مقاله مروری

مقاوم‌سازی سیستم‌های حفاظتی شبکه‌های قدرت در برابر حملات سایبری: مرور جامع

زهرا پوراحمد، رحمت‌الله هوشمند و سید محمد مدنی

چکیده: سیستم‌های حفاظتی، حیاتی‌ترین عنصر دفاعی شبکه‌های قدرت را در برابر شرایط غیرعادی تشکیل می‌دهند؛ بنابراین عملکرد نادرست آنها که توسط حملات سایبری ایجاد می‌شود، ممکن است عواقب بسیار زیادی برای شبکه‌های قدرت مانند خاموشی‌های گسترده ایجاد کند. از جمله مهم‌ترین سیستم‌های حفاظتی که در معرض نفوذ مهاجم سایبری است، سیستم حفاظتی ژنراتور، خط انتقال و ترانسفورمر می‌باشد. ناهنجاری‌های سایبری را می‌توان با استفاده از اقدام‌های استراتژیک به حاشیه راند و اثر آن را در شبکه کاهش داد. در این مقاله، با توجه به اهمیت سیستم حفاظت شبکه قدرت، مرور جامع روش‌های مقاوم‌سازی سیستم حفاظتی در برابر حملات سایبری مورد بررسی قرار گرفته است. بدین منظور در مرحله اول، جهت مقاوم‌سازی شبکه قدرت در برابر حمله سایبری، روش‌های مبتنی بر حفاظت ارائه می‌گردند. سپس در مرحله دوم، روش‌های مبتنی بر تشخیص برای ردیابی حمله سایبری احتمالی بیان می‌شوند. از آنجا که تضمین قطعی برای عدم نفوذ مهاجم سایبری وجود ندارد، با بهره‌گیری از روش‌های تشخیص حمله می‌توان از پیشرفت حمله جلوگیری کرد. به این منظور از دو دسته الگوریتم مبتنی بر داده و مبتنی بر مدل استفاده می‌شود. در الگوریتم‌های مبتنی بر داده می‌توان از دانش و اطلاعات شبکه به صورت بهینه استفاده کرد تا شرایط وقوع حمله سایبری را نسبت به شرایط بدون حمله سایبری تشخیص داد. در الگوریتم‌های مبتنی بر مدل با اجرای الگوریتم تخمین حالت و بر اساس روابط سیستم، پارامترهای شبکه تخمین زده می‌شود. سپس با محاسبه اختلاف مقادیر برآوردشده و مقادیر اندازه‌گیری‌شده، دستکاری در اطلاعات و نفوذ مهاجم سایبری، تشخیص داده می‌شود. در نتیجه استفاده از روش‌های جلوگیری و شناسایی نفوذ مهاجم سایبری در مطالعات مورد بررسی باعث افزایش امنیت سایبری سیستم حفاظت شبکه قدرت خواهد شد. در این راستا به‌کارگیری انواع الگوریتم‌های حفاظت و تشخیص برای مقابله با حملات سایبری بسیار حائز اهمیت است.

***کلیدواژه:* حمله سایبری، مقاوم‌سازی، شبکه قدرت، سیستم حفاظتی، رله.**

۱- مقدمه

یکی از مسائل مهم در بهره‌برداری شبکه‌های قدرت، حفظ امنیت آن است. اولین قدم در راه ارزیابی امنیت سیستم، نمایش شرایط بهره‌برداری است؛ به نحوی که پس از بررسی آن، تصمیم‌های احتمالی لازم جهت حفظ شرایط عملکرد مطلوب گرفته شود. این در حالی است که با اعمال گسترده فناوری‌های سایبری، شبکه قدرت در برابر حمله‌های سایبری مخرب، آسیب‌پذیر شده است. در طی سال‌های گذشته شبکه قدرت، سریعاً از شبکه سنتی به شبکه فیزیکی- سایبری تغییر کرده است [۱]. تفاوت بزرگ بین شبکه فیزیکی- سایبری پیشرفته و شبکه سنتی در استفاده وسیع‌تر از ابزار هوشمند پیشرفته، پیوستن اطلاعات سایبری و تکنولوژی کنترل است. تمام این برنامه‌ها به‌تدریج، شبکه برق را به یک شبکه فیزیکی- سایبری تبدیل می‌کنند؛ به طوری که قابلیت اطمینان شبکه افزایش می‌یابد [۲]. با این حال با گسترش لایه‌های سایبری در شبکه، آسیب‌پذیری‌های اینترنتی اجتناب‌ناپذیر خواهد بود و شبکه برق، حساس به انواع حملات سایبری می‌شود [۳]. مطالعات متعددی در مورد جنبه‌های مختلف امنیت سایبری شبکه قدرت وجود دارد که اهمیت امنیت سایبری را در فناوری‌ها [۴] و [۵]، تجهیزات [۶] و عناصر کلیدی شبکه [۷] برجسته می‌کند.

۱-۱ سیستم‌های حفاظتی شبکه قدرت

خرابی در شبکه برق می‌تواند به دلایل مختلفی رخ دهد و منجر به ایجاد جریان‌های بسیار زیادی در شبکه شود که ممکن است بیشتر از حد مجاز عناصر شبکه باشد و باعث خرابی و اختلال در تأمین انرژی مشترکین شود [۸]. بنابراین حفاظت از تجهیزات و اطمینان از عملکرد قابل اعتماد برای کل شبکه برق، بسیار مهم است. در این میان، دستگاه‌های حفاظتی، به‌خصوص رله‌های حفاظتی، به طور گسترده برای شناسایی و جداسازی مناطق معیوب از شبکه‌های عملیاتی استفاده می‌شوند. این دستگاه‌ها مطابق تنظیمات حفاظتی از پیش تعریف‌شده، کار می‌کنند که حاصل مطالعه سیستم قدرت است. سیستم حفاظتی از کلیدهای قطع‌کننده (CB)[1] برای جداسازی قسمت‌های معیوب، ابزار ترانسفورمر برای اندازه‌گیری ولتاژ (PT) و جریان (CT) و رله‌های حفاظتی برای شناسایی وضعیت خطا تشکیل می‌شود. جریان‌های بیش از حد، توسط تنظیمات از پیش تعریف‌شده رله ارزیابی می‌شود و هنگامی که یک خطا رخ می‌دهد، رله، مدار کنترل را برای خاموش‌کردن CB مربوطه راه‌اندازی می‌کند [۹].

پیکربندی تنظیمات در یک سیستم حفاظتی نمونه در شکل ۱ نشان داده شده است. دستگاه حسگر در وسط شکل، جریان و ولتاژ را با استفاده از ابزار ترانسفورمر اندازه‌گیری می‌کند. اندازه و زاویه فاز جریان و ولتاژ در طول بهره‌برداری شبکه در حالت پایدار با تحلیل پخش توان و جریان خطا

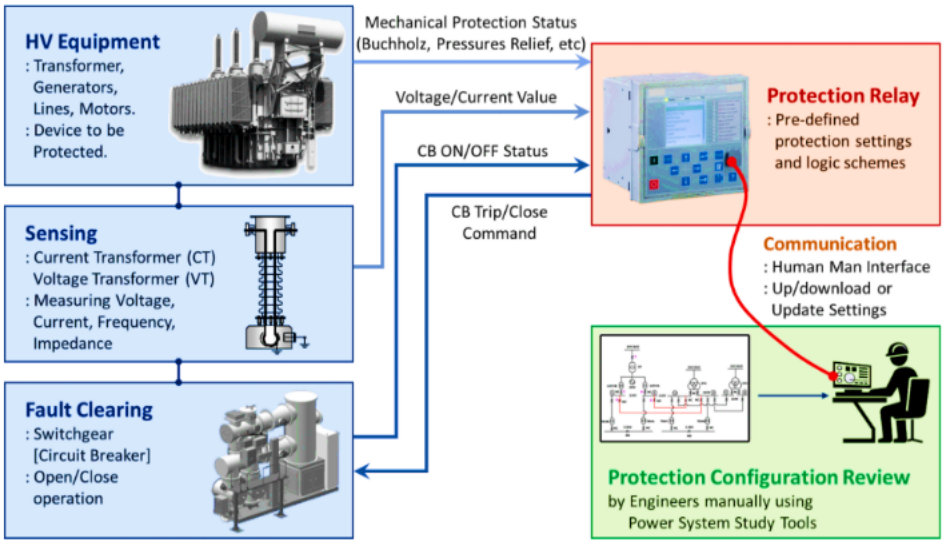
این مقاله در تاریخ ۵ شهریور ماه ۱۴۰۳ دریافت و در تاریخ ۱۷ شهریور ماه ۱۴۰۳ بازنگری شد. این مقاله به دعوت سردبیر نشریه به نگارش درآمده است.

زهرا پوراحمد، دانشکده فنی- مهندسی، گروه مهندسی برق، دانشگاه اصفهان، اصفهان، ایران، (email: z.pourahmad@eng.ui.ac.ir).

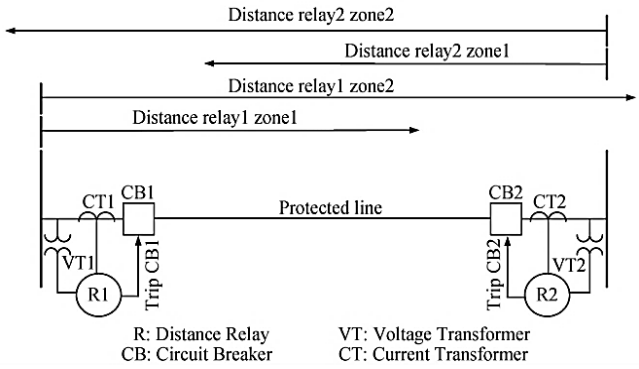
رحمت‌الله هوشمند (نویسنده مسئول)، دانشکده فنی- مهندسی، گروه مهندسی برق، دانشگاه اصفهان، اصفهان، ایران، (email: hooshmand_r@eng.ui.ac.ir).

سید محمد مدنی، دانشکده فنی مهندسی، گروه مهندسی برق، دانشگاه اصفهان، اصفهان، ایران، (email: m.madani@eng.ui.ac.ir).

1. Circuit Breaker



شکل ۱: طرح یک سیستم حفاظتی در شبکه قدرت [۹].

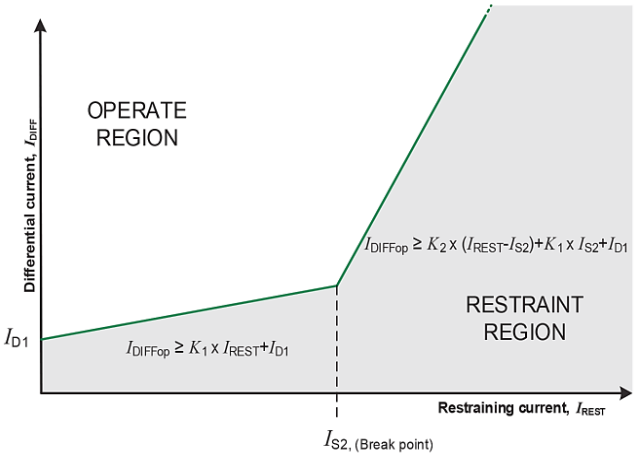


شکل ۲: حفاظت دیستانس خط [۱۰].

با استفاده از نرم‌افزارهای مختلف سیستم قدرت محاسبه می‌شود. گزارش حاصل از نرم‌افزار تجزیه و تحلیل سیستم قدرت، پارامترهایی را توصیه می‌کند که دستگاه حفاظتی بر اساس آن کار می‌کند. پارامترهای حاصل از مطالعه حفاظتی در رله برای پیکربندی تنظیمات استفاده می‌شوند [۹].

۱-۲ عملکرد رله دیستانس در سیستم حفاظتی

اساس حفاظت دیستانس، تقسیم مقادیر ولتاژ و جریان اندازه‌گیری‌شده در نقطه رله و مقایسه آن با امپدانس از پیش تعریف‌شده است. اگر امپدانس اندازه‌گیری‌شده توسط رله دیستانس کمتر از امپدانس تنظیمی از پیش تعریف‌شده باشد، رله وجود یک خطا را در نظر می‌گیرد و عمل می‌کند. برخلاف رله‌های اضافه جریان، پوشش خطای رله‌های دیستانس عملاً مستقل از تغییرات امپدانس منبع است که آنها را به یک تجهیز ایده‌آل برای حفاظت از خطوط انتقال تبدیل می‌کند. یک رله دیستانس شامل چندین ناحیه دسترسی به نام زون است. به طور معمول، ناحیه اول رله دیستانس فوراً عمل می‌کند و تقریباً ۸۰ درصد از خط انتقال را پوشش می‌دهد. به این ترتیب اطمینان حاصل می‌شود که رله فقط زمانی که خطا در خط محافظت‌شده رخ دهد، خاموش می‌گردد. این در حالی است که ناحیه دوم ۱۲۰ تا ۱۵۰ درصد خط را پوشش می‌دهد و با ۱۵ تا ۳۰ سیکل تأخیر زمانی کار می‌کند. در صورتی که رله دیستانس خط هنگام وقوع خطا عمل نکند، در این تأخیر زمانی، رله‌های مجاور عمل می‌کنند. به این ترتیب حفاظت ناحیه ۱ و ۲ همپوشانی دارند و محافظت ۱۰۰ درصد از خط انتقال و نیز حفاظت پشتیبان برای خطوط مجاور را فراهم می‌کند. این موضوع در شکل ۲ نشان داده شده است [۱۰].

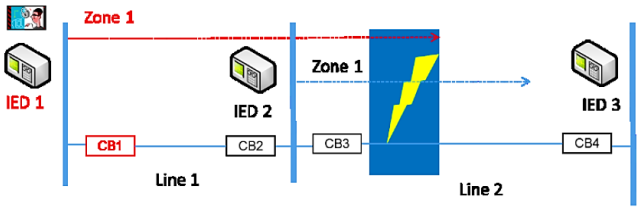


شکل ۳: منحنی عملکرد رله دیفرانسیل [۱۴].

عملکرد دو رله دیستانس در دو طرف خط به گونه‌ای صورت می‌گیرد که زمان وقوع خطا، خط از هر دو طرف قطع شود. به این منظور رله‌ها در دو طرف خط به واسطه لینک مستقیم با یکدیگر ارتباط داشته و هر رله پس از مشاهده خطا سیگنالی را به رله دیگر ارسال می‌کند تا فرمان تریپ بریکر در طرف دیگر خط نیز ارسال شود [۱۱].

۱-۳ عملکرد رله دیفرانسیل در سیستم حفاظتی

هدف اصلی رله‌های حفاظتی ترانسفورمر، تشخیص عیوب ترانسفورمر با حساسیت بالا و جداسازی آن در سریع‌ترین زمان ممکن است. تشخیص سریع و قطع انرژی عیوب ترانسفورمر، آسیب‌های وارده به ترانسفورمر و همچنین نیاز به تعمیرات بعدی را به حداقل می‌رساند. این وظیفه توسط رله دیفرانسیل ترانسفورمر انجام می‌شود [۱۲]. الگوریتم‌های حفاظت دیفرانسیل برای ترانسفورمرهای قدرت بر اساس مقایسه (دیفرانسیل) جریان دو سیم‌پیچ تشکیل‌دهنده ترانسفورمر (سیم‌پیچ اولیه و ثانویه) است. این محاسبه توسط یک میکروکنترلر واقع در مدار رله انجام می‌شود. عدم تعادل بین ورودی و خروجی سیستم، نشان‌دهنده یک خطای داخلی است و باعث می‌شود که رله، سیگنالی را به کلیدهای قطع‌کننده (CB) مدار ارسال کند [۱۳]. به طور دقیق‌تر رله دیفرانسیل فقط در صورتی فرمان تریپ را صادر می‌کند که نقطه عملیاتی آن در صفحه جریان دیفرانسیل- جریان بازدارنده، وارد منطقه تریپ شود. این منحنی، منطقه تریپ و منطقه بلاک رله دیفرانسیل در شکل ۳ نشان داده شده است. در این



شکل ۴: مفهوم ناهماهنگی رله‌های دیستانس در ناحیه ۱ [۱۸].

