.

$$\Delta\tau = \frac{c}{T_c} \sqrt{\frac{N_{TLoop}d}{2C/N_0}}; \Delta\theta = \frac{\lambda}{2\pi} \sqrt{\frac{N_{TLoop}d}{2C/N_0}} \quad (17)$$

که در آن، c سرعت نور، C/N_0 نسبت حامل به نویز، N_{TLoop} پهنای باند نویز معادل حلقه ردیابی و d فاصله شاخه‌های ابتدایی و انتهایی است که این‌جا $2d$ در نظر 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 به عنوان خروجی تخمین می‌زند، سپس، با فیلتر حلقه هموار می‌شود. در نهایت، 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.

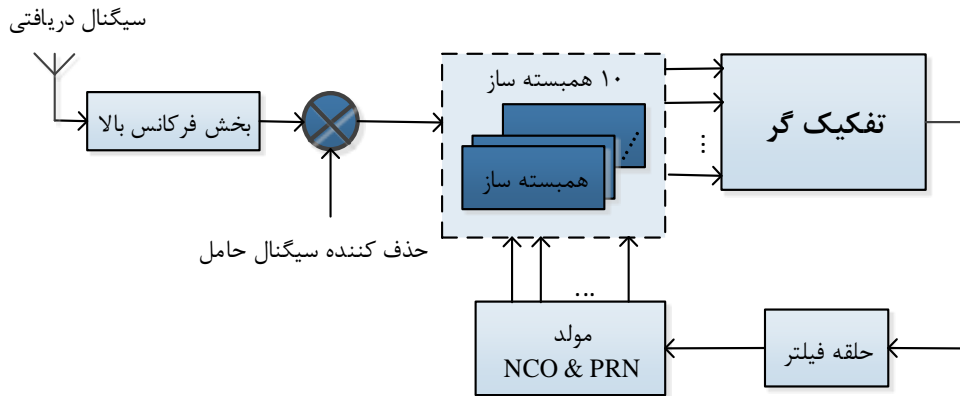
در کاهش فریب در مرحله پردازش سیگنال از راه‌کار همبسته‌ساز چندگانه مطابق شکل (۹) استفاده شده است [۲۳]. پس از تبدیل سیگنال RF به IF و حذف حامل از آن، سیگنال پردازش شده وارد بخش همبسته‌سازها می‌شود. تعداد بیشتر همبسته‌ساز کنترل حلقه ردیابی را آسان‌تر و دقیق‌تر می‌سازد. در برخی موقعیت‌ها تعدادی از این همبسته‌سازها 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 تأخیر یافته 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:

$$MSE(\hat{a}, \hat{\tau}, \hat{\theta}) = \int_{t-\tau}^t [r(t) - s(t)]^2 dt \quad (15)$$

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

$$\hat{\tau}_1 = \max_{\tau} \left[\text{Re} \left(R_{XX} - \sum_{x=1}^M \hat{a}_x R(\tau_1 - \hat{\tau}_x) \exp(j\hat{\theta}_x) \right) \exp(-j\hat{\theta}_1) \right] \quad (16)$$

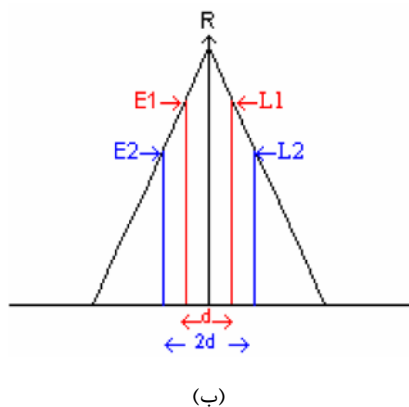
$$\hat{\theta}_1 = \arg \left[R_{XX}(\hat{\tau}_1) - \sum_{x=1}^M \hat{a}_x R(\tau_1 - \hat{\tau}_x) \exp(j\hat{\theta}_x) \right]$$



