بسمه تعالی

ترجمیک؛ پلتفرم جامع خدمات زبانی

شماره سفارش	۲۰۰٤۲۸۹
کد مترجم	۲۳۰۳۱۲
تاریخ اجرا	۱٤۰٤/۰۲/۲۲

افزایش امنیت سایبری و شناسایی حملات سایبری در ریزشبکه‌های هوشمند جریان مستقیم با بهره‌گیری از فناوری زنجیره‌بلوکی و تکنیک ماشین بردار پشتیبان

کلمات کلیدی:

- امنیت سایبری
- شناسایی حملات سایبری
- حمله تزریق داده جعلی
- زنجیره‌بلوکی
- ماشین بردار پشتیبان

چکیده

با گسترش کاربرد روش‌های هوشمند در کنترل، نظارت و مدیریت عملکرد ریزشبکه‌های جریان مستقیم (DC-MGs)، این سامانه‌ها بیش از پیش در معرض تهدیدات سایبری قرار گرفته‌اند. یک ریزشبکه جریان مستقیم معمولاً شامل اجزایی مانند باتری‌ها، آبَرخازن‌ها، تجهیزات الکترونیکی، سامانه‌های خورشیدی و بارهای مصرفی است. با توجه به این آسیب‌پذیری‌ها، شناسایی حملات سایبری و تأمین امنیت داده‌های مبادله‌شده در ریزشبکه‌های هوشمند جریان مستقیم ـ مشابه با سامانه‌های سایبر-فیزیکی (CPS) ـ به موضوعی حیاتی تبدیل شده است. در این مقاله، روشی نوین برای شناسایی حملات تزریق داده جعلی (FDIA) در ریزشبکه‌های جریان مستقیم پیشنهاد شده است که از تبدیل موجک و تکنیک ماشین بردار پشتیبان (SVM) در کنار فناوری زنجیره‌بلوکی بهره می‌برد. نتایج تحلیل نشان می‌دهد که ولتاژ خروجی در زمان وقوع حمله FDIA در ۰/۴ ثانیه از ۳۵۰ ولت به ۳۰۰ ولت کاهش یافته و در ۰/۷ ثانیه مجدداً به ۳۵۰ ولت بازگشته است. در بازه زمانی ۰/۴ تا ۰/۷ ثانیه نوسانات قابل‌توجهی مشاهده شده و مدل پیشنهادی توانسته است ۴۰۰ مورد منفی صحیح، ۱۹۱ مورد مثبت صحیح، ۱۰ مورد منفی کاذب و صفر مورد مثبت کاذبی را ثبت کند که نشان‌دهنده دقت بالای این مدل در شناسایی حملات FDIA است.

۱- مقدمه

با گسترش روزافزون بهره‌گیری از منابع انرژی تجدیدپذیر مانند انرژی خورشیدی در ریزشبکه‌های جریان مستقیم (DC-MGs)، ساختار شبکه‌های توزیع برق به سمت بهره‌وری بالاتر و سازگاری بیشتر با محیط زیست حرکت کرده‌است. با این حال، این تحول فناورانه، آسیب‌پذیری این سامانه‌ها را در برابر تهدیدات سایبری افزایش داده است. اجزایی نظیر باتری‌ها، ابرخازن‌ها و تجهیزات الکترونیکی قدرت که به تبادل داده در بسترهای ارتباطی متکی هستند، ریزشبکه‌ها را مستعد انواع حملات سایبری، به‌ویژه حملات تزریق داده جعلی (FDIA)، می‌سازند. حملات FDIA می‌توانند با وارد کردن داده‌های نادرست به سامانه‌های کنترلی ریزشبکه‌ها، موجب بی‌ثباتی در شبکه و بروز اختلالات عملیاتی جدی شوند. با توجه به جایگاه کلیدی این ریزشبکه‌ها در زیرساخت‌های نوین برق، تأمین امنیت سایبری آن‌ها به ضرورتی حیاتی تبدیل شده‌است. این موضوع موجب توسعه سازوکارهای پیشرفته برای شناسایی حملات سایبری و چارچوب‌های امنیتی بهینه‌شده برای ریزشبکه‌های هوشمند جریان مستقیم شده است [۱]. برای مقابله مؤثر با این تهدیدات، راهکارهای متنوعی ارائه شده‌اند که از جمله آن‌ها می‌توان به فناوری زنجیره‌بلوکی، مدل‌های شناسایی مبتنی بر هوش مصنوعی (AI) و الگوریتم‌های یادگیری ماشین اشاره کرد. زنجیره‌بلوکی به‌عنوان ابزاری قدرتمند با ایجاد بستری توزیع‌شده و تغییرناپذیر، تضمین‌کننده یکپارچگی اطلاعات و برقراری ارتباطات امن در بستر ریزشبکه است. افزون بر این، مدل‌های مبتنی بر هوش مصنوعی مانند یادگیری عمیق و روش‌های بهینه‌سازی، در شناسایی دقیق حملات FDIA عملکرد بسیار مطلوبی از خود نشان داده‌اند و می‌توانند داده‌های مخرب را از سیگنال‌های واقعی تفکیک کنند [۲]. این پیشرفت‌ها در زمینه شناسایی و پیشگیری از حملات سایبری، نقش مهمی در حفظ تاب‌آوری، قابلیت اطمینان و کارایی عملیاتی ریزشبکه‌های جریان مستقیم ایفا می‌کنند، به‌ویژه در شرایطی که استفاده از شبکه‌های هوشمند و فناوری‌های مبتنی بر اینترنت اشیا (IoT) به‌طور فزاینده‌ای در حال گسترش است. در نتیجه، امنیت سایبری تقویت‌شده در ریزشبکه‌های جریان مستقیم، نه تنها یک نیاز فناورانه بلکه یک مؤلفه بنیادین در دستیابی به توزیع انرژی پایدار در آینده محسوب می‌شود

ادغام فزاینده منابع انرژی تجدیدپذیر، سامانه‌های تولید پراکنده و تجهیزات ذخیره‌سازی انرژی در شبکه‌های قدرت نوین، منجر به ظهور ریزشبکه‌های هوشمند جریان مستقیم شده‌است. این ریزشبکه‌ها با بهبود بهره‌وری انرژی و افزایش پایداری، نقش مهمی در ساختار آینده‌محور شبکه‌های برق ایفا می‌کنند با این حال، گسترش دیجیتالی‌سازی در فرآیندهای عملیاتی آن‌ها، زمینه بروز تهدیدات گسترده‌ای همچون دستکاری اطلاعات، نفوذهای غیرمجاز و حملات انکار سرویس توزیع‌شده (DDoS) را فراهم کرده است بنابراین، تضمین امنیت سایبری در این ریزشبکه‌ها برای حفظ صحت عملکرد شبکه و جلوگیری از اختلالاتی که ممکن است منجر به قطع یا اختلال در تأمین انرژی شوند، ضرورتی انکارناپذیر است. در همین راستا، بهره‌گیری از راهکارهای مؤثر برای شناسایی و کاهش اثرات حملات سایبری، از ارکان حیاتی در طراحی زیرساخت‌های ایمن به شمار می‌رود [۳].

در میان فناوری‌های نوین، زنجیره‌بلوکی به‌عنوان ابزاری مؤثر برای ارتقای امنیت شبکه‌های هوشمند مطرح شده است. این فناوری با ویژگی‌هایی مانند غیرمتمرکز بودن، تغییرناپذیری اطلاعات و شفافیت بالا، بستری مطمئن برای تبادل داده‌ها، کنترل دسترسی و تأیید تراکنش‌ها در ریزشبکه‌های جریان مستقیم فراهم می‌آورد [۴]. با حذف وابستگی به نقاط متمرکز و بهره‌گیری از دفترکل توزیع‌شده یا سامانه ثبت غیرمتمرکز اطلاعات (DLT)، ریسک نفوذ و حملات سایبری کاهش یافته و امنیت کلی سامانه بهبود می‌یابد. افزون بر این، سازوکارهای اجماع در زنجیره‌بلوکی لایه‌ای مضاعف از امنیت ایجاد کرده و به ذی‌نفعان اجازه می‌دهند فعالیت‌های غیرمجاز را به‌صورت بلادرنگ شناسایی و مهار کنند [۵].

در کنار زنجیره‌بلوکی، استفاده از روش‌های پیشرفته پردازش سیگنال نظیر تبدیل ویولت نیز می‌تواند در شناسایی تهدیدات سایبری نقش کلیدی ایفا کند [۶]. تبدیل ویولت امکان تحلیل سیگنال‌های غیرایستا را فراهم می‌سازد؛ سیگنال‌هایی که در سامانه‌های پایش و کنترل شبکه به‌وفور دیده می‌شوند [۷]. با تجزیه سیگنال‌ها به مؤلفه‌های مختلف فرکانسی، تبدیل ویولت قادر است ناهنجاری‌هایی مانند نوسانات غیرطبیعی ولتاژ یا تزریق داده‌های جعلی را آشکار سازد [۸]. ترکیب قابلیت‌های زنجیره‌بلوکی با قدرت تحلیل تبدیل ویولت، یک راهکار جامع، چندلایه و مقاوم برای امنیت سایبری در ریزشبکه‌های هوشمند جریان مستقیم فراهم می‌آورد که نه‌تنها پاسخ‌گوی نیاز به شناسایی بلادرنگ تهدیدات است، بلکه تاب‌آوری بلندمدت شبکه در برابر حملات آینده‌نگر را نیز تضمین می‌کند.

۲- مرور پیشینه تحقیق

غیاثی و همکاران [۹] در پژوهش خود به بررسی تأثیر حملات سایبری، به‌ویژه حملات تزریق داده جعلی (FDIA)، بر ریزشبکه‌های هوشمند جریان مستقیم (DC-MG) پرداختند. این مطالعه آسیب‌پذیری ریزشبکه‌های جریان مستقیم را به دلیل وجود اجزایی مانند باتری‌ها، اَبَرخازن‌ها، تجهیزات الکترونیک قدرت، منابع انرژی تجدیدپذیر نظیر سیستم‌های خورشیدی فتوولتائیک (PV)، و شبکه‌های ارتباطی مورد استفاده برای تبادل داده‌ها، مورد تأکید قرار داد. به‌منظور تقویت امنیت سایبری، این تیم پژوهشی ترکیبی از تبدیل هیلبرت-هوانگ جهت تحلیل دقیق سیگنال‌ها و فناوری زنجیره‌بلوکی برای ایجاد دفترکل توزیع‌شده را پیشنهاد کرد. یافته‌های آن‌ها نشان داد که این ترکیب موجب افزایش دقت در شناسایی تهدیدات و ارتقای امنیت اطلاعات در DC-MGهای هوشمند می‌شود.

مادیچتی و همکاران [۱۰] یک چارچوب نوآورانه مبتنی بر حسگر مجازی طراحی کردند که قادر است به‌صورت مستمر، وضعیت سخت‌افزار ریزشبکه جریان مستقیم (DCMG) را پایش کرده و حملات سایبری را شناسایی کند. این روش، به افزایش دقت و سرعت واکنش به تهدیدات در سطح فیزیکی سیستم کمک می‌کند.

در پژوهشی دیگر، دهقانی و همکاران [۱۱] به مسئله شناسایی حملات سایبری در DC-MGs پرداختند و با تأکید بر رشد روزافزون آسیب‌پذیری سیستم‌های سایبر-فیزیکی (CPS) در حوزه برق، الگویی مبتنی بر یادگیری عمیق معرفی کردند. این روش که از یک رویکرد تجمعی گزینشی بهره می‌برد و با الگوریتم بهینه‌سازی گرگ خاکستری (GWO) پیکربندی شده بود، موفق شد با دقتی بیش از ۹۵٪ انواع مختلف حملات FDIA را شناسایی کند. نتایج نشان دادند که عملکرد این مدل نسبت به روش‌های پیشین از جمله مدل‌های کم‌عمق و تبدیل هیلبرت-هوانگ به‌مراتب بهتر است.

دای و همکاران [۱۲] به بررسی آسیب‌پذیری ریزشبکه‌ها در برابر حملات تزریق داده جعلی (FDIA) پرداختند و به‌ویژه به ضعف‌های موجود در فرآیند تبادل اطلاعات بین واحدهای کنترل‌کننده اشاره نمودند. برای مقابله با این تهدیدات، آن‌ها چارچوبی مقاوم در برابر حملات سایبری پیشنهاد دادند که با بهره‌گیری از فناوری زنجیره‌بلوکی، فرآیند تبادل داده‌ها و تراکنش‌ها را ایمن ساخته و جایگزین مناسبی برای روش‌های ارتباطی سنتی و غیرقابل‌اطمینان فراهم می‌کند.

گونگ و همکاران [۱۳] سازوکاری نوآورانه جهت شناسایی تهدیدات سایبری در ریزشبکه‌های مبتنی بر اینترنت اشیاء معرفی کردند که در آن از مبدل‌های قدرت استفاده می‌شود. در این رویکرد، هر عامل (Agent) با جمع‌آوری اطلاعات خود و همسایگان، تلاش می‌کند تا تنظیم خروجی مناسبی برای دستیابی به اجماع در توزیع توان داشته باشد. این روش برخلاف الگوهای تشخیص سنتی که مبتنی بر مدل‌سازی هستند، از تحلیل رفتار دینامیکی مبدل‌ها برای شناسایی جایگزینی مخفیانه سیگنال‌ها یا تحریکات مشکوک (تحریک مخرب عامل‌ها) بهره می‌برد.

پینتو و همکاران [۱۴] با تمرکز بر عملکرد سامانه‌های ریزشبکه جریان مستقیم، نقش کلیدی مبدل‌های الکترونیک قدرت و پروتکل‌های ارتباطی را در تضمین پایداری عملکرد سیستم مورد ارزیابی قرار دادند. آنان نشان دادند که این سامانه‌ها به شدت در معرض حملات سایبری به‌ویژه FDIA قرار دارند که با وارد کردن داده‌های نادرست می‌توانند موجب بی‌ثباتی در عملکرد ریزشبکه شوند.

در مطالعه‌ای دیگر، پینتو و همکاران [۲] بر افزایش تهدیدات سایبری هم‌زمان با توسعه فناوری‌های شبکه هوشمند تأکید کردند. آن‌ها هشدار دادند که این شبکه‌ها ممکن است در برابر حملات پیچیده‌ای از نوع جعبه‌سیاه (Deep Box) آسیب‌پذیر باشند؛ حملاتی که با استفاده از کتابخانه‌هایی مانند SecLib و Bouncy Castle و با اطلاعات اندک درباره هدف قابل پیاده‌سازی هستند.

راجییاگاری و همکاران [۱۵] با هدف ارتقای امنیت سایبری در شبکه‌های هوشمند مبتنی بر زنجیره‌بلوکی، ترکیبی از شبکه عصبی پیچشی (CNN) و الگوریتم بهینه‌سازی کرکس آفریقایی (AVOA) را پیشنهاد کردند. این رویکرد با هدف رفع معضلات رایج در روش‌های موجود ـ نظیر دقت پایین، پیچیدگی بالای محاسبات و محدودیت در نرخ انتقال داده ـ طراحی شده است و با بهره‌گیری از یک چارچوب هوشمند، عملکردی مؤثر در نظارت بر حملات و مدیریت داده‌ها ارائه می‌دهد.

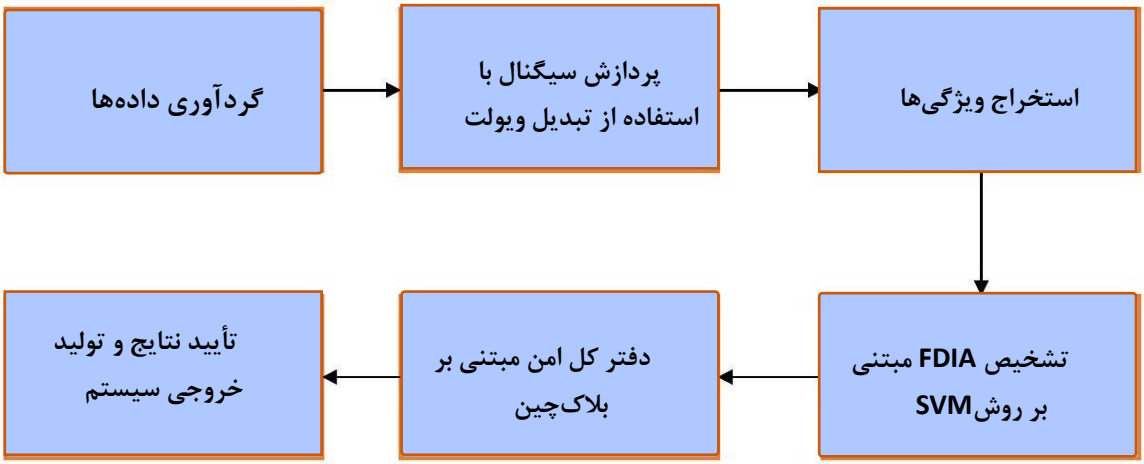
گونگ و همکاران [۱۶] مکانیزمی نوآورانه برای تشخیص حملات سایبری در ریزشبکه‌های جریان مستقیم مبتنی بر اینترنت اشیاء (IoT) و متشکل از مبدل‌ها پیشنهاد دادند. نتایج حاصل از شبیه‌سازی یک ریزشبکه ۹۰۰ ولت با ۵ عامل در محیط سیمولینک و آزمایش سخت‌افزاری یک شبکه ۸۰ ولت با ۳ عامل روی پلتفرم dSpace نشان داد که خطای تخمین کمتر از ۴/۹٪ بوده و کلیه حملات با موفقیت شناسایی شده‌اند، که اعتبار و کارایی روش پیشنهادی را به‌خوبی اثبات می‌کند.

