جبران‌سازی خطای فریب تأخیری در GPS با کاهش خطای ردیابی مبتنی بر شبکه‌های عصبی

سیدمحمدرضا موسوی میرکلایی[1]، مریم معاضدی[2]، امیررضا بازیار[3]

۱.استاد دانشکده مهندسی برق، دانشگاه علم و صنعت ایران، m_mosavi@iust.ac.ir

۲. دانشجوی دکتری، دانشگاه علم و صنعت ایران

۳. کارشناسی ارشد، دانشگاه علم و صنعت ایران

تاریخ دریافت: ۹۳/۲/۲۳ تاریخ پذیرش: ۹۳/۱۲/۵

چکیده

امروزه فریب‌دهنده یک تهدید ثابت‌شده برای گیرنده‌های GPS محسوب می‌شود. نتیجه حمله فریب، خطاهای بزرگ ناوبری در گیرنده ناآگاه با نتایج زیان‌آور است. به دلیل این‌که سیگنال فریب از سیگنال اصلی تقلید می‌کند، گیرنده متوجه حضور آن نمی‌شود. از این رو تشخیص و جبران‌سازی آن سخت‌تر از دیگر اختلال‌های مطرح‌شده برای GPS است. در این مقاله سعی می‌شود روش‌های پیشنهادی برای جبران‌سازی فریب که در گیرنده‌های معمولی تک‌فرکانسه قابل استفاده‌اند، به طور کامل بررسی گردند. ابتدا روند کلی هر روش به طور مختصر توضیح داده می‌شود و سپس چالش‌ها و نقاط ضعف و قوت هر روش مورد مطالعه قرار خواهند گرفت. پس از آن یک ایده جدید و کاربردی برای کاهش اثر فریب مبتنی بر شبکه‌های عصبی مطرح می‌گردد که در آن شبکه عصبی پس انتشار خطا در حوزه تغییرات فاصله به منظور برآورد و جبران خطاهای ردیابی فاز و کد استفاده خواهد شد. ملاحظه می‌گردد که با بهره‌گیری از شبکه عصبی خطای مکان‌یابی ناشی از فریب بر روی سه مجموعه داده با میانگین ۸۲ درصد و دامنه تغییرات حدود ۲ درصد کاهش می‌یابد.

کلیدواژه

گیرنده‌های تک‌فرکانسه GPS، حمله فریب، کاهش فریب، شبکه‌های عصبی، حلقه ردیابی.

مقدمه

هر نوع حمله فریب متناسب با روش مورد استفاده و دقت عملکرد آن، محدوده مشخصی به عنوان ناحیه هدف دارد. مشخصات سیگنال فریب تولیدی در این ناحیه، در حد قابل قبولی با نمونه معتبر تطابق دارد و در نتیجه گیرنده از حضور آن بی‌خبر می‌ماند. هرچند اغلب گیرنده‌های GPS قادرند فریب‌هایی را که در خارج از ناحیه هدف قرار دارند، شناسایی نمایند. اما در فضای محدود به ناحیه هدف گیرنده قادر به تفکیک سیگنال‌های معتبر و جعلی نیستند و با توجه به توان بزرگ‌تر سیگنال فریب، آن را به جای سیگنال اصلی ردیابی و پردازش می‌کنند[۱]. برای حل مشکلاتی از این قبیل، مطالعات گسترده‌ای در حال انجام است و روش‌های متنوعی برای مقابله با فریب ارائه و نمونه‌های عملی آن ساخته شده‌اند[۲]. قدم نخست در این مسیر شناسایی فریب و به عبارتی تشخیص وجود سیگنال فریب است. پس از آن‌که حمله فریب آشکار شد، مرحله بعد که قدم اصلی نیز می‌باشد، جبران‌سازی یا کاهش آن است. با توجه به آثار تخریبی که حمله فریب در گیرنده و بر روی سیگنال معتبر ایجاد می‌کند، شناسایی سیگنال فریب نسبت به جبران‌سازی آن دست‌یافتنی‌تر به نظر می‌رسد. نسبت بیشتر روش‌های ارائه‌شده برای شناسایی به نمونه‌های کاهش فریب، این ادعا را ثابت می‌کند[۳]. از این رو مطالعه در زمینه جبران‌سازی حمله فریب زمینه تحقیقاتی مناسبی برای پژوهشگران محسوب می‌شود.

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 مطرح شدن روش‌ها باشد تا روند بهبود و تکامل تکنیک‌های کاهش فریب توسط خواننده به طور مشهودی درک گردد. سپس به بحث در رابطه با کاربرد شبکه عصبی در حوزه تغییرات فاصله و عوامل مهم تأثیرگذار بر عملکرد آن پرداخته می‌شود. پس از آن به منظور کاهش اثر سیگنال‌های جعلی در محدوده تغییر فاصله استفاده از شبکه‌های عصبی پیشنهاد شده است. بخش دوم معماری سیستم ناوبری GPS، موقعیت شبکه عصبی در سیستم و مباحث مرتبط با آن را توصیف می‌کند. در بخش سوم معماری شبکه عصبی و نحوه پیش‌پردازش داده‌های آموزش توضیح داده می‌شوند. قوانین آموزش در این بخش تشریح خواهند شد. در بخش چهارم نیز برخی از نتایج شبیه‌سازی را ارائه نموده‌ایم.

مروری بر روش‌های مقابله با فریب

برای حل مشکل حمله فریب در GPS مطالعات گسترده‌ای در حال انجام است و روش‌های متنوعی برای مقابله با فریب ارائه و نمونه‌های عملی آن ساخته شده است[۴-۱۷]. قدم نخست در این مسیر شناسایی فریب و به عبارتی تشخیص وجود سیگنال فریب است. پس از آن‌که حمله فریب آشکار شد، مرحله بعد که قدم اصلی نیز می‌باشد، جبرانی‌سازی یا کاهش آن است. در این بخش روش‌های کاهش فریب به اجمال بررسی می‌شوند.

تخمین سیگنال معتبر

بخشی از روش‌های موجود مقابله با فریب که در ابتدای تحقیقات در این زمینه بیشتر مورد توجه واقع شد، بر مبنای مقایسه و بررسی مداوم اطلاعات داخلی و خارجی و تخمین سیگنال معتبر در صورت تشخیص وجود حمله، عمل می‌کنند[۴-۸]. به عنوان مثال بلوک دیاگرام شکل ۱، نمونه‌ای از روش تخمین با شبکه عصبی را نشان می‌دهد[۶]. اساس کار بر مقایسه مقدار شبه فاصله اندازه‌گیری‌شده و اطلاعات گیرنده تفاضلی[۱] (DGPS) استوار است که به عنوان ورودی شبکه عصبی عمل می‌کند. وظیفه این شبکه تشخیص وجود فریب است که در واقع مرحله آشکارسازی محسوب می‌شود. پس از تشخیص وجود فریب، شبه‌فاصله جبران‌شده در مرحله جبران‌سازی، محاسبه خواهد شد. اگر سیگنال GPS مورد فریب قرار گیرد، شبه‌فاصله تغییر می‌کند و خطا ایجاد می‌نماید. این تغییر در نرخ تغییرات شبه‌فاصله اثر می‌گذارد. ولی خطای ناشی از فریب در اطلاعات ارسالی از مکان ماهواره و مکان ایستگاه تأثیر ندارد. اگر فواصل زمانی بین اندازه‌گیری‌ها به اندازه کافی کم باشد خطاهای یونسفری، تروپسفری و ساعت گیرنده قابل چشم‌پوشی هستند. از آنجایی که ایستگاه DGPS اطلاعات درست مکانی ایستگاه و مدار ماهواره را در اختیار دارد، می‌تواند فاصله بین ماهواره و گیرنده را محاسبه کند. در مرجع[۷] نیز تحقیق مشابهی با فیلتر کالمن انجام شده است.