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

۴-۱-۲- همبسته ساز با کیفیت بالا

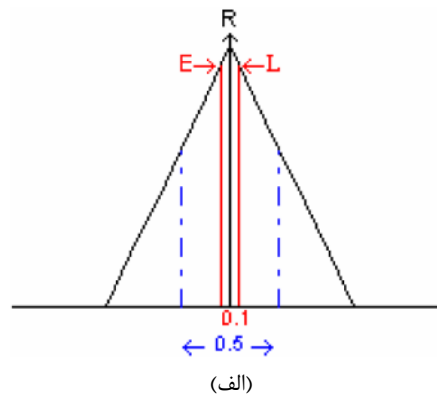
این نوع همبسته ساز از نوع همبسته ساز با تفاضل دوگانه است که برای کاهش فریب، دو همبسته ساز را به صورت موازی به کار می گیرد که در شکل (۱۰-ب) نشان داده شده است. این نوع از همبسته ساز در گروه همبسته سازها با خطای دو برابر شده قرار دارد که در توابع تفکیک کننده به جای یکی از دو همبسته ساز استفاده می کنند. همان طور که در شکل نیز مشاهده می شود، فاصله جفت دورتر دقیقاً دو برابر جفت نزدیک تر است. جفت همبسته ساز نزدیک دارای فاصله چپ ۰/۱ چپ و همبسته ساز دورتر، فاصله چپ ۰/۲ دارد. لازم به ذکر است که تفکیک کننده های کد براساس یک ترکیب خطی از همبسته سازها هستند.



(ب)

۴-۱-۱- همبسته ساز باند باریک

استفاده از فاصله چپ ۰/۱ در حلقه قفل فاز به GPS های اولیه برمی گردد، زیرا که برای به حداقل رساندن سخت افزار یک راه مناسب بود. در این تحقیق، ایده همبسته ساز باند باریک گسترش داده شده است. به جای استفاده از همبسته ساز استاندارد با فاصله چپ یک بین شاخه های اولیه و نهایی، یک همبسته ساز باند باریک با فاصله کمتر از ۱ چپ استفاده گردیده است تا تابع تفکیک کننده ساخته شود. بعد از بررسی های متعدد مقدار ۰/۱ چپ 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.



(الف)

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

کمینه کردن تابع هزینه، وزن های فیلتر با رابطه زیر بهینه می شوند:

$$L(n) = \|y(n) - \tilde{y}(n)\|^2 \quad (18)$$

بهینه سازی از نقطه نظر آماری به تئوری فیلتر وینر منجر می شود که یک نقطه کمینه قابل محاسبه با رابطه زیر را دارد:

$$\zeta = E[e(n)^2] \quad (19)$$

۴-۲- الگوریتم تطبیقی

در کاربردهایی که گیرنده متحرک است مانند کشتی و کامیون ها، همبسته ساز چندگانه پاسخ مناسبی ندارد و با گذشت زمان خطای مکان یابی افزایش می یابد. برای به روزرسانی مداوم مکان یابی از الگوریتم تطبیقی استفاده گردید. بلوک دیاگرام الگوریتم تطبیقی در شکل (۱۱) قابل مشاهده است. خروجی فیلتر با اعمال وزن های مناسب تخمین زده می شود. به منظور

$$w(n+1) = w(n) + \mu \text{sign}(e(n))x(n) \\ = w(n) + \left(\frac{\mu}{|e(n)|}\right)e(n)x(n) \quad (25)$$

پس از همگرایی الگوریتم یادگیری پارامترهای تخمین زده شده، قابل حصول است. بعد از پردازش فیلتر تطبیقی خروجی همبستگی را به دو بخش معتبر و فریب تفکیک می‌کند. در نهایت، پارامترهای تخمینی برای محاسبه همبستگی سیگنال معتبر به دست 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 ایجاد شده در I و Q باعث ایجاد خطای کد و فاز و در نتیجه، خطای ردیابی می‌شود. این خطا گیرنده را در روند موقعیت‌یابی فریب می‌دهد. ذخیره‌سازی و تأخیر در سیگنال حقیقی GPS به منظور تولید فریب در گذشته بررسی شده است [۲].

