تأثیرات توپولوژی شبکه سایبری بر روی قابلیت اطمینان شبکه هوشمند با درنظرگیری ارتباط مستقیم شبکه سایبر- قدرت

امیررضا حسنی آهنگر[۱]، دانشجوی دکتری؛ گئورگ قره پتیان[۲]، استاد؛ علی اصغر خدادوست آرانی[۳]، دانشجوی دکتری؛ حسین عسکریان ابیانه[۴]، استاد

۱ - دانشکده مهندسی برق- دانشگاه صنعتی امیرکبیر- تهران- ایران- hassaniahangar@aut.ac.ir

۲ - دانشکده مهندسی برق- دانشگاه صنعتی امیرکبیر- تهران- ایران- grptian@aut.ac.ir

۳ - دانشکده مهندسی برق- دانشگاه صنعتی امیرکبیر- تهران- ایران- a.a.khodadoost@aut.ac.ir

۴ - دانشکده مهندسی برق- دانشگاه صنعتی امیرکبیر- تهران- ایران- askarian@aut.ac.ir

چکیده: با توجه به اشتیاق روزافزون به استفاده از شبکه‌های هوشمند و ماهیت آن که با عدم قطعیت بالای پارامترهای این نوع شبکه‌های الکتریکی همراه است، ارزیابی قابلیت اطمینان این سیستم‌ها ضروری بوده و بسیار مورد توجه است. استفاده از زیرساخت‌های مخابراتی و فناوری اطلاعات در شبکه‌های هوشمند توزیع انرژی الکتریکی سبب شده است تا سیستمی متشکل از شبکه قدرت و شبکه سایبری (شبکه‌های کنترل، پایش و حفاظت) ایجاد شود. از آن‌جایی که سیستم‌های سایبری می‌توانند دچار خطاهایی بشوند، ضروری است برای ارزیابی شاخص‌های قابلیت اطمینان شبکه‌های هوشمند از روش‌هایی استفاده شود که دربرگیرنده عملکرد مناسب هر دو سیستم سایبری و قدرت باشد. در این مقاله، روش پیشنهادی ارزیابی قابلیت اطمینان بر روی شبکه‌ی نمونه و واقعی پیاده‌سازی می‌شود و اهمیت درنظرگیری خطاهای مستقیم شبکه سایبری بر روی قابلیت اطمینان سیستم مورد مطالعه قرار می‌گیرد. همچنین تغییر توپولوژی شبکه سایبری به‌عنوان راه‌کار اصلی مورد بحث در این مقاله به عنوان راه‌حلی مناسب برای بهبود قابلیت اطمینان ارائه شده است. روش پیشنهادی بر روی قسمتی از شبکه توزیع هرمزگان (فیدر آیسین) شبیه‌سازی شده است. در انتها نیز بهینه‌سازی توپولوژی شبکه سایبری نیز با درنظرگیری قیود مربوطه با استفاده از روش‌های بهینه‌سازی هوشمند جهت بهبود قابلیت اطمینان سیستم انجام شده است.

واژه‌های کلیدی: قابلیت اطمینان- شبکه هوشمند- بهینه‌سازی- توپولوژی شبکه- ارتباط شبکه سایبری و قدرت- منابع تولید پراکنده

Cyber Topologies Impacts on Smart Grid Reliability Considering Direct Cyber-Power Interdependency

Amirreza Hassani Ahangar[1], PhD student; G.B. Gharhepetian[2], Professor; Ali Asghar Khodadust Arani[3], PhD student; Hossein Askarian Abyaneh[4], Professor

1- Faculty of Electrical Engineering, Amirkabir University of Technology, Tehran, Iran, Email: amirrezahassani93@gmail.com
2- Faculty of Electrical Engineering, Amirkabir University of Technology, Tehran, Iran, Email: grptian@aut.ac.ir
3- Faculty of Electrical Engineering, Amirkabir University of Technology, Tehran, Iran, Email: a.a.khodadoost@aut.ac.ir
4- Faculty of Electrical Engineering, Amirkabir University of Technology, Tehran, Iran, Email: askarian@aut.ac.ir

Abstract: Due to the rising interest of using smart grids and its unreliable nature, the reliability analysis is highly regarded. The application of communication infrastructures and information technology in smart grids has created a system consisting power and cyber networks (control, monitoring, and protection networks). Due to the fact that cyber networks are prone to failure, using methods that cover the proper operation of both cyber and power networks together are essential for assessing reliability indices of smart grids. The importance of considering direct cyber network failures on reliability assessment is also studied. Cyber network topology transition is the main solution for the improvement of reliability assessment that is discussed in this paper. The method is simulated on an actual distribution network of Hormozgan Regional Electrical Company (HREC) of Iran. By calculating the reliability indices, the results clarify that smart grid reliability assessment will not be improved without considering an optimal cyber network topology. So, optimization techniques are used for improving reliability assessment, with the consideration of the constraints.

Keywords: Reliability, smart grid, optimization, network topology, cyber-power interdependency, distributed generation (DG).

ارسال مقاله: ۱۳۹۵/۰۸/۳۰

تاریخ اصلاح مقاله: ۱۳۹۵/۱۱/۱۴

تاریخ پذیرش مقاله: ۱۴/ ۱۳۹۶/۰۴

نام نویسنده مسئول: گئورگ قره پتیان

نشانی نویسنده مسئول: ایران - تهران – خیابان حافظ – پلاک ۴۲۴- دانشگاه صنعتی امیرکبیر-دانشکده مهندسی برق

۱- مقدمه

خاموشی‌ها و بروز قطعی‌های گسترده در شبکه قدرت نشان می‌دهد که بروز خطا در عملکرد سیستم‌های کنترل و پایش تأثیر بسیار مهم و نقش به‌سزایی در این نوع اتفاقات داشته است [۱]. در واقعیت برخی مواقع به‌خاطر محدودیت در دسترسی به اطلاعات مرکز پایش و یا کنترل، رویدادهای نامطلوبی در سراسر شبکه پخش می‌شود.

