آشکارسازی اختلال در گیرنده‌های GNSS با استفاده از شبکه عصبی آموزش یافته با الگوریتم تکاملی زنبور عسل

سمیرا توحیدی[۱]، آناهیت چایچی سلیمی[۲]، سید محمدرضا موسوی میرکلائی [*,۳].

۱- دانشجو دکتری، دانشکده مهندسی برق، دانشگاه علم و صنعت ایران، تهران

۲- کارشناسی، دانشکده مهندسی برق، دانشگاه علم و صنعت ایران، تهران

۳- نویسنده مسئول، استاد، دانشکده مهندسی برق، دانشگاه علم و صنعت ایران، تهران

چکیده

سامانه ناوبری ماهواره‌ای جهانی (GNSS)[۱] فناوری پیشرفته‌ای محسوب می‌شود که در موارد مختلفی مانند مکان‌یابی و ناوبری، زمان‌بندی دقیق و تنظیم فرکانسی کاربرد دارد. از آنجا که سیگنال‌های GNSS از ماهواره تا رسیدن به گیرنده زمینی مسافت نسبتاً طولانی طی می‌کنند، در سطح زمین توان پایینی دارند و لذا در برابر انواع اختلال آسیب‌پذیر خواهند بود. سه دسته اختلالاتی که عملکرد صحیح این سامانه را تحت تاثیر قرار می‌دهند، عبارتند از: فریب، جمینگ و چندمسیری. در این مقاله، تشخیص نوع تداخل احتمالی با استفاده از یک شبکه عصبی به عنوان الگوریتم دسته‌بندی کننده، انجام خواهد شد. به منظور دسته‌بندی قوی‌تر، شبکه عصبی طراحی شده، با الگویتم تکاملی زنبور عسل (ABC)[۲] آموزش داده می‌شود. لازم به ذکر است که هدف این مقاله بهبود تشخیص انواع اختلال و به طور خاص بهبود تشخیص حمله فریب در سامانه GNSS می‌باشد، چرا که این حمله به دلیل پنهانی بودن، خطرناک‌تر از دو اختلال دیگر یعنی جمینگ و چندمسیری بوده و تشخیص آن مشکل‌تر است. روش پیشنهادی، توانست به میانگین دقت آشکارسازی اختلال ۷۱.۵۳ درصد دست یابد و به طور خاص در تشخیص فریب، بهبود ۵.۰۸ درصدی و ۷.۷۷ درصدی نسبت به مراجع مورد مقایسه، حاصل شد.

کلمات کلیدی: GNSS، دسته‌بندی، آشکارسازی تداخل، الگوریتم تکاملی، شبکه‌های عصبی.

۱. مقدمه

سامانه‌ی ناوبری ماهواره‌ای جهانی (GNSS)، ابزاری مناسب برای اندازه‌گیری ساعت دقیق، ارتفاع، طول و عرض جغرافیایی هر نقطه از زمین می‌باشند. این سامانه با استفاده از امواج دریافتی از ماهواره‌های موجود در مدار و به کمک گیرنده‌های زمینی، مکان یک نقطه را در فضای سه‌بعدی تعیین می‌کند. GNSS از سامانه‌های ماهواره‌ای مختلف منطقه‌ای و جهانی تشکیل می‌گردد که هر کدام از آن‌ها متعلق به یک یا چند کشور بوده و هدف از ترکیب آن‌ها، افزایش دقت تعیین موقعیت و ناوبری می‌باشد.

سامانه GNSS نقاط ضعفی دارد که اختلال‌گران با بهره‌گیری از آن‌ها، حملات مختلف را ایجاد می‌کنند و این سامانه را تحت تأثیر قرار می‌دهند. به طور کلی می‌توان ضعف‌های این سامانه را در سه عبارت خلاصه کرد: ۱- سامانه ناوبری

* **Corresponding author (Email: m_mosavi@iust.ac.ir)**
[1] Global Navigation Satellite System
[2] Artificial Bee Colony

رادیویی، ۲- پایین بودن سطح توان سیگنال دریافتی از ماهواره‌ها در سطح زمین و ۳- نرخ به روز رسانی ضعیف. با توجه به این عیوب، دو راه اصلی برای حمله به گیرنده GNSS وجود دارد که به شرح زیر هستند [۱و۲]:

جمینگ: از آنجا که توان سیگنال معتبر GNSS در سطح زمین حدود 10^{-16} وات است، می‌تواند به طور موثری توسط سیگنالی با همان فرکانس، اما با توانی به مراتب بالاتر، منع گردد. در واقع، این اختلال گیرنده را از دنبال کردن سیگنال‌های اصلی GNSS باز می‌دارد [۲و۳]. علاوه بر این، اخلال‌گرها گاه با ایجاد شکاف بین آنتن و گیرنده موجب عدم دریافت سیگنال معتبر GNSS در گیرنده می‌شود [۲و۴] که به آن بلاکینگ گفته می‌شود.

