Iranian Electric Industry Journal
Quality & Productivity
P.P 11-18

Vol. 13/ No. 4/ Winter 2025
ISSN 2322-2344
EISSN 2717-1639

Optimizing the Topology of a Power Grid to Enhance its Resilience Against Cyber-Physical Attacks

Amir Khorsandi[1]، Mohammad Matin Hasani[2]

1 Amirkabir University of Technology - Tehran – Iran
a_khorsandi@aut.ac.ir
2 Amirkabir University of Technology - Tehran – Iran
hassanimohammadmatin1997@gmail.com

Abstract:

The increasing reliance on interconnected smart grids has made power systems vulnerable to sophisticated cyber-physical attacks (CPAs). These attacks, which combine cyber intrusions with physical disruptions, can lead to cascading failures and widespread blackouts, posing significant threats to critical infrastructure. This paper proposes a novel approach to enhance power grid resilience against CPAs by optimizing the network topology. The proposed method leverages Network Topology Optimization (NTO) to proactively adjust the grid's configuration, thereby mitigating the impact of potential attacks.The main idea is to strategically switch transmission lines and reconfigure bus connections to minimize disruption caused by targeted attacks. This approach aims to improve the grid's ability to withstand both cyber and physical threats by creating alternative pathways for power flow and reducing dependence on critical components. The NTO method considers various attack scenarios, including coordinated cyber-physical attacks that target both the control systems and the physical infrastructure of the grid. By anticipating potential attack vectors, the proposed approach proactively strengthens the grid's resilience.The optimization process involves formulating an objective function that minimizes load shedding under various attack scenarios. This function is subject to constraints that ensure the grid's operational limits are not violated during the reconfiguration process. The optimization problem is solved using a suitable algorithm that efficiently explores the space of possible network topologies to identify the most resilient configurations. The effectiveness of the proposed approach is demonstrated through case studies on the IEEE 57-bus test system. The results indicate that the optimized network topology significantly reduces load shedding compared to the original configuration under various attack scenarios. Additionally, the proposed method enhances the grid's ability to withstand cascading failures, which are often triggered by initial disruptions caused by CPAs.This paper makes several contributions to the field of power system resilience. First, it introduces a novel approach to enhance grid resilience against CPAs by optimizing network topology. Second, it develops a comprehensive optimization model that considers various attack scenarios and operational constraints. Third, it demonstrates the effectiveness of the proposed approach through case studies on a standard test system. The proposed approach offers a promising solution for enhancing power grid resilience against the growing threat of CPAs. By proactively adjusting network topology, the grid can become more robust and less susceptible to disruptions caused by malicious attacks. Future research directions include extending the proposed method to larger and more complex power systems and considering the dynamic nature of CPAs.
results demonstrate its effectiveness in fault location and fault resistance calculation.

Keywords: Cyber-physical attacks, network topology optimization (NTO), cyber security

Date of sending the article: 2024/01/27
Acceptance date of the article: 2025/02/08

Name of the Corresponding Author: Amir Khorsandi
Corresponding Author's Address: Amirkabir University of Technology - Tehran – Iran

[Downloaded from ieijqp.ir on 2026-01-29]

Iranian Electric Industry Journal
Quality & Productivity
ص.ص۱۸-۱۱

Vol. 13 / No. 4/ Winter 2025
ISSN 2322-2344
EISSN 2717-1639

بهینه سازی توپولوژی شبکه برق جهت مقاوم سازی در برابر حملات سایبری

محمدمتین حسنی[1]، کارشناسی ارشد، امیر خرسندی[2]، استادیار

۱- دانشکده مهندسی برق- دانشگاه صنعتی امیرکبیر- تهران- ایران
mmhasani@aut.ac.ir
۲- دانشکده مهندسی برق- دانشگاه صنعتی امیرکبیر - تهران- ایران
a_khorsandi@aut.ac.ir

چکیده: از گذشته تاکنون، امنیت سیستم‌های قدرت و حفظ آن‌ها در برابر حوادثی که با اثر زیاد و احتمال کم رخ می‌دهند مورد توجه بهره‌برداران سیستم‌های قدرت بوده است. با این حال، هنوز با وقوع حوادث شدید عملکرد سیستم‌های قدرت به طور شدیدی دچار اختلال می‌گردد. یک نمونه از این حوادث، حملات سایبری است. امروزه حملات و مخاطرات سایبری در شبکه برق افزایش یافته است. اگر سیستم بدون اقدامات متقابل و دفاعی مؤثر به کار گرفته شود، حملات مختلف سایبری ممکن است قابلیت اطمینان سیستم قدرت را به شدت به خطر بیاندازد. با توجه به اهمیت سیستم‌های قدرت، تقویت تاب آوری شبکه‌های برق علیه حملات مخرب سایبری به عنوان یک مساله‌ی مهم نمود پیدا می‌کند. بنابراین به منظور پیشگیری و جلوگیری از تهدیدات و حملات، باید تاب آوری توپولوژی شبکه برق را بهبود بخشید. در رابطه با این موضوع می‌توان مساله را در دو قدم مورد بررسی قرار داد:۱- انجام حملات هماهنگ سایبری به یک شبکه۲- دفاع در مقابل حملات انجام شده در قدم اولبرای دفاع در برابر حملات هماهنگ سایبری با شدت کمتر، معیار NTO پیشنهاد شده است که شامل اقدامات کلیدزنی و تقسیم بندی باس می‌باشد. به منظور نشان دادن تأثیرات حملات هماهنگ سایبری و همچنین اعتبار روش پیشنهادی، مطالعات موردی بر روی سیستم IEEE 57-BUS در نرم افزار GAMS انجام گرفته است.

