

کاهش اثر تداخل در گیرنده GPS با به کارگیری چند همبسته ساز

۱- سمیرا توحیدی، ۲- سید محمدرضا موسوی میرکلانی* ۳- مریم معاضدی

۱- دانشجوی دکتری، ۲- استاد دانشکده مهندسی برق، دانشگاه علم و صنعت ایران، ۳- استادیار، دانشکده فناوری های نوین، دانشگاه محقق اردبیلی (دریافت: ۱۳۹۹/۰۸/۰۹، پذیرش: ۱۴۰۰/۰۴/۱۳)

چکیده

استفاده از سامانه موقعیت یابی جهانی (GPS) در سامانه های فوق خودکار، روزبه روز رو به افزایش است و لذا مسئله امنیت این سامانه ها بسیار حائز اهمیت می باشد. یک خطر بزرگ در تخمین موقعیت توسط GPS، حمله فریب است. فریبنده سیگنال ماهواره را جعل می کند تا گیرنده را مجبور به تخمین اشتباه موقعیت نماید. تحقیقات بسیاری بر روی آشکارسازی و کاهش فریب در گیرنده GPS تمرکز دارند. در این مقاله، به کارگیری معماری چند همبسته ساز مبتنی بر شبکه عصبی جهت مقابله با حمله فریب پیشنهاد شده است. حمله فریب با سازوکار ترکیب و تأخیر بر مبنای یک سیگنال واقعی GPS ساخته شده است. نتایج شبیه سازی های انجام شده در گیرنده نرم افزاری، حاکی از مؤثر بودن راهکار پیشنهادی در جهت کاهش حمله فریب می باشد. با مورد مطالعه قرار دادن سه سناریو فریب عملی، روش پیشنهادی مورد ارزیابی قرار گرفت و نتایج حاصله نشان می دهند که میزان کاهش خطای فریب با به کارگیری این روش، ۸۸/۴۲٪ می باشد.

کلیدواژه ها: فریب، گیرنده GPS، معماری چند همبسته ساز، شبکه عصبی

۱- مقدمه

یک تداخل ساختاری است. سیگنال های جعلی که از طریق فریبنده ارسال می شوند، بسیار شبیه سیگنال های معتبر ارسالی از ماهواره ها هستند و می توانند به تدریج نتایج موقعیت یابی گیرنده هدف را به یک مکان کاذب القا کنند. به همین دلیل، در مقایسه با جمینگ، احتمال آشکارسازی حمله فریب^۲ توسط گیرنده هدف کمتر است و از این رو خطرناک تر است.

حملات فریب می توانند ساختار ساده و یا پیچیده ای داشته باشند. در یکی از انواع متداول ایجاد حمله فریب، فریبنده یک تقویت کننده قدرت و آنتن فرستنده به یک شبیه ساز سیگنال ماهواره ای متصل می شود و سیگنال های جعلی را به سمت گیرنده هدف پخش می کند؛ اما این نوع فریب که دارای ساختار ساده ای است، معمولاً نیاز به همراه شدن با جمینگ دارد تا بتواند گیرنده هدف را تحت کنترل گیرد. در سال ۲۰۰۸، نویسندگان در مرجع [۱۰] با موفقیت یک تکرار کننده را بر اساس گیرنده نرم افزاری ایجاد کردند که می تواند گیرنده هدف را به صورت مستقیم در مرحله ردیابی، فریب دهد. با گسترش فریبنده ها، تحقیقات در مورد گیرنده های ضد فریب به سرعت شروع به توسعه کرد. در سال ۲۰۱۲، نویسندگان در مرجع [۷] یک مطالعه جامع در مورد تهدیدات فریب انجام دادند و به طور خلاصه روش های مقابله با فریب را در دو دسته اصلی معرفی کردند: تشخیص فریب و کاهش فریب. به طور کلی با توجه به توضیحات بیان شده در مراجع مرتبط، اقداماتی که در راستای شناسایی و کاهش فریب انجام شده است را می توان به چهار گروه تقسیم نمود: تشخیص

سامانه موقعیت یابی جهانی (GPS)^۱ به طور گسترده ای به منظور موقعیت یابی و زمان سنجی مورد استفاده قرار می گیرد. این سامانه در تمامی وسایل نقلیه زمینی هوایی و دریایی جهت موقعیت یابی و یا کمک به موقعیت یابی به کار می رود. بنابراین، مسئله صحت موقعیت، سرعت و یا زمان سنجی مبتنی بر این سامانه خیلی بیشتر حائز اهمیت می باشد. از این رو، در سال های اخیر، بیشتر تحقیقات انجام شده در زمینه موقعیت یابی، روی شناسایی و کاهش مداخلات این سامانه ناوبری متمرکز شده است [۳-۱]. انواع مختلفی از مداخلات وجود دارد که می تواند عملکرد صحیح گیرنده های موقعیت یابی را به خطر بیندازد. مراجع [۹-۴]، برخی مطالعات انجام شده در این حوزه را نشان می دهند.

این تحقیقات نشان می دهند که وضعیت گیرنده GPS غیرنظامی به سادگی می تواند توسط اختلال تحت تأثیر قرار بگیرد. در واقع، سیگنال GPS به دلیل توان کم سیگنال در معرض انواع تداخلات قرار دارد. در مورد گیرنده های GPS، در حال حاضر دو نوع مداخله اصلی وجود دارد: جمینگ و فریب. در جمینگ اغلب از جمر توان بالا استفاده می شود که معمولاً منجر به از بین رفتن قفل حلقه ردیابی و عدم موقعیت یابی در گیرنده هدف می شود. از این رو، احتمال پنهان ماندن این مداخله ضعیف است؛ اما فریب

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

² Spoofing

¹ Global Positioning System

اکنون با توجه به عملکرد موفق معماری چند همبسته‌ساز و نیز الگوریتم‌های هوش مصنوعی در حوزه شناسایی و مقابله با اختلال، نویسندگان در این مقاله تلاش می‌نمایند با به‌کارگیری معماری چند همبسته‌ساز در واحد ردیابی و بررسی خروجی این همبسته‌سازها در یک شبکه عصبی چندلایه ادراک، به مقابله با اثرات اختلال فریب در گیرنده GPS بپردازند.