فریب: در این نوع اختلال، سیگنال‌های جعلی جایگزین سیگنال‌های معتبر می‌شوند. از آنجا که این حمله به صورت مخفیانه انجام می‌گردد، نسبت به نوع قبلی ظریف‌تر بوده و تشخیص آن مشکل‌تر است [۵-۹].

۲. فریب در گیرنده‌های GNSS

در حال حاضر، فریب به عنوان خطرناک‌ترین خطای عمدی GNSS شناخته می‌شود. هدف فریب‌دهنده آن است که گیرنده GNSS به جای راه‌حل ناوبری صحیح، راه‌حلی غلط تولید کند [۱۰-۱۳]. سیگنال جعلی به گونه‌ای طراحی می‌شود که بر سیگنال اصلی غلبه کند و کنترل گیرنده را برعهده گیرد. به دلیل پایین بودن سطح توان سیگنال اصلی، یک تداخل کم‌توان به راحتی می‌تواند یک گیرنده GNSS تجاری را در شعاع چند کیلومتری فریب دهد. هر سامانه فریب‌دهنده، بسته به نوع آن، محدوده اثر مشخصی دارد که فقط در آن ناحیه می‌تواند گیرنده‌های GNSS را منحرف نماید. این حمله و لذا مقابله با آن می‌تواند در هر یک از سطوح گیرنده از جمله بخش بیت داده، اکتساب، ردیابی، استخراج شبه‌فاصله و معادلات ناوبری صورت گیرد.

از آنجا که حذف کامل سیگنال معتبر GNSS مشکل است، در یک حمله فریب معمولاً ترکیبی از سیگنال‌های معتبر و جعلی وجود دارد که در بیشتر موارد موجب آسیب دیدن سیگنال معتبر خواهد شد. شدت تخریب سیگنال معتبر، فرصتی برای تشخیص حمله فریب است. بر این اساس، با بررسی مشخصات سیگنال GNSS دریافتی توسط گیرنده و مقایسه آن با سیگنال معتبر، می‌توان وجوه تمایز را استخراج نمود و به وجود فریب پی برد [۱۴-۱۷].

باید در نظر داشت که تولید سیگنال فریبی که به صورت هم‌زمان هر دو مشخصه توان و توزیع همبستگی آن منطبق با سیگنال اصلی باشد، بسیار مشکل است. لذا، با نظارت توام این دو مشخصه، دقت و صحت تشخیص بسیار افزایش می‌یابد. به این ترتیب، امکان تشخیص فریب‌های پیچیده با حضور چندمسیری و تفکیک اختلالات مختلف، ممکن می‌گردد [۱۲و۱۸]. روش ترکیبی، مستقل از نوع گیرنده بوده و با تغییر اندکی، می‌توان آن را برای محدوده وسیعی از گیرنده‌ها به کار برد.

۳. تشخیص حمله فریب در GNSS با استفاده از شبکه عصبی

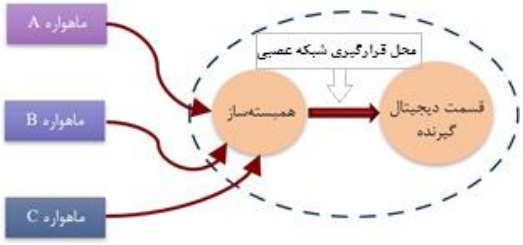
این مقاله یک شبکه عصبی پرسپترون چندلایه‌ی آموزش دیده شده با الگوریتم بهینه‌ساز زنبور عسل (ABC)[1] را به عنوان یک طبقه‌بندی کننده چندگانه برای تشخیص حملات فریب پیشنهاد می‌کند. با استفاده از الگویتم تکاملی ABC، وزن‌های شبکه عصبی جهت ایجاد شبکه‌ای با بهترین قدرت تشخیص اختلال، بصورت بهینه تعیین می‌گردد.

