مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
سال سوم، شماره ۱، بهار ۱۳۹۴، ص ۸۰-۶۹

تشخیص و آشکارسازی حمله فریب در گیرنده تک فرکانسه GPS مبتنی بر شبکه عصبی چندلایه

ابراهیم شفیعی[۱]، سید محمدرضا موسوی[۲*]، مریم معاضدی[۳]

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

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

۳- دانشجوی دکتری، دانشکده مهندسی برق، دانشگاه علم و صنعت ایران

(دریافت: ۹۳/۱۰/۰۴؛ پذیرش: ۹۴/۲/۲۱)

چکیده

فریب GPS تلاشی برای گمراه کردن گیرنده GPS با انتشار سیگنال‌های جعلی است. ساختار سیگنال فریب شبیه به سیگنال‌های معتبر ماهواره‌های GPS و کمی قوی‌تر از آن‌ها است. در سال‌های اخیر راه‌کارهای متنوعی جهت تشخیص و کاهش فریب ارائه گردیده است. شبکه‌های عصبی، روش محاسباتی نوینی برای یادگیری ماشین و سپس اعمال دانش به‌دست‌آمده در جهت پیش‌بینی پاسخ خروجی سامانه‌های پیچیده هستند. در مقاله حاضر، استفاده از سیستم هوشمند رویکرد اصلی در الگوریتم پیشنهادی تشخیص فریب GPS قرار داده‌شده است. با استفاده از مشخصه‌های همبستگی، سیگنال‌ها را با کمک شبکه عصبی دسته‌بندی نموده‌ایم. شاخص‌های فاز مقدم و مؤخر، دلتا و سطح کل سیگنال را به‌عنوان ورودی‌های شبکه عصبی چندلایه اعمال کرده تا سیگنال فریب را در حلقه ردیابی گیرنده GPS شناسایی کند. سیگنال‌های فریب و معتبر الگوی آماری متفاوتی در شاخص‌های نامبرده دارند و شبکه عصبی این تفاوت را تشخیص می‌دهد. شبکه عصبی با خطای کمتری نسبت به روش‌های پیشین سیگنال‌ها را دسته‌بندی می‌نماید، زیرا می‌تواند چندین روش را به‌طور هم‌زمان به‌کار گیرد. درنهایت، کمترین دقت به‌دست‌آمده از شبیه‌سازی گیرنده نرم‌افزاری مبتنی بر شبکه عصبی، دقت ۹۸/۷۸ درصدی در تشخیص صحیح سیگنال فریب از سیگنال معتبر است. همچنین بیشترین زمان تشخیص سیگنال فریب ۰٫۶ ثانیه است.

واژه‌های کلیدی: فریب GPS، شبکه عصبی، تشخیص و آشکارسازی سیگنال فریب.

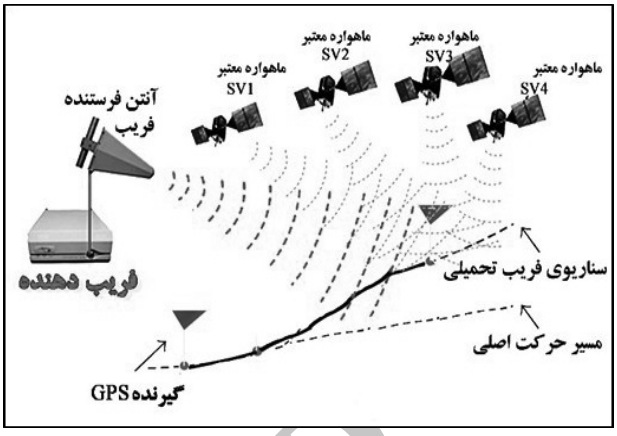
۱. مقدمه

افزایش اهمیت امنیت در سامانه های مخابراتی و الکترونیکی منجر به ارائه روش‌های محافظت از سیگنال‌ها شده است. از جمله سیگنال‌های مهم موجود می‌توان سیگنال GPS[1] را نام برد. سیگنال دریافتی از ماهواره‌های GPS در سطح زمین بسیار ضعیف و در برابر تداخل در باند آسیب‌پذیر است؛ بنابراین یک تداخل کم توان نیز می تواند به راحتی گیرنده GPS را فریب دهد. فریب یک دخالت عمدی است که هدف آن وادار کردن گیرنده ی GPS به تولید سیگنال ناوبری غلط است. سیگنال فریب می‌تواند تأخیر در انتشار مجدد سیگنال ذخیره‌شده معتبر GPS باشد. شکل (۱) یک فریب در حال اتفاق را نشان می‌دهد که فریب دهنده توانسته با در اختیار گرفتن پیک همبستگی گیرنده مطابق شکل (۲) ، داده ناوبری غلط تولید کند تا گیرنده GPS از مسیر اصلی به مسیر مورد نظر فریب‌دهنده منحرف گردد [۳-۱].

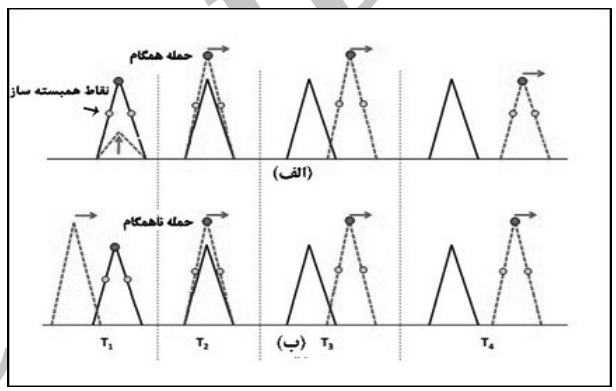
شکل (۲) دنباله‌ای از فریم‌ها را در دو نوع حمله به گیرنده GPS نشان می‌دهد. سه نقطه نشان‌دهنده نقاط ردیابی حلقه قفل تأخیر هستند که به‌طور پیوسته تلاش می‌کنند به‌صورتی خود را تطبیق دهند که نقطه مرکزی بیشینه و نقاط جانبی هم‌تراز شوند. بازه زمانی T_1 نشان می‌دهد که نقاط ردیابی به‌خوبی با بیشینه همبستگی سیگنال اصلی تطبیق پیدا کرده‌اند. در یک حمله فریب هم‌گام، درحالی‌که بیشینه سیگنال جعلی به‌طور پنهانی نزدیک می‌شود، بیشینه سیگنال جعلی در ابتدا کوچک‌تر از بیشینه سیگنال اصلی است. بعد از آن‌که تأخیر زمانی بیشینه همبستگی سیگنال فریب داده‌شده با بیشینه اصلی تطبیق پیدا کرد، توان سیگنال جعلی به تدریج افزایش پیداکرده تا شروع به کنترل نقاط ردیابی کند. درنهایت، سیگنال جعلی کنترل حلقه را تحت اختیار خود درآورده است. سه‌نقطه نمایش داده‌شده نمادی از سه‌شاخه همبسته‌ساز در

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

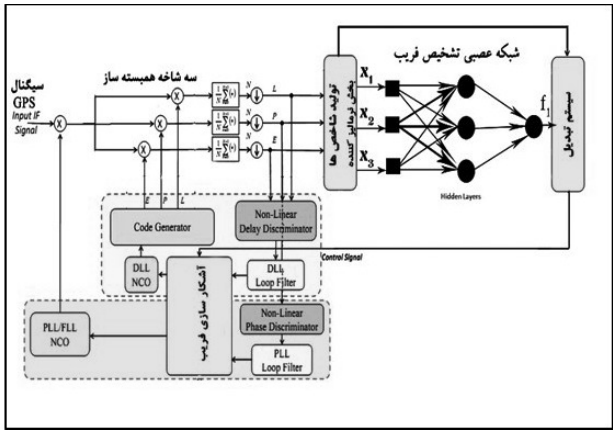
1-Global Positioning System



شکل (۱). سناریوی یک فریب در حال اتفاق، انحراف گیرنده GPS از مسیر اصلی.



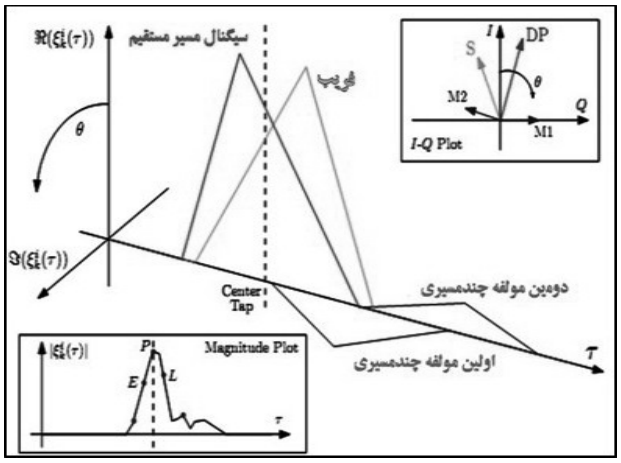
شکل(۲). دو سناریوی فریب، شکل ناحیه همبستگی در حلقه ره‌گیری: الف) فریب همگام و ب) فریب ساده [۸].