وتامبتی و همکاران [۱۷] آسیب‌پذیری‌های سیستم‌های سایبر-فیزیکی (CPS) در برابر حملات مخرب سایبری را مورد بررسی قرار دادند و چالش‌های ناشی از شبکه‌های ارتباطی را در تأمین امنیت و محرمانگی داده‌ها برجسته کردند. آنان الگوریتمی با عنوان «امضای سبک مبتنی بر بلاک‌چین» (LWBSA) طراحی کردند که با هدف کاهش بار محاسباتی، بهبود مقیاس‌پذیری، کاهش تأخیر و سربار پهنای‌باند، جایگزینی مناسب برای روش‌های سنتی بلاک‌چین در کاربردهای حساس ارائه می‌دهد. خلاصه‌ای از مطالعات مرور پیشینه پژوهش در جدول ۱ ارائه شده است.

جدول ۱. خلاصه مرور پیشینه پژوهش.

ردیف	نویسندگان	روش‌ها و تکنیک‌ها	مزایا	معایب
۱	غیاثی و همکاران [۹]	تبدیل هیلبرت-هوانگ و دفترکل مبتنی بر بلاک‌چین	افزایش دقت تشخیص حملات، ارتقای امنیت داده در ریزشبکه‌های DC	پیچیدگی محاسباتی بالا و هزینه اجرای زیاد
۲	مادیچتی و همکاران [۱۰]	چارچوب حسگر مجازی برای تشخیص حملات سایبری	پایش پیوسته و لحظه‌ای در سطح سخت‌افزار، تشخیص سریع حملات	نیازمند یکپارچگی بالا با سخت‌افزار، احتمال ایجاد گلوگاه عملکردی
۳	دهقانی و همکاران [۱۱]	رویکرد یادگیری عمیق جمعی بهینه‌سازی‌شده با الگوریتم گرگ خاکستری (GWO)	دقت بیش از ۹۵٪ در تشخیص حملات تزریق داده، عملکرد بهتر نسبت به مدل‌های کم‌عمق	وابستگی زیاد به کیفیت داده‌های آموزشی، احتمال بیش‌برازش در محیط‌های پویا
۴	دای و همکاران [۱۲]	چارچوب تاب‌آور سایبری و فناوری بلاک‌چین	امنیت در تبادل اطلاعات، افزایش مقاومت ریزشبکه در برابر حملات FDIA	پیاده‌سازی پیچیده بلاک‌چین، نیازمند پردازش پرهزینه
۵	گونگ و همکاران [۱۳]	تحلیل رفتار مبدل‌ها در ریزشبکه‌های DC مبتنی بر اینترنت اشیا	دستیابی به اجماع در اشتراک‌گذاری توان، تشخیص حملات پنهان یا تحریک عوامل	محدود به معماری خاص مبدل‌ها، مقیاس‌پذیری محدود

				در سیستم‌های پیچیده
۶	پینتو و همکاران [۱۴]	تحلیل مبدل‌های الکترونیک قدرت و پروتکل‌های ارتباطی در ریزشبکه‌های DC	شناسایی آسیب‌پذیری‌ها در حملات FDIA، بهبود درک پایداری سیستم	وابستگی زیاد به پیکربندی مبدل و پروتکل‌ها، کارایی محدود در سیستم‌های هیبریدی
۷	پینتو و همکاران [۲]	تشخیص حملات پیشرفته جعبه سیاه با استفاده از SecLib و Bouncy Castle	توانایی شناسایی حملات پیشرفته با دانش محدود از هدف	آسیب‌پذیر در برابر حملاتی با آگاهی عمیق از کتابخانه‌های رمزنگاری
۸	راجییاگاری و همکاران [۱۵]	ترکیب شبکه عصبی پیچشی (CNN) با الگوریتم بهینه‌سازی کرکس آفریقایی (AVOA)	افزایش دقت، کاهش پیچیدگی محاسباتی، بهبود نرخ تشخیص حملات	ممکن است در کاربردهای بلادرنگ با تأخیر در پردازش داده مواجه شود
۹	گونگ و همکاران [۱۶]	مکانیزم شناسایی حملات در ریزشبکه‌های DC مبتنی بر IoT و مبدل	اعتبارسنجی با شبیه‌سازی و سخت‌افزار، خطای تخمین کمتر از ۴.۹٪	نیاز به سخت‌افزارهای گران و یکپارچه‌سازی با سیستم‌های IoT، مقیاس‌پذیری محدود
۱۰	وتامبتی و همکاران [۱۷]	الگوریتم امضای سبک مبتنی بر بلاک‌چین (LWBSA)	کاهش پیچیدگی محاسباتی، بهبود مقیاس‌پذیری، کاهش تأخیر و سربار پهنای باند	همچنان وابسته به بلاک‌چین که ممکن است برای CPSهای بزرگ بهینه نباشد



شکل ۱- معماری روش پیشنهادی.

۲-۱- اهداف پژوهش

- تمرکز اصلی این تحقیق، طراحی و توسعه یک سازوکار مطمئن و کارآمد برای شناسایی و مهار حملات تزریق داده جعلی (FDIA) است؛ حملاتی که می‌توانند به طور جدی امنیت و یکپارچگی عملکرد میکروشبکه‌های هوشمند را دچار اختلال نمایند.

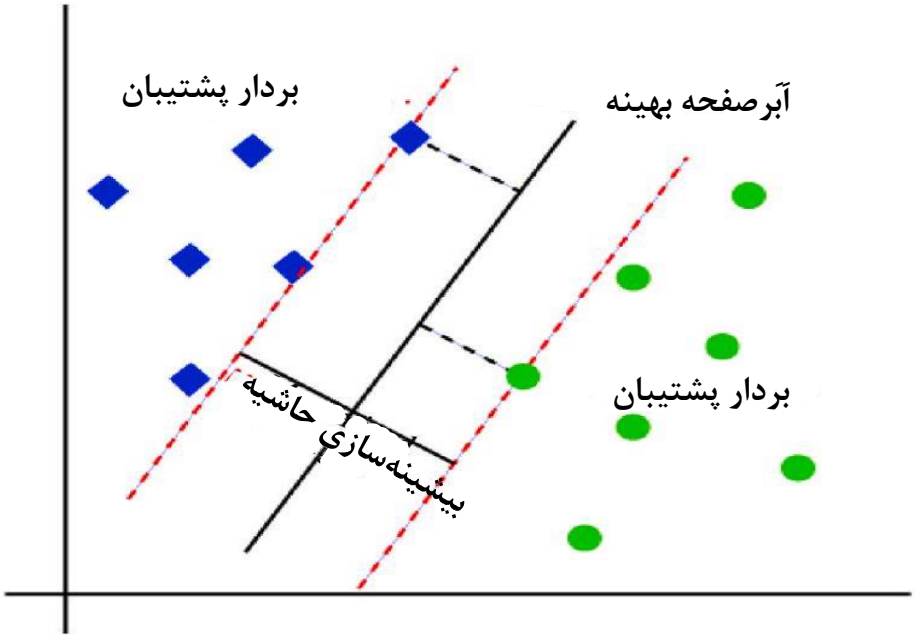
- در این راستا، تحقیق حاضر از توانمندی‌های روش تحلیل موجک برای استخراج ویژگی‌های مهم از داده‌های عملیاتی میکروشبکه بهره می‌گیرد و با به‌کارگیری الگوریتم ماشین بردار پشتیبان به عنوان ابزار طبقه‌بندی، تلاش می‌شود تا رفتارهای ناهنجار و حملاتی مانند FDIA با دقت از وضعیت‌های عادی تفکیک گردند.

- یکی از ارکان کلیدی در این طرح، استفاده از فناوری زنجیره بلوکی برای تقویت امنیت سامانه تشخیص است؛ به نحوی که از غیرقابل تغییر بودن و شفافیت تبادل داده‌ها در بستر شبکه اطمینان حاصل شود.

- در نهایت، کارایی و دقت الگوریتم پیشنهادی با استفاده از تحلیل دقیق شاخص‌های عملکردی مانند نرخ شناسایی صحیح، نرخ هشدار اشتباه و دقت نهایی مورد ارزیابی و اعتبارسنجی قرار می‌گیرد.

۳- روش پیشنهادی برای شناسایی حملات سایبری و ارتقای امنیت سایبری

در شکل ۱، روند کامل تشخیص حملات سایبری و ارتقاء سطح امنیتی در یک میکروشبکه DC هوشمند نمایش داده شده است. در این چارچوب، از ترکیب تحلیل سیگنال مبتنی بر تبدیل موجک و الگوریتم طبقه‌بندی ماشین بردار پشتیبان (SVM) بهره‌گیری شده و امنیت داده‌ها از طریق فناوری زنجیره بلوکی تضمین می‌گردد. فرآیند با مرحله «دریافت داده» آغاز می‌شود، که در آن داده‌های خام از سیستم میکروشبکه جمع‌آوری شده و برای تحلیل آماده می‌گردد. در گام بعدی، «پردازش سیگنال» با استفاده از تبدیل موجک انجام می‌شود. این تکنیک موجب تجزیه سیگنال خام به مؤلفه‌های فرکانسی متنوع می‌شود تا ویژگی‌های مهم زمانی-فرکانسی آن استخراج گردد. سپس در مرحله استخراج ویژگی، شاخص‌های مؤثر و مرتبط با حملات یا ناهنجاری‌های احتمالی از سیگنال‌های پردازش‌شده استخراج می‌شوند، که این ویژگی‌ها نقش مهمی در تشخیص دقیق تهدیدات سایبری ایفا می‌کنند (به شکل‌های ۲ تا ۶ مراجعه شود).



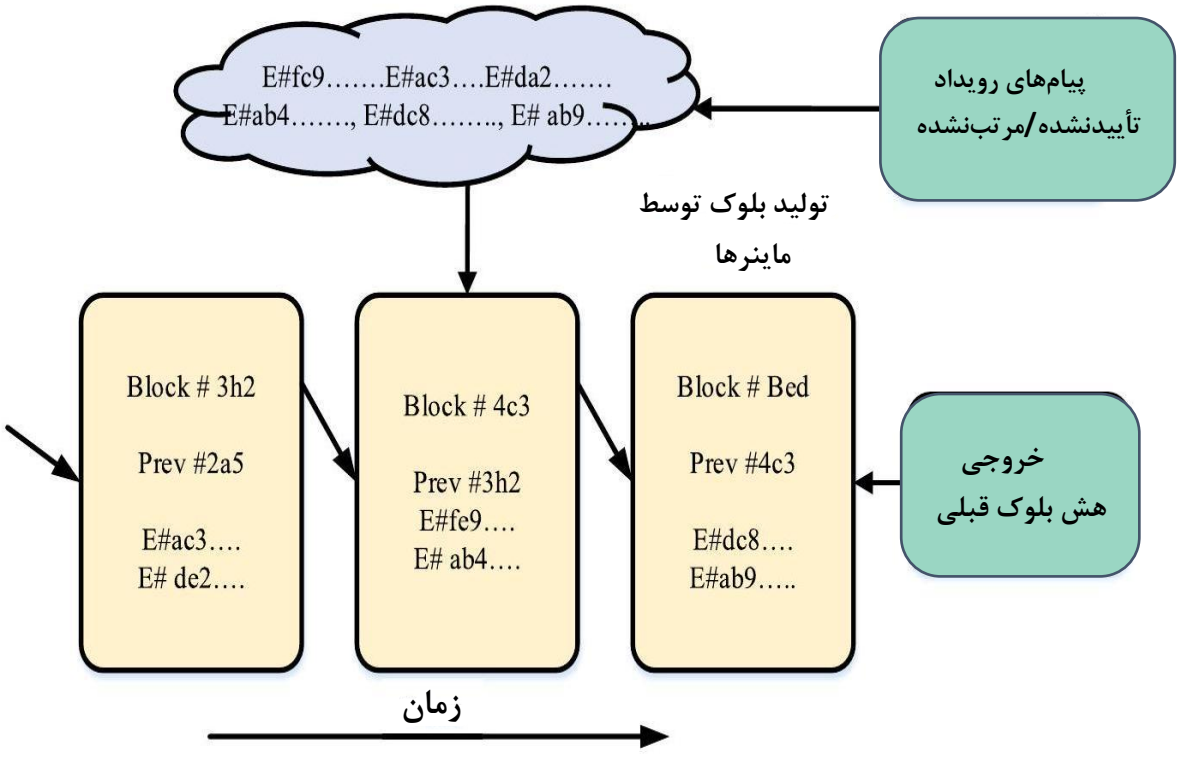
شکل ۲- یکپارچه‌سازی الگوریتم ماشین بردار پشتیبان (SVM) با فناوری بلاک‌چین.

ویژگی‌های به‌دست‌آمده به بخش تشخیص حملات FDIA منتقل می‌شوند، که در آن از الگوریتم ماشین بردار پشتیبان (SVM) به‌عنوان طبقه‌بند استفاده می‌شود. این مدل با بهره‌گیری از اطلاعات استخراج‌شده، تلاش می‌کند تا نشانه‌های حملات سایبری را شناسایی و تفکیک کند. پس از انجام موفقیت‌آمیز فرآیند تشخیص، داده‌ها به‌صورت ایمن در یک دفترکل رمزنگاری‌شده مبتنی بر فناوری بلاک‌چین ذخیره می‌شوند. این ساختار نه‌تنها تضمین‌کننده عدم تغییرپذیری اطلاعات است، بلکه امکان پیگیری و تأیید صحت داده‌ها را در صورت بروز حملات احتمالی فراهم می‌سازد. در گام پایانی، ماژول «بررسی نتایج و تولید خروجی سیستم»، عملکرد نهایی را ارائه داده و در صورت لزوم، بازخورد مناسبی برای اقدامات اصلاحی یا حفاظتی آینده فراهم می‌سازد.

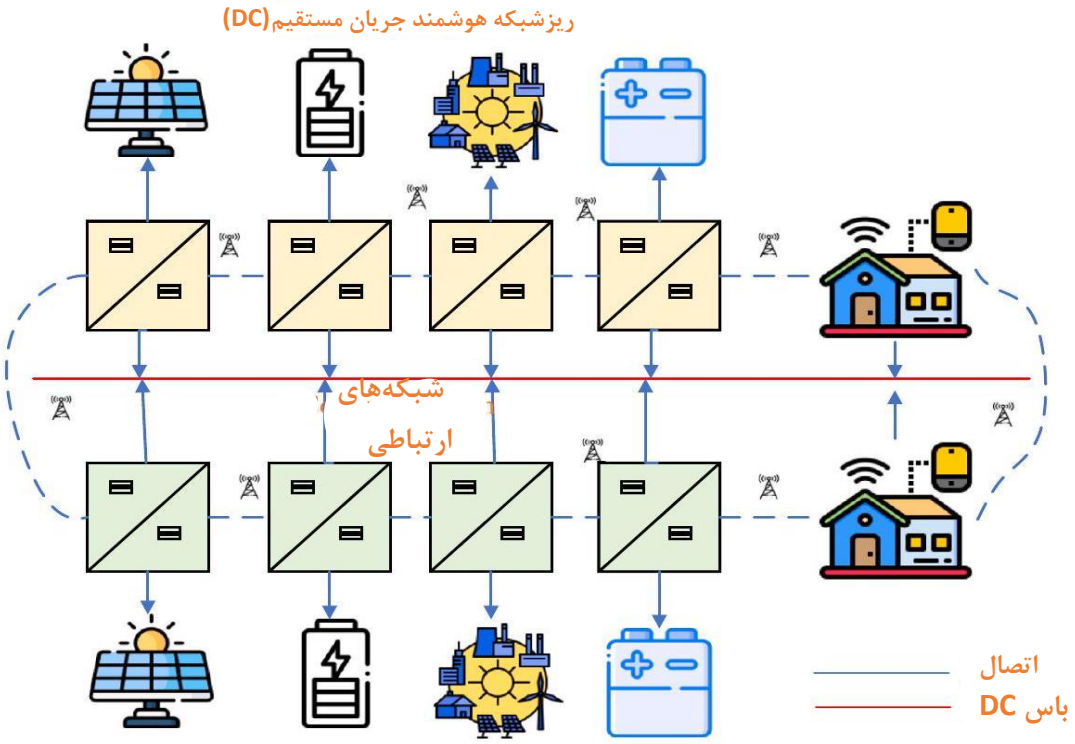
در جدول ۲، مجموعه‌ای از پارامترهای اساسی مورد استفاده در مدل SVM و تبدیل موجک نمایش داده شده‌اند. در میان این پارامترها، ابرپارامترهایی نظیر نوع تابع هسته‌ای (RBF)، مقدار پارامتر تنظیمی (C)، نرخ گاما و حد تلورانس در مدل SVM لحاظ شده‌اند که با هدف ارتقاء عملکرد طبقه‌بندی، به‌دقت بهینه‌سازی شده‌اند. همچنین در بخش تبدیل موجک، عواملی چون نوع موجک (Daubechies)، سطح تجزیه و شیوه اعمال آستانه به‌گونه‌ای انتخاب شده‌اند که میان حذف مؤثر نویز و حفظ محتوای اطلاعاتی سیگنال، تعادل مناسبی برقرار گردد. این انتخاب‌های فنی، نقش بنیادینی در دقت شناسایی حملات و طبقه‌بندی صحیح آن‌ها دارند.