ادامه مقاله در چهار بخش به بحث در این خصوص پرداخته می‌شود. در بخش ۲، طرح سامانه ارائه می‌شود. در بخش ۳، نحوه تولید سیگنال فریب شرح داده می‌شود. بخش ۴، روش پیشنهادی در این مقاله را مورد بحث و بررسی قرار می‌دهد. در بخش ۵، نتایج بیان می‌شود و در قسمت پایانی نیز نتیجه‌گیری ارائه شده است.

۲- طرح سامانه

ماهواره‌های GPS کدها و داده‌های ناوبری را در دو محدوده فرکانسی ارسال می‌کنند: L1 و L2. تنها سیگنال L1 که برای استفاده غیرنظامی در دسترس می‌باشد، در اینجا مورد تجزیه و تحلیل قرار گرفته است. در حالت کلی، سیگنال دریافتی از ماهواره‌ی شماره i ، در گیرنده GPS مطابق رابطه (۱) می‌باشد [۱]:

$$x(t) = S_{L1i}(t) + n(t) + I(t) = \sqrt{2p_t d_{i(t)} c_{i(t)}} \cos(2\pi f_{L1} t + \theta) + n(t) + I(t) \quad (1)$$

که در آن، $S_{L1i}(t)$ مبین سیگنال ارسال شده L1، P_t مبین توان سیگنال حامل، $D_i(t)$ مبین اطلاعات ناوبری، $C_i(t)$ مبین دنباله شبه تصادفی (کد C/A) با طول چپ f_{L1} ، T_c مبین فرکانس حامل L1 (۱۵۷۵/۴۲ MHz)، $n(t)$ مبین نویز و $I(t)$ مبین منبع تداخل در GPS هستند.

جهت بهبود آشکارسازی و مقابله با فریب شناخت اثرات فریب بر روی گیرنده GPS بسیار حائز اهمیت می‌باشد. اغلب تحقیقات بر روی تأثیر فریب بر روی شبه‌فاصله تخمین موقعیت و SNR تمرکز دارند. این معیارها نتیجه مستقیم یا غیرمستقیم رفتار حلقه‌های ردیابی گیرنده هستند. به‌منظور مطالعه جزئیات بیشتر در این مسئله، لایه پردازش سیگنال مورد بررسی قرار می‌گیرد.

پس از ورود سیگنال از بخش سرچلویی به قسمت نرم‌افزاری گیرنده، فرآیند استخراج داده‌های ناوبری آغاز می‌شود. در این مسیر، نخستین گام، اکتساب ماهواره‌ها است. وظیفه واحد اکتساب پیدا کردن ماهواره‌هایی که سیگنال آن‌ها را دریافت کرده‌ایم و نیز تخمین مقدار تأخیر کد و شیفت دوپلری ایجاد شده در آن سیگنال است. مقدار تأخیر فاز کد، زمان لازم برای

ناهنجاری در توان سیگنال [۱۱ و ۱۲]، تشخیص ناهنجاری در زمان ورود [۱۳ و ۱۴]، پردازش فضایی [۱۵-۱۸] و تشخیص اعوجاج در همبستگی [۲۳-۱۹]. در مرجع [۱۵]، نویسندگان آنتن آرایه تطبیقی را پیشنهاد کردند که از روش فرمان صفر استفاده می‌کند. این روش می‌تواند سیگنال‌های جعلی را از یک منبع مداخله محافظت نماید. مشکل اصلی این نوع روش‌ها نصب چند آنتن در گیرنده است که کاری دشوار است. با توجه به تنوع فریب، نویسندگان در مرجع [۲۴] از چندین روش ضد فریب به‌طور هم‌زمان بر روی گیرنده استفاده کرد و به‌روش کاهش فریب ساده دست یافته است. نویسندگان در مراجع [۲۵ و ۲۶]، با به‌کارگیری الگوریتم‌هایی مبتنی بر تبدیل موجک^۱ در مراحل اکتساب و ردیابی اثرات مخرب حمله فریب را بر گیرنده‌های GPS کاهش دادند.

با توجه به شباهت‌های موجود بین فریب و خطای ناشی از چندمسیری^۲، امکان‌سنجی استفاده از روش‌های کاهش میزان چندمسیری برای کاهش فریب در مرجع [۲۷] مورد بررسی قرار گرفت و الگوریتم جدیدی بر اساس حداکثر درست‌نمایی برای کاهش فریب پیشنهاد داده شد. این الگوریتم بر مبنای تخمین چندمسیری که یکی از روش‌های مهم کاهش اثرات چندمسیری است، طراحی شده است. در این مقاله، از معماری چند همبسته‌ساز استفاده شده است. لذا به اطلاعات بیشتری از تابع همبستگی دسترسی داشته و از این طریق مشخصات سیگنال اصلی و سیگنال اختلال بر اساس تحلیل خروجی همبسته‌سازها و به کمک تخمین‌گر حداکثر درست‌نمایی، برآورد شده است. این روش جهت مقابله با نوعی از فریب که مستقیماً در مرحله ردیابی طراحی شده‌اند، ارائه شده است. درواقع معماری چندهمبسته‌ساز، معماری جدید است که با افزایش تعداد همبسته‌سازها در واحد ردیابی، امکان بررسی دقیق‌تر اثرات سیگنال اختلال را در این واحد گیرنده فراهم می‌آورد. این معماری در مرجع [۲۸] جهت شناسایی اختلال در سامانه ناوبری ماهواره‌ای جهانی معرفی شد.

از سوی دیگر در سال‌های اخیر محققین در این حوزه، به‌کارگیری الگوریتم‌های هوش مصنوعی را در قسمت‌های مختلف گیرنده جهت آشکارسازی و مقابله با فریب معرفی نمودند. ازجمله این تحقیقات، می‌توان به مراجع [۲۹ و ۳۰] اشاره کرد که شبکه عصبی چندلایه ادراک را جهت آشکارسازی فریب به‌کار گرفتند. مرجع [۳۱] روش‌های بینایی ماشین را در این حوزه پیشنهاد نمودند. در مرجع [۳۲] تابع CAF^۳ به‌عنوان یک تصویر مورد پردازش قرار گرفت و با به‌کارگیری شبکه عصبی کانولوشن، آشکارسازی اختلال فریب انجام پذیرفت.