شکل (۳). ساختار گیرنده بردار پایه تشخیص فریب (رویکرد پیشنهادی مبتنی بر شبکه عصبی)

گیرنده GPS می‌باشند که در شکل (۳) ترسیم‌شده‌اند. همچنین نقاط همبستگی مختلط به نام‌های همبسته‌ساز بی‌درنگ[1]، همبسته‌ساز مقدم و مؤخر[2] (P، E و L) هستند که در شکل (۴) نشان داده شده‌اند [۵-۴].

1- Prompt Correlator
2- Early-Late Correlator



شکل(۴). ساختار سیگنال فریب، شکل ناحیه همبستگی مختلط یک حمله فریب و نمودار دامنه و فاز

روش‌های مختلفی برای تشخیص و مقابله با فریب وجود دارند [۶]. اغلب روش‌های مقابله با فریب متناسب با نوع حمله فریب طراحی و پیاده‌سازی می‌شوند. یکی از روش‌های ابتدایی در این زمینه به تحلیل دامنه‌های خروجی همبسته‌ساز برای آشکارسازی فریب می‌پردازد. رویکرد دیگر به بررسی نسبت حامل به نویز[3] (C/No) پرداخته و با تغییرات ناگهانی در سیگنال دریافتی حضور فریب را مشخص می‌نماید [۷].

در شرایط مناسب جوی، فقط تغییرات یونسفر و حرکت ماهواره‌ها می‌توانند تغییرات همواره تدریجی را در توان دریافتی به وجود آورند. در گیرنده ضدفریب، پی‌درپی C/No بررسی می‌شود و هر تغییر غیرعادی نسبت حامل به نویز می‌تواند نشانه‌ای از وجود حمله فریب باشد [۹].

روش‌های نظارت بر کیفیت سیگنال[4] (SQM) قله‌های غیرطبیعی نوک‌تیز سیگنال و یا یکسانی پیک‌های روی‌هم افتاده سیگنال GPS را که توسط فریبنده تحمیل می‌شود، تشخیص می‌دهند. این روش‌ها وقتی به‌کار گرفته می‌شوند که تابع همبستگی مختلط، نامتقارن می‌گردد. بررسی و تصمیم‌گیری برای حضور یا عدم حضور حمله فریب با آزمون‌های فرضیه آماری انجام می شود [۱۱-۱۰]. دفاع سیگنال باقی‌مانده[5] (VSD) روشی بر اساس نظارت بر خرابی ناحیه همبستگی مختلط است تا یک حمله فریب در جریان را تشخیص دهد. عملکرد این روش به میزان تضعیف سیگنال اصلی GPS در طول حمله فریب وابسته است. در این حالت اثری از سیگنال معتبر باقی می‌ماند و به‌عنوان یک انحراف از تابع همبستگی مختلط آشکار می‌شود [۱۲].

3-Carrier to Noise Ratio
4-Signal Quality Monitor
5-Vestigial Signal Defense

در روش بردار پایه[1] گیرنده GPS در حال ردیابی، بر روی تعقیب پیک همبستگی سیگنال اصلی تمرکز دارد. در این روش دامنه های خروجی پنج شاخه همبسته‌گر به‌طور اختصاصی در آزمون فرضیه آماری برای آشکارسازی فریب بررسی می‌گردند. به عبارتی خروجی بلوک هیستوگرام بر مبنای میانگین انحراف معیار خروجی همبسته‌سازها تعریف می‌شود و مقدار آزمون برای خروجی محاسبه می‌گردد. اگر همه پنج شاخه همبسته‌ساز زیر حد آستانه بودند، سیگنال معتبر است و تا زمانی که همه مقادیر آزمون به ازای همه شاخه‌ها به زیر حد آستانه نرسند، وجود حمله فریب مورد تأیید است [۱۲-۱۳].

تفکیک زمان ورود[2] (TOA) درصورتی‌که انتقال بیت داده ناوبری در لحظاتی از زمان با فاصله‌گذاری غیر از ۲۰ms رخ دهد، حمله فریبنده ظاهر می‌شود [۱۴]. در روش بررسی سازگاری موقعیت‌یابی گیرنده GPS با دیگر روش‌های تعیین موقعیت، می‌توان از اطلاعات تجهیزات کمکی موقعیت‌یابی برای تفکیک تهدید فریب کمک گرفت. به‌کاربردن این روش، پیچیدگی سخت‌افزاری و نرم‌افزاری گیرنده GPS را افزایش می‌دهد [۱۵].در رویکرد بررسی سازگاری و تخمین پارامترهای سیگنال ورودی، گیرنده سیگنال GPS را دریافت، ذخیره و با داده‌های دقیقه قبل مقایسه می‌کند. گیرنده با استخراج مشخصه‌های سیگنال و مشاهده هرگونه تغییرات بزرگ و پیش‌بینی‌نشده در اندازه آن، وجود فریب را اعلام می‌کند [۱۶].

روش انتخاب پیک معتبر بر اساس مشخصه CNR[3] ادغام شده با یک قاعده تصمیم‌گیری در مقابله با فریب به‌کار گرفته می‌شود. این روش پیاده‌سازی ساده‌ای دارد، ولی در حمله‌های تأخیری کارآیی مطلوبی ندارد [۱۷].

از دیگر روش‌های ارائه‌شده در این حوزه می‌توان به بررسی اندازه توان اشاره نمود. این روش با بررسی توان سیگنال‌های اصلی و جعلی می‌تواند وجود سیگنال فریب را در سناریوهای مختلفِ فریب، تشخیص دهد. معمولاً فرستنده‌های فریب، چندین سیگنال جعلی را از یک آنتن می‌فرستند، درحالی‌که سیگنال‌های معتبر GPS از ماهواره‌های مختلف در مسیرهای گوناگون فرستاده می‌شوند. از این‌رو می‌توان از روش پردازش فضایی، برای تخمین اثر سه‌بعدی سیگنال‌های دریافت شده و تفکیک این سیگنال‌ها استفاده کرد و اقدام به کاهش فریب نمود [۱۸].

به‌دلیل محدودیت‌های عملی، معمولاً فرستنده های فریب (به جزء فریب پیچیده) چندین سیگنال جعلی را از یک آنتن می‌فرستند، درحالی‌که سیگنال‌های معتبر GPS از ماهواره‌های مختلف در مسیرهای گوناگون فرستاده می‌شوند. ازاین رو می‌توان روش پردازش فضایی را برای تخمین اثر سه‌بعدی سیگنال‌های دریافت‌شده و تفکیک این سیگنال‌ها که رابطه فضایی مشخصی دارند، به‌کار گرفت. روش زاویه ورود برمبنای این واقعیت، 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. آرایه چند آنتنه، آرایه دو آنتنه و آرایه مصنوعی تک آنتنه متحرک سه روش متفاوت برای پیاده‌سازی آرایه مورد نظر هستند [۱۹-۲۲].

هدف از این مقاله، ارائه روش نوین آشکارسازی فریب سیگنال GPS مبتنی بر شبکه عصبی برای پیاده‌سازی در گیرنده نرم‌افزاری GPS است. بدین صورت که در حضور سیگنال فریب، شبکه عصبی به‌محض مشاهده هر توزیع غیرعادی، نسبت به آن واکنش نشان می‌دهد. این روش درواقع یک دفاع نرم‌افزاری محسوب می شود و بدون تغییر سخت‌افزاری در گیرنده GPS آن را در برابر فریب مقاوم می‌نماید. درنتیجه هزینه اجرای کمی دارد و ابعاد گیرنده را افزایش نمی‌دهد. در ادامه پس از توضیح پایه تئوری روش پیشنهادی، روش کار شبکه عصبی ارائه‌شده شرح داده می‌شود. درنهایت بعد از گزارش نتایج حاصل از ارزیابی شبکه عصبی به مقایسه کیفی با دیگر الگوریتم‌های شناسایی فریب می‌پردازیم.

۲- الگوریتم پیشنهادی تشخیص فریب مبتنی بر شبکه عصبی

از مزایای شبکه عصبی می‌توان به مواردی هم چون یادگیری تطبیقی، تحمل خطا، دسته‌بندی، تعمیم‌دهی، پایداری و انعطاف‌پذیری اشاره کرد؛ بنابراین می‌توان به‌منظور مقابله با فریب، از سامانه‌های هوشمند مانند شبکه عصبی بهره برد که در ادامه به شرح و بسط این ابزار و شبیه‌سازی آن جهت آشکارسازی فریب پرداخته می‌شود [۲۳].

شبکه عصبی پیشنهادی می‌تواند از چندین معیار و روش به‌صورت ترکیبی استفاده کند و ویژگی منحصربه‌فرد هر روش را به خود اختصاص دهد. روش‌های بررسی همبستگی در چندمسیری دچار خطا می‌شوند و روش‌های بر پایه توان به اختلال‌های دیگر حساس هستند. شبکه عصبی با ترکیب روش‌های نامبرده دقت و صحت اندازه‌گیری را بهبود می‌دهد و امکان تشخیص فریب‌های پیچیده با حضور چندمسیری و نویز را مؤثر می‌سازد [۲۴].