با توجه به کاربرد گسترده‌ی سامانه GNSS، نظارت و تشخیص تداخل برای محافظت از این سامانه بسیار مهم است. نظارت بر تداخل فرآیندی است که عموماً با استفاده از دو روش: ۱- پیش از انتشار و ۲- پس از انتشار انجام می‌شود. یکی از پرکاربردترین روش‌های پیش از انتشار، اندازه‌گیری قدرت سیگنال دریافتی در باند GNSS است. نظارت بر اعوجاج سیگنال دریافتی در حلقه ردیابی، یکی از معیارهای مورد استفاده برای تشخیص تداخل در سامانه GNSS است که در

[1] Artificial Bee Colony

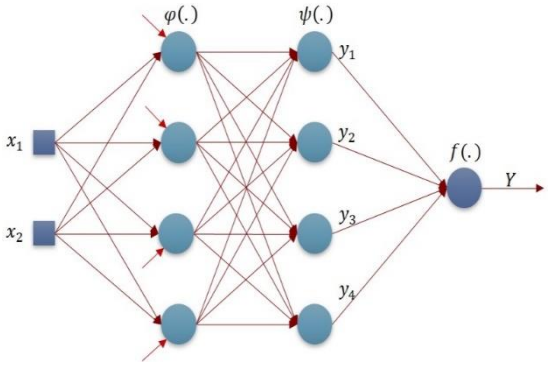
دسته روش‌های پس از انتشار قرار می‌گیرد [۱۹-۲۱]. روش پیشنهادی در این مقاله از این دو معیار، قدرت سیگنال دریافتی و اعوجاج تابع همبستگی، به عنوان بردار ویژگی استفاده می‌کند و تلاش می‌نماید سیگنال‌های دریافتی را به عنوان سیگنال‌های جمینگ، فریب، چندمسیری یا سیگنال بدون تداخل طبقه‌بندی کند.

شکل (۱) محل قرارگیری شبکه عصبی مذکور را در گیرنده GNSS نشان می‌دهد. در واقع، شبکه پس از همبسته‌سازها و قبل از واحد پردازش ناوبری قرار می‌گیرد.



شکل ۱: ساختار کلی گیرنده GNSS.

شکل (۲) ساختار شبکه پرسپترون چند لایه استفاده شده را نشان می‌دهد. این فرم عمومی شبکه به صورت اتصال کامل است. یعنی یک نرون از هر لایه شبکه به تمام نرون‌های لایه قبلی و لایه بعدی متصل می‌شود.



شکل ۲: ساختار شبکه عصبی استفاده شده به عنوان دسته‌بندی کننده.

۱-۳. مراحل تعلیم شبکه

مراحل تعلیم این شبکه عصبی به شرح زیر می‌باشد:

گام صفر: مقداردهی اولیه وزن‌ها

کلیه پارامترهایی که باید تنظیم گردند، با مقادیر کوچک و به صورت تصادفی با توزیع یکنواخت، مقداردهی اولیه می‌شوند.

گام اول: محاسبه ورودی نرون‌های اولین لایه مخفی مطابق رابطه (۱):

$$V_j = \sum_{i=1}^{2} x_i w_{ji} + b_j \; ; \text{j=1 to 4} \qquad (۱)$$

که در آن، x_i ورودی i ام، b_j مقدار بایاس نرون j ام و w_{ji} وزن انتقال ورودی i ام به نرون j ام در لایه بعدی می‌باشد.

گام دوم: محاسبه خروجی نرون‌های اولین لایه مخفی مطابق رابطه (۲):

$$z_j = \varphi_j[V_j] \quad (۲)$$

که در آن، φ_j تابع فعال‌ساز لایه مخفی اول و V_j بردار ورودی تابع است.

گام سوم: محاسبه ورودی نرون‌های دومین لایه مخفی مطابق رابطه (۳):

$$L_k = \sum_{j=1}^{4} z_j \beta_{kj} \; ; \; k = 1 \text{ to } 4 \quad (۳)$$

که در آن، z_i خدوجی i ام لایه مخفی اول و β_{kj} وزن انتقال نرون j ام لایه مخفی اول به نرون k ام در لایه بعدی می‌باشد.

گام چهارم: محاسبه خروجی نرون‌های دومین لایه مخفی مطابق رابطه (۴):

$$y_k = \Psi_k[L_k] \quad (۴)$$

که در آن، Ψ_k تابع فعال‌ساز لایه مخفی دوم و L_k بردار ورودی این تابع است.

گام پنجم: محاسبه ورودی نرون لایه خروجی مطابق رابطه (۵):

$$M(n) = \sum_{k=1}^{4} y_k \quad (۵)$$

گام ششم: محاسبه خروجی نرون لایه خروجی مطابق رابطه (۶):

$$Y(n) = f[M(n)] \quad (۶)$$

که در آن، $f[.]$ تابع خروجی می‌باشد.

گام هفتم: به‌روزرسانی تمام وزن‌های اتصالی و بایاس‌ها با استفاده از الگوریتم تکاملی ABC می‌باشد. جزئیات محاسبات این گام در بخش ۳-۲ مقاله شرح داده می‌شود.