واژه های کلیدی: حملات سایبری-فیزیکی، تاب آوری، امنیت سایبری، بهینه سازی توپولوژی شبکه (NTO)

تاریخ ارسال مقاله : ۱۴۰۲/۱۱/۰۷

تاریخ پذیرش مقاله : ۱۴۰۳/۱۱/۲۰

نام نویسنده‌ی مسئول : امیر خرسندی

نشانی نویسنده‌ی مسئول : ایران، تهران، دانشگاه صنعتی امیرکبیر(پلی تکنیک تهران)، دانشکده مهندسی برق، گروه قدرت

[Downloaded from ieijqp.ir on 2026-01-29]

فهرست علائم

g	ایندکس برای واحدهای تولید
i, j	ایندکس برای باس‌ها در شبکه
t	شاخص زمان
ε	مجموعه‌ی شاخه‌های انتقال در شبکه
N	مجموعه‌ی باس‌ها در شبکه
N_s / N_v	مجموعه‌ی باس‌ها با/بدون تقسیم بندی باس در شبکه
g / g_i	مجموعه‌ی واحدهای تولید در شبکه/متصل به باس i
M	عدد مثبت بزرگ
N^{BS}	حداکثر تعداد عملیات تقسیم بندی باس‌ها در شبکه
N^{TS}	حداکثر تعداد عملیات سوئیچینگ انتقال در شبکه
N^{NTO}	حداکثر تعداد عملیات BS و TS در شبکه
$p_g^{\max}$	حداکثر توان تولیدی توسط واحدهای تولید
$p_{i,j}^{\max}$	حداکثر توان مجاز عبوری از خطوط
$s_{g,t}$	وجود یا عدم وجود واحد تولیدی در شبکه
$s_{i,j,t}$	وجود یا عدم وجود خط انتقال در شبکه
$x_{i,j}$	راکتانس خطوط
$p_{i,t}$	مقدار بار موجود در هر باس در زمان t
$p_{g,t}$	توان اکتیو خروجی واحدهای تولید
$p_{g,t}^{\mathrm{I}} / p_{g,t}^{\mathrm{II}}$	توان خروجی واحدهای تولید متصل به باس I/II در BS
$p_{i,t}^{\mathrm{I}} / p_{i,t}^{\mathrm{II}}$	بار متصل شده به باس I/II در BS
$p_{i,j,t}$	توان عبوری از خطوط
$\omega_{g,t}$	اتصال واحد تولید به باس I/II در BS
$\omega_{i,t}^{D}$	اتصال بار به باس I/II در BS
$\omega_{i,j,t}^{Fr}$	اتصال خط انتقال به باس I/II در BS به باس i
$\omega_{i,j,t}^{To}$	اتصال خط انتقال به باس I/II در BS به باس j
$z_{i,t}$	تصمیم تقسیم بندی باس در باس i
$z_{i,j,t}$	پارامتری باینری که وضعیت سوئیچینگ انتقال در خطوط را مشخص می‌کند
$\delta_{i,t}$	بار حذف شده از باس i در زمان t
$\delta_{i,t}^{\mathrm{I}} / \delta_{i,t}^{\mathrm{II}}$	بار حذف شده از شین I/II از باس i در BS
$v_{i,t}$	زاویه ولتاژ در باس i در زمان t
$v_{i,t}^{\mathrm{I}} / v_{i,t}^{\mathrm{II}}$	زاویه ولتاژ در شین I/II از باس i در زمان t
$v_{i,j,t}^{Fr}$	زاویه ولتاژ شین I/II در عمل BS در باس i
$v_{i,j,t}^{To}$	زاویه ولتاژ شین I/II در عمل BS در باس j

[Downloaded from ieijqp.ir on 2026-01-29]

۱- مقدمه

انرژی الکتریکی یکی از مهمترین انرژی‌های مورد استفاده توسط انسان‌ها به منظور برآوردسازی نیازهای مختلف است. نقش انرژی الکتریکی در بخش‌های مختلف صنعتی،کشاورزی، تجاری و خانگی غیر قابل انکار است. دولت‌های مختلف حاکم بر کشورهای گوناگون، تأمین انرژی الکتریکی برای مصرف کنندگان مختلف را یکی از وظایف اصلی خود برمی‌شمارند، به طوری که انرژی الکتریکی علاوه بر ماهیت فنی، وجه سیاسی نیز پیدا کرده است. جوامع مدرن به طور گسترده‌ای وابسته به انرژی الکتریکی هستند. سیستم‌های قدرت به عنوان یکی از زیرساخت‌های حیاتی در جامعه‌ی مدرن، مسئول عرضه‌ی قابل اعتماد، امن و انعطاف‌پذیر برق به میلیاردها مشتری در سراسر جهان هستند. اختلالات در عملکرد عادی سیستم‌های قدرت می‌تواند تقریبا در هر صنعتی تاثیرات فراوانی را ایجاد کند. در سال‌های اخیر، سیستم‌های قدرت با خطرات رو به رشد و حوادث شدید مواجه هستند. این حوادث نه تنها بلایای طبیعی، بلکه حملات مخرب سایبری-فیزیکی توسط مهاجمان نیز می‌باشد. همچنین تقاضا برای انرژی الکتریکی با قابلیت اطمینان بالا روز به روز افزایش یافته است. این افزایش تقاضا، بهره-برداری از سیستم‌های قدرت را پیچیده‌تر کرده و احتمال روی دادن حملات در شبکه برق را افزایش داده است [۱].

در صورت رخ دادن خاموشی که به دنبال حملات موجود در شبکه پدید می‌آید جامعه انسانی با چالش‌هایی نظیر به خطر افتادن امنیت، سلامت و اقتصاد روبه‌رو می‌شود که پیامد چنین خاموشی‌هایی در طی سال‌ها نیز از بین نخواهد رفت. حتی تصور این که قطع جریان برق حتی برای چند ساعت می‌تواند چه صحنه‌های هولناکی را ایجاد کند غیرممکن است. بنابراین مقابله با این حملات به جهت هرچه کمتر کردن زمان خاموشی و احتمال رخداد آن‌ها نیازمند یک برنامه ریزی منسجم و دقیق می‌باشد.