در بررسی‌های قابلیت اطمینان سیستم‌های قدرت و تحلیل ریسک، تعداد کمی از مراجع به تاثیرات سیستم پایش و کنترل پرداخته‌اند. در مرجع [۲] قابلیت اطمینان و نرخ بروز خطا و عدم عملکرد صحیح سیستم کنترل مورد بررسی قرار گرفته است. اما اثرات عدم عملکرد صحیح سیستم کنترل بر روی سیستم قدرت تجزیه و تحلیل نشده است. از مراجعی که کنترل‌پذیری سیستم را با درنظرگیری نرخ بروز خطا و خرابی‌های سیستم (SCADA[۱]) مورد بررسی قرار داده است می‌توان به مرجع [۳] اشاره نمود.

در کنار تمام مزایای سیستم‌های هوشمند، به‌دلیل افزایش کاربردهای شبکه‌های سایبری نرخ بروز خطای سیستم قدرت افزایش می‌یابد. در چنین صورتی هوشمندسازی با استقرار سیستم در حالت بهره‌برداری عادی مخالفت نموده و عامل تهدید کننده به حساب می‌آید [۴، ۵].

دسته‌ای از خطاها که در شبکه‌های سایبری اتفاق می‌افتد پنهان بوده و تنها زمانی آشکار می‌شوند که یک عملکرد ناصحیح در سیستم سایبری-قدرت رخ می‌دهد. علاوه بر این موضوع، رفتارها و پارامترهایی که منجر به خطا و عملکرد ناصحیح اجزای شبکه سایبری می‌شوند بسیار پیچیده می‌باشند [۶].

عدم قطعیت، غیرقابل اطمینان بودن و غیرقابل پیش‌بینی بودن شبکه‌های سایبری به‌صورت نه‌چندان مناسبی بر شبکه‌های قدرت هوشمند تأثیر می‌گذارند. ساختار و طبیعت روش‌هایی که برای قابلیت اطمینان و یا مدیریت ریسک سیستم‌های قدرت متداول استفاده می‌شوند مانند آن‌چه در مرجع [۷] توضیح داده شده است، برای مدیریت و ارزیابی ریسک شبکه‌های قدرت و سایبری وابسته به یکدیگر[۲] کاربردی و قابل اعمال نمی‌باشد [۴، ۵].

تحقیقاتی در زمینه ارزیابی قابلیت اطمینان سیستم قدرت هوشمند، بررسی ارتباط شبکه سایبری و شبکه قدرت و هم‌چنین روش‌های بهبود قابلیت اطمینان شبکه هوشمند در مقالات دیگر ارائه شده است. ولی کارهای صورت پذیرفته از نقطه نظر موارد زیر دارای نواقصی می‌باشند.

۱- درنظرگیری منابع تولید پراکنده با ظرفیت ثابت تولید و لحاظ ننمودن عدم قطعیت منابعی مانند باد و خورشید. مراجعی مانند [۸، ۹] علی رغم تحلیل قابلیت اطمینان سیستم قدرت هوشمند تنها منابع تولید پراکنده‌ای با ظرفیت تولید ثابت را درنظرگرفته‌اند که با واقعیت فاصله دارد.

۲- وارد نکردن شبکه سایبری و خرابی‌های مربوط به تجهیزات آن در محاسبات مربوط به ارزیابی قابلیت اطمینان شبکه هوشمند. منابعی مانند [۱۲، ۱۳] موضوعاتی مانند عدم قطعیت و ماهیت تصادفی و آماری منابع تولید پراکنده تجدیدپذیر در سناریوهای مختلف و تکنولوژی‌های مختلف منابع تولید مانند انرژی‌های خورشیدی و بادی و ... مورد بررسی قرار گرفته است. اما ماهیت اتفاقی شبکه هوشمند با تمرکز بر آسیب‌پذیری شبکه سایبری مورد بحث واقع نشده است.

۳- ارائه روش بهبود قابلیت اطمینان جدید بر مبنای تغییر آرایش توپولوژی شبکه سایبری و تأثیر آن بر روی شبکه قدرت. در مراجعی مانند [۱۵- ۱۳] راه‌کارهای مرسوم و مبتنی بر شبکه قدرت بررسی شده است. در مرجع [۱۳] بهبود قابلیت اطمینان شبکه‌های توزیع انرژی الکتریکی با استفاده از انتخاب طرح حفاظتی و جایابی مناسب تجهیزات حفاظتی پرداخته شده است. یکی از راه‌کارهای دیگر برای مدیریت ریسک شبکه‌های توزیع، کنترل و کاهش نرخ خطاهای خطوط توزیع می‌باشد. در مقاله [۱۴]، ارائه راه‌کارهای کاهش نرخ بروز خطا با توجه به شاخص‌های اقتصادی و هزینه‌ای تعریف گردیده است. در مرجع [۱۵] با استفاده از جایابی بهینه منابع تولید پراکنده به بهبود قابلیت اطمینان شبکه هوشمند اشاره نموده است.

۴- لحاظ نکردن مدل بار مصرفی به صورت منحنی بار ساعتی روزانه، هفتگی و یا سالانه در تمامی مراجع ذکر شده در این بخش.