^۱ Wavelet Transform

^۲ Multi-path

^۳ Cross Ambiguity Function.

$$d_{PLL} = \arctan\left(\frac{Q_p}{I_p}\right) \quad (2)$$

$$d_{FLL} = \frac{\arctan 2(I_{P1}I_{P2} + Q_{P1}Q_{P2}, I_{P1}Q_{P2} - I_{P2}Q_{P1})}{t_2 - t_1} \quad (3)$$

که در آن، Q_p قسمت موهومی و I_p قسمت حقیقی خروجی بلوک انتگرال گیری را نشان می دهند. برای محاسبه d_{FLL} دو خروجی از نمونه های زمانی پشت سر هم در زمان های t_1 و t_2 مورد نیاز است. تفکیک کننده متداول DLL تفکیک کننده تقدم تاخر است. برای پیاده سازی آن به دو کپی از کد نیاز می باشد. یکی تأخیر یافته و یکی پیش رونده است و درواقع، به میزان زمان مشخص شیفت داده شده اند. آفست بین سیگنال تأخر و تقدم بر حسب چپ های PRN بیان می شود و به عنوان فاصله همبسته ساز DLL معرفی می گردد.

تفکیک کننده ها دو نوع می باشند: تفکیک کننده هم فاز یا تفکیک کننده غیر هم فاز. تفکیک کننده های نوع اول اندازه گیری کد را با دقت بیشتری انجام می دهند، اما تنها زمانی می توان از آن ها استفاده نمود که PLL روی فاز قفل شده است. تفکیک کننده غیر هم فاز به صورت زیر رابطه (۴) می باشد [۲]:

$$d_{DLL,NC} = \frac{\sqrt{I_E^2 + Q_E^2} - \sqrt{I_L^2 + Q_L^2}}{\sqrt{I_E^2 + Q_E^2} + \sqrt{I_L^2 + Q_L^2}} \quad (4)$$

تفکیک کننده هم فاز به صورت رابطه (۵) تعریف می شود [۲]:

$$d_{DLL,C} = \frac{I_E - I_L}{4I_p} \quad (5)$$

سیگنال فریب دارای ساختاری مشابه با ساختار سیگنال معتبر ماهواره است، با این تفاوت که دارای شیفت زمانی $\Delta \tau_{i,c}$ ، شیفت دوپلر $\Delta f_{i,D}$ و نیز سطح توان متفاوت می باشد.

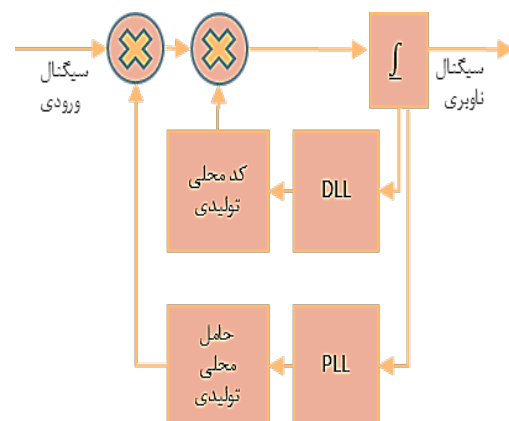
۳- نحوه تولید فریب

با گسترش ایده ذخیره سازی و تأخیر، به منظور تولید سیگنال فریب، الگوریتم تأخیر و ترکیب در گیرنده نرم افزاری به کار گرفته شده است. در حقیقت، مفهوم تأخیر و ترکیب به معنی ایجاد سیگنال فریب توسط ترکیب سیگنال حقیقی و سیگنال تأخیر یافته GPS می باشد. با توجه به رابطه (۱)، سیگنال در فرکانس $L1$ که از طریق ماهواره های GPS ارسال شده است با رابطه (۶) قابل بیان می باشد [۴].

$$S_A = A_c d_i(t) c_i(t) \cos(2\pi f_{L1}t + \phi_{L1}) \quad (6)$$

هم فاز نمودن کد PRN می باشد. تخمین تقریبی فاز کد و فرکانس حامل، به ترتیب، به منظور تولید کد PRN محلی منطبق با کد ورودی و حامل دریافتی، صورت می پذیرد تا در مرحله بعدی حذف گردند. سرعت ماهواره ها نسبت به گیرنده باعث ایجاد اثر دوپلر می شود که آن هم به نوبه خود فرکانسی بالاتر یا پایین تر از مقدار نامی فرکانس حامل ماهواره ها را نتیجه می دهد. در بدترین حالت، معمولاً محدوده انحراف فرکانس به اندازه ± 10 KHz در نظر گرفته می شود؛ بنابراین برای تولید سیگنال حامل محلی هم فرکانس با سیگنال حامل ورودی لازم است میزان انحراف فرکانس استخراج گردد.

گیرنده ها با تلفیق کردن سیگنال دریافتی با کد محلی و سیگنال حامل محلی، دمدولاسیون را انجام می دهد. به دلیل حرکت نسبی بین ماهواره ها و گیرنده، اثر دوپلر نیز باید منظور شود و کد محلی تولید شده بایستی به صورت پیوسته با توجه به سیگنال دریافتی تنظیم شود. گیرنده های سنتی GPS از دو حلقه ردیابی جهت هم زمان سازی سیگنال تولیدی محلی با سیگنال دریافتی استفاده می کنند. یکی برای ردیابی سیگنال حامل که معمولاً از حلقه قفل فاز^۱ (PLL) و یا حلقه قفل فرکانس^۲ (FLL) استفاده می شود و یکی به منظور ردیابی کد C/A که اغلب حلقه قفل تأخیر^۳ (DLL) به کار می رود. شکل (۱) قسمت دمدولاسیون یک گیرنده را نشان می دهد. نحوه عملکرد دو حلقه ردیابی شبیه هستند. آن ها از یک تفکیک کننده برای تخمین آفست بین سیگنال دریافتی و سیگنال محلی استفاده می کنند و یک فیلتر جهت تنظیم آن به کار می رود. این فیلتر می تواند با تغییر مرتبه و پهنای باند آن تنظیم شود.