می‌توان به منظور ارزیابی امنیت، حوادث را به چند دسته تقسیم‌بندی نمود و سپس به بحث در مورد امنیت در مقابل این حوادث پرداخت. حوادث و اغتشاشات که در مقابله با سیستم‌های قدرت احتمال وقوع آن‌ها وجود دارد به ۳ دسته تقسیم بندی می‌شوند که در ادامه بیان شده است.

دسته اول حوادثی هستند که اثرات آن‌ها زیاد نبوده و قابل برآورد هستند و همچنین احتمال وقوع مشخصی دارند این دستهٔ از حوادث را حوادث شناخته شده می‌نامند [۲].

دسته دوم حوادثی را شامل می‌شوند که بسیار کم اتفاق می‌افتند همچنین می‌توان عواقب وقوع چنین حوادثی را برآورد کرد، برای مثال در شهر تهران می‌توان وقوع یک زلزله را در نظر گرفت. با اینکه احتمال وقوع چنین حادثه‌هایی نامشخص است، اما به دلیل وجود چنین موردی در گذشته می‌توان عواقب و اثرات این حادثه را بر روی سیستم‌های قدرت تخمین زد چرا که موارد مشابهی در گذشته تجربه شده است. این دسته از حوادث را با نام‌های حوادث شناخته نشده یا قوی خاکستری یاد می‌کنند. همچنین این حوادث به حوادث با احتمال کم و اثر زیاد مشهور هستند [۳].

دسته سوم حوادثی هستند که به این دلیل که در گذشته حتی یک مورد از این حوادث رخ نداده است، عواقب و اثرات آن‌ها نامشخص است. بنابراین نمی‌توان در مورد احتمال وقوع آن‌ها صحبت کرد، اما می‌توان در مورد امکان وقوع چنین حوادثی صحبت کرد. به عنوان مثال، وقوع سونامی در شهر تهران اساساً از نظر فیزیکی غیرممکن است و لذا هرگز نباید مورد بحث قرار گیرد. شایان ذکر است که پس از وقوع حادثه‌هایی از این دسته، این حادثه از آن پس به دسته دوم منتقل می‌گردد، به این دسته از رخدادها، حوادث غیرقابل شناسایی یا قوی سیاه اطلاق می‌شود [۴].

حملات و خرابکاری‌های فیزیکی و سایبری نیز از جمله حوادث با اثر شدید و احتمال کم می‌باشند که در صورت وقوع می‌توانند خاموشی-های گسترده ای را رقم بزنند.

مقالات زیادی در زمینه حملات سایبری و فیزیکی منتشر شده است. این مقالات راهکارهای بسیاری برای مدل سازی حملات سایبری و فیزیکی و دفاع در برابر این حملات ارائه داده‌اند. که در ادامه به آن‌ها اشاره شده است.

اختلال در عملکرد عادی سیستم‌های قدرت می‌تواند تقریبا در هر صنعتی تاثیرات فراوانی را ایجاد کند و اثرات زیان بار مالی و امنیتی زیادی را به کل جامعه اعمال کند. در سال‌های اخیر، سیستم‌های قدرت با خطرات رو به رشد و حوادث شدید مواجه هستند. این خطرات نه تنها بلایای طبیعی، بلکه حملات مخرب توسط مهاجمان نیز می‌باشد [۵]. برای مثال می‌توان به حملات سایبری در شبکه برق اوکراین در سال های ۲۰۱۵ و ۲۰۱۶ اشاره کرد که با انجام این حملات، خسارات زیادی به شبکه قدرت وارد شده است [۶].

اطمینان از امنیت سیستم قدرت به عنوان یک مساله مهم و فوری هم برای دانشگاه و هم در صنعت برق در حال افزایش است. تقویت انعطاف پذیری سیستم‌های قدرت یک مساله بحرانی و مهم است تا بتوان به طور مؤثر و کارآمد خطرات مربوط به قابلیت اطمینان و امنیت شبکه‌ها را در مواجهه با حملات سایبری کاهش داد [۷]. تلاش‌های اخیر به طور فعال به تحقیق در مورد انعطاف پذیری سیستم قدرت تحت حملات شدید اختصاص داده شده است. مفاهیم اساسی، معیارها و اندازه‌گیری انعطاف پذیری سیستم قدرت در مرجع [۸] و [۹] معرفی شده است. در همین حال، یک استراتژی عملیاتی در مرجع [۱۰]

[Downloaded from ieijqp.ir on 2026-01-29]

پیشنهاد شده است تا انعطاف پذیری سیستم را تحت یک رویداد مرتبط با آب و هوا افزایش دهد. در مرجع [۱۱]، برای افزایش انعطاف پذیری شبکه برق یک مدل بهینه سازی مقاوم به منظور برنامه ریزی یکپارچه‌ی سیستم‌های انتقال برق و گاز طبیعی پیشنهاد شده است. علاوه بر این، در مرجع [۱۲] و [۱۳] به منظور افزایش انعطاف پذیری سیستم تحت وقایع شدید آب و هوایی، جزیره‌ای شدن سیستم‌های قدرت نیز مورد بررسی قرار گرفته و پیشنهاد شده است.

به تازگی، چندین مطالعه با تمرکز بر تاثیرات حملات سایبری- فیزیکی بر قابلیت اطمینان و امنیت سیستم قدرت انجام شده است. در مرجع [۱۴]، نویسندگان پیشنهاد می‌کنند پس از حملات سایبری-فیزیکی به شبکه‌ی برق، خرابی‌های خط با استفاده از رگرسیون بیزی تشخیص داده شود. یک چارچوب امنیتی سایبری-فیزیکی انعطاف پذیر در برابر حمله، در مرجع [۱۵] برای کاربردهای گسترده مانیتورینگ، حفاظت و کنترل در سیستم‌های برق پیشنهاد شده است.