در این مقاله برای مقابله با فریب در گیرنده GPS از شبکه عصبی برای آشکار کردن پیک‌های همبستگی جعلی هنگامی‌که

1-Vector-Base
2-Time of Arrival
3- Carrier to Noise Ratio

نزدیک به پیک اصلی هستند، استفاده شده است. شبکه عصبی با بهره‌گیری از سه شاخه همبسته‌ساز در حلقه ردیابی امکان تشخیص فریب را فراهم می‌کند.

در حضور یک سیگنال فریب، شبکه عصبی به محض مشاهده توزیع غیرعادی هر خروجی همبسته‌ساز با کمک ابزار حد آستانه‌های ضرایب معیار VSD و نظارت بر سطح سیگنال به‌هنجار شده همبستگی، فریب را آشکار می‌کند. شکل (۳) ساختار گیرنده تشخیص فریب مبتنی بر شبکه عصبی پیشنهادی را نشان می دهد. سیگنال GPS پس از عبور از سه شاخه همبسته‌گر وارد بلوک مولد شاخص‌های تشخیص فریب می‌شود. پس از آن به‌هنجار شده‌اند و آماده اعمال به شبکه عصبی پیشنهادی می‌گردند. به‌هنجار کردن مقادیر شاخص‌ها باعث جلوگیری از اشباع شدن نرون‌ها می‌شود. به دلیل متفاوت بودن گستره بازه تغییرات هر یک از شاخص‌های ورودی شبکه عصبی، آن‌ها را در محدوده [۱- و ۱+] به‌هنجار می‌کنیم. درصورتی‌که به‌هنجار نشوند و تغییرات در حد بالای مقادیر یک شاخص رخ دهد، باعث کاهش حساسیت نرون‌ها به ورودی‌ها می‌شود و با توجه به نمودار تابع tansig به‌ازای تغییرات در مقادیر بالای یک شاخص ورودی یک نرون، تغییرات جزئی در خروجی خواهد داشت و نرون اشباع‌شده است. شبکه با توجه به ورودی‌های خود می‌تواند وجود فریب را با یک شدن خروجی خود تشخیص دهد. همان‌گونه که در نمودار دامنه فاز شکل (۴) مشاهده می‌شود، تطبیق فاز سیگنال فریب با سیگنال معتبر صورت نگرفته است و این موضوع در نمودار I-Q بالای شکل مشخص‌تر است. سیگنال‌های چندمسیری[1] به علت انعکاس از اشیاء علاوه بر تضعیف دامنه دچار تأخیر نسبت به سیگنال مسیر مستقیم ماهواره می‌شوند. M_1 و M_2 مؤلفه اول و دوم چندمسیری[1] می‌باشند و مؤلفه‌های دیگر به‌علت تضعیف زیاد در نظر گرفته نشده است. روابط (۱) و (۲)، معادله سیگنال نمایش داده شده است. اساس دسته‌بندی سیگنال‌ها در این مطالعه، با توجه به ویژگی‌های بردارهای سیگنال‌ها بوده است. در واقع این روش از دشوار بودن ایجاد فریبی که بتواند به‌طور همزمان هر سه مشخصه توان، فاز و توزیع همبستگی سیگنال فریب را منطبق با سیگنال اصلی نگه دارد، استفاده می‌نماید؛ بنابراین معیارهای VSD و سطح سیگنال بهنجار شده از خروجی همبسته‌ساز استخراج و به ورودی‌های شبکه عصبی اعمال می‌شوند.

نحوه عملکرد شبکه عصبی MLP[2] برای دسته‌بندی و تخمین نظارت‌شده فریب بدین‌صورت است که یک بردار سه‌بعدی از معیارهای تشخیص فریب به لایه ورودی شبکه با سه گره وارد می‌شود. این بردار شامل مشخصه‌های مربوط به سیگنال GPS دریافتی است. فرض بر این است که برای هر سیگنال ورودی دو حالت فریب و معتبر وجود دارد. این دو حالت فریب و معتبر به ترتیب به دو عدد ۱+ و ۱- در لایه خروجی نسبت داده شده‌اند. ورودی‌ها پس از محاسبات داخلی به دسته‌ای که نشان‌دهنده ماهیت سیگنال است، در لایه خروجی با یک نرون نگاشته می‌شوند [۲۵].

۳- طراحی و ارزیابی عملکرد شبکه عصبی پیشنهادی

هنگام کار با شبکه عصبی MLP با دو مسئله انتخاب معماری مناسب و انتخاب الگوریتم آموزشی مناسب روبرو هستیم. معماری مناسب به معنی انتخاب بهینه تعداد لایه‌ها، تعداد نرون‌ها در هر لایه و نوع تابع تحریک هر نرون می‌باشد و الگوریتم بهینه شبکه‌های عصبی مبتنی بر مجموعه داده‌ها و ویژگی‌های آنان است. قبل از استفاده از شبکه عصبی برای دسته‌بندی سیگنال‌ها، ابتدا باید شبکه توسط بردار معیار سیگنال با دسته مشخص آموزش داده شود. شبکه عصبی شبیه‌سازی‌شده دارای سه معیار تشخیص فریب است که تلاش می‌کند به کمک فرآیند یادگیری LM[3] و نرون‌های پردازشگر با شناخت روابط ذاتی بین داده‌ها، نگاشتی میان فضای ورودی یا همان معیارهای تشخیص فریب (لایه ورودی) و فضای ماهیت سیگنال (لایه خروجی) برقرار کند [۲۶]. لایه‌های مخفی، اطلاعات دریافتی از لایه ورودی را پردازش کرده و در اختیار لایه خروجی قرار می‌دهند. هر شبکه با دریافت داده‌های معتبر و فریب آموزش می‌بینند. آموزش فرآیندی است که درنهایت منجر به یادگیری می‌شود. یادگیری شبکه زمانی انجام می‌گردد که وزن‌های ارتباطی بین لایه‌ها چنان تغییر کند که اختلاف بین مقادیر پیش‌بینی‌شده و محاسبه‌شده در حد قابل قبولی باشد. با دست‌یابی به این شرایط، فرآیند یادگیری محقق شده است. این وزن‌ها بیانگر حافظه و دانش شبکه می‌باشند. شبکه عصبی آموزش‌دیده می‌تواند جهت تشخیص فریب با مجموعه جدید داده‌های حقیقی GPS به‌کار رود [۲۷].

الگوریتم LM، الگوریتمی برای همگرایی سریع در آموزش شبکه‌های عصبی است. این الگوریتم، یک روش استاندارد برای مسائل حداقل مربعات غیرخطی بوده و به‌عنوان ترکیبی از روش نیوتن گوس و بیشترین شیب نزول بیان می‌شود. در این مقاله به‌منظور آموزش‌گیرنده GPS مجهز به تشخیص فریب از الگوریتم مطرح LM استفاده گردیده که از سرعت همگرایی بهتری در مقایسه با روش‌های دیگر استاندارد برخوردار است و محاسبات و حافظه کمتری لازم دارد [۲۷].

1-Multi-path
2-Multi-Layer Perceptron
3-Levenberg Marqurardt

در این مطالعه، مراحل آماده‌سازی شبکه عصبی جهت استفاده در الگوریتم‌های مقابله با فریب به‌صورت زیر است:

مرحله اول

این گام شامل به‌دست آوردن تابع مختلط همبستگی (هندسه بردارها) است که با استخراج داده‌ها از خروجی سه همبسته‌ساز صورت می‌گیرد. تطبیق فاز حامل سیگنال فریب با سیگنال اصلی برای فریبنده دشوار است. اگر همبستگی سیگنال C/A تولیدی با کل سیگنال ورودی گرفته شود، یک تابع همبستگی مختلط x در زمان t و تأخیر آفست مانند شکل (۴) ایجاد می‌گردد که طبق روابط (۱) و (۲) محاسبه می‌شود [۱۱]:

$$x(t,\tau)=x_d(t,\tau)+x_m(t,\tau)+x_s(t,\tau)+\eta(t,\tau) \quad (۱)$$

$$x(t,\tau)=\alpha_d(t)R(\tau-\tau_d(t))e^{j\theta_d(t)} + \sum_{k=1}^{N}\alpha_{m,k}(t)R(\tau-\tau_{m,k}(t))e^{j\theta_{m,k}(t)} + (\alpha_s(t)R(\tau-\tau(t))e^{j\theta_S(t)})\times 1_{spoofing} \quad (۲)$$

در رابطه (۱)، x_d بیانگر تابع همبستگی سیگنال معتبر مسیر مستقیم و به عبارتی دیگر سیگنال اصلی GPS است. x_m و x_s به ترتیب مبین جزء چندمسیری و سیگنال فریب می‌باشند و η مبین نویز سفید گوسی جمع شونده است. در رابطه (۲) نیز R(τ) بیانگر همبستگی مختلط، $0\le\alpha(t)\le 1$ عامل مقیاس‌بندی، $\tau(t)$ مبین تأخیر برحسب ثانیه و فاز برحسب رادیان است که همگی متغیر با زمان هستند.

