Scientific Journal of Electronical & Cyber Defence
Vol. 11, No. 1, Spring 2023, Serial No. 41

Reducing the Effects of Deception Attack on GPS Receivers of Phasor Measurement Units using Neural Networks

A. Tavassoli, N.Orouji, M. R. Moosavi*

* Professor, Faculty of Electrical Engineering, Iran University of Science and Technology, Tehran, Iran

(Received: 08/08/2021, Accepted: 06/02/2022)

ABSTRACT

Accurate timing is one of the key features of the Global Positioning System (GPS), which is employed in many critical infrastructures. Any imprecise time measurement in GPS-based structures, such as smart power grids, and Phasor Measurement Units (PMUs), can lead to disastrous results. The vulnerability of the stationary GPS receivers to the Time Synchronization Attacks (TSAs) jeopardizes the GPS timing precision and trust level. In this paper, the PMU receiver clock deviation monitoring method is used. In this method, a deception and fraud reduction algorithm is presented based on clock deviation observations. A multi-layer perceptron neural network is trained to track clock behavior information behavior and maintain a valid trend under time-synchronization attack conditions that can dramatically mimic clock deviation. Finally, the results were compared with a strong and low-memory RE estimator, which is one of the most recent methods of counteracting TSA, as well as an extended Kalman filter and a Luenberger observer. This indicates the good performance of the proposed method.

Keywords: Phasor Mesurement Units, Spoofing Attacks, Time Synchronization Attacks, Neural Network, Global Positioning System.

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

نشریه علمی "پدافند الکترونیکی و سایبری"
سال یازدهم، شماره ۱، بهار ۱۴۰۲، ص ۹۷-۱۰۵

علمی – پژوهشی

کاهش اثرات حمله فریب در گیرنده‌های GPS واحدهای اندازه‌گیری فازور با استفاده از شبکه‌های عصبی

افسانه سادات توسلی[۱]، نیلوفر اروجی[۲]، سید محمدرضا موسوی میرکلائی[۳*]

۱- دانشجوی کارشناسی ارشد، ۲- دکترا، ۳- استاد، دانشکده برق، دانشگاه علم و صنعت ایران، تهران، ایران

(دریافت: ۱۴۰۱/۰۱/۲۳، پذیرش: ۱۴۰۱/۰۴/۰۴)

چکیده

زمان‌سنجی دقیق یکی از ویژگی‌های کلیدی سامانه موقعیت‌یاب جهانی (GPS) است که در زیرساخت‌های بسیار مهمی از جمله واحدهای اندازه‌گیری فازور (PMU) مورد استفاده قرار می‌گیرد. هر برچسب زمانی نادقیق در شبکه‌های هوشمند قدرت می‌تواند منجر به اتفاقات فاجعه باری شود. آسیب‌پذیری گیرنده‌های GPS ثابت که در PMUها مستقر هستند، نسبت به حمله همگام‌سازی زمانی (TSA) باعث کاهش سطح اعتماد به زمان ارائه شده توسط این گیرنده‌ها می‌شود. در این مقاله، از روش نظارت بر انحراف ساعت گیرنده PMU استفاده شده است. در این روش، یک الگوریتم کاهش اثرات فریب بر اساس مشاهدات انحراف ساعت ارائه می‌شود. یک شبکه عصبی چندلایه (MLP) برای دنبال‌کردن رفتار اطلاعات انحراف ساعت و حفظ روند معتبر تحت شرایط حمله همگام‌سازی زمان آموزش داده شده است که می‌تواند به طرز چشمگیری روند انحراف ساعت را تقلید کند. در نهایت، نتایج حاصل با برآوردگر قوی و کم‌حافظه RE که یکی از به‌روزترین روش‌های مقابله با TSA است و همچنین فیلتر توسعه‌یافته کالمن (EKF) و ناظر LO، مقایسه شد که RMSE روش پیشنهادی بهبود حداقل شش برابری در تشخیص و اصلاح حمله را دارد که این نشان‌دهنده عملکرد خوب روش پیشنهادی است.

کلیدواژه‌ها: واحدهای اندازه‌گیری فازور، حملات فریب، حمله همگام‌سازی زمانی، شبکه عصبی، سامانه موقعیت‌یاب جهانی.

۱- مقدمه

طی چند سال اخیر، تغییرات قابل‌توجهی در شبکه‌های توزیع توان، به دلایل متعدد فنی و اقتصادی رخ داده است که عمدتاً می‌توان به آزادسازی بازار انرژی و افزایش پخش نیروگاه‌های تولید پراکنده[۱] اشاره نمود. تأثیر این تغییرات، بر لزوم مطالعه در مورد مسائل جدید مدیریتی، کنترل و پایش دلالت می‌کند [۱].

واحد اندازه‌گیری فازور[۲] PMU، ولتاژ و جریان فازور را اندازه‌گیری می‌کند و نقش مهمی در شبکه‌های قدرت دارد. اندازه‌گیری فازور همگام شده از واحد اندازه‌گیری فازور برای نظارت و کنترل بلادرنگ ارزشمند است [۲]. سامانه موقعیت‌یاب جهانی[۳] GPS که یک سامانه مبتنی بر ماهواره می‌باشد، منبع اصلی هماهنگ‌سازی است [۳]. GPS به طور گسترده‌ای به‌منظور موقعیت‌یابی و زمان‌سنجی مورد استفاده قرار می‌گیرد [۴]. سیگنال‌های GPS برای تعیین موقعیت، سرعت و زمان یا راه‌حل PVT[۴] گیرنده مورد استفاده قرار می‌گیرند. دقت موقعیت در شرایط آسمان باز برای گوشی‌های هوشمند حدود ۴/۹ متر است [۵]. اگرچه بسته به شرایط محیطی، دقت در شرایط چالش‌برانگیزتر کاهش می‌یابد. طبق مطالعات انجام شده در [۶]، دقت اندازه‌گیری‌های زمانی گیرنده‌های GPS به ترتیب نانوثانیه است. امنیت سایبری، مسئله‌ای مهم برای قابلیت اطمینان شبکه‌های قدرت محسوب می‌شود [۷]. استفاده گسترده از فناوری‌های اطلاعات و ارتباطی پیشرفته، فرصت‌هایی را برای حملات فریبGPS علیه واحد اندازه‌گیری فازور ایجاد می‌کند که به سیگنال‌های زمان‌بندی GPS شخصی بستگی دارد. حملات فریب سامانه موقعیت‌یاب جهانی با معرفی سیگنال‌های فریب GPS، هم‌زمان‌سازی دستگاه‌های اندازه‌گیری را به خطر می‌اندازد [۸].