گام هشتم: تکرار
بازگشت به گام ۱ و ادامه روند تا حصول همگرایی در کلیه وزن‌ها.

۳-۲. شبکه عصبی تعلیم یافته با الگوریتم تکاملی زنبور عسل برای آشکارسازی تداخل

همان‌طور که در بخش قبل بیان شد، در این مقاله، برای دسته‌بندی دقیق‌تر و دریافت پاسخ بهتر از شبکه عصبی، این شبکه با استفاده از الگوریتم تکاملی زنبور عسل آموزش داده شده است. این الگوریتم شامل ۴ بخش اصلی می‌باشد که در ادامه شرح داده شده‌اند [۲۲].

۳-۲-۱. تعریف مسئله بهینه‌سازی

در این مرحله، مواردی از قبیل تابع هدف، تعداد متغیرها، محدوده تغییرات متغیرها و ساختار پاسخ تعریف می‌شود. هدف ما بهینه‌سازی وزن‌های شبکه عصبی MLP است که ساختار ۱-۴-۴-۲ دارد (مطابق شکل (۲)). برای چنین ساختاری، مرتبه مطابق رابطه (۷) قابل محاسبه است.

$$\text{Order} = 2\times4 + 4\times4 + 4 = 28 \quad (۷)$$

بنابراین، به ۲۸ متغیر تصمیم‌گیری نیاز است و تغییرات آن‌ها را در بازه ۱± تنظیم می‌شود.

۲-۲-۳. تعریف پارامترهای الگوریتم ABC

در این بخش، اندازه جمعیت و تعداد تکرارهای مجاز برای الگوریتم تعیین می‌گردد. این مقادیر با توجه به نتایج حاصل از شبیه‌سازی و انتظارات ما، با آزمون و خطا تعیین می‌گردد.

۳-۲-۳. آماده‌سازی

در این فاز مشخص می‌شود که هر زنبور عسل و منبع غذایی که معرفی می‌کند، چه مشخصاتی دارد. منظور از مشخصات، مکان قرارگیری[1] و ارزش[2] آن می‌باشد. ابتدا پارامترهای مکان قرارگیری و ارزش را برای یک زنبور تعریف کرده و مقدار آن را خالی گذاشته و سپس این موارد را به تعداد زنبورها، یعنی nPop تکثیر کردیم.

به عنوان مقدار اولیه، باید بدترین حالت را در نظر بگیریم تا اولین پاسخ بتواند در مقایسه با آن اثر خود را نشان دهد. در مسائل کمینه‌سازی، بدترین حالت پاسخ بی‌نهایت بوده و در مسائل بیشینه‌سازی منفی بی‌نهایت می‌باشد. حال، به مکان قرارگیری، مقداری تصادفی نسبت می‌دهیم و ارزش متناظر را حساب می‌کنیم. درصورتی که ارزش حاصله، از بهترین جوابی که تاکنون گرفته‌ایم بهتر باشد، این عضو جایگزین بهترین جواب قبلی خواهد شد.

برای مکان قرارگیری، در برنامه نویسی MATLAB از دستور unifrnd استفاده شده تا با توزیع یکنواخت، برای هر کدام از متغیرها، یک عدد تصادفی در بازه تغییر آن، انتخاب گردد. یک شمارنده با مقدار اولیه صفر برای شمارش تعداد تکرارها به کار می‌رود. همچنین، برای گزارش‌گیری از الگوریتم، جواب‌ها را در یک ماتریس ذخیره می‌شود.

۴-۲-۳. حلقه اصلی الگوریتم

این حلقه به تعداد تکرار تعیین شده[3] انجام خواهد شد. هر حلقه سه قسمت دارد:

زنبورهای استخدام شده[4]

حرکت این زنبورها برای پیدا کردن نقاط جدید و بهتر، مطابق رابطه (۸) می‌باشد:

$$V_{ij} = x_{ij} + \Phi_{ij}\,(x_{kj} - x_{ij}) \qquad (۸)$$

که در آن، V_{ij} موقعیت جدید، x_{ij} موقعیت قبلی و عبارت داخل پرانتز اختلاف موقعیت مبدأ و مقصد است. k نیز عددی تصادفی بین ۱ تا n_{pop} است که مخالف i باشد. Φ_{ij} یک عدد تصادفی یکنواخت یا غیریکنواخت در بازه‌ی a– تا a است که مطابق رابطه (۹) به دست می‌آید.

$$\Phi_{ij} \sim u(-a,a) \qquad (۹)$$

حرکت می‌تواند در یک بعد یا تعداد بعد بیشتری باشد که در این صورت j به صورت تصادفی از بازه {1,2,…,D} که در آن، D تعداد بعدهاست، انتخاب می‌گردد. در اینجا برای سادگی این مقدار را حذف کردیم.