بر اساس آن‌چه در مورد ارتباط‌های شبکه سایبری (حفاظت، کنترل، پایش و مخابراتی) با شبکه قدرت بیان گردید، می‌توان اذعان داشت که یکی از عوامل تاثیرگذار در شبکه‌های هوشمند، شبکه سایبری و خرابی و خطاهای احتمالی آن است [۱۶]. در ضمن توپولوژی شبکه سایبری نیز مشابه توپولوژی شبکه قدرت می‌تواند وضعیت قابلیت اطمینان و ریسک سیستم را تحت تأثیر قرار دهد. از این‌رو یکی از روش‌های پیشنهادی برای مدیریت ریسک شبکه‌های هوشمند، بررسی آرایش‌های مختلف و بهینه شبکه‌های سایبری می‌باشد.

با توجه به توضیحات ارائه شده در مقدمه، نوآوری‌های این مقاله را می‌توان در موارد زیر خلاصه نمود:

۱- ارائه روش تحلیلی ارزیابی قابلیت اطمینان شبکه هوشمند با درنظرگیری ارتباط مستقیم شبکه سایبری و شبکه قدرت

۲- درنظرگیری منابع تولید پراکنده تجدیدپذیر مانند انرژی باد با منظور نمودن عدم قطعیت آن.

۳- بهبود قابلیت اطمینان شبکه هوشمند با استفاده از راه‌کار بررسی توپولوژی‌های مختلف شبکه سایبری و یافتن توپولوژی بهینه تحت شرایط خاص.

۲- انواع وابستگی (ارتباط) میان شبکه قدرت و سایبری

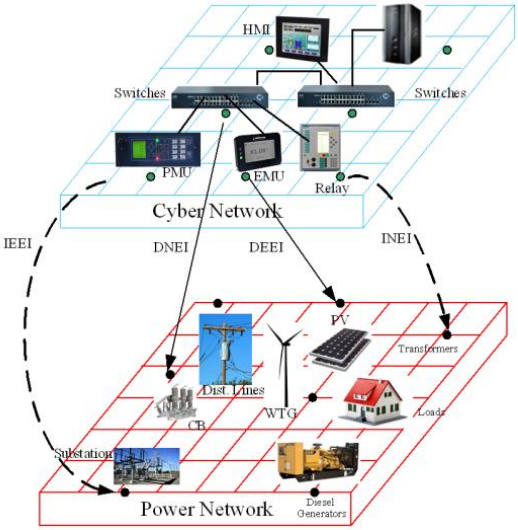
هر شبکه هوشمند از دو زیرسیستم نامتجانس قدرت و سایبری تشکیل می‌شود. شبکه هوشمند به عنوان یک شبکه سایبر- قدرت[۳] دارای ارتباط ویژه میان شبکه سایبری و شبکه قدرت است. ارتباط میان شبکه سایبری و قدرت به طور کلی به معنای عملکرد درست و مناسب یک تجهیز بوده که به وجود و عملکرد صحیح تجهیز دیگر وابسته است. خرابی‌ها در شبکه سایبری اثرات متفاوت و متنوعی بر روی شبکه قدرت می‌تواند

داشته باشد. به طور کلی دو نوع ارتباط میان شبکه‌های سایبری و قدرت وجود دارد که در ادامه به‌شرح آن پرداخته می‌شود.

۱. ارتباط مستقیم که سبب خرابی و یا تغییرات در رفتار تجهیز می‌شود.

۲. ارتباط غیرمستقیم که سبب خرابی و یا تغییر رفتار یک تجهیز نمی‌شود ولی عملکرد تجهیز را در برابر خرابی احتمالی تحت تأثیر قرار می‌دهد.

ارتباط میان دو شبکه قدرت و سایبری بر اساس ماهیت و مکان خرابی در شبکه سایبر عبارتند از: ارتباط مستقیم تجهیز به تجهیز (DEEI[۴])، ارتباط مستقیم شبکه– تجهیز (DNEI[۵])، ارتباط غیرمستقیم تجهیز به تجهیز (IEEI[۶])، ارتباط غیرمستقیم شبکه- تجهیز (INEI[۷]) [۸] . شکل ۱، انواع ارتباط‌های بیان شده را نشان می‌دهد.



شکل ۱: نمایش انواع خطا در شبکه سایبری و اثرات آن بر شبکه قدرت

۳- انواع توپولوژی‌های شبکه سایبری

چهارنوع توپولوژی معروف شبکه مانند باس، رینگ (حلقه)، ستاره و مش می‌باشند [۱۷].

۳-۱- توپولوژی باس

اولین و پایه‌ای‌ترین آرایشی که به‌عنوان توپولوژی شبکه سایبری در بررسی‌ها معرفی می‌شود آرایش باس است که مطابق با شکل ۲.الف نشان داده می‌شود. هر خرابی در این آرایش منجر به قطع ارتباط گره مربوطه با بقیه ساختار می‌شود. هر کلید ارتباطی به کلید قبلی خود توسط یک پورت ارتباطی متصل است.

۳-۲- ساختار رینگ (حلقه)

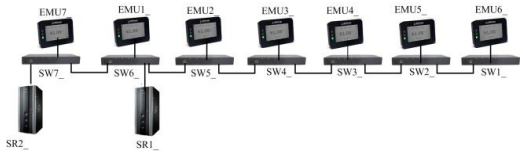
توپولوژی دوم که در شکل ۲.ب نشان داده شده می‌تواند خطا را پوشش داده و داده‌ها را از یک مسیر جای‌گزین ارسال نماید. به‌دلیل داشتن ساختار حلقه‌ای این آرایش، در صورت قطع یکی از نودها ارتباط داده‌ها از سمتی دیگر ادامه می‌یابد. قابلیت اطمینان این ساختار بیش‌تر از آرایش باس است.