مرحله دوم

در این مرحله شاخص‌های ورودی‌های شبکه عصبی جهت بررسی سیگنال GPS تولید می‌شوند. دلیل استفاده از شاخص (معیار) VSD و سطح کل سیگنال به‌هنجار شده، انتخاب بهترین ترکیب‌بندی تحلیل سیگنال است. معیار دلتا، ضریب معیار فاز مقدم و مؤخر و سطح کل سیگنال به‌هنجار شده برای استفاده به‌عنوان ورودهای شبکه عصبی به‌کار گرفته می‌شوند. شاخص‌های فریب به‌گونه‌ای محاسبه می‌گردند تا دسته‌های خروجی شبکه عصبی باهم همبستگی کم و واریانس بالا داشته باشند. ورودی اول شبکه عصبی معیار دلتا نامیده می‌شود و مطابق رابطه (۳) است [۱۲]:

$$x_1=\Delta_\tau(t),\ \Delta_\tau(t)=\frac{I_{E,\tau}(t)-I_{L,\tau}(t)}{2I_p(t)} \quad (۳)$$

در این رابطه، $I_{E,\tau}(t)$ و $I_{L,\tau}(t)$ به ترتیب بخش حقیقی شاخه‌های مقدم و مؤخر همبستگی می‌باشند که به اندازه τ ثانیه جلوتر و عقب‌تر از شاخه بی‌درنگ Ip(t) در جزء فازی در زمان t هستند. ورودی دوم شبکه عصبی معیار فاز مقدم و مؤخر است که از رابطه (۴) محاسبه می‌گردد [۱۸]:

$$x_2=ELP_\tau(t),\ ELP_\tau(t)=\tan^{-1}\left(\frac{Q_{L,\tau}(t)}{I_{L,\tau}(t)}-\frac{Q_{E,\tau}(t)}{I_{E,\tau}(t)}\right) \quad (۴)$$

در اینجا، $Q_{E,\tau}(t)$ و $Q_{L,\tau}(t)$ به بخش موهومی شاخه‌های مقدم و مؤخر اشاره می‌کنند که به اندازه τ ثانیه جلوتر و عقب‌تر از نواخت بی‌درنگ $I_p(t)$ در جزء توان ۲ در زمان t هستند. ورودی سوم شبکه عصبی x_3 سطح کل سیگنال به‌هنجار شده است:

$$x_3=SL,\ SL=\frac{1}{T}\int_T|x(t,\tau)|^2\,d\tau \quad (۵)$$

پس از تعیین شاخص‌های ورودی، داده‌های ورودی‌های شبکه عصبی را طبق روابط (۶) و (۷) بین [۱- و ۱+] به‌هنجار می‌نماییم.

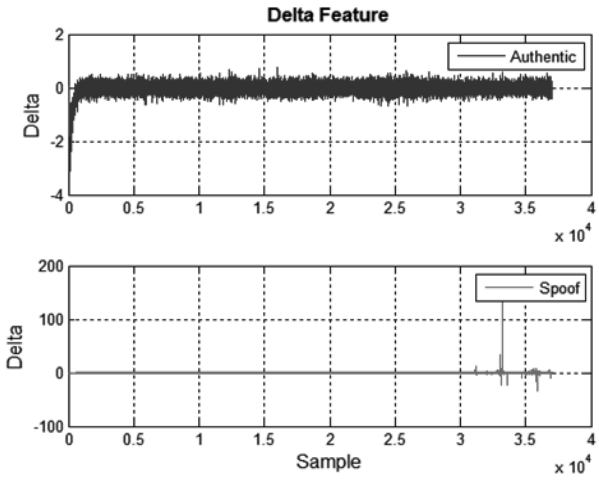
$$x_{Scale}=x_{input}\times S+O \quad (۶)$$

$$S=\frac{Hi-Low}{Max-Min},\ O=\frac{Max\times Low-Min\times Hi}{Max-Min} \quad (۷)$$

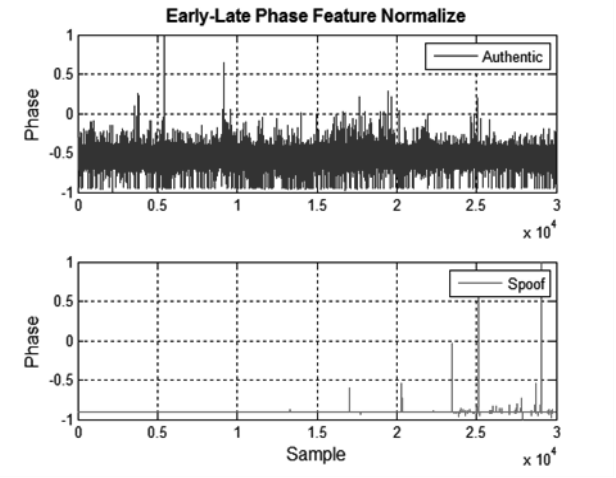
در رابطه (۶)، S و O به ترتیب مبین ضریب مقیاس و انحراف می‌باشند. پارامترهای Max و Min حداکثر و حداقل داده ورودی و Hi و Low تعیین‌کننده حدود مقیاس هستند. در شکل‌های (۷-۵) سه ورودی توصیف‌شده ترسیم شده‌اند. نمونه‌های سیگنال فریب در شاخص‌های دلتا و فاز مقدم و مؤخر شکل‌های (۶ - ۵) رفتاری متفاوت با سیگنال اصلی دارند. این بدین دلیل است که سیگنال فریب نتوانسته تطبیق فاز با سیگنال معتبر را حفظ کند و حفظ تطبیق فاز مستلزم نزدیک بودن فریب‌دهنده به مرکز فاز آنتن‌گیرنده است. فریب‌دهنده جهت در اختیار گرفتن پیک همبستگی گیرنده GPS نیاز به سطح سیگنال بالاتری نسبت به سیگنال معتبر دارد و این نیز در شکل (۷) مشاهده می‌شود. شکل (۸) فرآیند تشخص فریب الگوریتم پیشنهادی با توجه به مراحل توضیح داده‌شده را نشان می‌دهد.

مرحله سوم

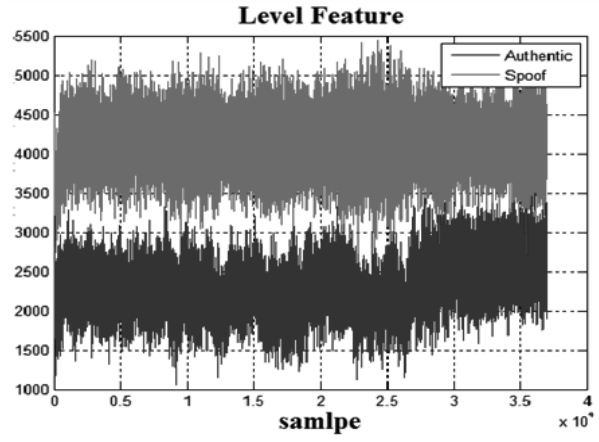
آموزش شبکه عصبی با داده‌های مناسب برای شرکت در دسته‌بندی بر اساس مشخصات آماری دسته‌ها و همچنین تفسیر دسته‌ها در این مرحله انجام می‌گردد. خروجی شبکه عصبی، f است که مبین معتبر یا جعلی بودن سیگنال ورودی است.



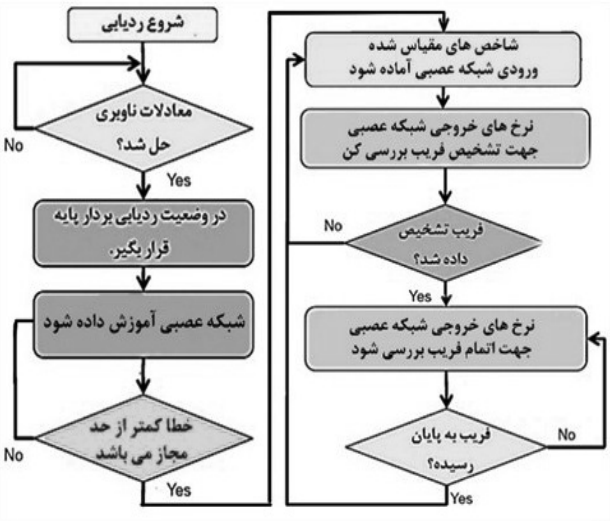
شکل(۵). ورودی اول شبکه عصبی پیشنهادی (شاخص دلتا).



شکل (۶). ورودی دوم شبکه عصبی پیشنهادی (شاخص فاز مقدم- مؤخر بهنجار)



شکل (۷). ورودی سوم شبکه عصبی پیشنهادی شاخص سطح سیگنال.