شکل I_d جریان دیفرانسیل[1] و I_r جریان بازدارنده[2] است که به عنوان مجموع مقدار جریان پایانه‌ها تعریف می‌شود [۱۴].

عملکرد رله دیفرانسیل خط (LCDR)[3] بر قانون‌های مداری جریان استوار است. بر اساس این قانون، رله دیفرانسیل جریان‌هایی را که از تمام پایانه‌های مربوطه وارد یا خارج می‌شوند مقایسه می‌کند. از این رو در LCDRهای یک خط، به ارتباط با یکدیگر و به اشتراک گذاشتن اندازه‌گیری‌های جریان همگام‌سازی شده با زمان نیاز است [۱۵] و [۱۶]. همان طور که برای رله دیفرانسیل ترانسفورمر شرح داده شد، اگر مسیر نقطه عملیاتی LCDR وارد منطقه تریپ در شکل ۳ شود، رله فرمان تریپ را صادر می‌کند.

۲- آسیب‌پذیری سیستم‌های حفاظتی در برابر حملات سایبری

پیشرفت شبکه برق به دلیل ادغام فناوری جدید، نگرانی‌هایی را در مورد قابلیت اطمینان آن از نظر عملکرد و امنیت ایجاد می‌کند. ادغام دستگاه‌های ارتباطی به منظور هوشمندسازی شبکه، آسیب‌پذیری آن را در برابر فعالیت‌های مخرب سایبری افزایش می‌دهد [۱۷]. از سوی دیگر سیستم‌های حفاظتی از حیاتی‌ترین اجزای آسیب‌پذیر سایبری هستند؛ زیرا مستقیماً بر یکپارچگی و پایداری شبکه‌های قدرت تأثیرگذارند [۵]. مهاجم برای اعمال ضرر به شبکه و گمراه‌کردن اپراتور راه‌های مختلفی می‌تواند اتخاذ کند. یک مهاجم خبره با انتخاب نقاط کلیدی شبکه، با کمترین هزینه بیشترین ضربه را به شبکه وارد می‌کند. حمله تزریق داده غلط (FDIA)[4] می‌تواند اندازه‌گیری‌های از راه دور را دستکاری کند تا در نقطه عملیاتی رله مداخله نماید [۱۸].

۲-۱ آسیب‌پذیری‌های رله‌های حفاظتی

رله‌های حفاظتی، حیاتی‌ترین عنصر دفاعی سیستم قدرت را در برابر شرایط غیرعادی تشکیل می‌دهند؛ بنابراین عملکرد نادرست آنها که توسط حملات سایبری ایجاد می‌شود، ممکن است عواقب بسیار زیادی برای سیستم‌های قدرت مانند خاموشی‌های گسترده ایجاد کند [۱۹]. در گزارشی که در سال ۲۰۱۸ توسط وزارت امنیت داخلی ایالات متحده (DHS)[5] منتشر شد، رله‌های دیجیتال به عنوان اهداف آسیب‌پذیر در برابر حملات سایبری شناسایی شدند [۲۰]. مهاجم می‌تواند از راه‌های مختلف به یک رله حفاظتی دسترسی پیدا کند و باعث اختلال و خرابی شود [۲۱]. به طور کلی تهدیدات رله‌های حفاظتی به سه دسته نفوذ به شبکه ارتباطی، نفوذ به سیستم عامل رله و نفوذ محلی تقسیم می‌شود. در ادامه این سه نوع تهدید بیان می‌شوند.

1. Differential Current
2. Restraining Current
3. Line Current Differential Relay
4. False Data Injection Attack
5. Department of Homeland Security

۱) حمله سایبری به رله از طریق شبکه ارتباطی: شبکه ارتباطی به دلیل پوشش وسیع، در معرض حملات سایبری است. رله‌های حفاظتی از طریق شبکه گسترده (WAN)[6] با استفاده از پروتکل‌های ارتباطی استاندارد (مانند DNP۳ و IEC۶۱۸۵۰) برای انتقال داده‌های حیاتی به مرکز کنترل متصل می‌شوند. استاندارد IEC۶۱۸۵۰ به طور گسترده برای اتوماسیون و حفاظت پست استفاده می‌شود. این استاندارد امکان ارتباط بلادرنگ و تبادل داده بین پست‌های دیجیتال و دستگاه‌های حفاظتی را فراهم می‌کند. با این حال، استاندارد IEC۶۱۸۵۰ از نظر حفاظت سایبری، امن نیست و از این رو پیامدهای خطرناک عدم ایمن‌سازی استاندارد IEC۶۱۸۵۰ مورد توجه محققان می‌باشد [۲۲]. در صورت عدم ایمن‌سازی این استانداردها، مهاجم مشروط بر این که بتواند فایروال‌ها را دور بزند، از طریق نقاط اتصال مختلف به شبکه ارتباطی نفوذ کرده و به رله حفاظتی دسترسی پیدا می‌کند. هنگامی که مهاجم به رله متصل می‌شود، می‌تواند تنظیمات دستگاه را بدون وقفه در عملکرد آن تغییر دهد [۲۳].

۲) حمله به سیستم عامل رله: این حمله می‌تواند پس از نصب سیستم عامل بر روی رله‌ها در حین نصب دستگاه اجرا شود و امکان دسترسی غیرمجاز به سیستم عامل را فراهم می‌کند. علاوه بر این، فروشندگان رله حفاظتی اغلب، به‌روزرسانی‌های سخت‌افزاری خود را به صورت آنلاین توزیع می‌کنند و فرصت دیگری برای مهاجمان بالقوه فراهم می‌کنند. لذا مهاجم می‌تواند یک عملکرد مخرب را پیاده‌سازی کند و آن را به گونه‌ای تنظیم کند که در یک زمان خاص فعال شود تا باعث نقص فعال یا غیرفعال شود [۲۴].

۳) حمله سایبری به رله از طریق دسترسی محلی: اگرچه برخی از دستگاه‌های حفاظتی در پست‌های کاملاً محافظت‌شده قرار می‌گیرند، اما ممکن است مهاجم نفوذ کند و برای کنترل دستگاه‌ها و تغییر تنظیمات به رله‌ها متصل شود. دسترسی به رله‌های واقع در وسط فیدر با موانع حفاظت فیزیکی کمتر، آسان‌تر است. به غیر از اتصال به پورت‌های فیزیکی، راه‌های دیگری مانند تداخل الکترومغناطیسی عمدی برای حمله به رله‌ها و تغییر مقادیر ذخیره‌شده در دستگاه یا تزریق اطلاعات دستکاری‌شده به دستگاه برای به خطر انداختن عملکرد رله وجود دارد [۲۵] و [۲۶].

۲-۲ حمله سایبری به رله دیستانس

تهدید دیگری که از جانب مهاجم می‌تواند گسترش پیدا کند، ایجاد ناهماهنگی بین دو رله دیستانس مجاور در خط انتقال است [۲۷]. شکل ۴ نشان می‌دهد که مهاجم می‌تواند تنظیمات ناحیه ۱ رله دیستانس IED۱ را تغییر دهد تا به تنظیمات ناحیه ۱ رله IED۲ بعدی برسد. هنگامی که خطا در خط ۲ رخ می‌دهد، همان طور که در ناحیه سایه نشان داده شده است، قطع‌کننده مدار CB۳ به طور معمول خاموش می‌شود، اما برای CB۱ نیز به اشتباه، فرمان خاموشی ارسال می‌شود. عملکرد حفاظت از راه دور در این حالت باعث قطعی خطوط، بیش از حد لازم می‌شود. در سیستم‌های فشارقوی، قطعی‌های مکرر، این پتانسیل را دارد که سیستم را از نظر حفظ سطح ولتاژ، تضعیف کند یا اپراتور را مجبور به پخش بار مجدد کند که حالت بهینه نباشد. گاهی اوقات، قطعی‌های متعدد می‌تواند منجر به خرابی‌های آبشاری شود که در نهایت باعث فروپاشی سیستم

6. Wide Area Network

خواهد شد [۲۸]. این تهدید را می‌توان در تمام تنظیمات رله دیستانس، یعنی ناحیه ۲، ناحیه ۳ و غیره انجام داد [۱۸].

لازم به ذکر است تا زمانی که دسترسی به رله برقرار باشد، هر نوع پارامتر قابل تنظیم می‌تواند دستکاری شود. البته تهدیدی که در اینجا توضیح داده شد برای رله‌های دیگر مانند رله اضافه جریان نیز قابل استفاده است. در مجموع هدف این حمله، ایجاد ناهماهنگی یک رله با همسایگانش است [۲۹].

۳-۲ حمله سایبری به رله دیفرانسیل

در برنامه‌ریزی‌ها برای حمله سایبری، اهمیت دارد که نرم‌افزار مخرب برای انجام وظیفه خود، داده‌ها را بیش از حد لازم دستکاری نکند؛ چون ممکن است توسط سیستم تشخیص داده شود. در حمله به رله دیفرانسیل، داده‌هایی که می‌توانند برای اختلال در الگوریتم حافظتی دیفرانسیل به کار گرفته شوند شامل جریان‌های ورودی و خروجی ترانسفورمر (I_p و I_s)، تعداد دور سیم‌پیچ‌های ترانسفورمر (N_1 و N_2) یا محاسبات دیفرانسیلی هستند. هدف حمله به الگوریتم حفاظت دیفرانسیل این است که یا حضور خطای واقعی در سیستم را پوشش دهد یا وانمود کند که خطای واقعی وجود دارد؛ در حالی که در واقع هیچ خطایی وجود ندارد. ابتدا پس از جمع‌آوری مجموعه داده‌ها، مقادیر جریان دیفرانسیل و جریان بازدارنده برآورد می‌شوند. حال مهاجم می‌تواند در اطلاعات، دستکاری کند و در عملکرد صحیح کلید قطع‌کننده مدار (CB) اختلال ایجاد نماید. زمانی که خطای واقعی در شبکه رخ دهد، سیستم مربوطه پیامی برای جداسازی ترانسفورمر دریافت نخواهد کرد و این اقدام برای دستگاه، ریسک بسیار زیادی دارد؛ زیرا همچنان در حالت ناامن فعالیت می‌کند. در رویکرد دیگر، وقتی که هیچ گونه خطایی وجود ندارد، رله به اشتباه قطع می‌کند. مهاجم می‌تواند با دسترسی به رله، مقدار جریان بازدارنده را با صفر جایگزین کند یا مقدار جریان دیفرانسیل را به بیشتر از مقدار جریان بازدارنده تغییر دهد. کافی است که رله دیجیتال، جریان دیفرانسیل بیشتر از جریان بازدارنده را تشخیص دهد تا ترانسفورمر را از شبکه جدا کند [۱۳].

۳- افزایش امنیت سایبری در سیستم حفاظتی

سیستم حفاظتی از بخش‌های بحرانی در شبکه قدرت است که در حفظ عملکرد صحیح و بهینه شبکه تأثیرگذار می‌باشد. بنابراین جلوگیری از تهدیدات سایبری به سیستم حفاظتی، امری حیاتی در ارتقای سطح امنیت و تاب‌آوری شبکه قدرت است [۱۰]، [۱۵]، [۱۶]، [۱۸] تا [۲۰]، [۲۸] و [۳۰]. پس از ارزیابی آسیب‌پذیری‌های رله‌های حفاظتی، لازم است اقداماتی برای مقابله این تهدیدات بررسی شود [۳۱]. اگرچه حملات سایبری را نمی‌توان به طور کامل از بین برد، اما این ناهنجاری‌ها را می‌توان با استفاده از چندین اقدام استراتژیک به حاشیه راند و اثر آن را در شبکه کاهش داد. چندین رویکرد اندازه‌گیری وجود دارد که می‌تواند برای کاهش انواع مختلف حملات سایبری در سیستم مورد استفاده قرار گیرد. احراز هویت چندعاملی، رمزگذاری داده‌های ارتباطی و نصب فایروال، اقدامات تقویتی هستند که می‌توانند برای کاهش احتمال حمله سایبری به رله از طریق شبکه ارتباطی مورد استفاده قرار گیرند [۳۲]. در نوع دیگری از حمله، هدف مهاجم این است که از طریق جعل داده‌ها در ابزار اندازه‌گیری، به رله‌های حفاظتی خط انتقال یا ترانسفورمر، باعث تریپ کاذب رله شود. در واقع، مهاجم با فریب‌دادن رله‌های محافظ و ارزیابی نادرست از این که خطا وجود دارد، منجر به عملیات قاطع ناخواسته می‌شود. به عبارت دیگر هیچ خطای واقعی در خط یا ترانسفورمر وجود ندارد؛ اما حمله باعث می‌شود که سیستم محافظت، وجود خطا را تشخیص دهد [۳۲]. اولین قدم برای مقابله با تهدیدهای سایبری در برابر سیستم حفاظتی و کنترلی، درک عمیق از نقاط بالقوه سیستم قدرت برای نفوذ مهاجم است که در ادامه به آن پرداخته می‌شود.

۳-۱ حملات سایبری به سیستم حفاظتی ژنراتور

عملکرد صحیح سیستم تولید برق (EGS)[1]، امری ضروری برای امنیت و قابلیت اطمینان شبکه قدرت است. جهت طراحی استراتژی کنترل ایمن برای EGS باید حملات احتمالی به این سیستم مورد مطالعه قرار گیرند. یکی از سیستم‌های مهم در کنترل EGS، سیستم کنترل تولید خودکار (AGC)[2] است که با حفظ فرکانس شبکه در محدوده قابل قبول، نقش برجسته‌ای را در شبکه‌های قدرت مدرن ایفا می‌کند. سیستم AGC نیروگاه تا حد زیادی به حملات سایبری آسیب‌پذیر است. از مهم‌ترین این حملات، حمله تزریق داده نادرست (FDIA) است که می‌تواند علیه یک سیستم AGC به صورت مخفیانه انجام شود. مهاجمان می‌توانند اندازه‌گیری‌های حسگر به‌کاررفته برای عملیات AGC را جعل کنند و باعث قطع سرویس و آسیب‌های زیرساختی شوند [۳۳]. شکست آبشاری ژنراتورها یکی از مسائل مهم در ارزیابی تاب‌آوری سیستم‌های قدرت تحت حملات متوالی است که مورد توجه محققان قرار گرفته است [۳۴]. روش پیشنهادی مقابله با این حملات به عنوان پلتفرم تشخیص و مقابله با حملات سایبری (CDMP)[3] شناخته می‌شود و از داده‌های پیش‌بینی‌شده برای شناسایی حملات استفاده می‌کند. استراتژی CDMP شامل سه مرحله برای عملیات بهینه است و هر گونه داده نادرست تزریقی به شبکه را شناسایی می‌کند [۳۵]. در روش دیگری برای شناسایی حملات، وضعیت‌های سیستم کنترل فرکانس بار (LFC)[4] با استفاده از رؤیتگر ورودی ناشناخته (UIO)[5] تخمین زده می‌شود و سپس تابع باقیمانده این ورودی (UIO) محاسبه می‌گردد. اختلاف بین توابع باقیمانده و یک آستانه از پیش تعریف‌شده نشان‌دهنده وجود یا عدم وجود حمله FDI است [۳۶]. برای تخمین حالت همزمان با وقوع حمله سایبری در سیستم AGC، یک فیلتر کالمن دومرحله‌ای بهینه (OTS-KF)[6] پیشنهاد شده است. به این منظور، حملات سایبری به عنوان ورودی‌های ناشناخته در دینامیک AGC مدل می‌شوند. از آنجا که تغییرات بار در هر ناحیه رخ می‌دهد، OTS-KF برای تخمین حالات و نقاط پرت به همراه تغییرات بار سیستم فرموله می‌شود [۳۷]. یکی از روش‌های مقابله با حمله سایبری، استفاده از داده‌های تاریخی مربوط به سیستم AGC است. به این ترتیب که داده‌های مربوط به عملکرد منظم سیستم و داده‌های حملات تزریق داده نادرست (FDI) به عنوان داده‌های تاریخی، بررسی و طبقه‌بندی می‌شوند. پارامترهای عملیاتی عادی و پارامترهای عملیات غیرعادی تحت سناریوهای مختلف حمله به عنوان نمونه‌هایی برای آموزش مدل تشخیص بر اساس سری‌های زمانی، جمع‌آوری می‌شوند. برای بهبود دقت مدل، مدل‌های آموزش داده‌های مختلف در طول فرایند عملیات جمع‌آوری می‌شوند. این روش تشخیص می‌تواند تشخیص حمله بلادرنگ را محقق کند و نتایج شناسایی را با پایگاه داده همگام‌سازی کند