در مرجع[۸] برای گیرنده دو حالت عملکردی طراحی شده است. در شرایط عادی اطلاعات دریافتی خود را معتبر می‌داند و در حالت هوشیار[۲] اطلاعاتی را که از تخمین‌گر پیش‌بینی‌کننده خود دریافت می‌کند، برای مکان‌یابی مورد استفاده قرار می‌دهد. وقتی که علائم مشکوک از بین رفت، به حالت عادی برمی‌گردد. پیش‌بینی در این سیستم نیز توسط فیلتر کالمن و حسگرهای داخلی انجام می‌شود. فیلتر کالمن تخمین دقیق‌تری را نتیجه می‌دهد و با گذشت زمان و طولانی شدن حالت هوشیار خطای کمتری ایجاد می‌کند. پارامترهایی که توسط این روش تخمین زده می‌شوند، عبارتند از مکان، آفست کلاک و اثر داپلر. پارامتر داپلر نتیجه بهتری دارد، زیرا تغییرات آن آرام‌تر است و امکان پیش‌بینی آن با خطای ثابت و کوچک در دوره طولانی‌تری از زمان وجود دارد در حالی‌که خطای مکان به صورت نمایی افزایش می‌یابد. به این ترتیب گیرنده هدف در صورت تشخیص حمله فریب با پیش-بینی مقدار اثر داپلر فرکانس سیگنال خود را متناسب با آن تغییر می‌دهد. علاوه‌برآن چون فریب‌دهنده روی زمین قرار دارد و با سرعت کمتر از ماهواره حرکت می‌کند، نمی‌تواند اثر داپلر یکسانی با سیگنال اصلی ایجاد کند. مگر این‌که فرکانس انتقال خود را برای تطبیق با یکی از گیرنده‌ها تغییر دهد که در این صورت با حمله پیچیده روبه‌رو هستیم.

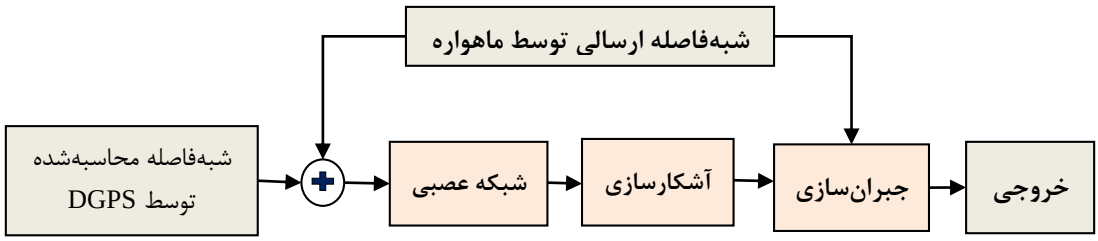
جبران‌سازی فریب با استفاده از پردازش فضایی

به دلیل محدودیت‌های عملی، اغلب فرستنده‌های فریب چندین سیگنال جعلی را از یک آنتن می‌فرستند. این در حالی است که سیگنال‌های معتبر GPS از ماهواره‌های مختلف در مسیرهای گوناگون فرستاده می‌شوند. ازاین‌رو می‌توان روش پردازش فضایی را برای تخمین اثر سه بعدی سیگنال‌های دریافتی و تفکیک این سیگنال‌ها که رابطه فضایی مشخصی دارند، به‌کار گرفت[۹-۱۵]. بر مبنای این واقعیت، روش زاویه ورود یکی از روش‌های معتبر و معمول برای شناسایی و کاهش فریب محسوب می‌شود. برای اجرای این روش به داشتن آرایه‌ای از آنتن‌ها نیاز است. یک آرایه آنتن می‌تواند توزیع فضایی سیگنال دریافتی را تخمین بزند و سیگنال رسیده از فرستنده معتبر را از نمونه جعلی تفکیک کند. در ادامه سه روش متفاوت برای پیاده‌سازی آرایه مورد نیاز شرح داده می‌شود.

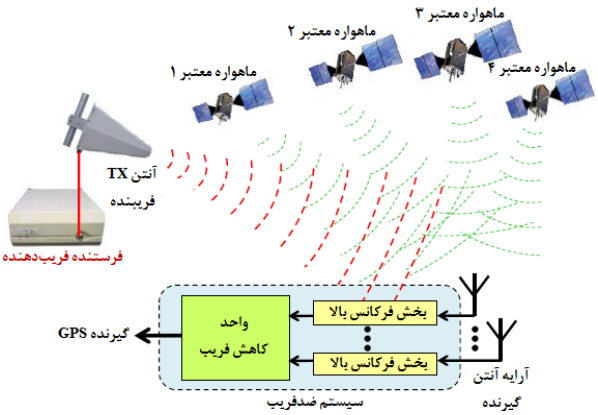
آرایه چندآنتنه

یک گیرنده چند آنتنه می‌تواند روش‌های پردازش آرایه‌ای را به‌دلیل شکل‌دهی پرتو به‌کار گیرد و بعد از آشکارسازی مسیر سیگنال فریب‌دهنده، این گیرنده می‌تواند یک صفر را به سمت منبع فریب هدایت کند و اثر مخرب آن را متوقف کند. در مرجع[۱۲] روشی ارائه شده است که می‌تواند به‌طور مؤثر سیگنال‌های فریب را بعد از تعیین همبستگی فضایی بین جفت سیگنال‌های دریافتی، خنثی کند. ازاین‌رو بردار بهره مناسب می‌تواند بعد از پردازش نسخه تمام سیگنال‌های باریک باند فریب و معتبر دریافتی، به‌دست آید. شمای کلی سیستم و اجزای داخلی بلوک مقابله با فریب به ترتیب در شکل‌های ۲ و ۳ نشان داده شده‌اند.

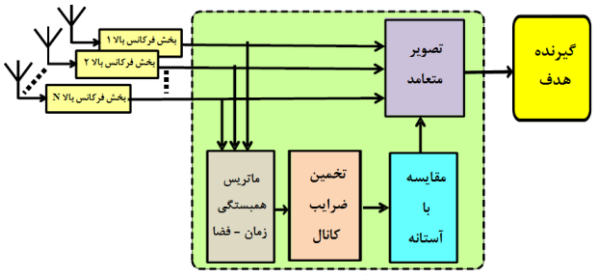
1.Differential GPS
2.Alert Mode



شکل۱. بلوک دیاگرام روش جبران فریب با تخمین توسط شبکه عصبی[۵].



شکل۲. سیستم ضدفریب نمونه با آرایه آنتنی [۱۲].



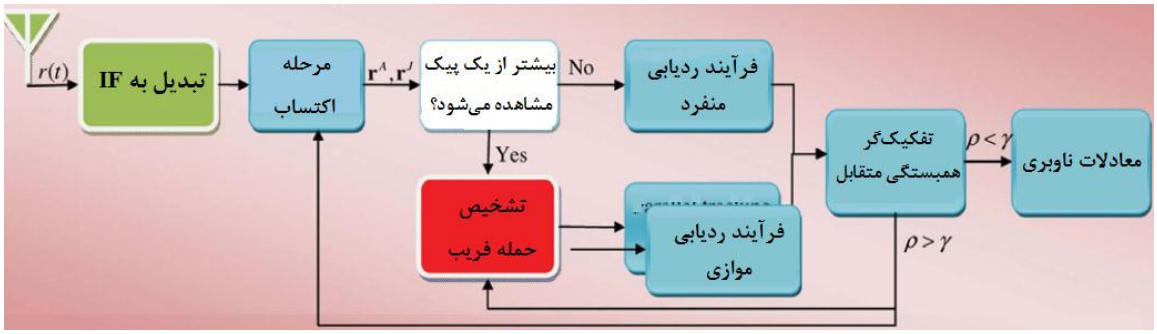
شکل۳. بخش داخلی سیستم مقابله با فریب [۱۲].

منطقه مبهم الگوی پرتو آنتن به نسبت زیادی با افزایش تعداد عناصر آرایه کاهش می‌یابد. البته این روش کاهش فریب ممکن است در حالت فریب پیچیده چندآنتنه کارآیی نداشته باشد. درکنار کارآیی نامناسب، این روش پیچیدگی پردازشی و سخت‌افزاری گیرنده را به‌طور قابل ملاحظه‌ای افزایش می‌دهد.

