Journal of Modeling in Engineering

Journal homepage: https://modelling.semnan.ac.ir/

ISSN: 2783-2538

Semnan University

Research Article

Cyber-Attacks Modelling and Detection in a Novel Overcurrent Protection Relays Based on logical Analysis of Grid Signal

M. Yousefi Kia [a], M. Saniei [a *], Gh. Seifossadat [a], A. Saffarian [a]

[a] *Department of Electrical Engineering, Faculty of Engineering, Shahid Chamran University of Ahvaz, Ahvaz, Iran.*

PAPER INFO

Paper history:

Received:
Revised:
Accepted:

Keywords:

Cyber attack;

Modelling;

overcurrent relay;

grid signals;

logical analysis;

ABSTRACT

Cyber attacks on protective relays lead to power grid outages. Any manipulation of the output and input signals of the relays and their settings is considered a cyber attack. So far, there has been various research on the detection of cyber attacks, but the access of a comprehensive method that uses signals in the network to detect and classify attacks with the least amount of computing time is an essential requirement of the power grid. In this article, a novel model of overcurrent relays based on two parameters, pick-up current and monitoring current, is proposed, and then three types of common attacks include Denial of service, injecting false data in measurement values, changing the setting values of the relay is implemented in the Matlab/Simulink software on a nine-bus and three machines IEEE standard network. The results show that the proposed detection method based on logical relationships between pick-up current, monitoring current, positive and negative sequence of voltage and current and the command sent from the relay to the circuit breakers provides an acceptable performance with high accuracy and without false trigger by detection time of 17 ms in simulation. This method is superior to other detection techniques because it does not depend on the operating point, relay protection scheme and type of cyber attack. The proposed logic could discriminate between symmetric and asymmetric faults and single and multiple cyber attacks. To achieve this goal, it only needs more signals from different buses and relays.

DOI: https://doi.org/

*** Corresponding author.**
E-mail address: m.saniei@scu.ac.ir

How to cite this article:

مقاله پژوهشی

مدل‌سازی و شناسایی حملات سایبری در رله حفاظت اضافه جریان بر اساس تحلیل منطقی سیگنال های شبکه

محمد یوسفی کیا[1]، محسن صنیعی[2*] ، سید قدرت اله سیف السادات [3] و علیرضا صفاریان[4]

اطلاعات مقاله

دریافت مقاله:
بازنگری مقاله:
پذیرش مقاله:

واژگان کلیدی:
حمله سایبری،
مدل سازی،
رله اضافه جریان،
سیگنال های شبکه،
تحلیل منطقی،

چکیده

حملات سایبری به رله های حفاظتی سبب خاموشی شبکه قدرت می شوند. هر گونه دستکاری در سیگنال های خروجی و ورودی رله ها و تنظیمات آنها حمله سایبری محسوب می شود. معرفی روش جامعی که با استفاده از سیگنال های موجود در شبکه و در کمترین زمان محاسباتی تشخیص و کلاسه بندی حملات را انجام دهد یک نیاز ضروری شبکه قدرت می باشد. در این مقاله ابتدا مدل جدیدی از رله های اضافه جریان مبتنی بر دو پارامتر جریان پیک آپ و جریان پایش پیشنهاد می شود و سپس حملاتی شامل توقف سرویس دهی، تزریق داده نادرست در مقادیر اندازه گیری ، تغییر مقادیر تنظیمی رله در محیط نرم افزار Matlab/Simulink بر روی شبکه نه باس و سه ماشین استاندارد IEEE پیاده سازی می شود. نتایج نشان می دهد که مدل پیشنهادی تشخیص مبتنی بر ایجاد روابط منطقی بین جریان پیک آپ، جریان پایش، توالی مثبت و منفی ولتاژ و جریان و فرمان ارسالی از رله به کلید ها عملکرد قابل قبولی با دقت بالا و بدون تشخیص کاذب و زمان تشخیص ۱۷ میلی ثانیه در شبیه سازی ارائه می دهد. این روش نسبت به سایر تکنیک های تشخیص برتری دارد زیرا به نقطه عملیاتی، طرح حفاظت رله و نوع حمله سایبری وابسته نیست. منطق پیشنهادی قابلیت تمایز انواع خطاهای متقارن، غیر متقارن و حملات سایبری تکی و چند گانه را دارد و برای رسیدن به این هدف صرفا نیاز به تعداد بیشتری سیگنال از باس های مختلف و رله ها دارد.

DOI: https://doi.org/

۱- مقدمه[1]

در سال‌های اخیر با گسترش شبکه‌های برق، اپراتور مستقل سیستم برای حفظ پایداری و قابلیت اطمینان سیستم در هر سه سطح تولید، انتقال و توزیع با چالش‌های بیشتری مواجه است. در عین حال توسعه و نفوذ سیستم های مخابراتی باعث بهبود عملکرد پایش شرایط در زمینه حفاظت و کنترل سیستم شده و در این راستا تجهیزات جدیدی مانند واحد اندازه گیری فازور و

* پست الکترونیک نویسنده مسئول: m.saniei@scu.ac.ir
۱. دانشجوی دکتری، دانشکده مهندسی ، دانشگاه شهید چمران اهواز
۲. دانشیار، دانشکده مهندسی ، دانشگاه شهید چمران اهواز
۳. استاد، دانشکده مهندسی ، دانشگاه شهید چمران اهواز
٤. دانشیار، دانشکده مهندسی ، دانشگاه شهید چمران اهواز
استناد به این مقاله: نحوه استناد فارسی در اینجا درج گردد.

متمرکز کننده داده های فازوری به شبکه اضافه شده اند [۱]. عملکرد صحیح سیستم های سایبری در شبکه های فیزیکی سایبری ضامن کارایی شبکه برق می باشد. با نگاهی به تاریخچه خاموشی ها در شبکه برق می توان دریافت که بیشتر این خاموشی ها به دلیل اختلال در شرایط عادی سیستم بوده و یکی از مهمترین نقاط ضعف و آسیب پذیر آن وقوع حملات سایبری است [۲]. بنابراین موضوع امنیت سایبری یکی از مهم ترین چالش های پیش روی شبکه های قدرت است و عدم توجه به این موضوع می تواند موجب خسارات اقتصادی، آسیب به تجهیزات و در نهایت خاموشی های گسترده و متوالی در سراسر شبکه برق شود [۳]. هدف اصلی حملات سایبری شامل دو بخش فیزیکی از قبیل تجهیزات الکترونیکی هوشمند و بخش سایبری شامل لایه‌های مخابراتی، محاسباتی و نرم‌افزاری است [۴].

به طور کلی، حملات سایبری رویدادهای مخربی هستند که باعث عملکرد نامناسب رابط ماشین و انسان(HMI[2]) ، سیستم های کنترل، خاموشی ماشین ها، ریزش بار و خرابی متوالی سیستم می شود [۵]. امروزه اجزای اساسی شبکه های برق از طریق کانال های مخابراتی به هم متصل می شوند[۶]. چالش های مختلف مربوط به امنیت سایبری شبکه های توزیع برق از جمله پیچیدگی و توسعه آنها در آینده، الزامات مخابراتی، تهدیدات و نقاط آسیب پذیر سیستم های ارتباطی ، عوامل تاخیر، پروتکل ها و برندهای ناهمگن، دستگاه های قدیمی، ارتباط امن دو طرفه و حریم خصوصی کاربر در مرجع [۷] بیان شده است.

در این مقاله ابتدا مدل جدیدی از مشخصه عملکرد رله اضافه جریان پیشنهاد می شود و سپس سه مدل حمله سایبری شامل تزریق داده های اندازه گیری نادرست به صورت حمله تکرار[۳] و تغییر مقادیر تنظیمی آستانه رله[۴] به صورت FDI[۵] و توقف سرویس دهی (DoS[6]) بر روی سیستم قدرت بر اساس مفهوم آنها در نرم افزار Matlab/Simulink مدلسازی شدند. با شروع حملات و دسترسی به مقادیر اندازه‌گیری سیستم، سیگنال‌های توالی مثبت و منفی جریان و ولتاژ در باس های مرتبط در سیستم قدرت و همچنین وضعیت فرمان های ارسالی به بریکرها نمونه برداری می‌شوند و در نهایت یک الگوریتم منطقی تشخیص و حفاظت مقاوم در برابر تهدیدات فیزیکی- سایبری برای شناسایی حملات سایبری پیشنهاد شده است.

۲- مفهوم امنیت سایبری در سیستم قدرت

به طور کلی برای دستیابی به یک سیستم قدرت غیرقابل نفوذ، لازم است سه گانه امنیت CIA (محرمانگی، یکپارچگی و در دسترس بودن) برآورده شود.

محرمانه بودن ویژگی است که در آن اطلاعات در اختیار افراد، نهادها یا فرآیندهای غیرمجاز قرار نمی گیرد یا افشا نمی شود [۸]. یکپارچگی ویژگی حفظ و اطمینان از صحت و کامل بودن داده ها در طول فرآیند یا محافظت از اطلاعات در برابر تغییر توسط اشخاص غیرمجاز است [۹] و از سوی دیگر در دسترس بودن ویژگی است برای اطمینان از اینکه اشخاص یا نهادهای مجاز می توانند در صورت نیاز به اطلاعات یا دستگاه ها دسترسی داشته باشند [۱۰].

اگر هر یک از این پارامترهای امنیتی برآورده نشود، سیستم در معرض تهدید یا حمله قرار می گیرد. این مقاله به بررسی برخی نکات اساسی مرتبط با تهدیدات امنیتی در رله حفاظتی دیجیتال اضافه جریان می پردازد. رایج‌ترین مدل‌های حمله در پژوهش های پیشین مرتبط با رله های حفاظتی شامل تزریق داده‌های نادرست ، توقف سرویس دهی، تغییر مقادیر تنظیمی آستانه، حمله مرد میانی[۷] و دستگاه های بدون مجوز[۸] است. در حمله مرد میانی مهاجم با دسترسی به کانال های ارتباطی و تغییر دستگاه های اندازه گیری، دو پارامتر محرمانگی و یکپارچگی را هدف قرار می دهد . جزئیات پیاده سازی و اثرات حمله مرد میانی به پیام های عمومی رویدادهای شی گرا (GOOSE) در پروتکل ارتباطی IEC 61850 روی رله های حفاظتی نصب شده در پست ها در [۱۱] ارائه شده است.

در حمله دستگاه بدون مجوز، نفوذگر با دسترسی فیزیکی به تجهیزاتی مانند واحد اندازه گیری فازور (PMU) و

[2] Human Machine Interface
[3] Replay Attack
[4] Altered Set point
[5] False Data Injection
[6] Denial of Service
[7] Man in the middle
[8] Rouge device

جایگزینی آن ، حمله را برنامه ریزی می کند و از این طریق با ارسال سیگنال ها و دستورات نادرست بر عملکرد سیستم تأثیر می گذارد[۱۲].

هدف اصلی حملات توقف سرویس دهی، اختلال در ویژگی دسترسی است که مهاجم با تاخیر یا مسدود کردن لینک های ارتباطی و ارسال حجم زیادی از داده ها با هدف ایجاد ترافیک، آن را آغاز می کند [۱۳]. احتمال وقوع حملات DoS در لایه‌های ارتباطی مختلف سیستم‌های قدرت، به صورت پارازیت در کانال برای لایه فیزیکی یا اثر تأخیر یا عدم ارسال پیام و همچنین تغییر پارامترهای آدرس MAC از طریق جعل داده ها وجود دارد [۱۴]. یک روش تشخیص تهدید در پستی با سیستم اتوماسیون مبتنی بر IEC61850 در [۱۵] پیشنهاد شده است. بررسی نقاط ضعف و آسیب پذیری بخش های مختلف سخت افزاری و نرم افزاری در برابر حملات DoS و اثرات آن بر سایر لایه ها از جمله انتقال و شبکه در [۱۶] بیان شده است. نمونه های ذکر شده از حملات DoS شامل جعل[۹]، گسیل[۱۰] و پارازیت[۱۱] است که نتیجه نهایی آن تاخیر یا عدم ارسال پیام های وابسته به زمان است و باعث اختلال در عملکرد سیستم و تجهیزات و عدم امکان برقراری ارتباط با تجهیزات می شود. بررسی شدت اثرات کلیدزنی مخرب و حملات DoS در رله‌های حفاظتی دیجیتال شبکه برق اوکراین با شبیه‌سازی حملات سایبری در [۱۷] انجام شده است.

در حملات با تزریق داده های نادرست هدف ایجاد تغییر در بردار دادهای ذخیره شده می باشد که در رایج ترین موارد با هدف حمله به بردار تخمین حالت و از مدار خارج کردن روش های تشخیص داده های بد[۱۲] انجام می شود [۱۸]. در سال‌های اخیر، مطالعات زیادی بر روی دامنه این حملات متمرکز شده‌اند که تزریق اطلاعات ناقص به سیستم کنترل تولید خودکار[۱۳] و پارامترهای بازار برق از بارزترین آن‌ها هستند [۱۹]. چندین تکنیک برای شناسایی و کاهش اثر چنین حملاتی در [۲۰] توسعه یافته است.

تأثیر حملات سایبری بر شبکه قدرت از نظر شدت آسیب بسیار متنوع است و از موارد کوچک سرقت انرژی تا خاموشی های گسترده و تخریب تجهیزات موتوری و ژنراتورها را شامل می شود. چند نمونه از حملات سایبری با تأثیر زیاد بر سیستم قدرت در [۲۱] بیان شده است.