۳-۳- توپولوژی ستاره

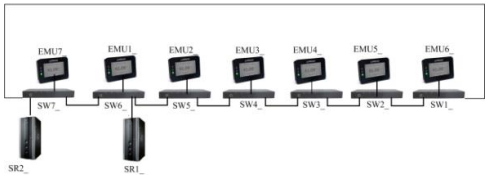
سومین آرایش پیشنهادی ساختار ستاره است که تمامی کنترل‌کننده‌ها و تجهیزهای مربوطه به کلید خاصی متصل می‌باشند. همان‌طور که در شکل ۲.ج نشان داده شده است، تمامی اتصالات کلیدهای ۱ تا ۵ به کلیدهای ۶ و ۷ وصل هستند و اطلاعات را از سرورها که بر روی این دو کلید اتصال دارند دریافت می‌کنند.

۳-۴- ساختار مش[۸]

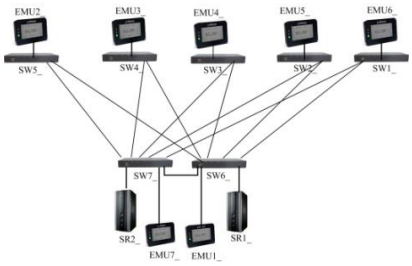
همان‌طور که در شکل ۲.د مشخص است توپولوژی مش ساختاری است که در آن هر تجهیز شبکه به تجهیز دیگری متصل است. در واقع در این ساختار هر گره در شبکه، کلیدهای اصلی و تجهیزات دیگر به یکدیگر اتصال دارند. در این حالت انتقال داده از هر مسیری می‌تواند انجام شود. البته در واقع در این توپولوژی وجود حداقل یک مسیر اضافه برای هر تجهیز تضمین شده است.



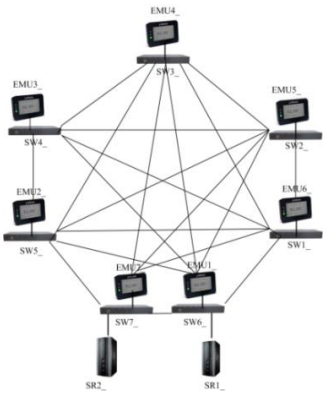
(الف)



(ب)



(ج)



(د)

شکل ۲: الف) توپولوژی باس، ب) توپولوژی حلقه، ج) توپولوژی ستاره، د) توپولوژی مش

۴- ارزیابی ریسک شبکه‌های هوشمند با درنظرگیری ارتباط مستقیم شبکه سایبری و شبکه قدرت

در این بخش، روش پیشنهادی ارزیابی قابلیت اطمینان شبکه‌های هوشمند با درنظرگیری خطاهای شبکه سایبری که به‌صورت مستقیم بر روی شبکه قدرت تأثیر می‌گذارند شرح داده خواهد شد. برای تشریح روش پیشنهادی به صورت کلی روندنمای شکل ۳ مراحل روش ارزیابی قابلیت اطمینان را با درنظرگیری ارتباط مستقیم شبکه سایبری با شبکه قدرت را نشان می‌دهد. روش پیشنهادی از سه قسمت اصلی تشکیل شده است. قسمت اول تحلیل تجهیزات شبکه قدرت و شبکه سایبری را انجام می‌دهد. در مرحله دوم مدل‌سازی منابع تولید پراکنده صورت می‌گیرد. و در بخش سوم ارزیابی قابلیت اطمینان و محاسبه شاخص‌ها بررسی می‌شود.

روش پیشنهادی برای نگاشت خطاهای سایبری به شبکه هوشمند به‌عنوان یک راه‌کار مناسب و عملیاتی برای درنظرگیری ارتباط‌های مستقیم سایبری- قدرت بر این اساس بنا نهاده شده است که حالت مورد مطالعه پایه و مرجع که شامل یک تجهیز سایبری خارج از دسترس باشد به حالت دیگری انتقال داده می‌شود که تجهیز قدرت مربوطه و دارای ارتباط مستقیم سایبری- قدرت نیز از دسترس خارج شود. به‌عنوان مثال، اگر واحد مدیریت انرژی[۹] متصل به یک بخش شبکه قدرت و مولد تولید پراکنده مربوطه دارای خطا شود، مولد تولید پراکنده مورد اشاره و بخش مورد ارتباط با این واحد مدیریت انرژی نمی‌تواند به کارکرد عادی و صحیح خود ادامه دهد و در نتیجه امکان بروز حالتی با شرایط دسترس‌ناپذیری EMU مذکور و دسترس‌پذیری بخش قدرت متناظر وجود ندارد.

۵- فرمولاسیون مسئله

فرمول‌های مربوط به ایجاد ماتریس حالت

اولین مرحله‌ای که برای تحلیل قابلیت اطمینان شبکه‌های هوشمند باید به‌کاربرد ایجاد ماتریس حالت[۱۰] است. ماتریس حالت شامل درایه‌های صفر و یک بوده که نشان دهنده دردسترس‌پذیری و یا دردسترس‌ناپذیری تجهیزات در هر وضعیت می‌باشد. رابطه (۱) این ماتریس را نشان می‌دهد.

$$S_i = \left[s_{i,1},\ldots,s_{i,N_C}, s_{i,N_C+1},\ldots,s_{i,N_C+N_P} \right] \quad (۱)$$

محاسبه احتمال هر حالت

در مرحله دوم، پس از ایجاد حالات مختلف سیستم، لازم است که احتمال رخداد هر حالت محاسبه شود. با توجه به قوانین احتمال، برای هر حالت مستقل، احتمال را می‌توان با کمک رابطه (۲) حساب نمود.

$$P_{r_{S_i}} = \prod_{k=1}^{N_c+N_p} A_k^{(1-S_{ik})} U_k^{(S_{ik})} \quad (۲)$$

در رابطه (۲)، A_k و U_k طبق رابطه (۳) محاسبه می‌شوند.

$$U_k = 1 - A_k = \frac{\lambda_k}{\lambda_k + \mu_k} \quad (۳)$$

محاسبه بارزدایی در حالات مختلف

معادله تعادل توان مطابق با رابطه (۴) خواهد بود.