آرایه دو آنتنه

در مرجع[۱۳]یک روش کاهش فریب دو آنتنه با پیچیدگی بسیار کم محاسباتی پیشنهاد شده است که قادر به فیلتر فضایی سیگنال‌های فریب می‌باشد. این روش همبستگی متقابل سیگنال‌های دریافتی از آنتن‌های مختلف را محاسبه می‌نماید. در مرحله بعد با شناسایی هر یک از سیگنال‌ها و بررسی اثر فضایی، سیگنال‌های فریب را مبنی بر نفوذ توان فضایی‌شان استخراج می‌کند. لازم به ذکر است که تمام عملیات پردازشی بر روی نمونه‌های اولیه سیگنال و قبل از باند باریک کردن سیگنال‌های معتبر و فریب انجام می‌گردد. فرض می‌شود که ماژول فریب‌دهنده چندین سیگنال PRN ارسال می‌کند که هر یک از آن‌ها سطح توان قیاس‌پذیر نسبت به سیگنال معتبر دارند.

در این شرایط بردار هدایت مشابه به سیگنال‌های فریب می‌تواند استخراج شود، زیرا تمام سیگنال‌های فریب از مسیر یکسان می‌آیند. این روش به آرایه کالیبراسیون یا هر اطلاعات قبلی راجع به آرایه جهت‌یابی آنتن نیاز ندارد و می‌تواند به‌عنوان یک آنتن سری مستقل ترکیب‌شده با بلوکی که سیگنال‌های فریب را قبل از ورود به گیرنده‌های متعارف GPS کاهش می‌دهد، استفاده شود. تا زمانی‌که توان سیگنال فریب به‌طور قابل ملاحظه‌ای از توان میانگین سیگنال‌های معتبر بیشتر باشد، این روش با موفقیت اثر سیگنال‌های فریب را کاهش می‌دهد.



شکل۴. بلوک دیاگرام کلی گیرنده دستی متحرک به همراه بخش ضدفریب[۱۴].

آرایه مصنوعی[3] تک آنتنه متحرک

گیرنده‌های دستی عموماً در معرض اختلال چندمسیری قرار دارند. علاوه برآن امکان نصب آرایه آنتنی در آن‌ها به دلیل محدودیت‌های هزینه و اندازه وجود ندارد. با این وجود، با تغییر مکان آنتن گیرنده منفرد در طول یک بازه زمانی کوتاه می‌توان آرایه آنتن مصنوعی تولید نمود. بلوک دیاگرام گیرنده دستی قابل حمل به‌همراه سیستم ضدفریب در شکل ۴ قابل مشاهده است. در مرجع[۱۴]گیرنده دستی قابل حمل به طور تصادفی جابجا شده و در هر لحظه سیگنال‌های GPS دریافت و ذخیره می‌گردند. مجموعه داده‌هایی که به این روش جمع‌آوری می‌شوند، با برخی ملاحظات اضافی می‌توانند به عنوان داده حاصل از آرایه آنتن چندمسیری تلقی شده و برای تفکیک سیگنال معتبر و جعلی مورد استفاده قرار گیرند.

بررسی صحت استقلال گیرنده[4] (RAIM) گسترش‌یافته

شپارد[5] در مرجع[۱۶] نشان داد که تداخل بین بیشینه همبستگی سیگنال اصلی و سیگنال فریب بسیار شبیه به تداخل چندمسیری و مسیر مستقیم است. بنابراین روش‌های آشکارسازی و کاهش چندمسیری می‌توانند برای فریب نیز مورد استفاده قرار گیرند. به عنوان نمونه بررسی کیفیت سیگنال[6] (SQM) یک روش آشکارسازی چندمسیری است که برای آشکارسازی حملات فریب بر روی گیرنده‌های ردیابی به کار برده شده است. لدوینیا[7] در سال ۲۰۱۰ آزمون‌های SQM را برای آشکارسازی فریب استفاده کرد و روش نظارت یکپارچه مستقل گسترش‌یافته را برای آشکارسازی و کاهش فریب در سطح ناوبری و مسائل مکان‌یابی ارائه داد[۱۷]. روش RAIM دفاعی عملی در مقابل خطای اندازه‌گیری شبه‌فاصله در گیرنده GPS مستقل است که از طریق فرضیه آماری، اندازه‌گیری شبه‌فاصله تک خطایی را آشکار و از مسئله ناوبری خطای اندازه‌گیری را حذف می‌کند. تا حد زیادی، کار تئوری و عملی برروی توسعه و آزمون سیستم‌های RAIM انجام شده است. دقت زیربنای RAIM و تأکید آن بر آزمون فرضیه آماری، آزمون‌های مشابه RAIM را برای آشکارسازی و کاهش فریب گسترش داده است.

روش RAIM استاندارد، با هدف آشکارسازی اندازه‌گیری فرکانس داپلر معیوب یا شبه‌فاصله غلط یا هر دو گسترش یافته است. آشکارسازی و کاهش فریب توسط RAIM گسترش‌یافته، زمانی رخ می‌دهد که این اندازه‌گیری‌ها به‌طور عمد غلط یا از دست رفته باشند. گسترش RAIM بر پایه روش حداقل مربعات وزن‌دار بنا شده است و با معادله اندازه‌گیری شبه‌فاصله خطی‌شده اساسی شروع می‌شود.

$$\vec{y} = H\vec{x} + \vec{v} \qquad (۱)$$

که در آن $\vec{y}$ بردار N×1 از اندازه‌گیری‌های شبه‌فاصله، H ماتریس انتقال اندازه‌گیری خطی N×4، $\vec{x}$ بردار حالت مجهول 4×1 و $\vec{v}$ بردار نویز اندازه‌گیری N×1 با کوواریانس P_v است. فرض بر این است که $\vec{v}$ ناهمبسته و گوسی با میانگین صفر باشد. برآورد حداقل مربعات به‌صورت زیر است:

$$\hat{x} = (H^T P_v^{-1} H)^{-1} H^T P_v^{-1} \vec{y} \qquad (۲)$$

برای اندازه‌گیری‌های حامل داپلر با انتقال فرکانسی نیز فرض می‌شود معادله اندازه‌گیری خطی‌شده شامل یک سیستم از پیش تعیین شده از معادلات است.

$$\vec{y}_D = H_D \vec{x}_D + \vec{v}_D \qquad (۳)$$

که فرض می‌شود تعداد المان‌ها در $\vec{y}_D$ با تعداد المان‌ها در $\vec{y}$ برابر است. H_D، ماتریس انتقال اندازه‌گیری خطی‌شده برای معادله اندازه‌گیری حامل داپلر با انتقال فرکانسی است. $\vec{x}_D = [\Delta\dot{x}; \Delta\dot{y}; \Delta\dot{z}; c\Delta\dot{\delta}_R]$ بردار حالت بوده و $\vec{v}_D$ بردار نویز اندازه‌گیری با کوواریانس $P_{v,D}$ است. خطای باقیمانده برای اندازه‌گیری‌های شبه‌فاصله به‌صورت زیر به‌دست می‌آید:

$$\vec{w} = \left[I - (H^T P_v^{-1} H)^{-1} H^T P_v^{-1} \right] \vec{y} \qquad (۴)$$

که در آن I ماتریس یکانی است. خطای باقیمانده برای اندازه‌گیری‌های حامل داپلر با انتقال فرکانسی نیز به‌صورت زیر به‌دست می‌آید:

$$\vec{w}_D = \left[I - (H_D{}^T P_{v,D}{}^{-1} H_D)^{-1} H_D{}^T P_{v,D}{}^{-1} \right] \vec{y}_D \qquad (۵)$$

آزمون آماری که نرمال‌شده مجموع مربعات باقیمانده خطا است، برای شبه‌فاصله و اندازه‌گیری‌های حامل داپلر با انتقال فرکانسی به‌صورت زیر تعریف می‌شود:

$$SSE_{PD} = \vec{w}^T P_v^{-1} \vec{w} + \vec{w}_D{}^T P_{v,D}{}^{-1} \vec{w}_D \qquad (۶)$$

که SSE_{PD} نرمال‌شده توزیع χ^2 با 2N-8 درجه آزادی است که N تعداد شبه‌فاصله‌ها یا اندازه‌گیری‌های حامل داپلر با انتقال فرکانسی می‌باشد. برای اجرا شدن آزمون آشکارسازی RAIM گسترش‌یافته باید یک آستانه تشخیص مناسب محاسبه شود. ممکن است این روش برای آشکارسازی و ممانعت از بیش از یک سیگنال جعلی گسترش یابد، اما در حال حاضر محدوده تحقیقات تا همین

3.Synthetic Array
4.Receiver Autonomous Integrity Monitoring
5.Shepard
6.Signal Quality Monitoring
7.Ledvina

جاست. به طور خلاصه نمونه گسترش‌یافته RAIM، سیگنال ماهواره با خطای اندازه‌گیری حامل داپلر یا اندازه‌گیری شبه‌فاصله را آشکارسازی نموده و از آن ممانعت می‌کند[۱۷].