۳-۱- تحلیل تبدیل ویولت برای ارتقای امنیت سایبری

تبدیل موجک یکی از روش‌های تحلیلی پیشرفته در حوزه ریاضیات است که به‌صورت ویژه در تحلیل داده‌های زمانی و سیگنال‌ها مورد استفاده قرار می‌گیرد و کاربرد آن در ارتقای امنیت سایبری میکروگریدهای هوشمند DC بسیار چشمگیر است. در زیرساخت‌های شبکه هوشمند، این روش با تجزیه‌ی سیگنال‌های پیچیده به مؤلفه‌هایی در سطوح فرکانسی مختلف، امکان بررسی دقیق‌تری از رفتار سیستم را فراهم می‌سازد [۱۸-۲۰]. به‌عنوان نمونه، در یک میکروگرید DC هوشمند، تبدیل موجک می‌تواند نوسانات و بی‌نظمی‌های موجود در سیگنال‌های الکتریکی را بررسی کرده و الگوهای غیرمعمولی را که ممکن است نشان‌دهنده‌ی نفوذ یا تهدید سایبری باشند، شناسایی نماید. ادغام این قابلیت تحلیلی با فناوری بلاک‌چین، که خود بستری ایمن، توزیع‌شده و غیرقابل‌تحریف برای ثبت داده‌ها فراهم می‌آورد، باعث شکل‌گیری سیستمی مطمئن برای نظارت و اعتبارسنجی پیوسته بر فعالیت‌های شبکه می‌شود [۲۱]. فناوری بلاک‌چین تضمین‌کننده‌ی حفظ اصالت و تمامیت داده‌های مربوط به ناهنجاری‌های شناسایی‌شده است، در حالی که تبدیل موجک، با عمق تحلیلی خود، امکان تمایز دقیق میان نوسانات طبیعی سیستم و تهدیدات واقعی سایبری را فراهم می‌کند. این هم‌افزایی میان ابزارهای تحلیل و امنیت، سبب تقویت اساسی ساختار دفاعی میکروگریدهای هوشمند DC خواهد شد.



شکل ۳. تولید بلاک‌چین از پیام‌های رویداد تأییدنشده.



شکل ۴. معماری کلی سیستم پیشنهادی.

روش EMD سیگنال‌های مختلف را به مجموعه‌ای از توابع حالت ذاتی (IMF) تجزیه می‌کند؛ این توابع پیوسته بوده و برای تحلیل دقیق سیگنال‌های غیرخطی و غیرایستا طراحی شده‌اند. برای هر سیگنال گسسته‌ی تعریف‌شده مانند $s(t)$، مقدار μ_1 میانگینی است از پوش‌های بالا و پایین که از نقاط محلی سیگنال به‌دست می‌آیند. نخستین مؤلفه‌ی IMF با استفاده از رابطه‌ی زیر محاسبه می‌شود:

$$\beta_1 = s(t) - \mu_1 \quad (1)$$

در گام بعدی فرآیند پردازش، متغیر η_1 به‌عنوان انباشت اطلاعات در نظر گرفته می‌شود و مقدار β_{11} به‌عنوان اختلاف بین β_1 و میانگین پوش‌های بیشینه و کمینه‌ی آن تعریف می‌شود:

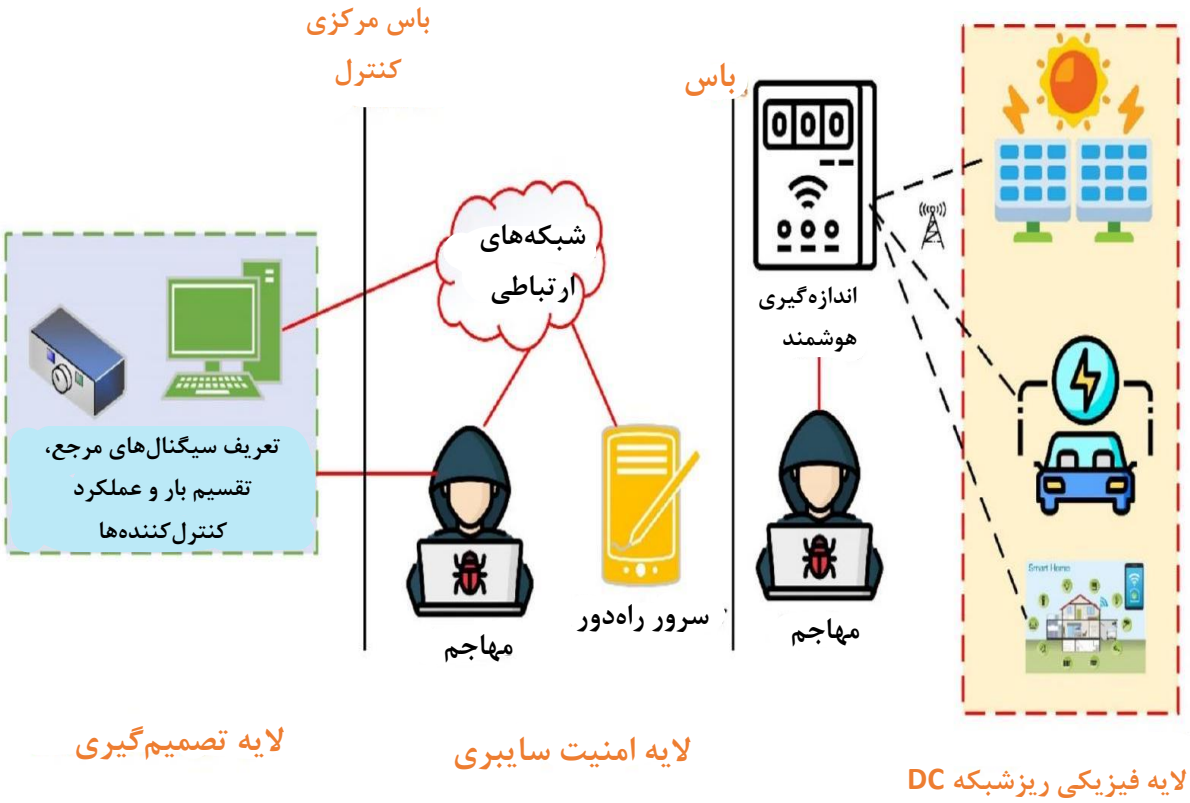
$$\beta_{11} = \beta_1 - \beta_{11} \quad (2)$$

این فرآیند چندین بار (k بار) تکرار می‌شود تا زمانی که مؤلفه‌ای حاصل شود که تمامی شرایط لازم برای تابع IMF را دارا باشد. این مؤلفه طبق رابطه‌ی زیر تعریف می‌شود:

$$\eta_{1(k-1)} - \mu_{1k} = \eta_{1k} \quad (3)$$

اگر عضو محاسبه‌شده شرایط توقف فرآیند استخراج IMF را ارضا کند، آنگاه η_1 به‌عنوان اولین تابع IMF در نظر گرفته می‌شود. پس از استخراج این تابع، سیگنال باقی‌مانده که حاوی سایر اجزای غیرخطی سیگنال اصلی است، به‌صورت زیر تعریف می‌شود:

$$r(t) = s(t) - \eta 1 \qquad (٤)$$



شکل ۵- نمودار بلوکی لایه سایبر-فیزیکی یک ریزشبکه (MG).

اگر تابع $r(t)$ معیار توقف در فرآیند EMD را برآورده سازد، به‌عنوان سیگنال باقی‌مانده‌ی نهایی در نظر گرفته شده و فرآیند تجزیه پایان می‌یابد. تکنیک پالایش IMF با حذف امواج مزاحم، توابع IMF متقارن‌تری را تولید می‌کند که حول صفر متمرکز هستند. به‌محض آن‌که شرط ریاضی توقف برقرار شود، فرآیند پالایش خاتمه می‌یابد و این تضمین را فراهم می‌کند که تجزیه‌ی انجام‌شده دقیق و بدون از بین رفتن اطلاعات است. رایج‌ترین معیار توقف، روش کاشی (Cauchy) است که زمانی فعال می‌شود که انحراف معیار بین دو تابع IMF متوالی به یک آستانه‌ی از پیش تعیین‌شده برسد. در این مجموعه، تعداد IMFهای تولیدشده، به سیگنال اصلی و همچنین مقدار آستانه انتخاب‌شده در معیار توقف بستگی دارد.

فرکانس با استفاده از تبدیل موجک (WT) محاسبه می‌شود. تابع مقدار واقعی $g(t)$ که از کلاس L_p است، می‌تواند از طریق بخش‌بندی مختلط به یک تابع تحلیلی $h(t)$ تبدیل شود که در رابطه‌ی (۵) آمده است:

$$h(t) = \frac{1}{\Pi} p \int_{-\infty}^{\infty} \frac{g(\beta)}{t-\alpha} d\beta \quad (۵)$$

که در آن p نشان‌دهنده‌ی مقادیر اصلی انتگرال است. بنابراین، با استفاده از WT، توابع تحلیلی را می‌توان به‌صورت زیر نمایش داد:

$$z(t) = g(t) + j.h(t) = \beta(t) \cdot e^{j\varphi(t)} \quad (۶)$$

$$\beta(t) = \sqrt{g^2 + h^2; \varphi(t)} = \text{arctg}\left(\frac{h}{g}\right) \quad (۷)$$

دامنه‌ی لحظه‌ای با β نشان داده می‌شود، در حالی‌که φ نمایانگر تابع فاز است. در نتیجه، فرکانس لحظه‌ای به‌صورت زیر تعریف می‌شود:

$$\varphi = -\frac{dw}{dt} \quad (۸)$$

رابطه‌ی بالا نشان‌دهنده‌ی توصیف دقیق رفتار محلی فاز و دامنه‌ی متغیر سیگنال‌های مثلثاتی در قالب تابع $g(t)$ است. همچنین انرژی طیفی سیگنال با رابطه‌ی زیر تعیین می‌شود:

$$SE = \beta(t)^2 \quad (۹)$$

لازم به ذکر است که تبدیل موجک برای تحلیل دقیق، عمدتاً بر سیگنال‌های تک‌مولفه‌ای قابل‌اتکا است و نتایج قابل اعتمادتری در این حالت ارائه می‌دهد.

۳-۲- ادغام ماشین‌های بردار پشتیبان در محیط بلاک‌چین

ترکیب الگوریتم ماشین بردار پشتیبان (SVM) با محیط بلاک‌چین، سطح جدیدی از امنیت و دقت در شناسایی تهدیدات سایبری را برای سامانه‌های پردازش داده فراهم می‌سازد. الگوریتم SVM که یکی از روش‌های قدرتمند در حوزه یادگیری ماشین محسوب می‌شود، عمدتاً برای طبقه‌بندی و شناسایی ناهنجاری‌ها به‌کار می‌رود و در تشخیص حملات پیشرفته‌ای مانند تزریق داده جعلی (FDIA) در زیرساخت‌های حیاتی از جمله شبکه‌های هوشمند و ریزشبکه‌ها کاربرد دارد [۲۲]. با ادغام در ساختار بلاک‌چین، این الگوریتم در بستری امن، غیرمتمرکز و مقاوم در برابر تغییر فعالیت می‌کند و از ویژگی‌های کلیدی بلاک‌چین نظیر تغییرناپذیری داده‌ها و دفتر کل توزیع‌شده بهره‌مند می‌شود.

در این ساختار، هر بلوک از زنجیره، نتایج حاصل از شناسایی تهدیدات را به‌صورت رمزنگاری‌شده ذخیره می‌کند و این امر تضمین می‌کند که اطلاعات توسط افراد غیرمجاز قابل تغییر نباشد. این فرآیند باعث می‌شود مجموعه

ویژگی‌های استخراج‌شده، نتایج تشخیص و وضعیت‌های سیستم، به‌صورت آنی و ایمن بین گره‌های مختلف به اشتراک گذاشته شود، بدون اینکه نیازی به یک مرکز کنترل مرکزی وجود داشته باشد. این معماری غیرمتمرکز، احتمال وقوع خطای نقطه‌ای (Single Point of Failure) یا تغییر عمدی در خروجی‌های SVM را به‌طور قابل‌توجهی کاهش می‌دهد. افزون بر این، مکانیسم اجماع در بلاک‌چین تضمین می‌کند که هرگونه به‌روزرسانی در داده‌های شناسایی یا پارامترهای مدل تنها در صورتی اعمال شود که تمامی گره‌ها آن را تأیید کنند؛ امری که شفافیت و انسجام کل سیستم را تضمین می‌کند.

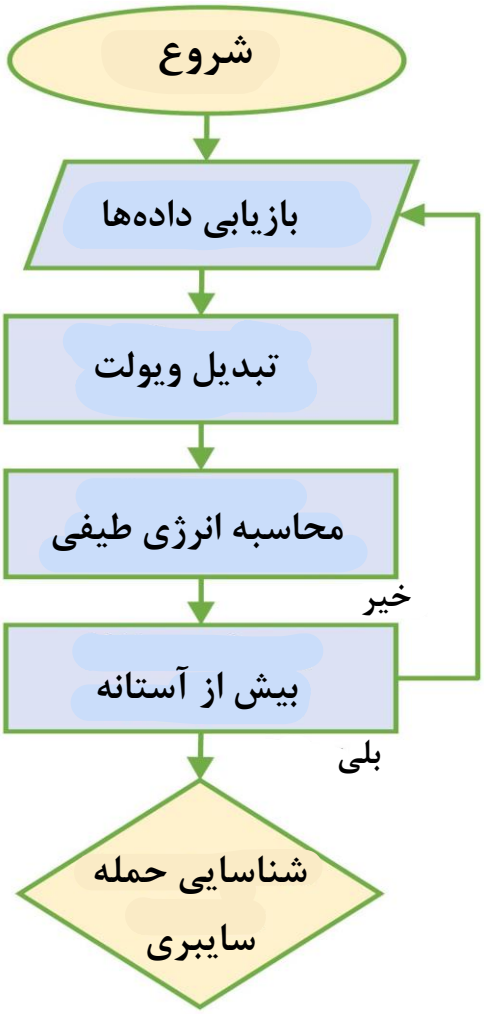
۳-۳- تحلیل روش‌های مبتنی بر بلاک‌چین

فناوری بلاک‌چین بر پایه دفتر کل توزیع‌شده‌ای عمل می‌کند که در آن، تراکنش‌ها به‌صورت شفاف، پی‌درپی و غیرقابل تغییر ثبت می‌شوند. این تراکنش‌ها در قالب بلوک‌هایی دسته‌بندی شده و از طریق شبکه‌ای غیرمتمرکز و همتا به همتا میان گره‌های مختلف بلاک‌چین منتشر می‌گردند [۲۳]. برای تضمین صحت و اعتبار بلوک بعدی، از مکانیزم اجماع بهره گرفته می‌شود. پس از اعتبارسنجی، بلوک به زنجیره بلاک‌چین اضافه شده و در میان تمام نودها پخش می‌گردد. هر شخص می‌تواند با نصب نرم‌افزار کلاینت روی رایانه شخصی خود ، به یک شبکه عمومی بلاک‌چین بپیوندد، یا از طریق دعوت‌نامه به یک شبکه بلاک‌چین خصوصی یا کنسرسیومی بپیوندد.

- در کاربردهای مرتبط با بازارهای انرژی، شرکت‌کنندگان اغلب کنسرسیومی را تشکیل می‌دهند که ساختار بلاک‌چین را به‌صورت یک سیستم نیمه‌خصوصی (کنسرسیومی) تعریف می‌کند. در این نوع، هیچ نهاد مرکزی به‌تنهایی بر کل فرآیند نظارت ندارد.