$$\sum P_G = \sum P_{load} \quad (۴)$$

علاوه بر تعادل توان شبکه، قیودی مانند سیلان توان، ظرفیت خطوط و حد تولید منابع تولید پراکنده و پست اصلی نیز مطابق با رابطه (۵) باید تأمین شود.

$$P_{G,DGs}(t) + P_{MainSub.}(t) \geq P_{Loads}(t) + P_{Loss}(t) \quad (۵)$$

برای محاسبه شاخص‌های قابلیت اطمینان شبکه از روابط (۶ تا ۹) استفاده می‌شود.

$$EENS(P.U.) = \sum_i P_{r_{\phi_i}} . LC_i^T \quad (۶)$$

$$LOLP(\%) = \sum_i P_{r_{\phi_i}} . sgn(LC_i^T) \quad (۷)$$

$$LOEE(Mwh/year) = \sum_i P_{r_{\phi_i}} . LC_i^T \times 8760 \quad (۸)$$

$$LOLE(hr/year) = \sum_i P_{r_{\phi_i}} . sgn(LC_i^T) \times 8760 \quad (۹)$$

در قسمت مدل‌سازی انرژی باد، برای بیان تابع توزیع احتمال کافی است دو پارامتر شکل (k) و مقیاس (c) توزیع احتمال ویبول معین گردند. با داشتن مقادیر k و c محاسبه احتمال وزش سرعت باد مطابق با رابطه (۱۰) به‌دست می‌آید.

$$f(v) = \frac{k}{c}\left(\frac{v}{c}\right)^{k-1} \exp\left[\left(-\frac{v}{c}\right)^k\right] \quad (۱۰)$$

هم‌چنین با در دست داشتن پارامترهایی مانند میانگین (v_m) و انحراف معیار (σ) داده‌های اندازه‌گیری شده مربوط به سرعت وزش باد، می‌توان شاخص‌های مقیاس و شکل توزیع وایبل را به‌صورت تقریبی مشابه آن‌چه در روابط (۱۱) و (۱۲) نشان داده شده است، محاسبه نمود [۱۹]. توان تولیدی توسط انرژی باد نیز با استفاده از رابطه (۱۳) به‌دست می‌آید.

$$k = \left(\frac{\sigma}{v_m}\right)^{-1.086} \quad (۱۱)$$

$$c = \frac{v_m}{\Gamma(1+1/k)} \quad (۱۲)$$

$$P_V(v) = \begin{cases} 0 & 0<v<v_{ci} \\ P_{rated} \times \dfrac{(v-v_{ci})}{(v_r-v_{ci})} & v_{ci}<v<v_r \\ P_{rated} & v_r<v<v_{ct} \\ 0 & v_{ct}<v \end{cases} \quad (۱۳)$$

در قسمت مدل‌سازی ماتریس ارتباطی میان کلیدها مطابق با نظریه گراف، ماتریس مجاورت[۱۱] برای نشان دادن اتصال کلیدها به‌صورت رابطه (۱۴) تعیین می‌شود.

$$\begin{bmatrix} x_{11} & x_{12} & x_{13} & \cdot & \cdot & \cdot & x_{1j} \\ x_{21} & x_{22} & x_{23} & \cdot & \cdot & \cdot & x_{2j} \\ x_{31} & x_{32} & x_{33} & \cdot & \cdot & \cdot & x_{3j} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ x_{i1} & x_{i2} & x_{i3} & \cdot & \cdot & \cdot & x_{ij} \end{bmatrix} \quad (۱۴)$$

درایه‌های این ماتریس به صورت رابطه (۱۵) تعریف می‌شود:

$$x_{ij} = \begin{cases} 1 & \text{i and j are connected} \\ 0 & \text{otherwise} \end{cases} \quad (۱۵)$$

که در آن x_{ij} یک متغیر باینری است. با توجه به ارتباط نداشتن یک المان با خود، در گراف مورد نظر، درایه مربوطه در ماتریس مجاورت، صفر درنظرگرفته می‌شود، و چون خطوط ارتباطی دو طرفه هستند ماتریس متقارن بوده و مقادیر آن‌ها نیز مساوی است. تساوی‌های زیر موید مطالب بیان شده است.

$$\begin{cases} x_{ii} = 0 \\ x_{ij} = x_{ji} \end{cases} \quad (۱۶)$$

برای برقرار بودن شرط دو اتصالی، هر گره حداقل می‌بایست با دو گره دیگر در ارتباط باشد. درنتیجه مجموع سطرها و ستون‌های ماتریس مجاورت باید بزرگ‌تر مساوی دو باشد. که به‌صورت زیر بیان می‌گردد:

$$\sum_{i,j} x_{ij} \geq 2 \quad (۱۷)$$

تابع هدفی که برای حل این مسئله در نظر گرفته می‌شود به‌صورت مجموع دو عبارت است. به این صورت که هزینه ایجاد شبکه که پریونیت‌شده‌ی تعداد شاخه‌ها بوده به همراه هزینه‌ی قابلیت اطمینان که پریونیت شده شاخص EENS بوده جمع شده و به‌عنوان تابع هدف درنظر گرفته می‌شود. با این کار تابع هدف طوری تعریف شده که هزینه ایجاد شبکه و شاخه‌ها را نیز دربرداشته باشد. تابع هدف بیان‌شده به‌طور همزمان شاخص قابلیت اطمینان ذکر شده و هزینه پریونیت‌شده ناشی از تعداد شاخه‌ها را کمینه می‌کند.

این تابع هدف در رابطه (۱۸) بیان شده است.