در بسیاری از مقالات ارائه شده، بر حملات سایبری و فیزیکی و دفاع در مقابل این حملات در شبکه‌های قدرت پرداخته شده است. هر کدام از این مقالات روش‌های متفاوتی را برای انجام حملات سایبری و فیزیکی و دفاع در مقابل حملات ارائه داده‌اند. دراین مقاله این حملات بر شبکه‌های هوشمند بحث و بررسی شده است. همچنین به منظور ارتقا انعطاف پذیری سیستم قدرت در مقابل این حملات، روش بهینه سازی توپولوژی شبکه NTO به کار گرفته شده است. بهینه سازی توپولوژی شبکه نه تنها با انجام سوئیچینگ روی خطوط انتقال بلکه با تقسیم‌بندی باس‌ها، انعطاف پذیری سیستم قدرت را افزایش می‌دهد تا تأثیرات حملات سایبری-فیزیکی بر اجزای حیاتی شبکه برق شامل واحدهای تولید، پست‌های برق و خطوط انتقال را کاهش دهد.

۲- مدلسازی مسئله

حملات به دو دسته هدفمند و بی هدف دسته بندی می‌شوند. هر چه سیستم آسیب پذیرتر باشد حملات بی هدف خسارت‌های بیشتری به سیستم تحمیل می‌کند. اما در حملات هدفمند، با اهداف مشخص مانند جاسوسی، جنگ یا تروریسم قصد آسیب رساندن به یک سیستم ارتباطی خاص وجود دارد.

در یک تقسیم بندی دیگر حملات توسط دو دسته از افراد انجام می‌گیرد. اولین دسته افرادی هستند که به منظور استفاده بیشتر جهت مقاصد خود از شبکه سوء استفاده می‌کنند. معمولا این افراد با قصد صدمه و خرابی این حملات را انجام نمی‌دهند و تنها برای استفاده بیشتر و سریع‌تر خود از شبکه سوءاستفاده می‌کنند. دومین دسته افرادی هستند که جهت صدمه زدن به شبکه بدون مقاصد فردی به شبکه حمله می‌کنند. اما اگر بخواهیم تعریف ساده و در عین حال دقیقی از حملات سایبری داشته باشیم می‌توان گفت حملات سایبری حملاتی هستند، که به زیر ساخت های مخابراتی و سیستم‌های هوشمند موجود در شبکه قدرت انجام می‌گیرد. این نوع حملات اغلب غیرقابل آشکارسازی هستند

۲-۱- دفاع در برابر حملات هماهنگ سایبری

درک روشنی از وضعیت امنیتی شبکه بسیار مهم است و آ سیب‌پذیری بیش از حد، می‌تواند باعث خاموش شدن تجهیزات و یا از بین ر فتن آن‌ها شود، بنابراین لازم است تمهیدات امنیتی جهت مقابله با حملات سایبری در نظر گرفت. در این مقاله به منظور کاهش بی شتر تأثیرات حملات هماهنگ سایبری، یک مدل مبتنی بر NTO پی شنهاد شده است که انعطاف پذیری سی ستم را با دو روش سوئیچینگ انت قال و تقسیم بندی باس افزایش می‌دهد. که فرمول بندی آن به شرح ز یر است:

$$\min \sum_{i\in N_v} \delta_{i,t} + \sum_{i\in N_s} \delta^{I}_{i,t} + \delta^{II}_{i,t} \quad (۱)$$

$$-M(S_{i,j,t} + Z_{i,j,t}) \le \frac{V^{Fr}_{i,j,t} - V^{To}_{i,j,t}}{X_{i,j}} - P_{i,j,t} \quad (۲)$$

$$\frac{V^{Fr}_{i,j,t} - V^{To}_{i,j,t}}{X_{i,j}} - P_{i,j,t} \le M(S_{i,j,t} + Z_{i,j,t}) \quad (۳)$$

$$-P^{max}_{i,j}(1 - S_{i,j,t}) \le P_{i,j,t} \le P^{max}_{i,j}(1 - S_{i,j,t}) \quad (۴)$$

$$-P^{max}_{i,j}(1 - Z_{i,j,t}) \le P_{i,j,t} \le P^{max}_{i,j}(1 - Z_{i,j,t}) \quad (۵)$$

$$V^{Fr}_{i,j,t} = V_{i,t} \quad (۶)$$

$$V^{To}_{i,j,t} = V_{j,t} \quad (۷)$$

$$-M\omega^{Fr}_{i,j,t} \le V^{Fr}_{i,j,t} - V^{I}_{i,t} \le M\omega^{Fr}_{i,j,t} \quad (۸)$$

$$-M(1 - \omega^{Fr}_{i,j,t}) \le V^{Fr}_{i,j,t} - V^{II}_{i,t} \le M(1 - \omega^{Fr}_{i,j,t}) \quad (۹)$$

$$-M\omega^{To}_{i,j,t} \le V^{To}_{i,j,t} - V^{I}_{j,t} \le M\omega^{To}_{i,j,t} \quad (۱۰)$$

$$-M(1 - \omega^{To}_{i,j,t}) \le V^{To}_{i,j,t} - V^{II}_{j,t} \le M(1 - \omega^{To}_{i,j,t}) \quad (۱۱)$$

$$\sum_{g\in G_i} P_{g,t} - (P_{i,t} - \delta_{i,t}) - \sum_{j\in N} P_{i,j,t} = 0 \quad (۲۲)$$

$$\sum_{g\in G_i} P^{I}_{g,t} - (P^{I}_{i,t} - \delta^{I}_{i,t}) - \sum_{j\in N} P^{I}_{i,j,t} = 0 \quad (۱۳)$$

$$\sum_{g\in G_i} P^{II}_{g,t} - (P^{II}_{i,t} - \delta^{II}_{i,t}) - \sum_{j\in N} P^{II}_{i,j,t} = 0 \quad (۱۴)$$