رله‌های حفاظتی علاوه بر عملکرد در شرایط خطا، امکان باز و بسته شدن از راه دور توسط اپراتور سیستم را با کمک کانال‌های ارتباطی دارند، بنابراین در صورت ناامن بودن این شبکه بی‌سیم، امکان تهاجم تسهیل می شود[۲۲]. در سال‌های اخیر مطالعات زیادی در زمینه افزایش امنیت سایبری در شبکه‌های قدرت و مقابله با تهدیدات سایبری انجام شده است که عمدتاً مبتنی بر تحلیل حالت پایدار است. حمله تزریق داده های نادرست می تواند با داشتن اطلاعات توپولوژی یک سیستم قبل از حمله منجر به اعوجاج الگوریتم تخمین حالت شود [۲۳].

مروری بر انواع حملات FDI و روش های تشخیص آنها بر اساس اطلاعات افشا شده توپولوژی سیستم در [۲۴] شرح داده شده است. یک روش ابتکاری با استفاده از اطلاعات محلی برای جلوگیری از حملات غیرقابل تشخیص توسط نفوذگر مبتدی در [۲۵] ارائه شده است. یک مبنای ریاضی برای تعیین کمی اثرات اقتصادی وقوع حملات داده های توپولوژیکی در بازار برق زمانی که مهاجم از استراتژی پیشنهاد مجازی استفاده می کند، در [۲۶] فرموله شده است. پس از آن، با تجزیه و تحلیل پایداری در خط انتقال، توانایی مهاجمان برای نفوذ به فرآیند مناقصه مجازی برای باس های خاص محاسبه می شود. در [۲۷] یک روش تاب آور برای شناسایی حمله FDI در رله های دیفرانسیل جریان خط توضیح داده شده که از دو ماژول محاسباتی، توالی مثبت (PS) و توالی منفی (NS) برای محاسبه ولتاژ در ترمینال و مقایسه با ولتاژ اندازه گیری شده و اعتبار سنجی جریان های اندازه گیری شده استفاده کرده است. طولانی بودن مراحل محاسباتی و امکان نقض محدودیت های زمانی مجاز برای کارکرد تجهیزات حفاظتی به عنوان عیب آن ذکر شده است. یک الگوریتم بهینه سازی فرا ابتکاری در حالت ثابت برای مقابله با سه نوع حمله سایبری استفاده می شود [۲۸].

در [۲۹]، FDI در سیستم اتوماسیون پست شامل رله های دیستانس و کلیدهای قدرت انجام شده است. یک

[9] Spoofing
[10] flooding
[11] Jamming
[12] Bad Data Detector
[13] Automatic Generator Controller

طرح حفاظتی تاب آور در برابر حملات سایبری با استفاده از اصول هماهنگی حفاظتی برای بررسی تغییرات تنظیمات حفاظتی و با استفاده از الگوریتم ضریب همبستگی بر اساس آنالیز اثر خطای گذرا (TFS) پیشنهاد شده است که در آن نقاط ضعف رله‌های اضافه جریان و جهتی حذف می‌شوند. این مرجع بدون توجه به مسائل کاربردی مربوط به پست ها، اقدام به پیاده سازی کرده است. در [۳۰]، اثرات حملات فیزیکی- سایبری در حوزه برق در حین دستکاری خرابکارانه مسیرهای ارتباطی و عملکرد منابع تولید پراکنده ارائه شده است. در مرجع [۳۱]، اثرات دینامیکی حملات سایبری به پست ها بررسی شده و مطالعات دینامیکی به عنوان راه حلی موثر برای شناسایی حملات سایبری بیان شده است. این مطالعه صرفا اثرات پویای حملات کلیدزنی را بررسی نموده و الگوریتمی برای مقابله با سایر حملات ارائه نکرده است.

در [۳۲] با تجزیه و تحلیل رابطه بین تنظیمات رله و منطق قطع کلیدها در هنگام حمله، روش جدیدی برای ارزیابی ریسک معرفی شده است. این روش ارزیابی تنها زمانی استفاده می شود که حملات رخ می دهند و در هنگام خطاهای فیزیکی معمولی موثر نیست. قابل توجه است که رفتار شبکه های قدرت در دو مورد حمله سایبری و خطای اتصال کوتاه متفاوت است و نیاز به فرضیات متفاوتی برای ارزیابی ریسک دارد. در این مرجع ارزیابی ریسک سیستم های قدرت در حملات سایبری با در نظر گرفتن نقش سیستم حفاظتی مانند تنظیمات رله و پارامتر ها مورد توجه قرار گرفته است. برای تشخیص از شاخص ELC[14] استفاده می شود اما دلیل انتخاب این شاخص و برتری آن نسبت به سایر روش ها به وضوح ذکر نشده است. در [۳۳]، حملات FDI، کلیدزنی، DoS و حمله تکرار[15] برای سیستم حفاظتی (رله های جریان اضافه)، دستگاه های الکترونیکی هوشمند و کلیدهای قدرت اعمال شده است. روش تشخیص مبتنی بر تجزیه و تحلیل حالت پویا است که در شرایط زمان واقعی پرهزینه است. در [۳۴]، تشخیص حملات سایبری از قبیل حمله مرد میانی، تزریق داده های نادرست، حمله به تنظیمات تپ چنجر ترانسفورماتور و حمله تکرار در رله های حفاظتی خط انتقال بر اساس یادگیری عمیق آموزش یافته توسط نمونه های اندازه گیری جریان و ولتاژ انجام شده است. نیاز به مجموعه داده های آموزشی و فقدان داده های واقعی و مناسب در شرایط حمله مشکل اصلی این روش محسوب می شود.

در [۳۵] رویکرد کنترل چند متغیره در هنگام تزریق داده های نادرست، حمله مرد میانی، حمله تکرار و حمله یکپارچگی برای افزایش امنیت رله های حفاظتی اضافه جریان اعمال می شود. این روش از چندین کنترلر استفاده کرده و توالی وقایع را به همراه ادغام داده های فیزیکی و سایبری دریافتی از سینکروفازورها[16] بررسی می کند. استفاده از تعداد زیاد عملگرهای منطقی در الگوریتم و مسیرهای مخابراتی متعدد، اشکال اصلی روش پیشنهادی است.

در [۳۶]، حمله تزریق داده های نادرست در تنظیمات رله اضافه جریان شناسایی می شود. شبیه سازی مونت کارلو برای آموزش مجموعه داده ها و بارگذاری دستورات شرطی با استفاده از روش طبقه بندی تقریبی انجام می شود. روش پیشنهادی اصول حفاظت تطبیقی را بر اساس تغییر نقاط تنظیم برخط رله ها اجرا نمی کند. علاوه بر این، نفوذ انرژی های تجدیدپذیر در روش پیشنهادی در نظر گرفته نشده است. در [۳۷]، آسیب‌پذیری طرح‌های حفاظتی مبتنی بر سیستم‌های مخابراتی در رله دیستانس خط انتقال در طول حمله توقف سرویس دهی و تزریق داده‌های نادرست بررسی شده است. روش‌های مخابراتی فیزیکی پیشنهاد شده در این مرجع به اندازه کافی برای مقابله با حملات سایبری تزریق داده‌های نادرست مؤثر نیستند. در [۳۸] حملات سایبری توپولوژیکی مستقیم مانند حمله اضافه شدن خط، حمله حذف خط و حمله تغییر خط با هدف ایجاد اختلال در سیستم قدرت معرفی شده است. یک الگوریتم بهینه سازی فرا ابتکاری جدید مانند الگوریتم تجمع طبیعی برای تشخیص استفاده می شود. این پژوهش تاثیر وقوع یک حمله سایبری را بر سیستم قدرت نشان می‌دهد و بهتر است حملات سایبری هماهنگ در چند نقطه اجرا شود.

[14] Expected Load Curtailment
[15] Replay
[16] synchrophasor

این مقاله یک سیستم قدرت استاندارد را در طول انواع متداول حملات سایبری پیاده‌سازی می‌کند تا اثرات دینامیکی القایی روی سیگنال‌های الکتریکی را ارائه کند.

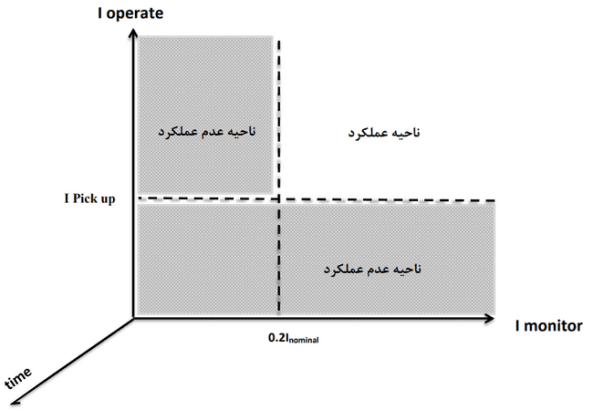
۳-۱- مدل پیشنهادی رله اضافه جریان

اصول عملکرد رله های اضافه جریان متداول به صورت پایش جریان ورودی به رله و عبور آن از یک مقدار آستانه و به عبارتی پیک آپ رله می باشد.

در مدل پیشنهادی علاوه بر جریان عملکرد (I_{op})، پارامتر دیگری تحت عنوان جریان پایش (I_{mon}) به ترتیب ذیل برای رله اضافه جریان بر مبنای اندازه گیری فازوری تعریف می شوند.

$$I_{op}[k]=\left|I_n[k]\right| \qquad (۱)$$

$$I_{mon}[k]=\left|\begin{matrix}\left|I_n[k]-I_n[k-N]\right|-\cdots\\ \left|I_n[k-N]-I_n[k-2N]\right|\end{matrix}\right| \qquad (۲)$$



شکل ۱- مشخصه پیشنهادی رله اضافه جریان

که در آن $\left|I_n[k]\right|$ فازور جریان در خط n ام تحت حفاظت در نمونه ی kام و $I_n[k-N]$ فازور جریان یک سیکل قبل و $I_n[k-2N]$ فازور جریان دو سیکل قبل از نمونه می باشد. بر اساس این مدل رله اضافه جریان هنگامی وارد ناحیه عملکرد می شود که شرایط زیر برقرار باشد:

$$I_{op}[k]\geq I_{Pick-up}\ \&\ I_{mon}[k]\geq 0.2I_{nominal} \qquad (۳)$$

که در آن $I_{Pick-up}$ جریان برداشت رله اضافه جریان و $I_{nominal}$ جریان نامی خط مورد حفاظت در شرایط کارکرد عادی شبکه می باشد. معمولاً انتخاب مقادیر آستانه پیک آپ بر اساس یک اصل مشخص است و مقدار آن عددی است بین حداکثر جریان بار آن فیدر و حداقل جریان خطای اتصال کوتاه سیستم و به صورت رابطه ذیل:

$$I_{load-max}\leq I_{pick-up}\leq I_{fault-min} \qquad (۴)$$

بدیهی است که تنظیمات جریان برای رله های اضافه جریان باید بالاتر از جریان بار فیدر باشد و جریان بار باس ملاک عمل نیست. در واقع، برای انتخاب صحیح تنظیمات جریان پیک آپ، باید حداکثر شرایط بارگذاری ممکن را در نظر گرفت. یک قانون سرانگشتی این است که جریان پیک آپ رله را روی ۱/۲۵ برابر حداکثر جریان بار و یا $\frac{2}{3}$ حداقل جریان خطا تنظیم نمود. انتخاب مقدار آستانه باید حدود عملی تنظیم رله را رعایت کند که معمولاً بین ۵۰ تا ۲۰۰ درصد جریان نامی رله است [۳۵].

برای ایجاد امنیت بیشتر، رله های اضافه جریان را می توان به واحدهای آشکارساز اختلال تجهیز نمود تا قبل از صدور فرمان تریپ توسط رله، وارد عمل شود. این بخش یک آشکارساز اختلال حساس به جریان است که بر عملکرد رله های اضافه جریان نظارت می کند. معمولا انواع تجاری رله های اضافه جریان برای تشخیص اختلالاتی از قبیل تغییرات بار، از دست رفتن تحریک و یا عملیات کلید زنی که منجر به انحراف فرکانس یا نوسانات توان می شوند مجهز می شوند. مطالعات نشان می دهند که انحراف فرکانس ۳ هرتز موجب می شود که حداکثر نامتعادلی خروجی جریان $0.15I_{nominal}$ باشد که در این صورت رله دچار تشخیص نادرست نمی شود. شایان ذکر است در حالت نوسانات توان در صورتی که تفاوت فرکانس دو باس مجاور حداکثر ۱/۸ هرتز باشد عملکرد رله اضافه جریان صحیح خواهد بود. هدف اصلی این بخش در مورد حملات سایبری رله اضافه جریان دیجیتال است. با توجه به مرور مقالات انجام شده اضافه کردن بخشی به مشخصه رله اضافه جریان شامل محاسبه اختلاف جریان ها در نقاط مذکور به عنوان نوآوری مدل پیشنهادی می باشد که

می تواند به طور مستقیم و غیر مستقیم در تشخیص حملات به کار رود.