شکل(۸). الگوریتم تشخیص فریب پیشنهادی

آموزش شبکه عصبی قبل از راه‌اندازی[1] گیرنده GPS پیشنهادی با دو مجموعه داده صورت می‌گیرد. الگوریتم پیشنهادی برای گیرنده‌های تجاری تک فرکانسه در نظر گرفته شده است. به‌منظور عملکرد بی‌درنگ گیرنده، آموزش در زمان موقعیت‌یابی صورت نمی‌گیرد. داده‌ها شامل دو مجموعه داده نرم‌افزاری و اندازه‌گیری شده می‌باشند. آموزش با داده‌های واقعی ذخیره‌شده (اندازه‌گیری شده) و شبیه‌سازی‌شده (نرم‌افزاری) در حضور فریب و عدم حضور آن همراه با نویز گوسی و سیگنال چندمسیری قبل از شروع به استفاده صورت می‌گیرد. ابتدا وزن نرون‌های شبکه با داده‌های نرم‌افزاری تعیین می‌گردند و در مرحله بعدی با داده‌های اندازه‌گیری‌شده مجدداً آموزش داده می‌شود تا شبکه در محیط‌های با نویز و سیگنال چندمسیری عملکرد بهتری داشته باشد. داده‌های آموزش و آزمون از این دو مجموعه داده نرم‌افزاری شبیه سازی‌شده و داده واقعی ثبت‌شده از گیرنده GPS انتخاب می‌گردند. شبکه ابتدا با داده‌های شبیه‌سازی‌شده که در ادامه روش تولید آن‌ها ذکر می‌گردد، آموزش داده‌شده و در مرحله بعد به‌منظور بهبود کارایی، شبکه با داده‌های واقعی آموزش داده می‌شود. ارزیابی شبکه عصبی طراحی شده، با داده‌های جمع‌آوری‌شده است. جمع‌آوری داده واقعی بدین صورت است که سیگنال‌های ماهواره‌های GPS که تحت تأثیر فریب قرار دارند، پس از دریافت از آنتن گیرنده تقویت‌شده و از بخش Front End عبور کرده و تبدیل به فرکانس باند میانی می‌شوند. سپس سیگنال مربوطه نمونه‌برداری شده و وارد قسمت‌های اکتساب و ردگیری گیرنده نرم‌افزاری GPS مجهز به الگوریتم پیشنهادی می‌گردد. درنهایت عملکرد الگوریتم مورد ارزیابی قرار می‌گیرد. فرآیند آموزش بدین صورت است که با داشتن نمونه‌های دوره

1- Offline

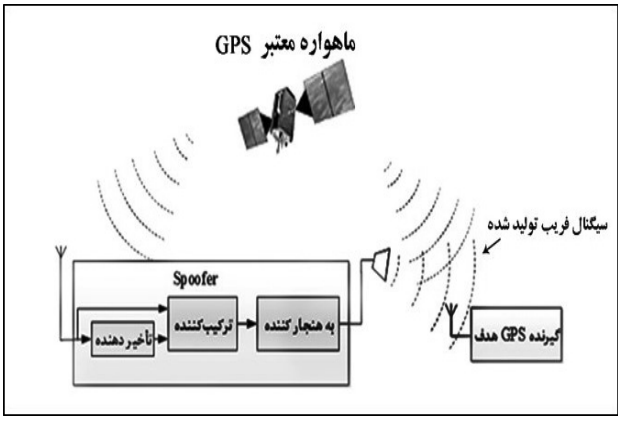
کد C/A از ماهواره‌های معتبر و فریب، شاخص‌های ذکرشده مرتبط با هر نمونه را استخراج کرده و به‌صورت تصادفی ۸۰ درصد آن به‌منظور آموزش انتخاب می‌گردد و با ۲۰ درصد از نمونه‌های باقی‌مانده، شبکه محک زده می‌شود. این عمل تقسیم داده‌ها برای هر دو نوع داده واقعی و داده شبیه‌سازی‌شده انجام می‌شود. در مرحله آموزش و آزمون، شاخص‌های مربوط به سیگنال فریب و معتبر مشخص شده است. اعتبارسنجی با مقایسه خروجی شبکه با مقدار مورد انتظار صورت می‌گیرد. در بخش بعدی، اعتبارسنجی با ماتریس درهم‌ریختگی نشان داده شده‌است.

برای آزمودن رویکرد پیشنهادی، ابتدا نمونه آزمایشگاهی داده فریب تأخیری تهیه شد. برای اجرای آن بازه مشخصی از داده با فرکانس ۵/۷ MHz نمونه‌برداری شد و در یک حافظه مناسب ذخیره گردید و پس از ایجاد تأخیر مناسب، با سیگنال‌های حقیقی GPS ترکیب شد. اگر رابطه زیر به‌عنوان سیگنال معتبر در نظر گرفته شود، با توجه به توضیحات بیان‌شده، سیگنال فریب به‌صورت رابطه زیر مدل می‌گردد:

$$R_{C/A}(t) = A_C^A(t)C_i^A(t)D_i^A(t)\sin(w_{L1}t+\phi_{L1}^A) + A_C^D(t)C_i^D(t)D_i^D(t)\sin(w_{L1}(t-\Delta t_D)+\phi_{L1}^D) \quad (۸)$$

رابطه (۸) معرف سیگنالی است که گیرنده هدف دریافت می‌کند که در آن بالانویس و زیرنویس A، D، L_1 و i به ترتیب بیان‌گر سیگنال معتبر، سیگنال تأخیر یافته، حامل کانال L_1 ماهواره‌های GPS و شماره ماهواره می‌باشند و توابع A، C و D به ترتیب دامنه، کد C/A و پیام ناوبری سیگنال GPS را نشان می‌دهند.

برای بی‌اثر کردن سیگنال معتبر GPS در گیرنده، می‌توان از افزایش نسبت توان سیگنال جعلی به معتبر بهره برد. می‌توان روند تولید سیگنال فریب تأخیری را به سبک نشان‌داده‌شده در شکل (۹)



شکل (۹). شمای کامل مجموعه فریب‌دهنده طراحی‌شده

ترسیم کرد. برای پیاده‌سازی عملی سناریو فریب تأخیری نیاز به تجهیزاتی هست 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[۲] در تولید سیگنال فریب مشکل‌ساز نمی‌شود.

شبیه‌سازی ساختار شبکه عصبی MLP با معماری‌های مختلف صورت گرفت. نتایج به‌دست‌آمده در جدول (۱) نشان داده‌شده است. ساختار ردیف اول با توجه به این‌که اندکی دقت بیشتری در دسته‌بندی نسبت به دیگر ساختارها دارد، ولی به‌دلیل زمان زیاد محاسبات، ساختاری با زمان پردازش معقول‌تر ترجیح داده‌شده است. ساختار ۱-۳-۲ پیچیدگی کمتری نسبت به ساختار ۱-۳-۳ دارد، ولی به علت یک نرون کمتر در ورودی، در بعضی از شرایط خطای بالایی داشته، درنتیجه ساختار بهینه (۱-۳-۳) انتخاب شده است. ساختارهای ممکن دیگر به‌دلیل زمان یا خطای بسیار نسبت به ساختارهای ذکر شده در جدول آورده نشده‌اند.

جدول (۱). نتایج حاصله از اعمال روش پیشنهادی تشخیص فریب مبتنی بر شبکه عصبی.

ساختار شبکه عصبی	پیچیدگی	زمان اجرا	درصد تشخیص صحیح		متوسط مربعات خطا	
			داده فریب واقعی	داده فریب نرم‌افزاری	داده فریب واقعی	داده فریب نرم‌افزاری
۳-۵-۱	۲۶	۲/۸۹۵s	۹۹/۳۵۸۳	۹۹/۳۷۲۹	۰/۰۰۶۸	۰/۰۰۶۷
۳-۳-۱	۱۶	۰/۶۳۱s	۹۹/۳۲۵۰	۹۹/۲۳۷۵	۰/۰۰۶۴	۰/۰۰۵۷
۲-۳-۱	۱۳	۰/۲۹۸s	۹۸/۷۵۸۳	۹۸/۸۸۵۴	۰/۰۰۹۴	۰/۰۰۸۹

1-Offline

تعداد نرون‌های لایه اول برابر با تعداد شاخص‌های ورودی است. تعداد نرون‌های لایه پنهان نیز برابر سه و تعداد نرون های لایه خروجی برابر یک می‌باشد. با این تعداد لایه‌بندی پیچیدگی شبکه عصبی پیشنهادی از رابطه (۹) محاسبه می‌شود:

$$Order = i \times j + j \times r + j + r \\ = 3 \times 3 + 3 \times 1 + 3 + 1 = 16 \quad (۹)$$

در این رابطه، i تعداد گره‌های ورودی، j تعداد نرون های لایه مخفی و r تعداد نرون‌های خروجی می‌باشند.

تلاش‌های فراوانی برای سرعت بخشیدن به همگرایی و بهبود دقت الگوریتم پس انتشار[1] خطا در آموزش شبکه‌های عصبی صورت گرفته است. از آن جمله می‌توان به استفاده از تطبیق اندازه حرکت[2] و نرخ یادگیری متغیر اشاره کرد که منجر به بهبود اندکی شده‌اند. همچنین با بزرگ کردن مصنوعی خطا برای نرون‌های عمل‌کننده در ناحیه اشباع نتایج بهتری گرفته شده است [۲۸]. با استفاده از روش‌های مختلف مرتبه دوم برای مثال روش نیوتن گرادیان مختلط و یا بهینه‌سازی LM بهبود قابل‌توجهی را می‌توان بر روی عملکرد تشخیص مشاهده کرد. شبیه‌سازی به‌صورت SDR[3] با رایانه‌ای دو هسته‌ای ۲/۸ GHz با ۴ GByte حافظه صورت‌گرفته و در نرم افزار متلب از ابزار آموزش شبکه عصبی روش LM استفاده شده است .

