آشکارسازی حمله‌ی فریب در بخش حلقه ردیابی گیرنده GPS مبتنی بر الگوریتم IPSO

لاله بهادری [۱]، نیلوفر دباغی داریان [۲]، سید محمد رضا موسوی میرکلایی [۳]

۱- کارشناسی ارشد، دانشکده مهندسی برق، دانشگاه علم و صنعت ایران، تهران، l_bahadori@vu.iust.ac.ir

۲- کارشناسی ارشد، دانشکده مهندسی برق، دانشگاه علم و صنعت ایران، تهران، n_dabaghi96@elec.iust.ac.ir

۳- استاد، نویسنده مسئول، دانشکده مهندسی برق، دانشگاه علم و صنعت ایران، تهران، M_Mosavi@iust.ac.ir

چکیده

واحدهای فازوری با استفاده از سامانه موقعیت‌یاب جهانی* (GPS) تحول عظیمی در بهره‌برداری از سامانه‌های قدرت ایجاد کرده‌اند. به‌عنوان یکی از منابع مهم داده‌های شبکه‌های هوشمند، واحد اندازه‌گیری فازور† (PMU) با خطر بالای حملات روبرو است. یکی از خطرناک‌ترین تداخلات سامانه GPS، اختلال فریب می‌باشد و گیرنده‌های دارای حلقه قفل تأخیر (DLL)‡ و قفل فاز§ (PLL) با پهنای باند کم‌تر در مقابل فریب مقاوم‌تر هستند. در تشخیص جعل GPS با گیرنده رادیو نرم‌افزار** (SDR)، زمانی که مهاجم بیشینه همبستگی گیرنده را اشغال می‌کند، جعل شناسایی می‌شود. این روش به سخت‌افزار اضافی نیاز ندارد، سیگنال‌های جعل نمونه‌برداری شده وارد سنجش اکتساب و ردیابی SDR مجهز به الگوریتم ضدجعل می‌شوند. در این پروژه، از همبسته‌ساز سیگنال‌های بدست‌آمده، به‌عنوان ورودی‌های شبکه عصبی چندلایه استفاده شده است تا بتوانیم سیگنال فریب را در حلقه ردیابی شناسایی کنیم و برای ارتقاء معیار دلتا از شبکه عصبی بهینه‌سازی حرکت ذرات†† (PSO) استفاده کردیم که باز هم به دلیل همگرایی کند و گیر افتادن در کمینه‌های محلی این شبکه، بهره‌گیری از بهینه‌سازی ازدحام ذرات با ضرایب شتاب متغیر زمان‡‡ (TACPSO) پیشنهاد شد. سپس، به منظور بهبود آشکارسازی، روش‌های هوشمند را ارتقاء دادیم که بدین منظور در روش پیشنهادی از یک شبکه عصبی بهبود یافته§§ (IPSO)، با ساختار (۱-۳-۳) استفاده کردیم که دقت شناسایی را افزایش می‌دهد. در نهایت، روش‌های بکار رفته را مقایسه و اثبات کردیم که شبیه‌سازی گیرنده نرم‌افزاری مبتنی بر شبکه عصبی IPSO با ضرایب اصلاح شده بیش‌ترین دقت (۹۹/۹۵ درصد) در تشخیص سیگنال فریب از معتبر را نسبت به سایر روش‌های مورد بررسی دارد.

کلمات کلیدی: شبکه عصبی، IPSO، واحد اندازه‌گیری فازور، سامانه توزیع قدرت، GPS، حمله فریب، همبستگی، اکتساب، معیار دلتا، ردیابی، گیرنده نرم‌افزاری، تشخیص و آشکارسازی.

---

* **Global Positioning System**
† **Phasor Measurement Unit**
‡ **Delay Lock Loop**
§ **Phase Lock Loop**
** **Soft Defined Radio**
†† **Particle Swarm Optimization**
‡‡ **Time Varying Accelaration Coefficients**
§§ **Improve Particle Swarm Optimization**

۱. مقدمه

شبکه‌های قدرت به‌عنوان یکی از حیاتی‌ترین و حساس‌ترین کاربردهای سامانه ماهواره‌ای موقعیت‌یابی جهانی* (GNSS) شناخته شده‌اند. اندازه‌گیری توسط واحدهای جمع‌بندی† (PDC)، جمع‌آوری شده و توسط متمرکز کننده‌های داده فازور PMU جمع‌بندی می‌شوند. به همراه تمامی این اندازه‌گیری‌ها، برچسب زمانی وجود دارد که دارای دقتی در حد نانوثانیه نسبت به زمان هماهنگ جهانی‡ (UTC) هستند. زمان‌سنجی دقیق، امکان نظارت و کنترل بلادرنگ را از طریق اندازه‌گیری جریان و ولتاژ فراهم می‌کند. همچنین، تشخیص و مکان‌یابی خطاها و مشکلات شبکه قدرت نیز از این طریق امکان‌پذیر است [۱].

سامانه‌های PMU نسبت به سامانه‌های کنترل، نظارت و جمع آوری داده§ (SCADA) دقت را تضمین می‌کند، ولی در برابر حملات سایبری آسیب‌پذیر است. حملات به سامانه‌های قدرت بر بسیاری از برنامه‌ها تأثیرات جدی دارند و خطاهای آبشاری و حتی خاموشی در مقیاس بزرگ را به دنبال دارند [۲]. PMU ها به‌عنوان نماینده‌های سامانه‌های کنترلی در Sandia National Lab استفاده می‌شوند، اما استفاده خودکار از آن‌ها هنوز محدود به انجام مشاهدات شبکه است، زیرا بیم آن می‌رود که حملات زمان‌سنجی، عملیات شبکه را دچار اختلال کنند [۳]. حملات فریب در سامانه موقعیت‌یابی جهانی GPS می‌توانند منجر به ناهنجاری‌هایی در حد میکروثانیه شوند که برای تخطی از حدود خطای فاز، کافی است و ممکن است باعث خطا در عملکرد مولدها شود.

گیرنده‌ی ناوبری ماهواره‌ای PMU در سامانه قدرت به سیگنال ماهواره‌ای فریبنده قفل می‌شود و باعث خطا به نظر رسیدن زاویه فاز اندازه‌گیری می‌شود و تخمین نادرست بار توان واقعی و هشدار کاذب برای ناپایداری توان را همراه دارد [۴]. با آزمون‌های انجام شده بر روی گیرنده‌ی ناوبری ماهواره‌ای و تجزیه‌وتحلیل آن‌ها، نشان داده شده است که خطای سرویس زمان ناوبری ماهواره‌ای ۱ میکروثانیه، منجر به جابه‌جایی محل خطا در حدود ۱۵۰ متر می‌شود. میزان تأثیر مکان خطا با طول خط انتقال تغییر می‌کند [۵]. گیرنده‌ی ناوبری ماهواره‌ای واحد اندازه‌گیری فازور PMU در سامانه قدرت، با سیگنال ماهواره‌ای فریبنده قفل می‌شود. فریب باعث عدم تطابق با استاندارد IEEE C37.118.2011 و ایجاد خطا در زاویه فاز اندازه‌گیری می‌شود [۶]. در سامانه GPS از دو روش شبه‌فاصله و اندازه‌گیری فاز حامل استفاده می‌شود. مرجع [۷]، از نظر تئوری تأثیر خروجی خطای پالس در ثانیه PPS توسط گیرنده ناوبری ماهواره‌ای بر PMU پست و PMU نیروگاه را تحلیل کرده و تأیید تجربی را انجام داده است. در مرجع [۵]، تأثیر تداخل سرویس زمان ناوبری ماهواره‌ای بر محل خطای خط انتقال به‌صورت کمی تحلیل می‌شود.

در مرجع [۸]، یک روش تشخیص جعل ارائه می شود، که در یک گیرنده GPS تعریف شده با نرم‌افزار SDR پیاده‌سازی شده است. همچنین، در آن نشان داده شده است که با اعمال NN، شاخص سیگنال فراتر از سطح آستانه مجاز حرکت می‌کند و زمانی که مهاجم می‌خواهد بیشینه همبستگی گیرنده را اشغال کند، جعل شناسایی می‌شود. روش ارائه شده، نیازی به سخت‌افزار اضافی ندارد و هزینه تولید را افزایش نمی‌دهد. در این رویکرد، نیازی به هیچ سیگنال معتبر پس از آموزش وجود ندارد.

در تشخیص جعل GPS با نرم‌افزار SDR، زمانی که مهاجم بیشینه همبستگی گیرنده را اشغال می‌کند، جعل شناسایی می‌شود. این روش به سخت‌افزار اضافی نیاز ندارد، سیگنال‌های جعل نمونه‌برداری شده وارد سنجش اکتساب و ردیابی SDR مجهز به الگوریتم ضدجعل می‌شوند.