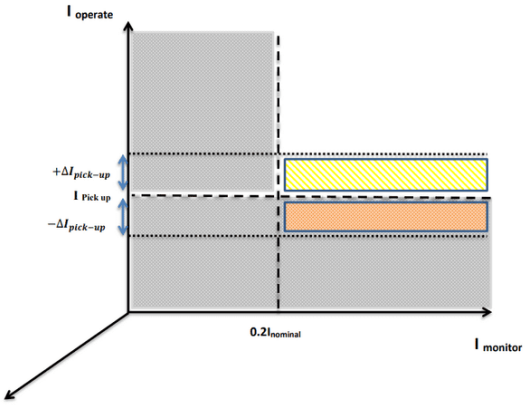
۳-۲- مدل پیشنهادی حملات سایبری

بر اساس گزارش منتشر شده توسط NERC در مورد عملکرد نادرست رله های حفاظتی، بیش از ۲۰ درصد از خطاهای این بخش به دلیل اختلال عملکرد کلیدهای قدرت و رله ها رخ می دهد [۳۹]. حمله سایبری یکی از دلایل احتمالی عملکرد غیرعادی رله ها به دلیل نفوذ هکرها در نقاط آسیب پذیر نرم افزارها و کانال های اطلاعاتی در سیستم قدرت می باشد. در چنین حالتی، بررسی رفتار عملیاتی سیستم قدرت بسیار مهم است. در میان حملات سایبری مختلف، حملات تزریقی که به عنوان حملات تزریق داده های نادرست (FDI) نیز شناخته می شوند، شامل تزریق پاسخ، تزریق اندازه گیری و تزریق فرمان، حملات DoS و حمله تکرار بیشترین امکان را دارند. تزریق‌های فرمان به سه دسته MPCI[17]، MFCI[18] و MSCI[19] گروه‌بندی می‌شوند. این بخش مدل پیشنهادی حملات سایبری از نوع تزریق داده نادرست شامل تغییر مقادیر تنظیمی و تغییر در داده های اندازه گیری جریان ورودی، حملات توقف سرویس دهی و حمله تکرار در رله های اضافه جریان را ارائه می نماید . در اینجا فرض بر این است که رله های اضافه جریان به واحد آشکارساز اختلال مجهز می باشد. بنابراین برای رله دو مقدار آستانه یکی برای عملکرد واحد آشکار ساز اختلال و دیگری به عنوان جریان پیک آپ و صدور سیگنال تریپ از رله به طرف بریکر تنظیم می شود.

- **تغییر مقادیر تنظیمی رله اضافه جریان**

در این نوع حمله مهاجم پارامترهای تنظمی تجهیز را تغییر می دهد و باعث می شود سیستم اقدامات کنترلی نادرستی انجام دهد. تغییر نقاط تنظیم منجر به تغییرات بعدی در رفتار سیستم می شود. این نوع حمله از نوع MPCI است که در آن مقادیر تنظیمی آستانه در رله حفاظتی تغییر می کند. این حملات متعاقباً منجر به خرابی ناگهانی سیستم می شود. یکی از انواع اصلی حملات به ویژگی یکپارچگی داده‌ها حمله نقطه تنظیم تغییر یافته کنترل و تغییر مقادیر از پیش تعریف شده رله اضافه جریان است که باعث اختلال در عملکرد رله‌های حفاظت دیجیتال می‌شود. در این حملات، مهاجم با دسترسی به کانال های ارتباطی، الگوریتم های کنترل و حفاظت، رله های دیجیتال را هک کرده و آن ها را به دلخواه هدایت می کند. اثر نهایی این حملات، عملکرد نادرست کلیدهای مدار، قطع بدون دلیل خطوط انتقال برق بدون بروز نقص فیزیکی و یا متصل نگه داشتن خطوط برق در هنگام اتصال کوتاه است. بنابراین، مدل‌سازی حمله تغییر مقادیر تنظیمی رله اضافه جریان با هدف دستکاری یکپارچگی می‌تواند به صورت دستکاری در مقادیر جریان پیک آپ رله تنظیم شود. در واقع در این حمله در صورت دسترسی به تنظیمات رله و پایگاه داده آن می تواند با کم کردن مقدار تنظیمی جریان و یا زیاد کردن آن رله را دچار اشتباه در تشخیص نماید. به طوری که با کم کردن آن حالات پر باری را مشابه با وقوع خطا دیده و با زیاد کردن آن از تشخیص خطاها جلوگیری نماید.

رابطه (۵) بیان ریاضی حمله مقدار تنظیمی رله اضافه جریان را از دید مهاجم نشان می دهد:



شکل ۲- حمله تغییر مقادیر تنظیمی رله اضافه جریان در مشخصه پیشنهادی

$$I^{m}_{(pick-up)} = | I_{(pick-up)} | \pm | \Delta I_{(pick-up)} | \quad (۵)$$

که در آن $| \Delta I_{(pick-up)} |$ و $I^{m}_{(pick-up)}$ به ترتیب میزان تغییر آستانه پیک آپ رله توسط مهاجم و مقدار نهایی آستانه رله پس از حمله می باشند.

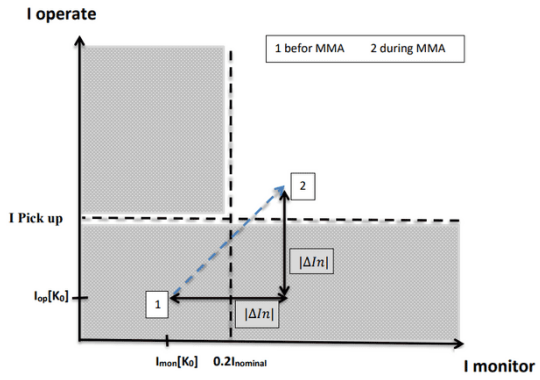
[17] Malicious Parameter Command Injection
[18] Malicious Function Code Injection
[19] Malicious State Command Injection

• تغییر جریان اندازه گیری ورودی به رله اضافه جریان

به منظور هدایت رله اضافه جریان به ناحیه عملکرد و صدور فرمان، مهاجم می تواند دامنه و زاویه فاز را دستکاری نماید. بنابراین در طول حمله تزریق داده غلط اگر جریان اندازه گیری شده از $(|I_n|\angle\theta_n)$ به $(|I_n|+|\Delta I_n|\angle\theta_n+\Delta\theta_n)$ تغییر پیدا کند. در این صورت جریان عملکرد دستکاری شده در طول حمله سایبری مطابق ذیل خواهد بود.

$$I_{op}^{m}[k]=\|In|+|\Delta In|\angle(\theta n+\Delta\theta n)| \quad (۶)$$

در صورتی که در شبکه اتصال کوتاهی مطرح نباشد و صرفا یک حمله سایبری به اندازه و زاویه جریان اندازه گیری شده صورت گرفته باشد با فرض اینکه جریان پایش قبل از شروع حمله $I_{mon}[k_0]$ باشد در این صورت در زمان شروع حمله $I_{mon}[k_0]+|\Delta I_n|$ خواهد بود. بنابراین برای اینکه مهاجم بتواند تریپ خط را صادر کند باید دامنه و زاویه جریان دستکاری شده به گونه ای انتخاب شده باشد که جریان حاصله وارد ناحیه عملکرد رله شود و شرط عبور از مقدار پیک آپ رله و بزرگتر بودن از ۰/۲ جریان نامی را داشته باشد. پس زمانی که رله های اضافه جریان مقادیر اندازه گیری شده خود را دریافت می کند می بایست مقدار $I_{mon}[k_0]$ برای تمام لحظات برای مهاجم قابل مشاهده باشد تا بتواند با تزریق در دامنه و فاز جریان اقدام به حمله نماید. حمله Magnitude Modification Attack به مفهوم تغییر در دامنه جریان اندازه گیری شده و ارسالی به رله می باشد.



شکل ۳- حمله تغییر دامنه جریان اندازه گیری شده ورودی به رله اضافه جریان در مشخصه پیشنهادی

هنگامی که مهاجم جریان |ΔIn| را به کمیت جریان اندازه گیری شده و ارسالی به رله اضافه می کند نقطه عملکرد رله از حالت ۱ روی نمودار به حالت ۲ تغییر وضعیت می دهد.

این قبیل دستکاری از طریق مسیرهای مخابراتی منتهی به رله های اضافه جریان قابل دسترس مهاجمین می باشد.

• توقف سرویس دهی در رله اضافه جریان

حمله DoS توسط هکرها برای جلوگیری از عملکرد رله ها در زمان مقتضی و برنامه ریزی شده می باشد. این نوع حمله مسیرهای ارتباطی یک سیستم را دستخوش تغییر قرار می دهد به طوری که به دیگر درخواست ها پاسخ نمی دهد در چنین شرایطی است که مهاجم با اشغال بیش از حد ظرفیت کانال های ارتباطی و ارسال ترافیک بیش از حد بر ویژگی در دسترس بودن اطلاعات به دست آمده تأثیر می گذارد. حمله DoS را می‌توان به دو شکل مدل‌سازی کرد. در مورد اول، حمله DoS به طور مداوم عملکرد رله‌ها را در هنگام خطا و موقعیت‌های اضطراری با انتقال اطلاعات مخرب به IED مورد نظر مسدود می‌کند. بنابراین رله ها ماموریت اصلی خود یعنی ارسال فرمان به موقع به کلیدهای مدار را انجام نمی دهند. در این حالت منطق عملکردی از پیش تعریف شده در رله است در صورت بروز هر گونه خطا به کلیدهای مدار ارسال نمی

شود. در مورد دوم حمله DoS، مهاجم از عملکرد رله ها و ارسال دستورات مناسب در صورت بروز خطا برای مدت زمان محدودی جلوگیری می کند. به عبارت دیگر، این نوع حمله با ایجاد تاخیر (عدم ارسال فرمان فوری) در سیگنال تریپ به کلید قدرت در هنگام بروز خطا اجرا می شود. سیگنال تزریق شده چنین حمله ای به صورت زیر بیان می شود:

$$S = e^{-T_0 t} \times trip\,signal \qquad (۷)$$

که در آن T_0 یک کمیت عددی مثبت است که توسط مهاجم مشخص می شود به نحوی که خروجی رله حفاظتی با تاخیر به کلید قدرت ارسال شود. این مقاله به بررسی اثر حمله DoS از نوع دوم توضیح داده شده در بالا می‌پردازد.

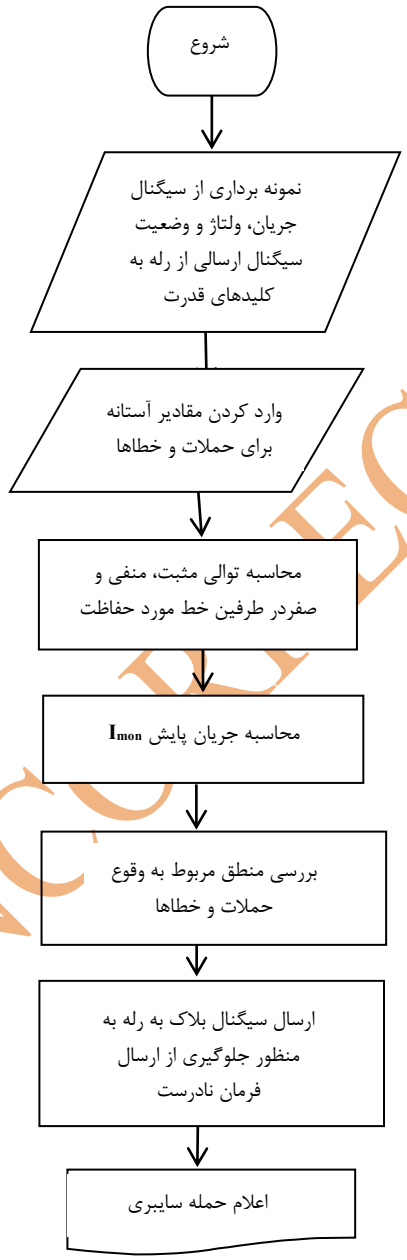
• حمله تکرار در رله اضافه جریان

حمله تکرار یک استراتژی جعل داده است که در آن یک داده معتبر تکرار شده است. هنگام وقوع این گونه حملات، مهاجمان می توانند داده های ثبت شده از یک پایگاه داده در معرض خطر یا ضبط کننده داده در مدت زمان معین را تکرار کنند. بنابراین مهاجمان می توانند برای نفوذ به شبکه از راه دور به اطلاعات دسترسی پیدا کنند و ممکن است به سادگی ترافیک شبکه را شنود کند. آنها می توانند مجموعه ای از داده های اختلالات رخ داده قبلی را با استفاده از یک ضبط کننده خطای دیجیتال (DFR) یا بر اساس گزارش وضعیت کلیدهای قدرت در یک بازه زمانی معین ثبت کنند. در این حالت مهاجم اطلاعات ثبت شده رویداد قبلی را در المان مورد نظر شبکه هدف (جریان ورودی به رله) برای شبیه سازی مجدد آن رویداد ارسال نموده، که ممکن است با ارسال فرمان تریپ نادرست برای کلیدهای قدرت منجر به خاموشی شبکه می شود. تشخیص چنین حمله ای بدون بررسی بیشتر اطلاعات واقعی دشوار است و چنین حملاتی معمولا محدودیت زمانی عملیاتی کلیدهای قدرت را نقض می کند. تمام حملات سایبری ذکر شده با در نظرگرفتن کانال های مخابراتی و با استفاده از نرم افزار MATLAB/Simulink مدل سازی شده اند.