- بنیادهای انرژی، به‌عنوان یک نهاد جهانی، به بررسی و تحلیل پتانسیل فناوری پیشنهادی در بخش انرژی می‌پردازند. بلاک‌چین‌های کنسرسیومی که از الگوریتم اثبات اعتبار (PoA) استفاده می‌کنند، از نظر توان عملیاتی تراکنش و کاهش مصرف انرژی عملکرد بهتری دارند. الگوریتم PoA رقابت میان اعتبارسنج‌ها برای تولید بلوک را حذف می‌کند که این موضوع تأثیر قابل‌توجهی در کاهش مصرف انرژی دارد.

- در شبکه‌های برق، نهادهای تنظیم‌گر همواره نقش کلیدی دارند و ساختار آن‌ها با نوعی تمرکز همراه است. با ورود فناوری بلاک‌چین به عملیات آینده شبکه‌های قدرت، نقش تنظیم‌گرها نیازمند بازتعریف خواهد بود. با این حال، حضور آن‌ها به‌عنوان ارکان تصمیم‌گیر و نظارتی، چه به‌صورت مستقیم و چه غیرمستقیم، همچنان اجتناب‌ناپذیر باقی می‌ماند.



شکل ٦- نمودار جریان فرآیند شناسایی حمله تزریق داده غلط (FDIA) با استفاده از تبدیل موجک.

جدول ۲: پارامترهای ماشین بردار پشتیبان (SVM) و تبدیل موجک.

پارامتر	مقدار	توضیح
هایپرپارامترهای SVM		
تابع کرنل	تابع پایه شعاعی (RBF)	تابع نگاشت برای مدل SVM را تعیین می‌کند.
پارامتر تنظیم (C)	۱/۰	میزان مصالحه بین حداکثر margin و نرخ خطا را کنترل می‌کند.
گاما (Gamma)	۰/۱	میزان تأثیر هر نمونه آموزشی را مشخص می‌نماید.
حد تحمل	۰/۰۰۱	معیار توقف فرآیند بهینه‌سازی را تعیین می‌کند.

حداکثر تعداد تکرار	**۱۰۰۰**	**بیشینه تعداد تکرارها برای همگرایی را مشخص می‌نماید.**
پارامترهای تبدیل ویولت		
نوع موجک	**Daubechies (db4)**	**انتخاب شده به‌دلیل تعادل مناسب بین دقت زمانی و فرکانسی.**
سطح تجزیه	**۴**	**سطح تفکیک سیگنال را در تبدیل موجک مشخص می‌کند.**
تکنیک آستانه‌گذاری	**آستانه‌گذاری نرم**	**برای حذف نویز در حوزه موجک استفاده می‌شود.**
مقدار آستانه	**۰/۲**	**مقدار از پیش تعیین‌شده برای تفکیک نویز از سیگنال.**
فرکانس نمونه‌برداری	**۵۰۰ هرتز**	**دقت زمانی تبدیل موجک را تعیین می‌کند.**

در این تحقیق، تمرکز اصلی بر بهره‌گیری از شبکه بلاک‌چین به‌منظور اثبات و تحقق اهداف کلیدی در حوزه امنیت سایبری در شبکه‌های برق هوشمند است:

به طور گسترده پذیرفته شده است که شبکه‌های بلاک‌چین کنسرسیومی شامل میزانی از تمرکزگرایی هستند که ممکن است به عنوان یک محدودیت تلقی شود. با این حال، این ویژگی لزوماً یک نقطه ضعف محسوب نمی‌شود، به‌ویژه زمانی‌که در شبکه‌های برق اعمال می‌گردد، چرا که این شبکه‌ها به‌طور معمول تحت نظارت نهادهای متمرکز فعالیت می‌کنند. به عنوان نمونه، پروژه Hyperledger Fabric وابسته به بنیاد لینوکس و پلتفرم بلاک‌چین Azure متعلق به مایکروسافت، نمونه‌هایی از چارچوب‌های بلاک‌چین تثبیت‌شده هستند. افزون بر این، بلاک‌چین‌های کنسرسیومی مبتنی بر اتریوم به‌دلیل بهره‌مندی از جامعه کاربری گسترده و کاربردپذیری بالا، از جایگاه ویژه‌ای برخوردار هستند. ویژگی بارز اتریوم، زبان برنامه‌نویسی پیش‌فرض آن است که امکان تعریف قراردادهای هوشمند را فراهم می‌سازد؛ قراردادهایی که در آن‌ها قوانین مربوط به تراکنش‌ها، تغییر وضعیت‌ها و دیگر عملکردها مشخص می‌گردد.

۳-۴- چارچوب بلاک‌چین برای تبادل داده میان ISO و عامل‌های زیرمجموعه

در این پژوهش، چارچوبی نوین بر پایه بلاک‌چین ارائه شده است که به‌منظور رفع موانع موجود در مسیر انتقال قابل اعتماد داده‌ها بین عامل‌های تولید پراکنده (DG) و بارهای هوشمند یا حسگرها طراحی گردیده است. این

راهکار با تکیه بر یک پایگاه داده توزیع‌شده و امن، امکان انتشار یکپارچه و محافظت‌شده پیام‌ها را فراهم می‌سازد، به‌گونه‌ای که هر گره در سامانه قادر به دستیابی و مدیریت اطلاعات به‌صورت مستقل خواهد بود [۲۴]. نکته حائز اهمیت آن است که ساختار این بلاک‌چین به‌گونه‌ای طراحی شده که قابلیت نگهداری مجزا توسط هر کشور را داراست و این امر باعث افزایش سازگاری و بهره‌برداری عملی از آن می‌شود. با وجود افزایش توجه به بلاک‌چین در سال‌های اخیر، همچنان چالش‌های بنیادین این فناوری از پیچیدگی بالایی برخوردار بوده و نیازمند بررسی‌های عمیق‌تر هستند [۲۵].

جدول ۳: پارامترهای سیستم.

پارامتر	مقدار	واحد
پارامترهای سلول سوختی		
توان خروجی سلول سوختی	**۴۰۰۰**	**وات (۴ کیلووات)**
ولتاژ سلول سوختی	**۷۲**	**ولت**
پارامترهای سامانه فتوولتاییک (PV)		
حداکثر توان پنل خورشیدی	**۴۰۰۰**	**وات (۴ کیلووات پیک)**
حداکثر ولتاژ پنل خورشیدی	**۷۲**	**ولت**
حداکثر جریان پنل خورشیدی	**۵۶/۶۴**	**آمپر**
پارامترهای ابرخازن		
ظرفیت ابرخازن	**۲۰۸/۳**	**فاراد**
ولتاژ ابرخازن	**۷۲**	**ولت**
پارامترهای باتری		
ظرفیت باتری	**۲۴۰**	**آمپر ساعت**
ولتاژ باتری	**۷۲**	**ولت**

نسبت‌های مبدل		
نسبت مبدل دوجهته	**۳۶/۱۱۰**	**ولت/ولت**
نسبت مبدل بوست	**۴۵/۱۱۰**	**ولت/ولت**
ولتاژ مرجع نامی DC	**۳۱۵**	**ولت**
پارامترهای بار		
بار DC ثابت	**۲**	**کیلووات**
بار DC متغیر	**۵**	**کیلووات**

۳-۴-۱- فرضیات

در این پژوهش فرض شده است که عوامل تولید پراکنده (DGAs) و تجهیزات هوشمند شامل بارها و حسگرها، از ارتباط اینترنتی پایدار بهره‌مند هستند. هر عامل به تجهیزات لازم مانند حسگرها، سامانه موقعیت‌یاب جهانی (GPS) و واحد پردازش روی‌برد مجهز است. این عوامل که از توان پردازشی بالایی برخوردارند، به دو گروه اصلی تقسیم می‌شوند: گره‌های کامل که در فرآیند تحلیل و استخراج اطلاعات نقش مستقیم دارند، و گره‌های عادی که در ارسال داده‌ها و تأیید صحت آن‌ها مشارکت می‌کنند [۲۶]. همچنین در نظر گرفته شده که پیام‌های مربوط به رخدادهای حیاتی در محدوده‌ای جغرافیایی مشخص منتشر شده و از دید دیگر عوامل پنهان نمانده تا تمامی نودهای نزدیک به آن، امکان دریافت و واکنش سریع به پیام را داشته باشند.

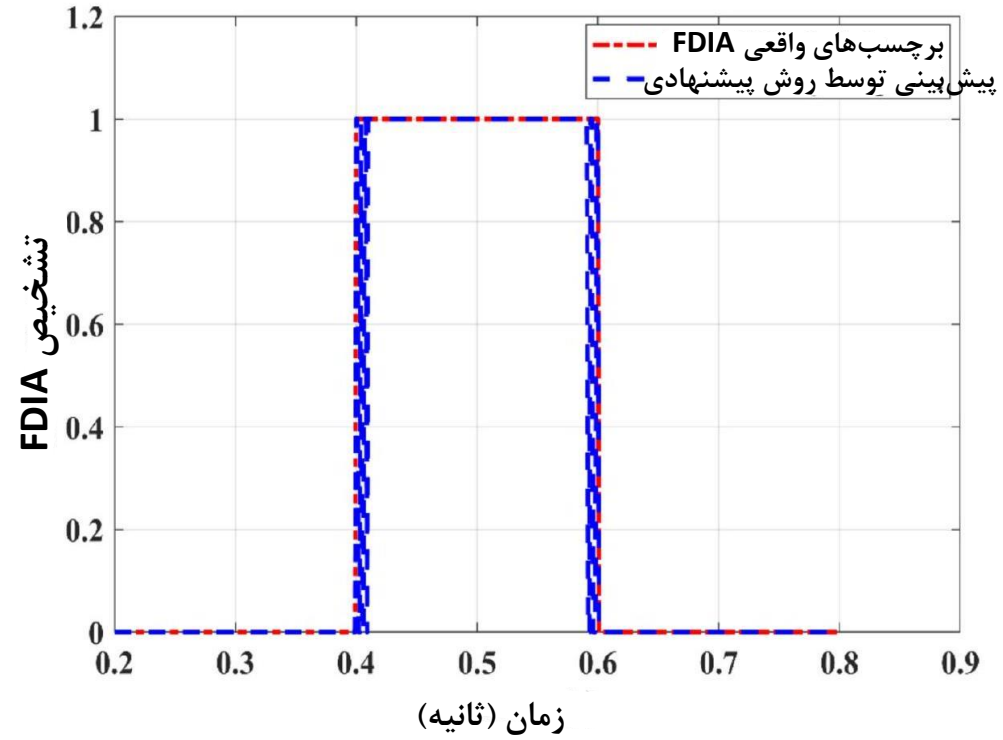
۳-۴-۲- سازوکار پیشنهادی بلاک‌چین برای انتقال داده بین ISO و عامل‌های زیرمجموعه

مکانیزم بلاک‌چین ارائه‌شده در این پژوهش با هدف ارتقای امنیت و اعتماد در فرآیند تبادل داده بین اپراتور مستقل سیستم (ISO) و سایر عوامل اجرایی در شبکه تولید پراکنده توسعه یافته است. این سامانه با تکیه بر دفترکل توزیع‌شده و غیرقابل تغییر، بستری فراهم می‌آورد که ارتباط میان ISO و واحدهای تولید برق، بارهای هوشمند و حسگرها به‌صورت ایمن، روان و بدون وابستگی به مرکز برقرار شود [۲۷]. تمامی پیام‌ها و داده‌های منتقل‌شده به‌صورت شفاف و بدون امکان دستکاری در بلاک‌چین ثبت می‌شوند و این امر، پاسخگویی و پیگیری دقیق اطلاعات را تضمین می‌کند. هر گره در شبکه بلاک‌چین، اعم از ISO یا عامل عملیاتی، در نگهداری بلاک‌چین، اعتبارسنجی تراکنش‌ها و تأیید صحت داده‌ها مشارکت دارد. در این سامانه، پیام‌های فوری و حساس نیز در محدوده‌های مکانی خاص منتشر شده و در دسترس کلیه گره‌های محلی قرار می‌گیرند تا در مواقع بحرانی واکنش سریع و هماهنگی لازم برقرار شود [۲۸]. این ویژگی، انتشار به‌موقع اطلاعات مهم و واکنش سریع به مسائل یا

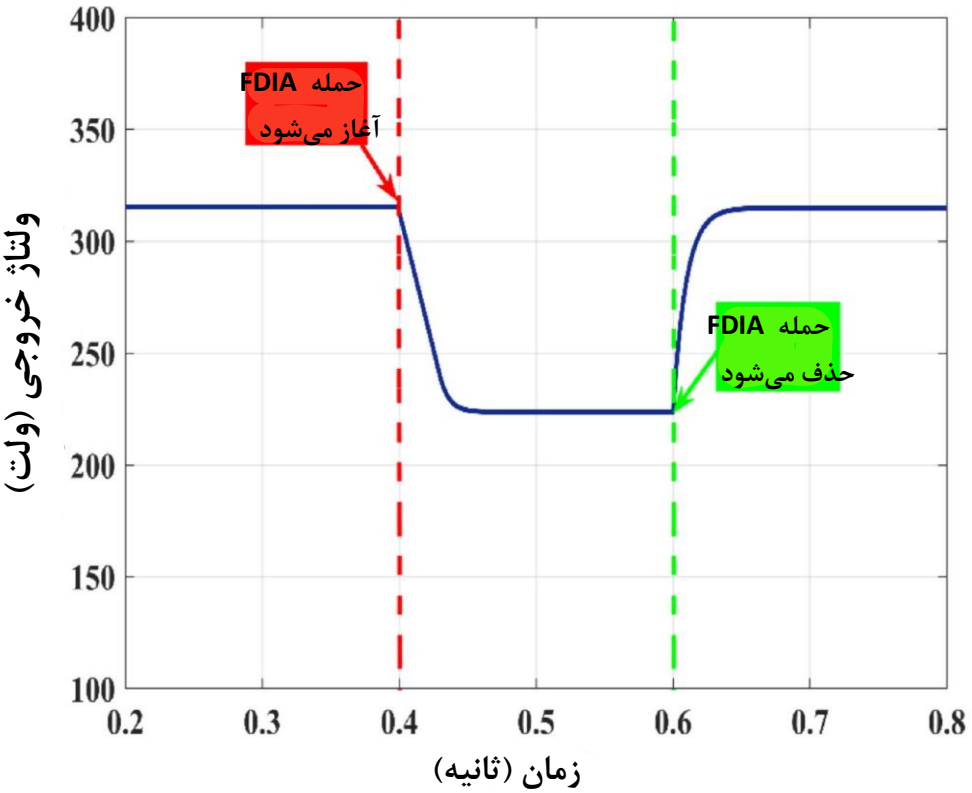
تغییرات عملیاتی را امکان‌پذیر می‌سازد. با استفاده از فناوری بلاک‌چین، این سیستم چارچوبی قدرتمند برای تبادل امن و کارآمد داده فراهم می‌کند که خطر نشت اطلاعات را کاهش داده و قابلیت اطمینان عملیاتی را افزایش می‌دهد. افزون بر این، ماهیت غیرمتمرکز بلاک‌چین به هر عامل مشارکت‌کننده امکان می‌دهد تا به‌طور مستقل داده‌ها را مدیریت و اعتبارسنجی کند که این موضوع تاب‌آوری سیستم را بهبود بخشیده و وابستگی به نهادهای متمرکز را کاهش می‌دهد [۲۹].

۴- نتایج و بحث‌ها

در این پژوهش، سیستمی متشکل از دو ریزشبکه جریان مستقیم (DC) به‌هم‌پیوسته مورد بررسی قرار گرفته است. هر ریزشبکه شامل سامانه تولید برق خورشیدی (PV)، پیل سوختی با پشتیبانی ذخیره‌ساز باتری و یک ابرخازن است که در قالب یک سامانه ترکیبی ذخیره انرژی (HESS) با بارها و مبدل‌های قابل کنترل یکپارچه شده‌اندHESS نقش حیاتی در تضمین پایداری عملکردی سیستم ایفا می‌کند؛ چرا که از طریق تنظیم دقیق فرآیندهای ذخیره و مصرف انرژی، پاسخگوی نیازهای عملیاتی ریزشبکه‌هاست. در این میان، ابرخازن نیز به دلیل توانایی ارائه چگالی انرژی بالا در زمان کوتاه، به‌ویژه در شرایط گذرا و بحرانی بسیار مؤثر عمل می‌کند. هر دو منبع انرژی پیل سوختی و سامانه PV از طریق مبدل بوست (boost converter) به باس متصل شده‌اند، در حالی‌که باتری‌ها و ابرخازن از طریق مبدل DC-DC متصل می‌گردند. افزون بر این، رویکردی مبتنی بر رایانش ابری اتخاذ شده است که طی آن، داده‌های سیستم به سرور ابری ارسال می‌شود تا مورد تحلیل قرار گیرد. این داده‌ها به سرور ابری ارسال شده و پس از تحلیل، منابع انرژی با بهره‌وری بالا بین کنترل‌کننده‌های محلی توزیع می‌شود؛ رویکردی که منجر به مدیریت هوشمند و یکپارچه انرژی در سطح ریزشبکه‌ها می‌گردد.



شکل ۷- تحلیل عملکرد سیستم در شناسایی حمله تزریق داده نادرست (FDIA).