۴- تحلیل نتایج اعمال الگوریتم تشخیص فریب و مقایسه با دیگر روش‌ها

پس از آموزش شبکه عصبی پیشنهادی، ارزیابی دقت شبکه عصبی انجام می‌شود. در این تحقیق به‌منظور ارزیابی صحت دسته‌بندی سیگنال‌ها و همچنین نحوه عملکرد الگوریتم‌های دسته‌بندی، سیگنال‌های GPS آزموده می‌شوند. عملکرد شبکه عصبی طراحی‌شده توسط ماتریس درهم‌ریختگی قابل ارزیابی است. هر ستون از آن، نمونه‌ای از مقدار پیش‌بینی‌شده و هر سطر نمونه‌ای واقعی را نشان می‌دهد؛ یعنی هنگامی که خطایی رخ نداده، نتیجه پیش‌بینی با حقیقی برابر است و مقدار یک در سطر و ستون یکسان مربوط به نوع سیگنال قرارمی‌گیرد. در رابطه‌های (۱۱-۱۰) به ترتیب ماتریس درهم‌ریختگی داده‌های آموزش و آزمون مشاهده می‌شود که نشان می‌دهد در حالت آزمون شبکه عملکردی بهتر داشته است. هر چه این ماتریس قطری‌تر باشد، دسته‌بندی بهتری صورت گرفته است. درآیه اول تعداد نمونه‌های سیگنال معتبر و درآیه چهارم نمونه‌های فریب در داده‌های آموزش و آزمون است. درآیه غیرقطری خطای دسته‌بندی می‌باشد. برای به‌دست آوردن پارامترهای موقعیت‌یابی و داشتن یک دوره کد C/A از ماهواره ها ،۳۷۰۰۰ نمونه[4] با فرکانس ۵/۷ MHz از سیگنال IF جهت پردازش احتیاج است. از این مقدار، ۸۰ درصد برای آموزش انتخاب شده و ۲۰ درصد برای آزمون الگوریتم پیشنهادی اعمال و ماتریس پیچیدگی آن در زیر آورده شده است.

$$Confusion\ Mat\ \_trianing = \begin{pmatrix} 29517 & 83 \\ 266 & 29344 \end{pmatrix} \quad (۱۰)$$

$$Confusion\ Mat\ \_test = \begin{pmatrix} 7374 & 26 \\ 63 & 7337 \end{pmatrix} \quad (۱۱)$$

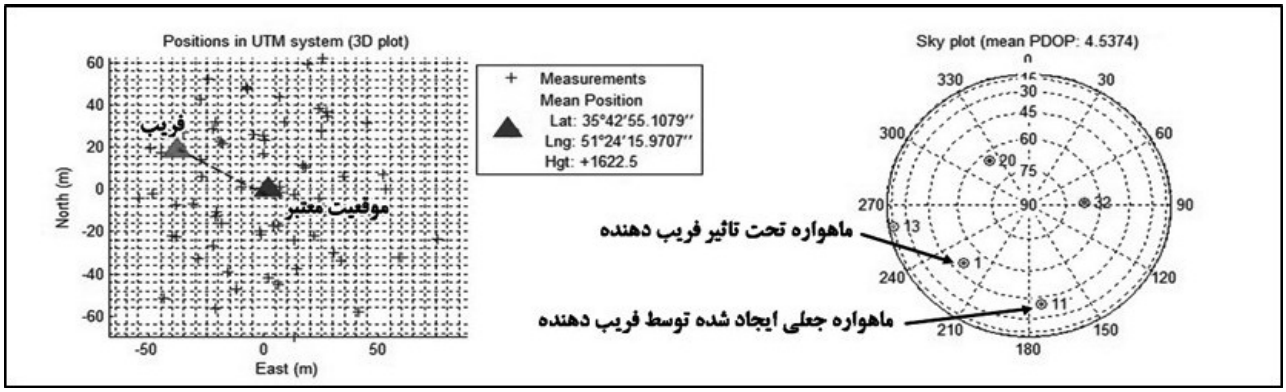
اگر خطایی در دسته‌بندی نمونه‌ای از سیگنال فریب رخ دهد از ستون مربوط به خود به ستون سیگنال‌های معتبر تغییر مکان می‌دهد. جهت ارزیابی دقت، یک سری شاخص‌ها وجود دارند که همواره برای نمایش نتایج دسته‌بندی به‌کار می‌روند. این شاخص‌ها عبارت‌اند از: صحت کل[5]، ضریب همبستگی کاپا[6]، دقت تولیدکننده[7]، دقت استفاده‌کننده[8]، خطای انباشته‌شده و خطای گماشته‌شده[9]. در ضریب همبستگی کاپا اطلاعات مربوط به ماتریس وابستگی خلاصه می‌شود. صحت کل، از تقسیم مجموع تعداد کل سیگنال‌هایی که به‌درستی در دسته مربوطه واقع‌شده‌اند، به تمام تعداد سیگنال‌ها به دست می‌آید. درصورتی که الگوهایی واقعاً متعلق به دسته مورد نظر باشند و پس از دسته‌بندی به دسته‌های دیگری تعلق گیرند، خطای انباشته رخ می‌دهد. درصورتی خطای گماشته رخ می دهد که بردارهایی که درواقع عضوهایی از دسته‌های دیگرند، عضوی از دسته مورد نظر شوند.

از نقطه نظر سرعت پردازش دسته‌بندی، شبکه عصبی سرعت بالاتری نسبت به روش‌های سنتی دارد. افزایش تعداد داده‌های آموزشی باعث افزایش دقت دسته‌بندی در روش «بیشتر شباهت» می‌شود، زیرا روشی آماری یک روش سنتی در دسته‌بندی است، ولی در روش شبکه عصبی با تعداد کمتری از داده‌های آموزشی می توان به نتایج بهتری رسید [۲۹].

آقای اُچین و همکاران در مرجع [۳۰] وجود فریب را با شناسایی ناسازگاری آماری از طریق بررسی مشخصات اصلی سیگنال‌های ماهواره‌ها تشخیص داده‌اند. مشکل اصلی که در این روش وجود دارد این است که برای اجرای موفق آن لازم است، اطلاعات سیگنال

1-Back Propagation
2-Momentum
3-Software Defined Radio

4-Sample
5-Overall Accuracy
6-Kappa Coefficient
7-Product Accuracy
8-Omission
9-Commission



شکل (۱۰) موقعیت‌یابی UTM و موقعیت ماهواره‌های ردیابی شده در حضور فریبنده GPS.

معتبر قبل از لحظه شروع فریب در دسترس باشد، زیرا پس از حمله فریب مشخصات سیگنال جعل‌شده در حد مجاز آستانه در نظر گرفته‌شده، قرار می‌گیرد. در رویکرد پیشنهادی پس از آموزش شبکه عصبی نیازی به‌وجود سیگنال معتبر از ابتدا نمی‌باشد و وجود سیگنال فریب به‌خوبی پس از راه‌اندازی گیرنده آشکار می‌شود.

با استفاده از روش بررسی سازگاری موقعیت یابی با دیگر روش‌های موقعیت‌یابی و ناوبری، می‌توان فریب گیرنده GPS را آشکار نمود [۱۵]. در این روش از اطلاعاتی که به‌وسیله تجهیزات کمکی مانند اندازه‌گیری حرکتی[1] (IMU)، اطلاعات موقعیت‌یابی ایستگاه‌های شبکه محلی بی‌سیم[2] (WLAN) و یا شبکه‌های موبایل به‌دست می‌آید، گیرنده از ناسازگاری این دو سیستم موقعیت‌یابی جهت تشخیص تهدید فریب استفاده می‌کند. عمده مشکل این روش پیچیدگی سخت‌افزاری و نرم‌افزاری گیرنده GPS می‌باشد. حسگرهای IMU به کالیبراسیون قبل از استفاده نیاز دارند. استفاده از فناوری مکان‌یابی بی‌سیم مانند شبکه‌های بافت سلولی علاوه بر نیاز به تجهیزات اضافه معمولاً راه‌حل‌های موقعیت‌یابی به‌دقت سیگنال GPS ارائه نمی‌دهد، ولی روش ارائه‌شده کنونی نیازی به سخت‌افزار اضافه ندارد و ابعاد و هزینه ساخت گیرنده را افزایش نمی‌دهد.