می‌دانیم در صورت 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 جمع‌آوری شده، ابتدا از سیگنال معتبر دریافتی به مدت کافی نمونه‌برداری و سپس در فضای حافظه در دسترس ذخیره‌سازی کردیم و پس از ایجاد تأخیر مناسب، آن را 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 در نهایت، سیگنال منتشر شده 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، این کار تنها با استفاده از شبیه‌ساز سیگنال GPS امکان‌پذیر است. شکل (۱۲-ب) سیستم آزمایشگاهی

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 به دلیل 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.

$$e(n) = y(n) - \hat{y}(n) \quad (20)$$

$$\hat{y}(n) = w^T(n) * x(n) \quad (21)$$

که در آن، $w(n)$ و $x(n)$ به ترتیب از روابط (۲۲) و (۲۳) به دست می‌آید:

$$w_n = [w_0, w_1, w_2, \dots, w_k] \quad (22)$$

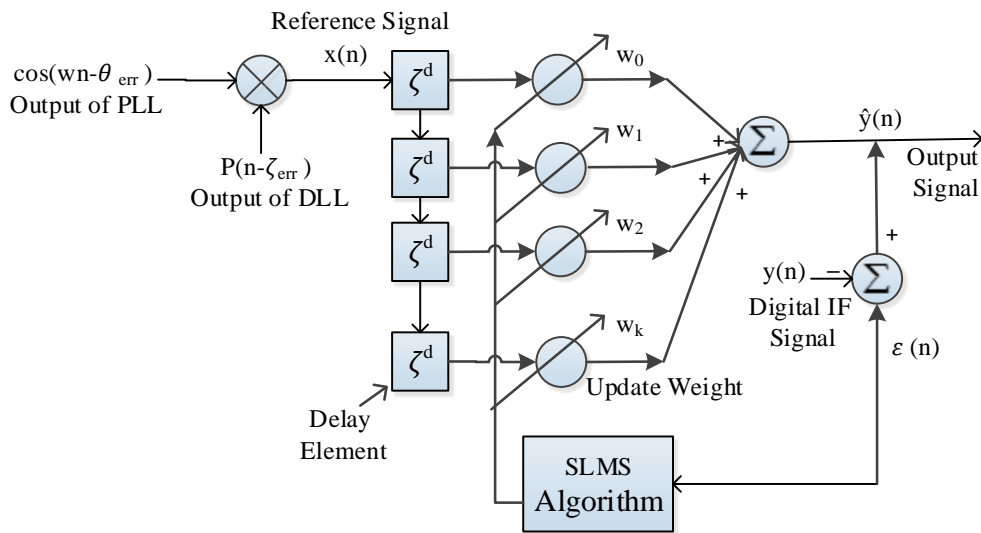
$$x(n) = [x(n), x(n-1), \dots, x(n-N+1)]^T \quad (23)$$