بنابراین در این بخش مدل پیشنهادی رله اضافه جریان در حملات سایبری مختلف مورد بررسی قرار گرفت و بستر جدیدی برای شبیه سازی حملات تحمیلی توسط مهاجم در این نوع رله ارائه گردید.

۳-۳- الگوریتم پیشنهادی تشخیص حملات سایبری

الگوریتم کلی تشخیص در شکل زیر نشان داده شده است:



شکل ۴- فلوچارت پیشنهادی برای تشخیص حمله سایبری

در این بخش یک روش تشخیص جدید برای حملات سایبری در رله های اضافه جریان معرفی می شود. این روش از ترکیب فازور تمام سیکل مقادیر اندازه گیری شده جریان و ولتاژ و محاسبه توالی مثبت و منفی آنها در باس های سیستم و مقایسه آنها با مقادیر آستانه از پیش تعیین شده، وضعیت فرمان های ارسالی از رله ها به کلیدهای قدرت، وقوع pick-up رله اضافه جریان و بررسی جریان پایش I_{mon} و عبور مقدار آن از ۰/۲ جریان نامی خط مورد حفاظت استفاده می نماید. سپس در بازه زمانی مجاز عملکرد رله و پیش از ارسال فرمان تریپ برای خط انتقال، واحد تشخیص حمله سایبری شروع به محاسبات نموده و در صورت تشخیص حمله، به صورت مقتضی فرمان تریپ در رله بلاک و یا به آن ارسال می گردد. در ادامه به بررسی منطق و شبه کد مربوط به تشخیص حملات سایبری به تفکیک می پردازیم.

الگوریتم ۱: تشخیص حمله سایبری تغییر مقدار تنظیمی رله

1: **Input**: I , V, *Command Signal*
2: **Initialize**: $\delta_i, i \in \{1,.....,12\}, I_{pick-up_j}$
3: **for** $j = 1,2$ **do**
4: **Calculate**: I_{PS_j}, I_{NS_j}, V_{PS_j}, V_{NS_j}, I_{mon_j}
5: **if** $I_{PS_j} \le \delta_i \,\&\, V_{PS_j} \le \delta_i \,\&\, V_{NS_j} = I_{NS_j} = 0 \cdots$
$I_{op_j} \le I_{pick-up_j} \,\&\, I_{mon_j} \ge 0.2 I_{nominal_j}$, **then**
6: *send* $\rightarrow$ *Command Signal*
7: **else if** $I_{PS_j} \le \delta_i \,\&\, V_{PS_j} \ge \delta_i \,\&\, V_{NS_j} = I_{NS_j} = 0 \cdots$
$I_{op_j} \ge I_{pick-up_j} \,\&\, I_{mon_j} \le 0.2 I_{nominal_j}$, **then**
8: *block* $\rightarrow$ *Command Signal*
9: **else**
10: **break**
11: **end if**
12: **end for**
13: **return**

الگوریتم شماره ۱ با داشتن مقادیر آستانه δ_i برای ولتاژ و جریان توالی مثبت و منفی در انواع خطاهای متقارن ،غیر متقارن و در حالت حمله تغییر مقدار تنظیمی رله (افزایش یا کاهش) برای تشخیص استفاده می شود.

الگوریتم شماره ۲ برای دو حمله تزریق نادرست جریان و حمله تکرار کاربرد دارد. در تمام الگوریتم های بالا در صورتی که حمله همزمان به رله های دو طرف خط صورت گیرد، شرایط در پشت باس مورد بررسی قرار می گیرد.

الگوریتم ۲: تشخیص حمله سایبری تزریق جریان نادرست

1: **Input**: I , V, *Command Signal*
2: **Initialize**: $\delta_i, i \in \{1,.....,12\}, I_{pick-up_j}$
3: **for** $j = 1,2$ **do**
4: **Calculate**: I_{PS_j}, I_{NS_j}, V_{PS_j}, V_{NS_j}, I_{mon_j}
5: **if** $I_{PS_j} \ge \delta_i \,\&\, V_{PS_j} \ge \delta_i \,\&\, V_{NS_j} = I_{NS_j} = 0 \cdots$
$I_{op_j} \ge I_{pick-up_j} \,\&\, I_{mon_j} \ge 0.2 I_{nominal_j}$, **then**
6: *block* $\rightarrow$ *Command Signal*
7: **else**
8: **break**
9: **end if**
10: **end for**
11: **return**

الگوریتم ۳: تشخیص حمله سایبری توقف سرویس دهی

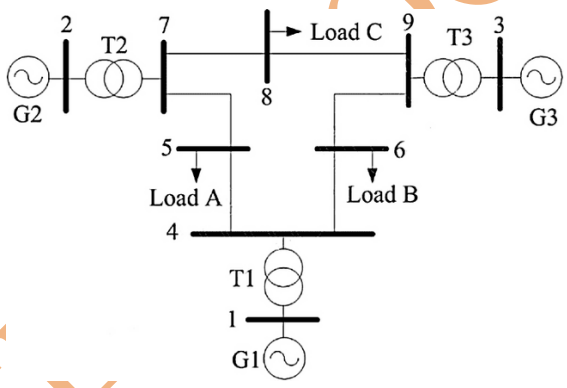
1: **Input**: I , V, *Command Signal*
2: **Initialize**: $\delta_i, i \in \{1,.....,12\}, I_{pick-up_j}, \beta$
3: **for** $j = 1,2$ **do**
4: **Calculate**: I_{PS_j}, I_{NS_j}, V_{PS_j}, V_{NS_j}, I_{mon_j}
5: **if** $I_{PS_j} \ge \delta_i \,\&\, V_{PS_j} \le \delta_i \,\&\, V_{NS_j} = I_{NS_j} = 0 \cdots$
$I_{op_j} \ge I_{pick-up_j} \,\&\, I_{mon_j} \ge 0.2 I_{nominal_j} \cdots$
$\&\, diff(Command\ Signal) \ge 0$ **then**
6: *send* $\rightarrow$ *Command Signal* *with* *delay*
7: **else**
8: **break**
9: **end if**
10: **end for**
11: **return**

در الگوریتم شماره ۳ تشخیص بر اساس تفاوت فرمان ارسالی قطع رله ها به سمت کلید مربوطه و پایدار ماندن آن از یک مقدار زمان تاخیر معین β بر اساس تنظیمات قبلی منطق (با حداقل زمان یک سیکل کامل معادل ۱۷ میلی ثانیه و انجام محاسبات توالی) و پیش از زمان باز شدن کلید توسط حمله می باشد.

در روش پیشنهاد شده مشکل اصلی روش‌های پیشین مقالات یعنی وابستگی طرح تشخیص به داده های از پیش آموزش داده شده، توپولوژی و طرح حفاظتی شبکه مرتفع شده و صرفا بر اساس شرایط واقعی شبکه می توان به تشخیص و مقابله با حملات پرداخت.

۴- سیستم قدرت مورد مطالعه

مدل استاندارد IEEE شامل سه ماشین و نه باس برای شبیه سازی حملات سایبری در نظر گرفته شده است (شکل ۵).



شکل ۵- سیستم استاندارد سه ماشین و نه باسWSCC

مجموع ۳۱۵ مگاوات بار در شبکه وجود دارد و سه ژنراتور یک، دو و سه با ظرفیت های ۲۴۷/۵، ۱۹۲ و ۱۲۸ مگا ولت آمپر و سطوح ولتاژ ۱۶/۵، ۱۸، و ۱۳/۸ کیلو ولت وظیفه تامین بارهای موجود را بر عهده دارند. ژنراتور اول به عنوان یک باس بی نهایت به باس شماره یک و ژنراتورهای ۲ و ۳ به ترتیب به باس دوم و سوم متصل می شوند. سه ترانسفورماتور افزاینده ۱۰۰ مگاولت آمپر با ضریب تبدیل ۱۸ /۲۳۰ کیلوولت، ۱۳/۸ /۲۳۰ کیلوولت و ۲۳۰/۱۶/۵ کیلوولت وظیفه تطبیق ولتاژ خروجی ژنراتورها با ولتاژ سطح انتقال را بر عهده دارند.

ولتاژ مبنای شبکه ۲۳۰ کیلو ولت است. سطح ولتاژ پایه برای ژنراتورها با سمت فشار ضعیف ترانسفورماتور یکسان در نظر گرفته می شود و بنابراین برای ترانسفورماتور واقع بین دو شین شماره ۲ و ۷ این مقدار برابر ۱۸ کیلو ولت، ترانسفورماتور بین دو شین شماره ۳ و ۹ برابر ۱۳.۸ کیلو ولت و برای ترانسفورماتور واقع بین شین ۱ و ۴ برابر ۱۶/۵ کیلو ولت است.

رله های اضافه جریان با دریافت مقادیر جریان ثبت شده توسط زیرساخت های اندازه گیری پیشرفته در سراسر شبکه و پست ها، فرمان مناسب را به کلیدهای مدار ارسال می کنند. در این مقاله هکر رله دیجیتال بین شین های ۷ و ۵ را هدف قرار داده و انواع حملات سایبری را به سیستم تحمیل می کند و از این طریق فرمان خروجی رله اضافه جریان به سمت کلید های قدرت را دچار اختلال می کند. فرکانس سیستم مورد مطالعه ۶۰ هرتز بوده و در مجموع سه بار با توان های ۱۰۰، ۱۲۵ و ۹۰ مگاوات به ترتیب به باس های شماره ۸، ۵ و ۶ متصل می شود. شش خط انتقال، باس های این شبکه را به هم متصل می کند. خلاصه ای از اطلاعات شامل داده های بار و داده های خط انتقال به ترتیب در جدول ۲ و جدول ۳ در پیوست [۴۰] موجود است.

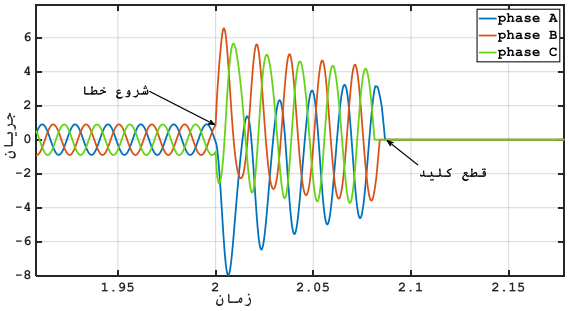
۵- نتایج شبیه سازی

مدل استاندارد IEEE سه ماشین و نه باس برای شبیه سازی در محیط MATLAB/Simulink در نظر گرفته شده است. زمان نمونه برداری و نرخ نمونه برداری این شبیه سازی به ترتیب ۵۰ میکروثانیه و ۲۰ کیلوهرتز است. یک خطای ۳ فاز به زمین و چند نمونه حمله سایبری متداول برای شبکه مفروض پیاده سازی شده و اثرات دینامیکی خطاها و حملات به طور جداگانه تجزیه و تحلیل می شوند. در این مقاله، فرض بر این است که هکر عملکرد یک ایستگاه فرعی را کنترل می کند، که تا حدودی با واقعیتی که مهاجم اطلاعات محدودی در مورد سیستم دارد، مطابقت دارد. حملات سایبری رله‌های آسیب‌پذیر را دستکاری می‌کنند. به دلیل ایجاد اختلال در عملکرد رله، سیستم قدرت رفتار دینامیکی غیر منتظره ای را تجربه می کند که ممکن است منجر به خاموشی شود. سناریوهای مختلف به همراه اثرات دینامیکی آنها بر روی سیستم قدرت در زیر بررسی شده است.

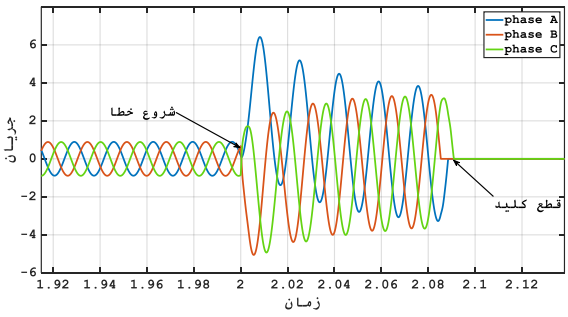
۵-۱- اثر خطای متقارن سه فاز

ابتدا، اثر خطای اتصال کوتاه سه فاز به زمین تحلیل می‌شود. همانطور که مشخص است رله های اضافه جریان با دریافت مداوم تغییرات جریان از طریق CT ها و انجام محاسبات داخلی افزایش جریان بیش از حد معمول را

تشخیص می دهند و با ارسال فرمان تریپ به کلید قدرت خطا را برطرف می کنند. عموماً در شرایط خطای جریان گذرا و در صورت عدم وجود ریکلوزر ، اپراتور باید در محل تابلو حضور پیدا کند و رله لاک اوت را ریست کند تا امکان اتصال مجدد کلید قدرت فراهم شود. با این حال، چنین الزامی برای خطاهای ولتاژی وجود ندارد و به محض رفع عیب، سیستم آماده اتصال مجدد است. در خطاهای جریان دائمی، امکان وصل مجدد کلید پس از رفع منشا خطا وجود دارد. این بخش یک خطای جریان دائمی را شبیه سازی می کند. یک خطای سه فاز به زمین با Rg=۰/۰۰۱ اهم (مقاومت زمین) در t=۲ ثانیه در وسط خط شماره ۵-۷ اعمال می شود. رله های دو طرف خط مربوط به پست شماره ۷ و شماره ۵ با تشخیص افزایش سطح جریان نسبت به مقدار تعریف شده، فرمان قطع را به کلیدهای قدرت ارسال می کنند. جریان خطا در باس۷ و باس۵ به ۶ پریونیت افزایش می یابد و بنابراین رله اضافه جریان به سرعت این وضعیت غیرعادی را تشخیص می دهد.