در شبکه‌های برق، PMUها به موقعیت‌یابی جهانی تکیه می‌کنند. سامانه GPS برای تولید زمان دقیق اندازه‌گیری است. اطمینان از یک‌پارچگی داده‌های فازور هم‌زمان شده وابسته به زمان GPS است. قدرت سیگنال‌های GPS حاصل از ماهواره‌ها در سطح زمین بسیار ضعیف است. پخش ضعیف این سیگنال‌ها باعث می‌شود که توسط سیگنال‌هایی با همان باند فرکانس ردیابی شوند و ازآنجاکه ساختار سیگنال‌های GPS موجود است، تقلید و فریب آن‌ها آسان می‌گردد.

PMUها مجهز به سامانه امنیت سطح بالایی هستند و تقریباً از حملات یک‌پارچگی داده‌های معمولی مانند تزریق کاذب

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

[1] Distributed Generation
[2] Phasor Measurement Units (PMU)
[3] Global Positioning System
[4] Position, Velocity and Time

ناشر: دانشگاه جامع امام حسین (ع)

داده‌ها مصون هستند. بااین‌وجود، وابستگی PMUها به سیگنال ضعیف GPS آن‌ها را مستعد حمله فریب سامانه موقعیت‌یاب جهانی GSA[1] می‌کند. حمله فریب GPS به داده‌های عمومی محدود است و فقط می‌تواند مرجع زمانی اندازه‌گیری PMU را مختل کند و با ارجاع زمان اشتباه به طور پی‌درپی باعث ایجاد خطا در زاویه فاز اندازه‌گیری حاصل از PMU شود [۲و۹].

حمله فریب به دلیل مخفیانه بودن، حمله‌ای ظریف‌تر نسبت به بلاکینگ یا جمینگ است و در دهه اخیر به‌عنوان خطرناک‌ترین دخالت عمدی در GPS شناخته شده است. هدف فریبنده وادارکردن گیرنده GPS به تولید راه‌حل ناوبری غلط است. گیرنده GPS که در معرض حمله فریب قرار دارد، دو مجموعه سیگنال اصلی و فریب را هم‌زمان دریافت می‌کند. سیگنال فریب به‌گونه‌ای طراحی می‌شود که بر سیگنال اصلی GPS غلبه نموده و کنترل گیرنده ناآگاه را در اختیار گیرد. حمله فریب و مقابله با آن می‌تواند در هریک از سطوح گیرنده از جمله بخش بیت داده، اکتساب، ردیابی، استخراج شبه‌فاصله و معادلات ناوبری انجام پذیرد [۱۰].

در ادامه، مقاله در پنج بخش به بحث دراین‌خصوص پرداخته می‌شود. در بخش ۲، به بررسی روش‌های مقابله با حمله فریب پرداخته می‌شود. در بخش ۳، اصول و سازوکار شبکه عصبی MLP برای کاهش فریب شرح داده می‌شود. بخش ۴، نحوه جمع‌آوری مجموعه داده عنوان شده است. در بخش ۵، نتایج پیاده‌سازی روش پیشنهادی بیان می‌شود و در قسمت پایانی نیز نتیجه‌گیری ارائه شده است.

۲- بررسی روش‌های مقابله با حمله فریب

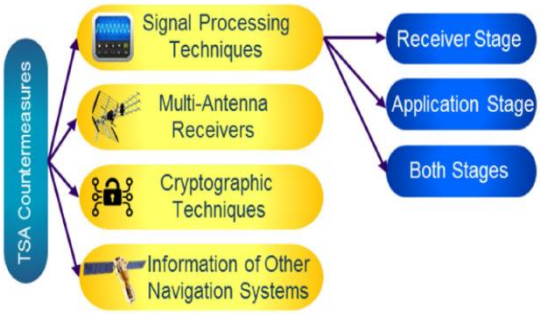
تعداد زیادی از اقدامات متقابل و روش‌های حفاظتی برای شناسایی یا کاهش اثرات TSA پیشنهاد شده‌اند که می‌توانند به چهار کلاس طبقه‌بندی شوند [۱۱].

دسته اول: شامل روش‌های پردازش سیگنال است که ویژگی‌های سیگنال را برای هر گونه ناهنجاری غیرمنتظره در کیفیت، قدرت یا هر پارامتر قابل‌مشاهده دیگری بررسی و تجزیه‌وتحلیل می‌کند [۱۲و۱۳].

دسته دوم: گیرنده‌های چندآنتنی و بازرسی‌های طیف رادیویی هستند و از زاویه ورود هر سیگنال برای تشخیص جهت منبع آن بهره‌برداری می‌کنند [۱۴].

دسته سوم: روش‌های رمزنگاری راه‌حل‌هایی را ارائه می‌کنند که بر ساختار سیگنال GPS نسل بعدی [۱۵] یا ارتباط بین سیگنال‌های نظامی و سیگنال‌های معتبر برای شناسایی تهاجم متکی است [۱۶].

دسته چهارم: همبستگی اطلاعات GPS را با سایر منابع زمانی مانند GLONASS[2] نشان می‌دهد [۱۷].



شکل (۱). دفاع در برابر TSAها به ۴ کلاس طبقه‌بندی می‌شوند [۱۸]

روش‌های رمزنگاری در برابر حملات فریب متوسط و پیشرفته مقاوم هستند. بااین‌حال، آن‌ها مستعد حملات ساده انگارانه مانند مکر کردن هستند]۱۵[. بنابراین، اکیداً پیشنهاد می‌شود از روش همراه با سایر راه‌حل‌های دفاعی برای دستیابی به حداکثر سطح حفاظت استفاده شود. تسهیلات رمزنگاری فقط بر روی سیگنال‌ها و سرویس‌های جدید GPS و سامانه گالیله در دسترس است که به طور گسترده مورد بهره‌برداری قرار نمی‌گیرد.

به‌عنوان یک مزیت، هیچ نیازی به تغییر پروتکل‌های سیگنال یا ماهواره‌ها برای اعتبارسنجی اطلاعات GPS توسط سایر GNSS[3] یا منابع داده وجود ندارد. بااین‌حال، اعتبارسنجی مبتنی بر شبکه، حجم عظیمی از ترافیک داده را از طریق شبکه ایجاد می‌کند و در برابر حملات سایبری آسیب‌پذیر است. علاوه بر این، تأیید اطلاعات با سایر سامانه‌های ماهواره‌ای نیاز به گیرنده‌های اضافی دارد که بسیار مقرون‌به‌صرفه نیست. مصونیت دفاع‌های چندآنتنی در برابر SDR[4] تولید شده حملات و مقاومت ذاتی آن‌ها در برابر فریب آن‌ها را به‌عنوان یک انتخاب قوی برای گیرنده‌های ایمن متمایز می‌کند. بااین‌حال، استفاده از گیرنده‌های چندآنتنی و تجزیه‌وتحلیل طیف رادیویی بسیار پرهزینه است.