در مراجع [۳۱ و ۳۲] از تخمین‌گر فیلتر کالمن برای پیش‌بینی مشخصات سیگنال لحظه بعد استفاده می‌کنند. درصورتی اختلاف قابل‌توجهی بین مقادیر اندازه‌گیری و تخمین‌زده‌شده مشاهده شود، وجود حمله فریب تشخیص داده می‌شود. در حملات متوسط و پیچیده گیرنده- فریبنده ابتدا پیک همبستگی گیرنده را تسخیر می‌کند و به آرامی از پیک معتبر دور می‌شود که این عمل به قدری به‌کندی صورت می‌گیرد که فیلتر کالمن مشخصات لحظه بعد سیگنال فریب را پیش‌بینی می‌کند و فریب آشکار نمی‌گردد. در شبکه عصبی روش پیشنهادی شاخص سطح سیگنال در هنگامی که گیرنده-فریبنده می‌خواهد پیک همبستگی گیرنده را در اختیار بگیرد، از حد آستانه مجاز تخطی کرده و فریب آشکار می‌شود.

در مرجع [۱۹]، با اندازه‌گیری تفاوت فازی دیده‌شده بین دو آنتن، ثابت شده و با دانستن رفتار آرایه آنتن و مسیر حرکت ماهواره‌ها،تفاوت‌های فاز نظری محاسبه‌شده و فاز عملی دیده‌شده توسط آرایه آنتن مقایسه و فریب را آشکار می‌کند. همچنین در مرجع [۲۰] یک ساختار آرایه آنتنی برای آشکارسازی و کاهش سیگنال فریب استفاده کرده است که مبتنی بر همبستگی فضایی[3] است. مشکل روشی که از پردازش فضایی استفاده می‌کند، الگوریتم زمان‌بر آن است. به‌طور کلی ایراد روش‌های که مبتنی بر آنتن هستند، علاوه‌بر افزایش ابعاد و غیرقابل حمل کردن گیرنده، احتیاج به آرایه آنتن کالیبره‌شده دارند و یا نیازمند آنتنی با جهت مشخص می‌باشند. به‌علت مشخص نبودن نوع سخت‌افزار مورد استفاده در مقالات مشابه برای پیاده‌سازی الگوریتم‌ها و نیز عدم دسترسی به داده‌ها و پارامترهای نرم‌افزاری الگوریتم‌های مربوطه برای سنجش، روش پیشنهادی به‌صورت کیفی مورد مقایسه قرار گرفته است. در شکل (۱۰) نشان می‌دهد که موقعیت‌یابی به‌علت وجود دو ماهواره جعلی دچار اختلال گردیده و مکان‌یابی به‌صورت نادرست در مکان دیگری صورت گرفته است. تفاوت در ماهیت سیگنال ماهواره‌های معتبر و فریب توسط الگوریتم پیشنهادی تشخیص داده می‌شود تا از ابزارهای دیگر موقعیت‌یابی استفاده گردد.

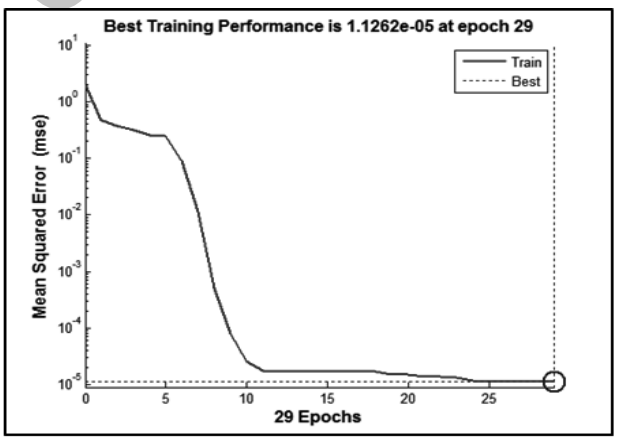
جدول (۲) مقایسه‌ای کیفی بین روش‌های پیشین و الگوریتم پیشنهادی را ارائه می‌نماید. همان‌طور که ملاحظه می‌شود، کارآیی شبکه عصبی ارائه‌شده نسبت به دیگر روش‌ها برتری قابل‌توجه دارد.

شکل (۱۱) روند تغییرات خطای آموزش را در هر دوره آموزشی نشان می‌دهد. استفاده از میزان بیشتری دوره‌ها و داده‌های آموزشی می‌تواند امر جداسازی بردارها را آسان‌تر و دقیق‌تر نموده و دقت دسته‌بندی را بالا برد. در شکل (۱۲) نمودار خطای دسته‌بندی قابل مشاهده است.

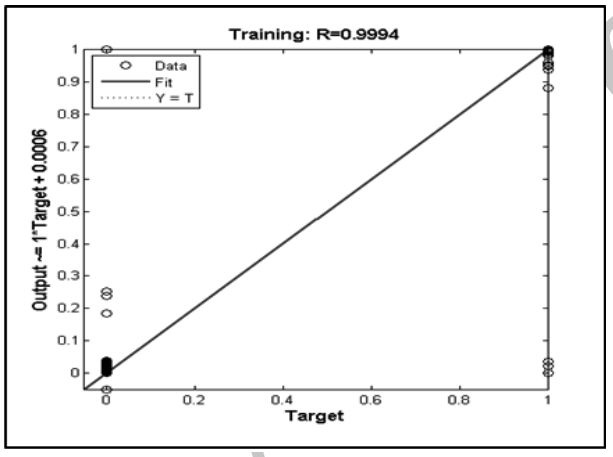
1-Inertial Measurement Unit
2-Wireless Local Area Network
3-Spatial Correlation

جدول (۲). مقایسه کارآیی بین روش‌های پیشین و الگوریتم پیشنهادی.

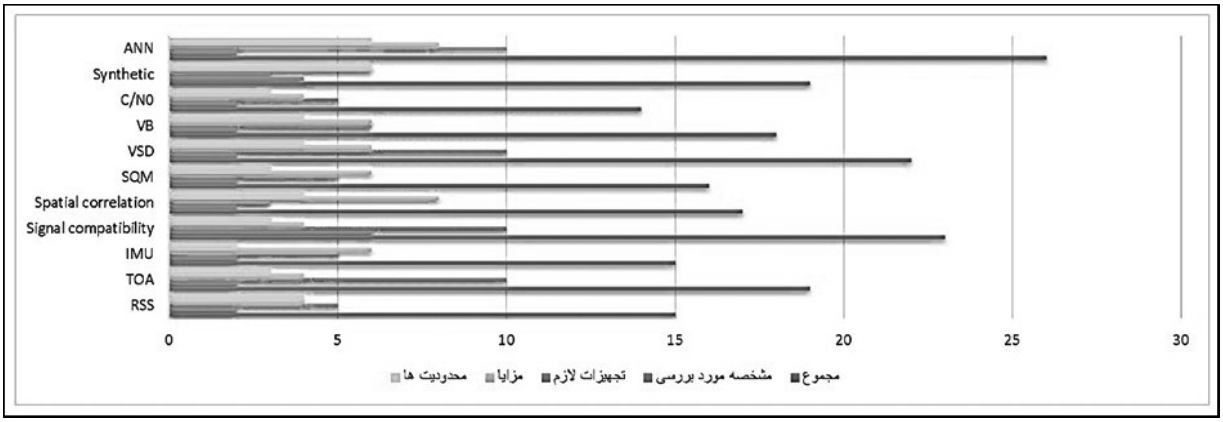
روش‌های تشخیص	مشخصه مورد بررسی	تجهیزات لازم	مزایا	محدودیت‌ها
بررسی توان سیگنال	توان و دامنه	سخت‌افزار برای اندازه‌گیری توان	سادگی	محدوده بزرگ آسیب‌پذیری و گران بودن تجهیزات درصورت نیاز
TOA	زمان دریافت	ارتقای نرم‌افزاری	پیاده‌سازی آسان	عدم کارآیی در حضور اختلال دیگر و پیش‌بینی TOA توسط فریبنده
سازگاری با دیگر روش‌های ناوبری	نتایج ناوبری	تجهیزات ناوبری غیر از GPS	قابلیت اطمینان بالا	هزینه بالا و پوشش محدود تجهیزات دیگر
سازگاری سیگنال ورودی	چندین پارامتر به‌طور همزمان	ارتقای نرم‌افزاری	هزینه پایین	نیاز به اطلاعات قبل از شروع حمله و عدم کارآیی در فریب‌های هماهنگ
پردازش فضایی	جهت ورود سیگنال به گیرنده	آرایه آنتن ویژه و ارتقای نرم‌افزاری	قابلیت اطمینان بالا و عدم نیاز داده قبلی	هزینه بالا و عدم کارآیی در چندمسیری و چندآنتنه
SQM	همبستگی	ارتقای نرم‌افزاری و سخت‌افزار اضافه	تشخیص آسان	عدم کارآیی در چندمسیری و نیاز به اطلاعات قبل از شروع حمله
VSD	همبستگی	ارتقای نرم‌افزاری	امکان تفکیک چندمسیری	عدم کارآیی در فریب هماهنگ
VB	همبستگی	حلقه ردیابی اضافی	دقت تشخیص بالا	هزینه بالا
C/No	نسبت حامل به نویز	سخت‌افزار برای اندازه‌گیری	سادگی	آسیب‌پذیر در مقابل حملات هماهنگ و حملاتی که فریبنده کنترل توان می‌کند
ترکیبی	همبستگی و توان	ارتقای نرم‌افزاری و سخت‌افزار اضافه	قابلیت اطمینان بالا	کاهش کارآیی در حضور چندمسیری
الگوریتم ارائه‌شده در این مقاله	همبستگی	ارتقای نرم‌افزاری	قابلیت اطمینان بالا، سرعت بالای تشخیص و پیاده‌سازی آسان	نیاز الگوریتم به آموزش



شکل (۱۱). روند خطای دوره‌های آموزش در شبکه عصبی پیشنهادی.