1. Electricity Generation System
2. Automatic Generation Control
3. Cyber-Attack Detection and Mitigation Platform
4. Load Frequency Control
5. Unknown Input Observer
6. Optimal Two Stage Kalman Filter

[۳۸]. استفاده از برنامه تخمین حالت، یک طرح کنترل انعطاف‌پذیر برای تشخیص حمله سایبری در سیستم AGC است. رویکرد پیشنهادی، نیازمند افزونگی ابزار اندازه‌گیری در سطح انتقال سیستم قدرت است و از برنامه‌ریزی خطی عدد صحیح مختلط (MILP)[1] استفاده می‌کند. الگوریتم پیشنهادی، سنسورهای مورد حمله را در حضور نویز شناسایی می‌کند. سپس سنسورهای بدون حمله میانگین‌گیری شده و در اختیار کنترل‌کننده بازخورد قرار می‌گیرند [۳۹]. برای بررسی حملات سایبری بر روی عملکرد سیستم AGC، با در نظر گرفتن شرایط مختلف انرژی‌های تجدیدپذیر می‌توان از روش تجزیه و تحلیل حمله- دفاع استفاده نمود. در مرحله اول، یک حمله سایبری بر روی الگوریتم AGC با سطوح مختلف نفوذ تجدیدپذیر انجام می‌شود تا تأثیر یک حمله با حضور انرژی‌های تجدیدپذیر تحلیل شود. سپس یک الگوریتم جدید برای سیستم AGC با استفاده از رویکرد مبتنی بر کنترل PID استفاده می‌شود و حمله برای ارزیابی تأثیر آن، تکرار می‌شود. در مرحله دوم، یک الگوریتم برای کاهش حمله طراحی شده و عملکرد آن با الگوریتم AGC تجزیه و تحلیل می‌شود [۴۰]. از سوی دیگر الگوریتمی تکمیلی از مدل‌های فیزیکی و داده‌های آماری شبکه توسعه داده شده است. چارچوب پیشنهادی، نیازی به به‌روزرسانی سخت‌افزاری واحدهای تولید ندارد و برای سیستم قدرت با چند ناحیه مناسب است. در این روش از مدل‌سازی‌ها و روابط نواحی مختلف در شبکه قدرت با چند ناحیه استفاده می‌شود [۴۱]. امروزه با توسعه الگوریتم‌های یادگیری عمیق در بسیاری از پژوهش‌ها به کاربرد این الگوریتم‌ها در مقابله با حملات سایبری پرداخته شده است [۴۲]. مدل یادگیری عمیق توسط ویژگی‌های فرکانس، آموزش داده می‌شود و باعث بهبود مدل در برابر عدم قطعیت‌های پارامترهای AGC و عوامل غیرخطی مدل‌سازی می‌شود [۴۳].

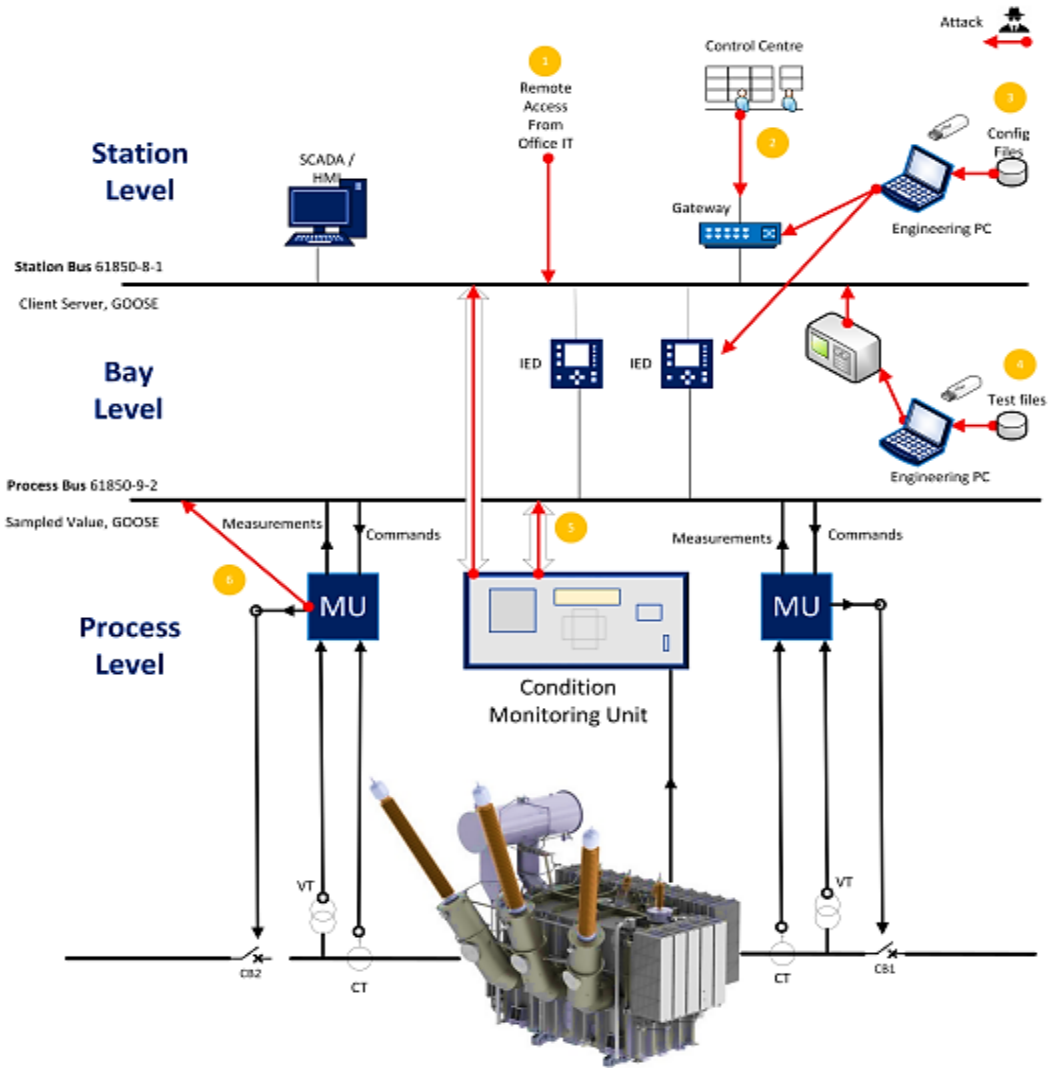
۳-۲ حملات سایبری به سیستم‌های حفاظتی خط

در سیستم‌های قدرت از رله‌های دیفرانسیل جریان خط (LCDR)[2] برای محافظت از خطوط انتقال به طور گسترده استفاده می‌شود. در صورتی که با عملکرد غلط رله، خط انتقال دچار قطعی شود، می‌تواند باعث ایجاد تراکم در سایر خطوط شبکه شود [۴۴]. به این ترتیب با حمله به یک خط، توان انتقالی از آن خط تأمین نشده و احتمال قطع بار وجود دارد. از سوی دیگر، اگر مهاجم به چندین خط حمله کند و باعث ایجاد خطاهای آبشاری شود، آسیب جدی به شبکه وارد می‌شود که این مورد با توجه به هزینه زیاد حمله و سخت‌بودن برنامه حمله، نتایج مخرب‌تری خواهد داشت [۴۵]. باید توجه داشت که مهاجم خبره همواره به دنبال ایجاد حداکثر آسیب است؛ بنابراین طرح حمله سایبری برای ایجاد خطاهای آبشاری اهمیت ویژه‌ای دارد [۴۶]. تأثیر حملات تزریق داده نادرست (FDIA) بر عملکرد LCDRها مورد توجه بسیاری از محققان است [۴۷]. در این زمینه، تکنیکی برای تشخیص حمله FDI در برابر LCDRها و تمایز آنها از خطاهای واقعی در دو ترمینال خط پیشنهاد شده است. در روش ارائه‌شده، زمانی که یک LCDR خطایی را تشخیص می‌دهد، به‌جای قطع فوری خط با استفاده از زیرماژول‌های پیشنهادی دنباله مثبت (PS)[3] و دنباله منفی (NS)[4]، ولتاژ روی ترمینال محلی خود را محاسبه و اندازه‌گیری می‌کند. برای محاسبه این ولتاژ، LCDR خط محافظت‌شده با جزئیات مدل می‌شود و بقیه سیستم با معادل تونن آن جایگزین می‌گردد که پاسخ‌های دقیقی را در پایانه‌های خط ایجاد کند. سپس ولتاژ هر دنباله با استفاده از اندازه‌گیری از راه دور جریان، توسط زیرماژول‌های PS و NS محاسبه می‌شود. اگر تفاوت بین ولتاژهای محاسبه‌شده و اندازه‌گیری‌شده در هر دنباله نشان دهد که اندازه‌گیری‌های جریان از راه دور معتبر نیستند، فرمان تریپ LCDR مسدود می‌شود [۴۸]. برای آن دسته از رله‌های حفاظتی که به‌شدت به همگام‌سازی زمانی متمرکز وابسته هستند، نمی‌توان تهدید از دست دادن همزمانی داده‌ها را نادیده گرفت. از آنجا که عملکرد رله دیستانس بر مبنای محاسبه امپدانس خط است، نسبت به این نوع حمله بسیار آسیب‌پذیر می‌باشد. در این حمله سایبری، برچسب زمانی اندازه‌گیری‌ها دستکاری می‌شود که در صورت عدم وجود اقدامات متقابل، منجر به عملکرد نادرست سیستم حفاظتی می‌شود. برای رویارویی با حمله سایبری به همزمانی داده‌ها، یک طرح حفاظتی اصلی اصلاحی مبتنی بر اطلاعات اندازه‌گیری در خط انتقال، مستقل از اطلاعات زمان‌بندی پیشنهاد شده است. با توجه به تفاوت بین خطای داخلی و خطای خارجی، بر اساس جمع امپدانس اندازه‌گیری‌شده در هر دو انتها یک رله امپدانس جمع معرفی شده است. هنگامی که خط انتقال تحت شرایط بدون خطا، شرایط خطای داخلی و همه شرایط خطای خارجی قرار دارد، مجموع امپدانس اندازه‌گیری‌شده در هر دو انتها اساساً صفر است. در مورد خطا با مقاومت بالا، مجموع امپدانس اندازه‌گیری‌شده به طور قابل توجهی بزرگ‌تر از صفر خواهد بود که کاملاً با شرایط فوق متفاوت است. بنابراین ویژگی برجسته یک رله امپدانس جمع، حساسیت به شناسایی یک خطا با مقاومت بالا است. با در نظر گرفتن این قواعد، روابط محاسبه امپدانس در هر دو سمت خط انتقال بازبینی می‌شود. در واقع، معیار مبتنی بر امپدانس جمع قدرمطلق پیشنهادی، تنها شامل عملیات حسابی قدرمطلق است و قطعاً تحت تأثیر از دست دادن همزمانی داده‌های ناشی از حمله زمان‌بندی قرار نمی‌گیرد [۴۹].

۳-۳ حملات سایبری به سیستم حفاظتی ترانسفورمر

ترانسفورمر به عنوان یک عنصر حیاتی در سیستم‌های قدرت امروزی، دیجیتال شده و به طور بالقوه در برابر کارشکنی‌های سایبری آسیب‌پذیر است. دیجیتالی‌کردن ترانسفورمرها شامل مجموعه‌ای از حسگرها، ابزار جمع‌آوری داده، رله و به طور کلی تجهیزات نظارت وضعیت آنلاین (OLCM)[5] می‌شود که روی هر ترانسفورمر نصب می‌شود تا امکان نظارت در زمان واقعی را فراهم کند [۵۰]. در سیستم نظارت عملکرد ترانسفورمر، تجهیزات مانیتورینگ بلادرنگ با استفاده از سیستم‌های جمع‌آوری داده، حجم عظیمی از داده‌ها را تهیه می‌کنند که باید محافظت شوند. از این رو امنیت داده‌ها، تمرکز اصلی امنیت ترانسفورمر قدرت است. از آنجا که اختلال در حفاظت ترانسفورمر باعث خرابی فاجعه‌بار سیستم و اختلالات قابل توجه و طولانی‌مدت تأمین بار می‌شود، امنیت سایبری آن بسیار حائز اهمیت است [۵۱]. حال اگر حمله سایبری موفق شود یک ترانسفورمر را از مدار خارج کند، کلیه بارهای متصل به آن ترانسفورمر دچار قطعی می‌شود و در نتیجه، خسارت‌ها و هزینه‌های زیادی از جمله خسارت بارهای صنعتی و مسکونی و هزینه اجرای برنامه پاسخ تقاضا به شبکه تحمیل خواهد شد. انواع مختلفی از حملات از جمله حمله تزریق

1. Mixed Integer Linear Programming
2. Line Current Differential Relay
3. Positive-Sequence
4. Negative-Sequence
5. Online Condition Monitoring

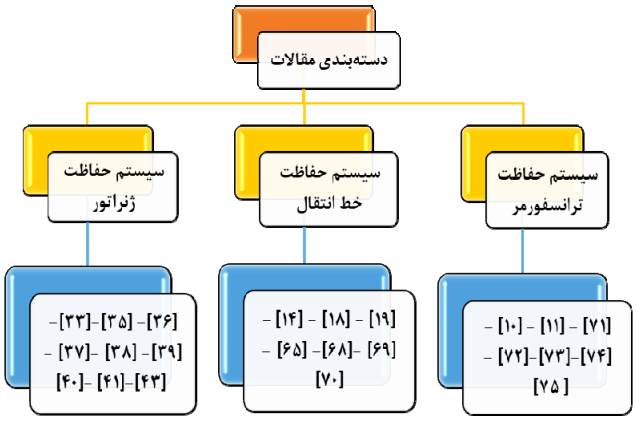


شکل ۵: سطح حمله با استفاده از معماری ترانسفورمر پست [۱۳].