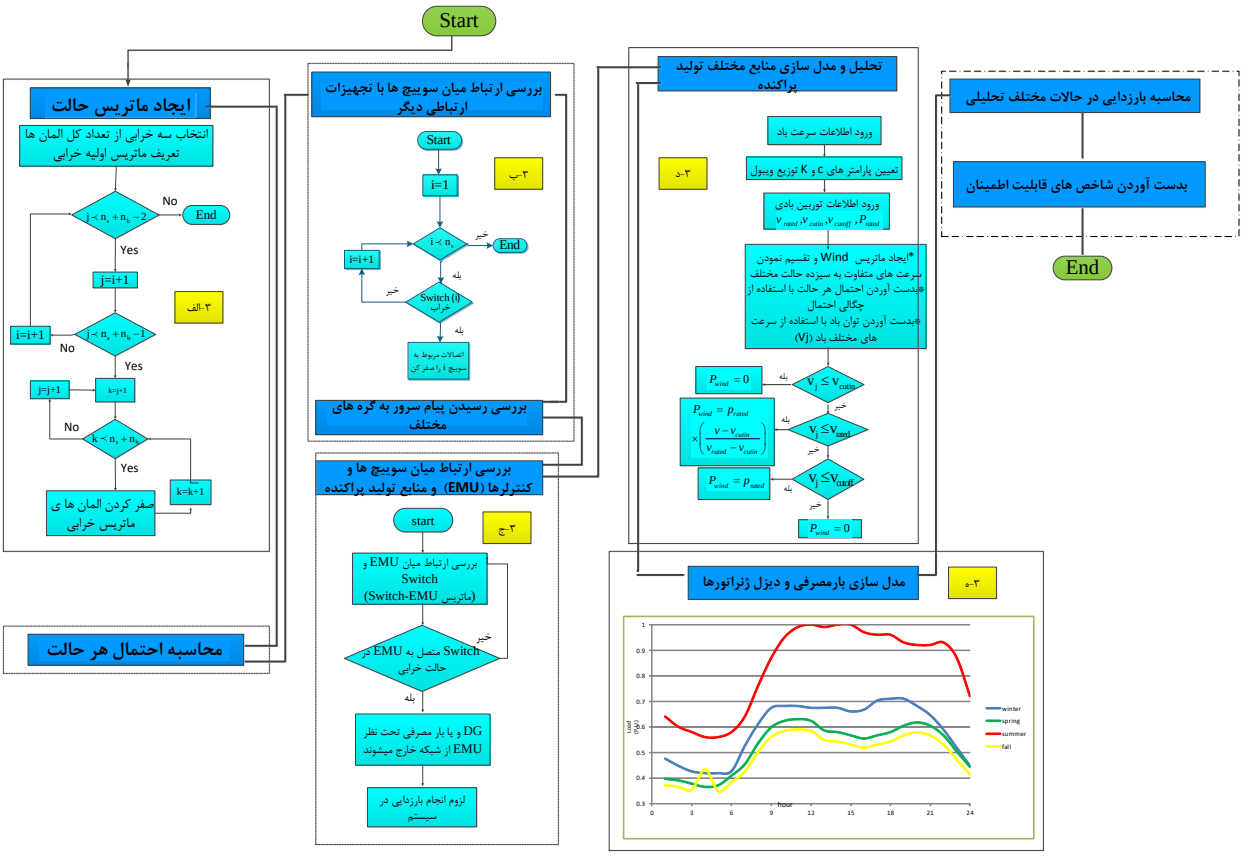
$$\min(\text{Cost Function}) = \frac{\text{Number of Network Branches}}{\text{Maximum Branches}} + \frac{EENS}{EENS_{Max}} \quad (۱۸)$$

۶- الگوریتم پیشنهادی

۶-۱- ایجاد ماتریس حالت

روشی که برای ارزیابی قابلیت اطمینان درنظرگرفته شده روشی تحلیلی بوده که الگوریتم پیشنهادی آن در شکل ۳ نمایش داده شده است.

با توجه به شکل ۳ اولین مرحله‌ای که برای تحلیل قابلیت اطمینان شبکه‌های هوشمند باید به‌کاربرد ایجاد ماتریس حالت[۱۲] است. ماتریس حالت شامل درایه‌های صفر و یک بوده که نشان‌دهنده دردسترس‌پذیری و یا دردسترس‌ناپذیری تجهیزات در هر وضعیت می‌باشد. رابطه (۱) در بخش فرمولاسیون مسئله این ماتریس را نشان می‌دهد.



شکل ۳: روندنمای روش پیشنهادی

در رابطه (۱) هرگاه تجهیزی در دسترس باشد، مقدار صفر برای جزء مربوطه اختصاص داده خواهد شد و اگر تجهیزی خارج از دسترس باشد، المان متناظر در ماتریس حالت سیستم برابر یک خواهد بود. از این رو بر اساس عناصر صفر و یک در ماتریس حالت، حالات مختلف سیستم را می‌توان تشکیل داد. روندنمای مربوط به ایجاد ماتریس حالت و توضیحات تفصیلی مربوط به روش پیشنهادی جهت نگاشت خطا از شبکه سایبری به شبکه قدرت در قسمت الف شکل ۳ آمده است. با درنظرگیری تنها دو و یا سه خرابی به طور همزمان ماتریس حالت تشکیل می‌شود.

۶-۲- محاسبه احتمال هر حالت

در مرحله دوم، پس از ایجاد حالات مختلف سیستم، لازم است که احتمال رخداد هر حالت محاسبه شود. با توجه به قوانین احتمال، برای هر حالت مستقل، احتمال را می‌توان با کمک رابطه (۲) محاسبه نمود.