$$0 \le P_{g,t} \le P^{max}_{g}(1 - S_{g,t}) \quad (۱۵)$$

$$0 \le P^{I}_{g,t} \le P^{max}_{g}(1 - S_{g,t}) \quad (۱۶)$$

$$0 \le P^{II}_{g,t} \le P^{max}_{g}(1 - S_{g,t}) \quad (۱۷)$$

$$0 \le \delta_{i,t} \le P_{i,t} \quad (۱۸)$$

$$0 \le \delta^{I}_{i,t} \le P^{I}_{i,t} \quad (۱۹)$$

$$0 \le \delta^{II}_{i,t} \le P^{II}_{i,t} \quad (۲۰)$$

$$P^{I}_{i,t} = P_{i,t}(1 - \omega^{D}_{i,t}) \quad (۲۱)$$

$$P^{II}_{i,t} = P_{i,t}\omega^{D}_{i,t} \quad (۲۲)$$

[Downloaded from ieijqp.ir on 2026-01-29]

$$0 \le P_{g,t}^{\mathrm{I}} \le P_g^{max}(1-\omega_{g,t}) \quad (۲۳)$$

$$0 \le P_{g,t}^{\mathrm{II}} \le P_g^{max}\omega_{g,t} \quad (۲۴)$$

$$-(1-\omega_{i,j,t}^{Fr})P_{i,j}^{max} \le P_{i,j,t}^{\mathrm{I}} \le (1-\omega_{i,j,t}^{Fr})P_{i,j}^{max} \quad (۲۵)$$

$$-\omega_{i,j,t}^{Fr}P_{i,j}^{max} \le P_{i,j,t}^{\mathrm{II}} \le \omega_{i,j,t}^{Fr}P_{i,j}^{max} \quad (۲۶)$$

$$-(1-\omega_{i,j,t}^{To})P_{i,j}^{max} \le P_{i,j,t}^{\mathrm{I}} \le (1-\omega_{i,j,t}^{To})P_{i,j}^{max} \quad (۲۷)$$

$$-\omega_{i,j,t}^{To}P_{i,j}^{max} \le P_{i,j,t}^{\mathrm{II}} \le \omega_{i,j,t}^{To}P_{i,j}^{max} \quad (۲۸)$$

$$\mathrm{P_{i,j,t}} = P_{i,j,t}^{\mathrm{I}} + P_{i,j,t}^{\mathrm{II}} \quad (۲۹)$$

$$\mathrm{P_{i,j,t}} = -(P_{j,i,t}^{\mathrm{I}} + P_{j,i,t}^{\mathrm{II}}) \quad (۳۰)$$

$$-MZ_{i,t} \le V_{i,t}^{\mathrm{I}} - V_{i,t}^{\mathrm{II}} \le MZ_{i,t} \quad (۳۱)$$

$$\omega_{i,j,t}^{Fr} \le Z_{i,t} \quad (۳۲)$$

$$\omega_{i,j,t}^{To} \le Z_{j,t} \quad (۳۳)$$

$$\omega_{g,t} \le Z_{i,t} \quad (۳۴)$$

$$\omega_{i,t}^{D} \le Z_{i,t} \quad (۳۵)$$

$$\sum_{\mathrm{i}\in \mathrm{N_s}} Z_{i,t} \le N^{BS} \quad (۳۶)$$

$$\sum_{(\mathrm{i,j})\in\varepsilon} Z_{i,j,t} \le N^{TS} \quad (۳۷)$$

$$\sum_{\mathrm{i}\in \mathrm{N_s}} Z_{i,t} + \sum_{(\mathrm{i,j})\in\varepsilon} Z_{i,j,t} = N^{NTO} \quad (۳۸)$$

که معادله (۱) بیانگر تابع هدف می‌باشد. هدف اپراتور سیستم این است که قطعی کل بار در شبکه را به حداقل برساند. اولین بخش در معادله‌ی (۱) قطع بار در باس‌ها بدون اقدامات BS است و بخش دوم بار قطع شده با اقدامات BS است.

معادلات (۲) و (۳) و (۴) قیود پخش بار بوده، که در آن $Z_{i,j,t}$، تصمیم TS شاخه‌ی انتقال بین باس i و باس j در زمان t است که اگر خط انتقال در مدار نباشد یک است و در غیر این صورت، برابر صفر است.

همچنین قیود (۵) تا (۱۰) اطمینان حاصل می‌کند که زاویه‌ی ولتاژ در هر دو شاخه ی انتقال، با باس یا شینی که به آن متصل است برابر است. $\omega_{i,j,t}^{Fr}$ و $\omega_{i,j,t}^{To}$ باس‌هایی را نشان می‌دهد که شاخه‌ی انتقال به آن‌ها متصل است. هنگامی که $\omega_{i,j,t}^{Fr}$ و یا $\omega_{i,j,t}^{To}$ برابر با صفر هستند به این معنی است که شاخه‌ی انتقال به ترتیب به باس ۱ در اقدام BS متصل است. و هنگامی که مقدار آن‌ها برابر با یک است یعنی شاخه ی انتقال به باس II متصل است.

قید (۱۱) تعادل توان را در باس‌های بدون اقدامات BS را حفظ می‌کند، در حالی که قیدهای (۱۲) و (۱۳) تعادل توان در شین های I و II از باس‌های با اقدامات BS در شبکه را بیان می‌کند.

معادلات (۱۴) تا (۱۶) بیانگر محدودیت‌های توانی واحدهای تولید بر اساس وضعیت آن‌ها در شبکه است.

قیود (۱۷) تا (۱۹) مربوط به عدم تجاوز بار حذف شده از هر باس از مقدار بار موجود در هر باس می‌باشد. همچنین قیود (۲۰) و (۲۱) نشان دهنده وضعیت اتصال بار در اقدامات BS می‌باشد که در آن $\omega_{i,t}^{D}$ نشان دهنده‌ی باسی است که بار به آن متصل است. هنگامی که $\omega_{i,t}^{D}=0$، به این معنی است که بار به شین I متصل است و هنگامی که برابر با یک است، به این معنی است که بار به شین II متصل است.