پس از تعریف مقادیر k و Φ، مکان جدید مطابق رابطه (۸) محاسبه شده و ارزش متناظر با آن محاسبه می‌گردد. سپس، این مقدار با بهترین جواب مقایسه شده و در صورت نیاز، مقدار آن را به روز می‌کند. پس از این مراحل، شمارنده مربوط به تعداد تکرار، یکی اضافه می‌شود و شایستگی متناظر با هر کدام محاسبه شده و بر اساس آن، احتمال انتخاب هر پاسخ به دست می‌آید.

زنبورهای جستجوگر[5]

[1] Position
[2] Cost
[3] MaxIt
[4] Employed Bees
[5] Onlooker Bees

در اینجا نیز مراحل، مشابه مرحله قبل است، با این تفاوت که می‌خواهیم این زنبورها به صورت تصادفی منابع را که دارای احتمال P هستند، جستجو نمایند. پس باید متغیر i به صورت تصادفی انتخاب گردد که برای این کار از چرخه رولت استفاده شده است. پس از انتخاب تصادفی i، مراحل این زنبورها مشابه زنبورهای استخدام شده خواهد بود.

زنبورهای پیش‌آهنگ[1]

در این مرحله، پاسخ‌هایی که تعداد تکرار آن‌ها به حد مجاز رسیده است با پاسخ‌های تصادفی جدید جایگزین خواهند شد و شمارنده مربوط به تعداد تکرار صفر می‌گردد. سپس بار دیگر، بهترین پاسخ به روز می‌شود. در انتهای الگوریتم، مکان بهترین پاسخ‌ها را در متغیری ذخیره شده تا در تابع مربوط به شبکه عصبی به عنوان مقادیر وزن‌ها و بایاس‌ها استفاده شود.

به طور خلاصه می‌توان گفت که دقت کلاس‌بندی شبکه عصبی به تنظیم صحیح وزن‌های سیناپسی شبکه مربوط است. بر این اساس و برای بهبود دقت کلاس‌بندی، از الگوریتم زنبورعسل برای آموزش شبکه عصبی استفاده کرده‌ایم. شبکه عصبی ۴ لایه معرفی شده در شکل (۲)، سیگنال دریافتی GNSS را در ۴ کلاس (۱) بدون تداخل، (۲) چندمسیری، (۳) جمینگ و (۴) فریب دسته‌بندی می‌کند. نورون‌های مصنوعی هر لایه، توسط سیناپس‌ها به نورون‌های لایه‌های قبل و بعد خود متصل هستند. هر کدام از این اتصالات وزنی دارد که مقدار آن، توسط الگوریتم تکاملی ABC تعیین می‌شود. در واقع، الگوریتم تکاملی در نقش الگوریتم یادگیری شبکه عصبی، به تدریج به روز خواهند شد. خروجی وزن‌دار هر نرون از لایه‌های مخفی و لایه خروجی، از یک تابع فعال‌ساز استخراج شده است. این توابع که بر روی نرون‌های شکل (۲) با نام‌های φ، ψ و f مشخص شده‌اند، مطابق روابط (۱۰) تا (۱۲) تعریف می‌شوند.

$$\varphi(x) = xe^{-\frac{1}{2}x^2} \quad (10)$$

$$\psi(x) = \frac{1}{1+e^{-x}} \quad (11)$$

$$f(y_1.y_2.y_3.y_4) = \begin{cases} 1 & ;if\ \max(y_1.y_2.y_3.y_4) = y_1 \\ 2 & ;if\ \max(y_1.y_2.y_3.y_4) = y_2 \\ 3 & ;if\ \max(y_1.y_2.y_3.y_4) = y_3 \\ 4 & ;if\ \max(y_1.y_2.y_3.y_4) = y_4 \end{cases} \quad (12)$$

در واقع، تابع شایستگی الگوریتم، تابع حداقل مربع خطا است. یعنی هر چه تفاوت بین مقادیر واقعی و مقادیر تخمینی یک کلاس‌بندی کمتر باشد، مطلوب‌تر است. برای محاسبه خطا از رابطه (۱۳) استفاده می‌شود.