اقدامات متقابل پردازش سیگنال را می‌توان با به‌روزرسانی سامانه عامل آن‌ها و تجهیز آن‌ها به جدیدترین روش‌های دفاعی روی گیرنده‌ها اعمال کرد. بااین‌حال، آن‌ها به هیچ‌گونه تغییر سخت‌افزاری یا تنظیم در ساختار سیگنال نیاز ندارند. در این تحقیق، یک الگوریتم کاهش اثرات فریب بر اساس مشاهدات انحراف ساعت ارائه می‌دهد که در دسته‌بندی بیان شده قرار دارد. یک شبکه عصبی چندلایه (MLP)[5] برای دنبال‌کردن آموزش

[1] GPS Spoofing Attack (GSA)

[2] Global Orbiting Navigation Satellite System
[3] Global Navigation Satellite System
[4] Software-Defined Radio
[5] Multi-Layer Perceptron Neural Network

داده شده است. رفتار اطلاعات انحراف ساعت و حفظ روند معتبر تحت شرایط TSA[1] شبکه انحرافات معرفی شده در اطلاعات را کاهش می‌دهد و دقت قابل قبولی را برای PMUها، دکل‌های ارتباطی و سایر برنامه‌های کاربردی وابسته به زمان نشان می‌دهد.

۳- اصول و سازوکار شبکه عصبی MLP برای کاهش فریب

شبکه‌های پیش‌رونده چندلایه یکی از دسته‌بندی‌های بسیار محبوب شبکه‌های عصبی را تشکیل می‌دهند. آن‌ها را روبه‌جلو می‌نامند، زیرا سیگنال ورودی از طریق ساختار منتشر می‌شود که می‌تواند یک یا چندلایه پنهان در جهت روبه‌جلو داشته باشد. معمولاً این شبکه‌ها که از آن‌ها به‌عنوان شبکه عصبی MLP یاد می‌شود، می‌توانند پس از دریافت آموزش مناسب، راه‌حل‌هایی برای طیف متنوعی از مشکلات پیچیده ارائه دهند. الگوریتم پس انتشار خطا (BP)[2] برای آموزش شبکه عصبی MLP در یک روال نظارت شده استفاده می‌شود و از دو بخش تشکیل شده است: بخش روبه‌جلو و بخش روبه‌عقب. در طول عبور به جلو، پاسخ هر لایه به سیگنال ورودی دقیقاً بررسی می‌شود، درحالی‌که وزن شبکه ثابت می‌ماند. در گذر به عقب، خطا با اختلاف بین خروجی حاصل و مقدار مورد نظر به دست می‌آید. این خطا برای تنظیم وزن‌ها و آستانه‌ها مورد استفاده قرار می‌گیرد. دستیابی به حداقل خطای ممکن با تعداد معقول تکرار، هدف نهایی فرایند یادگیری است [۱۸].

۳-۱- آموزش شبکه بر اساس الگوریتم BP

به‌عنوان‌مثال، شبکه‌ای با گره‌های p در لایه ورودی، نورون‌های q در لایه پنهان و نورون‌های r در لایه خروجی با N(p,q,r) که در شکل (۲) نشان داده شده است پارامترهای شبکه در روابط (۱) تا (۶) تعریف می‌شوند [۱۸]:

$$\boldsymbol{X}(k) = [x_1(k), x_2(k), \dots, x_p(k)] \quad (۱)$$

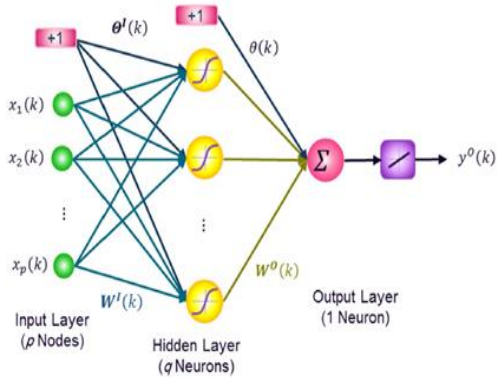
$$\boldsymbol{W}^I(k) = \begin{bmatrix} w^I_{11}(k) & \cdots & w^I_{1q}(k) \\ \vdots & \ddots & \vdots \\ w^I_{p1}(k) & \cdots & w^I_{pq}(k) \end{bmatrix} \quad (۲)$$

$$\boldsymbol{\Theta}^I(k) = [\theta_1(k), \theta_2(k), \dots, \theta_q(k)] \quad (۳)$$

$$\boldsymbol{W^O}(k) = \left[w^O_1(k), w^O_2(k), \dots, w^O_q(k)\right] \quad (۴)$$

$$\boldsymbol{V^I}(k) = [v^I_1(k), v^I_2(k), \dots, v^I_q(k)] \quad (۵)$$

$$\boldsymbol{Y^I}(k) = [y^I_1(k), y^I_2(k), \dots, y^I_q(k)] \quad (۶)$$



شکل (۲). ساختار عمومی شبکه N(p,q,1) [۱۸]

که در آن، X(k) برابر p × 1 بردار ورودی است، $\boldsymbol{W}^I(k)$ ماتریس وزن‌های ورودی با اندازه q × p است، $\boldsymbol{\Theta}^I(k)$ برابر q × 1بردار آستانه ورودی را بیان می‌کند، $\boldsymbol{W}^O(k)$ با اندازه q × 1 وزن خروجی را نشان می‌دهد و θ(k) آستانه خروجی است. تحریک نورون‌ها در لایه پنهان با بردار $\boldsymbol{V}^I(k)$ با اندازه q × 1 و تحریک نورون لایه خروجی با $\boldsymbol{V}^O(k)$ نشان داده می‌شود. خروجی نورون‌های لایه پنهان با بردار $\boldsymbol{Y}^I(k)$ و اندازه q × 1 است. خروجی نهایی شبکه و مقدار مورد نظر به ترتیب با $y^o(k)$و d(k) نشان داده می‌شوند. تابع فعال‌سازی هر نورون یک تابع سیگموئید است. تابع و مشتق آن در (۷) و (۸) ارائه می‌شود که در آن $\boldsymbol{\sigma'}(x)$ نشان‌دهنده مشتق سیگموئید است.

$$\sigma(x) = \frac{2}{1+e^{-2x}} - 1 \quad (۷)$$

$$\boldsymbol{\sigma'}(x) = \sigma(x)(1-\sigma(x)) \quad (۸)$$

روند تعلیم شبکه عصبی با الگوریتم پس انتشار به شرح زیر است:

گام اول- مقداردهی اولیه به بردار وزن‌ها: تمامی وزن‌ها و حد آستانه‌ها با اعداد تصادفی کوچک که توزیع یکنواخت دارند، مقداردهی می‌شوند.

گام دوم- محاسبات روبه‌جلو:

$$v_j(n) = \sum_{i=1}^{i=p} w_{ji}(n)x_i(n) + \theta_j(n) \quad (۹)$$

$$y_j(n) = \sigma\left(v_j(n)\right) = \frac{2}{1+e^{-2v_j}} - 1 \quad (۱۰)$$

$$o(n) = \sum_{j=1}^{j=q} w_j(n)y_j(n) + \theta(n) \quad (۱۱)$$

در این روابط، $v_j(n)$ و $y_j(n)$ به ترتیب مبین سیگنال فعال‌سازی و خروجی j امین نورون در لایه مخفی و در لحظه n هستند.