شکل (۱): لایه پردازش سیگنال گیرنده GPS

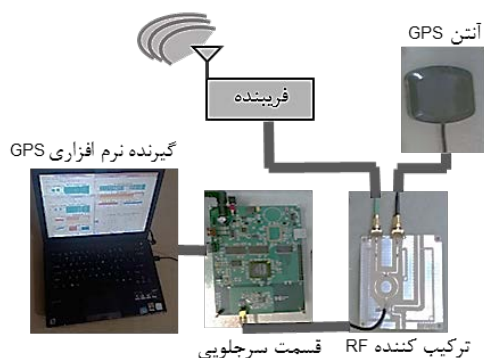
تفکیک کننده بهینه برای PLL و FLL به صورت رابط (۲ و ۳) می باشد [۲]:

^۱ Phase Lock Loop

^۲ Frequency Lock Loop

^۳ Delay Lock Loop

ترکیب کننده RF، ادغام شده و سپس این سیگنال ترکیبی در واحد سرجلویی دریافت می شود. واحد سرجلویی در گیرنده های GPS بعد از آنتن قرار می گیرند و قادر به تقویت و دریافت سیگنال GPS هستند. در نهایت، از سیگنال تولید شده نمونه برداری می شود و در گیرنده نرم افزاری بررسی شده و داده های ناوبری استخراج می گردند.



شکل (۲): شمای کلی رویه تولید فریب و جمع آوری داده ها.

۴- روش پیشنهادی

با مطالعه ساختار سیگنال فریب ملاحظه می شود که فریب و چندمسیری شباهت بسیاری دارد، چرا که سیگنال دریافتی در چندمسیری برآیند سیگنال مسیر مستقیم و سیگنال رسیده از مسیرهای غیرمستقیم می باشد. در واقع، هم فریب و هم چندمسیری قله های همبستگی سیگنال ترکیبی را تحت تأثیر قرار می دهند. اگر فرکانس حامل سیگنال جعلی از سیگنال معتبر مربوطه انحراف داشته باشد، انحراف اوج همبستگی سیگنال ترکیبی قابل تشخیص خواهد بود. اما اگر فرکانس حامل سیگنال جعلی با سیگنال معتبر مربوطه مطابقت داشته باشد، اوج همبستگی سیگنال ترکیبی فریب شبیه به چندمسیری خواهد بود که دشوارترین وضعیت برای تشخیص و کاهش فریب است. از این رو، در سناریوهای فریب شبیه سازی شده، فرکانس حامل سیگنال جعلی و سیگنال معتبر مربوط به آن یکسان هستند (حالت قفل فرکانس). با این وجود، سیگنال های جعلی که از طریق فریبند منتقل می شوند و سیگنال های چندمسیری تفاوت قابل توجهی دارند. عمده اختلافات به شرح زیر است:

۱. به جز مورد خاصی که سیگنال مستقیم مسدود شده است، سیگنال های چندمسیری دریافتی از ماهواره به طور معمول ضعیف تر از سیگنال مستقیم آن هستند و توان پایین تری دارند، در حالی که توان سیگنال های جعلی مربوط به فریب، معمولاً کمی بیشتر از توان سیگنال های معتبر هستند.

۲. قله های همبستگی سیگنال های چندمسیره از قله همبستگی سیگنال مستقیم مربوطه عقب تر هستند، چراکه

این رابطه بخشی از سیگنال ماهواره های GPS را نشان می دهد که توسط گیرنده های غیرنظامی قابل دریافت می باشد. حال اگر رابطه (۶) را به عنوان سیگنال معتبر در نظر بگیریم، سیگنال فریب با سازوکار تأخیر و ترکیب به صورت رابطه (۷) نمایش داده می شود:

$$I_{C/A} = A_c^A d_i^A(t) c_i^A(t) \cos(2\pi f_{L1}t + \phi_{L1}^A) + A_c^D d_i^D(t) c_i^D(t) \cos(2\pi f_{L1}t + \phi_{L1}^D) \quad (7)$$

این رابطه معرف سیگنالی است که برای فریب گیرنده ارسال می شود. بالانویس و زیرنویس A و D به ترتیب بیان گر سیگنال معتبر و تأخیر یافته می باشند. برای تولید این سیگنال، ابتدا به ذخیره سازی سیگنال معتبر GPS نیاز است. سپس، سیگنال ذخیره شده که گویای سیگنال تأخیری است، با سیگنال حقیقی ترکیب می شود. بعد از تهیه سیگنال جعلی و ارسال آن به سمت گیرنده، مجموعه سیگنال دریافتی در گیرنده همانند رابطه (۸) بیان می شود:

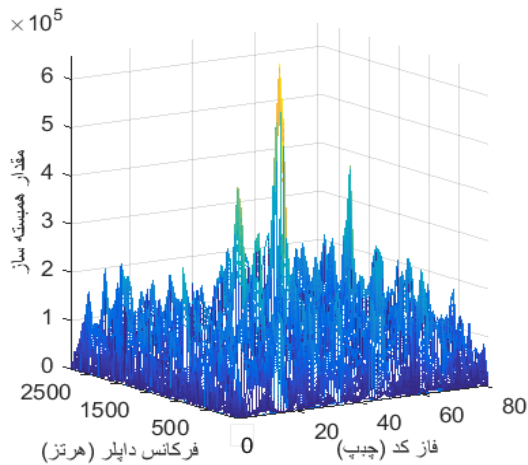
$$R_{C/A} = S_{C/A}(t) + I_{C/A}(t) \quad (8)$$

برای بی اثر کردن سیگنال معتبر GPS در گیرنده، می توان از افزایش نسبت توان سیگنال جعلی به معتبر بهره برد. برای تنظیم مناسب سطح توان سیگنال جعلی چنان که به راحتی قابل تشخیص نباشد و در عین حال، نسبت به سیگنال معتبر محیط مورد آزمایش قوی تر باشد، از تخمین گر توان و تنظیم کننده دامنه به ترتیب در ورودی و خروجی استفاده می شود. تخمین گر پس از دریافت سیگنال معتبر، سطح متوسط توان سیگنال را در زمان و مکان حاضر می سنجد. تنظیم کننده، دامنه سیگنال ترکیبی تولیدی را حدود ۲ dB بالاتر از سطح توان سیگنال محیط تنظیم می کند. با این کار، در عین حال که با حداقل توان مصرفی سیگنال معتبر GPS بی اثر می گردد، افزایش بی رویه توان سیگنال جعلی، موجب اتلاف توان نمی شود و نیز به راحتی توسط آشکارسازهای معمول قابل تشخیص نخواهند بود. با توجه به توضیحات بیان شده، در نهایت سیگنال دریافتی در آنتن گیرنده در شرایط حضور حمله فریب به شکل زیر اصلاح می شود [۴]:

$$R_{C/A} = A_c^A d_i^A(t) c_i^A(t) \cos(2\pi f_{L1}t + \phi_{L1}^A) + A_c^D d_i^D(t) c_i^D(t) \cos(2\pi f_{L1}(t - \Delta t_D) + \phi_{L1}^D) \quad (9)$$