۶-۳- بررسی ارتباط میان کلیدها و تجهیزات ارتباطی دیگر

در مرحله بعدی اتصال کلیدها که وظیفه دریافت، تحلیل و ارسال داده‌ها را دارند با یکدیگر بررسی می‌شود. در ابتدا، یک ماتریس با ابعاد $n_s \times n_s$ تعریف می‌شود که در آن هر المان می‌تواند مقادیر صفر و یا یک را قبول کند. مقدار باینری یک برای هر المان بدین معناست که اتصال میان کلیدها وجود ندارد. همان طور که در روندنمای شکل ۳-ب مشاهده می‌شود در این حالت بررسی ارتباط میان این تجهیزات باید انجام شود. اگر کلید در حالت خرابی باشد تمامی اتصالات میان آن و دیگر تجهیزات مرتبط با آن نیز قطع می‌شود. در نتیجه در ماتریس ارتباطی میان کلیدها با یکدیگر، عنصر باینری یک میان دو تجهیز موردنظر به صفر تغییر می‌کند.

۶-۴- بررسی رسیدن پیام سرورها به گره‌های مختلف

چهارمین مرحله در توضیح روش پیشنهادی مشخص نمودن رسیدن صحیح پیام سرور به کلیدهای مختلف خواهد بود. در صورت رسیدن پیام از یک سرور به کلید دلخواه باید تمامی کلیدهای متصل به کلید مربوطه پیام ارسالی را دریافت نمایند.

جهت انجام این مرحله، ابتدا از ماتریس ارتباطی میان کلید و سرور که یک ماتریس $n_s \times n_{sr}$ بعدی می‌باشد استفاده می‌شود. این ماتریس بیان‌گر اتصال هر سرور به کلید است و با استفاده از آن ارتباط میان این تجهیزات بررسی می‌شود. به این صورت که هر درایه صفر بدین معنا بوده که اتصال میان سرور و کلید مربوطه قطع است و در صورت وجود درایه یک، اتصال مربوطه برقرار است.

۶-۵- بررسی ارتباط میان کلیدها، کنترل‌کننده‌ها و منابع تولید پراکنده

پس از گذراندن مرحله چهارم، موضوعی که باید مورد مطالعه قرار گیرد رسیدن پیام سرور به کنترل کننده(EMU) است. این موضوع با استفاده از ماتریس‌های ارتباطی میان کلیدها و EMU ها بررسی می‌شود. با تحلیل ماتریس حالات خرابی مربوط به EMU ها دریافت پیام EMU ها از سرور مشخص می‌شود. پس از تحلیل و بررسی شبکه سایبری و ارتباطات مختلف میان عناصر آن، شبکه قدرت در حالات مختلف خرابی که به‌دست آمده مورد ارزیابی قرار می‌گیرد. مطابق روندنمایی که در قسمت ج شکل ۳ نشان داده شده است، هر EMU می‌تواند DG و بار مصرفی متناظر با آن را کنترل کند. در صورت خرابی در EMU ها، بار مصرفی و DG مربوطه از شبکه خارج می‌شوند. در نتیجه تعادل توان (تولید و مصرف) در شبکه قدرت از بین می‌رود. بنابراین بارزدایی در شبکه ضروری خواهد بود. از این رو در حالات مختلف بارزدایی شبکه محاسبه می‌شود.

۶-۶- مدل‌سازی منابع تولید پراکنده و بارهای مصرفی

در این بخش به بررسی منابع تولید پراکنده پرداخته می‌شود. دیزل ژنراتورها منابع تولید توان با ظرفیت ثابت و بدون عدم قطعیت درنظرگرفته می‌شوند. درنتیجه در شبیه‌سازی‌ها توان ثابتی برای آن در نظرگرفته می‌شود. از آن جایی که منابع بادی، به‌صورت پراکنده و دارای رفتار تصادفی هستند، توزیع سرعت باد به طور عمده‌ای عملکرد و امکان‌پذیری سیستم‌های توان بادی را مشخص می‌نماید. مدل‌سازی سرعت باد با استفاده از تابع توزیع احتمال مناسب پارامترهایی را مشخص می‌نماید که با استفاده از آن می‌توان به مدل‌سازی توان باد و محاسبه آن دست یافت [۱۸].

در مورد سرعت وزش باد (v)، استفاده از تابع توزیع احتمال ویبول متداول است [۱۸]. در رابطه (۱۰)، تابع توزیع احتمال ویبول برای سرعت باد نمایش داده شده است. برای بیان تابع توزیع احتمال کافی است دو پارامتر شکل (k) و مقیاس (c) توزیع احتمال ویبول معین گردد. با داشتن مقادیر k و c محاسبه احتمال وزش سرعت باد مطابق با رابطه (۱۰) به دست می‌آید. سپس ویژگی‌های احتمالاتی و آماری سرعت وزش باد مشخص خواهد شد.

همچنین با در دست داشتن پارامترهایی مانند میانگین (v_m) و انحراف معیار (σ) داده‌های اندازه‌گیری شده مربوط به سرعت وزش باد، می‌توان شاخص‌های مقیاس و شکل توزیع وایبل را به صورت تقریبی مشابه آنچه در روابط (۱۱) و (۱۲) نشان داده شده است، محاسبه نمود [۱۹].

میزان توان تولید توربین بادی در سرعت‌های متفاوت به سیزده حالت مختلف تقسیم بندی می‌شود، که در هر حالت کسری از توان نامی به آن اختصاص می‌یابد. گام‌های توان در هر مرحله به اندازه ۰/۱ توان نامی درنظرگرفته می‌شود. ماتریسی به نام wind ایجاد شده که چند ستون مختلف دارد، ستون اول آن سرعت‌های باد است که از ۰ تا ۲۶ متر بر ثانیه تقسیم می‌شود. در ستون دوم میزان توان اختصاص یافته در هر حالت مشخص می‌شود. در ستون بعدی نیز محاسبه احتمال هر حالت درنظرگرفته می‌شود. به دست آوردن توان باد در حالات مختلف با

استفاده از روندنمای قسمت د شکل ۳ انجام می‌شود. توان خروجی واحد تولید بادی مبتنی بر سرعت باد و پارامترهای منحنی توان توربین بادی است. توان خروجی واحد تولیدی بادی به‌صورت رابطه (۱۳) به دست می‌آید [۲۰].