گام سوم- فرایند تعلیم: روش پس انتشار، برای کمینه‌کردن تابع

[1] Time Synchronization Attack
[2] Back Propagation

هزینه مربعات خطا به کار می‌رود [۱۹]:

$$E(n)=\frac{1}{2}e^2(n)=\frac{1}{2}[o(n)-d(n)]^2 \quad (۱۲)$$

که در آن، d(n) بیانگر خروجی مطلوب در لحظه n است. وزن بین j امین نورون مخفی و i امین نورون ورودی در هر لحظه مطابق رابطه (۱۳) تغییر می‌کند:

$$\Delta w_{ji}=-\eta\frac{\partial E}{\partial w_{ji}}=\eta e\frac{\partial o_j}{\partial y_j}\frac{\partial y_j}{\partial v_j}\frac{\partial v_j}{\partial w_{ji}}= \eta e w_j \acute{\sigma}(v_j)x_i \quad (۱۳)$$

در اینجا، η ضریب یادگیری است که برای کنترل‌کردن سرعت همگرایی الگوریتم به کار می‌رود. وزن بین j امین نورون مخفی و نورون خروجی نیز به همین ترتیب طبق رابطه (۱۴) محاسبه می‌گردد:

$$w_{ji}=-\eta\frac{\partial E}{\partial w_j}=\eta e\frac{\partial o}{\partial w_j}=\eta e y_j \quad (۱۴)$$

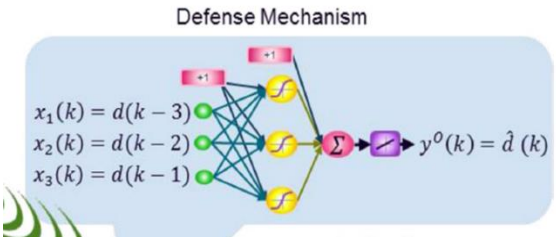
به‌هنگام‌سازی حد آستانه‌ها به طور مشابه با مشتق‌گیری از تابع هزینه حاصل می‌شود:

$$\Delta\theta_j=-\eta\frac{\partial E}{\partial \theta_j}=\eta e\frac{\partial o_j}{\partial y_j}\frac{\partial y_j}{\partial v_j}\frac{\partial v_j}{\partial \theta_j}= \eta e w_j \acute{\sigma}(v_j) \quad (۱۵)$$

$$\square\square=-\eta\frac{\partial E}{\partial \theta}=\eta e\frac{\partial o}{\partial \theta}=\eta e \quad (۱۶)$$

گام چهارم- تکرار: روابط (۹) تا (۱۶) تکرار می‌شوند تا معیارهای از پیش تعیین شده برای پایان این روند، برآورده شوند. به‌عنوان‌مثال، اگر دفعات تکرار الگوریتم به بیشترین تعداد دوره‌ها برسد و یا مقدار خطا از حد تعیین شده کمتر شود، روند تکرار الگوریتم متوقف می‌شود.

هدف نهایی TSA تأثیرگذاری بر اطلاعات انحراف ساعت و ایجاد خطا در مهرهای زمانی است. بنابراین، یک شبکه عصبی MLP می‌تواند کمک بزرگی برای تخمین روند واقعی انحراف ساعت و حفظ گیرنده از پیامدهای فاجعه‌بار TSA باشد. استفاده کارآمد از شبکه عصبی MLP مستلزم انتخاب مناسب ویژگی‌های شبکه، مانند نوع معماری، تعداد لایه‌ها و نورون‌ها و الگوریتم آموزشی است. به‌طورکلی، تصمیمات بهینه از طریق روش آزمون‌وخطا ساخته می‌شوند [۲۰]. در شبکه پیشنهادی، از نمونه‌های قبلی انحراف ساعت به‌عنوان ورودی برای پیش‌بینی شبکه آینده استفاده می‌شود. همان‌طور که در شکل (۳) نشان داده شده است، ورودی‌های شبکه سه نمونه قبلی از اطلاعات انحراف ساعت به ترتیب d(k − 1)، d(k − 2) و d(k − 3) هستند. در نتیجه، خروجی تخمین انحراف ساعت است که $\hat{d}(k)$ در لحظه کنونی k نشان داده می‌شود.



شکل(۳). سازوکار دفاعی [۱۸]

در این مقاله، یک شبکه عصبی MLP سه لایه پیشنهاد شده و توسط الگوریتم خطای BP به‌صورت نظارت شده آموزش داده شده است. این تصمیم با درنظرگرفتن مبادله بین پیچیدگی محاسباتی و میانگین مربعات خطا (MSE)[1] فرایند آموزش هدایت می‌شود. وزن‌ها و آستانه‌های پیچیدگی شبکه ترتیب یک شبکه عمومی N(p,q,1) به این صورت است که با ابعاد شبکه ارتباط مستقیم دارد، در رابطه (۱۷) تعریف می‌شود:

$$\text{Network Order} = (p + 2)q + 1 \quad (۱۷)$$

فرایند آموزش شبکه توسط ۷۰ درصد داده‌ها انجام می‌شود، درحالی‌که عملکرد آن توسط ۱۵ درصد از نمونه‌ها تأیید می‌شود و ۱۵ درصد دیگر از داده‌ها برای آزمایش کارایی شبکه استفاده می‌شود. این شبکه با الگوریتم لونبرگ-مارکوارت[2] آموزش داده شده است که پاسخ قابل‌قبول و نرخ همگرایی سریع را ارائه می‌دهد. مطابق با رابطه (۱۷) شبکه دارای درجه ۳۱ است که نشان‌دهنده میزان معقولی از پیچیدگی است.

۴- جمع‌آوری داده

مجموعه داده استاندارد مورد استفاده در این پروژه از طریق درگاه داده IEEE تهیه شده است که مجموعه داده‌های Open Access را در دسترس همگان قرار می‌دهد. مجموعه داده GNSS با استفاده از یک LabSat[3] نسخه ۳ در داخل گلخانه دانشگاه ویرجینیای غربی ایالات متحده آمریکا و دو ضبط خارجی نیز برای ارائه یک مرجع و مقایسه باکیفیت، سه داده خام (داده‌های درون فازی و چهارگانه با رادیو نرم‌افزاری و فایل‌های مشاهده‌ای)، ثبت شد.

مکان بیرونی باید مکانی ایدئال برای دریافت سیگنال ماهواره‌ای باشد و مکان داخلی یک اتاق گلخانه‌ای بود که در آن دید ماهواره‌ای محدود، مستعد تضعیف، انسداد و چندمسیره بود. این ضبط‌ها همگی ثابت هستند و با استفاده از LabSat نسخه ۳، یک شبیه‌ساز GNSS چند صورت فلکی که امکان ضبط و

[1] Mean Squared Error
[2] Levenberg–Marquardt Algorithm
[3] Laboratory Satellite

پخش مجدد سیگنال‌های واقعی GPS/GNSS را فراهم می‌کند، ساخته شده‌اند.