شکل (۱۲). نمودار خطای دسته‌بندی (نتایج ماتریس درهم‌ریختگی).



شکل (۱۳). نمودار مقایسه روش‌های تشخیص فریب.

هر دایره نشان‌دهنده یک نمونه سیگنال است. اگر دایره‌ها روی خط قرار گیرند، دسته‌بندی به‌خوبی صورت گرفته است و انحراف دایره از روی خط بیانگر خطا در تشخیص هویت آن نمونه سیگنال است. در شکل (۱۳) مقایسه نموداری روش‌های پیشین با روش پیشنهادی آماده است. این نمودار بر اساس تعداد ویژگی‌های مورد بررسی، تجهیزات مورد استفاده، مزایا و معایب هر روش ترسیم شده است.

۵- نتیجه‌گیری

در این مقاله سعی شده است علاوه بر به‌کارگیری روش‌های پیشین یک رویکرد نوین در تشخیص فریب گیرنده GPS ارائه شود. جهت آشکارسازی فریب GPS از شاخص‌های پردازش سیگنال در ورودی‌های شبکه عصبی بهره بردیم. این الگوریتم بر روی گیرنده نرم‌افزاری GPS در نرم‌افزار متلب با داده‌های واقعی آزموده شده است و کمترین دقت به‌دست‌آمده از شبیه‌سازی‌گیرنده نرم‌افزاری مبتنی بر شبکه عصبی، دقت ۹۸/۷۸ درصدی در تشخیص صحیح سیگنال فریب از سیگنال معتبر است. همچنین بیشترین زمان تشخیص سیگنال فریب ۰/۶ ثانیه است. استفاده از سامانه‌های هوشمند تاکنون جهت مقابله با فریب GPS استفاده‌نشده است و یک گام نوین در تشخیص فریب در گیرنده GPS است.

۶- مراجع

[1] F. Shafiee and M. R. Mosavi, "Narrowband Interference Suppression for GPS Navigation using Neural Networks," Journal of GPS Solutions, pp. 1-11, 2015 (DOI 10.1007/ s10291-015-0442-8).

[2] A. Jovanovic, C. Botteron, and P. A. Farine, "Multi-test Detection and Protection Algorithm Against Spoofing Attacks on GNSS Receivers," IEEE Position, Location and Navigation Symposium, pp. 1258-1271, May 2014.

[3] 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.

[4] M. R. Mosavi, M. J. Rezaei, N. Hosseinzadeh and R. A. Kiaamiri, "New Intellogent Methods for Detection and Mitigation of Spoofing Signal in GPS Receivers", Journal of Electronics and Cyber Defense, Vol.2, No.1, pp.71-81, 1393. (in Persian)

[5] 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.

[6] 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," The 23rd International Technical Meeting of the Satellite Division of the Institute of Navigation, pp. 1-11, Sep. 2010.

[7] A. J. Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS Vulnerability to Spoofing Threats and a Review of Anti-spoofing Techniques," Journal of Navigation and Observation, vol. 20, pp. 1-16, May 2012.

[8] 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.

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

[10] 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.

[11] K. D. Wesson, B. L. Evans, and T. E. Humphreys, "A Combined Symmetric Difference and Power Monitoring GNSS Anti-Spoofing Technique," IEEE Global Conference on Signal and Information Processing, pp. 1-4, Dec. 2013.

[12] M. Pini, M. Fantino, A. Cavaleri, S. Ugazio, and L. L. Presti, "Signal Quality Monitoring Applied to Spoofing Detection," The 24th International Technical Meeting of the Satellite Division of the Institute of Navigation, pp. 1-9, Sep. 2011.

[13] M. Lashley and D. Bevly, "What About Vector Tracking Loops," GNSS Solutions, pp. 1-6, May/June 2009.

[14] S. C. Lo and P. K. Enge, "Authenticating Aviation Augmentation System Broadcasts," IEEE/ION Position, Location and Navigation Symposium, pp. 708-717, 2010.

[15] M. G. Petovello, "Real-Time Integration of a Tactical-Grade IMU and GPS for High-Accuracy Positioning and Navigation," Ph.D. Thesis, Department of Geomatics Engineering, University of Calgary, Alberta, Canada, 2003.

[16] T. E. Humphreys, M. L. Psiaki, P. M. Kintner and B. M. Ledvina, "GNSS Receiver Implementation on a DSP: Status, Challenges and Prospects", Proc. ION GNSS, pp. 1-13, 2006.

[17] C. E. Mcdowell, "GPS Spoofer and Repeater Mitigation System using Digital Spatial Nulling-US Patent 7250903 B1," 2007.

[18] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS Spoofer Countermeasure Effectiveness based on Signal Strength, Noise Power and C/N0 Observables," International Journal of Satellite Communications and Networking, vol. 30, no. 4, pp. 181-191, 2012.

[19] 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," The Institute of International Technical Meeting of the Institute of Navigation, pp. 1-7, Jan. 2009.

[20] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, "A Multi-Antenna Defense: Receiver-Autonomous GPS Spoofing Detection," Inside GNSS Magazine, vol. 4, no. 2, pp. 40-46, March/April 2009.

[21] S. C. Lo and P. K. Enge, "Authenticating Aviation Augmentation System Broadcasts," IEEE/ION Position, Location and Navigation Symposium, pp. 708-717, 2010.

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

[23] A. Tabatabaei and M. R. Mosavi, "Rapid and Precise GLONASS GDOP Approximation using Neural Networks," Journal of Wireless Personal Communications, vol. 77, no. 4, pp. 2675-2685, 2014.

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

[25] M. R. Mosavi, K. Mohammadi, M. H. Refan, and M. Farrokhi, "Prediction of Errors and Improvement of Position Accuracy on Low Cost GPS Receiver with MLP Neural Network," The 11th Iranian Conference on Electrical Engineering, vol. 3, pp. 513-520, 6-8 May 2003.

[26] T. Martin and B. Menhaj, "Training Feedforward Networks with the Marquardt Algorithm," IEEE Transactions on Neural Networks, vol. 5, no. 6, pp. 989-993, November 1994.

[27] M. R. Mosavi, "GPS Receivers Timing Data Processing using Neural Networks: Optimal Estimation and Errors Modeling," Journal of Neural Systems, vol. 17, no. 5, pp. 383-393, October 2007.

[28] R. Pasti and L. N. De Castro, "Bio-Inspired and Gradient based Algorithms to Train MLPs: the Influence of Diversity," Information Sciences, vol. 179, no. 10, pp. 1441-1453, Apr. 2009.

[29] I. Kanellopoulos, A. Varfis, G. Wilkinson, and J. Meiger, "Land Cover Discrimination in SPOT HRV Imagery using Artificial Neural Network 20 Class Experiment," Journal of Remote Sensing, vol. 13, pp. 917-924, 1992.

[30] E. Ochin, L. Dobryakova, and L. Lemieszewski, "Antiterrorism-Design and Analysis of GNSS Anti-spoofing Algorithms," Scientific Journals Zeszyty Naukowe Maritime University of Szczecin, pp. 93-101, 2012.

[31] 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, Korea, 2011.

[32] P. Papadimitratos and A. Jovanovic, "GNSS Based Positioning: Attacks and Countermeasures," IEEE Military Communications Conference (MILCOM), pp. 1-7, 2008.

Journal Of Electronical & Cyber Defence
Vol. 3, No. 1, 2015, Serial No.9

Detection of Spoofing Attack Based on Multi-Layer Neural Network in Single-Frequency GPS Receivers

E. Shafiee, M. R. Mosavi* and M. Moazedi

*Iran University of Science and Technology

(Received: 25/12/2014, Accepted: 10/05/2015)

ABSTRACT

A GPS spoofing attack attempts to deceive a GPS receiver by broadcasting counterfeit GPS signals. Structured to resemble a set of normal GPS signals, but it is a little stronger. In the recent years, there have been presented many different solutions for detection and reduction of spoofing attack. Neural Networks (NNs) are the modern computational method for learning machine and then imposing the acquired knowledge for predicting the output response of complicated systems. This paper presents a main approach to GPS spoofing detection based on intelligent systems. Signals are classified using auto-correlation features. Indices of early-late phase, delta and total signal level as inputs of multi-layer NN in order to detect spoofing signal in GPS receiver tracking loop. Authentic and spoof signals have different statistical pattern in named parameter and NN can detected it. Since NN is able to exploit multiple features from different methods, it classifies signals with error less than the conventional techniques. Finally, the least precision obtained from simulation of NN based GPS software receiver is 98.78% in correct detection of spoofing signal from valid signal. Moreover, the detection time is less than the existing methods.

Key words: Detection, GPS, Spoofing Attack, Neural Network.

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