شکل ۸. بررسی تغییرات ولتاژ خروجی در حضور حمله FDIA.

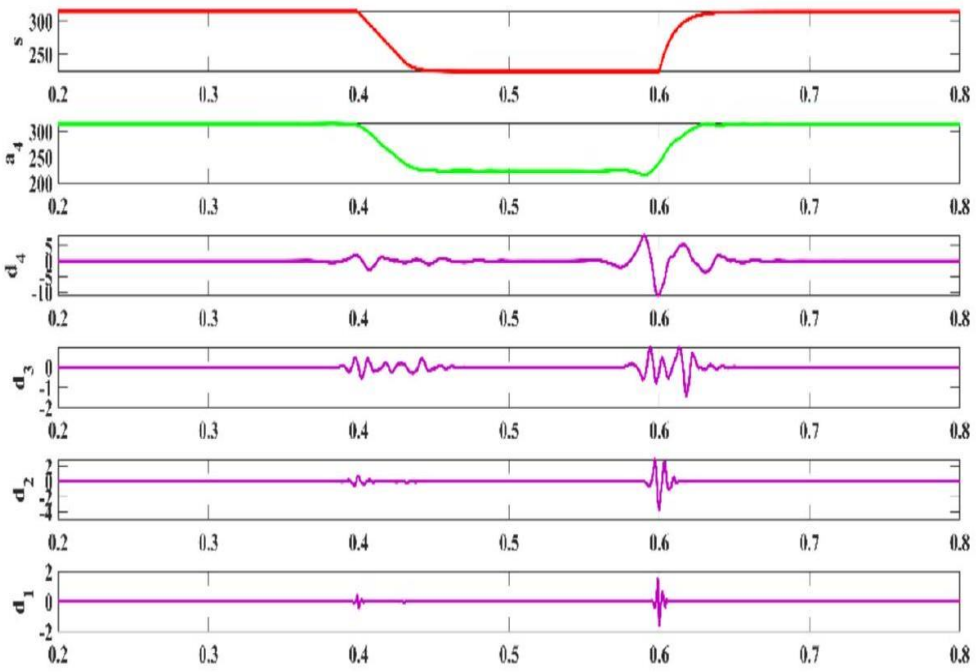
۴-۱- نتایج شبیه‌سازی

جدول ۳ به‌طور دقیق پارامترهای اصلی یک سامانه ترکیبی انرژی شامل پیل سوختی، آرایه خورشیدی (PV)، ابرخازن و باتری را تشریح می‌کند. توان نامی پیل سوختی و آرایه PV هر دو برابر با ۴۰۰۰ وات (۴ کیلووات) و ولتاژ آن‌ها ۷۲ ولت است که نشان‌دهنده هم‌ترازی در ظرفیت تولید توان آن‌هاست.

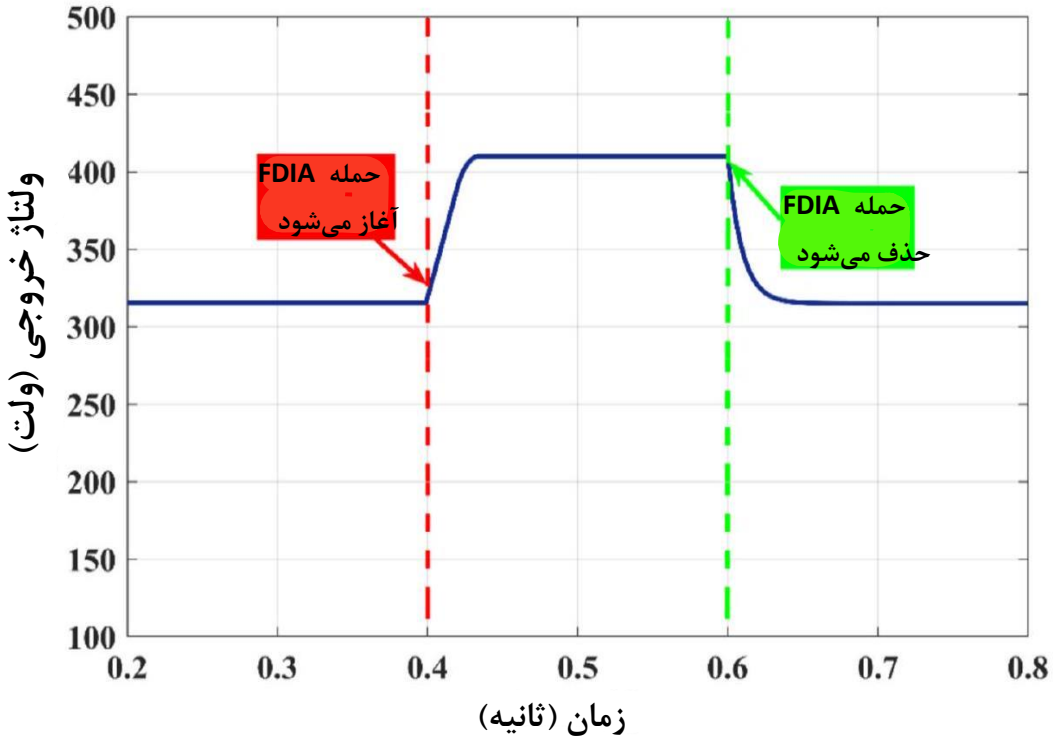
سیستم PV قابلیت تأمین جریان لحظه‌ای (پیک جریان) معادل ۵۶/۶۴ آمپر را داراست. ابرخازن با ظرفیت ۲۰۸/۳ فاراد و ولتاژ ۷۲ ولت، به‌منظور پاسخ‌دهی سریع در شرایط گذرا به کار گرفته شده، در حالی‌که باتری با ظرفیت بالای ۲۴۰ آمپرساعت در همان ولتاژ، نقش ذخیره‌سازی انرژی در بازه‌های زمانی طولانی‌تر را بر عهده دارد. مدیریت تبدیل توان توسط یک مبدل دوسویه با نسبت تبدیل ۳۶/۱۱۰ و یک مبدل بوست با نسبت ۴۵/۱۱۰ انجام می‌شود که تنظیم بهینه توان را تضمین می‌کند. ولتاژ مرجع نامی در این سیستم برابر با ۳۱۵ ولت در نظر گرفته شده است. این ساختار توانایی تأمین بار ثابت ۲۰۰۰ وات و نیز بار متغیر تا سقف ۵۰۰۰ وات را دارد و لذا برای پاسخگویی به تقاضاهای متغیر انرژی در محیط‌های دینامیک بسیار کارآمد است.

۴-۱-۱- تحلیل سناریو حالت اول

در شکل ۷ فرآیند شناسایی حملات تزریق داده نادرست (FDIA) در ریزشبکه DC هوشمند با بهره‌گیری از رویکردهای پیشرفته امنیت سایبری به تصویر کشیده شده است. محور افقی، زمان را بر حسب ثانیه نشان می‌دهد که طی آن سامانه به‌طور مداوم عملکرد خود را در شناسایی حمله‌ها ارزیابی می‌کند؛ در حالی‌که محور عمودی نشان‌دهنده میزان موفقیت در شناسایی، از مقدار صفر تا یک است که مقدار یک بیانگر شناسایی کامل حمله است.



شکل ۹- تحلیل هم‌زمان ولتاژ خروجی و ضرایب تبدیل موجک در طول حمله.

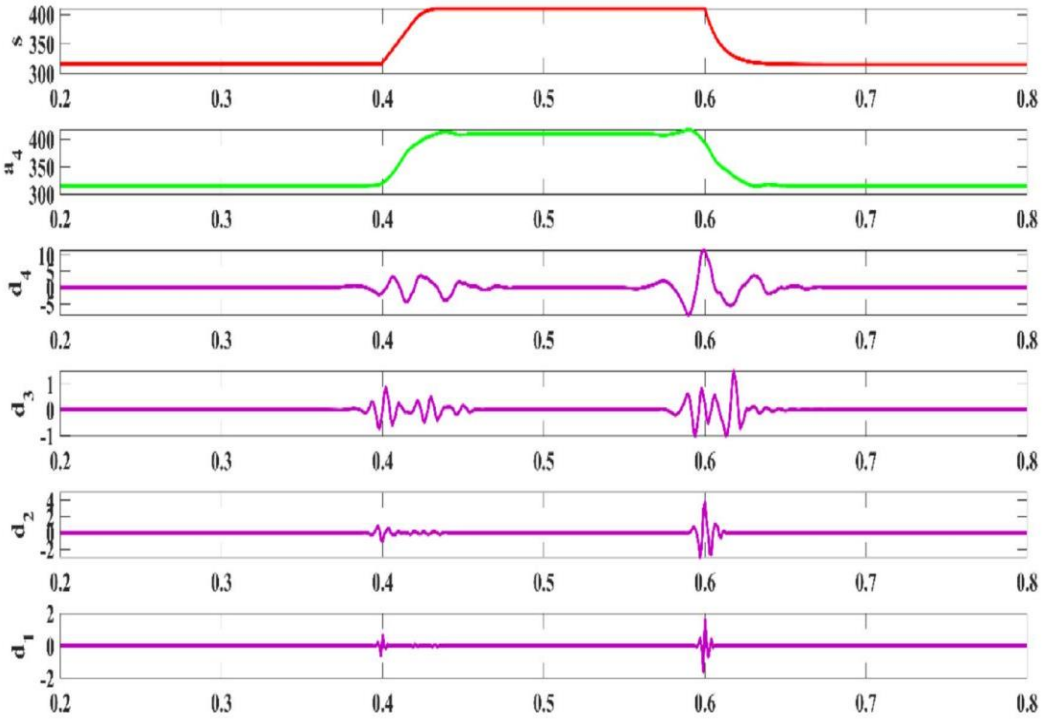


شکل ۱۰- تأثیر حمله تزریق تشخیص غلط بر ولتاژ خروجی سیستم.

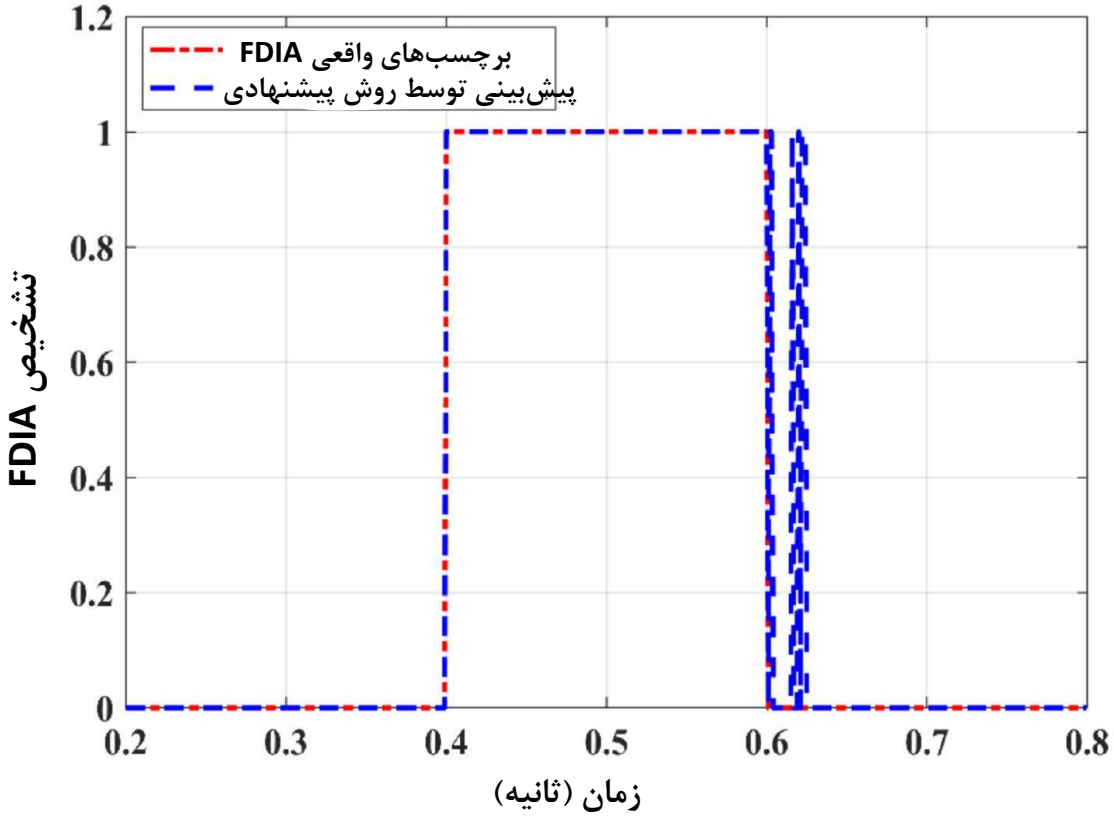
رویکرد ارائه‌شده با ترکیب فناوری بلاک‌چین، تبدیل موجک و الگوریتم ماشین بردار پشتیبان (SVM)، سطح بالایی از محافظت سایبری را فراهم می‌سازد. انطباق نزدیک بین خطوط قرمز و آبی در بازه‌های وقوع حمله، دقت و قابلیت اعتماد بالای روش پیشنهادی را در شناسایی آنی حملات FDIA نشان می‌دهد. این همبستگی قوی بیانگر توانمندی روش ارائه‌شده در حفظ یکپارچگی و پایداری ریزشبکه‌های DC هوشمند در برابر حملات سایبری است؛ به‌گونه‌ای که موجب کاهش اختلالات عملکردی و افزایش امنیت کلی سیستم می‌شود.

شکل ۸ روند تغییرات ولتاژ خروجی سیستم را در واکنش به اجرای الگوریتم تشخیص و جداسازی خطا (FDIA) در طول زمان ترسیم می‌کند. محور افقی زمان را بر حسب ثانیه و محور عمودی ولتاژ خروجی را بر حسب ولت نمایش می‌دهد. در زمان ۰ = t، ولتاژ خروجی در مقدار پایدار تقریباً ۳۵۰ ولت قرار دارد. در لحظه ۰.٤ = t، که با یک خط چین قرمز مشخص شده است، الگوریتم FDIA فعال می‌شود و منجر به کاهش ناگهانی ولتاژ تا سطح ثابتی در حدود ۳۰۰ ولت می‌شود. این افت نشان‌دهنده عملکرد مؤثر الگوریتم در شناسایی و ایزوله‌سازی خطاست. اختلاف ولتاژ ایجادشده تقریباً ۵۰ ولت است. ولتاژ در این سطح پایین تا زمان ۰.۷ s = t پایدار باقی می‌ماند؛ در این لحظه، حذف FDIA که با خط چین سبز نشان داده شده، صورت می‌گیرد. پس از حذف آن، ولتاژ خروجی به‌تدریج افزایش یافته و طی تقریباً ۰.۱ ثانیه به مقدار اولیه ۳۵۰ ولت بازمی‌گردد.

شکل ۹ نمودار چندبخشی از رفتار زمانی متغیرهای مختلف سیستم را ارائه می‌دهد که در آن، محور افقی زمان (بر حسب ثانیه) و محور عمودی تغییرات متغیرهای مختلف سیستم را نشان می‌دهد. در پنل بالایی، ولتاژ خروجی در ابتدا در مقدار ثابت ۳۵۰ ولت قرار دارد. در لحظه ۰.۴ ثانیه و با شروع FDIA، این ولتاژ به‌طور ناگهانی به حدود ۳۰۰ ولت کاهش می‌یابد. پس از حذف FDIA در ۰/۷ ثانیه، ولتاژ به‌تدریج بازیابی شده و مجدداً به سطح ۳۵۰ ولت بازمی‌گردد. در پنل دوم، متغیر a در سطح پایداری حدود ۲۵۰ ولت حفظ می‌شود و نوسانات ناچیزی را نشان می‌دهد که بیانگر ثبات عملکردی این بخش از سیستم است. پنل سوم، متغیر d_1 را با نوسانات شدید در لحظه فعال‌سازی FDIA نمایش می‌دهد که احتمالاً ناشی از پاسخ گذرای سیستم به آشفتگی است. متغیر d_2 نیز در پنل چهارم رفتار مشابهی را از خود نشان می‌دهد که وجود تداخلات و واکنش دینامیکی سیستم در شرایط خطا را تأیید می‌کند. پنل پنجم، متغیر d_3 را نمایش می‌دهد که نوسانات ملایم‌تری نسبت به d_1 و d_2 دارد و نشان‌دهنده پاسخ پایدارتری است که ممکن است ناشی از عملکرد حلقه‌های کنترلی یا مکانیزم‌های فیدبک باشد. نهایتاً، پنل ششم که متغیر d_4 را نشان می‌دهد، تقریباً بدون تغییر باقی می‌ماند و فعالیت قابل‌توجهی در آن مشاهده نمی‌شود که این امر حاکی از وضعیت پایدار یا حساسیت کم آن نسبت به تغییرات ناشی از FDIA است. در مجموع، این نمودار چندبخشی، واکنش سیستم به فعال‌سازی و حذف FDIA را به‌خوبی به تصویر می‌کشد و سطوح مختلفی از پایداری و نوسان را در میان متغیرهای مختلف نشان می‌دهد؛ در این میان، تغییرات ولتاژ خروجی در پنل بالایی بیشترین توجه را به خود جلب می‌کند.