---

* **Global Navigation Satelite System**
† **Phasor Data Concentrators**
‡ **Coordinated Universal Time**
§ **Supervisory Control and Data Acquisition**

داده‌های PMU در اثر حمله فریب تغییر فاز یکسانی دارند. [۹]، پس ثابت و معلوم بودن مکان PMU سبب می‌شود تا به‌طور دقیق تعداد ماهواره‌ها در ساعات مختلف تعیین شود و می‌توان از روش‌هایی بر اساس تحلیل مداری سامانه قدرت یا مدل آماری تخمین وضعیت همگام‌سازی فازورهای سامانه قدرت استفاده کرد. در مقاله [۱۰]، یک مدل آماری برای تخمین وضعیت همگام‌سازی فازورهای سامانه قدرت پیشنهاد شده است. یکی دیگر از روش‌های قابل‌توجه، روش مطرح شده در [۱۱] است که با ارائه یک مدل اندازه‌گیری جدید و با استفاده از یک مسئله بهینه‌سازی آسیب‌پذیرترین PMU ها را مشخص می‌کند. مقاله [۱۲]، همانند دو روش پیشین، پیشرفت بسیار مؤثری را بر اساس تخمین‌های شبکه قدرت در کاهش اثرات حمله فریب همگام‌سازی زمانی ارائه کرده است. یکی از بروزترین و مؤثرترین روش‌های مقابله، تخمینگر مقاوم ارائه شده در [۱۳] است.

اما این الگوریتم‌ها، مشکلاتی از جمله تلقی اشتباه حمله به PMU ها، در شرایطی که در یکی از آن‌ها اتفاق غیر منتظره‌ای رخ دهد یا عدم تشخیص فریب پیچیده را دارند. یک MLP NN می‌تواند تخمین روند صحیح انحراف ساعت را انجام داده و گیرنده را از آثار فاجعه‌بار TSA در شبکه قدرت حفظ کند [۱۴].

۲. اثر جعل در شبکه قدرت

بر اساس یک مدل پویا برای حالت سامانه قدرت مرجع [۱۵]، یک الگوریتم SE ایجاد می‌کند که علاوه بر حالت سامانه قدرت، جریان فازهای ناشی از جعل GPS در طول زمان را ارائه می‌دهد. دو روش برای SE پویا وجود دارد. رویکرد اول، ولتاژهای گذرگاه را به‌عنوان متغیرهای حالت نشان می‌دهد که ساده‌ترین مدل دینامیکی مربوط تا یک سیر تصادفی شناخته شده است. در رویکرد دوم، مدل‌های دینامیکی مولدها در نظر گرفته می‌شوند که در آن زاویه روتور و سرعت روتور متغیرهای حالت می‌باشند و سیر تصادفی را برای وضعیت ولتاژ شبکه تصویب می‌کند. اولین سهم، استخراج یک مدل وضعیت و اندازه‌گیری است که به‌طور صریح زوایای حمله جعلی GPS را مدل می‌نماید. در مرجع [۱۶] یک جعل کننده، انحراف ساعت گیرنده GPS را تغییر می‌دهد، مهرهای زمانی اندازه‌گیری‌ها تغییر می‌کند و در نتیجه زوایای فاز اندازه‌گیری تغییر می‌کند. بنابراین، جعل می‌تواند استاندارد synchrophasor IEEE-C37.118 را برای سامانه‌های قدرت نقض کند [۱۷].

سه نوع جعل داریم، شامل جعل در سطح داده و در سطح سیگنال و حمله مجدد [۱۸]، در دو نوع اول زمان گیرنده تغییر می‌کند، در حالی که موقعیت آن تغییر نمی‌کند. جعل‌کننده خطاهای زاویه فاز قابل توجهی ایجاد می‌کند، در نوع اول خطای زاویه فاز این جعل تا ۵۲ درجه در سامانه قدرت ۶۰ هرتز ایجاد می‌شود و جعل در سطح سیگنال، جعل‌کننده سیگنال جعلی را که ارسال می‌کند، داده‌های ناوبری را که هم‌زمان توسط ماهواره‌های GPS پخش می‌شوند، منتقل می‌نماید. در حمله نوع سوم، سیگنال‌های GPS معتبر با تأخیرهای زمانی ضبط و بازپخش می‌شوند. بنابراین، زمان محاسبه‌ی گیرنده GPS با تأخیر مواجه می‌شود و خطایی برای انحراف ساعت اعمال می‌شود، خطای زاویه فاز این جعل می‌تواند تا ۲۰ درجه در سامانه قدرت ۶۰ هرتز ایجاد شود [۱۹].

با توجه به ثابت بودن گیرنده در سامانه قدرت، فریب پیچیده برای آن دور از دسترس نیست که تشخیص آن از دو نوع دیگر سخت‌تر است. از اثرات منفی جعل بر عملکرد PMU می‌توان به تشخیص خطای خط انتقال در سامانه پایش ولتاژ و برای مکان‌یابی خطا در شبکه قدرت نام برد.

در تقسیم‌بندی روش‌های حملات داده‌های PMU روش استفاده از داده منفرد و روش استفاده از داده‌های دو انتهای خط برای تشخیص فریب نوع دوم و سوم مناسب نیستند و روش‌های برآورد حالت و استفاده از داده‌های PMU چند ترمینال مناسب‌تر هستند [۲۰] و [۲۱]. در مرجع [۲۲] بنا بر ماهیت فریب که در آن فریبنده سیگنال جعلی را مشابه سیگنال اصلی تولید می‌کند تا کاربر قادر به تشخیص مسیر جعلی از اصلی نباشد، شناسایی و آشکارسازی این حمله پیچیده‌تر است. ترکیب

الگوریتم پیشنهادی با هر یک از الگوریتم‌های موجود به بستری برای شناسایی و ردیابی حملات از داخل و خارج از سامانه WAMS راه‌اندازی می‌کند و هر الگوریتم با اطمینان بیش‌تر برای مقابله با هرگونه حمله جعلی ارائه می‌شود. نتایج الگوریتم ضد جعل در [۲۳] که محدودیت را در هر ۳۰ ثانیه برآورد کرده نشان می‌دهد که زاویه‌های فاز دارای مقدار جابه‌جایی یکسان هستند. بنابراین، جعل در هر بازه زمانی گزارش‌شده و با تغییر زاویه داده‌ها را می‌توان پالایش کرد.

۳. انواع حملات فریب

حمله فریب با اتکا بر تولید سیگنال جعلی با توان مناسب، قفل گیرنده زمان‌سنج یا موقعیت‌یاب را از سیگنال اصلی برمی‌دارد. اگر نسبت توان فریب به سیگنال اصلی حدود ۱/۱ برابر باشد، گیرنده روی سیگنال فریب قفل خواهد شد. تنها تفاوت‌های قابل شناسایی بین سیگنال‌های ماهواره معتبر و سیگنال‌های فریب، منحصر به اختلافات جزئی در زمان سنجی، جهت سیگنال، توان، نوبت داپلر (سرعت نسبی بین ماهواره/ فریب‌دهنده و گیرنده) و نسبت سیگنال به نویز است .

✓ حمله تخمین کد امنیتی و بازپخش (SCER)

در این حمله، فریب که یکی از حملات فریب متوسط محسوب می‌شود، فریب‌دهنده باید فرکانس حامل، فاز کد و داده ناوبری را به‌طور دقیق بازیابی کرده و بر طبق آن سیگنال‌های جعلی را تولید نماید. ایده اصلی در روش حمله فریب متوسط، تخمین موقعیت و سرعت آنتن گیرنده هدف و انتشار سیگنال جعلی متناظر با سیگنال معتبر است. هدف این نوع حملات، پیش‌بینی سیگنال معتبر به منظور تولید سیگنال فریب، با کم‌ترین میزان تأخیر است. حداقل تأخیر می‌تواند ارسال سیگنال را با تخمین صحیح برای بیت‌های غیرقابل پیش‌بینی، تضمین نماید. چنین سامانه‌ای به فریب‌دهنده امکان استفاده اختیاری از تأخیرهای وابسته بین کانال‌های فریب مختلف را می‌دهد. حمله SCER به‌عنوان یک تهدید برای همه روش‌هایی که از رمزنگاری برای امنیت سیگنال GNSS استفاده می‌کنند، به شمار می‌رود. در غیاب روش‌های حفاظتی اصالت و احراز اصالت، روش‌های تداخل ساده، گیرنده را به راحتی متأثر می‌نمایند.