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

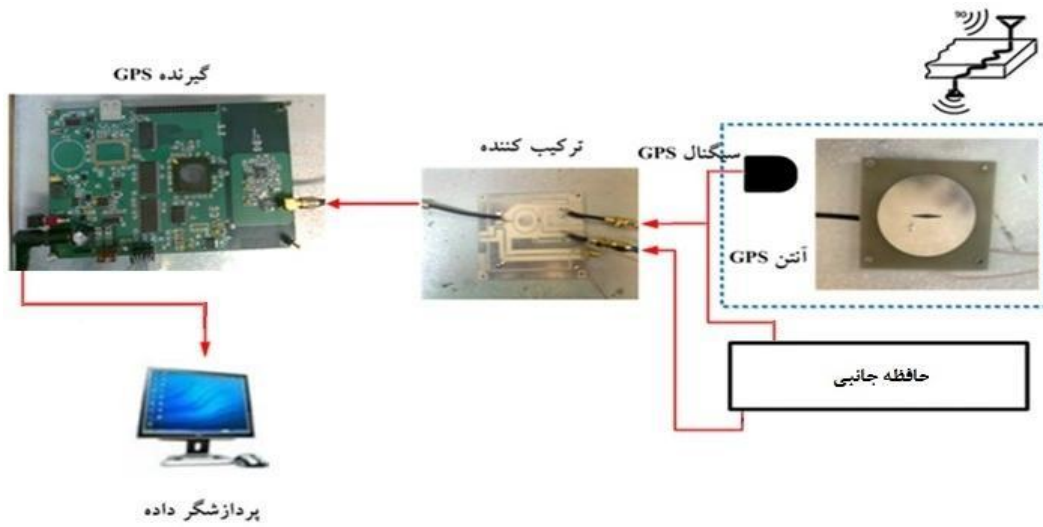
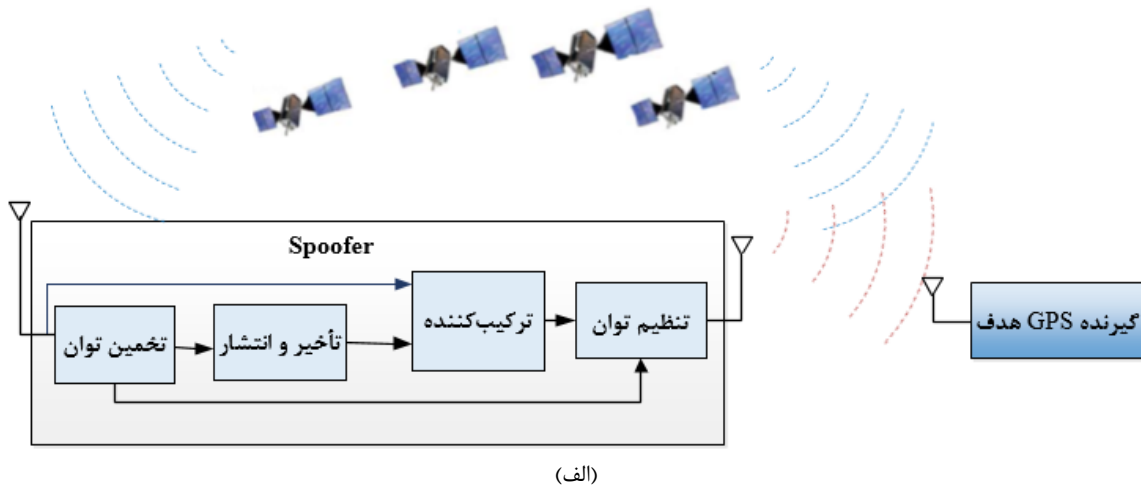
$$w(n+1) = w(n) + 2\mu e(n)x(n) \quad (24)$$

این الگوریتم بعد از همگرایی می‌تواند خطای فریب را کاهش دهد. به منظور بهبود کارایی الگوریتم LMS، نمونه‌های ارتقاء یافته‌های آن معرفی شده‌اند. با توجه به این که 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، هر چند که سرعت همگرایی بالایی دارد. الگوریتم $SLMS^1$ گام پیشرفت متغیری دارد. با نزدیک شدن 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.

مورد استفاده را نشان می‌دهد.



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



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

٪ حاصل شده است.

جدول (۵) مقایسه کمی بین دو تخمین گر پیاده سازی شده را نشان می دهد. مشاهده می گردد که راه کار پیشنهادی بر پایه تخمین گر تطبیقی توانسته است به طور میانگین ۹۳٪ خطای فریب آزمایشگاهی و ۸۷٪ خطای اندازه گیری را کاهش دهد. در حالی که راه کار پیشنهادی بر پایه تخمین گر باند باریک خطای مکان بانی داده آزمایشگاهی را بطور میانگین ۹۵٪ و خطای فریب داده اندازه گیری را ۸۹٪ کاهش داده است. به این ترتیب، می توان نتیجه گرفت که الگوریتم پیشنهادی بر پایه تخمین گر تطبیقی کارآیی بهتری دارد.