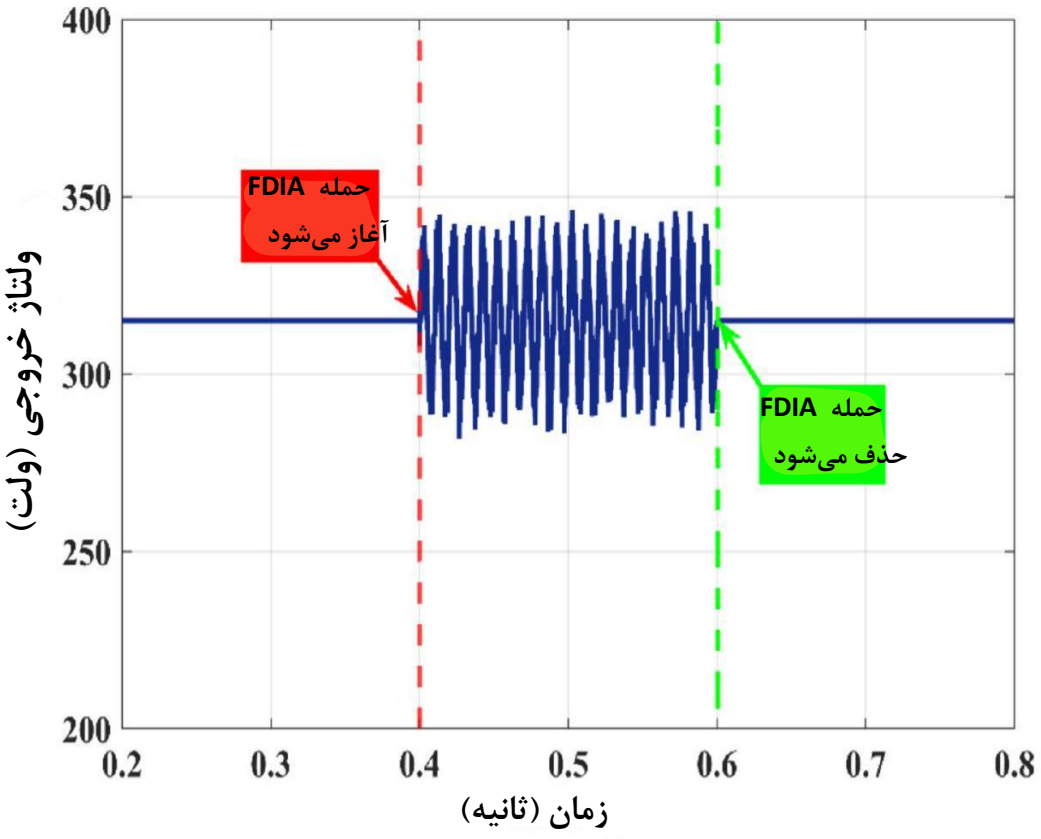
شکل ۱۱- بررسی پاسخ دینامیکی سیستم به حمله FDIA.



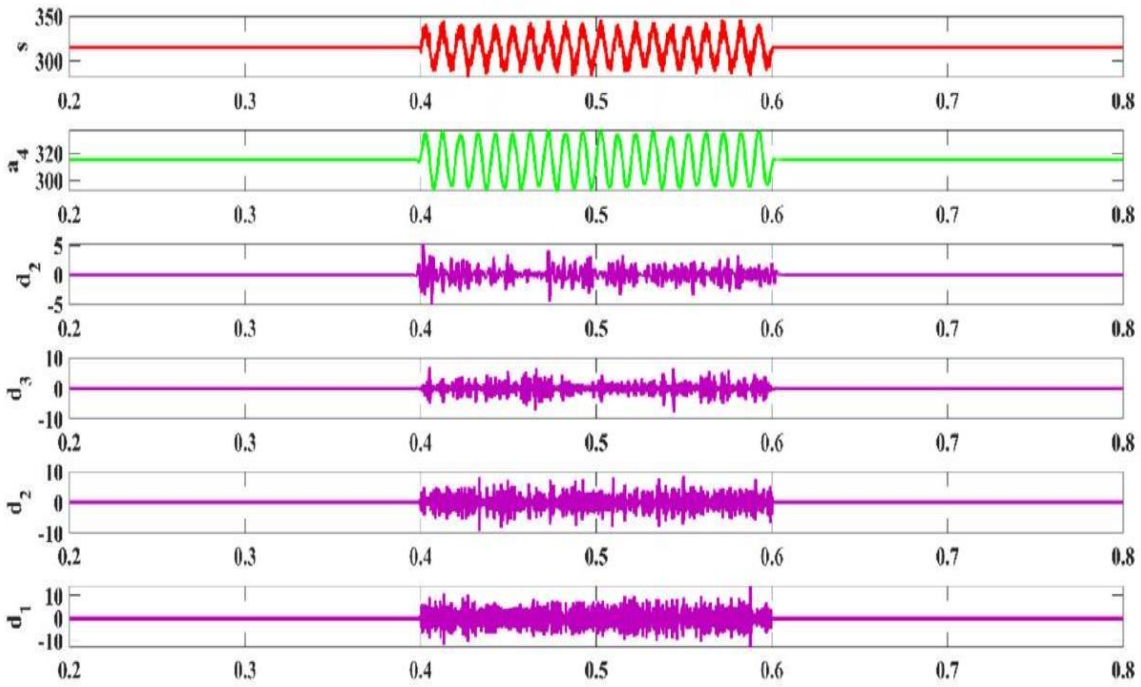
شکل ۱۲- مقایسه روش پیشنهادی و روش واقعی در تشخیص حمله FDIA.

۴-۱-۲- تحلیل سناریو حالت دوم

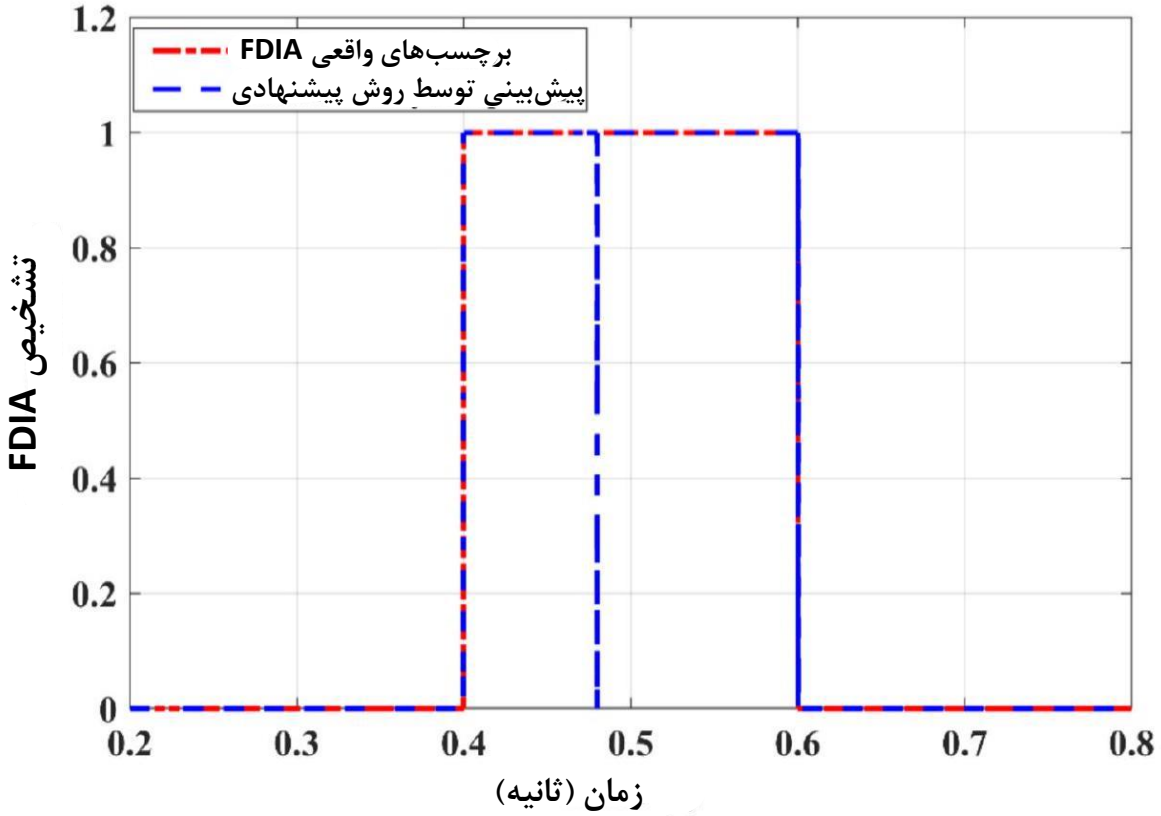
شکل ۱۰ تأثیر حمله FDIA را بر ولتاژ خروجی در طول زمان نشان می‌دهد و نمای دقیقی از مراحل کلیدی آن ارائه می‌دهد. در مرحله ابتدایی، از زمان ۰/۲ تا ۰/۴ ثانیه، ولتاژ خروجی در حدود ۳۰۰ ولت پایدار باقی می‌ماند که نشان‌دهنده وضعیت پایدار سیستم پیش از حمله است. در لحظه ۰/۴ ثانیه، هم‌زمان با شروع حمله FDIA که با خط‌چین قرمز مشخص شده، ولتاژ خروجی به‌طور ناگهانی به مقدار ۳۵۰ ولت افزایش می‌یابد. این افزایش نشان‌دهنده تأثیر مستقیم حمله بر داده‌های کنترلی سیستم است. طی بازه زمانی ۰/۴ تا ۰/۶ ثانیه، ولتاژ در این سطح بالا تثبیت شده باقی می‌ماند و نمایانگر تداوم اثر حمله است. با حذف FDIA در زمان ۰/۶ ثانیه، که با خط‌چین سبز نمایش داده شده، روند کاهش تدریجی ولتاژ آغاز می‌شود. در فاصله ۰/۷ تا ۰/۸ ثانیه، ولتاژ بار دیگر به سطح اولیه ۳۰۰ ولت بازمی‌گردد و سیستم به وضعیت پایدار قبل از حمله بازمی‌گردد. این روند بازیابی موفقیت‌آمیز بیانگر اثربخشی الگوریتم شناسایی و ایزوله‌سازی خطا در بازگرداندن پایداری سیستم است.



شکل ۱۳- بررسی اثرات حمله FDIA بر ولتاژ خروجی سیستم.



شکل ۱۴- تحلیل سیگنال های سیستم در طول تزریق تشخیص نادرست.



شکل ۱۵- ارزیابی عملکرد تشخیص حمله FDIA.

شکل ۱۱ مجموعه‌ای از زیرنمودارها را شامل می‌شود که تغییرات خروجی‌های سیستم در مواجهه با حمله تزریق داده نادرست (FDIA) را در طول زمان نمایش می‌دهد. در زیرنمودار مربوط به سیگنال خروجی (S)، سیستم بین زمان‌های ۰/۲ تا ۰/۴ ثانیه ولتاژی پایدار نزدیک به ۳۰۰ ولت را حفظ می‌کند. هم‌زمان با آغاز FDIA در زمان تقریبی ۰/۴ ثانیه، ولتاژ به‌طور چشمگیری افزایش یافته و به حدود ۴۰۰ ولت می‌رسد. با حذف حمله در زمان ۰/۶ ثانیه، ولتاژ به مقدار اولیه‌ی خود، یعنی حدود ۳۰۰ ولت بازمی‌گردد و نشان‌دهنده بازیابی پایداری سیستم است. در نمودار مربوط به سیگنال کنترلی (a_4)، ولتاژ در بازه‌ی آغازین (۰/۲ تا ۰/۴ ثانیه) در مقدار ثابت ۳۵۰ ولت باقی مانده و تنها اندکی در زمان اجرای حمله واکنش نشان می‌دهد؛ سپس در پایان حمله، در همان زمان ۰/۶ ثانیه، مجدداً به حالت پایدار خود بازمی‌گردد.

شکل ۱۲ تشخیص حمله تزریق داده نادرست (FDIA) را در طول زمان نمایش می‌دهد و بر مقایسه بین برچسب‌های واقعی حمله و مقادیر پیش‌بینی‌شده توسط روش پیشنهادی تمرکز دارد. در بازه‌ی زمانی ۰/۲ تا ۰/۴ ثانیه، هر دو مقدار واقعی و پیش‌بینی‌شده برابر با صفر باقی می‌مانند که به‌درستی نشان می‌دهد حمله‌ای در این بازه وجود ندارد. در زمان آغاز حمله، یعنی در ۰/۴ ثانیه، مقدار برچسب واقعی به عدد یک تغییر می‌کند که نشان‌دهنده وقوع حمله است و مقدار پیش‌بینی‌شده نیز به‌درستی از آن پیروی می‌کند که مؤید شناسایی موفق حمله می‌باشد.

در مدت وقوع حمله (۰/۴ تا ۰/۶ ثانیه)، هر دو مقدار در سطح یک باقی می‌مانند و سازگاری بین آن‌ها دقت بالای تشخیص روش پیشنهادی را نشان می‌دهد. با پایان یافتن حمله در ۰/۶ ثانیه، برچسب واقعی به صفر بازمی‌گردد و مقدار پیش‌بینی‌شده نیز بلافاصله هماهنگ می‌شود که توانایی سیستم در تشخیص پایان حمله را تأیید می‌کند. در ادامه و از زمان ۰/۶ تا ۰/۸ ثانیه، هر دو مقدار در صفر باقی می‌مانند و تأیید می‌کنند که سیستم حمله جدیدی را مشاهده نکرده و شرایط پایدار حفظ شده است.

۴-۱-۳- *تحلیل سناریو حالت سوم*

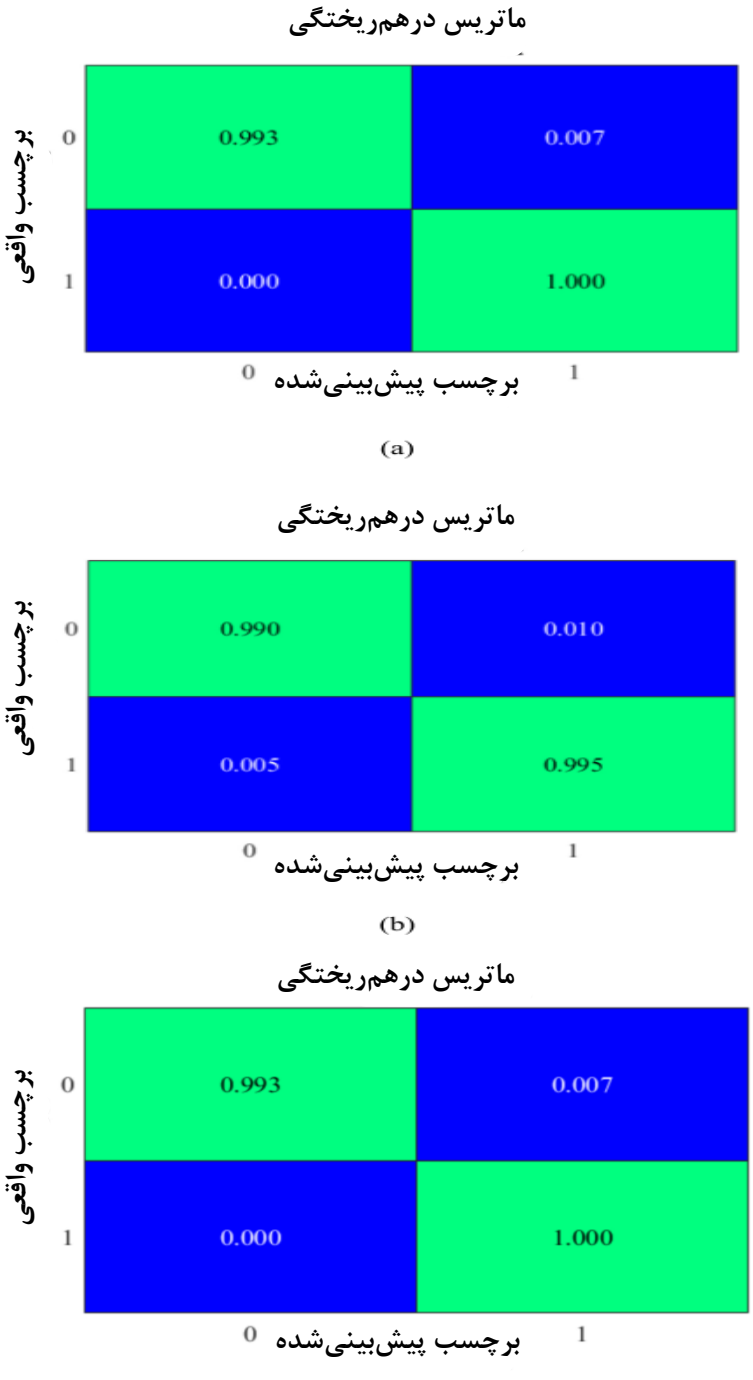
شکل ۱۳ تغییرات ولتاژ خروجی سیستم را در واکنش به حمله‌ی تزریق داده نادرست (FDIA) در طول زمان نمایش می‌دهد. در گام ابتدایی، یعنی از ۰/۲ تا ۰/۴ ثانیه، ولتاژ خروجی در حدود ۳۰۰ ولت ثابت است که بیانگر عملکرد عادی و بدون اختلال سیستم می‌باشد. در لحظه ۰/۴ ثانیه، با شروع حمله، ولتاژ خروجی با یک افزایش ناگهانی تا حدود ۳۵۰ ولت مواجه می‌شود. به‌دنبال آغاز حمله، سیستم وارد فاز ناپایداری می‌شود و ولتاژ خروجی دچار نوسانات قابل‌توجهی بین ۳۰۰ تا ۳۵۰ ولت می‌شود. در ادامه، از ۰/۴ تا ۰/۶ ثانیه، نوسانات شدت بیشتری یافته و دامنه آن‌ها به‌سرعت بین ۲۰۰ تا ۳۵۰ ولت تغییر می‌کند که حاکی از اختلال شدید در سیستم است. با حذف حمله در زمان ۰/۶ ثانیه، روند نوسانات کاهش یافته و ولتاژ به تدریج به سطح اولیه‌ی ۳۰۰ ولت بازمی‌گردد. پس از این زمان، سیستم مجدداً به وضعیت پایدار بازمی‌گردد و عملکرد عادی خود را بازیابی می‌کند.