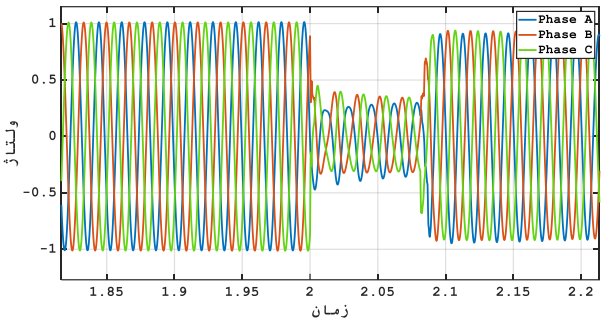
شکل۶ - جریان خط از سمت باس ۷



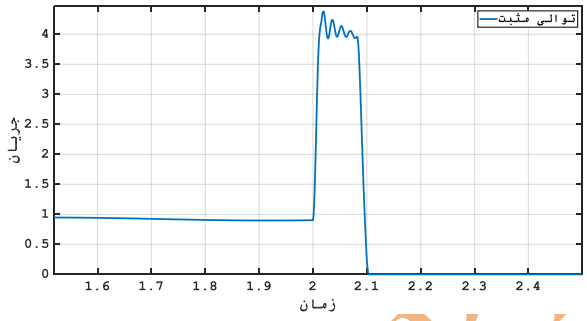
شکل۷ - جریان خط از سمت باس ۵

فرآیند ارسال فرمان و قطع کلید پس از ۴ سیکل تکمیل می شود که در حد استانداردهای عملی سیستم قدرت می باشد. توانهای اکتیو تحویلی ژنراتورها و زوایای بار در اثر این خطا دارای نوسان هستند. این گونه نوسانات به تدریج میرا می شوند و سیستم قدرت پس از رفع خطا به حالت پایداری باز می گردد. ولتاژ سه فاز در هر دو باس در حالت خطا به سمت صفر کاهش می یابد و پس از رفع آن به مقدار قبلی همگرا می شود.

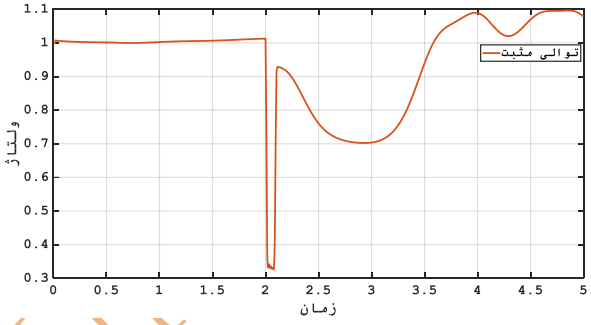
نتایج جریان و ولتاژ توالی مثبت در باس ۷ در شکل های زیر نشان داده شده است. با توجه به اینکه خطای سه فاز رخ داده مقادیر توالی منفی در تشخیص این نوع خطا لحاظ نمی شود.



شکل۸ - ولتاژ در باس ۷



شکل۹ - والی مثبت جریان باس ۷

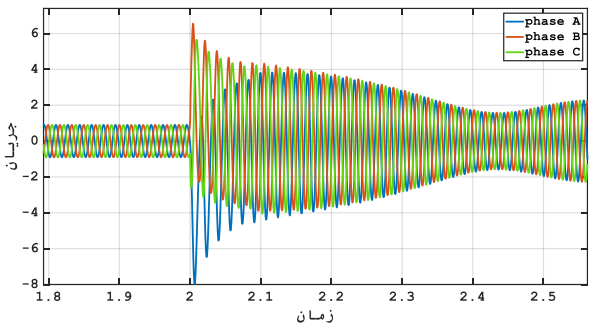


شکل۱۰- توالی مثبت ولتاژ باس ۷

۵-۲- اثرحمله تغییر مقدار تنظیمی رله اضافه جریان

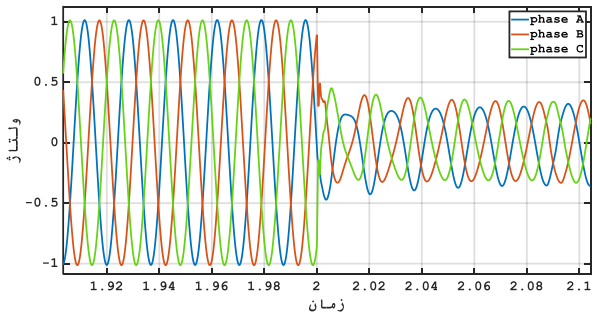
هنگام راه اندازی سیستم قدرت، یک لیست تنظیمات برای پیکربندی رله ها استفاده می شود که در آن مقادیر آستانه تنظیم می شود. برای تشخیص عیوب شبکه باید تنظیمات رله ها به دقت انجام شود تا در مواقع نیاز

بتوانند فرمان مقتضی را به کلیدها ارسال کنند. هر گونه دستکاری در مقادیر تنظیمی رله ها یک حمله سایبری است. اگر هکر مقادیر آستانه را افزایش دهد، خطای اتصال کوتاه توسط رله تشخیص داده نمی شود و کلیدها در چنین شرایط غیرعادی عمل نمی کنند و خطا ایزوله نمی شود. از طرفی در صورت کاهش مقادیر آستانه در اثر حمله، این امکان وجود دارد که هر گونه افزایش بار سیستم به عنوان خطا در نظر گرفته شود و دستور تریپ توسط رله ارسال شود. در این بخش حمله فوق برای مدل استاندارد IEEE با در نظر گرفتن ارسال فرمان از طریق کانال های مخابراتی پیاده سازی شده است. طبق استانداردها، مقدار جریان پیک آپ دو برابر (برابر ۲۰۰٪) جریان نامی رله خط مورد حفاظت ۵-۷ می باشد. بنابراین در این نوع حملات فرض بر این است که هکر با هجوم و نفوذ به تنظیمات رله ها و تغییر تنظیمات از پیش تعریف شده آنها، مقدار جریان پیک آپ رله شماره ۷ را از ۲pu به pu ۱۵ افزایش می دهد. سپس یک خطای سه فاز به زمین در وسط خط انتقال مفروض در t=۲ ثانیه اعمال می شود و در t=۵ ثانیه خاتمه می یابد. بنابراین اضافه جریان ناشی از خطا از طریق رله اضافه جریان تشخیص داده نمی شود و علت اصلی آن حمله خرابکارانه و تغییر مقدار تنظیمی رله است. در نتیجه این حمله، کلید نصب شده در باس ۷ به کار خود ادامه می دهد و قطع نمی شود. بنابراین، خطا به طور مداوم در سیستم باقی می ماند و زوایای قدرت ژنراتورها به شدت نوسان می کند که می تواند منجر به ناپایداری کلی سیستم شود. جریان خط از سمت باس ۷ نشان داده شده است. رله و کلید موجود در باس شماره به عملکرد عادی خود ادامه می دهند.



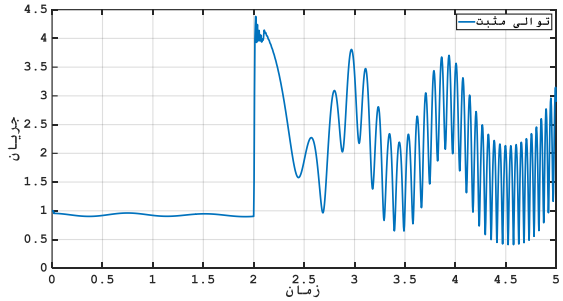
شکل۱۱- جریان خط از سمت باس ۷

ولتاژ در باس ۷ در طول حمله مانند شکل نزدیک به صفر باقی می ماند و در اطراف آن نوسان می کنند.

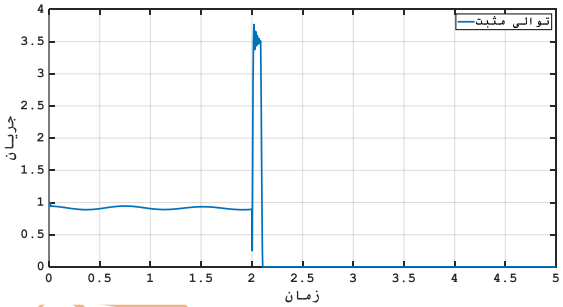


شکل۱۲ - ولتاژ در باس ۷

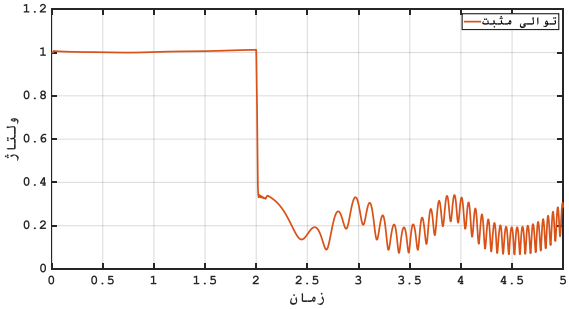
در این حالت که حمله سایبری صرفا به رله شماره ۷ صورت گرفته رله شماره ۵ فرمان قطع را به کلید مربوطه ارسال می کند و جریان تغذیه خطا از طرف باس ۵ به صفر می رسد و ولتاژ این باس تقریبا به یک پریونیت برمی گردد نتایج جریان و ولتاژ توالی مثبت در باس های ۷ و ۵ در شکل های زیر نشان داده شده است.



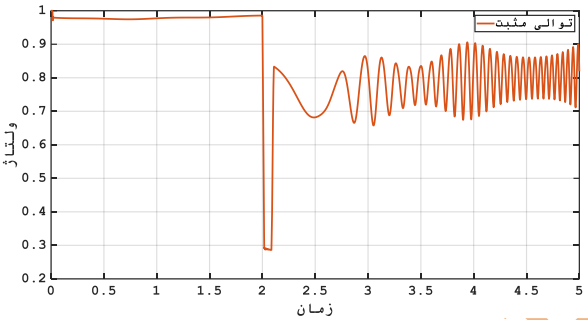
شکل۱۳- توالی مثبت جریان باس ۷



شکل۱۴- توالی مثبت جریان باس ۵



شکل ۱۵- توالی مثبت ولتاژ باس ۷

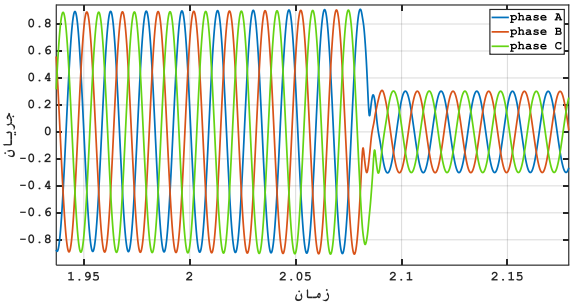


شکل۱۶ - توالی مثبت ولتاژ باس۵

همان طور که از شکل ها مشخص است جریان توالی مثبت باس ۷ به صورت نوسانی و افزایشی ادامه دارد و متعاقبا ولتاژ آن افت شدیدی دارد و برای باس ۵ به دلیل عملکرد رله و ارسال فرمان ولتاژ به سمت تثبیت در مقدار قبلی و جریان خطا قطع شده است.

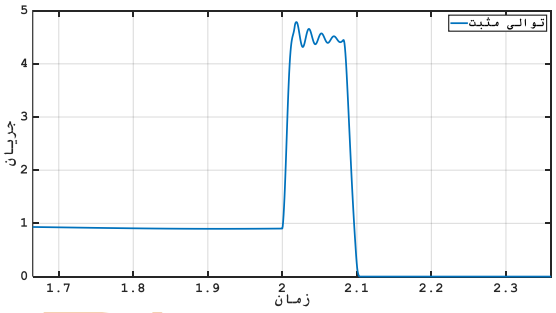
۵-۳- اثرحمله تزریق داده نادرست

حمله تزریق داده نادرست در این قسمت به صورت تزریق داده جریان ثبت شده خطای قبلی به جریان ورودی به رله است که هم زمان به دامنه و فاز جریان حمله صورت می گیرد. حمله تکرار به رله حفاظتی اضافه جریان به منظور دستکاری در داده های اندازه گیری حفاظت انجام می شود که در سبب ارسال فرمان نادرست به کلید می شود. در این حالت نتایج ثبت شده یک خطای سه فاز به زمین در وسط خط انتقال ۷-۵ در t=۲ ثانیه به ورودی جریان اندازه گیری رله شماره ۷ تزریق می شود. هکر در اینجا قادر است با دسترسی به کانال های ارتباطی داده های فرایند قبلی را به ورودی رله تزریق کند. در نتیجه، در حالی که هیچ خطای واقعی در سیستم وجود ندارد، رله شماره ۷ کلید را باز می کند. حمله تزریق داده از نوع تکرار ممکن است برای یک واحد کوچک شدید نباشد اما می تواند با ایجاد حملات هماهنگ اثرات فاجعه باری ایجاد کند. در حین حمله تکرار، در حالی که هیچ نقص واقعی در سیستم وجود ندارد و متعاقباً هیچ اختلالی در جریان بار ولتاژ، وجود ندارد سیستم حفاظت اضافه جریان دستخوش یک سناریوی خطای جعلی توسط مهاجم می شود. اگر سیستم حفاظتی قادر به مشاهده پارامترهای دینامیکی بلادرنگ شبکه مانند جریان خط، ولتاژ و وضعیت فرمان های ارسالی رله های مجاور باشد شرایط خطا را از سناریوهای حمله متمایز می کند، به طوری که از باز کردن و بستن غیر ضروری کلیدها جلوگیری می شود. منحنی تزریق جریان از سمت باس ۷ و توالی مثبت آن مطابق با حالت خطای سه فاز بوده و کلید مربوط با دیدن خطای کاذب باز می شود و جریان به صفر می رسد در حالی که جریان باس ۵ به علت باز شدن خط از بالا مانند شکل زیر تغییر کرده و عملا در مقدار کمی به اندازه شارژ خازنی خط انتقال قرار می گیرد.