کاهش حملات فریب در گیرنده‌های GPS برداری[8] (VB)

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. با فرض این‌که گیرنده ابتدا بر روی بیشینه‌های همبستگی اصلی قفل شده است، حمله فریب سعی می‌کند گیرنده را از طریق دنبال‌کردن بیشینه‌های همبستگی غلط خودش فریب دهد. تداخل بین بیشینه‌های همبستگی سیگنال اصلی و فریب در حین حمله فریب، اندازه‌گیری‌های حلقه ردیابی محلی را غیرمعتبر می‌نماید. بنابراین فیلترکالمن در گیرنده‌های ردیابی، بردار اندازه‌گیری‌های شبه‌فاصله آن PRNهایی را که تحت حمله فریب هستند، نادیده می‌گیرد. اگرچه‌وابمعتبر برای مکان هنوز در دسترس باشد، نوسان‌سازهای کنترل‌شده عددی[9] (NCO) حلقه‌های ردیابی که توسط اندازه‌گیری‌های سطح ناوبری فریب داده شده‌اند، از گیرنده VBراه‌اندازی خواهند شد.

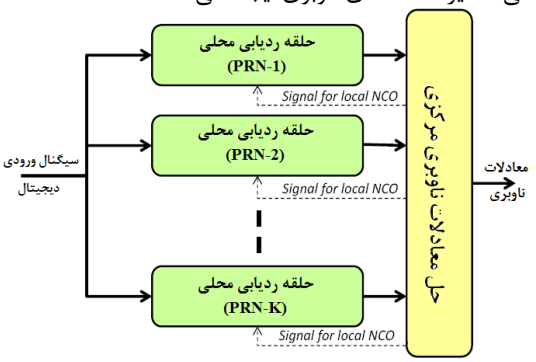
فریبنده مجبور است برای تصرف نقطه ردیابی گیرنده اصلی، بیشینه همبستگی خودش را از بیشینه همبستگی سیگنال اصلی دور نماید. این روش ضدفریب در این لحظه فریب را آشکار می‌کند و پس از آن گیرنده VB از اندازه‌گیری‌های حلقه‌های ردیابی کنار گذاشته شده استفاده می‌کند[۱۸]. به عبارتی دیگر گیرنده باید قادر باشد سیگنال اصلی از دست رفته را بازیابی نماید، که برای این هدف ساختار ردیابیVB به‌کار گرفته می‌شود. در حقیقت ایده اصلی این روش، ترکیب پاسخ ناوبری و تحمیل سیگنال ردیابی برای افزایش قدرت گیرنده‌های GPS و حفظ آن‌ها در برابر تداخل است.

شکل ۵ ساختار یک گیرنده VB زنجیره‌ای را نشان می‌دهد که می‌تواند سطح ناوبری و اندازه‌گیری‌های حلقه‌های ردیابی را برای راه‌اندازیNCO هر PRN جمع کند. گیرنده‌هایVB می‌توانند به‌طور کلی اندازه‌گیری‌ها را از حسگرهای متفاوت جمع‌آوری نمایند. بنابراین وقتی‌که تعدادی از اندازه‌گیری‌های اصلی به‌خاطر حمله فریب دارای خطا هستند،گیرنده VB هنوز می‌تواند براساس یک جواب ناوبری معتبر، NCOهای متشابه آن‌ها را راه‌اندازی و فاصله تداخل سیگنال اصلی و فریب را متصل نماید و سرانجام بیشینه همبستگی اصلی را بعد از این‌که بیشینه فریب دور شد، جبران کند.

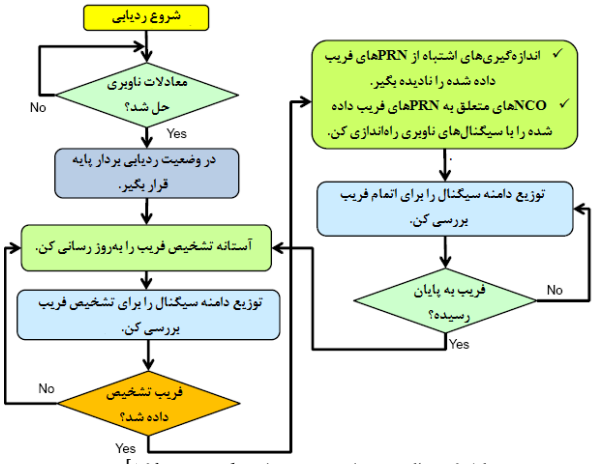
ساختار آشکارسازی فریب برروی خروجی‌های همبسته‌ساز و پرچم‌ها در حضور یک سیگنال فریب به‌محض مشاهده توزیع غیرعادی هر خروجی همبسته‌ساز، فعال می‌شود. ساختار کاهش فریب باید اندازه‌گیری‌های محلی را که از فیلترهای حلقه ردیابی می‌آید، نادیده بگیرد و از اندازه‌گیری‌های سطح ناوبری برای راه‌اندازیNCOها، استفاده کند. این حالت باقی می‌ماند تا زمانی‌که بیشینه همبستگی فریب دور شود و همبسته‌ساز به فرآیند ردیابی سیگنال اصلی بازگردد. شکل ۶ الگوریتم کاهش فریب را نشان می‌دهد[۱۹].

قاعده انتخاب بیشینه معتبر بر پایه اندازه‌گیری C/No[10]

مشخصه C/No یکی از معیارهایی است که در مقابله با فریب به طور معمول مورد استفاده قرار می‌گیرد[۲۰]. در این روش بررسی C/No با یک قاعده تصمیم‌گیری ادغام شده است. در فریب مورد استفاده در این روش که در مناطق شهری معمول است، مکان جعلی در ناحیه هدف تصادفی تغییر نماید. سیگنال فریب در ناحیه هدف، با مدولاسیون تصادفی فاز کد و اثر داپلر در بازه کوچکی از فضای کلی تأخیر کد، خطای ناوبری ایجاد می‌کند.



شکل۵. ساختار یک گیرنده VBزنجیره‌ای[۱۹].



شکل۶. عملکرد ضدفریب پیشنهادی گیرندهVB[۱۹].