قیدهای (۲۲) و (۲۳)، قیدهای خروجی واحدهای تولید با توجه به اقدامات BS است. که در آن $\omega_{g,t}$ نشان دهنده‌ی باسی است که واحد تولید g در اقدام BS، به آن متصل است، هنگامی که $\omega_{g,t}=0$ است یعنی واحد تولید g به شین I متصل است و هنگامی که برابر با یک است، به این معنی است که واحد تولید g به شین II متصل است.

قیود (۲۴) تا (۲۹) مربوط به قیود پخش بار با اقدامات BS است. قیود (۳۰) به این معنی است که اگر هیچ اقدام BS در پست برق وجود نداشته باشد زاویه‌ی ولتاژ دو باس در یک پست برق باید یکسان باشد،که در آن $Z_{i,t}$ نشان دهنده اقدام BS در شین I است. هنگامی که $Z_{i,t}=1$، به این معنی است که یک اقدام BS در باس وجود دارد. در غیر این صورت $Z_{i,t}=0$ می‌باشد.

قیدهای (۳۱) تا (۳۵) بیانگر این است که هنگامی که یک اقدام BS در باس مربوطه انجام می‌شود، شاخه‌های انتقال، واحدهای تولید و بار در یک باس، تنها می‌توانند به دو شین مستقل متصل شوند. در عمل، حداکثر تعداد اقدامات NTO که می‌توان روی شبکه اعمال نمود محدود است. بنابراین، محدودیت های این نوع اقدامات به صورت معادلات (۳۶) تا (۳۸) بیان شده است.

۲-۲- شاخص تاب‌آوری

به منظور ارزیابی عملکرد سیستم قدرت در افزایش تاب آوری شبکه در برابر حملات مخرب سایبری-فیزیکی، سطح انعطاف پذیری سیستم قدرت باید به طور کمی ارزیابی شود. برای مشخص نمودن میزان تاب آوری یک شبکه باید یک معیار مشخص جهت ارزیابی تاب آوری تعریف نمود. در این مساله، به این دلیل که در تابع هدف از بار حذف شده استفاده شده است، بنابراین از بار حذف شده هم برای محاسبه شاخص تاب آوری استفاده می‌شود که معادله آن در (۳۹) بیان شده است.

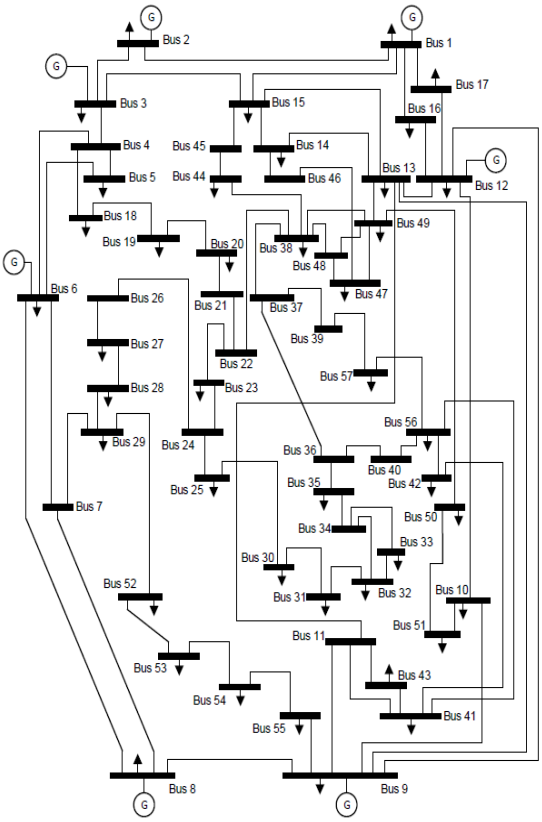
$$R = \frac{\sum_{\mathrm{i}\in\mathrm{N}}(P_{i,t}-\delta_{\mathrm{i,t}})}{\sum_{\mathrm{i}\in\mathrm{N}} P_{i,t}} \quad (۳۹)$$

شاخص تاب آوری عددی بین صفر و یک است. هر چه مقدار این عدد به یک نزدیک‌تر باشد، به این معنی است که بار کمتری قطع شده است و سیستم تاب آوری زیادی دارد. اما هر چه این عدد به صفر نزدیک شود، میزان تاب آوری سیستم کمتر خواهد بود.

[Downloaded from ieijqp.ir on 2026-01-29]

۳- شبیه‌سازی و تحلیل نتایج

برای بررسی حملات سایبری-فیزیکی همان طور که در شکل (۱) مشاهده می‌شود شبکه ۵۷ باس IEEE جهت آزمایش استفاده شده است. این شبکه دارای ۵۷ باس و ۷ واحد تولید می‌باشد. مجموع توان تولیدی واحدها برابر ۱۲۷۹/۳ است. شبکه ۵۷ باس IEEE دارای ۸۰ خط انتقال است که بارهای مصرفی و نیروگاه‌ها را به یکدیگر متصل کرده است. کل بار موجود در این شبکه برابر ۱۲۵۰/۸ مگاوات است.



شکل (۱) شبکه ۵۷ باس IEEE

۳-۱- حالت اول: بهره‌برداری در شرایط عادی

در این حالت فرض شده است که شبکه در حالت عادی بهره برداری می‌شود و اتفاقی یا حمله‌ای در شبکه حادث نشده است. این حالت به منظور ارزیابی سایر حالت‌های اتفاق افتاده برای سیستم تعریف می‌شود. در این حالت، هیچ‌گونه قطع باری در سیستم رخ نداده است و چون سیستم هم در شرایط بهره‌برداری عادی قرار دارد، چیزی بیشتر از این انتظار نمیرفت. همچنین به دلیل این که هیچ‌گونه قطع باری در شبکه در چنین شرایطی رخ نداده است، بنابراین میزان انعطاف‌پذیری ۱۰۰ درصد بوده و سیستم در حالت ایده‌آل است.