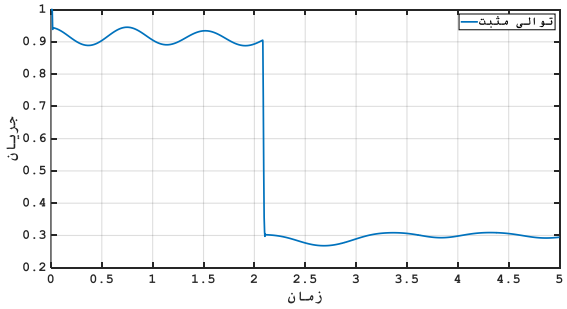


شکل ۱۷- جریان خط از سمت باس ۵

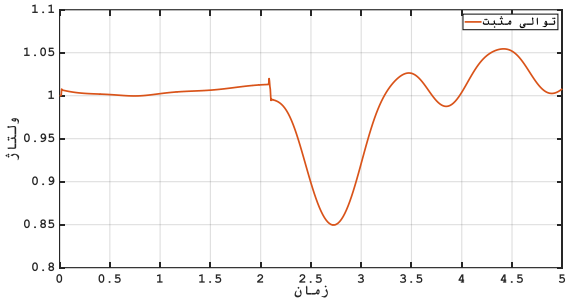
ولتاژ هر دو باس در اثر کلید زنی در باس شماره ۷ نوسان کوچکی داشته و تقریبا بدون تغییر باقی می مانند. جریان توالی مثبت و ولتاژ توالی مثبت هر دوباس در ادامه نشان داده شده است.



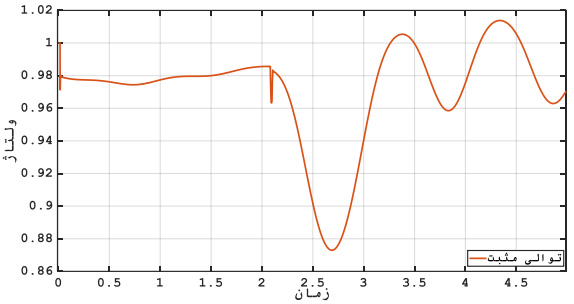
شکل ۱۸- توالی مثبت جریان باس ۷



شکل ۱۹- توالی مثبت جریان باس ۵



شکل ۲۰- توالی مثبت ولتاژ باس ۷

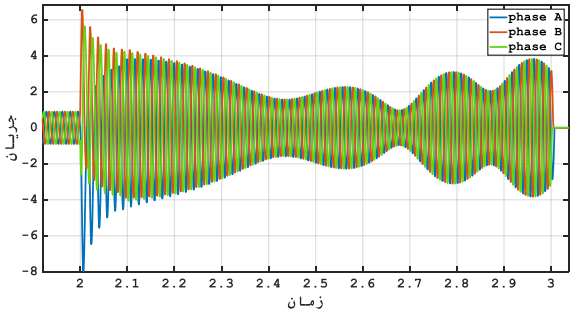


شکل ۲۱- توالی مثبت ولتاژ باس ۵

۵-۴- اثرحمله توقف سرویس دهی

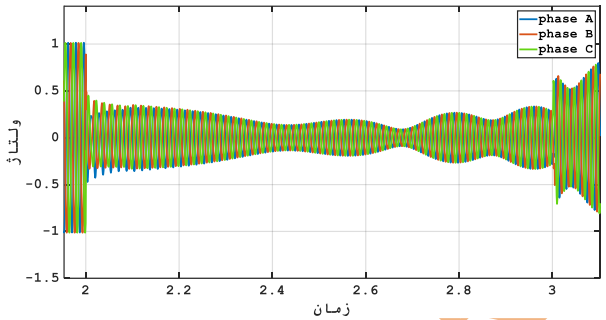
حملات DoS معمولاً با ایجاد تأخیر یا جلوگیری کامل در ارسال دستورات از رله‌های دیجیتال به کلیدها شروع می‌شوند. در حین اجرای این حملات، نفوذگر می تواند عملکرد رله ها را در سه حالت بلاک کردن، تاخیر و یا رد کردن تنظیم کند و نتیجه یک حمله موفقیت آمیز می تواند منجر به خسارات جبران ناپذیری در عملکرد و رفتار دینامیکی سیستم شود.

برای اجرای یک حمله DoS، یک خطای سه فاز به زمین در وسط خط انتقال ۷-۵ در t=۲ ثانیه اعمال می شود. به دلیل وجود الگوریتم های حفاظتی، رله اضافه جریان بلافاصله وقوع عیب را تشخیص می دهد، اما فعال شدن حمله توقف سرویس دهی باعث می شود که فرمان قطع با تاخیر ۱ ثانیه ارسال شود و سپس کلید قطع شود. . اصولاً حداکثر تأخیر قابل قبول هنگام صدور فرمان قطع کلید در شبکه برق که به صورت مجموع تأخیرهای محاسباتی و ارتباطی محاسبه می شود، ۴ سیکل در نظر گرفته می شود. در این حالت، به دلیل اینکه تاخیر اعمال شده بیشتر از مقدار استاندارد است، باعث ایجاد نوسانات شدید در رفتار دینامیکی سیستم می شود. واضح است که اگر خطای اتصال کوتاه بیش از زمان تعریف شده استاندارد (۰/۲ ثانیه) باقی بماند و تجهیزات حفاظتی به موقع کار نکنند، شبکه قدرت در مقایسه با حالت رفع عیب به موقع، شرایط ناپایداری را تجربه خواهد کرد [۴۱]. جریان خط از باس ۷ در شکل نشان داده شده است.



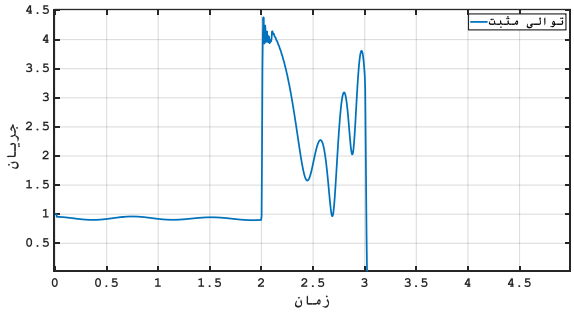
شکل ۲۲- جریان خط از سمت باس ۷

ولتاژ در باس ۷ در طول حمله مانند شکل نزدیک به صفر باقی می ماند و در اطراف آن نوسان می کند و سپس به به مقدار نامی همگرا می شود.



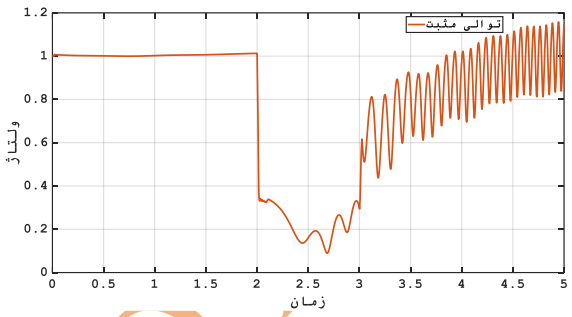
شکل۲۳ - ولتاژ در باس ۷

جریان توالی مثبت از سمت باس ۷ مانند شکل زیر تغییر میکند ولی چون رله ۵ مورد حمله واقع نشده کلید آن در زمان مقتضی عمل می کند و توالی مثبت جریان آن بدون تغییر و شبیه به زمان اعمال خطای سه فاز باقی می ماند.

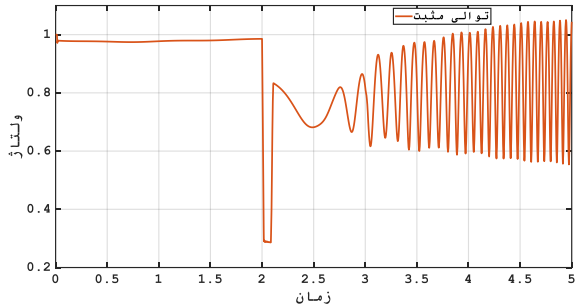


شکل۲۴ - توالی مثبت جریان باس ۷

رفتار دینامیکی ولتاژ توالی مثبت در هر دو باس در ادامه نشان داده شده است. همان طورکه مشاهده می شود توالی مثبت ولتاژ در باس ۷ دستخوش تغییرات طولانی تر و با نوسان بیشتر قرار گرفته و پس از اتمام حمله به مقدار قبلی همگرا می شود این در حالی است که ولتاژ توالی مثبت در باس ۵ نیز با عبور از مراحل نوسانی به یک پریونیت همگرا می شود.



شکل ۲۵ - توالی مثبت ولتاژ باس ۷



شکل ۲۶ - توالی مثبت ولتاژ باس ۵

۵-۵- تشخیص حملات سایبری به روش پیشنهادی

برای شناسایی حملات سایبری مختلف، از سیگنال های مختلف شامل جریان، ولتاژ باس ها و فرمان رله ها استفاده شده است. استفاده از سیگنال های الکتریکی که معمولاً برای اهداف کنترلی و نظارت بر شرایط در سیستم استفاده می شود، از نظر عملی، فنی و اقتصادی کاملاً موجه است و بنابراین هزینه های مربوط به طراحی و مسائل فنی ناشی از نصب تجهیزات و سنسورهای جدید به طور کامل حذف شده اند. هدف اصلی روش پیشنهادی تشخیص جامع و همچنین داشتن حداقل حجم محاسبات می باشد[۴۲].

در این مقاله برای تشخیص انواع خطا و حملات سایبری و کلاسه بندی آنها از نتایج توالی مثبت و منفی جریان و ولتاژ باس ها در بخش شبیه سازی ۵-۱ تا ۵-۴ و استخراج ویژگی های مورد نظر از آنها مطابق ذیل برای تشخیص و مقابله با خطای سه فاز و برخی حملات سایبری استفاده می‌شود. ابتدا با انجام شبیه سازی خطای سه فاز در m=۵۰ نقطه مختلف از طول خط انتقال و سه نوع حمله سایبری یک مقدار آستانه مشترک برای هر کدام از کمیت های توالی مثبت ولتاژ و جریان در هر باس مطابق ذیل تعیین می شود که عبور از آن یکی از شرایط شروع پروسه تشخیص است:

$$\delta_I = \min\{\delta_1,\ldots,\delta_m\}$$
$$\delta_V = \max\{\delta_1,\ldots,\delta_m\} \qquad (۸)$$

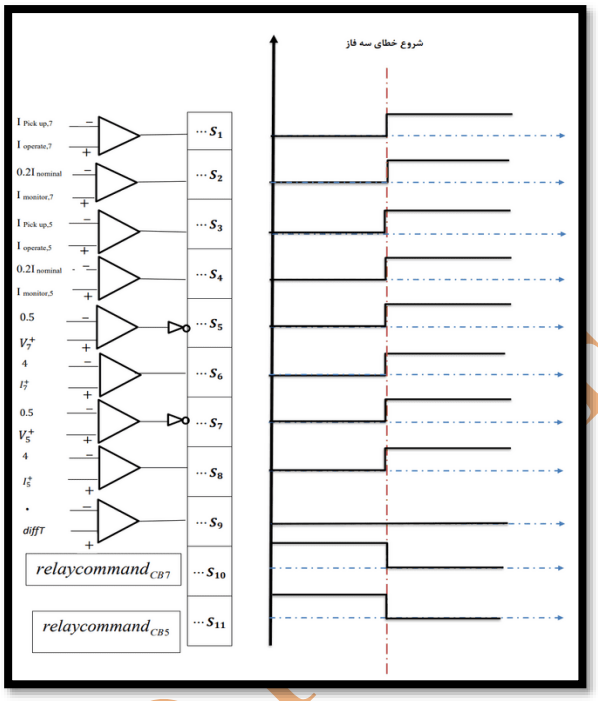
با تکرار شبیه سازی در یک حالت بهره برداری مشخص می توان مقادیر آستانه را برای تشخیص تعیین نمود و در صورتی که نقطه کار بهره برداری شبکه تغییر کند این مقادیر در الگوریتم بروز رسانی می شوند.