شکل (۲) نحوه جمع آوری داده های آزمایشگاهی فریب را نمایش می دهد. واحد فریبند که خود مجهز به آنتن GPS می باشد، داده جعلی فریب را تولید می نماید. سیگنال تولید شده در این واحد با سیگنال GPS دریافت شده از آنتن در واحد

همزمان سیگنال معتبر و سیگنال فریب این دو قله را به هم نزدیک می گرداند و در نتیجه نسبت آن ها کم می شود و گاهی کمتر از حد آستانه اکتساب می شود. در نتیجه، کانال مورد نظر از دست می رود و همین موجب ایجاد خطا در موقعیت یابی می شود. در اینجا به منظور مقابله با این مشکل، در حلقه ردیابی همه کانال هایی که قبل از وقوع حمله فریب در دسترس بوده اند، ردیابی می شوند.



شکل (۴): نمایی از فضای همبسته سازها.

همان طور که در بالا بیان شد، در اینجا حملات فریب هم فرکانس طراحی شده اند. بنابراین، جهت ردیابی کانال های از دست رفته، مولد فرکانس حامل به منظور تولید سیگنال محلی مناسب، بر روی فرکانس حامل سیگنال دریافتی قبل از رخداد فریب، تنظیم می شود.

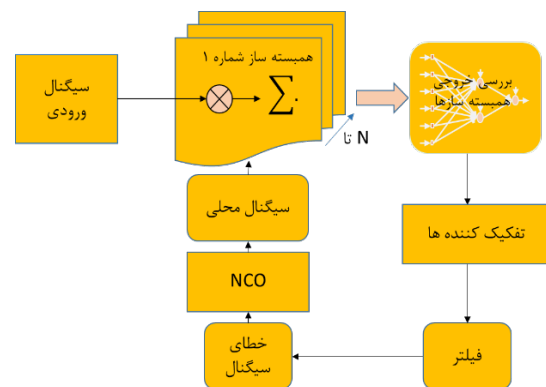
با گسترش تعداد همبسته سازها در بعد فاز کد، قله هایی که در اثر سیگنال فریب در تابع همبستگی ایجاد شده اند، قابل مشاهده خواهند شد. در ادامه، خروجی همبسته سازها در یک شبکه عصبی مورد بررسی قرار می گیرد. با انتخاب شاخه هایی از همبسته سازها که مقدار خروجی آن ها از حد آستانه بالاتر بوده و بررسی آن در شبکه عصبی مقدار مناسب تأخیر کد جهت تولید سیگنال محلی مناسب، به DDL ارسال می شود.

در اینجا ۱۸ شاخه همبستگی در نظر گرفته شده که ۶ شاخه به عنوان ورودی شبکه عصبی انتخاب می شود. شبکه عصبی سه لایه ادراک با معماری (۶-۳-۱) برای این کار طراحی شده است. با بررسی توابع مختلف سیگموئید، تانژانت هایپربولیک، تانژانت هایپربولیک معکوس و تابع موجک به عنوان توابع فعال سازی در شبکه مورد نظر، نهایتاً با به کارگیری تابع موجک به نتایج مطلوب رسیدیم و این تابع به عنوان تابع فعال سازی لایه پنهان و خروجی انتخاب شد.

سیگنال مسیر مستقیم، کوتاه ترین فاصله را تا رسیدن به گیرنده می پیماید و لذا سریع تر می رسد. فاصله بین این دو نوع قله معمولاً کاملاً نزدیک است و همپوشانی مؤثر این دو نوع قله فاصله کاملاً نزدیک را نشان می دهد. در مقابل، سیگنال های جعلی فریب می توانند همراه با سیگنال های معتبر، حتی پیش از سیگنال های معتبر هم تراز شوند. فاصله بین قله های همبستگی این دو نوع سیگنال ممکن است بسیار دور یا نزدیک باشد.

این بدان معناست که حلقه ردیابی معمول که بر اساس همبسته سازهای تقدم، تأخر و بلادرنگ طراحی شده است و همواره روی قله ای که حداکثر همبستگی را ایجاد می نماید، قفل می شود؛ به طور خاص برای چند مسیری طراحی شده است و نمی تواند به عنوان ضد فریب خیلی کارا باشد.

در معماری چند همبسته ساز با توجه به گسترش تعداد همبسته سازها امکان مطالعه بیشتر تابع همبستگی فراهم می شود و می توان قله هایی که در اثر وجود سیگنال هایی غیر از سیگنال اصلی در فضای همبسته سازها ایجاد شده اند را بررسی نمود. از این رو، در اینجا حلقه ردیابی با معماری چند همبسته ساز جهت کاهش فریب به کار گرفته می شود و از شبکه عصبی چند لایه جهت بررسی خروجی همبسته سازها استفاده می شود. شکل (۳) نمای کلی حلقه ردیابی با معماری چند همبسته ساز و شکل (۴) تعداد قله ها در فضای دو بعدی کد فاز- فرکانس دوپلر را نمایش می دهند. وجود بیش از یک قله با مقدار همبستگی بالا، نشان دهنده حضور سیگنال اختلال می باشند.



شکل (۳): بلوک دیاگرام حلقه ردیابی با معماری چند همبسته ساز مبتنی بر شبکه عصبی

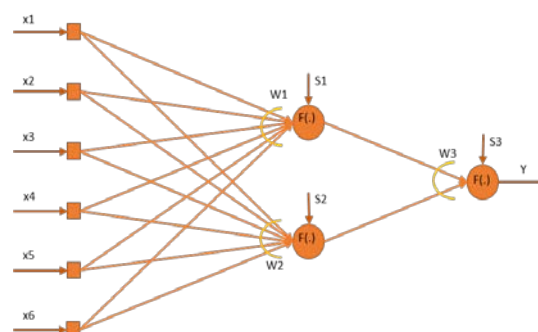
تشابه موجود بین سیگنال فریب و سیگنال معتبر اغلب منجر به از دست رفتن برخی کانال ها در مرحله اکتساب می گردد. چرا که در مرحله اکتساب نقطه ای که حداکثر همبستگی را ایجاد می کند بایستی نسبت به دیگر قله های موجود در فضای همبستگی از مقدار حد آستانه اکتساب بالاتر باشد و وجود