✓ حملات همگام‌سازی زمانی (TSA)

جدول نجومی ماهواره در کم‌تر از یک دقیقه به دست می‌آید، درحالی‌که برای ۱۲.۵ دقیقه بدون تغییر باقی می‌ماند. بنابراین، گیرنده از این ثبات برای بازتولید قاب داده بهره می‌برد. به علاوه، بیت‌های حالت سلامت ماهواره، به‌وسیله فریب‌دهنده دستکاری شده و منجر به گمراه شدن گیرنده در ردیابی سیگنال‌های ماهواره معتبر می‌شوند. مهاجم می‌تواند داده ناوبری معتبر را دمدوله یا پیش‌بینی کرده و آن را تغییر دهد. سپس، دوباره آن را ارسال نماید که به تخمین زمان، موقعیت و فاصله اشتباه در گیرنده منجر شود.

✓ حمله فریب ضبط و بازپخش (Meaconing)

حمله ضبط و بازپخش، ساده‌ترین نوع حمله فریب است که در آن سیگنال اصلی، ضبط شده و پس از تأخیر مشخصی مجددا ارسال می‌گردد. به علت آنکه زمان نسبی دریافت سیگنال ماهواره‌های در دیدرس گیرنده در این حمله تغییر نمی‌کند، راه‌حل ناوبری مطابق میل مهاجم تغییر می‌یابد. همچنین، همانند راه‌حل ناوبری، راه‌حل زمانی نیز مطابق خواسته مهاجم

دارای تأخیر بازپخش خواهد بود. سیگنال‌های پخش شده به‌وسیله فریب‌دهنده، نسخه‌های دارای تأخیر سیگنال GPS معتبر هستند و منجر به تخمین اشتباه شبه‌فاصله می‌شوند. TSA می‌تواند منجر به خطای انحراف ساعت گیرنده بدون تغییر زیاد در مکان گیرنده نسبت به مقدار پیش از حمل شود. در مقابل، یک حمل بازپخش، زمانی که تعداد ماهواره‌های فریب داده شده نسبت به تعداد ماهواره‌های در دیدرس توسط گیرنده کم‌تر باشد، توانایی حفظ مکان گیرنده نسبت به حالت پیش از حمله را ندارد. بنابراین، از آنجا که PMU ثابت است، گیرنده می‌تواند به راحتی فریب را با مقایسه موقعیت تخمین زده شده قبلی با موقعیت فعلی تشخیص دهد.

۴. روش‌های تشخیص فریب

حمله‌ی فریب و مقابله با آن می‌تواند در هریک از سطوح گیرنده از جمله بخش بیت داده، اکتساب، ردیابی، استخراج شبه فاصله و معادلات ناوبری صورت پذیرد [۴]. در این مقاله، هدف آشکارسازی حمله‌ی فریب در مرحله ردیابی می‌باشد. برای عملکرد بهتر روش‌های ضدفریب، لازم است ابتدا شناخت جامعی از روش‌ها و انواع فریب‌دهنده‌ها داشته باشیم. در جدول (۱) خلاصه ای از روش های تشخیص فریب آمده است. دسته‌ی اول روش های فریب، روش‌های مبتنی بر رمزنگاری است که حفاظتی در برابر بازپخش و SCERE ایجاد نمی کنند. دسته‌ی دوم روش‌های مبتنی بر آرایه‌های آنتنی و طیف رادیویی است که در [۲۴] به آن پرداخته شده است. دسته‌ی سوم روش‌های مبتنی بر پردازش سیگنال است.
در مراحل مختلف این فرآیند، امکان نظارت بر اکتساب و ردیابی سیگنال‌ها برای یافتن موارد نامعمول وجود دارد که ممکن است نشانگر وقوع حمله فریب باشد. این روش‌ها با روش‌های دفاعی فیزیکی یا رمزنگاری متفاوت است. زیرا، نیاز به تغییرات فیزیکی در تجهیزات موجود یا پروتکل‌های سیگنال ندارد و تنها از طریق به‌روزرسانی نرم‌افزار گیرنده اجرا می‌شود. نظارت صحت خودکار گیرنده (RAIM)، قدیمی‌ترین و پراستفاده‌ترین راهکار ضدفریب در گیرنده‌های GNSS است و می‌تواند تمامی سیگنال‌های GNSS را از نظر هماهنگی مکانی بازرسی کرده و سیگنال‌های ماهواره‌های گمراه شده را حذف کند. در مورد سیگنال‌های اصلی، فرکانس با توجه به اثر داپلر تغییر می‌کند و تأخیری در کد PRN برای حفظ قفل سیگنال ایجاد می‌شود. ممکن است یک فریب‌دهنده کم کیفیت نتواند این تغییرات را اجرایی کند. ایراد اساسی روش RAIM، این است که فرض می‌کند هر حمله فریب محدود به یک یا دو ماهواره و نه کل سامانه، می‌شود. کاربر زمان‌سنج نیز هیچ اطلاعاتی در مورد آزمون‌های انجام شده در روش ندارد. بنابراین، نمی‌تواند سطح حفاظت ایجاد شده را بسنجد. استفاده از روش‌های کارآمدی همانند بهینه‌سازی حرکت ذرات از ویژگی‌های مهم این روش در مقابل با حملات فریب امروزی استفاده کرده‌اند.

جدول ۱- خلاصه‌ای از روش‌های مقابله با فریب.

روش‌های مبتنی بر رمزنگاری	هزینه	قابلیت اجرایی شدن
رمزنگاری کد گسترده	زیاد	زیاد
احراز هویت پیام ناوبری	متوسط	متوسط
رمزنگاری پیام ناوبری	زیاد	کم
TESLA	زیاد	کم
روش‌های مبتنی بر آنتن		
زاویه ورود سیگنال	متوسط	زیاد
آنتن در حال حرکت	متوسط	کم

دو آنتن متفاوت	متوسط	کم
ارسال سیگنال نول (صفر)	زیاد	کم
روش‌های مبتنی بر همبستگی با سایر منابع		
سایر ماهواره‌های GNSS	متوسط	کم
منابع غیر GNSS	زیاد	کم
روش‌های مبتنی بر پردازش سیگنال		
RAIM	کم	زیاد
SNR	کم	زیاد
توان مطلق [۲۵]	کم	زیاد
آزمون شیفت داپلر	کم	زیاد
قله همبستگی	زیاد	کم
انحراف ساعت	متوسط	زیاد

هدف نهایی TSA تأثیرگذاری بر داده‌های انحراف ساعت و ایجاد خطا در برچسب‌های زمانی است. به همین علت، یک MLP NN می‌تواند کمک بزرگی برای تخمین روند صحیح انحراف ساعت باشد و گیرنده PMU را از آثار فاجعه‌بار TSA در شبکه قدرت، حفظ کند. به‌کارگیری مؤثر MLP NN نیازمند انتخاب مناسب ویژگی‌های شبکه از جمله نوع معماری، تعداد لایه‌ها و نرون‌ها و نوع الگوریتم آموزش است. عموماً، انتخاب‌های بهینه از طریق یک‌روند آزمون و خطا مشخص می‌شوند [۲۶]. در این شبکه‌ها از نمونه‌های قبلی انحراف ساعت به‌عنوان ورودی برای پیش‌بینی نمونه بعدی آن، استفاده می‌شود. این تصمیم از طریق انجام یک مصالح بین پیچیدگی محاسباتی و میانگین مربعات خطا در روند آموزش، اتخاذ شده است.

در حضور سیگنال فریب، شبکه عصبی به محض مشاهده هر توزیع غیرعادی، نسبت به آن واکنش می‌دهد. این روش در واقع در گیرنده GPS آن را در برابر فریب مقاوم می‌نماید. در نتیجه، هزینه‌ی اجرای کمی دارد و ابعاد گیرنده را افزایش نمی‌دهد.