8.Vector-Based
9.Numerically Controlled Oscillators

10.Carrier to Noise

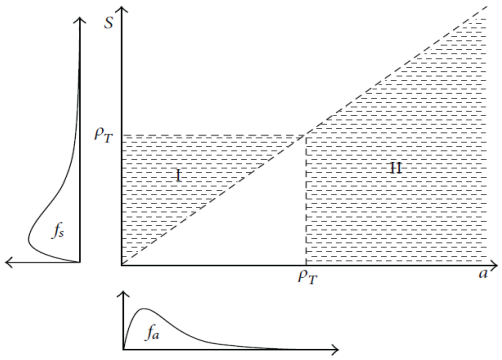
فریبنده آفست داپلر سیگنال‌های جعلی را تطبیق می‌دهد و فاز کد را به نحوی تنظیم می‌نماید که بر ناحیه هدف منطبق باشد. مرز ناحیه هدف دقیقاً مشخص نیست، اما تأثیر فریب خارج از آن به شدت افت می‌کند[۲۱]. عملکرد این روش، بر پایه تخمین C/No بیشینه همبستگی سیگنال‌های GPS منتشرشده، قرار دارد. در صورتی‌که نویز سیگنال را گوسین استاندارد در نظر بگیریم، می‌توان نشان داد که رابطه (۷) بین C/No و خودهمبستگی سیگنال ورودی برقرار است.

$$\rho_a \equiv \left|x^a\right|^2 - 1$$
$$\rho_s \equiv \left|x^s\right|^2 - 1 \qquad (۷)$$

که در آن X نشان‌دهنده خودهمبستگی سیگنال مربوطه و ρ مقدار C/No آن سیگنال می‌باشند. ρs نماد C/No سیگنال فریب و ρa مربوط به سیگنال معتبر می‌باشد. مسئله اصلی در این روش تعیین حد آستانه بهینه برای مقایسه C/No است. در صورتی‌که توان سیگنال فریب شناخته شده باشد انتخاب ρT بهینه مشکل نیست، اما در ازای ρs نامعلوم، ρT با بهینه‌سازی تعیین می‌گردد. فرض می‌شود که در اثر وجود فریب دو بیشینه همبستگی در سیگنال وجود دارد و از احتمال وجود بیشینه دیگر در اثر چندمسیری و طراحی ضعیف گیرنده صرف نظر شده است. قاعده به کار رفته برای تشخیص سیگنال فریب به این نحو است که اگر شرط $(\rho_a < \rho_T) \cap (\rho_s < \rho_T)$ برقرار باشد، بیشینه بزرگ‌تر به سیگنال واقعی نسبت داده می‌شود و در غیراین‌صورت بیشینه بزرگ‌تر را متعلق به سیگنال فریب فرض می‌نماید.با توجه به این قاعده، در دو حالت مشخص‌شده در رابطه (۸) خطا رخ می‌دهد. مجموع احتمال این دو حالت، میزان احتمال خطای کلی (Pe) را به دست می‌دهد که اندازه آن مبین میزان مؤثر بودن حمله فریب است. مناطق هاشورخورده در شکل ۷، دو حالت ممکن خطا را نشان می‌دهند که با جمع دو حالت و ساده‌سازی‌های مناسب رابطه (۹) برای خطا حاصل می‌شود که f در آن گویای تابع چگالی احتمال و F بیان‌گر توزیع تجمعی می‌باشند.

$$\{(\rho_a < \rho_T) \cap (\rho_s < \rho_T)\} \cap (\rho_a < \rho_s)$$
$$\{(\rho_a > \rho_T) \cup (\rho_s > \rho_T)\} \cap (\rho_s < \rho_a) \qquad (۸)$$

$$P_e = \int_0^{\rho_T} f_s(\rho_s) F_a(\rho_s) d\rho_s + \int_{\rho_T}^{\infty} f_s(\rho_a) F_s(\rho_a) d\rho_a \qquad (۹)$$



شکل۷. نمایش گرافیکی دو نوع خطای ممکن[۲۱].

کاهش خطای فریب با شبکه‌های عصبی

شبکه‌های عصبی ابزارهای قدرتمندی در مسائل غیرخطی و پیچیده محسوب می‌شوند و در بسیاری از کاربردهای وابسته به ارتباطات دیجیتال بکار می‌روند. در سال‌های اخیر برای مقابله با اختلال در GPS نیز به طور گسترده بکارگرفته شده‌اند. بر این اساس در این تحقیق روشی برای کاهش فریب در GPS با استفاده از شبکه‌های عصبی پیشنهاد شده است. هدف از اعمال شبکه عصبی کاهش اثر فریب در حلقه ردیابی و در نتیجه آن جبران‌سازی فریب در موقعیت‌یابی و ناوبری می‌باشد.

در ورودی گیرنده سیگنال دریافتی از هر ماهواره با سیگنال‌های رسیده از چندین ماهواره GPS ترکیب می‌گردد. ابتدا سیگنال دریافتی اولیه با پیش‌تقویت‌کننده کم نویز، تقویت شده و به فرکانس پایین‌تر تغییر یافته است. سیگنال آنالوگ جدید ابتدا از یک فیلتر میان‌گذر برای محدود کردن باند فرکانسی و از بین بردن نویز و تداخل امواج آن و در مرحله بعد از یک مبدل A/D عبور می‌کند و در نهایت سیگنال دیجیتال خروجی حاصل می‌شود. سیگنال‌های ماهواره‌های مختلف توسط همبسته‌سازها از هم تفکیک شده و قسمت دیجیتال گیرنده GPS که شامل فرآیندهای ردیابی کد و حامل است، پردازش سیگنال را انجام می‌دهد. می‌توان سیگنال دیجیتال GPS را در خروجی همبسته‌ساز به دو جزء هم‌فاز و متعامد تفکیک کرد. روابط زیر این اجزا را برای یک همبسته‌ساز نشان می‌دهند.

$$I(j) = \sum_{m=0}^{N} a_m K_c(\varepsilon_r - \Delta\tau_m + d\tau_j)\cos(\varepsilon_\theta + \Delta\theta_m + n_I) \qquad (۱۰)$$

$$Q(j) = \sum_{m=0}^{N} a_m K_c(\varepsilon_r - \Delta\tau_m + d\tau_j)\sin(\varepsilon_\theta + \Delta\theta_m + n_q) \qquad (۱۱)$$

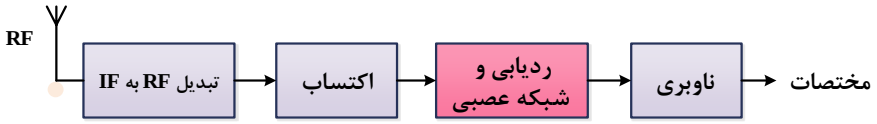
که در آن‌ها α_m دامنه سیگنال فریب، τ و θ مبین تأخیر و فاز

سیگنال معتبر، $\Delta\tau_m$ و $\Delta\theta_m$ به ترتیب مبین تأخیر و فاز نسبی سیگنال فریب نسبت به سیگنال معتبر، Kc تابع همبستگی کد، $\Delta\theta$ و $d\tau$ به ترتیب تأخیر فاز و تأخیر زمان بین سیگنال فریب و معتبر، ε_τ و ε_θ خطاهای ردیابی کد و حامل و n_I و n_Q به ترتیب نویزهای هم‌فاز و متعامدی هستند که شامل سیگنال‌های تبدیل‌شده به باند پایه مربوط به دیگر ماهواره‌ها می‌باشند.