۶- مقایسه روش پیشنهادی با روش های موجود

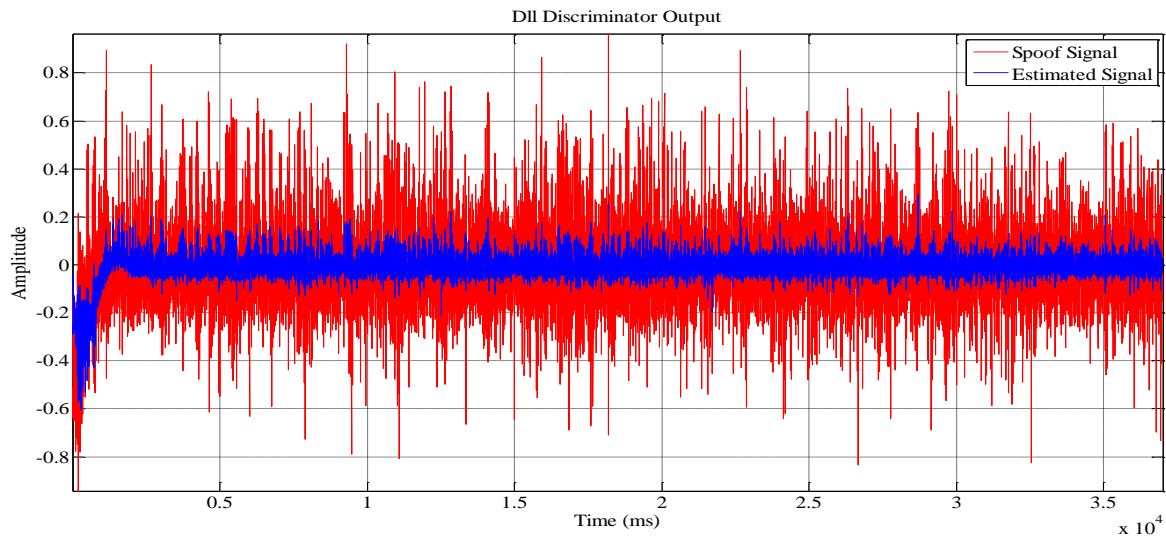
با توجه به این که مقالات موجود در حوزه فریب نتایج کمی از نتیجه کار خود ارائه نداده اند، امکان مقایسه درصدی روش پیشنهادی با نمونه های موجود وجود ندارد. جدول (۷) مقایسه ای تحلیلی بین روش های پیشین و الگوریتم پیشنهادی بر پایه تجهیزات مورد استفاده، مزایا و محدودیت ها ارائه می نماید. به منظور مقایسه و قضاوت صحیح بین روش های موجود امتیازدهی انجام می دهیم. به این ترتیب که برای هر ویژگی بهترین و بدترین حالت در نظر می گیریم. بسته به این که وضعیت الگوریتم در رابطه با آن ویژگی به چه شکلی باشد، به این ویژگی در الگوریتم از ۰ تا ۱۰ امتیاز تعلق می گیرد. به عنوان مثال، برای ویژگی تجهیزات لازم، اگر روشی هیچ سخت افزار اضافی لازم نداشته باشد، امتیاز ۱۰ و اگر نیاز به تغییر اساسی در ساختار گیرنده باشد، امتیاز صفر تعلق می گیرد. معیار امتیازدهی مقادیر ارائه شده در [۲۴] می باشد که در آن نیز مقایسه به همین نحو انجام شده است. ملاحظه می شود که روش پیشنهادی با ۲۵ امتیاز بهترین کارآیی را از خود نشان می دهد.

در روش الگوریتم تطبیقی، از لحاظ پیچیدگی زمانی، مدتی که حلقه ردیابی پردازش انجام می دهد، ۱٪ افزایش می یابد. فیلترهای تطبیقی برای کاهش پیچیدگی محاسباتی از تبدیل فوریه استفاده می کنند. پیچیدگی محاسباتی الگوریتم تطبیقی پیشنهادی از درجه N است که برابر با طول فیلتر مورد استفاده تعریف می گردد و در این جا، ۱۰ در نظر گرفته شده است. ملاحظه می گردد که روش پیشنهادی از کارآیی مطلوبی در مقایسه با دیگر روش ها برخوردار است. محدودیت بارز آن، عدم پاسخ مناسب در برابر فریب هماهنگ است.