داده غلط (FDI) [۵۲]، حمله پارازیت[1]، جعل GPS [۵۳] و حمله همگام‌سازی[2] زمانی [۵۴] وجود دارد. با این حال، حمله FDI از شناخته‌شده‌ترین و رایج‌ترین حملات است [۵۵]. تا جایی که حمله FDI برای ترانسفورمرهایی که مجهز به سیستم‌های حفاظتی رله در شبکه هستند، حیاتی‌تر می‌شود [۵۱]. ترانسفورمرها را می‌توان از طریق تجهیزات مرتبط با آنها در سطح پست مورد حمله قرار داد. در نتیجه عملکرد کلی شبکه می‌تواند به طور قابل توجهی تحت تأثیر اختلال این تجهیزات توسط مهاجمان قرار گیرد [۵۶] و [۵۷]. هر گونه تغییر جعلی در داده‌ها منجر به ارسال دستوری به بریکر برای قطع جریان، جهت محافظت از تجهیزات می‌شود. می‌توان برای افزایش بهره‌وری، وضعیت کلیدهای مدار (شرایط باز/ بستن) را از راه دور مدیریت کرد؛ با این حال باعث دسترسی بیشتر برای مهاجمان می‌شود [۵۸]. اضافه بارهای دوره‌ای می‌تواند منجر به تخریب عایق ترانسفورمر در طول زمان و در نهایت خرابی و از بین رفتن عملکرد آن شود. به این منظور سناریوهای فرضی اضافه بار یک ترانسفورمر در [۵۶] مورد مطالعه قرار گرفته و اثرات آن با شبیه‌سازی نشان داده شده است. در [۵۷]، [۵۹] و [۶۰] سناریوهای حمله سایبری بر روی دستگاه‌های حفاظت دیفرانسیل مرتبط با ترانسفورمرها به عنوان یک عنصر حیاتی سیستم قدرت مورد مطالعه قرار گرفته است. شکل ۵ سطح حمله را با استفاده از معماری ترانسفورمر پست نشان می‌دهد. نقاط دسترسی از راه دور (مانند مرکز فناوری اطلاعات و مرکز کنترل شبکه) ممکن است توسط عوامل مخرب در معرض خطر قرار گیرند [۱۳]. یک مسیر رایج، از دست دادن اعتبار ورود تجهیزات با استفاده از یک صفحه جعلی است. تجهیزات تست یا تجهیزات حفاظتی معمولاً به باس پست متصل می‌شوند که سطح حمله دیگری را ایجاد می‌کند. شرکت‌هایی که متوجه این خطر شده‌اند، سیستم آزمایشی را از باس جدا کرده‌اند؛ با این حال، تجهیزات تست هنوز باید به باس متصل باشند تا آزمایش کامل شود. دسترسی غیرمجاز از طریق کامپیوتر می‌تواند با معرفی یک فایل مخرب، درگاه‌ها و IEDها را هدف قرار دهد [۶۱]. بر اساس مدل‌های تهدید، به‌طور کلی سه دسته آسیب‌پذیری جعل و دستکاری، افشای اطلاعات و انکار رایج است [۶۲]. این موارد عمدتاً تجهیزات نظارتی مرتبط با ترانسفورمرها را هدف قرار می‌دهند [۶۳].

مسئله بسیار مهم در عملکرد حالت پایدار ترانسفورمر، مسائل گذراست که باید در نظر گرفته شود تا مدار حفاظت دیفرانسیل به طور قابل اعتماد عمل کند. شار هسته ترانسفورمرها باعث ایجاد جریانی به نام جریان مغناطیسی می‌شود. جریان مغناطیسی به عنوان یک جریان دیفرانسیل برای رله ظاهر می‌شود. هنگامی که تغییر ناگهانی در ولتاژ تحریک رخ دهد، می‌تواند جریان مغناطیسی بزرگی جریان یابد. از سوی دیگر وقتی ترانسفورمر در نقطه پیک موج ولتاژ تغذیه سوئیچ شود، پیک موج شار

1. Jamming Attack
2. Synchronization Attack



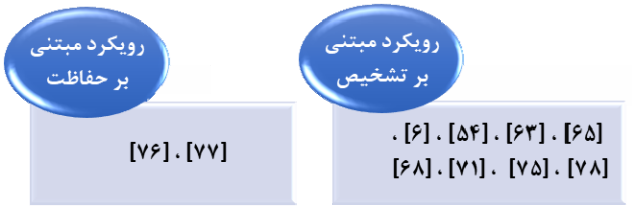
شکل ۶: دسته‌بندی امنیت سایبری در سیستم‌های حفاظتی.

هسته به شار باقیمانده ایجاد خواهد شد. جریان مغناطیسی شار هسته می‌تواند هشت تا ده برابر مقدار آن در حالت بار کامل معمولی باشد و هیچ معادلی در سمت ثانویه ندارد. این پدیده جریان هجومی مغناطیسی نامیده می‌شود و در شبکه به عنوان یک خطای داخلی سیستم حفاظت دیفرانسیل ظاهر خواهد شد. این موضوع باید در نظر گرفته شود تا قطع‌کننده مدار در اثر جریان هجومی مغناطیسی عمل نکند. برای حل این مسئله از خواص هارمونیکی جریان هجومی، جهت جلوگیری از عملکرد اشتباه رله به دلیل جریان‌های هجومی زیاد استفاده می‌شود. به این منظور ابتدا سیگنال‌های ترانسفورمر جریان و ولتاژ (CT, VT) از طریق اکتساب داده‌ها دریافت شده و این داده‌ها با استفاده از مبدل آنالوگ به دیجیتال (ADC) پردازش می‌شوند. سپس این سیگنال با استفاده از تبدیل فوریه، تجزیه و با یک مقدار آستانه قابل تنظیم مقایسه می‌شود. در طول شرایط جریان هجومی مغناطیسی، مؤلفه اصلی، مؤلفه DC، هارمونیک دوم، هارمونیک سوم، هارمونیک چهارم و مؤلفه هارمونیک پنجم به‌ترتیب برابر با مقدار ۱۰۰، ۵۵، ۶۳، ۸/۲۶، ۵/۱ و ۱/۴ درصد می‌باشد. جریان هجومی مغناطیسی به مؤلفه جریان هارمونیک دوم می‌رسد؛ بنابراین شرایط جریان هجومی مغناطیسی در ترانسفورمر بر اساس هارمونیک دوم و نسبت جریان اصلی تشخیص داده می‌شود. از الگوریتم تبدیل فوریه سریع (FFT)[1] می‌توان جهت استخراج مؤلفه اساسی و سایر مؤلفه‌های هارمونیکی برای همه حالت‌ها شامل بدون بار، بار کامل و سیگنال‌های جریان خطا استفاده کرد. به عبارت دیگر الگوریتم FFT می‌تواند اجزای دقیق فرکانس اساسی را از یک سیگنال ورودی مشخص استخراج کند. بر اساس الگوریتم FFT، اگر مؤلفه هارمونیک دوم جریان بیش از ۲۰ درصد مؤلفه اصلی افزایش یابد، آنگاه این وضعیت به عنوان یک جریان هجومی مغناطیسی در نظر گرفته می‌شود. به این ترتیب اگر مقدار هارمونیک ازحد معین بیشتر باشد، حفاظت هارمونیک روشن می‌شود و در غیر این صورت حفاظت هارمونیک خاموش است [۱۳].

۴-۳ دسته‌بندی مطالعات امنیت سایبری سیستم حفاظتی

هدف از این پژوهش، بررسی مطالعاتی است که در آنها تأثیر این حملات بر روی سیستم‌های حفاظتی شبکه قدرت در نظر گرفته شده است. دسته‌بندی مطالعات در زمینه مقابله با حملات سایبری در سیستم‌های حفاظتی شبکه قدرت در شکل ۶ مشاهده می‌شود.

1. Fast Fourier Transform



شکل ۷: دو رویکرد کلی ارتقای سطح امنیت سایبری شبکه قدرت.

حمله FDI به طور گسترده توسط بسیاری از محققین در شبکه‌های هوشمند مورد مطالعه قرار گرفته است [۶۴] تا [۶۷]. از سوی دیگر به دلیل اهمیت بسیار زیاد تأثیر حملات سایبری در سیستم‌های حفاظتی، این موضوع مورد توجه محققان قرار گرفته و در ۳ دسته کلی ارائه شده است:

۱) سیستم حفاظت خط انتقال [۱۴]، [۱۸]، [۱۹]، [۶۵] و [۶۸] تا [۷۰]
۲) سیستم حفاظت ترانسفورمر [۱۰]، [۱۱] و [۷۱] تا [۷۵]
۳) سیستم حفاظت ژنراتور [۳۳]، [۳۵] تا [۴۱] و [۴۳]

در ادامه به روش‌های مقاوم‌سازی[2] سیستم در برابر حملات سایبری پرداخته می‌شود.

۴- مقاوم‌سازی شبکه قدرت در برابر حمله سایبری

مقاوم‌سازی شبکه قدرت در برابر حمله سایبری این گونه است که دستگاه‌های نصب‌شده در سطح سیستم قدرت، هر کدام به صورت جداگانه حفاظت‌شده هستند؛ به این صورت هر یک از بخش‌های ابزار اندازه‌گیری، شبکه ارتباطی، سیستم تخمین حالت، سیستم مدیریت انرژی و کلیه سیستم‌های نظارتی و کنترل شبکه، حفاظت می‌شوند. در نتیجه، امنیت اطلاعات و صحت تصمیم‌گیری‌های اپراتور ارتقا پیدا می‌کند. به این ترتیب در مرحله اول با روش‌های مبتنی بر حفاظت تا حد امکان از نفوذ مهاجم سایبری جلوگیری می‌شود. در مرحله دوم با استفاده از روش‌های مبتنی بر تشخیص به ردیابی حمله سایبری احتمالی پرداخته می‌شود. از آنجا که تضمین قطعی برای عدم نفوذ مهاجم سایبری وجود ندارد، با بهره‌گیری از روش‌های تشخیص حمله می‌توان از پیشرفت حمله جلوگیری کرد. باید توجه داشت جلوگیری از پیشرفت حمله در هر مرحله می‌تواند مانع خسارت‌های کلان و حتی خاموشی سراسری شود. در جدول ۱ روش‌های مقابله با حملات سایبری در پژوهش‌ها به طور مختصر ارائه شده است. در شکل ۷ پژوهش‌های مقاوم‌سازی شبکه قدرت در برابر حمله سایبری در دو دسته مبتنی بر تشخیص و مبتنی بر حفاظت مشخص شده است.

۴-۱ روش‌های مبتنی بر مقاوم‌سازی

این روش‌ها در اصل، پیشگیری از وقوع حمله است. پیشگیری از وقوع حمله به معنای پیشگیری از خسارت، خرابی و ضرر به شبکه است. با استفاده از روش مبتنی بر حفاظت، کار به مرحله تشخیص نیز کشیده نمی‌شود و لذا بسیار ارزشمند است. در این راستا استفاده از زیرساخت‌های اندازه‌گیری و اندازه‌گیرهای پیشرفته واحدهای اندازه‌گیری فازوری (PMU)[3] برای حفاظت از نظارت، مدیریت و کنترل شبکه، بسیار اهمیت دارد. به طور کلی افزونگی[4] مناسب ابزار PMU در شبکه باعث افزونگی مناسب داده‌های امن می‌شود. منظور از داده‌های امن، اطلاعاتی از شبکه

2. Defense
3. Phasor Measurement Units
4. Redundancy

جدول ۱: روش‌های مقابله با حملات سایبری.

رویکرد	روش پیشنهادی	مراجع
مبتنی بر حفاظت	جایابی ابزار PMU با در نظر گرفتن استراتژی حمله سایبری و مدل AC شبکه	[۷۶]
	جایابی ابزار PMU با در نظر گرفتن استراتژی حمله سایبری و مدل DC شبکه	[۷۷]
مبتنی بر تشخیص	برآورد تفاوت بین توزیع‌های احتمال با اندازه‌گیری‌ها	[۶]
	تجزیه و تحلیل مدل حمله مهاجم	[۵۴]
	تحلیل مؤلفه اصلی قوی با معرفی قیود عناصر اصلی	[۶۳]
	تشخیص تزریق داده نادرست در سیستم تخمین حالت	[۶۵]
	انتخاب ابزار اندازه‌گیری کلیدی برای تشخیص حمله	[۶۸]
	مقایسه داده‌های جدید با پایگاه اطلاعات حملات	[۷۱]
	حفاظت از متغیرهای حالت بحرانی و تشخیص حمله	[۷۵]
	برنامه تخمین حالت پیشرفته	[۷۸]

است که دسترسی مهاجم به آنها غیرممکن یا بسیار دشوار می‌باشد یا در صورت تغییر جعلی آنها شبکه دچار مشکل نمی‌شود. تأمین افزونگی مناسب از داده‌های امن با برنامه جایابی PMUها صورت می‌گیرد.

از سوی دیگر استراتژی حمله، برنامه‌ریزی برای تزریق داده نادرست به پارامترهای اساسی شبکه است؛ به نحوی که حمله توسط اپراتور تشخیص داده نشود. در واقع استراتژی حمله، طرح حمله سایبری از نگاه مهاجم است؛ به نحوی که با حداقل هزینه، بیشترین خسارت و اختلال ایجاد شود. برنامه استراتژی حمله می‌تواند بر اساس مدل AC یا DC سیستم و با طرح مسائل بهینه‌سازی صورت بگیرد. از روش‌های مؤثر برای مقابله با این استراتژی‌ها استفاده از ابزار قدرتمند اندازه‌گیری داده‌های فازوری (PMU) است. در این برنامه علاوه بر امنیت سایبری، بهینه‌سازی هزینه‌ها نیز در نظر گرفته می‌شود. این رویکرد با بهره‌گیری از مدل AC سیستم قدرت در [۷۶] و با استفاده از مدل DC شبکه در [۷۷] ارائه شده است. در استراتژی حمله بر مبنای مدل AC که همه پارامترهای شبکه در نظر گرفته می‌شود، روابط و محاسبات آن پیچیده‌تر است؛ اما در استراتژی حمله بر مبنای مدل DC تعداد متغیرهای حالت، کمتر و روابط مدل‌سازی بسیار ساده‌تر است. به همین علت در مدل DC سرعت محاسبات سریع‌تر است و از متغیرهای حالتی که در نتیجه نهایی تأثیر کمی دارند، صرف نظر می‌شود.

۲-٤ روش‌های مبتنی بر تشخیص

روش‌های مبتنی بر تشخیص[1] در واقع بر مبنای تشخیص خطا عمل می‌کند و شامل الگوریتم‌های متفاوتی است که بنا به تخصص و سلیقه متخصصین این امر، طراحی شده و روش‌های زیادی نیز در مقالات آمده‌اند. آنچه که در روش‌های تشخیص حمله بسیار اهمیت دارد، بازگشت شبکه به حالت عادی بعد از وقوع یک حمله سایبری است [۷۸] تا [۸۱].

اگرچه برمبنای روش‌های حفاظتی، سیستم از وقوع بسیاری حملات محفوظ خواهد بود، اما همچنان احتمال آن که مهاجم موفق شود، وجود دارد. بر این اساس، روش‌های تشخیص می‌توانند حمله را ردیابی و از پیشرفت خطا جلوگیری کنند [۶]. لازمه دفاع قوی از شبکه در برابر حملات سایبری، بررسی مسئله از منظر مهاجم است. از این رو طرح حمله سایبری و بررسی استراتژی حمله از منظر مهاجم مورد توجه بسیاری از محققان این حوزه می‌باشد [۷۰].