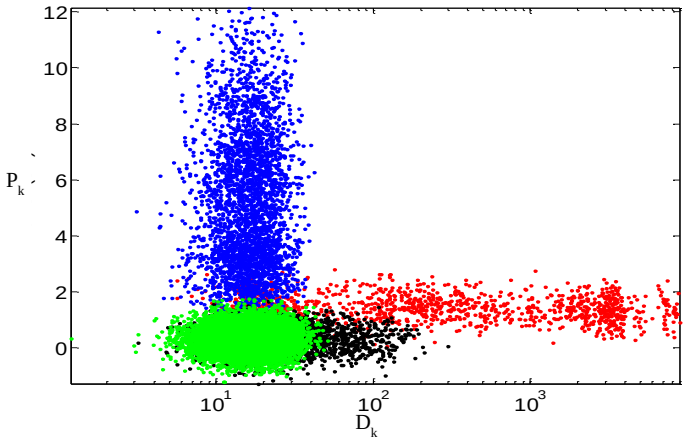
$$MSE = \sqrt{\sum_{k-1}^{n}(Y_{d_k} - Y_{c_k})^2} \quad (13)$$

بنابراین، هدف از اجرای الگوریتم زنبورعسل، یافتن بردار وزنی است که مجموع مربعات خطا را برای شبکه عصبی به حداقل برساند. با همگرایی الگوریتم زنبورعسل، وزن‌های بهینه شبکه عصبی به دست می‌آیند و می‌توان از این وزن‌ها برای شبکه‌ای با ظرفیت کلاس‌بندی سیگنال‌های GNSS دریافت شده، استفاده نمود.

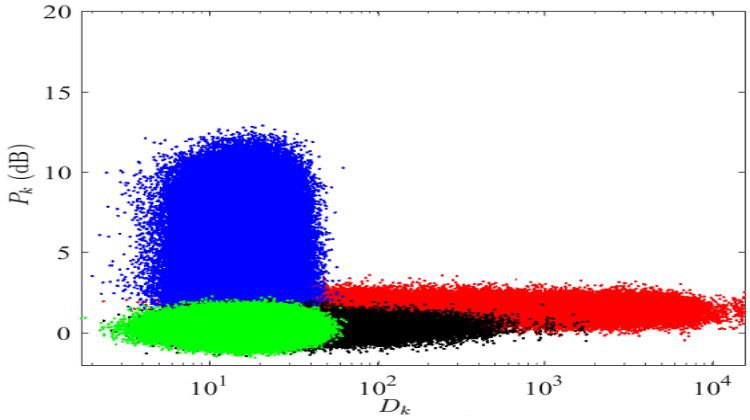
۴. نتایج

پس از شبیه‌سازی الگوریتم دسته‌بندی کننده، مدل پیشنهادی توسط داده‌های آزمایشگاهی ارائه شده توسط مرجع [۱۸] تحت آزمون قرار گرفت. در شکل (۳)، این مجموعه داده بر اساس دو مشخصه توان و میزان اعوجاج سیگنال ورودی ترسیم شده است. شکل (۴) نمایش همین مجموعه داده را که توسط مرجع [۱۸] گزارش شده است، نشان می‌دهد.

[1] Scott Bees



شکل ۳ : نمایش داده‌ها بر اساس اندازه‌گیری‌های اعوجاج تابع همبستگی D_k و توان دریافتی P_k.



شکل ۴ : نمایش مجموعه داده‌ها گزارش شده در مرجع [۱۸].

مجموعه داده مورد استفاده شامل ۲۴۰۰۰۰ داده است که تعداد آن‌ها در کلاس‌های مختلف، برابر می‌باشد. در شکل‌های (۳) و (۴) رنگ سبز نشان‌دهنده‌ی سیگنال‌های بدون اختلال است. در سیگنال بدون اختلال، مقادیر D_k کوچک است، زیرا فقط نویز حرارتی وجود دارد. رنگ سیاه نشان دهنده‌ی داده‌های تحت چندمسیری می‌باشد. در این موارد، D_k نسبت به موارد بدون اختلال، مقادیر بیشتری دارد. رنگ قرمز سیگنال‌های تحت فریب را نشان می‌دهد. در این سیگنال‌ها، محدوده‌ی D_k با چندمسیری هم‌پوشانی دارد، اما دامنه وسیع‌تری را نشان می‌دهد. رنگ آبی سیگنال‌های تحت جمینگ را نشان می‌دهد. D_k تقریباً از اعوجاج سیگنال‌های بدون اختلال قابل تشخیص نیست، زیرا جمینگ تأثیر کمی بر تابع همبستگی دارد [۱۸و۱۲]، اما توان دریافتی در این مورد بسیار بیشتر می‌باشد.

در اینجا، نتایج دسته‌بندی سیگنال‌های GNSS در چهار دسته بدون تداخل، تداخل چندمسیری، فریب و جمینگ بررسی شده و نتایج حاصله با نتایج گزارش شده در مرجع [۱۱] و [۱۸] مقایسه می‌شوند. نتایج شبیه‌سازی روش پیشنهادی به شرح جدول (۱) است. جداول (۲) و (۳) به‌ترتیب نتایج گزارش شده در مراجع [۱۸] و [۱۱] را نمایش می‌دهند.