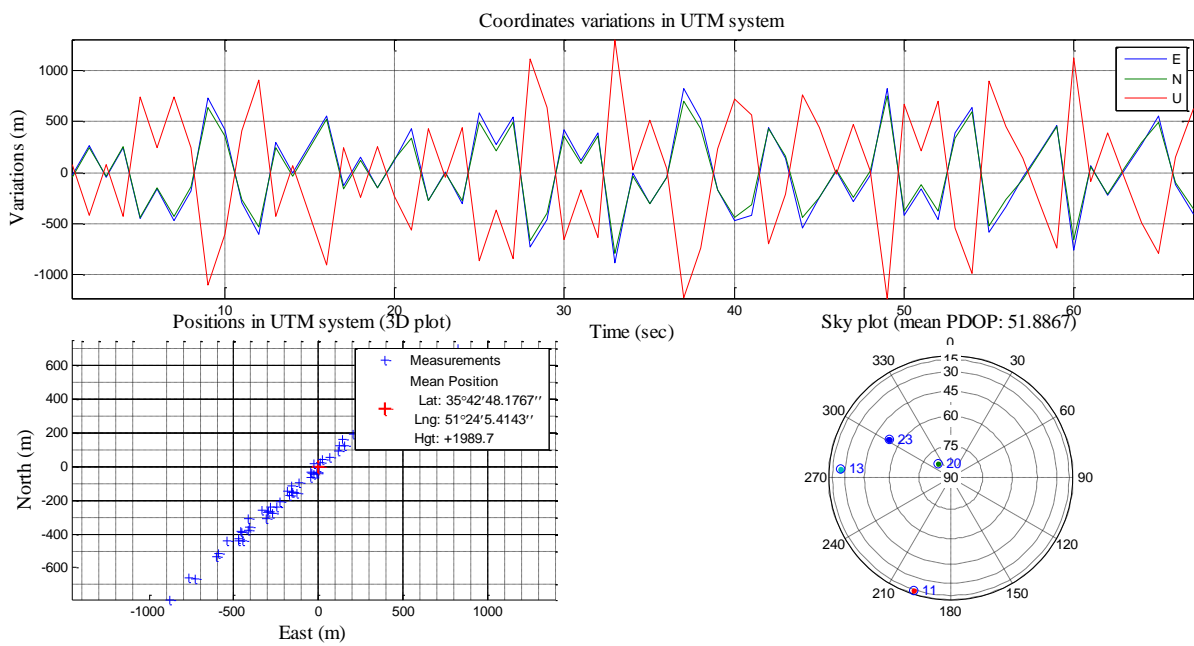
شکل (۱۳) خروجی نمونه حلقه DLL قبل و بعد از اعمال الگوریتم ضد فریب بر روی داده فریب نمونه را نشان می دهد. همان طور که ملاحظه می شود خطای خروجی همبسته سازها بعد از اعمال الگوریتم در باز ۰/۱ محدود شده است. در حالی که برای داده فریب بازه تغییرات در سیگنال فریب در بازه ۰/۸ است. متوسط قدر مطلق داده معتبر ۰/۳ با انحراف معیار ۰/۰۹ به دست 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، زیرا که مقدار خروجی حلقه در عرض ۲ ثانیه به تعادل رسیده است.

اشکال (۱۴-۱۵) یک نمونه پاسخ ناوبری را به ترتیب قبل و بعد از اعمال الگوریتم ضد فریب نشان می دهند. نمودار بالایی در شکل ها مربوط به تغییرات مختصات جغرافیایی در هر سه بعد است. نمودار پایین سمت چپ تغییرات مختصات به دست آمده در سطح افق را نشان می دهد و نمودار سمت راست پایین در رابطه با ماهواره های در دید می باشد. همان طور که از شکل (۱۴) مشخص است، تغییرات مکان بانی در بازه حدود ۸۰۰ متر می باشد که بعد از اعمال الگوریتم ضد فریب، مطابق شکل (۱۵) این مقدار به ۱۰۰ متر کاهش یافته است. در سطح افق نیز سیگنال فریب موجب شده که گیرنده هدف متحرک به نظر برسد، در حالی که بعد از اعمال روش پیشنهادی مشابه سیگنال معتبر اصلی داده ساکن استخراج شده است.