جدول ۱- آستانه پیشنهادی برای تشخیص خطای سه فاز و انواع حمله

δ_{V^+5}	δ_{I^+5}	δ_{V^+7}	δ_{I^+7}
۰/۵	۴	۰/۵	۴

- **منطق پیشنهادی تشخیص خطای سه فاز**

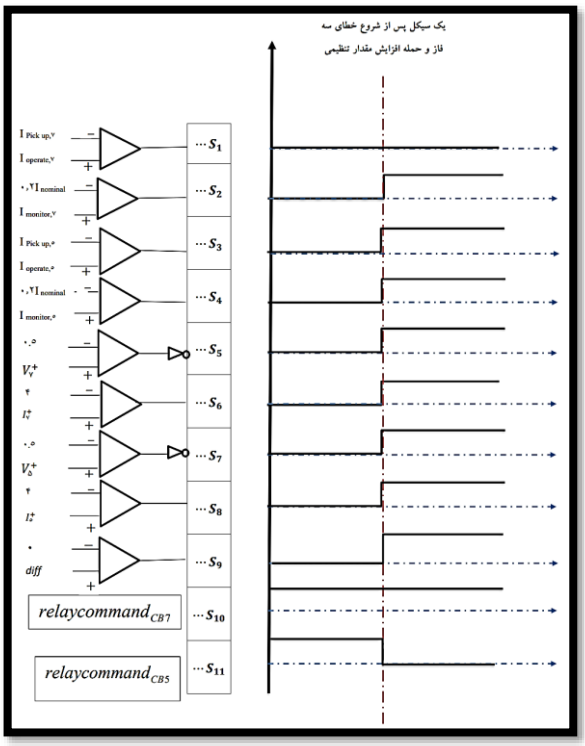
برای تشخیص خطای سه فاز ۱۱ کمیت در دو طرف خط تحت حفاظت مورد مقایسه قرار می گیرد. در صورتی که آستانه ولتاژ توالی مثبت هر دو طرف خط کمتر از ۰/۵ پریونیت (S_5 و S_7) و آستانه جریان توالی مثبت بیشتر از ۴ پریونیت باشد (S_6 و S_8) در شرایطی که هر دو رله پیک آپ کرده باشند (S_1 و S_3) و جریان پایش بیشتر از ۰/۲ پریونیت باشد (S_2 وS_4) اعلام خطای سه فاز توسط منطق پیشنهادی زیر صورت و با توجه به یازده سیگنال S_1 تا S_{11} می گیرد و سیگنال خروجی رله به سمت کلید اعمال می شود. سیگنال های S_9 , S_{10} و S_{11} به ترتیب اختلاف دامنه فرمان دو رله طرفین خط، فرمان رله شماره ۷ و فرمان رله شماره ۵ می باشند.



شکل ۲۷- بردار سیگنال منطقی خروجی در خطای سه فاز

- **منطق پیشنهادی تشخیص حمله افزایش مقدار تنظیمی**

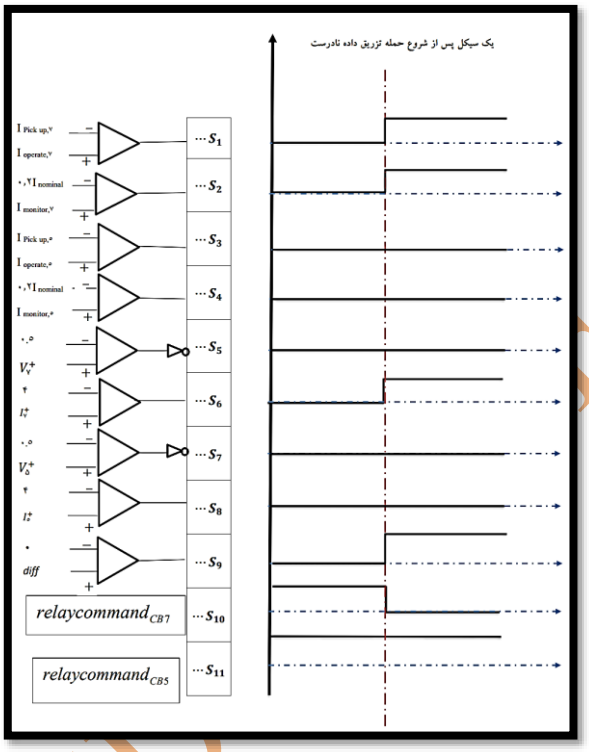
برای تشخیص حمله افزایش مقدار تنظیمی به رله ۷ در حین خطای سه فاز در صورتی که آستانه ولتاژ توالی مثبت هر دو طرف خط کمتر از ۰/۵ پریونیت و آستانه جریان توالی مثبت بیشتر از ۴ پریونیت باشد در صورتی که رله شماره ۵ پیک آپ کرده ولی رله شماره ۷ پیک آپ نکرده باشند و جریان پایش هر دو طرف بیشتر از ۰/۲پریونیت باشد و همچنین اختلاف دامنه فرمان قطع بین دو رله (diff) یک باشد اعلام حمله توسط منطق پیشنهادی زیر صورت می گیرد و سیگنال فرمان قطع از رله ۷ پس از زمان مشخص (β) به کلید اعمال می شود.



شکل ۲۸- بردار سیگنال منطقی خروجی در حمله افزایش مقدار تنظیمی

- **منطق پیشنهادی تشخیص حمله تزریق داده نادرست**

برای تشخیص حمله تزریق داده نادرست جریان به ورودی رله ۷ در صورتی که آستانه ولتاژ توالی مثبت هر دو طرف خط بیشتر از ۰/۵ پریونیت و آستانه جریان توالی مثبت فقط رله ۷ بیشتر از ۴ پریونیت باشد در صورتی که فقط رله شماره ۷ پیک آپ کرده باشند و جریان پایش رله ۷ بیشتر از ۰/۲ پریونیت باشد و همچنین اختلاف دامنه فرمان قطع بین دو رله (diff) یک باشد اعلام حمله توسط منطق پیشنهادی صورت می گیرد و سیگنال فرمان بلاک رله ۷ پس از مدت زمان معین (β) به سمت کلید اعمال می شود.

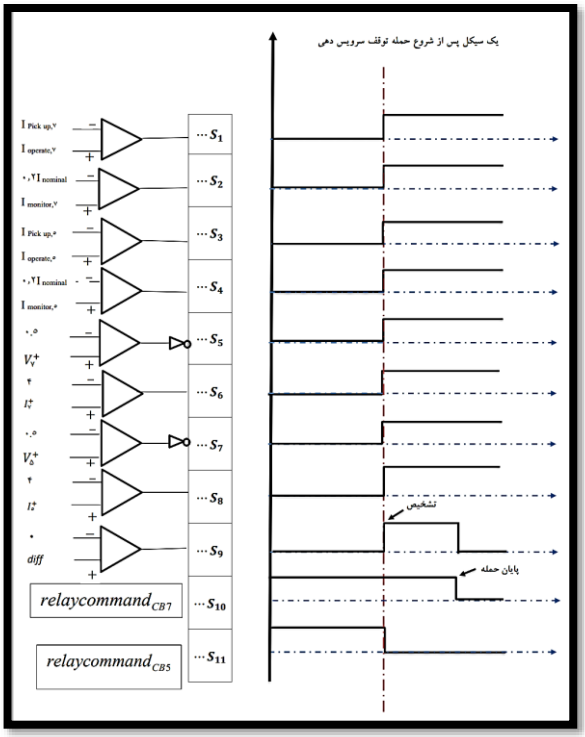


شکل ۲۹- بردار سیگنال منطقی خروجی در حمله تزریق داده نادرست

- **منطق پیشنهادی تشخیص حمله توقف سرویس دهی**

برای تشخیص حمله توقف سرویس دهی رله ۷ در خطای سه فاز در صورتی که آستانه ولتاژ توالی مثبت هر دو طرف خط کمتر از ۰/۵ پریونیت و آستانه جریان توالی مثبت هر دو رله بیشتر از ۴ پریونیت باشد در صورتی که هر دو رله پیک آپ کرده باشند و جریان پایش بیشتر از ۰/۲ پریونیت باشد در صورتی که رله شماره ۵ فرمان قطع ارسال کند ولی رله شماره ۷ فرمان ارسال نکند در صورتی که اختلاف دامنه فرمان قطع بین دو رله (diff) یک باشد سیگنال فرمان قطع به رله شماره ۷ پس از زمان معین (β) ارسال می شود و اعلام حمله صورت گیرد.

پوشش همه جانبه شرایط مختلف و قابلیت اجرا در محیط های صنعتی از قابلیت های اصلی روش توصیف شده به شمار می رود. برای ارزیابی حساسیت روش پیشنهادی، خطاهای نامتقارن با نرخ نمونه برداری مختلف پیاده‌سازی شد. در چنین شرایطی ماهیت روش پیشنهادی تغییر نداشت و فقط مقادیر آستانه توالی مثبت جریان و ولتاژ بروز رسانی شد.

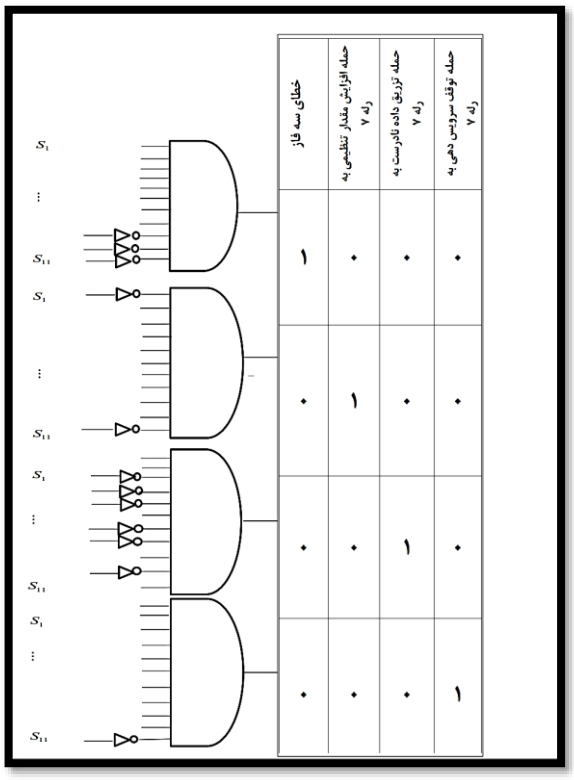


شکل ۳۰- بردار سیگنال منطقی خروجی در حمله توقف سرویس دهی

بنابراین می توان نتیجه گرفت که روش جدید برای تغییر نوع خطا ، شرایط بهره برداری و نرخ نمونه برداری سیگنال مقاوم است. در صورتی که الگوریتم‌های ذکر شده در این بخش در نتایج نشان داده شده در بخش ۵-۲ تا ۵-۴ اعمال شوند از ادامه عملکرد سیستم در حالت حمله سایبری جلوگیری می شود و از شدت حمله سایبری و اثرات آن تا حد زیادی کاسته می شود. نکته قابل توجه در الگوریتم پیشنهادی افزایش زمان پردازش سیگنال با افزایش تعداد تجهیزات حفاظتی و متعاقبا تعدد عملگرهای منطقی می‌باشد که در این مقاله با فرض حمله به یک رله از محدوده مجاز زمانی عملکرد کلید تجاوز نمی‌کند و مقابله با حمله به موقع صورت می گیرد. در ادامه جدول سیگنال های خروجی در هر شرایط نشان داده شده است و گیت های منطقی مربوط به تشخیص هر کدام از حملات با توجه به عدم تداخل در تشخیص نشان داده شده است.

جدول ۲- سیگنال های خروجی منطق پیشنهادی برای تشخیص خطای سه فاز و انواع حمله

رویداد	خطای سه فاز	حمله افزایش مقدار تنظیمی به رله ۷	حمله تزریق داده نادرست به رله ۷	حمله توقف سرویس دهی به رله ۷
S_1	۱	۰	۱	۱
S_2	۱	۱	۱	۱
S_3	۱	۱	۰	۱
S_4	۱	۱	۰	۱
S_5	۱	۱	۰	۱
S_6	۱	۱	۱	۱
S_7	۱	۱	۰	۱
S_8	۱	۱	۰	۱
S_9	۰	۱	۱	۱
S_{10}	۰	۱	۰	۱
S_{11}	۰	۰	۱	۰



شکل ۳۱ – دیاگرام منطقی الگوریتم پیشنهادی تشخیص

۶- بحث و نتیجه گیری

در این مقاله مدل جدیدی برای مشخصه رله اضافه جریان با افزودن پارامتر جریان پایش به آن و همچنین اجرای سه نوع حمله سایبری در این بستر پیشنهاد گردید. مزیت عمده چنین مدل‌سازی قابلیت آن در فرآیند تشخیص و تمایز حملات به صورت مستقیم در برخی موارد و همچنین به صورت غیر مستقیم می باشد. الگوریتم تشخیص پیشنهادی به عنوان ترکیبی از جریان عملکرد رله، جریان پایش، سیگنال های توالی مثبت و منفی جریان، ولتاژ و فرمان ارسالی توسط رله ها و مقایسه آنها با مقادیر آستانه از پیش تعریف شده در منطق حاکم بیان می‌شود. روش پیشنهادی به داده‌های آموزشی حملات احتمالی که غیر قابل پیش بینی بوده و در دسترس شبکه نیست وابستگی ندارد. نتایج نشان می‌دهد که با فرض اجرای حملات تکی به یک رله الگوریتم قابلیت تشخیص و تمایز حملات سایبری تعریف شده را در مدت زمان ۱۷ میلی ثانیه داشته و فرمان مقتضی را به رله تحت حمله ارسال می کند. شایان ذکر است که الگوریتم منحصر به فرد پیشنهادی در برابر هرگونه تغییر در شرایط بهره برداری، نرخ نمونه برداری و اشباع CT مقاوم است. این روش نسبت به سایر تکنیک های تشخیص برتری دارد زیرا به نقطه عملیاتی، طرح حفاظت رله و نوع حمله سایبری وابسته نیست. اجرای الگوریتم به دلیل نیاز نظارت مستمر شرایط زمان واقعی پرهزینه است ولی با توجه به هزینه بالای زیان تحمیلی و ریسک ایجاد شده از ناحیه حملات سایبری در سیستم قدرت تخصیص مقادیر بالای بودجه به این حوزه به منظور افزایش امنیت سایبری از نظر اقتصادی در مجامع بین المللی توجیه پذیر می باشد.