در ادامه، با اعمال داده‌های تولید شده در ۳ سناریو فریب به گیرنده، دقت مکان‌یابی آن اندازه‌گیری شد. نتایج در جدول (۱) ثبت شده‌است. این نتایج نشان می‌دهند که الگوریتم پیشنهادی به‌صورت میانگین $88/42\%$ در کاهش خطای ایجاد شده در موقعیت گیرنده مؤثر بوده است. در ادامه، میزان کاهش فریب بدست آمده بر اساس الگوریتم پیشنهادی در این مقاله با روش‌های بیان شده در مراجع [۳] و [۱۲] مقایسه شد. همان‌طور که در جدول (۲) ملاحظه می‌شود، الگوریتم پیشنهادی نسبت به نتایج اعلام شده در مرجع [۳]، ۱۸ درصد و نسبت به نتایج اعلام شده در مرجع [۱۲]، ۱۴ درصد بهبود داشته است.

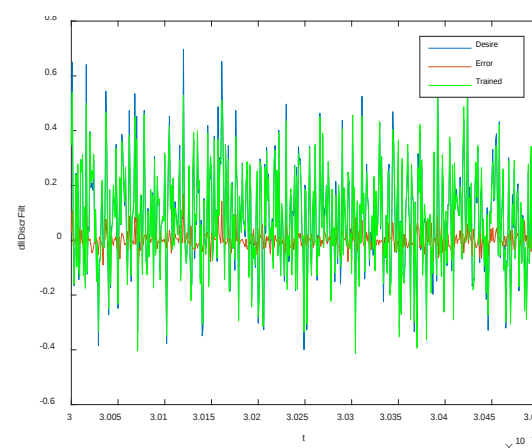
درازای دقت بالاتری که در الگوریتم پیشنهادی ارائه شده است، پیچیدگی محاسباتی در بلوک ردیابی گیرنده افزایش یافته است. در واحد ردیابی گیرنده GPS، اندازه بردار سیگنال ورودی وابسته به زمان انتگرال‌گیری همدوس و فرکانس نمونه برداری می‌باشد که اندازه بردار ورودی در این مقاله به‌زای فرکانس نمونه برداری 5714 MHz و $5/7143$ و زمان انتگرال‌گیری همدوس 1 ms ، 5714 است. جهت سنجش میزان همبستگی این سیگنال با سیگنال محلی 5714 عمل ضرب و 5713 عمل جمع مورد نیاز است؛ بنابراین، میزان پیچیدگی محاسبه همبستگی در یک شاخه همبسته‌ساز 11427 می‌باشد و در گیرنده معمول با ۶ شاخه همبسته‌ساز این مقدار 68562 است. میزان پیچیدگی در شبکه عصبی سه لایه بیان شده، با فرض محاسبه توابع فعال‌ساز تا ۷ جمله بسط تیلور، ۷۷ است که در مقابل پیچیدگی قسمت همبسته‌سازها، صرفه‌نظر می‌شود. بنابراین، میزان پیچیدگی الگوریتم پیشنهادی به میزان تعداد همبسته‌سازهای به‌کار گرفته شده، افزایش می‌یابد. لذا، در نهایت پیچیدگی این الگوریتم 205686 می‌باشد.

درواقع، هزینه محاسباتی این طرح به دلیل اضافه نمودن تعداد همبسته‌سازها افزایش می‌یابد که در گیرنده نرم‌افزاری موجب افزایش زمان ردیابی خواهد شد. در اینجا، افزایش تعداد همبسته‌سازها از ۶ به ۱۸ عدد موجب افزایش زمان ردیابی از s $181/87$ به $258/08$ در هر کانال شد که افزایش $41/35\%$ را نشان می‌دهد. این نتایج در گیرنده نرم‌افزاری بر پایه نرم‌افزار Matlab در کامپیوتری با قدرت پردازنده $2/5\text{ GHz}$ که دارای حافظه داده با ظرفیت 6 GBytes می‌باشد، به‌دست آمده است.

در پایان، به‌منظور صحت‌سنجی دقیق‌تر، روش پیشنهادی با دیگر روش‌های معمول در موضوع آشکارسازی و مقابله با فریب مورد مقایسه کیفی قرار گرفت که نتایج آن در جدول (۳) ملاحظه می‌گردد.

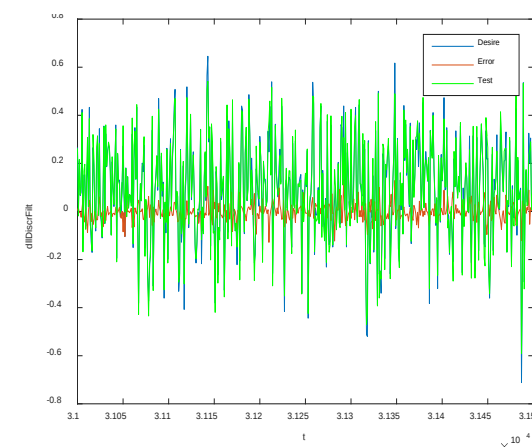


شکل (۵): بلوک دیاگرام شبکه عصبی سه لایه ادراک



شکل (۶): نتیجه محاسبه خطای DLL توسط شبکه

عصبی در فاز آموزش



شکل (۷): نتیجه محاسبه خطای DLL توسط شبکه

عصبی در فاز آزمون

۵- نتایج

برای ارزیابی روش پیشنهادی ابتدا شبکه عصبی موردنظر با داده‌های بدون اختلال آموزش یافته و پس از تعیین ضرایب شبکه، شبکه عصبی در حلقه ردیابی گیرنده قرار گرفت. شکل (۶) نتیجه محاسبه خطای DLL توسط شبکه عصبی در فاز آموزش و شکل (۷) نتیجه محاسبه خطای DLL توسط شبکه عصبی در فاز آزمون را نشان می‌دهند.

جدول (۱): نتایج حاصل از اعمال الگوریتم مقابله با فریب.