1. Detect

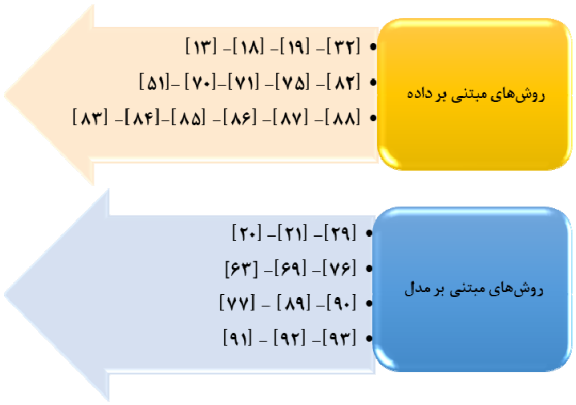
در اندازه‌گیری و انتقال داده‌های سیستم قدرت (مانند توان تزریقی در باس‌ها، توان خطوط و ترانسفورماتورها و مقادیر ولتاژ)، انتظار وجود نویز و خطا هست. در نتیجه، کمیته مهندسی برق، تکنیک‌های پیچیده‌ای برای تخمین حالت بخش‌های رؤیت‌ناپذیر شبکه و فیلتر داده‌های غلط، ایجاد کرده [۷۸] که این تکنیک‌ها برای اشتباهات احتمالی و خطای اندازه‌گیری مورد انتظار در شبکه سودمند است. با این حال، این نگرانی وجود دارد که ممکن است خطاهایی با روش مرسوم و فیلتر داده غلط، یافتنی نباشد. هنگامی که خطا از یک منبع مخرب (برای مثال، مهاجم سایبری) باشد، دیگر یک نویز مورد انتظار نیست و یک حمله سایبری محسوب می‌شود. اگر مهاجم بتواند از فیلترهای داده غلط[2] گذر کند، به عنوان یک حمله یک‌پارچه داده رؤیت‌ناپذیر[3] شناخته می‌شود [۶۴]. بنابراین تشخیص حمله سایبری فراتر از یک خطای اندازه‌گیری ساده است و با فیلترهای معمولی قابل ردیابی نیست. روش تشخیص داده بد[4] (BDD) برای خلاص‌شدن از اندازه‌گیری‌های اشتباه ناشی از حملات سایبری مورد استفاده قرار می‌گیرد. با این حال تضمینی برای آن که تمامی حملات با استفاده از روش BDD ردیابی شوند، وجود ندارد [۶۴]. حمله تزریق داده نادرست (FDI) که از مهم‌ترین حملات سایبری است، می‌تواند از سیستم BDD عبور کند و هر گونه تأثیری را بر روی مقادیر تخمین حالت وارد نماید. حملات تزریق داده نادرست به عنوان حمله فریبنده مخفی، حمله توزیع مجدد بار، حمله اطلاعات مخرب و حمله یکپارچه داده در پژوهش‌های مختلف شناخته شده است [۱]، [۲]، [۳۳]، [۳۸]، [۵۲]، [۵۴]، [۶۴] تا [۶۷] و [۸۲]. در [۶۵] تأثیر تزریق اطلاعات نادرست بر سیستم تخمین حالت، مدل‌سازی شده و یک طرح دفاعی مبتنی بر حفاظت و استراتژی دفاعی مبتنی بر تشخیص، پیشنهاد شده است.

مراجع [۶]، [۵۴]، [۶۳] و [۶۸] روش‌هایی برای تشخیص داده غلط ارائه کرده‌اند. به طور کلی، تشخیص نفوذ به دو نوع تشخیص سوءاستفاده[5] و تشخیص غیرمتعارف[6] دسته‌بندی می‌شود. در نوع اول، تشخیص بر مبنای خصوصیات شناخته‌شده حملات است. داده جدید با پایگاه دانش حملات مورد مقایسه قرار می‌گیرد و در صورت تطابق به عنوان حمله تشخیص داده می‌شود. این روش، قابلیت شناسایی حملات ناشناخته را ندارد. در نوع دوم یا همان تشخیص غیرمتعارف، رفتار متعارف و نرمال سیستم تعریف می‌شود و در صورت عدم تطابق داده‌های ثبت‌شده با رفتار نرمال سیستم به عنوان حمله سایبری گزارش خواهد شد. این روش، قابلیت شناسایی حملات ناشناخته را دارد [۸۳].

رویکرد دیگری که برای شناسایی حملات سایبری به کار می‌رود، تجزیه و تحلیل مدل حمله دشمن و ارائه روش دفاع متناظر است. این رویکرد نیز به دو دسته تقسیم می‌شود: می‌توان اندازه‌گیری‌های پایه‌ای را که توسط ابزار اندازه‌گیری (برای مثال دستگاه‌های PMUها) تهیه می‌شوند، بررسی کرد و راه دیگر، بازبینی متغیرهای حالت مستقل با استفاده از روش استراتژیک است [۵۴].

در دفاع از شبکه مقابل حمله سایبری، حفاظت از متغیرهای حالت بحرانی بسیار حائز اهمیت است؛ به این صورت که بعضی از متغیرهای حالت شبکه، کلیدی و مهم هستند. با شناسایی این متغیرها می‌توان خطا را ردیابی کرد [۷۵].

2. Bad Data Filters
3. Unobservable Data Integrity Attack
4. Bad Data Detection
5. Misuse Detection
6. Anomaly Detection



شکل ۸: دسته‌بندی الگوریتم‌های مقابله با حملات سایبری.

سیستم‌های قدرت فعلی از آشکارساز باقیمانده در روش تشخیص داده غلط استفاده می‌کنند. اندازه‌گیری باقیمانده، تفاوت بین اندازه‌گیری‌های مشاهده‌شده و اندازه‌گیری‌های برآوردشده (اندازه‌گیری‌هایی که بر اساس روابط تخمین زده می‌شوند) را محاسبه می‌کند. مقدار تفاوت محاسبه‌شده با یک حد از پیش تعیین‌شده مقایسه می‌شود و اگر از آستانه معین بیشتر باشد، یعنی خطایی رخ داده است و حمله تزریق داده نادرست شناسایی می‌شود [۵۴].

۵- الگوریتم‌های مقابله با حملات سایبری

دسته‌بندی الگوریتم‌های مقابله با حملات سایبری در شکل ۸ مشاهده می‌شود. همچنین خلاصه‌ای از مجموعه الگوریتم‌های مورد استفاده در زمینه روش‌های تشخیص حمله سایبری در شبکه قدرت در جدول ۲ ارائه شده است. مطابق جدول ۲ این الگوریتم‌ها را می‌توان به دو دسته کلی زیر طبقه‌بندی کرد:

۱) مبتنی بر داده [۱۳]، [۱۸]، [۱۹]، [۳۲]، [۵۱]، [۷۰]، [۷۱]، [۷۵] و [۸۲] تا [۸۸]

۲) مبتنی بر مدل [۲۰]، [۲۱]، [۲۹]، [۶۳]، [۶۹]، [۷۶]، [۷۷]، و [۸۹] تا [۹۳]

تجزیه و تحلیل آمارها نشان می‌دهد استفاده از الگوریتم‌های داده‌محور، بیشتر مورد توجه محققان قرار گرفته است. علت این امر، محدودیت الگوریتم مبتنی بر مدل در شبکه در حال رشد و افزایش پیچیدگی آن است [۵۱].

۵-۱ روش‌های مبتنی بر داده

در بسیاری از پژوهش‌ها برای مسئله مقابله با حمله سایبری در شبکه قدرت از الگوریتم‌های مبتنی بر داده استفاده می‌شود. در این نوع الگوریتم‌ها می‌توان از دانش و اطلاعات شبکه به صورت بهینه استفاده کرد تا شرایط وقوع حمله سایبری را نسبت به شرایط بدون حمله سایبری تشخیص داد. از مهم‌ترین روش‌های مبتنی بر داده که مورد توجه بسیاری از محققان در زمینه حفاظت سایبری می‌باشد، می‌توان به الگوریتم‌های یادگیری ماشین و یادگیری عمیق اشاره کرد. با توجه به ادغام شبکه قدرت فیزیکی به شبکه سایبری، به پیکربندی بهینه و قابل اطمینان اجزای شبکه پرداخته شده است. بدین منظور از مسئله بهینه‌سازی با روش مبتنی بر یادگیری- آموزش استفاده شده تا در کنار پیکربندی فیزیکی شبکه قدرت، سطح امنیت سایبری شبکه نیز ارتقا یابد. در این روش،

جدول ۲: دسته‌بندی الگوریتم‌های مقابله با حملات سایبری.

روش	الگوریتم استفاده‌شده	مراجع
مبتنی بر داده	برنامه‌نویسی پایتون	[۱۳]
	داده‌های تنظیمات عناصر حفاظتی مجاور	[۱۸]
	یادگیری ماشین	[۱۹]
	یادگیری عمیق	[۳۲]
	یادگیری ماشین	[۵۱]
	یادگیری عمیق	[۷۰]
	یادگیری ماشین- یادگیری عمیق	[۷۱]
	یادگیری عمیق چندعاملی توزیع‌شده	[۷۵]
	یادگیری ماشین	[۸۲]
	یادگیری عمیق	[۸۳]
	یادگیری- آموزش	[۸۴]
	یادگیری ماشین عمیق	[۸۵]
	بررسی هماهنگی داده‌های مربوط به تنظیمات رله‌ها	[۸۶]
	استفاده از داده‌های واحد اندازه‌گیری فازوری (PMU)	[۸۷]
	شبکه عصبی عمیق	[۸۸]
مبتنی بر مدل	تخمین حالت	[۲۰]
	مدل بازی دونفره مجموع صفر	[۲۱]
	مدل‌سازی بر اساس شبکه مؤلفه خطا	[۲۹]
	تطابق با مدل تپ‌چنجر ترانسفورمر	[۶۳]
	نسبت جریان تزریقی به ولتاژ باس در ترانسفورمر شیفت فاز	[۶۹]
	استراتژی حمله بر اساس مدل AC و جایابی ابزار PMU	[۷۶]
	استراتژی حمله بر اساس مدل DC و جایابی ابزار PMU	[۷۷]
	استفاده از روابط نسبت اختلاف به مجموع جریان و ولتاژ	[۸۹]
	مدل‌سازی منابع تجدیدپذیر و پارامترهای مورد نظر حمله	[۹۰]
	مدل رگرسیون خطی چندگانه	[۹۱]
	تخمین حالت دینامیکی	[۹۲]
	استفاده از مدل تخمین حالت شبکه	[۹۳]

شاخص انرژی مورد انتظا تأمین‌نشده (EENS)[1] ملاک آموزش الگوریتم قرار گرفته تا به این ترتیب مزایای زیادی را از جمله کاهش خاموشی و افزایش سود اقتصادی به همراه داشته باشد [۸۴]. همچنین در [۸۵] از روش‌های مبتنی بر داده، الگوریتم یادگیری ماشین عمیق است که در بسیاری از پژوهش‌ها از آن برای مقابله با حملات سایبری استفاده می‌شود. هدف از روش پیشنهادی، جلوگیری از حملاتی است که قرائت اطلاعات مشترکین را دستکاری می‌کنند و حضور منابع تجدیدپذیر نیز در نظر گرفته شده است. برای تشخیص حملات یک شبکه هوشمند در مقیاس بزرگ، روش یادگیری عمیق بدون نظارت می‌تواند از نظر محاسباتی، کارآمد و قابل اعتماد باشد. این روش منجر به نرخ بالای تشخیص می‌شود و طبق نتایج شبیه‌سازی، مطابقت خوبی دارد [۷۰]. برخی از مطالعات موردی در استرالیای جنوبی نشان می‌دهد که تکنیک‌های یادگیری ماشین، مانند یادگیری عمیق در شناسایی و پاسخ به تهدیدات سایبری کمک می‌کند [۷۱]. برای حفاظت دیفرانسیل شین‌ها روش تشخیص حمله سایبری با استفاده از الگوریتم یادگیری عمیق با حمله مقدار نمونه (SV)[2] ارائه شده است. برای مقابله با این حمله سایبری، روش دسته‌بندی داده‌های شبکه بررسی شده است. همچنین برای تشخیص خطاهای باسبار و حملات SV، یک الگوریتم بهینه‌سازی

1. Expected Energy Not Supplied
2. Sampled Value

معرفی می‌شود و داده‌های بهبودیافته از طریق یک معیار حفاظت دیفرانسیل مبتنی بر مؤلفه خطا تأیید می‌شوند [۸۳]. پژوهش‌های محدودی جهت توسعه یک چارچوب دفاع سایبری مبتنی بر هوش مصنوعی برای محافظت از ترانسفورمرها صورت گرفته است. برخی از روش‌های قبلی به دلیل محاسبات بالا و نیازهای سیستم ذخیره‌سازی برای شبکه‌های بزرگ و پیچیده مناسب نیستند [۷۰]. جهت مقابله با تهدیدات امنیتی ترانسفورمرها باید بر روی امنیت عملیات فنی و مدیریت داده‌های سیستم تمرکز شود. این موضوع، شامل افزایش قابلیت اطمینان و تاب‌آوری، نظارت و ذخیره داده‌ها و اطلاعات است. از آنجا که ابزار اندازه‌گیری و لوازم جانبی موجود در ترانسفورمرها، قدرت محاسباتی محدودی دارند، حملات خصمانه باید بررسی شوند. در این راستا شناسایی منابع مختلف تهدیدات و چالش‌های امنیتی از جمله حملات شناخته‌شده و ناشناخته باید مورد مطالعه قرار گیرد. تاکنون تحقیقات گسترده‌ای بر روی کنتورهای هوشمند برای شناسایی حملات و دفاع‌های مختلف در برابر آنها انجام شده است [۳۲]. ماهیت جمع‌آوری اطلاعات دوره‌ای کاملاً منحصربه‌فرد و متفاوت از کنتورهای هوشمند است. این اطلاعات شامل نظارت و مانیتورینگ زمان واقعی پارامترهای حیاتی ترانسفورمر مانند تنظیم ولتاژ OLTC، کنترل دما و سیستم خنک‌کننده می‌شود. سیستم تشخیص حمله سایبری مبتنی بر یادگیری عمیق برای رله‌های حفاظتی خطوط انتقال، ابتدا با اندازه‌گیری‌های جریان و ولتاژ آموزش داده می‌شود که نشان‌دهنده انواع مختلف خطاها در خطوط انتقال است. سپس از سیستم تشخیص حمله سایبری برای شناسایی اندازه‌گیری‌های جریان و ولتاژی که به طور مخرب توسط مهاجم تزریق می‌شوند، استفاده می‌شود تا رله‌های حفاظتی خط را فعال کنند [۳۲]. هدف از سیستم تشخیص حمله سایبری پیشنهادی، شناسایی الگوهایی در اندازه‌گیری‌های ابزار CT و VT است که با رفتار عادی اندازه‌گیری‌ها مطابقت ندارند. لازم به ذکر است که مفهوم رفتار عادی اندازه‌گیری‌ها در این مقاله شامل دینامیک بدون عیب شبکه و دینامیک در هنگام خطاهای معمول سیستم قدرت است. در مرحله آموزش آفلاین جهت اعتبارسنجی و آزمایش، مدل پیشنهادی رفتار طبیعی اندازه‌گیری‌های جریان و ولتاژ را در هنگام خطاهای خط یاد می‌گیرد. در مرحله عملیاتی بلادرنگ، سیستم تشخیص حمله سایبری اندازه‌گیری‌های غیرعادی را شناسایی می‌کند که با رفتار عادی اندازه‌گیری‌ها مطابقت ندارند. در [۳۲] سیستم شناسایی حملات سایبری پیشنهادی، هر اندازه‌گیری غیرمتعارف را به عنوان یک حمله سایبری دسته‌بندی می‌کند. این بدان معنا است که در حالت شناسایی، یک هشدار تولید می‌شود و یا در حالت شناسایی و کاهش، دستوراتی به IEDها (تجهیزات الکتریکی توزیع) ارسال می‌شود تا اندازه‌گیری‌های غیرمتعارف به‌طور خودکار مسدود شوند. در چارچوب‌های تشخیص ناهنجاری معمولی، نوع ناهنجاری تمایز داده نمی‌شود؛ زیرا به‌طور صریح مدل نمی‌شود. مزیت این روش آن است که حملات سایبری جدیدی که پیش‌تر شناخته نشده‌اند، تا زمانی که شامل اندازه‌گیری‌های غیرمتعارف باشند، قابل شناسایی هستند [۳۲]. از دیگر روش‌های مبتنی بر داده، الگوریتم چندعاملی یادگیری عمیق توزیع‌شده (MADDL)[1] است. در واقع، رله‌های دیستانس در سیستم حفاظتی شبکه قدرت به عنوان عوامل یک سیستم چندعاملی در نظر گرفته می‌شوند. این عوامل بر اساس یک گراف معادل به یکدیگر متصل شده و برای آن نظریه گراف جبری معرفی می‌شود. لازم به ذکر است که اتصالات بین عوامل سیستم چندعاملی مورد نظر بهینه‌سازی شده‌اند تا هزینه‌های اتصال کمینه شود [۷۵]. علاوه بر این، سیاست جدیدی برای طبقه‌بندی وضعیت‌های شبکه انتخاب می‌شود. در واقع برای هر رله دیستانس، زمانی که خطا در یک خط رخ داده است، ولتاژها و جریان‌های اندازه‌گیری‌شده توسط عوامل همسایه که همان رله‌های دیستانس مجاور هستند، تحت تأثیر قرار می‌گیرند؛ بنابراین ورودی‌های طبقه‌بندی‌کننده در هر عامل، کلیه ولتاژها و جریان‌های محلی و همسایه است. نهایتاً یک شبکه عصبی عمیق برای ارائه یک طبقه‌بندی سریع به کار گرفته می‌شود که توانایی دسته‌بندی تعداد زیادی داده از عوامل همسایه دارد. روش پیشنهادی بر اساس سیستم توزیع و رله‌های دیستانس بخش‌های مختلف است [۷۵].