۵. آشکارسازی اختلال در بخش حلقه ردیابی گیرنده

بنا بر ماهیت فریب که در آن، فریبنده سیگنال جعلی را مشابه سیگنال اصلی تولید می‌کند تا کاربر قادر به تشخیص مسیر جعلی از اصلی نباشد، شناسایی و آشکارسازی این حمله پیچیده است. با استفاده از گیرنده‌ی رادیو نرم‌افزاری و بررسی معیار دلتا در مرحله حلقه ردیابی گیرنده و با استفاده از رسم نمودارهای بخش هم‌فاز و متعامد دو داده اصلی و جعلی، سعی در تشخیص وجود هرگونه ناهنجاری و تغییر شکل به وجود آمده در سیگنال، جهت آشکارسازی حمله‌ی احتمالی فریب صورت گرفته است. با استفاده از دو منبع داده که حاوی سیگنال اصلی و جعل‌شده است، نتایج اکتساب و ردیابی مقایسه گردید و نموداری بر اساس معیار دلتا برای هر دو حالت رسم شد. در نهایت، با استفاده از تفاوت‌های نمودار خروجی همبسته‌ساز سیگنال اصلی و جعلی، می‌توان به وجود فریب در سیگنال جعلی پی برد. از مزایای استفاده از روش گیرنده نرم‌افزاری که در اینجا بر اساس همبسته‌سازها تعریف شده است، می‌توان به انعطاف‌پذیری و عدم نیاز به تجهیزات سخت‌افزاری اشاره کرد که البته دارای دقت بسیاری می‌باشد و از نظر حافظه، نیازی به اطلاعات قبلی ندارد. در نهایت به دلیل ضعف هایی

که معیار دلتا دارد و برای بهبود این روش از شبکه عصبی PSO برای تشخیص استفاده شده است و نتایج با الگوریتم‌های TACPSO، AGPSO و IPSO مقایسه گردید.

۶. 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 بکار گرفته‌شده‌اند. بر این اساس در این مقاله برای کاهش فریب در GPS استفاده از شبکه‌های عصبی پیشنهادشده است. هدف از اعمال شبکه عصبی افزایش آشکارسازی حمله فریب در حلقه ردیابی می‌باشد.

در این مقاله 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، مؤخر و دلتا و سطح کل سیگنال را به عنوان ورودی شبکه عصبی 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 به طور همزمان به کار گیرد.

هدف از این تحقیق، ارائه یک روش آشکارسازی فریب سیگنال GPS مبتنی بر شبکه عصبی برای پیاده‌سازی در گیرنده نرم‌افزاری GPS است. این روش در واقع یک دفاع نرم‌افزاری محسوب می‌شود و بدون تغییر سخت‌افزاری در گیرنده GPS آن را در برابر فریب مقاوم می‌نماید. در نتیجه هزینه اجرای کمی دارد و ابعاد گیرنده را افزایش نمی‌دهد.

هنگام کار با شبکه عصبی با دو مسئله انتخاب معماری مناسب و انتخاب الگوریتم آموزشی مناسب روبرو هستیم. معماری مناسب به معنی انتخاب بهینه تعداد لایه‌ها و 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.

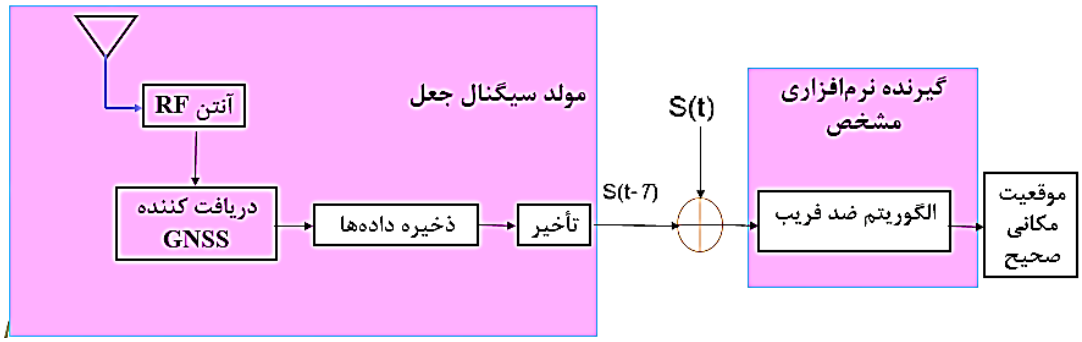
۷. شبیه سازی و بررسی نتایج

در این قسمت به تشخیص و آشکارسازی حمله فریب در حلقه ردیابی با استفاده از معیار دلتا می‌پردازیم تا هرگونه ناهنجاری در سیگنال آشکار شود و سپس با کمک شبکه عصبی دقت تشخیص بهبود داده می‌شود. به این منظور، از نرم‌افزار منبع باز Soft GNSS که به زبان برنامه‌نویسی MATLAB است بهره می‌گیریم. این نرم‌افزار یک گیرنده‌ی نرم‌افزاری برای استخراج اطلاعات از سیگنال ماهواره‌ای محسوب می‌گردد. در آن، ابتدا تنظیمات اولیه انجام می‌شود تا مقادیر اولیه فراخوانی شود. سپس، ماهواره‌های قابل دید شناسایی شده و تخمینی از فرکانس حامل و فاز کد سیگنال محاسبه می‌شود. در مرحله‌ی بعد سیگنال‌های موردنظر ردیابی می‌شوند و مقادیر دقیق فرکانس حامل و فاز کد سیگنال محاسبه می‌شود. در پایان با استفاده از تابع post navigation و انجام پردازش‌های لازم، شبه‌فاصله محاسبه می‌شود تا در نهایت، مکان گیرنده به‌دست آید. با توجه به تعریف معیار دلتا، این معیار قادر به شناسایی ناهنجاری‌های موجود در بخش هم‌فاز سیگنال است.

✓ جمع آوری داده‌ها

برای پیاده‌سازی فریب با دو عامل دامنه و زمان تأخیر سیگنال، از داده‌های GPS معتبر به مدت ۷۰ ثانیه استفاده شده

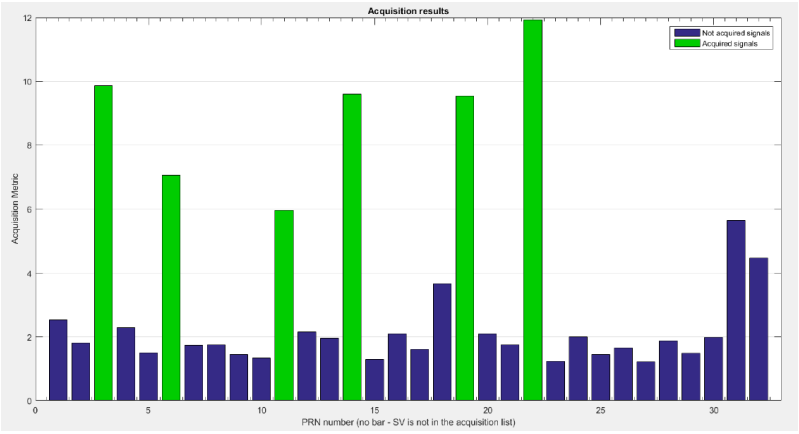
است. بدین گونه که ابتدا محدوده زمانی مشخصی از سیگنال معتبر را ذخیره کرده و سپس از انجام پیش‌پردازش‌های لازم (تغییر دامنه)، در زمان تأخیرهای مختلف با سیگنال معتبر ترکیب کرده و در نهایت، به سمت گیرنده هدف ارسال می‌کنیم. برای تولید داده های فریب از داده های اصلی بهره گرفته و پس از ذخیره داده های واقعی اطلاعات ناوبری استخراج شده C/A شیفت داده و با داده های اصلی ترکیب شده است (شکل۱).



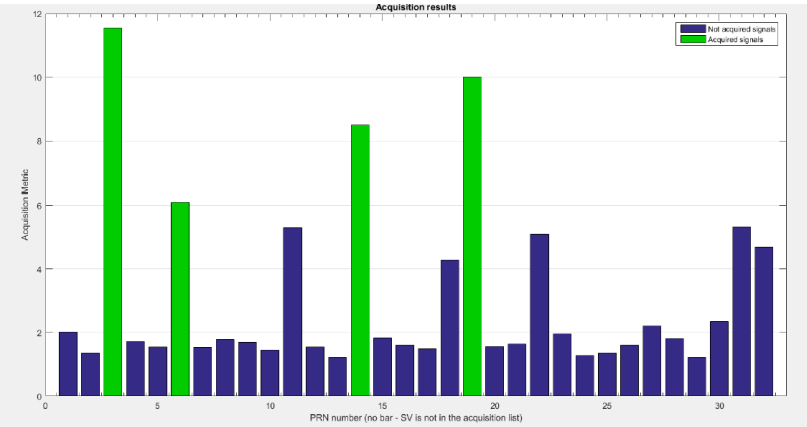
شکل ۱- بلوک دیاگرام جمع‌آوری داده‌ها.

✓ نخستین گام بخش نرم افزاری گیرنده؛ اکتساب

با استفاده از داده‌های اصلی توانستیم ۶ کانال PRN22، PRN11، PRN19، PRN14، PRN6 و PRN3 را به‌عنوان ماهواره‌های در دید شناسایی کنیم (شکل۲). حال اگر همین مراحل را با داده فریب یافته تکرار کنیم، این بار تنها قادر به شناسایی ۴ ماهواره PRN19، PRN14، PRN6 و PRN3 خواهیم بود (شکل۳)، به طوری که سطح اکتساب PRN22 و PRN11 از مقدار آستانه کم‌تر شده و در نتیجه به مرحله ردیابی راه نمی‌یابد.