این نتیجه گیری همچنین می تواند در تشخیص حملات سایبری هماهنگ به چند رله نیز مورد استفاده قرار گیرد. در این صورت می بایست کمیت های مشابه در پشت رله ها و دیگر باس ها نیز در الگوریتم وارد شود. در این صورت با افزایش تعداد تجهیزات حفاظتی زمان پردازش مورد نیاز داده‌ها در باس های مختلف افزایش می‌یابد که عیب عمده‌ی بهره‌گیری از روش‌های بر مبنای مقایسه است. در این صورت می توان اثر گسترده کردن سیستم

تشخیص و تقسیم بندی آن به نواحی مختلف، به منظور کاهش زمان عملکرد و قرار گرفتن آن در محدوده عملی مجاز کلیدها و به موقع عمل کردن و رفع حملات سایبری را بررسی نمود.

در ادامه می‌توان مدل پیشنهادی رله و الگوریتم تشخیص حملات سایبری را در شبکه های توزیع استاندارد بررسی نمود. تاثیر سناریوهای متعدد از قبیل برخورد صاعقه و سایر موارد گذرا، وجود شرایط بهره برداری از پیش تعیین نشده، امپدانس های مختلف خطا ، نفوذ منابع انرژی توزیع شده بر روش پیشنهادی و امکان سنجی حملات سایبری ذکر شده در سیستم ارتباطی واقعی، هدف آتی تحقیقات می باشد.

پیوست

جدول۳ - داده های بار

شماره باس	توان اکتیو (مگاوات)	توان راکتیو (مگاوار)
۵	۱۲۵	۵۰
۶	۹۰	۳۰
۸	۱۰۰	۳۵

جدول ۴- داده های خطوط انتقال

شماره خط انتقال	مقاومت (اهم بر کیلومتر)	اندوکتانس (میلی هانری بر کیلومتر)	کاپاسیتانس (نانو فاراد بر کیلومتر)	طول خط (کیلومتر)
۵-۴	۰/۰۵۲۹	۱/۱۹۲	۸/۸۲	۱۰۰
۶-۴	۰/۰۸۹۹۳	۱/۲۹	۷/۹۲۲	۱۰۰
۷-۵	۰/۲۰۶۳۱	۲/۳۸	۱۷/۹۵	۱۰۰
۹-۶	۰/۱۶۹۲۸	۲/۲۵۹	۱۵/۳۴	۱۰۰
۸-۷	۰/۰۴۴۹۶۵	۱/۰۱	۷/۴۷۱	۱۰۰
۹-۸	۰/۰۶۲۹۵۱	۱/۴۱۴	۱۰/۴۷	۱۰۰

مراجع

[1] Tesfay, Teklemariam Tsegay. *Cybersecurity solutions for active power distribution networks*. No. 7484. EPFL, 2017.

[2] Huseinović, Alvin, Saša Mrdović, Kemal Bicakci, and Suleyman Uludag. "A survey of denial-of-service attacks and solutions in the smart grid." *IEEE Access* 8 (2020): 177447-177470.

[3] Wang, Shouxiang, Dong Liang, Leijiao Ge, and Xudong Wang. "Analytical FRTU deployment approach for reliability improvement of integrated cyber-physical distribution systems." *IET Generation, Transmission & Distribution* 10, no. 11 (2016): 2631-2639.

[4] Hasan, Mohammad Kamrul, AKM Ahasan Habib, Zarina Shukur, Fazil Ibrahim, Shayla Islam, and Md Abdur Razzaque. "Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations." *Journal of network and computer applications* 209 (2023): 103540.

[5] He, Haibo, and Jun Yan. "Cyber-physical attacks and defences in the smart grid: a survey." *IET Cyber-Physical Systems: Theory & Applications* 1, no. 1 (2016): 13-27.

[6] Santos, B. Paiva, F. Charrua-Santos, and T. M. Lima. "Industry 4.0: an overview." In *Proceedings of the World Congress on engineering*, vol. 2, pp. 4-6. IAEN, London, UK, 2018.

[7] Delgado-Gomes, Vasco, Joao F. Martins, Celson Lima, and Paul Nicolae Borza. "Smart grid security issues." In *2015 9th International conference on compatibility and power electronics (CPE)*, pp. 534-538. IEEE, 2015.

[8] Rawat, Danda B., and Chandra Bajracharya. "Cyber security for smart grid systems: Status, challenges and perspectives." *SoutheastCon 2015* (2015): 1-6.

[9] Shapsough, Salsabeel, Fatma Qatan, Raafat Aburukba, Fadi Aloul, and A. R. Al Ali. "Smart grid cyber security: Challenges and solutions." In *2015 international conference on smart grid and clean energy technologies (ICSGCE)*, pp. 170-175. IEEE, 2015.

[10] Al-Garadi, Mohammed Ali, Amr Mohamed, Abdulla Khalid Al-Ali, Xiaojiang Du, Ihsan Ali, and Mohsen Guizani. "A survey of machine and deep learning methods for internet of things (IoT) security." *IEEE communications surveys & tutorials* 22, no. 3 (2020): 1646-1685.

[11] Zhang, Hang, Bo Liu, and Hongyu Wu. "Smart grid cyber-physical attack and defense: A review." *IEEE Access* 9 (2021): 29641-29659.

[12] Krause, Tim, Raphael Ernst, Benedikt Klaer, Immanuel Hacker, and Martin Henze. "Cybersecurity in power grids: Challenges and opportunities." *Sensors* 21, no. 18 (2021): 6225.

[13] Boeding, Matthew, Kelly Boswell, Michael Hempel, Hamid Sharif, Juan Lopez Jr, and Kalyan Perumalla. "Survey of cybersecurity governance, threats, and countermeasures for the power grid." *Energies* 15, no. 22 (2022): 8692.

[14] Aslan, Ömer, Semih Serkant Aktuğ, Merve Ozkan-Okay, Abdullah Asim Yilmaz, and Erdal Akin. "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions." *Electronics* 12, no. 6 (2023): 1333

[15] Premaratne, Upeka Kanchana, Jagath Samarabandu, Tarlochan S. Sidhu, Robert Beresh, and Jian-Cheng Tan. "An intrusion detection system for IEC61850 automated substations." *IEEE Transactions on Power Delivery* 25, no. 4 (2010): 2376-2383.

[16] Jin, Dong, David M. Nicol, and Guanhua Yan. "An event buffer flooding attack in DNP3 controlled SCADA systems." In *Proceedings of the 2011 Winter Simulation Conference (WSC)*, pp. 2614-2626. IEEE, 2011.

[17] Liang, Gaoqi, Steven R. Weller, Junhua Zhao, Fengji Luo, and Zhao Yang Dong. "The 2015 Ukraine blackout: Implications for false data injection attacks." *IEEE transactions on power systems* 32, no. 4 (2016): 3317-3318.

[18] Li, Yang, Xinhao Wei, Yuanzheng Li, Zhaoyang Dong, and Mohammad Shahidehpour. "Detection of false data injection attacks in smart grid: A secure federated deep learning approach." *IEEE Transactions on Smart Grid* 13, no. 6 (2022): 4862-4872.

[19] Li, Yuncheng, and Yuanyuan Wang. "False data injection attacks with incomplete network topology information in smart grid." *IEEE Access* 7 (2018): 3656-3664.

[20] Bi, Suzhi, and Ying Jun Zhang. "Graphical methods for defense against false-data injection attacks on power system state estimation." *IEEE Transactions on Smart Grid* 5, no. 3 (2014): 1216-1227.

[21] AEMO: 'Australian energy sector cyber security framework education workshop', October (2018)

[22] Gurevich, Vladimir. *Cyber and electromagnetic threats in modern relay protection*. Crc Press, 2014.

[23] Deng, Ruilong, Gaoxi Xiao, and Rongxing Lu. "Defending against false data injection attacks on power system state estimation." *IEEE Transactions on Industrial Informatics* 13, no. 1 (2015): 198-207.

[24] Wang, Qi, Wei Tai, Yi Tang, and Ming Ni. "Review of the false data injection attack against the cyber-physical power system." *IET Cyber-Physical Systems: Theory & Applications* 4, no. 2 (2019): 101-107.

[25] Kim, Jinsub, and Lang Tong. "On topology attack of a smart grid: Undetectable attacks and countermeasures." *IEEE Journal on Selected Areas in Communications* 31, no. 7 (2013): 1294-1305.

[26] Choi, Dae-Hyun, and Le Xie. "Economic impact assessment of topology data attacks with virtual bids." *IEEE Transactions on Smart Grid* 9, no. 2 (2016): 512-520.

[27] Ameli, Amir, Ali Hooshyar, and Ehab F. El-Saadany. "Development of a cyber-resilient line current differential relay." *IEEE Transactions on Industrial Informatics* 15, no. 1 (2018): 305-318.

[28] Liang, Gaoqi, Steven R. Weller, Junhua Zhao, Fengji Luo, and Zhao Yang Dong. "A framework for cyber-topology attacks: Line-switching and new attack scenarios." *IEEE Transactions on Smart Grid* 10, no. 2 (2017): 1704-1712.

[29] Hong, Junho, Reynaldo F. Nuqui, Anil Kondabathini, Dmitry Ishchenko, and Aaron Martin. "Cyber attack resilient distance protection and circuit breaker control for digital substations." *IEEE Transactions on Industrial Informatics* 15, no. 7 (2018): 4332-4341.

[30] Johnson, Jay, Jimmy Quiroz, Ricky Concepcion, Felipe Wilches-Bernal, and Matthew J. Reno. "Power system effects and mitigation recommendations for DER cyberattacks." *IET Cyber-Physical Systems: Theory & Applications* 4, no. 3 (2019): 240-249.

[31] Ten, Chee-Woo, Koji Yamashita, Zhiyuan Yang, Athanasios V. Vasilakos, and Andrew Ginter. "Impact assessment of hypothesized cyberattacks on interconnected bulk power systems." *IEEE Transactions on Smart Grid* 9, no. 5 (2017): 4405-4425.

[32] Liu, Xindong, Mohammad Shahidehpour, Zuyi Li, Xuan Liu, Yijia Cao, and Zhiyi Li. "Power system risk assessment in cyber attacks considering the role of protection systems." *IEEE Transactions on Smart Grid* 8, no. 2 (2016): 572-580.

[33] Amin, BM Ruhul, Seyedfoad Taghizadeh, Md Shihanur Rahman, Md Jahangir Hossain, Vijay Varadharajan, and Zhiyong Chen. "Cyber attacks in smart grid–dynamic impacts, analyses and recommendations." *IET Cyber-Physical Systems: Theory & Applications* 5, no. 4 (2020): 321-329.

[34] Khaw, Yew Meng, Amir Abiri Jahromi, Mohammadreza FM Arani, Scott Sanner, Deepa Kundur, and Marthe Kassouf. "A deep learning-based cyberattack detection system for transmission protective relays." *IEEE Transactions on Smart Grid* 12, no. 3 (2020): 2554-2565.

[35] Rahman, Md Shihanur, Md Apel Mahmud, Aman Maung Than Oo, and Hemanshu Roy Pota. "Multi-agent approach for enhancing security of protection schemes in cyber-physical energy systems." *IEEE transactions on industrial informatics* 13, no. 2 (2016): 436-447.

[36] Mohamed, Nancy, and Magdy MA Salama. "Data mining-based cyber-physical attack detection tool for attack-resilient adaptive protective relays." *Energies* 15, no. 12 (2022): 4328.

[37] Jahromi, Amir Abiri, Anthony Kemmeugne, Deepa Kundur, and Aboutaleb Haddadi. "Cyber-physical attacks targeting communication-assisted protection schemes." *IEEE Transactions on Power Systems* 35, no. 1 (2019): 440-450.

[38] Liang, Gaoqi, Steven R. Weller, Junhua Zhao, Fengji Luo, and Zhao Yang Dong. "A framework for cyber-topology attacks: Line-switching and new attack scenarios." *IEEE Transactions on Smart Grid* 10, no. 2 (2017): 1704-1712.

[39] NERC: 'Misoperations report'. Protection System Misoperations Task Force-NERC Planning Committee, 2013

[40] Sauer, P. W., and M. A. Pai. "Power System Dynamics and Stability, Prentice-Hall." *New Jersey* (1998).

[41] Rebizant, Waldemar, Janusz Szafran, and Andrzej Wiszniewski. "Digital signal processing in power system protection and control." (2011): 978-0.

[42] Yousefi kia, Mohammad, Mohsen Saniei, and Seyyed Ghodratollah Seifossadat. "A novel cyber-attack modelling and detection in overcurrent protection relays based on wavelet signature analysis." *IET*

Generation, Transmission & Distribution 17, no. 7 (2023): 1585-1600.