روش یادگیری ماشین برای افزایش امنیت سایبری رله‌های محافظ دیفرانسیل ترانسفورمر در سیستم‌های قدرت بسیار مؤثر است. الگوریتم‌های یادگیری ماشین مانند الگوریتم‌های خوشه‌بندی، رگرسیون یا طبقه‌بندی می‌تواند به‌طور خاص برای ترانسفورمرها مورد بررسی قرار گیرد و به این ترتیب، زمانی که لازم است بین داده‌های واقعی و داده‌های جعلی مخرب تمایز داده شود. بنابراین به نظر می‌رسد که استفاده از چارچوب‌های مبتنی بر هوش مصنوعی و تکنیک‌های یادگیری ماشین، راهی مؤثر برای ارتقای امنیت سایبری سیستم قدرت ارائه می‌دهد [۵۱]. به این منظور رمزگذاری برای اندازه‌گیری‌های فعلی که عاری از حملات سایبری هستند، آموزش داده می‌شود تا بتواند چنین اندازه‌گیری‌های بدون حمله را به دقت بازسازی کند. از آنجایی که بازسازی اندازه‌گیری‌های غیرعادی که در طول حملات رخ می‌دهند ممکن است به خوبی بازسازی نشود، رمزگذار خودکار روی داده‌های حاوی حملات سایبری آموزش ندیده است. هدف، استفاده از آستانه خطای بازسازی خودکار رمزگذار به‌عنوان ابزاری برای تشخیص اندازه‌گیری‌های غیرعادی است که می‌تواند نشان‌دهنده حملات سایبری باشد. اگرچه اپراتورهای پست و مرکز کنترل، خاموش‌شدن ترانسفورمر را مشاهده می‌کنند، اما نمی‌توانند قبل از انجام یک بررسی جامع در مورد دلیل خاموش‌شدن ترانسفورمر، آن را مجدداً روشن کنند [۱۹].

وجود الگوریتم‌های یادگیری ماشین برای تشخیص ناهنجاری، یک استراتژی کاهش برای جلوگیری از عملکرد نادرست رله حفاظتی ناشی از حملات سایبری ارائه می‌کند [۱۹]، [۵۱]، [۷۱] و [۸۵]. حمله به سیستم حفاظتی می‌تواند به این صورت باشد که رله در شرایط وقوع خطا از داده ورودی رله دیگری استفاده کند و در نتیجه، نادرست عمل خواهد کرد. طبق فرض این پژوهش، تهدید ایجادشده توسط رله‌ها فقط در زمان وقوع خطا برای شبکه است. در رویکرد پیشنهادی از یک روش مبتنی بر یادگیری ماشین استفاده شده که در آن دو شبکه عصبی مختلف به نام‌های تولیدکننده و تشخیص‌دهنده در شرایط یک بازی صفر- جمعی با یکدیگر رقابت می‌کنند و زیان یکی، بهره‌ای برای دیگری است. این تکنیک به یادگیری داده‌های جدید تولیدی با آمارهای مجموعه آموزشی داده‌شده می‌پردازد [۸۲]. در نتیجه یک ترانسفورمر قدرت همراه با الگوریتم‌های حفاظتی آن در عمل شبیه‌سازی می‌شود. این الگوریتم‌ها بر روی یک رایانه صنعتی مجزا اجرا می‌شوند تا از طریق آنها ترانسفورمر از انواع خطاها محافظت شود. همچنین از این شبیه‌سازی‌ها برای تحلیل سطح حمله سایبری و نقاط مداخله در یک ترانسفورمر که مهاجم می‌تواند علیه آنها عمل کند، استفاده شده است [۱۳]. روش دفاعی پیشنهادی دیگر برای نوع حمله به تنظیمات رله می‌باشد و مستلزم این است که رله‌های حفاظتی در تعیین ثبات تنظیمات رله جدید با یکدیگر همکاری کنند. به این ترتیب هر رله به برقراری ارتباط با رله‌های همسایه و رله‌های محافظ

1. Multi-Agent Distributed Deep Learning

نیاز دارد. با اجرای این طرح، رسیدن به حمله موفقیت‌آمیز برای مهاجم سخت می‌شود و موفقیت تنها در صورتی حاصل می‌شود که همه رله‌ها مورد حمله قرار گیرند. رله‌ها می‌توانند داخل یک پست یا در پست‌های مختلف قرار گیرند. این همکاری مستلزم آن است که هر رله، اطلاعات مربوط به تنظیمات رله‌های همسایه خود و همچنین اطلاعات امپدانس تمام خطوط اطراف خود را ذخیره کند. در نتیجه هر رله، ارزیابی مستقلی از تغییرات پیشنهادی در تنظیمات انجام می‌دهد و می‌تواند به طور مستقل در مورد هماهنگی تنظیمات پیشنهادی رله‌های همسایه با تنظیمات خودش تصمیم بگیرد. اگر حداقل یک رله، تغییرات تنظیمات را تأیید نکند، تنظیمات پیشنهادی نهایی نمی‌شوند. به عبارت دیگر، رله غیرمنطبق، سیگنالی را صادر می‌کند که توسط رله هدف دریافت می‌شود و تلاش برای تغییر تنظیمات رله را مسدود می‌کند [۱۸].

استراتژی برای عملکرد زون ۳ یک رله فاصله با استفاده از داده‌های واحد اندازه‌گیری فازوری (PMU)[1] پیشنهاد شده است. به این ترتیب، یک طرح نظارتی رله‌محور (RCS)[2] ارائه شده است که از جریان دیفرانسیل خطوط پشتیبان یک رله معین، برای تصمیم‌گیری و نظارت استفاده می‌کند. حمله مورد نظر، حمله مقدار نمونه (SV) می‌باشد. برای تشخیص خطاهای شین و حملات SV، یک الگوریتم بهینه‌سازی معرفی می‌شود و داده‌های بهبودیافته از طریق یک معیار حفاظت دیفرانسیل مبتنی بر مؤلفه خطا تأیید می‌شوند [۸۷].

۵-۲ روش‌های مبتنی بر مدل

یکی از رویکردهای مقابله با حملات سایبری، استفاده از برنامه تخمین حالت است. به این ترتیب که با اجرای الگوریتم تخمین حالت و بر اساس روابط سیستم، پارامترهای شبکه، تخمین زده می‌شود. سپس با محاسبه اختلاف مقادیر برآوردشده و مقادیر اندازه‌گیری‌شده، دستکاری در اطلاعات و نفوذ مهاجم سایبری تشخیص داده می‌شود؛ چرا که مهاجم با دستکاری در اندازه‌گیری‌های ورودی، مقادیر خروجی تخمین حالت را تغییر می‌دهد [۹۳]. تزریق داده‌های نادرست (FDI)، نوعی حمله سایبری مخرب در برابر تخمین حالت می‌باشد. در این نوع حمله، مهاجمان با دستکاری در اندازه‌گیری‌های شبکه، خروجی تخمین حالت‌ها را تغییر می‌دهند. این تزریق اطلاعات نادرست می‌تواند به نحوی انجام شود که بدون تأثیر بر باقی اندازه‌گیری‌ها با موفقیت کنار گذاشته شود و اپراتور را گمراه کند. از دست رفتن و یا انحراف اندازه‌گیری‌ها باعث توزیع توان غیربهینه و یا قطع بارهای غیرضروری می‌شود. این به آن علت است که اپراتور، تصمیم‌های غیراقتصادی، غیربهینه و یا خطرناک خواهد گرفت و این موضوع به علت اطلاعات دستکاری‌شده دریافتی است [۹۴].

در رویکرد مبتنی بر مدل، یک مدل نظری جامع برای ارتباط بین هزینه و احتمال حمله سایبری موفق ارائه شده است [۲۱]. به این منظور، مسئله تخصیص بودجه بهینه، معیار تقویت بهینه بر اساس بودجه موجود و پیکربندی سیستم توزیع ارائه می‌شود. همچنین تعامل بین مهاجم و مدافع با استفاده از مدل بازی دونفره مجموع صفر به صورت ریاضی فرموله می‌شود تا بهترین استراتژی تقویتی پیدا شود. در مدل بازی خصمانه دونفره مجموع صفر، مدافع یک استراتژی برای به حداقل رساندن بازده مهاجم به کار می‌گیرد و مهاجم استراتژی را برای به حداکثر رساندن آن انتخاب می‌کند. مهاجم سعی می‌کند روی مجموعه‌ای از رله‌ها در سیستم توزیع آسیب برساند که میزان تأثیرگذاری آن، انرژی مورد انتظار مصرف‌نشده (EENS)[3] در سیستم است. از طرف دیگر، مدافع سعی می‌کند EENS را با استفاده از روش‌های موجود برای تقویت رله‌ها با تخصیص بهینه بودجه موجود به حداقل برساند. یک طرح حفاظتی دیفرانسیل توان بر اساس شبکه مؤلفه خطا (FCN)[4] پیشنهاد می‌شود که عاری از تشخیص جریان هجومی است و محاسبات مورد نیاز کمی دارد. به این ترتیب که ابتدا توان دیفرانسیل جزء خطا (FCDP)[5] که به عنوان دیفرانسیل توان اکتیو ترانسفورمر در FCN تعریف می‌شود، تحت شرایط مختلف، تجزیه و تحلیل می‌شود. سپس طرح حفاظت از ترانسفورمر بر اساس FCDP و دیفرانسیل توان معمولی ارائه شده است. همچنین الگوریتم حذف جریان DC میراشونده (DDC)[6] برای تخمین دقیق FCDP توسعه داده شده است [۲۹]. برخی محققان بر روی رله دیفرانسیل خط (LCDR) تمرکز داشته و روشی برای تشخیص FDIA با استفاده از رؤیتگر ورودی ناشناخته (UIO)[7] پیشنهاد شده است [۸۸]. روش پیشنهادی دارای یک مدل دنباله مثبت (PS) و یک دنباله منفی (NS) است که هر کدام از یک UIO برای تخمین حالات سیستم بر اساس مدل فضای حالت خط معیوب تشکیل می‌شود. تابع باقیمانده (RF)[8] برای هر مدل، تفاوت بین ولتاژ اندازه‌گیری‌شده و تخمین دنباله مرتبط با آن مدل تعریف می‌شود. افزایش RFها پس از برداشت اطلاعات LCDR نشان‌دهنده حمله FDI است و سیگنال تریپ LCDR مسدود می‌شود. با این حال روش پیشنهادی در سیستم‌های اتوماسیون پست مبتنی بر IEC۶۱۸۵۰، تنها در صورتی قابل اجراست که اندازه‌گیری‌های محلی به اشتراک گذاشته‌شده توسط واحدهای مربوطه، ایمن باشند [۲۰]. یک طرح پیشنهادی دیگر در مسئله حمله سایبری مقابل LCDR استفاده از یک شبکه عصبی عمیق (DNN)[9] است که به صورت آفلاین بر روی ویژگی‌های استخراج‌شده از اندازه‌گیری‌های موجود برای LCDRها آموزش داده شده است [۸۸].

موضوع حمله سایبری در تپ‌چنجر و ترانسفورمر شیفت فاز نیز حائز اهمیت است. یک شاخص تشخیص نفوذ سایبری با توجه به ویژگی‌های مشخص، حملات پنهان را از سناریوهای عملیاتی عادی متمایز می‌کند. ترانسفورمرها به طور مکرر با استفاده از تغییردهنده‌های تپ بار (OLTC) جهت تطابق با مجموعه‌ای از ولتاژهای مشخص، تحت یک طرح کنترل ولتاژ خودکار، تغییر می‌کنند؛ بنابراین این تجهیز می‌تواند هدف بسیاری از حمله‌های سایبری باشد [۶۳] و [۶۹]. جهت بهبود عملکرد رله، پیشنهاد شده است که در الگوریتم مربوطه، از هردو نمونه‌های ولتاژ و جریان، برای محاسبات عملکرد رله دیفرانسیل، استفاده شود. به این صورت که دو شرط به شرط اصلی جریان دیفرانسیل در رله دیفرانسیل اضافه کرده و باعث بهبود عملکرد رله شده است. دو شرط ارائه‌شده از نسبت اختلاف جریان (ولتاژ) به مجموع جریان (ولتاژ) دو طرف ترانسفورمر بهره گرفته است [۸۹]. در یک سیستم قدرت، دستورات شیفت فاز از طریق سیستم SCADA انتقال می‌یابد؛ به همین دلیل کنترل مربوطه، قابلیت حملات سایبری، به ویژه حملات پنهان را دارد. دستورات شیفت فاز جعلی می‌تواند

1. Phasor Measurement Unit
2. Relay Centric Supervisory
3. Expected Energy not Served
4. Fault Component Network
5. Fault Component Differential Power
6. Decaying Direct Current
7. Unknown Input Observer
8. Residual Function
9. Deep Neural Network

شکل ۹: شاخص‌های ارزیابی تاب‌آوری در برابر حملات سایبری.

باعث بارزدایی شدید در خطوط حیاتی شود که موجب قطع آنها شده و باعث زیان‌های مالی می‌شود. یک روش مقابله با حملات پنهان (که سیستم تشخیص داده‌های غلط را دور می‌زند) الگوریتمی است که بر مبنای شاخص نسبت جریان تزریقی باس به ولتاژهای انتهایی، استوار است [۶۹].