پایگاه داده‌ها	قبل از اعمال الگوریتم پیشنهادی				بعد از اعمال الگوریتم پیشنهادی				درصد کاهش فریب
	X(m)	Y(m)	Z(m)	RMS(m)	X(m)	Y(m)	Z(m)	RMS(m)	
مجموعه داده اول	۳۲۳۵۵۳ ۷۸/۳	۴۰۵۳۴۶ ۶۵/۴	۳۷۰۳۷۰ ۹۹/۶	۷۸۰/۱۴	۳۲۳۴۹۷ ۱۷/۹	۴۰۵۳۰۶ ۹۵/۴	۳۷۰۳۵ ۵۵/۱۸	۸۰/۹۱	۸۹/۶۲
مجموعه داده دوم	۳۲۳۵۵۱ ۹۲/۵	۴۰۵۳۴۵ ۰۶/۲	۳۷۰۳۷۰ ۱۸/۱	۷۵۷/۵۸	۳۲۳۴۹۰ ۶۹/۴	۴۰۵۲۹۹ ۲۱/۴	۳۷۰۳۴۶ ۷۵/۹	۴۵/۴۳	۹۴/۰۰
مجموعه داده سوم	۳۲۳۵۲۵ ۹۷/۲	۴۰۵۳۲۶ ۵۹/۹	۳۷۰۳۵۹ ۶۹/۸	۴۲۱/۸۵	۳۲۳۴۹۸ ۳۹/۰	۴۰۵۳۰۶ ۵۷/۰	۳۷۰۳۵۱ ۸۱/۵	۷۷/۴۱	۸۱/۶۴

جدول (۲): مقایسه روش پیشنهادی با سایر روش‌ها.

روش کاهش فریب	درصد کاهش فریب	محل اعمال الگوریتم
روش نیلسون [۱۲]	٪۷۴	اکتساب و ردیابی
روش تیموری [۳]	٪۷۰	ناوبری
روش پیشنهادی	٪۸۸	ردیابی

جدول (۳): مقایسه کیفی روش پیشنهادی با سایر روش‌ها.

روش کار	محدودیت	مزیت	تجهیزات مورد نیاز	معیار	آشکار سازی	مقابله
نظارت بر توان	محدوده بزرگ عدم کارایی	تشخیص آسان و پیچیدگی کم	ارتقاء نرم افزاری و سخت افزاری	توان سیگنال	بلی	خیر
نظارت بر همبستگی	عدم کارایی در حضور چند مسیری	تشخیص آسان	ارتقاء نرم افزاری	شاخه‌های همبسته ساز	بلی	خیر
نظارت بر زمان ورود	تشخیص پس از تسلط فریبنده و قابلیت پیش بینی بیت‌ها توسط فریبنده	تشخیص آسان	ارتقاء نرم افزاری	داده‌های ناوبری	بلی	خیر
پردازش فضایی	عدم کارایی در حملات پیچیده	قابلیت اطمینان بالا	ارتقاء نرم افزاری و سخت افزاری	سیگنال IF	بلی	بلی
روش مبتنی بر موجک	عدم کارایی در حملات هماهنگ نشده	پیاده سازی آسان	ارتقاء نرم افزاری	تابع اکتساب	خیر	بلی
روش پیشنهادی	غیر قابل اطمینان در حملات پیچیده با توان تطبیق یافته	قابلیت اطمینان بالا	ارتقاء نرم افزاری	شاخه همبسته ساز	بلی	بلی

۶- نتیجه گیری

بیشتر تابع همبستگی فراهم می‌شود. در این مقاله، با تلفیق معماری چند همبسته ساز و شبکه عصبی ادراک سه لایه (۶-۳-۱) خروجی همبسته سازها بررسی شده و میزان خطای DLL تصحیح می‌شود. عملکرد الگوریتم پیشنهادی در سه سناریو فریب ارزیابی شد که نتایج حاکی از کاهش ٪۸۸/۴۲ خطای ناشی از فریب می‌باشد.

در حمله فریب، سیگنال اختلال با ساختاری مشابه سیگنال اصلی GPS منتشر می‌شود. حضور این سیگنال مؤثر بر مقادیر تابع همبستگی اندازه گیری شده در گیرنده خواهد بود و موجب افزایش تعداد قله‌های ایجاد شده در فضای همبستگی خواهد شد. لذا با افزایش تعداد همبسته سازها در حلقه ردیابی امکان بررسی