مجموعه داده آزمایشگاهی شامل پنج داده فریب و مجموعه داده اندازه گیری شامل سه داده فریب هستند. جداول (۱-۴) نتایج اعمال الگوریتم بر پایه دو تخمین گر متفاوت را بر روی هر دو مجموعه داده اندازه گیری و نرم افزاری نشان می دهند. برای بررسی دقیق تر مقدار خطا قبل و بعد از اعمال الگوریتم در دو بعد افق و ارتفاع نیز گزارش شده است. جداول (۱-۲) نتایج اعمال الگوریتم ضد فریب با تخمین گر کیفیت بالا را به ترتیب برای داده های آزمایشگاهی و اندازه گیری گزارش می کنند. متوسط کاهش خطا برای داده های آزمایشگاهی ۹۰٪ و برای داده های اندازه گیری ۸۳/۵٪ حاصل شده است. نویز بیشتر در داده های اندازه گیری دقت الگوریتم را کاهش داده است. جداول (۳-۴) نتایج اعمال الگوریتم ضد فریب با تخمین گر باند باریک برای داده های آزمایشگاهی و اندازه گیری را نشان می دهند. متوسط کاهش خطا برای داده های آزمایشگاهی ۹۲٪ و برای داده های اندازه گیری ۸۸٪



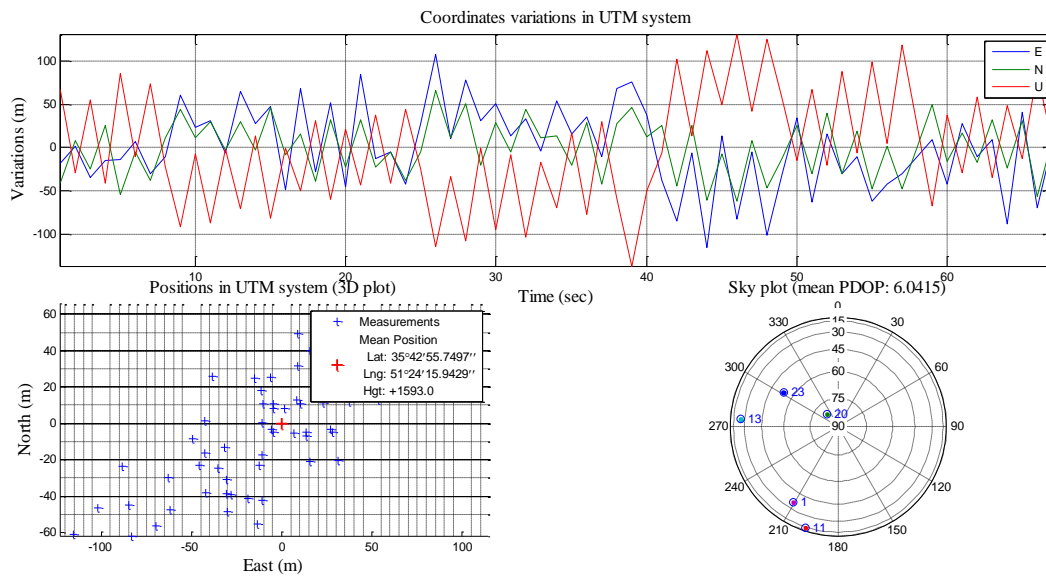
شکل (۱۳): خروجی حلقه DLL قبل و بعد از اعمال الگوریتم ضد فریب.



شکل (۱۴): نتایج ناوبری داده‌های دارای فریب.

جدول (۱): نتایج اعمال الگوریتم ضد فریب با تخمین گر 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 تخمین گر 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 تخمین گر 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 تخمین گر 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 تخمین گر پیشنهادی در الگوریتم ارایه شده.

داده اندازه گیری (%)		داده آزمایشگاهی (%)		روش ها
متوسط کاهش	بازه تغییرات	متوسط کاهش	بازه تغییرات	
۸۷	۱۸	۹۳	۱۷	همبسته ساز چندگانه
۸۹	۱۲	۹۵	۸	تطبیقی

جدول (۶) جمع بندی ویژگی های راه کار پیشنهادی.