شکل ۲- نتایج مرحله اکتساب معتبر.



شکل ۳- نتایج مرحله اکتساب جعلی.

✓ حلقه ردیابی

پردازش داده‌ها شامل بخش‌های اکتساب، ردیابی و حل معادلات ناوبری است. ابتدا ماهواره‌های قابل دید شناسایی می‌شوند و با توجه به منبع داده و تعداد کانال‌های مورد پردازش شش ماهواره در دید برای داده‌های اصلی، آشکار می‌شوند. ماهواره‌هایی که نسبت همبستگی بیشینه اول و دوم آن از مقدار ۵/۸ بیش‌تر باشد، به عنوان ماهواره قابل دید در مرحله اکتساب آشکار می شوند. تابع اکتساب از الگوریتم فاز کد موازی استفاده می‌کند و جستجوی سیگنال GPS در گام‌های فرکانس ۰/۵ کیلوهرتز انجام می‌پذیرد و برای هر گام جستجوی کد موازی انجام می‌شود. نتایج همبستگی ذخیره می‌شود و این عمل به ازای گام بعدی فرکانس ادامه می‌یابد تا تمام باند فرکانس را شامل گردد.

در مرحله بعد، تابع به دنبال حداکثر مقدار همبستگی (بیشینه همبستگی) در نتایج حاصل از تمام سطوح فرکانس است. پس از تشخیص بیشینه اول، تابع به دنبال دومین بیشینه همبستگی در سطح فرکانس یکسان از بالاترین قله می‌گردد. پس نسبت دو قله برای قانون تشخیص سیگنال استفاده می‌شود. این نسبت با مقدار از پیش تعیین شده در متغیر گیرنده acq-thershold مقایسه می‌شود. اگر مقدار نسبت بیشینه، بزرگ‌تر از مقدار تعیین‌شده‌ی حد آستانه باشد، فرکانس حامل از طریق رویکرد FFT پس از همبستگی یافت می‌شود. این کار باید برای کمک به PLL در حلقه ردیابی برای شروع ردیابی سیگنال انجام شود. خروجی یک آرایه به نام acq Results است. نتایج شامل نتایج جستجو برای همه ماهواره‌های مشخص‌شده در acq-satellite list است. همان‌طور که در شکل (۴) مشاهده می‌شود، برای داده‌های اصلی ۶ ماهواره به‌ترتیب توان، مرتب شده‌اند؛ PRN22 که دارای بیش‌ترین سطح توان است به‌عنوان کانال اول و PRN11 که دارای کم‌ترین توان است به‌عنوان کانال آخر مرتب می‌گردند. برای داده‌های فریب در خروجی ۴ کانال شناسایی شده‌اند و سطح توان‌های سیگنال متفاوت است (شکل (۵)).

Channel	PRN	Frequency	Doppler	Code Offset	Status
1	22	1.40407e+06	-1323	249	T
2	3	1.40533e+06	-70	5032	T
3	14	1.40302e+06	-2380	871	T
4	19	1.40326e+06	-2141	1830	T
5	6	1.40561e+06	214	2338	T
6	11	1.39993e+06	-5465	2057	T

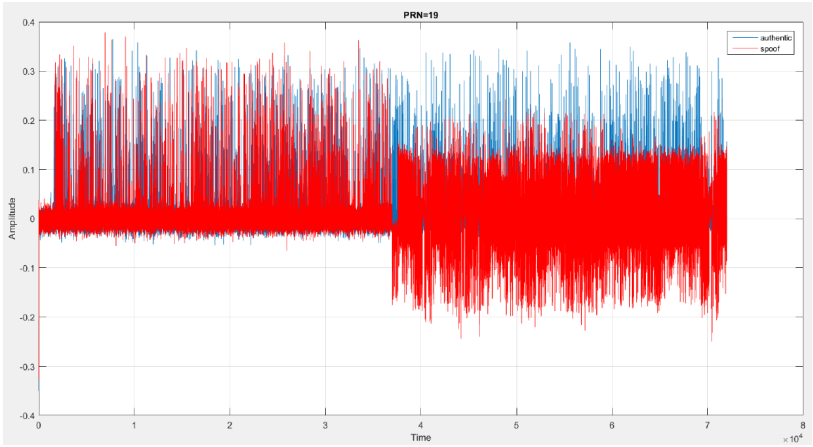
شکل۴- خروجی تابع PreRun داده‌های اصلی.

Channel	PRN	Frequency	Doppler	Code Offset	Status
1	3	1.40533e+06	-70	2176	T
2	19	1.40325e+06	-2151	4819	T
3	14	1.40309e+06	-2304	3876	T
4	6	1.40561e+06	214	5178	T
5	---	----------	-----	------	Off
6	---	----------	-----	------	Off

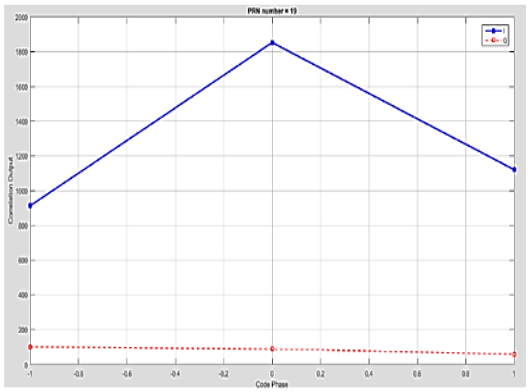
شکل۵- خروجی تابع PreRun داده‌های فریب.

در اینجا از دو منبع داده حقیقی و جعل شده استفاده می‌شود تا در نهایت، با مقایسه تفاوت‌های این دو داده، توسط معیار دلتا بتوانیم داده‌ی معتبر را از جعلی تمیز دهیم. برای کانال‌های ردیابی شده نمودار دلتا را رسم می‌کنیم که در اینجا نمودار PRN19 آورده شده است. در شکل (۶) مشاهده می شود که فریب دامنه سیگنال را کم می‌کند. در سناریو فریب سیگنال جعلی در لحظه‌ی ۳۶ ثانیه اعمال شده است. همان‌طور که در شکل‌های مربوطه ملاحظه می‌شود نمودار دلتا داده‌های اصلی و داده‌های فریب تا لحظه‌ی ۳۶ ثانیه کاملاً منطبق هستند؛ در حالی که بعد از لحظه اعمال سیگنال فریب، نمودار معیار دلتا محاسبه شده در سناریو فریب کاملا متمایز از نمودار مربوط به سناریو بدون فریب می‌باشد که این تمایز، حاکی از وجود فریب در داده‌های جعلی است.

شکل (۷) نمودار همبستگی سیگنال اصلی است، به‌طوری که در حالت معتبر، مقدار هم‌فاز همواره از مقدار متعامد بزرگ‌تر بوده و به‌صورت تقریباً متقارن است. مراحل فوق را برای داده فریب بکار می‌بریم. در این حالت، سطح خروجی همبسته‌ساز هم‌فاز کاهش می‌یابد. در واقع، اختلاف بین هم‌فاز و متعامد در حالت فریب کم و نتایج نمودار دلتا از تقارن مثلثی کمی خارج و دچار اعوجاج می‌شود.



شکل ۶- نمودار دلتا مرحله ردیابی PRN=19 سیگنال اصلی و جعلی.

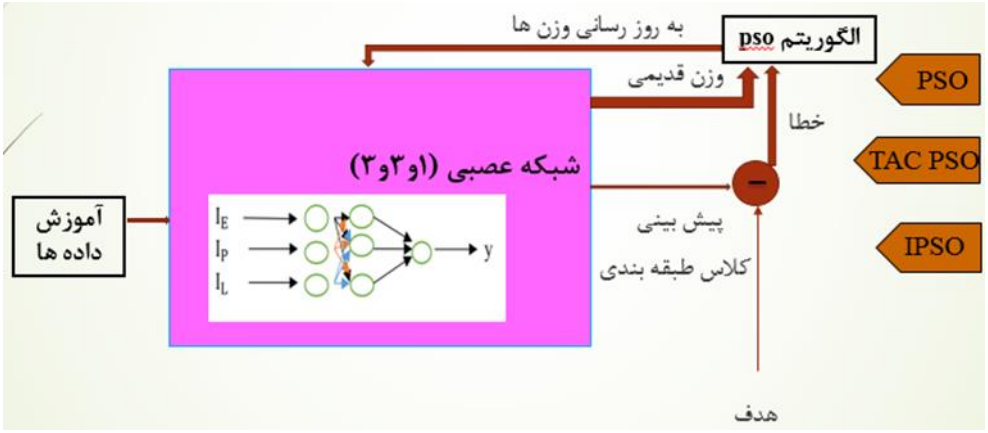


شکل ۷- خروجی همبسته‌ساز داده اصلی PRN=19.