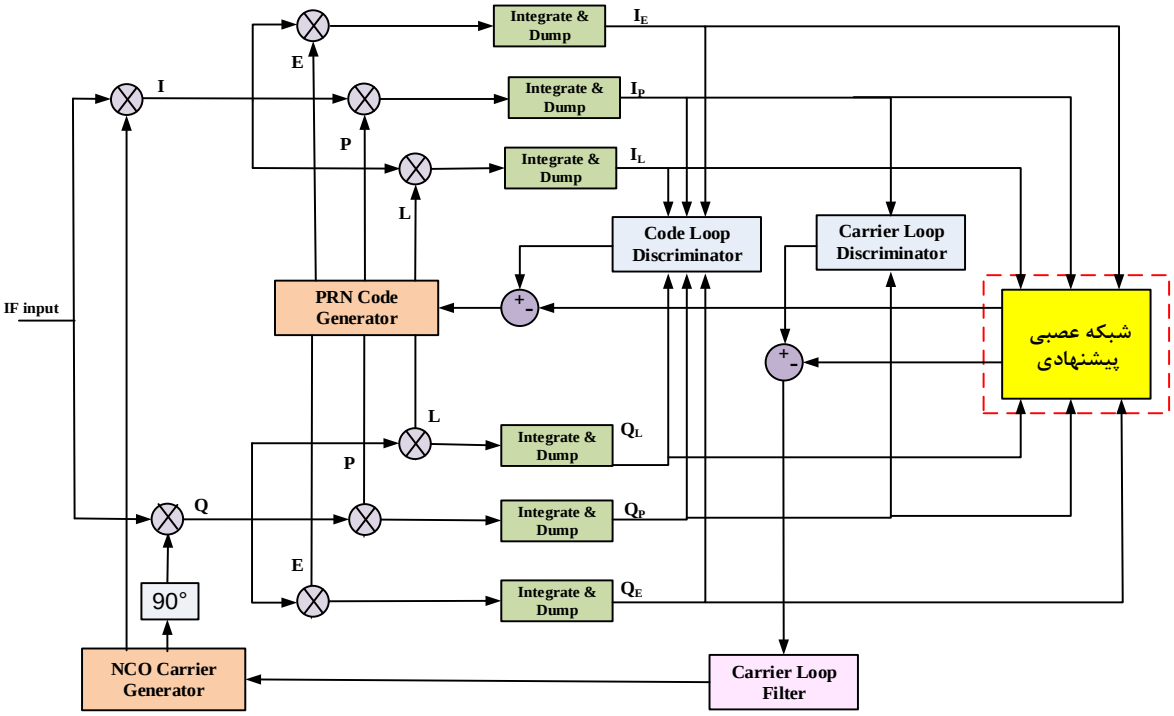
از آنجا که SNR سیگنال دریافتی قبل از تبدیل به باند پایه خیلی ضعیف است، نمی‌تواند به عنوان ورودی شبکه عصبی بکار رود زیرا منجر به زمان آموزش طولانی خواهد شد. بعد از تبدیل طیف گسترده به باند پایه، سیگنال‌های ناخواسته تضعیف می‌شوند، زیرا که کدهای فرستنده‌های متفاوت متعامد بوده و به عنوان نویز اضافی در نظر گرفته می‌شوند. بنابراین گذاشتن شبکه عصبی دقیقاً بعد از همبسته‌سازها و تفکیک سیگنال دریافتی مناسب است، زیرا که در آن سیگنال‌های ناخواسته به لطف متعامد بودن کدها خنثی شده‌اند و SNR به طور قابل توجهی افزایش یافته است.

شکل ۸ موقعیت شبکه عصبی در سیستم گیرنده GPS را نشان می‌دهد. چنان‌که از شکل نیز مشخص است، ساختار پیشنهادی در حلقه ردیابی اعمال شده است. در شکل ۹ نحوه اعمال شبکه عصبی در حلقه ردیابی با جزئیات بیشتر قابل مشاهده است. شبکه عصبی آموزش‌دیده درست بعد از همبسته‌سازها قرار گرفته و خروجی آن شامل خطای ردیابی فاز و کد تخمینی می‌باشد.

ورودی شبکه عصبی نیز شامل اجزای هم‌فاز و متعامد خروجی همبسته‌سازها است که عبارتند از: I_p، I_L، I_E، Q_p، Q_L و Q_E. عملکرد شبکه عصبی به چندین عامل بستگی دارد و تعریف دقیق این عناصر برای طراحی یک شبکه عصبی کارآمد حیاتی است. پیش‌پردازش داده‌ها، مقادیر اولیه وزن‌ها، نرخ و الگوریتم یادگیری نقش بسیار مهمی را در عملکرد شبکه عصبی ایفا می‌کنند. شکل ۱۰ معماری شبکه عصبی پیشنهادی در این مقاله را نشان می‌دهد. مشخصات دقیق شبکه عصبی به همراه جزئیات آموزش در جدول ۱ مشاهده می‌شود. شبکه‌ای با سه لایه شامل یک لایه ورودی، یک لایه پنهان و یک لایه خروجی در نظرگرفته شده است. نرون‌های خروجی نیز شامل خطای کد و خطای فاز می‌باشد. ساختار مورد استفاده شبکه پرسپترون چند لایه می‌باشد و برای آموزش آن از الگوریتم پس انتشار بهره گرفته‌ایم. آموزش شبکه عصبی در حالت نظارتی و به منظور برآورد خطای ردیابی فاز و کد ناشی از فریب انجام شده است. به دلیل پیچیدگی بالای محاسبات، مجموعه داده‌آموزشی و خروجی سیگنال‌های مطلوب به صورت غیربلادرنگ محاسبه می‌گردند. آموزش شبکه عصبی درگیرنده فعال GPS نیز قبل از راه‌اندازی انجام یافته است. سپس خروجی همبسته‌سازها به عنوان بردار ورودی اعمال شده و شبکه عصبی محاسبات پیش‌رو را برای تخمین خطاهای ردیابی کد و فاز اجرا می‌نماید.

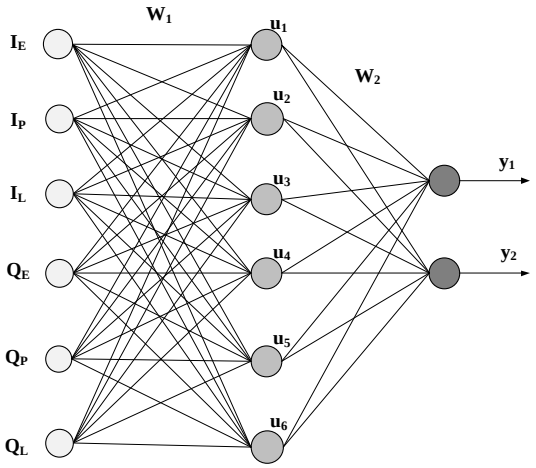


شکل ۸. موقعیت شبکه عصبی در سیستم گیرنده.



شکل ۹. شماتیک نشان‌دهنده مکان شبکه عصبی در قسمت پردازش سیگنال GPS.

داده‌های هر نمونه	



شکل ۱۰. معماری شبکه عصبی پیشنهادی.

نتایج شبیه‌سازی

پس از آموزش شبکه عصبی با داده‌های آموزش، شبکه عصبی با داده‌های آزمون مورد ارزیابی قرار گرفت. نتایج ارزیابی شبکه عصبی در شکل‌های ۱۱ و ۱۲ داده شده است. همان‌طور که در نمودارها مشاهده می‌شود، ساختار پیشنهادی با دقت مورد قبولی توانسته است خطای ردیابی کد و فاز را تخمین بزند.

کلیه مراحل آموزش، آزمون و ارزیابی در کامپیوتر شخصی با حافظه 6GB و پردازنده Intel Corei5-1.8GHz انجام شد. زمان مکان یابی گیرنده نرم افزاری GPS بعد از اعمال شبکه عصبی آموزش دیده از حدود ۳ دقیقه به ۳ دقیقه و ۲۰ ثانیه افزایش یافته است.

شبکه عصبی آموزش دیده به حلقه ردیابی در گیرنده GPS اعمال شده و پس از استخراج داده ناوبری و حل معادلات مربوطه، مختصات نهایی به همراه مشخصات سیگنال‌های معتبر اولیه استخراج گردید. آموزش شبکه عصبی به صورت غیربلادرنگ انجام می‌شود و پس از ارزیابی و تصحیح مجدد مقادیر وزن‌ها، در حلقه ردیابی قرار می‌گیرد که با توجه به استفاده از خروجی همبسته‌سازهای تولیدی در خود گیرنده، بار محاسباتی چندانی به گیرنده GPS اعمال نمی‌کند.

جدول ۲ مقدار فریب موجود در مجموعه داده‌های مورد بررسی، مقدار خطای باقیمانده پس از اعمال الگوریتم پیشنهادی و درصد کاهش خطای ناشی از فریب با اعمال الگوریتم را نشان می‌دهد.

جدول ۱. مشخصات شبکه عصبی.