آنتنی که برای این کار استفاده می‌شود یک آنتن GPS/GNSS پچ L1 است. این ضبط‌ها در یک زمان از روز (ظهر) انجام شده‌اند، به‌طوری که برای همه مجموعه‌های داده سازگار و قابل مقایسه بوده و تقریباً ۱/۵ ساعت طول دارند. علاوه بر ضبط‌های خام، فایل‌های مشاهده RINEX پس از پردازش با نرم‌افزار GNSS-SDR و پخش داده‌ها در گیرنده Novatel OEM-638 برای هر مجموعه داده گنجانده شده است. راه‌حل‌های موقعیت پردازش شده به‌دست‌آمده با کتابخانه منبع‌باز RTKLIB نیز برای مرجع گنجانده شده‌اند.

این ضبط‌ها همچنین در یک گیرنده نرم‌افزاری (GNSS-SDR) با استفاده از فایل L1_E1.conf پخش شدند که به سیگنال‌های گالیله اجازه می‌دهد تا فایل‌های RINEX زیر را دریافت کنند. شایان ذکر است که این فایل‌ها RINEX و در قالب ۳/۰۲ هستند.

GSDR302c05.20O

GSDR315b49.20O

GSDR307x52.20O

GSDR309n41.20O

GSDR310p27.20O

سایر فایل‌های خروجی مفید توسط GNSS-SDR نیز در پوشه Run گنجانده شده است. RTKLIB فایل‌های خروجی RINEX از NovAtel و GNSS-SDR با استفاده از RTKLIB (Rtkpost) نسخه ۲,۴,۲ پردازش شدند. برای RTKLIB از تنظیمات زیر استفاده شد:

۱- حالت موقعیت/نوع راه‌حل: ppp سینماتیک
۲- نوع فیلتر ترکیبی
۳- تصحیح/پخش LC بدون Iono
۴- تصحیح تروپوسفر Saastamoinen
۵- پخش ماهواره‌ای Ephemeris/Clocks (از GPS و Galileo برای پخش فایل‌های Ephemeris استفاده شده و SP3 و CLK از CDDIS/IGS در نظر گرفته شده است).

فایل‌های ایستگاه و مدار بارگیری شده شامل CDDIS بوده که برای پردازش داده‌ها استفاده می‌شوند. Rtkpost راه‌حل‌های خود را در قالب فایل .pos و .stat خروجی می‌دهد. برای پردازش پس از راه‌حل‌های GNSS-SDR، فایل‌های خروجی GSDR#Month_#day و برای NovAtel NV#month_#day نامیده می‌شوند. در این پوشه، فایل‌های .mat برای هر روز برای NovAtel و GNSS-SDR نیز ضمیمه شده است. این فایل‌ها حاوی داده‌های استخراج شده از فایل‌های .pos و .stat هستند تا بتوان آن‌ها را در Matlab تجزیه‌وتحلیل کرد. ارقام خروجی از Rtkpost نیز گنجانده شده است.

مجموعه داده PVT که شامل ۵۲۷۰۶ نمونه از انحراف ساعت گیرنده‌های ثابت GPS که از خارج این گلخانه جمع‌آوری شده است و مطابق با صورت‌مسئله یعنی گیرنده ثابت در شبکه قدرت مورد استفاده قرار می‌گیرند. استفاده از متغیر Rx_time به‌عنوان انحراف ساعت مطابق با روشی که در [۲۱] عنوان شده است.

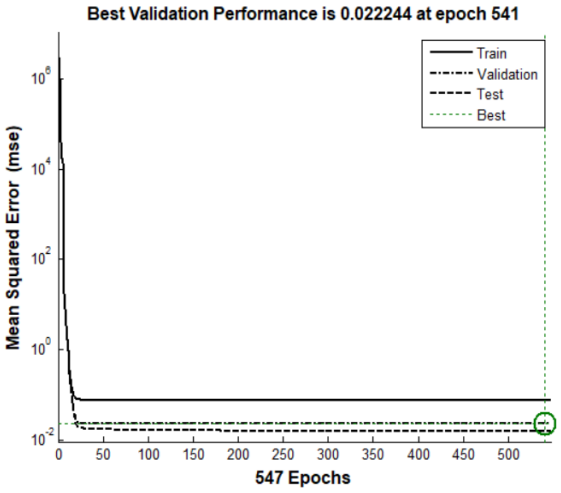
۵- نتایج پیاده‌سازی روش پیشنهادی

آزمایش‌های متعددی روی مجموعه داده با ۵۲۷۰۶ نمونه از انحراف ساعت که از طریق گیرنده‌های ثابت GPS که خارج گلخانه دانشگاه ویرجینیای غربی قرار گرفته، انجام گرفت. شبکه‌های عصبی MLP با تعداد سه، چهار و پنج ورودی و تعداد نورون‌های لایه مخفی بین ۲ تا ۲۰ متغیر بوده تا انتخاب بهینه تعیین شود. از تابع فعال‌سازی سیگموئید که در تخمین روند انحراف ساعت به‌خوبی عمل می‌کند، استفاده شده است.

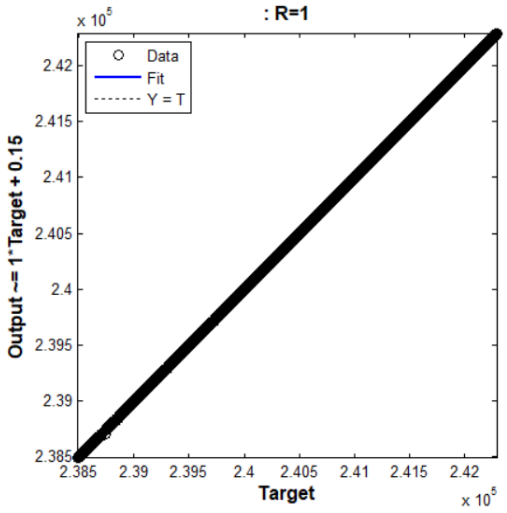
به طور خاص، شبکه‌هایی با چهار و پنج ورودی و تعداد ۱۰ تا ۲۰ نورون در لایه مخفی دارای نرخ همگرایی سریع‌تری هستند. مطابق با جدول (۱) و نیز اشکال (۴) تا (۶)، دراین‌بین شبکه عصبی چندلایه با چهار ورودی و پنج نورون در لایه مخفی (MLP(4.5.1))، دارای بهترین عملکرد در بین شبکه‌های آموزش‌دیده دیگر هم از لحاظ نرخ همگرایی و هم شاخص MSE است.