معیار دلتا معایبی دارد که برای ارتقاء آن از شبکه عصبی PSO استفاده شده است که باز هم به دلیل همگرایی کند و گیرکردن در کمینه‌های محلی، شبکه عصبی TACPSO بکار رفته و به منظور بهبود آشکارسازی می‌توان روش‌های هوشمند را ارتقاء داد که بدین منظور یک شبکه عصبی IPSO با ساختار (۱و۳و۳) استفاده شده است و می‌تواند دقت را افزایش دهد.

✓ معماری شبکه عصبی

PSO یکی از رایج‌ترین الگوریتم‌های بهینه‌سازی است که به‌طور گسترده مورد استفاده قرار می‌گیرد. یکی از مزایای PSO که باعث محبوبیت آن شده است، سادگی و محاسبه کم‌هزینه آن است. با این‌حال، به دام افتادن در بهینه محلی و کندی سرعت همگرایی دو موضوع اجتناب‌ناپذیر، برای اکثر الگوریتم‌های تکاملی هستند. یکی از روش‌های رسیدگی به این مشکلات، استفاده از تنظیم پارامتر پویا است که کارآیی الگوریتم PSO را بدون افزایش هزینه محاسباتی بهبود می‌بخشد. در شکل (۸) معماری شبکه عصبی پیشنهادی آورده شده است



شکل۸- معماری یک شبکه عصبی PSO با ساختار (۱و۳و۳).

در الگوریتم اصلی PSO، ذرات از نظر جستجوی محلی و عمومی رفتار مشابهی دارند. شباهت این راهبردها به این معنی است که تمام پارامترها دقیقاً مانند یکدیگر با یک راهبرد تنظیم می‌شوند، به این معنی که ذرات موظف به جستجوی بدون هوش هستند، اما در الگوریتم‌های AGPSO و TACPSO و IPSO به جای آن، راه‌های مختلفی برای تنظیم پارامترهای بهینه‌سازی امتحان می‌شود.

در AGPSO ضرایب به‌گونه‌ای تعریف شده است که در طول تکرار، C_1 کاهش و C_2 افزایش می‌یابد. این بدان معناست که در اولین تکرارهایی که C_1 بزرگ‌تر از C_2 است، ذرات تمایل به کاوش در محدوده محلی دارند. سپس، در تکرارهای بعدی که C_2 بزرگ‌تر از C_1 شد، به‌طورکلی منطقه را جستجو می‌کنند [۲۷]. نتایج به‌دست آمده از شبیه‌سازی نشان می‌دهد که AGPSO3 عملکرد طبقه‌بندی بهتری در مقایسه با AGPSO1 و AGPSO2 دارد. به‌طور خاص، تشخیص سیگنال چندمسیره دارای دقت عالی ۹۵.۳۳٪ است و جعل و پارازیت به‌ترتیب ۹۰.۱۱٪ و ۹۸.۶۷٪ دقیق هستند [۲۷].

پس از تحلیل عملکرد، نتایج به‌دست آمده در [۲۷] با روش‌های [۲۸]، [۲۹] و [۳۰] برای ارزیابی طبقه‌بندی کننده طراحی شده، نشان داد که الگوریتم AGPSO می‌تواند از نظر دقت طبقه‌بندی در مقایسه با معیارهای روش‌های دیگر قبل از آن نتایج بهتری را بدهد. نتایج نشان می‌دهد که، تشخیص چندمسیری حدود ۹۵ درصد بهبود یافته است و تشخیص جعل و پارازیت تقریباً ۳ و ۱ درصد در مقایسه با نتایج [۲۸] دقیق‌تر است.

روشی برای انجام طبقه‌بندی سیگنال‌های GNSS و تشخیص تداخل‌های مختلف، بر اساس ویژگی‌های استخراج شده با روش PD-ML معرفی شده است. در آن از NN های آموزش دیده با الگوریتم TAC-PSO به‌عنوان ابزار طبقه‌بندی استفاده شده است. NN ها ابزار قوی برای انجام طبقه‌بندی بر روی الگوهای غیرخطی قابل تفکیک هستند و الگوریتم TAC-PSO توانایی زیادی برای یافتن و همگرایی به بهینه جهانی را دارد. در الگوریتم طبقه‌بندی [۳۱] آشکارساز اصلی PD-ML، در سیگنال‌های چندمسیری و جعل و همچنین طبقه‌بندی کننده PSO-NN در سیگنال‌های بدون تداخل و پارازیت، بهتر عمل می‌کند. اما با پیچیدگی محاسباتی بیش‌تری همراه است. بنابراین، در کاربردهای خاص باید نسبت به آشکارساز اصلی PD-ML انتخاب شود [۳۲]. روش‌های زیادی برای تشخیص و مقابله با تداخل‌های عمدی و طبیعی در [۳۳] پیشنهاد شده است، (مانند آشکارساز قدرت اعوجاج (PD)) که از قدرت سیگنال و اعوجاج پروفایل همبستگی استفاده می‌کند.

یک شبکه عصبی با ۳ ورودی در نظر می‌گیریم. معماری (۳،۳،۱) که ۳ ورودی، ۱ لایه مخفی با ۳ نرون و ۱ لایه خروجی که یک نرون دارد. همچنین، می‌توانیم از ساختار (۶،۶،۱) نیز استفاده کنیم که این سه مورد Q-E، Q-L و Q-P اضافه می‌شوند. با توجه به پیچیدگی که شبکه دارد و با نماد N-var آن را نشان می‌دهیم، اگر (۳،۳،۱) باشد، پیچیدگی شبکه برای ساختار (۳،۳،۱) از رابطه (۱) و برای ساختار (۶،۶،۱) از رابطه‌ی (۲) استفاده می‌کنیم.

$$order = i * j + j * r + j*r + r = 3 *3 + 3*1 + 3*1 + 1 = 16 \quad (۱)$$

$$order = i * j + j * r + j*r + r = 6 *6 + 6*1 + 6*1 + 1 = 49 \quad (۲)$$

دو مجموعه داده داریم. یک ماتریس تعریف می‌کنیم؛ ۳*۲۰۰۰ برای حالت اول، ۶*۲۰۰۰ برای حالت دوم که در هر کدام ۱۰۰۰ تای اول برای داده اصلی و ۱۰۰۰ تای دوم برای داده‌های جعلی هستند.

با توجه به مقدار در نظر گرفته شده برای ضرایب، الگوریتم PSO به انواع مختلفی از جمله SPSO، TACPSO، MPSO و IPSO تقسیم می‌شود. اگر ضرایب C_1 و C_2 ثابت و به‌طور معمول برابر ۲ در نظر گرفته شوند، آن را SPSO می‌نامیم. اگر مقادیر این دو پارامتر یکسان و به‌صورت رابطه (۳) باشند، TACPSO گفته می‌شوند. در الگوریتم MPSO، توابع برای محاسبه C_1 و C_2 به‌صورت رابطه (۴) [۳۴] و در الگوریتم IPSO با تغییر در محاسبه C_1 و C_2 به‌صورت رابطه (۵) می‌باشند. با توجه به بررسی‌های انجام شده و نتایج شبیه‌سازی‌ها، IPSO عملکرد بهتری داشته و احتمال به دام افتادن آن در بهینه محلی کم‌تر از دیگر انواع الگوریتم اعلام PSO می‌باشد [۳۵]. بنابراین، در این پروژه نتایج تشخیص فریب حاصل از الگوریتم IPSO و TACPSO اعمال شده است و بیان می‌شود که روش پیشنهادی IPSO با اصلاح ضرایب، پتانسیل بالایی در تئوری و آزمایش دارد.

$$C_1 = C_2 = 2.2 - \exp\left[-(4t/T)^2\right] \quad (۳)$$

$$C_1 = \left(-\frac{2.05}{T}\right) t + 2.55$$

$$C_2 = \left(\frac{1}{T}\right) t + 1.25 \quad (۴)$$

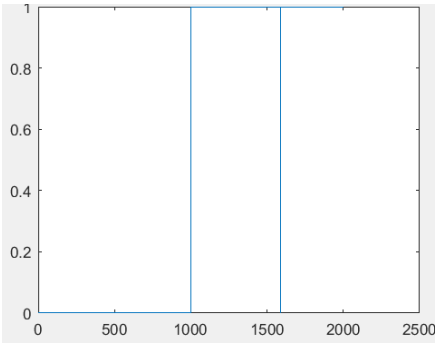
$$C_1 = 2.5 + 2\left(\frac{t}{T}\right)^2 - 2\left(\frac{2t}{T}\right)$$

$$C_2 = 0.5 - 2\left(\frac{t}{T}\right)^2 + 2\left(\frac{2t}{T}\right) \quad (۵)$$

که در آن‌ها C_1 و C_2 عوامل شتاب منفی (یا عوامل یادگیری) هستند که به‌ترتیب توانایی خودآموزی و توانایی یادگیری اجتماعی ذرات را کنترل می‌کنند و t و T به‌ترتیب تعداد فعلی و حداکثر تعداد تکرارها هستند.