نوع شبکه عصبی	MLP
الگوریتم آموزش	BP با ناظر
تعداد لایه‌های پنهان	یک لایه
تعداد گره های ورودی، تعداد نرون های لایه پنهان، تعداد خروجی ها	۶، ۶، ۲
نرخ آموزش (LearningRate)	$۱۰^{-۳}$
تعداد تکرار آموزش (net.trainParam.epochs)	۱۰۰۰۰۰
شرط توقف شبکه (net.trainParam.goal)	$۱۰^{-۷}$
تعداد نمونه ها (Samples)	۳۷۰۰۰
تعداد داده‌های هر نمونه	۶
تعداد داده‌های مورد استفاده برای آموزش	۷۰ ٪ از کل داده‌های هر نمونه
تعداد داده‌های مورد استفاده برای ارزیابی و آزمون	۳۰ ٪ از کل

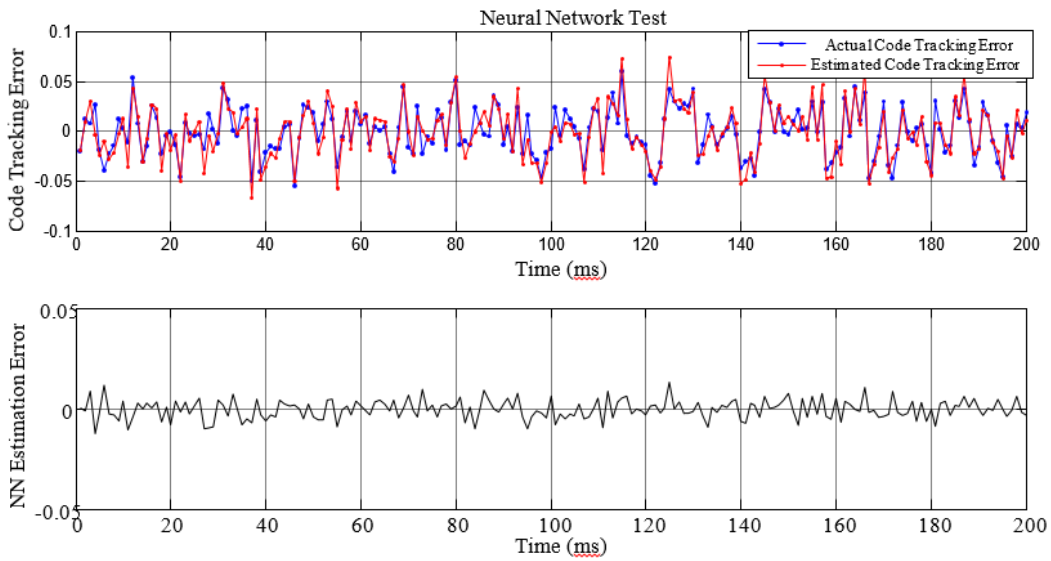
برای اجرای الگوریتم از مجموعه داده فریب با ساز و کار تأخیر و ترکیب استفاده شده است[۲۲].

همان‌طور که مشاهده می‌شود از لحاظ مقدار فریب تنوع خوبی بین مجموعه داده‌ها وجود دارد که جامعیت الگوریتم پیشنهادی در مقابله با فریب‌های مختلف تأخیری را نشان می‌دهد. چنان‌که ملاحظه می‌گردد در این سه مجموعه داده به طور متوسط فریب به اندازه ۸۲/۱۰ درصد با تلورانس ۱/۷۲ درصد کاهش یافته است. می‌توان نتیجه گرفت که کارآیی الگوریتم پیشنهادی به میزان فریب وابسته نبوده و درصد کاهش نزدیک هم در فریب‌های مختلف حاصل شده است.

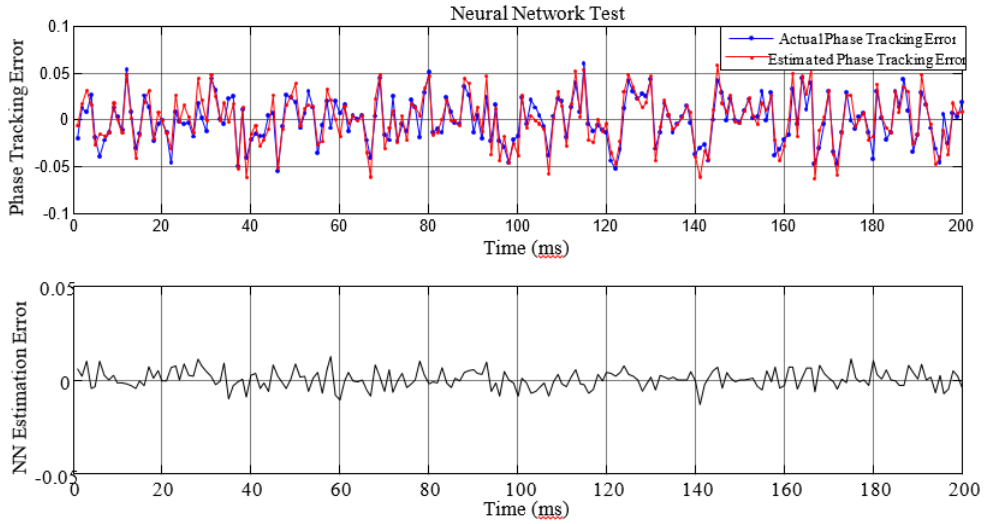
سناریوی تولید فریب در همه انواع داده‌های مورد استفاده یکسان است. ابتدا از سیگنال معتبر دریافتی به مدت کافی نمونه‌برداری و در فضای حافظه در دسترس ذخیره‌سازی گردید و پس از ایجاد تأخیر مناسب، برای ترکیب با سیگنال‌های حقیقی GPS منتشر یافت. در حقیقت ساز و کار تأخیر و ترکیب به منظور ایجاد سیگنال جعلی توسط ترکیب سیگنال حقیقی و سیگنال تأخیریافته GPS می‌باشد. برای مطالعه بیشتر در رابطه داده فریب مورد استفاده به مرجع[۲۲]مراجعه شود. آموزش شبکه عصبی با یک مجموعه داده فریب با طول ۳۷ ثانیه و مرحله ارزیابی آن با حدود ۱۰ ثانیه از یک مجموعه داده دیگر انجام شدند. بعد از تنظیم نهایی وزن‌ها، شبکه عصبی در گیرنده GPS قرار گرفت و سه مجموعه داده‌ای که در گزارش آمده اند به گیرنده اعمال گردید.

جمع‌بندی و نتیجه‌گیری

در این مقاله انواع روش‌های کاهش فریب را بررسی نمودیم. ابتدا نحوه پیش‌بینی مشخصه‌های سیگنال توسط تخمین‌گرهای مناسب توضیح داده شد. عملکرد تخمین‌گرهای شبکه عصبی، فیلترکالمن و حسگرهای داخلی مورد بررسی قرار گرفت. ملاحظه شد که خطای تخمین حسگر داخلی با افزایش زمان فریب نسبت به شبکه عصبی و فیلتر کالمن بیشتر می‌شود. البته این روش تنها برای فریب‌دهنده‌های ساده که تخریب شدید آنی روی سیگنال GPS ایجاد می‌کنند، کاربرد دارد. پس از آن روش پردازش فضایی بررسی شد. این تکنیک در صورت امکان تهیه آرایه آنتنی عملکرد قابل قبولی دارد، اما گزینه مناسبی برای تفکیک سیگنال واقعی و معتبر در حضور اختلال چندمسیری نمی‌باشد. زیرا در این حالت هر دو سیگنال چندمسیری و فریب از جهت‌های مختلف به گیرنده ارسال می‌شوند. همان‌طور که اشاره شد SQM یک روش آشکارسازی چندمسیری است که برای شناسایی حملات فریب بر روی گیرنده‌های ردیابی نیز به‌کار برده شده است. در این مطالعه دو روش RAIM و VB که بهبود یافته روش SQM هستند و در کاهش فریب مورد استفاده قرار می‌گیرند، مطرح گردید. در نهایت نیز روشی مبتنی بر شبکه‌های عصبی برای جبران خطای ردیابی ناشی از فریب ارائه شد. خلاصه‌ای از ویژگی‌های روش‌های موجود و پیشنهادی در جدول ۲ گزارش شده است. ملاحظه می‌گردد که روش پیشنهادی از کارآیی مطلوبی در مقایسه با دیگر روش‌ها برخوردار است. محدودیت بارز آن، آموزش شبکه عصبی به صورت غیربلادرنگ است. همچنین لازم است نوع فریب توسط آشکارساز مناسب شناسایی گردد. با توجه به امکانات موجود، تنها فریب تأخیری مورد استفاده قرار گرفت، اما به نظر می‌رسد در برابر انواع مختلف حمله فریب، روش پیشنهادی بتواند کارآیی قابل قبولی داشته باشد.