شکل ۱۴ روند تغییر سیگنال‌های متاثر از حمله‌ی تزریق داده نادرست (FDIA) را در طول زمان و از طریق چند نمودار مجزا ارائه می‌دهد. سیگنال خروجی (s) در مرحله‌ی ابتدایی، یعنی بین ۰/۲ تا ۰/۴ ثانیه، رفتار پایداری از خود نشان داده و مقدار آن در حدود ۳۰۰ ولت ثابت است. با آغاز حمله در زمان ۰/۴ ثانیه، سیگنال به‌طور محسوس دچار نوسان شده و مقدار آن تا حدود ۳۵۰ ولت افزایش می‌یابد. در بازه‌ی ۰/۶ تا ۰/۸ ثانیه، با وجود حذف حمله، نوسانات همچنان ادامه دارد ولی سرانجام سیگنال به مقدار اولیه‌ی ۳۰۰ ولت بازمی‌گردد و به پایداری می‌رسد. سیگنال کنترلی a_4 نیز در فاز پیش از حمله در حدود ۳۲۰ ولت قرار دارد و تغییرات جزئی را تجربه می‌کند. با شروع FDIA، این سیگنال نیز دچار نوسانات شدید می‌شود که نشانه‌ی واکنش ناپایدار سیستم به حمله است. پس از اتمام حمله، سیگنال کنترل به‌تدریج پایدار شده و به مقدار اولیه‌ی خود، یعنی نزدیک به ۳۲۰ ولت، بازمی‌گردد که بیانگر بازگشت سیستم به عملکرد عادی است.

شکل ۱۵ روند زمانی مقایسه میان برچسب‌های واقعی حمله‌ی FDIA و مقادیر پیش‌بینی‌شده توسط روش پیشنهادی را نمایش می‌دهد. در این نمودار، برچسب‌های واقعی لحظات دقیق وقوع حمله را نشان می‌دهند و مقادیر پیش‌بینی‌شده عملکرد الگوریتم تشخیص را ارزیابی می‌کنند. همخوانی کامل بین این دو، مؤثر بودن روش پیشنهادی در شناسایی حملات را تأیید می‌نماید. در بازه‌ی زمانی ۰/۲ تا ۰/۴ ثانیه، هر دو مقدار در سطح صفر قرار دارند که به‌درستی نشان‌دهنده‌ی عدم وقوع حمله است. با شروع FDIA در ۰/۴ ثانیه، مقدار واقعی به ۱ جهش می‌یابد و سیستم پیشنهادی نیز بلافاصله این مقدار پیش‌بینی‌شده را به ۱ افزایش می‌دهد، که بیانگر عملکرد دقیق الگوریتم در شناسایی شروع حمله است. در طول مدت حمله، از ۰/۴ تا ۰/۶ ثانیه، هر دو مقدار بدون تغییر در مقدار ۱ باقی می‌مانند و دقت پایداری را در طول مدت حمله نمایش می‌دهند. پس از خاتمه‌ی حمله در ۰/۶ ثانیه، مقدار واقعی مجدداً به صفر بازمی‌گردد و مقدار پیش‌بینی نیز با اندکی تأخیر، کاهش یافته و به صفر می‌رسد. این رفتار نشان‌دهنده‌ی توانایی الگوریتم در تشخیص به‌موقع پایان حمله است. در مرحله‌ی بعد از حمله، یعنی بین ۰/۶ تا ۰/۸ ثانیه، هر دو مقدار صفر باقی می‌مانند و عدم وجود حمله به‌درستی تأیید می‌شود.

در شکل ۱۶، ماتریس‌های درهم‌ریختگی (Confusion Matrices) مربوط به سه مدل طبقه‌بندی دودویی ارائه شده است که برای ارزیابی دقت عملکرد مدل‌ها در تشخیص صحیح نمونه‌ها به‌کار رفته‌اند. این ماتریس‌ها عملکرد مدل‌ها را از نظر برچسب‌های واقعی و پیش‌بینی‌شده نمایش می‌دهند؛ در این ماتریس‌ها، خانه‌های روی قطر اصلی معرف نمونه‌هایی هستند که به‌درستی شناسایی شده‌اند، در حالی که خانه‌های خارج از قطر بیانگر مواردی هستند که به اشتباه طبقه‌بندی شده‌اند. زیرشکل (الف) نتایج مدل اول را نمایش می‌دهد که توانسته نرخ تشخیص درست نمونه‌های مثبت (TPR) را به‌طور کامل (۱/۰۰۰) و نرخ تشخیص نمونه‌های منفی (TNR) را با دقت بسیار بالا (۰/۹۹۳) حاصل کند؛ به‌گونه‌ای که تنها درصد اندکی از موارد به اشتباه مثبت تشخیص داده شده‌اند (۰/۰۰۷). زیرشکل (ب) مربوط به مدل دوم است که نرخ TNR آن اندکی کمتر و برابر با ۰/۹۹۰ و TPR آن معادل ۰/۹۹۵ است؛ این مقادیر نشان‌دهنده‌ی افزایش جزئی در نرخ خطاهای مثبت و منفی کاذب (مثبت کاذب: ۰/۰۱۰ و منفی کاذب: ۰/۰۰۵) هستند. ماتریس ترکیبی (شکل پایین) عملکرد کلی سیستم را با تجمیع نتایج نمایش می‌دهد که

در آن نرخ TNR همچنان برابر با ۰/۹۹۳ و نرخ TPR معادل ۱/۰۰۰ باقی می‌ماند؛ این مقادیر حاکی از پایداری و کارایی بالای روش پیشنهادی هستند. این ماتریس‌ها دقت و قابلیت اطمینان مدل‌ها را در تفکیک دو کلاس به‌خوبی نمایان می‌سازند.



شکل ۱۶- ماتریس آشفتگی مدل های پیشنهادی طبقه‌بندی FDIAدر سه سناریوی مورد بررسی.

۴-۲- تحلیل شاخص‌های عملکرد برای سناریوهای مختلف

شکل ۱۷ به بررسی و مقایسه عملکرد چهار الگوریتم یادگیری ماشین شامل جنگل تصادفی (RF)، شبکه عصبی مصنوعی (ANN)، بیز ساده (NB) و ماشین بردار پشتیبان (SVM) می‌پردازد که براساس چهار شاخص کلیدی دقت کلی (accuracy)، دقت مثبت (precision)، یادآوری (recall) و امتیاز F۱ ارزیابی شده‌اند. نتایج این ارزیابی در قالب سه زیرشکل (الف)، (ب) و (ج) برای سه مجموعه‌داده یا شرایط آزمایشی مختلف ارائه شده‌اند. در زیرشکل (الف)، الگوریتم SVM در تمامی شاخص‌ها بهترین عملکرد را دارد که نشان‌دهنده توانایی بالای آن در طبقه‌بندی دقیق در آن مجموعه‌داده است، در حالی که الگوریتم RF عملکرد ضعیف‌تری ارائه داده است. زیرشکل (ب) نشان می‌دهد که ANN و SVM به‌طور تقریباً برابر عمل می‌کنند؛ به‌ویژه ANN در شاخص‌های دقت (precision) و یادآوری (recall) نسبت به SVM عملکرد بهتری داشته، ولی RF و NB در این سناریو از نظر شاخص‌های یادآوری و امتیاز F۱ عملکرد ضعیف‌تری دارند. در نهایت، زیرشکل (ج) که نمایی کلی از نتایج ارائه می‌دهد، نشان می‌دهد که SVM در تمامی شاخص‌های ارزیابی عملکرد، بالاترین سطح دقت را حفظ کرده است. پس از آن، ANN در رده دوم قرار می‌گیرد، و دو الگوریتم NB و RF عملکرد مشابه اما پایین‌تری، به‌ویژه در معیار یادآوری، دارند.

در شکل ۱۸، منحنی‌های ROC مربوط به چهار الگوریتم طبقه‌بندی یعنی جنگل تصادفی (RF)، شبکه عصبی مصنوعی (ANN)، بیز ساده (NB) و ماشین بردار پشتیبان (SVM) به تصویر کشیده شده‌اند. منحنی ROC نمایانگر موازنه میان نرخ مثبت صحیح (TPR) و نرخ مثبت کاذب (FPR) برای هر مدل است و عملکرد تفکیک‌پذیری آن‌ها را به‌خوبی نمایش می‌دهد. الگوریتم‌های SVM و ANN با قرارگیری نزدیک به نقطه مطلوب گوشه بالا-چپ نمودار، بالاترین سطح دقت و کمترین خطای ممکن را ارائه می‌دهند. در مقابل، الگوریتم NB که با منحنی سبزرنگ نشان داده شده، اندکی از نظر عملکرد پایین‌تر است، و RF با قرار گرفتن در نزدیکی خط قطری (نمایانگر طبقه‌بندی تصادفی)، ضعیف‌ترین عملکرد را دارد. این تحلیل، SVM را به‌عنوان دقیق‌ترین مدل در شناسایی درست کلاس‌ها معرفی می‌کند و ANN نیز با فاصله‌ای اندک در جایگاه بعدی قرار می‌گیرد. NB و RF در مقایسه با این دو، کارایی پایین‌تری دارند. منحنی‌های ROC به‌طور مؤثری توانایی مدل‌ها در تمایز بین کلاس‌ها را نشان می‌دهند و مساحت زیر این منحنی‌ها (AUC) معیار مناسبی برای ارزیابی نهایی عملکرد آن‌ها به شمار می‌رود.

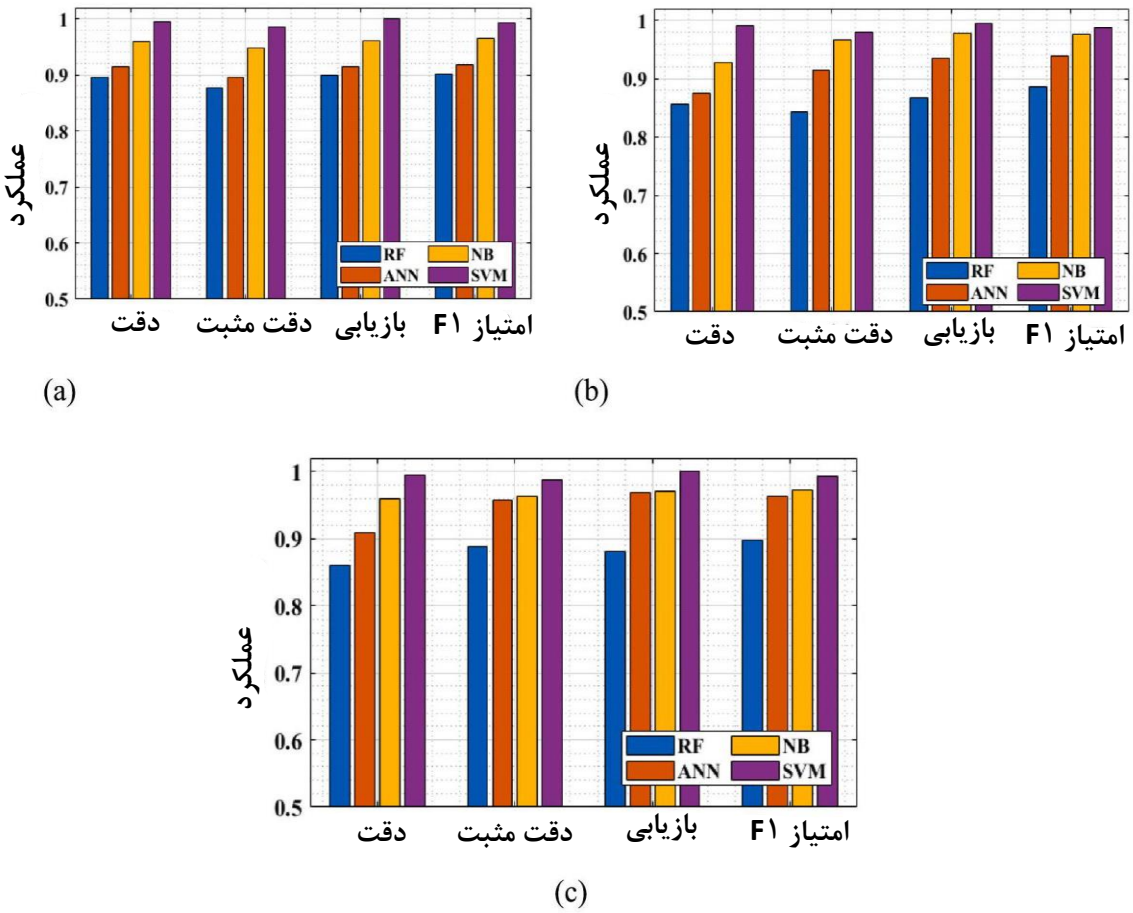
۴-۳- نتایج و پیامدها

این پژوهش گام مهمی در ارتقاء شناسایی و کنترل حملات تزریق داده نادرست (FDIA) در ریزشبکه‌های DC هوشمند برداشته است. ترکیب راهکارهای پیشرفته امنیت سایبری نظیر فناوری بلاک‌چین، تبدیل موجک، و الگوریتم SVM، دقت سامانه در تشخیص حملات را به‌طور چشمگیری افزایش داده است. انطباق دقیق بین

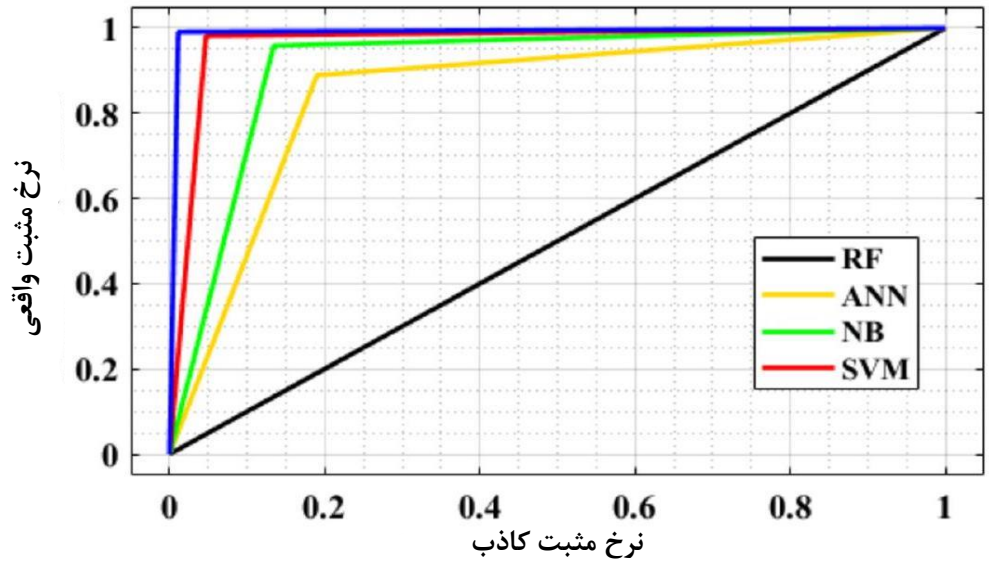
برچسب‌های واقعی حمله و خروجی مدل پیشنهادی در طول زمان، به‌وضوح این دقت را نشان می‌دهد. این هم‌راستایی بیانگر دقت و قابلیت اعتماد بالای روش پیشنهادی در شناسایی و واکنش مؤثر به وقایع FDIA است؛ به‌گونه‌ای که موجب حفظ یکپارچگی و پایداری ریزشبکه می‌شود. بررسی تغییرات ولتاژ خروجی طی وقوع حملات، که در نمودارها نشان داده شده‌اند، گویای آن است که حمله منجر به بی‌ثباتی در عملکرد سیستم شده و پس از پایان آن، وضعیت سیستم به حالت پایدار بازمی‌گردد. به‌طور کلی، این پژوهش اثربخشی روش پیشنهادی در کاهش اختلالات عملیاتی و افزایش امنیت در برابر حملات سایبری را برجسته می‌سازد و در نتیجه، به بهره‌برداری ایمن‌تر و مقاوم‌تر از شبکه‌های هوشمند کمک می‌کند. در مجموع این نتایج مؤید آن است که راهکار ارائه‌شده، نه‌تنها اختلالات ناشی از حملات سایبری را به حداقل می‌رساند، بلکه زمینه‌ساز افزایش تاب‌آوری و امنیت در بهره‌برداری از ریزشبکه‌های هوشمند خواهد بود.