٦- شاخص‌های تاب‌آوری در برابر حملات سایبری

مسئله تاب‌آوری در برابر کارشکنی‌های سایبری به رله‌ها به عنوان اجزای کلیدی و مهم سیستم‌های حفاظتی شبکه، موضوع بسیار مهمی است که تاکنون کمتر به آن پرداخته شده است [۹۵]. به طور کلی یک راهکار خوب برای سیستم کنترلی و حفاظتی با تاب‌آوری بالا، استفاده از روش‌های کدگذاری/ رمزگشایی برای محافظت از اطلاعات اساسی و سیگنال‌های ارسالی است [۹۶]. از سوی دیگر باید تاب‌آوری برنامه‌های تخمین حالت در نظر گرفته شود. همان طور که پیش‌تر شرح داده شد، خروجی برنامه تخمین حالت در سیستم تشخیص حملات سایبری بسیار حائز اهمیت و ارتقای تاب‌آوری آن مورد توجه محققان است [۹۷]. تلاش در جهت افزایش تاب‌آوری خروجی سیستم‌های کنترلی در برابر حملات سایبری، باعث تشخیص موفق‌تر حمله فریب ناشناخته خواهد شد [۹۸] تا [۱۰۰]. به منظور بررسی ارتقای تاب‌آوری سیستم، معیارهای مختلف مناسب برای سنجش تاب‌آوری ارائه می‌گردد. تعیین کمیت توانایی و هزینه لازم برای بازیابی سیستم در اثر یک حمله سایبری، به عنوان یک معیار مناسب سنجش تاب‌آوری پیشنهاد شده است [۷۴]. روش دیگر ارزیابی تاب‌آوری برای سیستم‌های قدرت، تحت حملات متوالی پیشنهاد می‌شود. به این منظور، شکست آبشاری ژنراتورها در نظر گرفته شده و شاخص تاب‌آوری جدید برای منعکس‌کردن قابلیت سیستم قدرت برای ارائه توان تحت حملات متوالی پیشنهاد شده است [۳۴]. همچنین نسبت بارهای عرضه‌شده در شبکه در طول فرایند بازیابی پس از حمله به عنوان شاخص ارزیابی تاب‌آوری شبکه در برابر حمله سایبری استفاده شده است [۱۰۱].

در شکل ۹ دسته‌بندی انواع شاخص‌های ارزیابی تاب‌آوری مشاهده می‌شود. به طور کلی در تعریف شاخص‌های تاب‌آوری، میزان بار از دست رفته یا هزینه‌های تحمیل‌شده به شبکه مورد بررسی قرار می‌گیرد. با توجه به این که جلوگیری از پیشرفت حمله سایبری بسیار حائز اهمیت می‌باشد، ارزیابی تاب‌آوری شبکه در برابر حمله سایبری توسط شاخص ارزیابی تاب‌آوری، بسیار مفید است.

۷- نتیجه‌گیری

با توجه به اهمیت امنیت سایبری سیستم‌های حفاظتی در شبکه قدرت، در این مقاله به بررسی و دسته‌بندی پژوهش‌های مربوطه پرداخته شد. در ابتدا انواع آسیب‌پذیری‌های سیستم حفاظتی، شامل سیستم ژنراتور، خط انتقال و ترانسفورمر ارائه گردید. سپس به راهکارهای مقابله با حملات سایبری پرداخته شد. در مقابله با نفوذ مهاجم سایبری ابتدا باید راهکارهای پیشگیری و جلوگیری از وقوع حمله را اتخاذ کرد. در بعضی از پژوهش‌ها با استفاده از ابزار اندازه‌گیری PMU افزونگی اندازه‌گیری‌های امن افزایش یافته تا دست مهاجم در طرح حمله سایبری بسته شود. در مرحله بعد برای مقابله با حملات سایبری، سیستم تشخیص حمله ارائه می‌گردد. هدف از تشخیص حمله، جلوگیری از پیشرفت مهاجم و متوقف‌کردن خسارت‌های احتمالی است. به این منظور می‌توان از روش‌های مبتنی بر مدل و مبتنی بر داده استفاده نمود. الگوریتم‌های مختلفی طبق بررسی‌های صورت‌گرفته برای روش مبتنی بر داده به کار می‌رود که از مهم‌ترین آنها می‌توان به الگوریتم یادگیری عمیق، یادگیری ماشین و شبکه عصبی اشاره کرد. همچنین در رویکرد مبتنی بر مدل، برنامه تخمین حالت و استفاده از روابط حاکم بر شبکه قدرت، اهمیت بسزایی دارد. نهایتاً توجه به مجموعه تلاش محققان در زمینه مقابله با حملات سایبری و به‌کارگیری روش‌های مؤثر، گامی مهم در ارتقای سطح امنیت سایبری است. باید توجه داشت که مهاجم سایبری نیز متقابلاً روش‌های نفوذ قوی‌تر و حملات سایبری جدید، برنامه‌ریزی می‌کند. بنابراین ارائه روش‌های حفاظت و تشخیص جدید، مستقل از نوع حمله سایبری، اهمیت ویژه‌ای دارد که باید به آن پرداخته شود.

مراجع

[1] Y. Xiang, Z. Ding, Y. Zhang, and L. Wang, "Power system reliability evaluation considering load redistribution attacks," *IEEE Trans. on Smart Grid*, vol. 8, no. 2, pp. 889-901, Mar. 2017.

[2] Y. Xiang and L. Wang, "A game-theoretic study of load redistribution attack and defense in power systems," *Electric Power Systems Research*, vol. 151, pp. 12-25, Oct. 2017.

[3] N. Rajeswaran, *et al.*, "A study on cyber-physical system architecture for smart grids and its cyber vulnerability," In: H. Haes Alhelou, N., Hatziargyriou, and Z. Y. Dong (eds) Power Systems Cybersecurity. Power Systems *Power Systems Cybersecurity*, pp. 413-427, Springer, 2023.

[4] J. Sakhnini, H. Karimipour, A. Dehghantanha, R. M. Parizim, and G. Srivastava, "Security aspects of Internet of Things aided smart grids: a bibliometric survey," *Internet of Things*, vol. 14, Article ID: 100111, Jun. 2021.

[5] S. Riahinia, A. Ameli, M. Ghafouri, and A. Yassine, "Cyber-security of protection system in power grids-part 1: vulnerabilities and counter-measures," In: H. Haes Alhelou, N., Hatziargyriou, and Z. Y. Dong (eds) Power Systems Cybersecurity. Power Systems *Power Systems Cybersecurity*, pp. 203-237, Springer, 2023.

[6] A. Hassan, *et al.*, "A survey and bibliometric analysis of different communication technologies available for smart meters," *Cleaner Engineering and Technology*, vol. 7, Article ID: 100424, Apr. 2022.

[7] J. Jarmakiewicz, K. Parobczak, and K. Maślanka, "Cybersecurity protection for power grid control infrastructures," *International J. of Critical Infrastructure Protection*, vol. 18, pp. 20-33, Sept. 2017.

[8] GE Power Management, *Relay Selection Guide*, 40 pp., https://www.gegridsol utions.com/multilin/notes/get-8048a.pdf

[9] K. Islam, D. Kim, and A. Abu-Siada, "A review on adaptive power system protection schemes for future smart and micro grids, challenges and opportunities," *Electric Power Systems Research*, vol. 230, Article ID: 110241, May 2024.

[10] Y. M. Khaw, *et al.,* "Preventing false tripping cyberattacks against distance relays: a deep learning approach," in *Proc. IEEE Int. Conf. on Communications, Control, and Computing Technologies for Smart Grids*, 6 pp., Beijing, China, 21-23 Oct. 2019.

[11] T. A. Abd Almuhsen and A. J. Sultan, "Coordination of directional overcurrent, distance, and breaker failure relays using genetic algorithm including pilot protection," in *Proc. IOP Conf. Series: Materials Science and Engineering*, vol. 1105, 14 pp., Baghdad, Iraq, 21-22 Dec. 2021.

[12] M. Zare Jahromi, A. Abiri Jahromi, S. Sanner, D. Kundur, and M. Kassouf, "Cybersecurity enhancement of transformer differential protection using machine learning," *IEEE Power & Energy Society General Meeting,* 5 pp., Montreal, Canada, 2-6 Aug. 2020.

[13] J. Olijnyk, B. Bond, and J. Rrushi, "Design and emulation of physics-centric cyberattacks on an electrical power transformer," *IEEE Access*, vol. 10, pp. 15227-15246, 2022.

[14] EN IEC 60255-187-1: 2021.

[15] A. Ayad, E. F. El-Saadany, M. M. A. Salama, and A. Youssef, "A learning-based framework for detecting cyber-attacks against line current differential relays," *IEEE Trans. on Power Delivery*, vol. 36, no. 4, pp. 2274-2286, Aug. 2020.

[16] A. M. Saber, A. Youssef, D. Svetinovic, H. H. Zeineldin, E. F. El-Saadany, "Anomaly-based detection of cyberattacks on line current differential relays," *IEEE Trans. on Smart Grid*, vol. 13, no. 6, pp. 4787-4800, Nov. 2022.

[17]] A.A. Bouramdane. "Cyberattacks in smart grids: challenges and solving the multi-criteria decision-making for cybersecurity options, including ones that incorporate artificial intelligence, using an analytical hierarchy process," *Journal of Cybersecurity and Privacy*, vol. 3, no. 4, pp. 662–705, 2023.

[18] R. Nuqui, J. Hong, A. Kondabathini, D. Ishchenko, and D. Coats, "A collaborative defense for securing protective relay settings in electrical cyber physical systems," in *Proc. 2018 Resilience Week*, pp. 49-54, Denver, CO, USA, 20-23 Aug. 2018.

[19] M. Zare Jahromi, A. Abiri Jahromi, S. Sanner, D. Kundur, and M. Kassouf, "Cybersecurity enhancement of transformer differential protection using machine learning," *IEEE Power & Energy Society General Meeting,* 5 pp., Montreal, Canada, 2-6 Aug. 2020.

[20] A. Ameli, A. Hooshyar, E. F. El-Saadany, and A. M. Youssef, "An intrusion detection method for line current differential relays," *IEEE Trans. on Information Forensics and Security*, vol. 15, pp. 329-344, 2019.

[21] M. Ganjkhani, M. M. Hosseini, and M. Parvania, "Optimal defensive strategy for power distribution systems against relay setting attacks," *IEEE Trans. on Power Delivery*, vol. 38, no. 3, pp. 1499-1509, Jun. 2023.

[22] V. S. Rajkumar, *et al.*, "Cyber attacks on power system automation and protection and impact analysis," in *Proc. IEEE PES Innovative Smart Grid Technologies Europe*, pp. 247-254, Hague, The Netherlands, 26-28 Oct. 2020.

[23] J. Wurm, K. Hoang, O. Arias, A. R. Sadeghi, and Y. Jin, "Security analysis on consumer and industrial IoT devices," in *Proc. IEEE 21st Asia South Pacific Des. Automat. Conf.,* pp. 519-524, Macao, China, 25-28 Jan. 2016.

[24] C. W. Johnson, M. H. Saleem, M. Evangelopoulou, M. Cook, R. Harkness, and T. Barker, "Defending against firmware cyber attacks on safety-critical systems," *J. Syst. Saf.*, vol. 54, no. 1, pp. 16-21, Spring 2018.

[25] D. Formby, S. S. Jung, S. Walters, and R. Beyah, "A physical overlay framework for insider threat mitigation of power system devices," in *Proc. IEEE Int. Conf. on Smart Grid Communications,* pp. 970-975, Venice, Italy, 3-6 Nov. 2014.

[26] A. Chattopadhyay, A. Ukil, D. Jap, and S. Bhasin, "Toward threat of implementation attacks on substation security: case study on fault detection and isolation," *IEEE Trans. Ind. Inform.*, vol. 14, no. 6, pp. 2442-2451, Jun. 2018.

[27] T. E. McDermott, J. D. Doty, J. G. O'Brien, C. R. Eppinger, and T. Becejac, *Cybersecurity for Distance Relay Protection*, No. PNNL-29663. Pacific Northwest National Lab., Richland, WA, USA, 2020.

[28] A. K. Maurya, P. Singhaal, and H. K. Pathak, "Analysis of cyber security attacks on power system networks and its protection schemes," in *Proc. 4th Int. Conf. on Advances in Electrical, Computing, Communication and Sustainable Technologies*, 6 pp., Bhilai, India, 11-12 Jan. 2024.

[29] F. Peng, *et al.*, "Power differential protection for transformer based on fault component network," *IEEE Trans. on Power Delivery*, vol. 38, no. 4, pp. 2464-2477, Aug. 2023.

[30] D. Yang, Y. Zhang, X. An, and Y. Hou, "Analysis of relay protection fault propagation mechanism and attack detection method under cyber attack," in *Proc. 3rd Int. Conf. on Electronic Information Engineering and Computer Communication,* 5 pp., Wuhan, China, 22-24 2023.

[31] Z. Q. Bo, X. N. Lin, Q. P. Wang, Y. H. Yi, and F. Q. Zhou, "Developments of power system protection and control," *Protection and Control of Modern Power Systems*, vol. 1, Article ID: 7, 2016.

[32] Y. M. Khaw, *et al.*, "A deep learning-based cyberattack detection system for transmission protective relays," *IEEE Trans. on Smart Grid*, vol. 12, no. 3, pp. 2554-2565, May 2020.

[33] L. Yu, X. M. Sun, and T. Sui, "False-data injection attack in electricity generation system subject to actuator saturation: analysis and design," *IEEE Trans. on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, pp. 1712-1719, Aug. 2019.

[34] L. Zeng, *et al.*, "Resilience assessment for power systems under sequential attacks using double DQN with improved prioritized experience replay," *IEEE Systems J.*, vol. 17, no. 2, pp. 1865-1876, Jun. 2022.

[35] S. D. Roy and S. Debbarma, "Detection and mitigation of cyber-attacks on AGC systems of low inertia power grid," *IEEE Systems J.*, vol. 14, no. 2, pp. 2023-2031, Jun. 2019.

[36] A. Ameli, A. Hooshyar, E. F. El-Saadany, and A. M. Youssef, "Attack detection and identification for automatic generation control systems," *IEEE Trans. on Power Systems*, vol. 33, no. 5, pp. 4760-4774, Sept. 2018.

[37] A. S. L. V. Tummala and R. K. Inapakurthi, "A two-stage Kalman filter for cyber-attack detection in automatic generation control system," *J. of Modern Power Systems and Clean Energy*, vol. 10, no. 1, pp. 50-59, Jan. 2021.

[38] Z. Qu, *et al.*, "Detection of false data injection attack in AGC system based on random forest," *Machines*, vol. 11, no. 1, Article ID: 83, Jan. 2023.

[39] S. Alhalali, N. Christopher, and R. El-Shatshat, "Mitigation of cyber-physical attacks in multi-area automatic generation control," *International J. of Electrical Power & Energy Systems*, vol. 112, pp. 362-369, Nov. 2019.

[40] S. Sarangan, V. K. Singh, and M. Govindarasu, "Cyber attack-defense analysis for automatic generation control with renewable energy sources," in *Proc. North American Power*, 6 pp., Fargo, ND, USA, 9-11 Sept. 2018.

[41] T. Huang, B. Satchidanandan, P. R. Kumar, and L. Xie, "An online detection framework for cyber attacks on automatic generation control," *IEEE Trans. on Power Systems*, vol. 33, no. 6, pp. 6816-6827, Nov. 2018.

[42] Z. Amiri, *et al.*, "Adventures in data analysis: a systematic review of deep learning techniques for pattern recognition in cyber-physical-social systems," *Multimedia Tools and Applications*, vol. 83, pp. 22909-22973, 2024.

[43] T. Behdadnia and G. Deconinck, Anomaly Detection in Automatic Generation Control Systems Based on Traffic Pattern Analysis and Deep Transfer Learning, arXiv preprint arXiv: 2209.08099, 2022.

[44] A. Ameli, A. Hooshyar, and E. F. El-Saadany, "Development of a cyber-resilient line current differential relay," *IEEE Trans. on Industrial Informatics*, vol. 15, no. 1, pp. 305-318, Jan. 2018.

[45] V. S. Rajkumar, A. Stefanov, A. Presekal, P. Palensky, and J. L. R. Torres, "Cyber attacks on power grids: causes and propagation of cascading failures," *IEEE Access*, vol. 11, pp. 103154-103176, 2023.