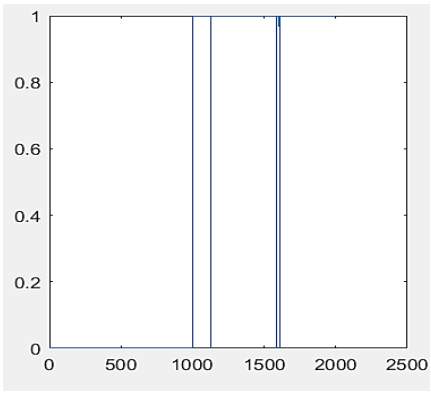
✓ تشخیص فریب در مرحله ردیابی مبتنی بر شبکه‌های عصبی

ردیابی با شبکه عصبی PSO تعریف شده است، نتایج تشخیص فریب نسبت به حالت قبل خیلی بهتر شده است. در این حالت شبیه‌سازی با دو خطا انجام شده، همچنین دقت آن ۹۹/۹ درصد است (شکل ۹).



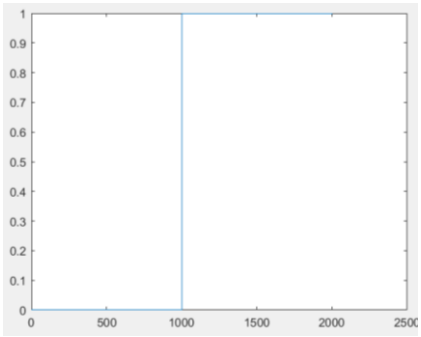
شکل ۹- نمودار بهبود نتایج با شبکه‌ی عصبی PSO.

مقادیر بهترین تجربه شخصی و بهترین تجربه عمومی برای PSO را متغیر با زمان تغییر داده‌ایم. در واقع، شبکه عصبی PSO را به شکل IPSO اصلاح کرده‌ایم. با ۴ خطا شبیه‌سازی انجام شده است و دقت آن ۹۹/۸ درصد است (شکل ۱۰).



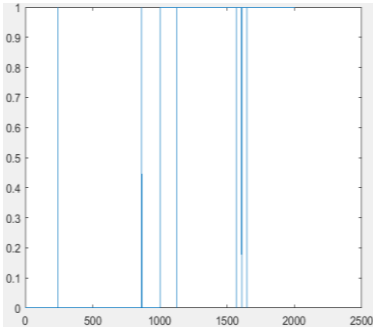
شکل ۱۰- نمودار نتایج با شبکه‌ی عصبی IPSO.

مقادیر بهترین تجربه شخصی و بهترین تجربه عمومی برای IPSO متغیر با زمان تغییر دادیم. در واقع، ضرایب شبکه عصبی را به شکل IPSO با ضرایب اصلاح شده شبیه‌سازی کردیم. با ۱ خطا شبیه‌سازی انجام شده است و دقت آن ۹۹/۹۵ درصد است(شکل ۱۱).



شکل ۱۱- نمودار بهبود نتایج با شبکه‌ی عصبی IPSO با ضرایب اصلاح شده.

شبیه‌سازی را برای TACPSO با ضرایب بهترین تجربه ی شخصی و بهترین تجربه‌ی عمومی را نیز انجام دادیم که با ۷ خطا انجام شده است و نتایج مطابق شکل (۱۲) به دست آمد که دقت ۹۹/۶۵ درصد است.



شکل ۱۲- نمودار بهبود نتایج با شبکه‌ی عصبی TACPSO.

✓ مقایسه‌ی عملکرد شبکه‌های عصبی در تشخیص فریب

الگوریتم BP برای آموزش MLP NN با محاسبه وزن‌ها و بایاس‌های اتصال استفاده می‌شود اما از معایبی که دارد، ممکن است به دلیل وابستگی زیاد به پارامترهای اولیه، در بهینه محلی به دام افتد. نرخ همگرایی آن کند است و ممکن است نتایج کم‌تری ایجاد کند. شبکه عصبی IPSO می‌تواند تشخیص فریب را توسط متلب انجام دهد، در شبیه‌سازی از PSO و TACPSO و IPSO استفاده‌شده است که بیش‌ترین دقت در تشخیص را IPSO داشته است. با مقایسه‌ی نتایج تشخیص فریب این سه الگوریتم هوشمند، می‌توان دریافت که IPSO می‌تواند تشخیص فریب را به دقت انجام دهد و در کارایی شناسایی و عملکرد در حال اجرا از برخی الگوریتم‌های رایج پیشی می‌گیرد، علاوه بر این IPSO پیش از موعد خاتمه نمی‌یابد و در طی شناسایی وارد بهینه‌سازی محلی می‌شود، که نشان می‌دهد IPSO در بهبود روش محاسبه وزن اینرسی مؤثر است. در جدول (۲) مقایسه ی نتایج تشخیص فریب الگوریتم‌های آزموده شده آورده شده است.

جدول۲- مقایسه‌ی نتایج حاصل از تشخیص فریب مبتنی بر شبکه‌های عصبی.

ساختار شبکه عصبی	پیچیدگی	تعداد خطا	درصد تشخیص صحیح
IPSO (با ضرایب اصلاح‌شده)	۱۶	Z=۱	۹۹/۹۵
PSO	۱۶	Z=۲	۹۹/۹۰
TACPSO	۱۶	Z=۷	۹۹/۶۵
IPSO	۱۶	Z=۴	۹۹/۸
AGPSO	۱۶	Z=۱۹۷	۹۰/۱۱

۸. جمع‌بندی و نتیجه‌گیری

در این مقاله، انواع حملات فریب و روش‌های تشخیص فریب و مقایسه‌ی آن‌ها معرفی‌شده‌اند، که در میان آن‌ها روش‌های مبتنی بر پردازش سیگنال، هزینه‌ی کم‌تری و قابلیت اجرای بیش‌تری دارند، به همین جهت از پردازش سیگنال برای آشکارسازی فریب استفاده شده است. با استفاده از گیرنده رادیو نرم‌افزار SDR و بررسی دلتا در مرحله‌ی حلقه ردیابی گیرنده، با رسم نمودارهای بخش هم‌فاز و متعامد و داده اصلی و جعلی، سعی در تشخیص هرگونه ناهنجاری و تغییر شکل در سیگنال جهت آشکارسازی حمله فریب صورت گرفته است. روش گیرنده نرم‌افزاری بکار رفته دقت بالایی دارد و نیاز به سخت‌افزار اضافه ندارد. به‌منظور ردیابی سیگنال برای هر دو داده‌ی اصلی و فریب از معیار دلتا به‌صورت جداگانه تعریف شده است.

در حالت فریب اختلاف بین هم‌فاز و متعامد کم می‌شود و نتایج نمودار دلتا از تقارن مثلثی کمی به هم می‌خورد و دچار اعوجاج می‌شود. به‌منظور بهبود آشکارسازی یک شبکه عصبی IPSO، با ساختار (۱و۳و۳) استفاده شده است که دقت را افزایش داده است. در نهایت، نتایج شبیه‌سازی الگوریتم‌های پیشنهادی مقایسه می‌شوند، که در بین آن‌ها IPSO با ضرایب اصلاح شده با دقت ۹۹/۹۵ درصد، کم‌ترین خطا را نشان می‌دهد. همچنین، در این مقاله از سه همبسته‌ساز برای ردیابی و نظارت سیگنال استفاده شد. با افزایش تعداد همبسته‌سازها می‌توان دقت این روش را افزایش داد.

۹. مراجع

[1] M. Garcia, T. Catanach, S. Vander Wiel, R. Bent, and E. Lawrence, "Line Outage Localization using Phasor Measurement Data In Transient State," IEEE Transactions on Power Systems, vol. 31, no. 4, pp. 3019-3027, 2015.