پارامتر	ویژگی مربوطه
محل اعمال الگوریتم	حلقه ردیابی
متغیر مورد بررسی	خروجی همبسته سازها
پیچیدگی زمانی الگوریتم تطبیقی	۱٪ زمان شبیه سازی حلقه ردیابی
نوع فریب	فریب تأخیری
سیگنال GPS ورودی بخش ضد فریب	دوبیتی (۴ سطحی)
تخمینگرها	۱- همبسته ساز چندگانه و ۲- الگوریتم تطبیقی
تعداد همبسته ساز چندگانه	۱۰
فاصله همبسته سازها	۰/۱ چپ
الگوریتم تطبیقی	SLMS
متغیر استفاده شده برای ارزیابی	RMS خطای مکانی فریب بر حسب متر

جدول (۷): مقایسه روش های موجود کاهش فریب با راه کار پیشنهادی.

روش های تشخیص	محدودیت ها	مزیت ها	تجهیزات مورد نیاز	معیارهای بررسی شده	نمره نهایی
SQM	نیاز به داده قبلی، عدم کارایی در حملات هماهنگ (۲)	تشخیص آسان (۵)	ارتقا نرم افزاری (۶)	شاخه همبسته ساز (۵)	۱۸
VSD	ناکارآمد در حملات هماهنگ، نیاز به داده های قبلی (۵)	توانایی تفکیک چندمسیری (۷)	ارتقاء سخت افزاری و نرم افزاری (۳)	شاخه همبسته ساز (۴)	۱۹
گیرنده برداری	هزینه و پیچیدگی بالا (۳)	دقت تشخیص بالا (۸)	حلقه ردیابی اضافی (۲)	شاخه همبسته ساز (۳)	۱۶
ترکیبی	غیرقابل اطمینان در چندمسیری و بلادرنگ نبودن (۴)	امنیت بالا (۷)	ارتقاء نرم افزاری و سخت افزار اضافی (۲)	همبسته ساز و توان (۳)	۱۶
RAIM	غیرقابل اطمینان در شرایط بیش از دو ماهواره جعلی (۲)	پیاپی سازی آسان (۵)	ارتقاء نرم افزاری (۶)	شبه فاصله (۳)	۱۶
پردازش فضایی	غیرقابل اطمینان در حملات فریب پیچیده (۶)	قابلیت اطمینان بالا (۷)	ارتقاء نرم افزاری و سخت افزار اضافی (۰)	سیگنال IF (۵)	۱۸
کار پیشنهادی	نیاز به داده های قبلی (۵)	پیاپی سازی آسان، سریع و قابل اطمینان (۹)	ارتقاء نرم افزاری (۶)	همبسته ساز (۵)	۲۵

در برابر انواع مختلف حمله فریب، روش پیشنهادی بتواند کارایی قابل قبولی داشته باشد.

با توجه به امکانات موجود، در ارزیابی الگوریتم پیشنهادی تنها فریب تأخیری مورد استفاده قرار گرفت، اما به نظر می رسد

۷- نتیجه گیری

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

در بخش کاهش فریب همبستگی سیگنال به دست آمده با خود همبستگی سیگنال دریافتی جمع می‌شود تا همبستگی سیگنال GPS معتبر استخراج گردد. با استفاده از همبسته ساز باند باریک با فاصله چیپ ۰.۱ بین ۰ تا ۱ در قسمت ردیابی نرم افزار GPS، مشاهده شد که میزان خطای ناشی از فریب به میزان چشمگیری کاهش می‌یابد. متوسط میزان کاهش خطا برای داده‌های آزمایشگاهی ۹۵٪ و برای داده‌های اندازه گیری ۸۹٪ حاصل شد.

۸- منابع

- [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. Huang, 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.
- [1] A. Broumandan, A. Jafarnia-Jahromi, and G. Lachapelle, "Spoofing Detection, Classification and Cancellation (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.

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