جدول ۱: نتایج طبقه‌بندی اختلال با بکارگیری روش پیشنهادی.

	حالت واقعی			
تصمیم‌گیری	H0	H1	H2	H3
H0	۰/۲۹۲۶	۰/۱۴۹۹	۰/۰۳۳۱	۰/۰۱۴۹

H1	۰/۷۰۰۸	۰/۶۹۱۱	۰/۰۲۸۶	۰/۰۰۲۸
H2	۰/۰۰۰۵	۰/۱۵۵۶	۰/۸۹۷۱	۰/۰۰۱۶
H3	۰/۰۰۶۱	۰/۰۰۳۴	۰/۰۴۱۲	۰/۹۸۰۷

جدول ۲: نتایج طبقه‌بندی اختلال گزارش شده در مرجع [۱۸].

تصمیم‌گیری	حالت واقعی			
	H0	H1	H2	H3
H0	۰/۹۹۴۷	۰/۹۰۸۳	۰/۰۶۷۰	۰/۰۰۳۹
H1	۰	۰/۰۶۹۸	۰/۰۱۱۷	۰
H2	۰/۰۰۴۳	۰/۰۲۱۴	۰/۸۴۶۳	۰/۰۱۵۵
H3	۰/۰۰۱۰	۰/۰۰۰۵	۰/۰۷۵۰	۰/۹۸۰۶

جدول ۳: نتایج طبقه‌بندی اختلال گزارش شده در مرجع [۱۱].

تصمیم‌گیری	حالت واقعی			
	H0	H1	H2	H3
H0	۰/۸۷۴۵۰	۰/۵۳۴۳۳	۰۴۹۸۲/۰	۰۱۰۲۲/۰
H1	۰/۰۹۸۷۳	۰/۴۰۹۷۵	۰/۰۷۷۶۳	۰/۰۰۰۴۶
H2	۰	۰/۰۴۱۳۱	۰/۸۱۹۴۶	۰
H3	۰/۰۲۶۷۶	۰۱۴۵۸/۰	۰/۰۵۳۰۷	۰/۹۸۹۳۱

در این جداول، H0، H1، H2 و H3 به ترتیب داده‌ها را در دسته‌های بدون اختلال، چند مسیری، فریب و جمینگ نشان می‌دهند. همان‌طور که مشاهده می‌شود روش پیشنهادی در تشخیص چندمسیری نسب به روش مرجع [۱۸]، ۶۲.۱۳ درصد و نسبت به مرجع [۱۱]، ۲۸.۱۳ درصد بهبود داشته است. این روش در تشخیص جمینگ نسبت به مرجع [۱۸]، ۱ درصد عملکرد بهتری داشته است و نیز در تشخیص فریب که به طور خاص مدنظر این مقاله می‌باشد، بهبود ۵.۰۸ درصدی نسبت به مرجع [۱۸] و بهبود ۷.۷۷ درصدی نسبت به مرجع [۱۱] حاصل شده است. میانگین دقت آشکارسازی روش پیشنهادی در انواع اختلال ۷۱.۵۳ درصد می‌باشد.

۵. نتیجه‌گیری

در این مقاله، برای دسته‌بندی و تشخیص انواع تداخل GNSS دریافت شده در گیرنده‌های GNSS، از روش جدیدی بهره گرفته شد. در این روش، دسته‌بندی مبتنی بر شبکه‌های عصبی مصنوعی ارائه گردید و برای دسته‌بندی دقیق‌تر، شبکه عصبی توسط الگوریتم تکاملی زنبور عسل تعلیم داده شد. در واقع، از آنجا که اختلال‌های مورد نظر به صورت خطی قابل جداسازی نیستند، از شبکه مصنوعی بهره گرفته شده تا امکان دسته‌بندی دقیق‌تر به صورت غیرخطی وجود داشته باشد. از طرفی دیگر، عملکرد مناسب شبکه‌های عصبی منوط بر وزن‌دهی مناسب به سیناپس‌ها می‌باشد. به همین دلیل، برای تعیین مقادیر این وزن‌ها، از الگوریتم تکاملی زنبور عسل استفاده گردید. روش به‌کار برده شده در این مقاله، توانست به میانگین دقت آشکارسازی اختلال ۷۱.۵۳ دست یابد.

۶. مراجع

[۱] سید محمدرضا موسوی میرکلائی، "پردازش داده‌ها در گیرنده تک فرکانسه GPS"، انتشارات دانشگاه علم و صنعت ایران، ۱۳۹۰.