جدول (۱). شبکه عصبی MLP با ۴ ورودی و ۵ نورون لایه مخفی (s)

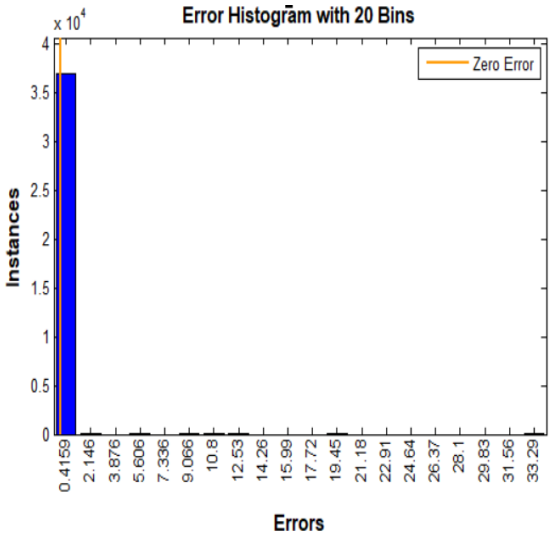
شبکه عصبی	MLP (4,5,1)
عملکرد کلی	۰/۰۵۸۵
عملکرد آموزش	۰/۷۵۵۰
عملکرد ارزیابی	۰/۰۲۲۲
عملکرد آزمون	۰/۰۱۵۳
MSE	۰/۰۲۲۲
دوره	۵۴۱



شکل (۴). فرایند یادگیری MLP (4,5,1) و MSE هر تکرار (m)



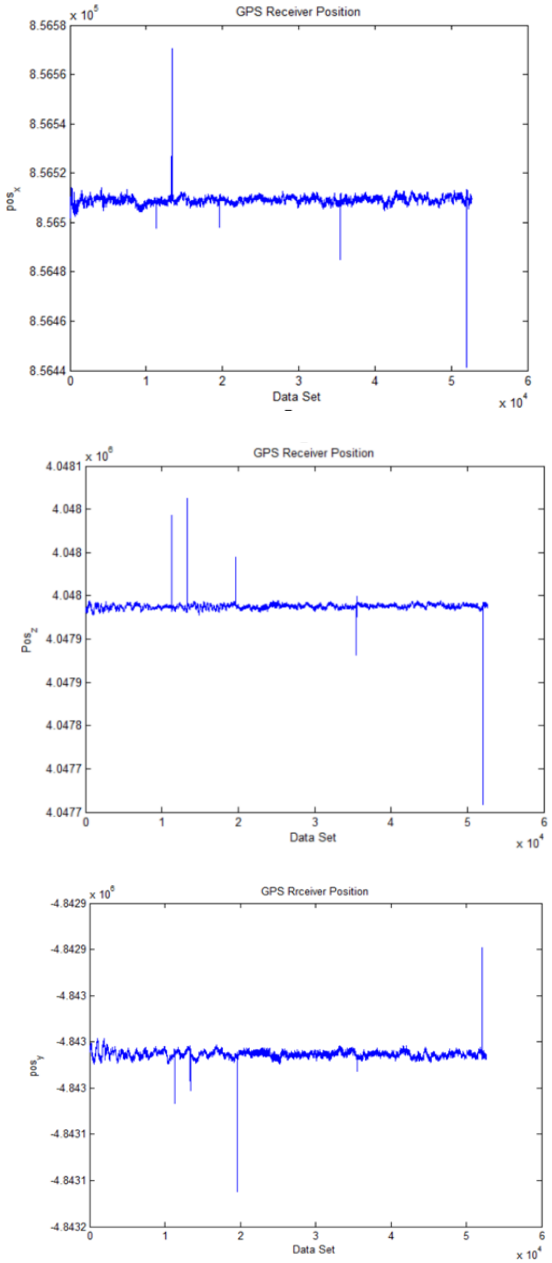
شکل (۵). رگرسیون



شکل(۶). هیستوگرام خطا

۵-۱- روش‌های پیکربندی و تخمین TSA

نوع اول TSA توسط یک سیگنال پله‌ای شکل با انحراف ۸۰۰۰ متر یا معادل زمان ۲۶٫۶۸ میکروثانیه پیکربندی می‌شود. حمله به طور ناگهانی به سیگنال در ۲۵۶ مین نمونه زمان روی مجموعه داده با طول ۲۰۰۰۰ نمونه اول این مجموعه که جمع‌آوری شده از خارج گلخانه دانشگاه ویرجینیای غربی که این داده‌ها، داده‌های گیرنده ثابت GPS در خارج از این گلخانه هستند، اضافه می‌شود. نوع دوم TSA یک سیگنالی است که به طور مداوم کاهش پیدا می‌کند. این نوع حمله تنها بر اطلاعات انحراف ساعت تأثیر می‌گذارد، درحالی‌که مکان گیرنده مطابق شکل (۷) ثابت باقی می‌ماند.



شکل (۷). موقعیت ثابت گیرنده GPS

حمله نوع دوم بر تمامی شبه‌فاصله‌های ماهواره‌های در دیدرس تأثیر می‌گذارد. بنابراین، تأثیر آن در گیرنده فقط بر اطلاعات زمانی بوده و مکان آن تغییری نمی‌کند. بر این اساس اگر گیرنده مجهز به سامانه نظارت بر مکان باشد، نمی‌تواند وقوع این حمله را تشخیص دهد و تنها راه شناسایی نظارت بر مؤلفه انحراف ساعت است. تأثیرات هر دو حمله بر مجموع داده‌ها تا آخرین نمونه باقی می‌ماند.

TSAها به همان روشی که در کار، لی و همکاران [۲۲] برای مقایسه منصفانه با شبکه عصبی MLP پیشنهادی که عنوان شده است، تولید می‌شوند. علاوه بر این، عملکرد شبکه عصبی MLP با فیلتر کالمن توسعه‌یافته (EKF)[1] و ناظر لونبرگ (LO)[2] به‌عنوان رویکردهای کلاسیک برای تخمین انحراف ساعت مقایسه می‌شود. برآوردگر ناوبری GPS باید موقعیت، تغییر ساعت و رانش ساعت را در برنامه‌های ثابت تخمین بزند. الگوریتم ناوبری اندازه‌گیری‌های خام گیرنده و موقعیت‌های ماهواره را برای تخمین وضعیت کاربر ادغام می‌کند. EKFها به طور گسترده در سامانه‌های مستقل مورد استفاده قرار می‌گیرند و مدل‌ها را با بهترین برآورد فعلی از وضعیت گیرنده خطی می‌کنند. علاوه بر این، LO یک سیستم خطی ثابت زمان است که قادر به حذف اختلالات نویز اندازه‌گیری‌ها است. EKF و LO هر دو روش‌های کلاسیک تخمین وضعیت گیرنده هستند که در برابر هر نوع حملات فریب مقاوم نیستند. شبکه عصبی MLP پیشنهادی در یک الگوریتم تشخیص مبتنی بر خطا مورد بهره‌برداری قرار گرفته است که می‌تواند نوع TSA را شناسایی کند. خطای تخمین شبکه به‌صورت رابطه (۱۸) تعریف می‌شود:

$$e_{est}(k) = d(k) - \hat{d}(k) \qquad (۱۸)$$

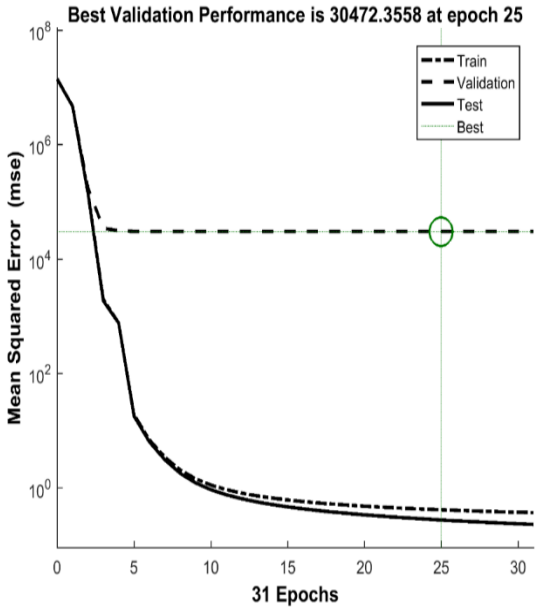
که در آن، d(k) اطلاعات انحراف ساعت استخراج شده از راه‌حل ناوبری گیرنده و $\hat{d}(k)$ تخمین نمونه فعلی بر اساس سه نمونه قبلی است.

۵-۱-۱- حمله نوع اول همگام‌سازی زمان (TSA 1)

در حمله نوع اول، خطای انحراف ساعت به طور ناگهانی به نمونه‌ها وارد می‌شود. بنابراین، $e_{est}(k)$ یکباره به شدت افزایش می‌یابد و الگوریتم را برای شناسایی حمله هدایت می‌کند. خطای تخمین یک ضریب تصحیح برای پالایش نمونه در نظر گرفته می‌شود و میزان انحراف ساعت تزریقی را بیان می‌کند. نتایج پیاده‌سازی حمله نوع اول روی شبکه عصبی MLP انتخابی مطابق جدول (۲) و شکل (۸) صورت گرفته است.

جدول (۲). نتایج پیاده‌سازی حمله نوع اول روی شبکه MLP (4,5,1) (s)

حمله همگام‌سازی زمان نوع اول شبکه عصبی	TSA 1 MLP (4,5,1)
عملکرد کلی	۴۵۷۲/۲
عملکرد آموزش	۰/۴۱۶۲
عملکرد ارزیابی	۳۰۴۷۲
عملکرد آزمون	۰/۲۷۶۲
MSE	۳۰۴۷۲
دوره	۲۵



شکل (۸). حمله نوع اول با فرایند یادگیری MLP NN و MSE هر تکرار (m)

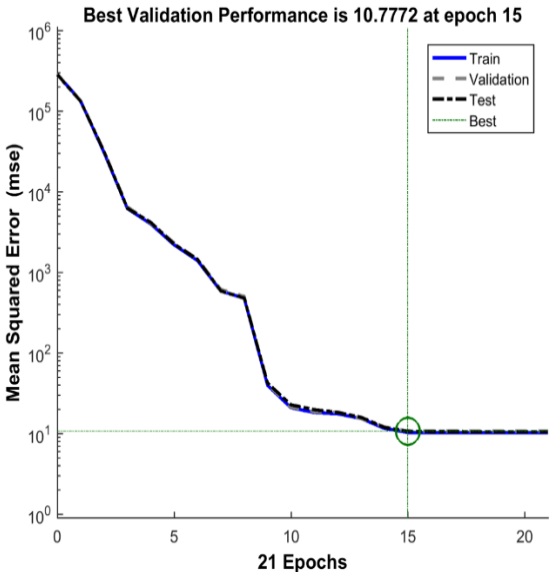
۵-۱-۲- حمله نوع دوم همگام‌سازی زمان (TSA 2)

نوع دوم حمله همگام‌سازی زمان، انحراف ساعت را به طور مشخص تغییر می‌دهد، خطا به‌تدریج به نمونه‌ها اضافه می‌شود. در حمله نوع اول، ضریب تصحیح ثابت می‌ماند، درحالی‌که برای حمله دوم، مقدار باید در هر تکرار بر اساس $e_{est}(k)$ به روز شود. نتایج پیاده‌سازی نوع دوم حمله همگام‌سازی زمان در جدول (۳) و شکل (۹) قرار گرفته است.

[1] Extended Kalman Filter
[2] Luenberger Observer

جدول (۳). نتایج پیاده‌سازی حمله نوع دوم روی شبکه MLP (4,5,1) (s)

حمله همگام‌سازی زمان نوع دوم شبکه عصبی	TSA 2 MLP (4,5,1)
عملکرد کلی	۱۰/۵۱۶۲
عملکرد آموزش	۱۰/۴۰۹۱
عملکرد ارزیابی	۱۰/۷۷۷۲
عملکرد آزمون	۱۰/۷۵۵۰
MSE	۱۰/۷۷۷۲
دوره	۱۵



شکل (۹). حمله نوع دوم با فرایند یادگیری MLP NN و MSE هر تکرار (m)

RE برای کاربردهای ثابت تحت حملات فریب به مدل پویا متکی است. مسئله اصلی در مورد برآوردهای مبتنی بر مدل‌های سامانه، دانش محدود آن‌ها از سیگنال است که باعث بدتر شدن شرایط تخمین می‌شود. روش پیشنهادی دارای یک تخمین خطا پایدار است. دلیل پایداری شبکه عصبیMLP دانش آن از روند انحراف ساعت است که در روش آموزش به دست می‌آید. باتوجه‌به نتایج جدول (۴) روش پیشنهادی MSE کمتری نسبت به روش‌های دیگر دارد که نشان از عملکرد خوب روش پیشنهادی در شناسایی و تصحیح حملات همگام‌سازی زمان دارد.

جدول (۴). MSEهای هر روش تحت شرایط TSA نوع اول و دوم (μs)

حملات نوع اول و دوم	فیلتر کالمن توسعه‌یافته (EFK)	ناظر لورنبرگ (LO)	RE	شبکه عصبی پیشنهادی
TSA 1	۲۷/۲۴	۲۶/۰۵	۲/۱۹	۰/۰۳
TSA 2	۲۶۱/۰۰۳	۲۶۱/۳۷	۱/۳۰	۰/۱۰

۶- نتیجه‌گیری

در این مقاله، یک الگوریتم کاهش اثرات فریب بر اساس مشاهدات انحراف ساعت ارائه شد. یک شبکه عصبی چندلایه برای دنبال‌کردن رفتار اطلاعات انحراف ساعت و حفظ روند معتبر تحت شرایط حمله همگام‌سازی زمان آموزش داده شد که می‌تواند به طرز چشمگیری روند انحراف ساعت را تقلید کند. ازآنجاکه هر مجموعه داده از نظر رفتار انحراف ساعت دارای الگوی مشابه با سایر داده‌ها است، شبکه یک‌بار آموزش داده می‌شود و نیازی به آموزش آن با هر مجموعه داده جدید نیست. بااین‌حال، برآوردگرها بدون آگاهی مناسب از ویژگی‌های سیگنال، مسیر سیگنال معتبر را از دست می‌دهند. بنابراین، یک شبکه عصبی چندلایه برای دنبال‌کردن روند داده‌ها پیشنهاد می‌شود. تفاوت اصلی بین روش پیشنهادی و برآوردگرهای معمولی، اتکای شبکه به اطلاعات آموزشی متشکل از ویژگی‌های سیگنال است.