[2] A. Xue, F. Xu, J. Xu, J. H. Chow, S. Leng, and T. Bi, "Online Pattern Recognition and Data Correction of PMU Data Under GPS Spoofing Attack," Journal of Modern Power Systems Clean Energy, vol. 8, no. 6, pp. 1240-1249, 2020.

[3] C. Riedel, G. Fu, D. Beyette, and J. C. Liu, "Measurement System Timing Integrity in the Presence Of Faults And Malicious Attacks," IEEE Conference on Smart Grid Synchronized Measurements and Analytics (SGSMA), pp. 1-8, 2019.

[4] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, and A. D. Domı, "Spoofing GPS Receiver Clock Offset of Phasor Measurement Units," IEEE Transactions on Power Systems, vol. 28, no. 3, pp. 3253-3262, 2013.

[5] Y. Zuo, X. Zhang, B. Li, and J. Fu, "Reaserch on the Impact of Satellite Navigation Time Service Interference on Power System Transmission Line Fault Location," IEEE Chinese Automation Congress (CAC), vol. 5, pp. 1449-1453, 2020.

[6] K. E. Martin, "Synchrophasor Measurements", IEEE Transactions on Power Delivery, vol. 30, no. 3, pp. 1514-1522, 2015.

[7] W. T. Li, C. K. Wen, J. C. Chen, K. K. Wong, J. H. Teng, and C. Yuen, "Location Identification of Power Line Outages using PMU Measurements with Bad Data," IEEE Transactions on Power Systems, vol. 31, no. 5, pp. 3624-3635, 2015.

[8] E. Shafiee, M. R. Mosavi, and M. Moazedi, "Detection of Spoofing Attack using Machine Learning Based on Multi-Layer Neural Network in Single-Frequency GPS Receivers," The Journal of Navigation, vol. 71, no. 1, pp. 169-188, 2018.

[9] X. Fan, S. Pal, D. Duan, and L. Du, "Closed-Form Solution for Synchrophasor Data Correction Under GPS Spoofing Attack," IEEE Power & Energy Society General Meeting (PESGM), vol. 6, pp. 1-5, 2018.

[10] X. Fan, L. Du, and D. Duan, "Synchrophasor Data Correction Under GPS Spoofing Attack: A State Estimation-Based Approach," IEEE Transactions on Smart Grid, vol. 9, no. 5, pp. 4538-4546, 2017.

[11] P. Risbud, N. Gatsis, and A. Taha, "Vulnerability Analysis of Smart Grids to GPS Spoofing," IEEE Transactions on Smart Grid, vol. 10, no. 4, pp. 3535-3548, 2018.

[12] Y. Zhang, J. Wang, and J. Liu, "Attack Identification and Correction for PMU GPS Spoofing in Unbalanced Distribution Systems," IEEE Transactions on Smart Grid, vol. 11,

no. 1, pp. 762-773, 2019.

[13] J. Lee, A. F. Taha, N. Gatsis, and D. Akopian, "Tuning-Free, Low Memory Robust Estimator to Mitigate GPS Spoofing Attacks," IEEE Control Systems Letters, vol. 4, no. 1, pp. 145-150, 2019.

[14] E. Shafiee, M. R. Mosavi, and M. Moazedi, "Detection of Spoofing Attack using Machine Learning Based on Multi-Layer Neural Network in Single-Frequency GPS Receivers," The Journal of Navigation, vol. 71, no. 1, pp. 169-188, 2018.

[15] P. Risbud, N. Gatsis, and A. Taha, "Multi-Period Power System State Estimation with PMUs Under GPS Spoofing Attacks," Journal of Modern Power Systems Clean Energy, vol. 8, no. 4, pp. 597-606, 2020.

[16] M. Yasinzadeh and M. Akhbari, "Detection of PMU Spoofing in Power Grid Based on Phasor Measurement Analysis," IET Generation Transmission Distribution, vol. 12, no. 9, pp. 1980-1987, 2018.

[17] K. E. Martin et al., "Standard for Synchrophasors for Power Systems," IEEE Transactions on Power Delivery, vol. 13, no. 1, pp. 73-77, 1998.

[18] L. Heng, J. J. Makela, A. D. Dominguez-Garcia, R. B. Bobba, W. H. Sanders, and G. X. Gao, "Reliable GPS-Based Timing for Power Systems: A Multi-Layered Multi-Receiver Architecture," Power and Energy Conference At Illinois (PECI), vol. 14, pp. 1-7, 2014.

[19] S. A. Desilva, J. Kim, E. Cotilla-Sanchez, and T. Hagan, "On PMU Data Integrity Under GPS Spoofing Attacks: A Aparse Error Correction Framework," IEEE Transactions on Power Systems, vol. 5, pp. 432-443, 2021.

[20] J. Zhang, Z. Chu, L. Sankar, and O. Kosut, "False Data Injection Attacks on Phasor Measurements That Bypass Low-Rank Decomposition," IEEE Conference on Ssmart Grid Communications (Smart Grid Comm), vol. 7, pp. 96-101, 2017.

[21] T. A. Alexopoulos, G. N. Korres, and N. Manousakis, "Complementarity Reformulations for False Data Injection Attacks on PMU-Only State Estimation," Electric Power Systems Research, vol. 189, p. 106796, 2020.

[22] S. M. Moosavi and S. M. S. Moazedi, "High-Sensitivity GPS Spoof Data Classification Based On Fuzzy Logic," Scientific Quarterly of Sea Technologies, vol. 8, no. 1, pp. 115-126, 2021.

[23] Y. Fan, Z. Zhang, M. Trinkle, A. D. Dimitrovski, J. B. Song, and H. Li, "A Cross-Layer Defense Mechanism Against GPS Spoofing Attacks on PMUs in Smart Grids," IEEE Transactions on Smart Grid, vol. 6, no. 6, pp. 2659-2668, 2014.

[24] J. Magiera, "A Multi-Antenna Scheme For Early Detection and Mitigation of Intermediate GNSS Spoofing," Sensors, vol. 19, no. 10, p. 2411, 2019.

[25] A. Jafarnia Jahromi, "GNSS Signal Authenticity Verification in the Presence of Structural Interference," University of Calgary, vol. vol 30, no 4, pp. 181–191, 2013.

[26] M. R. Mosavi, E. Shafiee, and M. Moazedi, "Detection and Detection of Deception Attack in Single-Frequency GPS Receiver Based on Multilayer Neural Network," Electronic and Cyber Defense, vol. 3, no. 1, 2015.

[27] M. R. Ghasemi, S. Tohidi, and M. R. Mosavi, "GNSS Interference Classification using Multi-Layer Perceptron Neural Network Trained by AGPSO," International Journal of Computer Science Network Security, vol. 06190426, 2021.

[28] K. D. Wesson, J. N. Gross, T. E. Humphreys, and B. L. Evans, "GNSS Signal Authentication Via Power and Distortion Monitoring," IEEE Transactions on Aerospace Electronic Systems, vol. 54, no. 2, pp. 739-754, 2017.

[29] J. N. Gross, C. Kilic, and T. E. Humphreys, "Maximum-Likelihood Power-Distortion Monitoring for GNSS-Signal Authentication," IEEE Transactions on Aerospace Electronic Systems, vol. 55, no. 1, pp. 469-475, 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," IEEE 25th International Computer Conference, Computer Society of Iran (CSICC), vol. 45, pp. 1-5, 2020.

[31] A. R. Kazemi, S. Tohidi, and M. R. Mosavi, "Enhancing Classification Performance Between Different GNSS Interferences using Neural Networks Trained by TAC-PSO Algorithm," IEEE Symposium onTelecommunications (IST), vol. 8, pp. 150-154, 2020.

[32] A. Nobahari, M. Safari, M. Mosavi, P. Amiri, and S. Processing, "Analog 8-Point DFT Processor With Low-Power Consumption and High-Speed For Interference Mitigation in GPS Receivers," Analog Integrated Circuits, vol. 102, no. 1, pp. 181-203, 2020.

[33] J. N. Gross, C. Kilic, and T. E. Humphreys, "Maximum-Likelihood Power-Distortion Monitoring For GNSS-Signal Authentication," IEEE Transactions on Aerospace Electronic Systems, vol. 55, no. 1, pp. 469-475, 2018.

[34] G. Bao and K. Mao, "Particle Swarm Optimization Algorithm with A Symmetric Time Varying Acceleration Coefficients," IEEE Conference on Robotics and Biomimetics (ROBIO), vol. 7, pp. 2134-2139, 2009.

[35] B. Abbasi and M. R. Mosavi, "Reduce The Effect of Intervention in The GPS Navigation System by using The Evolutionary Gap Filter," Electronic and cyber defense, vol. 8, no. 4, pp. 95-106, 2020.