۷- مراجع

- Method Using a Multi-Antenna Array," Proceedings of the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2012), pp. 1233-1243, 2012.
- [16] J. Nielsen, A. Broumandan, and G. Lachapelle, "GNSS Spoofing Detection for Single Antenna Handheld Receivers," *Navigation*, vol. 58, no. 4, pp. 335-344, 2011.
- [17] J. Nielsen, A. Broumandan, and G. Lachapelle, "Spoofing Detection and Mitigation with a Moving Handheld Receiver," *GPS world*, vol. 21, no. 9, pp. 27-33, 2010.
- [18] P. Y. Montgomery, "Receiver-Autonomous Spoofing Detection: Experimental Results of a Multi-Antenna Receiver Defense against a Portable Civil GPS Spoofer," in *Radionavigation Laboratory Conference Proceedings*, 2011.
- [19] K. D. Wesson, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "An Evaluation of the Vestigial Signal Defense for Civil GPS Anti-Spoofing," in *Radionavigation Laboratory Conference Proceedings*, 2011.
- [20] P. Daniel and E. Todd, "Characterization of Receiver Response to Spoofing Attacks," Proceedings of the 24th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2011), Portland, pp. 2608-2618, 2011.
- [21] M. Pini, M. Fantino, A. Cavaleri, S. Ugazio, and L. L. Presti, "Signal Quality Monitoring Applied to Spoofing Detection," in Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011), pp. 1888-1896, 2011.
- [22] B. M. Ledvina, W. J. Bencze, B. Galusha, and I. Miller, "An In-line Anti-spoofing Device for Legacy Civil GPS Receivers," in Proceedings of the 2010 International Technical Meeting of the Institute of Navigation, pp. 698-712, 2010.
- [23] A. Cavaleri, B. Motella, M. Pini, and M. Fantino, "Detection of Spoofed GPS Signals at Code and Carrier Tracking Level," in 2010 5th IEEE ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), pp. 1-6, 2010.
- [24] A. Broumandan, A. Jafarnia-Jahromi, and G. Lachapelle, "Spoofing Detection, Classification and Cancellation (SDCC) Receiver Architecture for a Moving GNSS Receiver," *GPS Solut.*, vol. 19, no. 3, pp. 475-487, 2015.
- [25] A. Baziari, M. Mosavi, and M. Moazedi, "Spoofing Mitigation Using Double Stationary Wavelet Transform in Civil GPS Receivers," *Wireless Personal Communications*, vol. 109, no. 3, pp. 1827-1844, 2019.
- [26] M. Mosavi, R. Zebarjad, and M. Moazedi, "Novel Anti-spoofing Methods Based on Discrete Wavelet Transform in the Acquisition and Tracking Stages of Civil GPS Receiver," *Int. J. Navig. Obs.*, vol. 25, no. 4, pp. 449-460, 2018.
- [27] Y. Guo, L. Miao, and X. Zhang, "Spoofing Detection and Mitigation in a Multi-correlator GPS Receiver Based on the Maximum Likelihood Principle," *Sensors*, vol. 19, no. 1, p. 37, 2019.
- [28] J. N. Gross, C. Kilic, and T. E. Humphreys, "Maximum-likelihood Power-distortion Monitoring for GNSS-signal Authentication," *IEEE Trans Aerosp Electron Syst*, vol. 55, no. 1, pp. 469-475, 2019.
- [1] K. D. Wesson, J. N. Gross, T. E. Humphreys and B. L. Evans, "GNSS Signal Authentication Via Power and Distortion Monitoring," in *IEEE Trans Aerosp Electron Syst*, vol. 54, no. 2, pp. 739-754, April 2018.
- [2] M. Moazedi, M. R. Mosavi, and A. Sadr, "Real-time interference detection in tracking loop of GPS receiver," *Iranian Journal of Electrical and Electronic Engineering*, vol. 13, no. 2, pp. 194-204, 2017.
- [3] P. Teymouri, M. Mosavi, and M. Moazedi, "Delay Spoofing Reduction in GPS Navigation System based on Time and Transform Domain Adaptive Filtering," *Iranian Journal of Electrical and Electronic Engineering*, vol. 14, no. 3, pp. 222-235, 2018.
- [4] M. R. Mosavi, M. Moazedi, M. J. Rezaei, and A. tabatabaei, "Interference Mitigation in GPS Receivers," *Iran University of Science and Technology Publications*, 2015.
- [5] M. Moazedi, M. Mosavi, Z. Nasrpooya, and A. Sadr, "GPS Spoofing Mitigation using Adaptive Estimator in Tracking Loop," *Journal of Electronical & Cyber Defence*, vol. 6, no. 3, 2018. (In Persian)
- [6] F. Dovis, "GNSS Interference Threats and Countermeasures," *Artech House*, 2015.
- [7] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques," *Int. J. Navig. Obs.*, vol. 2012, 2012.
- [8] D. Borio, F. Dovis, H. Kuusniemi, and L. L. Presti, "Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers," *Proc. IEEE*, vol. 104, no. 6, pp. 1233-1245, 2016.
- [9] B. Xu, Q. Jia, and L. T. Hsu, "Vector Tracking Loop-Based GNSS NLOS Detection and Correction: Algorithm Design and Performance Analysis," *IEEE Trans Instrum Meas*, vol. 69, no. 7, pp. 4604-4619, 2019.
- [10] 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," in *Radionavigation Laboratory Conference Proceedings*, 2008.
- [11] A. Jafarnia Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS Spoofer Countermeasure Effectiveness Based on Signal Strength, Noise Power and C/N0 Measurements," *Int. J. Satell. Commun. Netw*, vol. 30, no. 4, pp. 181-191, 2012.
- [12] J. Nielsen, V. Dehghanian, and G. Lachapelle, "Effectiveness of GNSS Spoofing Countermeasure Based on Receiver CNR Measurements," *Int. J. Navig. Obs.*, vol. 2012, pp. 1-9, 2012.
- [13] S. Lo, D. De Lorenzo, P. Enge, D. Akos, and P. Bradley, "Signal Authentication: A secure Civil GNSS for Today," *Inside GNSS*, vol. 4, no. 5, pp. 30-39, 2009.
- [14] S. C. Lo and P. K. Enge, "Authenticating Aviation Augmentation System Broadcasts," in *IEEE/ION Position, Location and Navigation Symposium*, Indian Wells, CA, 2010.
- [15] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandan, and G. Lachapelle, "A low-Complexity GPS Anti-Spoofing

- [31] S. Semanjski, I. Semanjski, W. De Wilde, and A. Muls, "Use of Supervised Machine Learning for GNSS Signal Spoofing Detection with Validation on Real-world Meaconing and Spoofing Data—part I," *Sensors*, vol. 20, no. 4, 2020.
- [32] P. Borhani Daria, H. LI, P. Wu, and P. Closas, "Deep Neural Network Approach to Detect GNSS Spoofing Attacks," *Proc. ION GNSS*, 3241-3252, September 21-25, 2020.
- [29] E. Shafiee, M. 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*, vol. 71, no. 1, pp. 169-188, 2018.
- [30] S. Tohidi and M. R. Mosavi, "Effective Detection of GNSS Spoofing Attack Using A Multi-Layer Perceptron Neural Network Classifier Trained by PSO," *2020 25th International Computer Conference, Computer Society of Iran (CSICC)*, Tehran, Iran, pp. 1-5, 2020.

Reducing the Interference Effect on GPS Receivers Using the Multi-Correlation Architecture

S. Tohidi¹, M. R. Mosavi^{2*}, M. Moazedi³

* School of Electrical Engineering, Iran University of Science and Technology, Tehran ,Iran

(Received: 30/10/2020, Accepted: 04/07/2021)

ABSTRACT

The use of Global Positioning System (GPS) in highly automated systems is increasing day by day. Therefore, its security of these systems is getting important more and more. The reliability of the obtained position by GPS is in danger by spoofing attacks. A spoofer transmits replicas of authentic satellite signals to force the victim receiver to misjudge the its position estimate. Numerous researches have been focused on spoofing detection and mitigation in the GPS receivers. In this paper, mitigation of spoofing attack is suggested by using multi-correlator architecture associated with neural network. Spoofing signal is generated by mixing two signals which are produced by authentic GPS signal and its shifted. The results of the simulations which was performed in the software defined receiver, indicate the solution was effective in mitigating the spoofing attack. By studying three scenarios of spoofing, the proposed method was evaluated and the results show that the rate of reduction of deception error is 88.42% by using multi-correlation architecture.

Keywords: Spoofing, GPS Receiver, Multi-correlation Architecture, Neural Network

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