۳-۲- حالت دوم: بهره‌برداری بعد از وقوع حملات سایبری

در این حالت چنین فرض شده که حمله کننده فقط قادر به انجام حملات سایبری بوده و همچنین فرض بعدی بر این است که حمله کننده یک حمله سایبری به ژنراتور انجام داده و همچنین یک حمله سایبری به یک باس متصل به ژنراتور انجام داده است که در حالت دوم نیز با حمله به یک باس متصل به یک ژنراتور، ژنراتور متصل به آن باس از مدار خارج می‌شود. بنابراین حملات فقط به ژنراتور ها انجام شده و باعث خروج واحدهای تولیدی از شبکه شده است. همچنین لازم به ذکر است این حملات تصادفی می‌باشد. برای ارزیابی حملات تعداد ۲۰ حمله سایبری تصادفی انجام شده است که نتایج آن در جدول (۱) نشان داده شده است.

جدول (۱) نتایج حملات سایبری

ردیف	اعداد تصادفی در حمله سایبری	بار حذف شده بر حسب مگاوات
۱	ژنراتور ۲ و ۶	۱۱
۲	ژنراتور ۴ و ۶	۲۴
۳	ژنراتور ۶ و ۷	۳۳۴
۴	ژنراتور ۱ و ۶	۱۷۴
۵	ژنراتور ۵ و ۶	۲۲۱
۶	ژنراتور ۳ و ۴	۵
۷	ژنراتور ۳ و ۶	۴۳
۸	ژنراتور ۱ و ۷	۴۳۰
۹	ژنراتور ۱ و ۲	۱۲۸
۱۰	ژنراتور ۱ و ۳	۱۴۵
۱۱	ژنراتور ۲ و ۷	۲۳۹
۱۲	ژنراتور ۳ و ۵	۲۴۱
۱۳	ژنراتور ۲ و ۵	۱۶۸
۱۴	ژنراتور ۵ و ۷	۴۷۸
۱۵	ژنراتور ۴ و ۵	۱۹۸
۱۶	ژنراتور ۱ و ۵	۴۰۰
۱۷	ژنراتور ۴ و ۷	۲۵۲
۱۸	ژنراتور ۳ و ۵	۲۴۱
۱۹	ژنراتور ۱ و ۴	۱۰۵
۲۰	ژنراتور ۴ و ۷	۲۵۳

[Downloaded from ieijqp.ir on 2026-01-29]

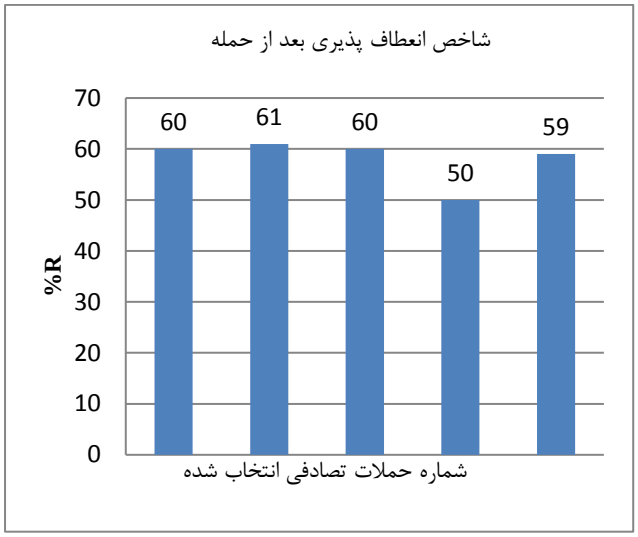
به منظور نشان دادن عملکرد مدل پیشنهادی بخش قبل برای افزایش انعطاف پذیری سیستم‌های قدرت در برابر حملات سایبری، دفاع روی سیستم ۵۷ باسه انجام شد. در این حالت با تغییر در توپولوژی شبکه شامل TS و BS به دفاع در مقابل حملات با بار حذف شده پرداخته شده است. نتایج شبیه‌سازی در جدول (۲) نشان داده شده است. نتایج نشان می‌دهد که با تغییر در توپولوژی شبکه، بار حذف شده کاهش مطلوبی داشته و میزان انعطاف‌پذیری شبکه افزایش خواهد داشت که نشان از مناسب بودن مدل پیشنهادی می‌باشد.

جدول (۲) دفاع در برابر حملات سایبری

ردیف	بار حذف شده پس از دفاع	بار حذف شده قبل از دفاع
۱	۰	۱۱
۲	۰	۲۴
۳	۳۰۸	۳۳۴
۴	۱۵۷	۱۷۴
۵	۱۹۸	۲۲۱
۶	۰	۵
۷	۰	۴۳
۸	۳۹۹	۴۳۰
۹	۹۶	۱۲۸
۱۰	۱۰۱	۱۴۵
۱۱	۱۹۶	۲۳۹
۱۲	۱۹۹	۲۴۱
۱۳	۱۳۷	۱۶۸
۱۴	۳۹۶	۴۷۸
۱۵	۱۴۸	۱۹۸
۱۶	۳۲۷	۴۰۰
۱۷	۲۰۱	۲۵۲
۱۸	۱۹۵	۲۴۱
۱۹	۸۱	۱۰۵
۲۰	۲۳۳	۲۵۳

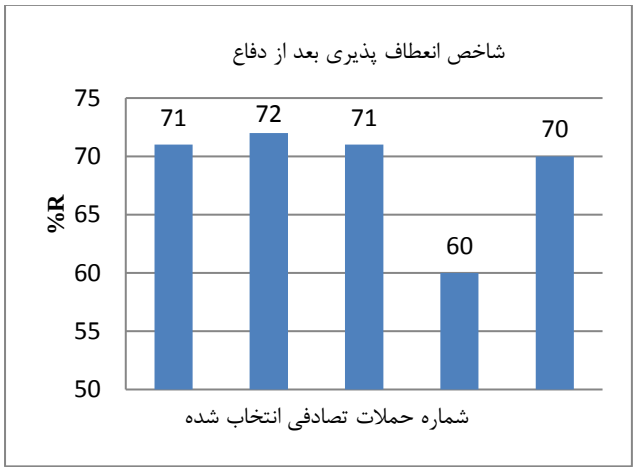
همانطور که از نتایج جدول مشخص است مقدار بار حذف شده بسیار متغیر بوده و در حملاتی که به ژنراتور های ۱ یا ۵ یا ۷ حمله شده مقدار بار حذف شده زیاد می‌باشد. علت این امر مقدار توان تولیدی بالای این واحدها است.