[46] A. Khaleghi, M. S. Ghazizadeh, and M. R. Aghamohammadi, "A deep learning-based attack detection mechanism against potential cascading failure induced by load redistribution attacks," *IEEE Trans. on Smart Grid*, vol. 14, no. 6, pp. 4772-4783, Nov. 2023.

[47] A. Ameli, *et al.*, "Vulnerabilities of line current differential relays to cyber-attacks," in *Proc. IEEE Power & Energy Society Innovative Smart Grid Technologies Conf.*, 5 pp., Washington, DC, USA, 18-21 Feb. 2019.

[48] A. Ameli, A. Hooshyar, and E. F. El-Saadany, "Development of a cyber-resilient line current differential relay," *IEEE Trans. on Industrial Informatics*, vol. 15, no. 1, pp. 305-318, Jan. 2019.

[49] L. Chen, *et al.*, "Remedial pilot main protection scheme for transmission line independent of data synchronism," *IEEE Trans. on Smart Grid*, vol. 10, no. 1, pp. 681-690, Jan. 2019.

[50] L. I. U. Raanaa, Condition Monitoring of Power Transformers in Digital Substations, MS Thesis, NTNU, 2020.

[51] H. Rahimpour, *et al.*, *Cybersecurity Challenges of Power Transformers*, arXiv preprint arXiv: 2302.13161, 2023.

[52] D. B. Unsal, T. S. Ustun, S. M. S. Hussain, and A. Onen, "Enhancing cybersecurity in smart grids: false data injection and its mitigation," *Energies*, vol. 14, no. 9, Article ID: 2657, May-1 2021.

[53] Y. Wang and J. P. Hespanha, "Distributed estimation of power system oscillation modes under attacks on GPS clocks," *IEEE Trans. on Instrumentation and Measurement*, vol. 67, no. 7, pp. 1626-1637, Jul. 2018.

[54] E. Shereen, *et al.*, "Feasibility of time-synchronization attacks against PMU-based state estimation," *IEEE Trans. on Instrumentation and Measurement*, vol. 69, no. 6, pp. 3412-3427, Jun. 2019.

[55] K. D. Lu and Z. G. Wu, "Genetic algorithm-based cumulative sum method for jamming attack detection of cyber-physical power systems," *IEEE Trans. on Instrumentation and Measurement*, vol. 71, Article ID: 9004810, 10 pp., 2022.

[56] P. Top, *et al.*, "Simulation of a RTU cyber attack on a transformer bank," in *Proc. IEEE Power & Energy Society General Meeting*, 5 pp., Chicago, IL, USA, 16-20 Jul. 2017.

[80] J. K. Narang and B. Bag, "Replay attack detection in overcurrent relays using mathematical morphology and LSTM autoencoder," in *Proc. IEEE Int. Conf. on Advanced Networks and Telecommunications Systems*, 6 pp., Gandhinagar, India, 18-21 Dec. 2022.

[81] L. Wang, *et al.*, "Power electronic attack targeting relay protection and corresponding detection method," in *Proc. IEEE 3rd Int. Conf. on Circuits and Systems,* pp. 203-206, Chengdu, China, 29-31 Oct. 2021.

[82] A. Aflaki, H. Karimipour, and A. N. Jahromi, "A GAN-based false data injection and civil attack detection framework for digital relays with feature selection," in *Proc. IEEE Int. Conf. on Systems, Man, and Cybernetics*, pp. 5027-5033, Honolulu, Oahu, HI, USA, 1-4 Oct. 2023.

[83] J. Mo and H. Yang, "Sampled value attack detection for busbar differential protection based on a negative selection immune system," *J. of Modern Power Systems and Clean Energy*, vol. 11, no. 2, pp. 421-433, Mar. 2022.

[84] M. Hamzeh, B. Vahidi, and A. Foroughi Nematollahi, "Optimizing configuration of cyber network considering graph theory structure and teaching-learning-based optimization (GT-TLBO)," *IEEE Trans. on Industrial Informatics*, vol. 15, no. 4, pp. 2083-2090, Apr. 2018.

[85] M. Ismail, M. F. Shaaban, M. Naidu and E. Serpedin, "Deep learning detection of electricity theft cyber-attacks in renewable distributed generation," *IEEE Trans. on Smart Grid*, vol. 11, no. 4, pp. 3428-3437, Jul. 2020.

[86] R. Nuqui, J. Hong, A. Kondabathini, D. Ishchenko, and D. Coats, "A collaborative defense for securing protective relay settings in electrical cyber physical systems," in *Proc. Resilience Week*, pp. 49-54, Denver, CO, USA, 20-23 Aug. 2018.

[87] M. Chougule, G. Gajjar, and S. A. Soman, "PMU supervised secure backup protection of distance relays," in *Proc. IEEE PES Innovative Smart Grid Technologies Europe*, 5 pp., Bucharest, Romania, 29 Sept.-2 Oct. 2019.

[88] A. M. Saber, A. Youssef, D. Svetinovic, H. H. Zeineldin, and E. F. El-Saadany, "Cyber-immune line current differential relays," *IEEE Trans. on Industrial Informatics*, vol. 20, no. 3, pp. 3597-3608, Mar. 2024.

[89] E. Ali, *et al.*, "Power transformer differential protection using current and voltage ratios," *Electric Power Systems Research*, vol. 154, pp. 140-150, Jan. 2018.

[90] P. Zhao, *et al.* "Cyber-resilience enhancement and protection for uneconomic power dispatch under cyber-attacks," *IEEE Trans. on Power Delivery*, vol. 36, no. 4, pp. 2253-2263, Aug. 2020.

[91] D. P. Chinta, *et al.* "Cyber resilient differential protection scheme for transmission lines," in *Proc.* 2023 *IEEE 3rd. Int. Conf. on Smart Technologies for Power, Energy and Control,* 4 pp., Bhubaneswar, India, 10-13 Dec. 2023.

[92] S. Shafiulla and M. K. Jena, "Dynamic state estimation based cyber attack detection scheme to supervise distance relay operation in transmission line," in *Proc. IEEE Int. Conf. on Power Electronics, Smart Grid, and Renewable Energy*, 6 pp., Trivandrum, India, 17-20 Dec. 2023.

[93] H. Margossian, R. Kfouri, and R. Saliba, "Measurement protection to prevent cyber-physical attacks against power system state estimation," *International J. of Critical Infrastructure Protection*, vol. 43, Article ID: 100643, Dec. 2023.

[94] A. Kemmeugne, A. A. Jahromi, and D. Kundur, "Resilience enhancement of pilot protection in power systems," *IEEE Trans. on Power Delivery*, vol. 37, no. 6, pp. 5255-5266, Dec. 2022.

[95] S. Pola, M. Jovanovic, M. A. Azzouz, and M. Mirhassani, "Cyber resiliency enhancement of overcurrent relays in distribution systems," *IEEE Trans. on Smart Grid*, vol. 15, no. 4, pp. 4063-4076, Jul. 2023.

[96] Y. Joo, Z. Qu, and T. Namerikawa, "Resilient control of cyber-physical system using nonlinear encoding signal against system integrity attacks," *IEEE Trans. on Automatic Control*, vol. 66, no. 9, pp. 4334-4341, Sept. 2020.

[97] G. Chen, Y. Zhang, S. Gu and W. Hu, "Resilient state estimation and control of cyber-physical systems against false data injection attacks on both actuator and sensors," *IEEE Trans. on Control of Network Systems*, vol. 9, no. 1, pp. 500-510, Mar. 2021.

[98] S. Liu, *et al.*, "Adaptive resilient output feedback control against unknown deception attacks for nonlinear cyber-physical systems," *IEEE Trans. on Circuits and Systems II: Express Briefs*, vol. 71, no. 8, pp. 3855-3859, Aug. 2024.

[99] W. Zhang, S. Mao, J. Huang, L. Kocarev, and Y. Tang, "Data-driven resilient control for linear discrete-time multi-agent networks under

[57] C. Avci, B. Tekinerdogan, and C. Catal. "Design tactics for tailoring transformer architectures to cybersecurity challenges," *Cluster Computing*, vol. 27, pp. 9587-9613, 2024.

[58] United States Senate Republican Policy Committee, *Infrastructure Cybersecurity: The US Electric Grid*, 2021.

[59] J. Olijnyk, B. Bond, and J. Rrushi, "Design and emulation of physics-centric cyberattacks on an electrical power transformer," *IEEE Access*, vol. 10, pp. 15227-15246, 2022.

[60] S. Hasheminejad. "A new protection method for the power transformers using Teager energy operator and a fluctuation identifier index," *Electric Power Systems Research*, vol. 213, Article ID: 108776, Dec. 2022.

[61] A. Klien, Y. Gosteli, and S. Mattmann, "Design and commissioning of a secure substation network architecture," in *Proc. 15th Int. Conf. on Developments in Power System Protection*, 5 pp., Liverpool, UK, 9-12 Mar. 2020.

[62] B. Ahn, *et al.*, "Security threat modeling for power transformers in cyber-physical environments," in *Proc. IEEE Power & Energy Society Innovative Smart Grid Technologies Conf.*, 5 pp., Washington, DC, USA, 16-18 Feb. 2021.

[63] S. Chakrabarty and B. Sikdar, "Detection of hidden transformer tap change command attacks in transmission networks," *IEEE Trans. on Smart Grid*, vol. 11, no. 6, pp. 5161-5173, Nov. 2020.

[64] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Trans. on Smart Grid*, vol. 11, no. 3, pp. 2218-2234, May 2020.

[65] L. Xu, L. Xiaoyi, and Y. Sun, "Detection of false data injection attacks in smart grid based on machine learning," In *Advances in Artificial Intelligence and Security: 7th Int. Conf., ICAIS 2021,* Dublin, Ireland, Jul. 2021, Proc. Part III 7, Springer, 2021.

[66] J. Q. Ruan, *et al.*, "AC sparse modeling for false data injection attack on smart gird," in *Proc. Asian Conf. on Energy, Power and Transportation Electrification*, 5 pp., Singapore, 24-26 Oct. 2017.

[67] C. Liu, H. Liang, T. Chen, J. Wu and C. Long, "Joint admittance perturbation and meter protection for mitigating stealthy FDI attacks against power system state estimation," *IEEE Trans. on Power Systems*, vol. 35, no. 2, pp. 1468-1478, Mar. 2020.

[68] M. Z. Jahromi, *et al.*, "Data analytics for cybersecurity enhancement of transformer protection," *ACM SIGEnergy Energy Informatics Review*, vol. 1, no. 1, pp. 12-19, Nov. 2021.

[69] S. Chakrabarty and B. Sikdar, "Detection of malicious command injection attacks on phase shifter control in smart grids," *IEEE Trans. on Power Systems*, vol. 36, no. 1, pp. 271-280, Jan. 2021.

[70] H. Karimipour, *et al.*, "A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids," *IEEE Access*, vol. 7, pp. 80778-80788, 2019.

[71] W. Sattinger, Critical Infrastructure Cyber Security: Applications of Machine Learning and Artificial Intelligence in Detecting, Responding, to and Containing Threats, CIGRETech. Rep., Ref D2-210_2020, 2020.

[72] N. Tatipatri and S. L. Arun, "A comprehensive review on cyber-attacks in power systems: impact analysis, detection and cyber security," *IEEE Access*, vol. 12, pp. 18147-18167, 2024.

[73] V. Dave and A. Sharma, "Operation of differential relay for power transformer using support vector machine," in *Proc. IEEE/PES Transmission and Distribution Conf. and Exposition.* 6 pp., Chicago, IL, USA, 21-24 Apr. 2008.

[74] A. Clark and S. Zonouz, "Cyber-physical resilience: definition and assessment metric," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1671-1684, Mar. 2019.

[75] M. Rajaee and K. Mazlumi, "Multi-agent distributed deep learning algorithm to detect cyber-attacks in distance relays," *IEEE Access*, vol. 11, pp. 10842-10849, 2023.

[76] Z. Pourahmad, R. A. Hooshmand, and M. Ataei. "Optimal placement of PMU and PDC in power systems by considering the vulnerabilities against cyber-attacks," *Electrical Engineering*, vol. 106, no. 1, pp. 93-109, 2024.

[77] Z. Pourahmad and R. A. Hooshmand, "Smart grid protection against cyber-attacks using PMUs and DC system model," in *Proc. 13th Smart Grid Conf.*, 8 pp., Tehran, Iran, 5-6 Dec. 2023.

[78] A. Moradi and S. M. Madani, "Technique for inrush current modelling of power transformers based on core saturation analysis," *IET Generation, Transmission & Distribution*, vol. 12, no. 10, pp. 2317-2324, May 2018.

[79] S. W. Kim, "Detection and mitigation of false data injection in cooperative communications," in *Proc. IEEE 16th Int. Workshop on Signal Processing Advances in Wireless Communications,* pp. 321-325, Stockholm, Sweden, 28 Jun.-1 Jul. 2015.

unconfined cyber-attacks," *IEEE Trans. on Circuits and Systems I: Regular Papers*, vol. 68, no. 2, pp. 776-785, Feb. 2020.
[100] S. Hu, X. Chen, J. Li and X. Xie, "Observer-based resilient controller design for networked stochastic systems under coordinated DoS and FDI attacks," *IEEE Trans. on Control of Network Systems*, vol. 11, no. 2, pp. 890-901, Jun. 2024.
[101] Z. Liu and L. Wang, "A distributionally robust defender-attacker-defender model for resilience enhancement of power systems against malicious cyberattacks," *IEEE Trans. on Power Systems*, vol. 38, no. 6, pp. 4986-4997, Nov. 2022.

زهرا پوراحمد تحصیلات خود را در مقاطع کارشناسی و کارشناسی ارشد مهندسی برق- قدرت به‌ترتیب در سال‌های ۱۳۹۶ و ۱۳۹۸ در دانشگاه اصفهان به پایان رسانده است. نام‌برده در حال حاضر در مقطع دکتری مهندسی برق-قدرت در دانشکده فنی و مهندسی دانشگاه اصفهان مشغول به تحصیل بوده و زمینه‌های تحقیقاتی مورد علاقه ایشان عبارتند از: شبکه‌های هوشمند، حملات سایبری در سیستم قدرت و قابلیت اطمینان در سیستم قدرت.

رحمت‌الله هوشمند تحصیلات خود را در مقاطع کارشناسی و کارشناسی ارشد مهندسی برق- قدرت به‌ترتیب در سال‌های ۱۳۶۸ و ۱۳۷۰ از دانشگاه فردوسی مشهد و دانشگاه تهران و در مقطع دکتری مهندسی برق- قدرت در سال ۱۳۷۴ از دانشگاه تربیت مدرس تهران به پایان رسانده است و هم‌اکنون استاد گروه مهندسی برق دانشکده فنی مهندسی دانشگاه اصفهان می‌باشد. زمینه‌های تحقیقاتی مورد علاقه ایشان عبارتند از: شبکه‌های هوشمند، منابع انرژی تجدیدپذیر و سیستم‌های قدرت تجدید ساختاریافته.

سید محمد مدنی تحصیلات خود را در مقاطع کارشناسی و کارشناسی ارشد مهندسی برق- قدرت به‌ترتیب در سال‌های ۱۳۶۸ و ۱۳۷۰ از دانشگاه صنعتی شریف و دانشگاه تهران و در مقطع دکتری مهندسی برق- قدرت در سال ۱۳۷۸ از دانشگاه صنعتی آیندهون هلند به پایان رسانده است و هم اکنون استاد گروه مهندسی برق دانشکده فنی مهندسی دانشگاه اصفهان می‌باشد. زمینه‌های تحقیقاتی مورد علاقه ایشان عبارتند از: حفاظت سیستم‌های قدرت، میکروگرید، کنترل منابع تجدیدپذیر و درایوهای الکتریکی.