یک مجموعه داده مرجع می‌تواند برای آموزش شبکه در حالت خارج از خط مورد استفاده قرار گیرد. بنابراین، هیچ الزامی برای آموزش شبکه در مرحله راه‌اندازی گیرنده وجود ندارد. علاوه بر این، وزن‌های آموزش‌دیده را می‌توان در حافظه گیرنده ذخیره کرد و در هر راه‌اندازی مورد استفاده قرار داد.

سازوکار دفاعی روش پیشنهادی مستقل از روند تولید TSA است و فقط بر اصلاح اثرات مخرب بر روی انحراف ساعت متمرکز است. بنابراین، می‌تواند تعداد زیادی از TSAها را بدون نگرانی در مورد روش‌های جدید یا تولید حمله جدید پوشش دهد که بر اطلاعات انحراف ساعت تأثیر می‌گذارند.

شبکه عصبی MLP پیشنهادی در یک الگوریتم تشخیص مورد استفاده قرار می‌گیرد که می‌تواند نوع حمله را تشخیص دهد. این الگوریتم به فضای حافظه کم نیاز دارد و به ابزارهای ریاضی پیچیده و تعداد زیادی منابع محاسباتی نیاز ندارد. بنابراین، به‌روزرسانی سامانه عامل گیرنده شامل چند جدول جستجو و روال الگوریتم است.

عملکرد MLP NN پیشنهادی از طریق یک مجموعه داده دنیای واقعی و دو نوع شناخته شده TSA ارزیابی شده است. نتایج ریشه میانگین مربعات خطا در مقایسه با سایر روش‌های مرسوم و پیشرفته، حداقل شش برابر بهبود را نشان می‌دهند.

۷- مراجع

[1] P. P. Barker and R. W. De Mello, "Determining the Impact of Distributed Generation on Power Systems: Part 1-Radial Distribution Systems," Proc. IEEE PES Summer Power Meeting, Seattle, WA, pp. 1645-1656, Jul. 2000.

[2] S. Silva, T. Hagan, J. Kim, E. Cotilla-Sanchez et al., "Sparse Error Correction for PMU Data under GPS Spooning Attack," *IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, pp. 902-906, 2018.

[3] IEEE Standard for Synchrophasors for Power Systems, IEEE Std. C37.118-2005 (Revision of IEEE Std. 1344-1995), 2006.

[4] M. Mosavi, S. Tohidi, M. Moazedi, "Reduce the Effect of Interference on the GPS Receiver by using Multiple Correlators," Journal of Electronic and Cyber Defense, vol. 9, no. 3, pp. 49-57, December 2021, (In Persian).

[5] F. Diggelen, P. Enge, "The world's First GPS MOOC and Worldwide Laboratory using Smartphones," *In Proceedings of the 28th International Technical Meeting of the Satellite Division of the Institute of Navigation" (ION GNSS+ 2015*), pp. 361-369, 2015.

[6] W. Lewandowski, G. Petit, C. Thomas "Precision and Accuracy of GPS Time Transfer," IEEE Tra Instrum Meas, vol. 42, no. 2, pp. 474-479, 1993.

[7] M. Cui, J. Wang, and M. Yue, "Machine Learning Based Anomaly Detection for Load Forecasting under Cyberattacks," IEEE Trans. Smart Grid, vol. 10, no. 5, pp. 5724-5734, Sep 2019.

[8] J. S. Warner and R. G. Johnston, "A Simple Demonstration That the Global Positioning System (GPS) is Vulnerable to Spoofing," Journal of Security Administration, vol. 25, pp.19-28, 2003.

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

[10] M. Mosavi, M. Moazedi, M. Rezaee, A. Tabatabaei, "Dealing with Disturbances in GPS Receivers," Iran University of Science and Technology Publications, 2015.

[11] D. Schmidt, K. Radke, S. Camtepe, E. Foo, M. Ren, "A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures," ACM Comput Surv, vol. 48, no. 4, pp. 1-31, 2016.

[12] E. Schmidt, J. Lee, N. Gatsis, D. Akopian, "Rejection of Smooth GPS Time Synchronization Attacks via Sparse Techniques," IEEE Sens J, vol. 21, no. 1, pp. 776-789, 2020.

[13] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, A. D. Dominguez-Garcia, "Spoofing GPS Receiver Clock Offset of phasor Measurement Units," IEEE Trans Power Syst, vol. 28, no. 3, pp. 3253-3262, 2013.

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

[15] K. Ghorbani, N. Orouji, M. R. Mosavi, "Navigation Message Authentication Based on one-way Hash Chain to Mitigate Spoofing Attacks for GPS L1," Wireless Pers Commun, vol. 113, no. 4, pp. 1743-1754, 2020.

[16] M. L. Psiaki, B. W. O'Hanlon, J. A. Bhatti, D. P. Shepard, T. E. Humphreys, "GPS Spoofing Detection via Dual-Receiver Correlation of Military Signals," IEEE Trans Aerosp Electron Syst, vol. 49, no. 4, pp. 2250-2267, 2013.

[17] M. R. Mosavi, A. Tabatabaei, M. J. Zandi, "Positioning Improvement by Combining GPS and GLONASS Based on Kalman Filter and Its Application in GPS Spoofing Situations," Gyroscop Navig, vol. 7, no. 4, pp. 318-325, 2016.

[18] N. Orouji and M. R. Mosavi, "A Multi-Layer Perceptron Neural Network to Mitigate the Interference of Time Synchronization Attacks in Stationary GPS Receivers," GPS Solut, vol. 25, no. 3, Jul. 2021.

[19] J. A. Volpe, "Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System," 2001.

[20] M. R. Mosavi, F. Shafiee, "Narrowband Interference Suppression for GPS Navigation using Neural Networks," GPS Solutions, vol. 20, no. 3, pp. 341-351, 2016.

[21] F. A. Ibrahim, "Optimal Linear Neuron Learning and Kalman Filter Based Backpropagation Neural Network for DGPS/INS Integration," IEEE Conference on Position, Location and Navigation Symposium, pp. 1175-1189, 2008.

[22] J. Lee, A. F. Taha, N. Gatsis, 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.