برای بررسی انعطاف‌پذیری از بین حملات تصادفی انجام شده تعداد پنج حمله که بیشترین مقدار بار حذف شده را داشتند انتخاب کرده و شاخص انعطاف پذیری شبکه بعد از حملات برای هر یک حساب شده است که نتایج آن در شکل (۲) آورده شده است.



شکل (۲) نمودار شاخص انعطاف پذیری بعد از حملات

شکل (۲) نشان می‌دهد که انعطاف‌پذیری کاهش زیادی داشته است. همچنین برای بررسی روش پیشنهادی شاخص انعطاف پذیری بعد از دفاع در برابر حملات نیز محاسبه شده است. در شکل (۳) مشاهده می‌شود که بعد از دفاع شاخص انعطاف پذیری افزایش مناسبی داشته است و باعث افزایش انعطاف پذیری شبکه شده است.



شکل (۳) نمودار شاخص انعطاف پذیری بعد از دفاع

[Downloaded from ieijqp.ir on 2026-01-29]

۴- نتیجه گیری

در این مقاله یک استراتژی برای مقابله با حملات هماهنگ سایبری بیان شد به منظور افزایش انعطاف پذیری سیستم قدرت، یک مدل بهینه‌سازی توپولوژی شبکه برای کاهش تاثیرات حملات هماهنگ سایبری به شبکه پیشنهاد شد. نتایج حاصل از مسئله بر روی سیستم اصلاح شده ۵۷ باسه IEEE شبیه سازی شد که برای به حداقل رساندن بار قطع شده می‌توان با کلیدزنی و انجام عمل تقسیم بندی بار قطع شده را کاملا قطع کرده یا به طور زیادی کاهش داد.

مراجع

[1] Papic, M., Ekisheva, S. and Cotilla-Sanchez, E., 2020. A risk-based approach to assess the operational resilience of transmission grids. *Applied Sciences*, *10*(14), p.4761.

[2] Billinton, R., 1970. *Power system reliability evaluation*. Taylor & Francis.

[3] Zadeh, L.A., 1978. Fuzzy sets as a basis for a theory of possibility. *Fuzzy sets and systems*, *1*(1), pp.3-28.

[4] Gholami, A., Aminifar, F. and Shahidehpour, M., 2016. Front lines against the darkness: Enhancing the resilience of the electricity grid through microgrid facilities. *IEEE Electrification Magazine*, *4*(1), pp.18-24.

[5] Liu, Z. and Wang, L., 2020. Leveraging network topology optimization to strengthen power grid resilience against cyber-physical attacks. *IEEE Transactions on Smart Grid*, *12*(2), pp.1552-1564.

[6] Kshetri, N. and Voas, J., 2017. Hacking power grids: A current problem. *Computer*, *50*(12), pp.91-95.

[7] Golan, M.S. and Mohammadi, J., 2022, October. Mapping Disruption Sources in the Power Grid and Implications for Resilience. In *2022 North American Power Symposium (NAPS)* (pp. 1-6). IEEE.

[8] Panteli, M., Trakas, D.N., Mancarella, P. and Hatziargyriou, N.D., 2017. Power systems resilience assessment: Hardening and smart operational enhancement strategies. *Proceedings of the IEEE*, *105*(7), pp.1202-1213.

[9] Panteli, M., Mancarella, P., Trakas, D.N., Kyriakides, E. and Hatziargyriou, N.D., 2017. Metrics and quantification of operational and infrastructure resilience in power systems. *IEEE Transactions on Power Systems*, *32*(6), pp.4732-4742.

[10] Wang, C., Hou, Y., Qiu, F., Lei, S. and Liu, K., 2016. Resilience enhancement with sequentially proactive operation strategies. *IEEE Transactions on Power Systems*, *32*(4), pp.2847-2857.

[11] Shao, C., Shahidehpour, M., Wang, X., Wang, X. and Wang, B., 2017. Integrated planning of electricity and natural gas transportation systems for enhancing the power grid resilience. *IEEE Transactions on Power Systems*, *32*(6), pp.4418-4429.

[12] Panteli, M., Trakas, D.N., Mancarella, P. and Hatziargyriou, N.D., 2016. Boosting the power grid resilience to extreme weather events using defensive islanding. *IEEE Transactions on Smart Grid*, *7*(6), pp.2913-2922.

[13] Bie, Z., Lin, Y., Li, G. and Li, F., 2017. Battling the extreme: A study on the power system resilience. *Proceedings of the IEEE*, *105*(7), pp.1253-1266.

[14] Soltan, S., Mittal, P. and Poor, H.V., 2019. Line failure detection after a cyber-physical attack on the grid using Bayesian regression. *IEEE Transactions on Power Systems*, *34*(5), pp.3758-3768.

[15] Ashok, A., Govindarasu, M. and Wang, J., 2017. Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid. *Proceedings of the IEEE*, *105*(7), pp.1389-1407.

[16] Liu, Z. and Wang, L., 2020. Leveraging network topology optimization to strengthen power grid resilience against cyber-physical attacks. *IEEE Transactions on Smart Grid*, *12*(2), pp.1552-1564.

[Downloaded from ieijqp.ir on 2026-01-29]