[۲] سید محمدرضا موسوی میرکلائی، مریم معاضدی، محمدجواد رضایی و امیر طباطبایی،"مقابله با اختلال در گیرنده های تک فرکانسه GPS"، انتشارات دانشگاه علم و صنعت ایران، ۱۳۹۴.

[3] 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, Jun. 2016.

[4] M. Bakula, P. Przestrzelski, and R. Kazmierczak, "Reliable Technology of Centimeter GPS/GLONASS Surveying in Forest Environments", IEEE Transactions on Geoscience and Remote Sensing, Vol.53, No.2, pp.1029-1035, 2015.

[5] T.E. Humphreys, J.A. Bhatti, and B.M. Ledvina, "The GPS Assimilator: a Method for Upgrading Existing GPS User Equipment to Improve Accuracy, Robustness, and Resistance to Spoofing," In Proceedings of the 23rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2010), Portland, OR, pp. 1942-1952, September 24, 2010.

[6] C. Sun, J.W. Cheong, A.G. Dempster, L. Demicheli, E. Cetin, H. Zhao, and W. Feng "Moving Variance-based Signal Quality Monitoring Method for Spoofing Detection," GPS Solutions, vol. 22, no. 3, pp. 1-13, 2018.

[7] J. S. Warner, R. G. Johnston, "GPS Spoofing Countermeasures," Homeland Security Journal, vol. 25, PP.19-27, 2003.

[8] C. Tanil, S. Khanafseh, M. Joerger, and B. Pervan, "Kalman Filter-Based Innovation Monitor to Detect GNSS Spoofers Capable of Tracking Aircraft Position," 2016 IEEE/ION Position, Location and Navigation Symposium (PLANS), pp. 1027-1034, 2016.

[9] B. Kujur, S. Khanafseh, and B. Pervan, "Detecting GNSS Spoofing of ADS-B Equipped Aircraft Using INS," 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS), pp. 548-554, 2020.

[10] P. B. Darian, H. Li, P. Wu, and P. Closas, "Deep Neural Network Approach to Detect GNSS Spoofing Attacks," Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020), pp. 3241-3252, 2020.

[11] 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.

[12] 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 and Electronic Systems, vol. 54, no. 2, pp. 739-754, 2017.

[13] 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," International Journal of Wireless Information Networks, vol. 25, no. 4, pp. 449-460, 2018.

[14] M. Mosavi and M. Azarbad, "Multipath Error Mitigation based on Wavelet Transform in L1 GPS Receivers for Kinematic Applications," AEU-International Journal of Electronics and Communications, vol. 67, no. 10, pp. 875-884, 2013.

[15] A. Baziar, M. Moazedi, and M. R. Mosavi, "Analysis of Single Frequency GPS Receiver under Delay and Combining Spoofing Algorithm," Wireless Personal Communications, vol. 83, no. 3, pp. 1955-1970, 2015.

[16] M. Moazedi, M. Mosavi, and A. Sadr, "Real-Time Interference Detection and Mitigation in Robust Tracking Loop of GPS Receiver," Analog Integrated Circuits and Signal Processing, vol. 95, no. 1, pp. 93-113, 2018.

[17] 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," The Journal of Navigation, vol. 71, no. 1, pp. 169-188, 2018.

[18] J. N. Gross, C. Kilic, and T. E. Humphreys, "Maximum-Likelihood Power-Distortion Monitoring for GNSS Signal Authentication", IEEE Transactions on Aerospace and Electronic Systems, vol. 55 , no. 1, pp. 469-475, 2019.

[19] A. Broumandan, A. Jafarnia-Jahromi, S. Daneshmand, and G. Lachapelle, "Effect of Tracking Parameters on GNSS Receivers Vulnerability to Spoofing Attack," in Proceedings of the 29th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2016), pp. 3033-3043, 2016.

[20] A. Broumandan, A. Jafarnia-Jahromi, and G. Lachapelle, "Spoofing Detection, Classification and Cancelation (SDCC) Receiver Architecture for a Moving GNSS Receiver", Gps Solutions, vol.19, no.3, pp.475-487, 2015.

[21] A. Broumandan, A. Jafarnia-Jahromi, G. Lachapelle, and R. T. Ioannides, "An Approach to Discriminate GNSS Spoofing from Multipath Fading," in 2016 8th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), pp. 1-10, 2016.

[22] D. Karaboga and B. Basturk, "Artificial Bee Colony (ABC) Optimization Algorithm for Solving Constrained Optimization Problems," in International fuzzy systems association world congress, Springer, pp. 789-798, 2007.