۵- نتیجه‌گیری و چشم‌اندازهای آتی

این مطالعه بر اهمیت روزافزون امنیت سایبری در حوزه ریزشبکه‌های DC تأکید دارد؛ چرا که این شبکه‌ها به دلیل ساختار پیچیده و وابستگی به سامانه‌های ارتباطی، در معرض تهدیدهای سایبری قرار دارند. با پیشرفته‌تر شدن این شبکه‌های هوشمند — که شامل اجزایی مانند باتری‌ها، ابرخازن‌ها، مبدل‌های الکترونیک قدرت، پیل‌های سوختی، سیستم‌های فتوولتائیک، و سامانه‌های ارتباطی پیشرفته هستند — احتمال بروز تهدیدهای سایبری افزایش می‌یابد. روش تشخیص پیشنهادی که ترکیبی از تبدیل ویولت و ماشین بردار پشتیبان (SVM) است، راهکاری مقاوم و مؤثر برای شناسایی حملات تزریق داده نادرست (FDIA) ارائه می‌دهد. کارایی این مدل با افت محسوس ولتاژ از ۳۵۰ ولت به حدود ۳۰۰ ولت در حین وقوع حمله، و بازگشت آن به سطح اولیه در زمان ۰.۷ ثانیه، همراه با نوسانات قابل توجه بین ۰.۴ تا ۰.۶ ثانیه به اثبات رسیده است. نتایج ارزیابی مدل نیز حاکی از عملکرد بسیار دقیق آن است؛ به‌گونه‌ای که بدون هیچ مثبت کاذب، با تنها ۱۰ منفی کاذب، موفق به شناسایی ۱۹۱ مورد مثبت واقعی و ۴۰۰ مورد منفی واقعی شده است. این آمار، گواهی بر دقت بالا و قابلیت اعتماد روش پیشنهادی در محیط‌های عملیاتی واقعی دارد. در آینده، می‌توان این مدل را با رویکردهای یادگیری عمیق یا سامانه‌های تشخیص توزیع‌شده تلفیق کرد تا توان عملیاتی و مقیاس‌پذیری آن در ریزشبکه‌های گسترده‌تر افزایش یابد.



شکل ۱۷- تحلیل شاخص‌های عملکرد (دقت، صحت، بازخوانی و امتیاز F۱) در سه سناریوی مختلف.



شکل ۱۸- تحلیل نرخ تشخیص صحیح (TPR) و نرخ تشخیص نادرست (FPR).

یافته‌های کلیدی:

نتایج حاصل از این مطالعه مؤید دقت بالای الگوریتم پیشنهادی در شناسایی حملات FDIA است. مدل توانسته است ۱۹۱ مورد حمله واقعی و ۴۰۰ نمونه عادی را به‌درستی شناسایی کند، که نشان‌دهنده عملکرد بسیار قابل اطمینان آن است. تشخیص صحیح زمان آغاز حمله در ۰/۴ ثانیه و زمان توقف آن در ۰/۶ ثانیه، همراه با همخوانی کامل میان خروجی مدل و برچسب‌های واقعی، اثباتی بر دقت و پایداری الگوریتم است. در طول مدت وقوع حمله (از ۰.۴ تا ۰.۶ ثانیه)، مقدار خروجی الگوریتم به‌صورت پیوسته بر ۱ باقی مانده و به‌درستی نشان‌دهنده حضور حمله بوده است. با وجود ثبت ۱۰ منفی کاذب — که ممکن است ناشی از پیچیدگی شرایط یا نویز سیگنال باشد — مدل در حال بهبود و تقویت است تا این موارد نادر را نیز پوشش دهد و عملکرد خود را ارتقاء بخشد.

نتایج به‌دست‌آمده نشان‌دهنده برتری قابل توجه روش پیشنهادی نسبت به مدل‌های موجود است، به‌طوری‌که دقت بالا و میزان خطای بسیار اندکی را در شناسایی حملات ارائه می‌دهد. در گام‌های آتی، می‌توان با تمرکز بر کاهش نرخ منفی کاذب و گسترش دامنه پوشش مدل برای انواع متنوع‌تری از تهدیدات سایبری، اثربخشی آن را افزایش داد. همچنین، ادغام سیستم‌های پایش بلادرنگ با تکنیک‌های یادگیری ماشین می‌تواند موجب افزایش تطبیق‌پذیری سیستم شود و حفاظت قوی‌تری در برابر تهدیدات سایبری در حال تکامل در ریزشبکه‌های DC فراهم آورد.

«بیانیه مشارکت نویسندگان (CRediT authorship contribution statement)»

Revathi Subramaniam: مسئولیت نگارش اولیه مقاله، انجام تحلیل‌های رسمی، طراحی مدل مفهومی، تدوین روش‌شناسی، توسعه نرم‌افزار و اجرای فرآیندهای اعتبارسنجی را بر عهده داشته است.

Androse Joseph Sheela: در فرآیند نگارش و تدوین اولیه، توسعه ابزارهای تصویری، نظارت علمی، مدیریت منابع و پروژه، توسعه نرم‌افزار، طراحی روش تحقیق و ایده‌پردازی نقش مؤثری ایفا کرده است.

Abdullah Alwabli: در بازنگری و ویرایش نهایی مقاله، انجام مطالعات تحقیقی، ارزیابی‌های تحلیلی و جذب منابع مالی مشارکت داشته است.

بیانیه تضاد منافع

نویسندگان اذعان دارند که هیچ تضاد منافع مالی یا شخصی قابل‌توجهی که بتواند روند پژوهش یا نتایج ارائه‌شده در این مقاله را تحت‌تأثیر قرار دهد، وجود نداشته است.

مراجع

[١] Ghiasi M, Niknam T, Wang Z, Mehrandezh M, Dehghani M, Ghadimi N. A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. Electr Pow Syst Res ٢٠٢٣;٢١٥:١٠٨٩٧٥.

[٢] Aurangzeb M, Wang Y, Iqbal S, Naveed A, Ahmed Z, Alenezi M, et al. Enhancing cybersecurity in smart grids: Deep black box adversarial attacks and quantum voting ensemble models for blockchain privacy-preserving storage. Energy Rep ٢٠٢٤;١١:٢٤٩٣-٥١٥.

[٣] Faheem M, Raza B, Bhutta MS, Madni SHH. A blockchain-based resilient and secure framework for events monitoring and control in distributed renewable energy systems. IET Blockchain ٢٠٢٤.

[٤] Suprabhath Koduru S, Machina VSP, Madichetty S. Cyber-attacks in cyber-physical microgrid systems: A comprehensive review. Energies ٢٠٢٣;١٦(١٢):٤٥٧٣.

[٥] Chang Z, Wu J, Liang H, Wang Y, Wang Y, Xiong X. A review of power system false data attack detection technology based on big data. Information ٢٠٢٤;١٥(٨):٤٣٩.

[٦] Nassar AA, Morsi WG. Early detection of cyber-physical attacks on electric vehicles fast charging stations using wavelets and deep learning. IEEE Trans Ind Cyber-Phys Syst ٢٠٢٤.

[٧] Sawas A. Cyber-physical attacks detection and resilience methods in smart grids; ٢٠٢٣.

[٨] Meydani A, Shahinzadeh H, Ramezani A, Nafisi H, Gharehpetian GB. A review and analysis of attack and countermeasure approaches for enhancing smart grid cybersecurity. In ٢٠٢٤ ٢٨th international electrical power distribution conference (EPDC) (pp. ١-١٩). IEEE; ٢٠٢٤, April.

[٩] Ghiasi M, Dehghani M, Niknam T, Kavousi-Fard A, Siano P, Alhelou HH. Cyberattack detection and cyber-security enhancement in smart DC-microgrid based on blockchain technology and Hilbert Huang transform. Ieee Access ٢٠٢١;٩: ٢٩٤٢٩-٤٠.

[١٠] Madichetty S, Mishra S. Cyber-attack detection and correction mechanisms in a distributed DC microgrid. IEEE Trans Power Electron ٢٠٢١;٣٧(٢):١٤٧٦-٨٥.

[١١] Dehghani M, Niknam T, Ghiasi M, Bayati N, Savaghebi M. Cyber-attack detection in DC microgrids based on deep machine learning and wavelet singular values approach. Electronics ٢٠٢١;٢٠٢١(١٠):١٩١٤.

[١٢] Dai J, Yang J, Wang Y, Xu Y. Blockchain-enabled cyber-resilience enhancement framework of microgrid distributed secondary control against false data injection attacks. IEEE Trans Smart Grid ٢٠٢٣.

[١٣] Gong S, Dragicevic T, Mijatovic N, Zhang Z. Event-triggered attack detection and identification in power-electronics-based DC microgrid. Authorea Preprints ٢٠٢٣.

[١٤] Pinto SJ, Siano P, Parente M, Ozdemir G. Resilience and stability analysis of distributed secondary controllers in DC microgrids under cyber attacks and communication delays. IEEE Access ٢٠٢٣;١١:١٣٢٢٩٦-٣١١.

[١٥] Rajeyyagari S, Saravanan M, Pandey PS, Devi A, Shankar SS. Convolutional Neural network-based African vulture optimization algorithm for the enhancement of cybersecurity in the blockchain-based Smart grid. Multimed Tools Appl ٢٠٢٤;٨٣ (٢٠):٥٨٥٢٧-٥٣.

[١٦] Gong S, Dragičević T, Mijatovic N, Zhang Z. A novel attack identification mechanism in IoT-based converter-composed DC grids. IEEE Internet Things J ٢٠٢٢;١٠(٩):٧٥٥٤-٦٧.

[١٧] Vatambeti R, Divya NS, Jalla HR, Gopalachari MV. Attack detection using a lightweight blockchain based elliptic curve digital signature algorithm in cyber systems. Int J Saf Security Eng ٢٠٢٢;١٢(٦).

[١٨] Divya R, Umamaheswari S, Stonier AA. Machine learning based smart intrusion and fault identification (SIFI) in inverter based cyber-physical microgrids. Expert Syst Appl ٢٠٢٤;٢٣٨:١٢٢٢٩١.

[١٩] Mahvash H, Taher SA, Guerrero JM. Detecting and mitigating cyber-attacks in AC microgrid composed of marine current turbine DFIGs to improve energy management system. e-Prime-Advances in Electrical Engineering in Electronics and Energy ٢٠٢٤;٧:١٠٠٤٦٤.

[٢٠] Gong S, Dragicevic T, Mijatovic N, Zhang Z. Event-triggered attack detection and identification in power-electronics-based DC microgrid. Authorea Preprints ٢٠٢٣.

[٢١] Alohali MA, Elsadig M, Al-Wesabi FN, Al Duhayyim M, Hilal AM, Motwakel A. Blockchain assisted optimal machine learning based cyberattack detection and classification scheme. Comput Syst Sci Eng, ٢٠٢٣;٤٦(٣):٣٥٨٣-٩٨.

[٢٢] Jadidi S, Badihi H, Zhang Y. Design of an intelligent hybrid diagnosis scheme for cyber-physical PV systems at the microgrid level. Int J Electr Power Energy Syst ٢٠٢٣;١٥٠:١٠٩٠٦٢.

[٢٣] Taher MA, Behnamfar M, Sarwat AI, Tariq M. False data injection attack detection and mitigation using non-linear autoregressive exogenous input-based observers in distributed control for DC microgrid. IEEE Open J Ind Electron Soc ٢٠٢٤.

[٢٤] Halgamuge MN. Leveraging deep learning to strengthen the cyber-resilience of renewable energy supply chains: a survey. IEEE Commun Surv Tutorials ٢٠٢٤.

[٢٥] Pawar V, Sachdeva S. ParallelChain: a scalable healthcare framework with lowenergy consumption using blockchain. Int Trans Oper Res ٢٠٢٤;٣١(٦):٣٦٢١-٤٩.

[٢٦] Laghari AA, Khan AA, Alkanhel R, Elmannai H, Bourouis S. Lightweight-biov: blockchain distributed ledger technology (bdlt) for internet of vehicles (iovs). Electronics ٢٠٢٣;١٢(٣):٦٧٧.

[۲۷] Wang Q, Yu J, Chen S, Xiang Y. SoK: DAG-based blockchain systems. ACM Comput Surv ۲۰۲۳;۵۵(۱۲):۱-۳۸.

[۲۸] Sisi Z, Souri A. Blockchain technology for energy-aware mobile crowd sensing approaches in Internet of Things. Trans Emerg Telecommun Technol ۲۰۲٤;۳۵(٤): e٤۲۱۷.

[۲۹] Babu RM, Satamraju KP, Gangothri BN, Malarkodi B, Suresh CV. A hybrid model using genetic algorithm for energy optimization in heterogeneous internet of blockchain things. Telecommun Radio Eng ۲۰۲٤;۸۳.

رواتی سوبرامانیام تحصیلات کارشناسی خود را در رشته مهندسی برق و الکترونیک در سال ۲۰۱۲ از کالج مهندسی و فناوری ولالار، ایرووود، و مقطع کارشناسی ارشد را در سال ۲۰۱۴ در رشته الکترونیک کاربردی از کالج مهندسی کونگو به پایان رسانده است. ایشان هم‌اکنون به عنوان عضو هیئت علمی و استادیار در گروه مهندسی برق و الکترونیک در کالج مهندسی و فناوری کونگونادو در تریچی، ایالت تامیل نادو فعالیت می‌کنند. سوابق علمی ایشان شامل مشارکت در کنفرانس‌های علمی متعدد و انتشار مقالات پژوهشی مختلف است. زمینه‌های تخصصی مورد علاقه وی شامل الکترونیک قدرت، شبکه‌های هوشمند، امنیت سایبری و بهبود کیفیت توان می‌باشد.

دکتر A. Sheela دارای مدرک کارشناسی در رشته مهندسی برق و الکترونیک (۲۰۰۱)، کارشناسی ارشد در سیستم‌های قدرت (۲۰۰۴) و دکترای تخصصی در مهندسی برق (۲۰۱۶) می‌باشد. ایشان با انتشار حدود ۷۵ مقاله در مجلات و کنفرانس‌های بین‌المللی معتبر، سابقه پژوهشی پرباری دارند. همچنین، در زمینه دریافت حمایت مالی از سازمان‌های مختلف برای برگزاری رویدادهای

علمی و اجرای پروژه‌های تحقیقاتی نیز عملکرد موفقی داشته‌اند. زمینه‌های تحقیقاتی مورد علاقه ایشان شامل شبکه‌های هوشمند، محاسبات نرم و امنیت در سامانه‌های برق است.

عبدالله الوابلی در سال ۲۰۱۲ مدرک کارشناسی مهندسی برق را از دانشگاه ام‌القرای عربستان سعودی دریافت کرد و سپس در سال ۲۰۱۵ موفق به اخذ مدرک کارشناسی ارشد مهندسی برق از مؤسسه فناوری فلوریدا (Florida Institute of Technology) در ایالات متحده شد. وی تحصیلات خود را در همان مؤسسه ادامه داد و در سال ۲۰۲۱ مدرک دکتری خود را در همین رشته اخذ کرد. از آن زمان تاکنون به‌عنوان عضو هیئت علمی در گروه مهندسی ارتباطات و الکترونیک دانشگاه ام‌القرای مشغول به تدریس است و در حال حاضر ریاست این گروه را نیز بر عهده دارد. زمینه‌های تدریس او شامل ارتباطات بی‌سیم، ارتباطات شخصی و طراحی مدارهای مایکروویو است. حوزه‌های تحقیقاتی اصلی او نیز طیف متنوعی از موضوعات از جمله بهینه‌سازی، ارتباطات رادیویی، سیستم‌های سلولی، شبکه‌های حسگر بی‌سیم، سامانه‌های راداری و ارتباطات ماهواره‌ای را در بر می‌گیرد.