شکل ۱۱. ارزیابی شبکه عصبی بعد از آموزش تخمین کد.



شکل ۱۲. ارزیابی شبکه عصبی بعد از آموزش تخمین فاز.

جدول۲. نتایج اعمال الگوریتم پیشنهادی در کاهش خطای ناوبری روی سه مجموعه داده فریب.

	مقدار فریب در سطح افق (متر)		مقدار فریب در ارتفاع(متر)		مقدار فریب در کل (متر)		درصدکاهش 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	۴۷,۸۹	۵,۷۴	۵۲,۵۱	۱۱,۶	۷۱,۰۷	۱۲,۹۵	۸۱,۷۸
مجموعه داده دوم	۳۰,۲۷	۵,۶۶	۱۸,۴۲	۱,۹۱	۳۵,۴۳	۵,۹۷	۸۳,۱۳
مجموعه داده سوم	۳۷۷,۸۴	۵۷,۰	۸۹۳,۶۶	۱۷۱,۰۴	۹۷۰,۲۶	۱۸۰,۲۹	۸۱,۴۱

جدول۳. مقایسه روش‌های مختلف کاهش فریب.

روش‌های کاهش فریب	عملکرد روش	سخت افزار مورد نیاز	محل اعمال الگوریتم	مزایا	محدودیت‌ها
تخمین‌گر	پیش‌بینی مختصات بر پایه اطلاعات قبلی	حسگر داخلی یا تخمین‌گر	مکان‌یابی	سادگی پیاده‌سازی	افزایش خطا در حمله طولانی مناسب در فریب ساده با تخریب آنی
پردازش فضایی	حذف سیگنال فریب	آرایه انتن	سیگنال IF ورودی	اطمینان بالا	هزینه بالا عدم کارآیی در حضور چندمسیری
بردار پایه	کنارگذاشتن سیگنال فریب در حلقه ردیابی	حلقه ردیابی اضافی	حلقه ردیابی	کارآیی و اطمینان بالا	هزینه بالا
RAIM	استخراج شبه‌فاصله	-	ناوبری	دقت بالا	پیچیدگی محاسباتی عدم کارآیی در حضور چندمسیری
انتخاب پیک معتبر	ردیابی پیک سیگنال معتبر	-	اکتساب و ردیابی	سادگی پیاده سازی	عدم کارایی در حمله تأخیری
روش پیشنهادی	تصحیح خطای ناوبری	-	حلقه ردیابی	هزینه پایین و سادگی پیاده سازی	نیاز به آموزش برون‌خطی

مراجع

[1] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon and P. M. Kintner, "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer", 21st International Meeting of the Satellite Division of The Institute of Navigation, pp. 2314 - 2325, Sep. 2008.

[2] T. E. Humphreys, J. Bhatti and B. Ledvina, "The GPS Assimilator: a Method for Upgrading Existing GPS User Equipment to Improve Accuracy, Robustness and Resistance to Spoofing", 23rd International Meeting of the Satellite Division of The Institute of Navigation, pp. 1-11, Sep. 2010.

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

[4] M. H. Jin, Y. H. Han, H. H. Choi, C. Park, M. B. Heo and S. J. Lee,"GPS Spoofing Signal Detection and Compensation Method in DGPS Reference Station", 11th International Conference on Control, Automation and Systems, pp. 1616-1619, Oct. 2011.

[5] Z. Lin, C. Haibin and Z. Naitong, "Anti-Spoofing Extended Kalman Filter for Satellite Navigatin Receiver", International Conference on Wireless Communications, Networking and Mobile Computing, pp. 996-999, Sept. 2007.

[۶] سید امین علی‌کیاامیری، سید محمدرضا موسوی میرکلایی، محمدجواد رضایی و نیما حسین زاده، "ارائه روشی مبتنی برشبکه‌های عصبی به منظور مقابله با سیگنال فریب درGPS"، کنفرانس الکترونیک و فرصت‌های فرارو، تهران، دانشگاه صنعتی شریف، ۱۵-۱۷ اسفند، ۱۳۹۱.

[۷] سید محمدرضا موسوی، زهرا نصرپویا، محمدجواد رضائی و علی‌اصغر عابدی، "ارائه روشی برای مقابل با فریب در GPS به کمک فیلتر کالمن"، ششمین کنفرانس جنگ الکترونیک ایران، تهران، ۱۳۹۲.

[8] P. Papadimitratos and A. Jovanovic, "GNSS-Based Positioning: Attacks and Countermeasures", IEEE Military Communications Conference, pp. 1-8, 2008.

[9] P. Y. Montgomery, T. E. Humphreys and B. M. Ledvina, "Receiver-Autonomous Spoofing Detection: Experimental Results of a Multi-Antenna Receiver Defense Against a Portable Civil GPS Spoofer", Institude of International Technical Meeting of the Satellite Division of The Institute of Navigation, pp. 1-7, Jan. 2009.

[10] A. Broumandan, A.J. Jahromi, V. Dehgahanian, J. Nielsen and G. Lachapelle, "GNSS Spoofing Detection in Handheld Receivers Based on Signal Spatial Correlation",ION Position Location and Navigation Symposium, pp. 479-487, April 2012.

[11] C. E. McDowell, "GPS Spoofer and Repeater Mitigation System Using Digital Spatial Nulling", U.S. Patent 7250903 B1, 31 July 2007.

[12] S. Daneshmand, A. J. Jahromi, A. Broumandan and G. Lachapelle, "GNSS Spoofing Mitigation in Multipath Environments Using Space-Time Processing", European Navigation Conference, pp. 1-12, April 2013.

[13] S. Daneshmand, A. J. Jahromi, A. Broumandan and G. Lachapelle, "A Low Complexity GNSS Spoofing Mitigation Technique Using a Double Antenna Array", GPS World Magazine, Vol. 22, No. 12, pp. 44–46, Dec. 2011.

[14] 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, 2010.

[15] 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, 2011.

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

[17] B. M. Ledvina, W. J. Bencze, B. Galusha and I. Miller, "An In-Line Anti-Spoofing Device for Legacy Civil GPS Receivers", 23rd International Technical Meeting of the Satellite Division of the Institute of Navigation, pp. 689-712, Jan. 2010.

[18] M. Lashley and D. Bevly, "What About VectorTracking Loops?", Inside GNSS Magazine, pp. 1-6, May/June 2009.

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

[20] A. J. Jahromi, A. Broumandan, J. Nielsen and G. Lachapelle, "GPS Spoofer Countermeasure Effectiveness Based on Signal Strength, Noise Power and C/No Observables", International Journal of Satellite Communications and Networking, Vol. 30, No. 4, pp. 181–191, 2012.

[21] J. Nielsen, V. Dehghanian, and G. Lachapelle, “Effectiveness of GNSS spoofing Countermeasure Based on Receiver CNR Measurements”, International Journal of Navigation and Observation, pp. 1-9, 2012.

[۲۲] امیررضا بازیار، محمدرضا موسوی میرکلایی، عبدالرضا رحمتی و مریم معاضدی، "ارائه روشی جدید و ارزان قیمت برای تولید داده فریب GPS به منظور محافظت از سامانه‌های ناوبری دریایی"، مجله دریا فنون، دانشگاه علوم دریایی امام خمینی (ره) نوشهر، جلد اول، شماره اول، ش.ص.۱-۱۲، ۱۳۹۲.