الگوی بار مصرفی توسط مدل‌سازی انجام شده در مراجع و IEEE-RTS به دست می‌آید. منحنی بار شبکه هوشمند مورد مطالعه مطابق قسمت ه شکل ۳ به صورت گام‌هایی با بازه یک ساعت برای یک روز نمونه در چهار فصل سال به‌صورت درصدی از پیک مصرف هر نقطه (پریونیت) در مطالعات لحاظ می‌شود.

۶-۷- محاسبه بارزدایی در حالات مختلف

اگر هر باس در وضعیت خرابی باشد، باری که متناظر با آن است باید از شبکه خارج شود. در غیر این صورت مقادیر اختلاف میان تولید و مصرف باید تصحیح شده و لزوم انجام بارزدایی ضروری خواهد بود.

۷- معرفی شبکه‌ی نمونه پیشنهادی

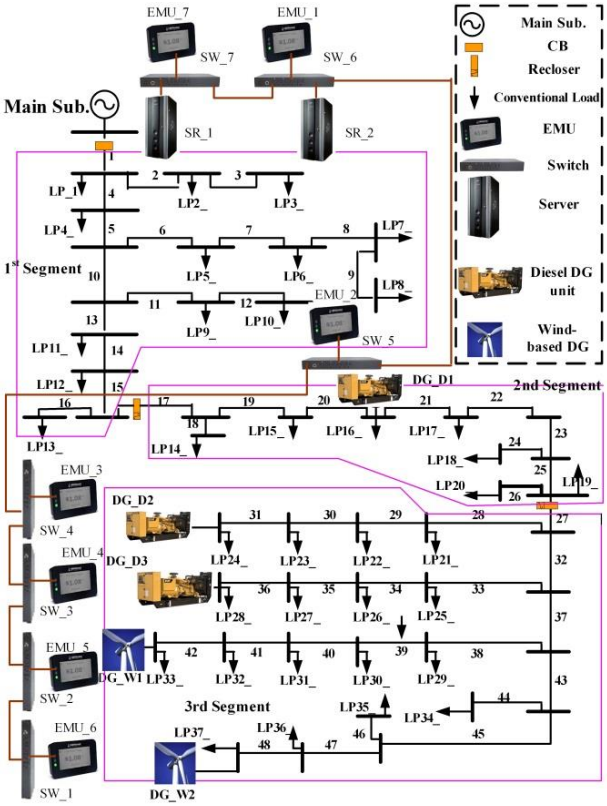
شبکه معرفی شده در این مقاله، شبکه واقعی از شرکت توزیع بندرعباس با نام فیدر آیسین است. همان‌گونه که در شکل ۴ مشاهده می‌شود، سه تجهیز حفاظتی در شین ابتدایی خطوط ۱، ۱۷ و ۲۷ وجود دارد. بر اساس مفاهیم و مبانی شرح داده شده در بخش‌بندی سیستم، شبکه توزیع فوق به سه بخش تقسیم خواهد شد. هر کدام از بخش‌های شماره یک، شماره دو و شماره سه به‌ترتیب دارای پیک بار تجمیعی ۱/۸۴۷، ۱/۳۰۰ و ۲/۹۴۷ مگاوات هستند. استخوان‌بندی اصلی شبکه برای هوشمندسازی در مسئله مورد بحث در مقاله، فیدر آیسین بوده که مطابق شکل ۴ است که بررسی شبکه سایبری بر روی شبکه قدرت بر روی آن انجام می‌شود. پنج مولد تولید پراکنده درنظر گرفته شده است. مولدهای درنظر گرفته شده در دو نوع بادی و دیزل ژنراتور می‌باشند. مولدهای تولید پراکنده دیزل ژنراتور در باس‌های ۱۶ بخش دوم و نقاط بار ۲۸ و ۳۷ بخش سوم متصل می‌باشند. ظرفیت هر کدام از این دیزل ژنراتورها برابر ۹۰۰ کیلووات است. همچنین مولدهای تولید پراکنده تجدیدپذیر بادی با ظرفیت ۳۷۵ کیلووات در نقاط بار ۳۳ بخش سوم و ۲۴ بخش دوم نصب شده‌اند. اطلاعات و نرخ خرابی تجهیزات مانند منابع تولیدپراکنده و سایر اجزای شبکه بر اساس اطلاعات استخراج شده از مراجع [۱۱، ۱۲ و ۲۲] درنظرگرفته شده است. نرم‌افزار مورد استفاده برای شبیه‌سازی این شبکه و تحلیل‌های مورد نیاز MATLAB R2013b بوده است.

۸- پیاده‌سازی روش بر روی شبکه نمونه معرفی شده در [۱۱، ۱۲]

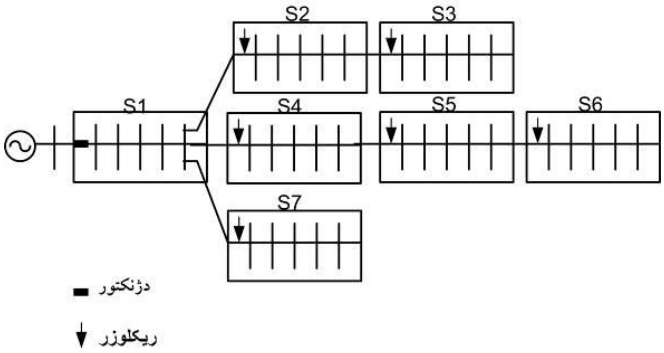
که شبکه توزیع به وسیله بخش‌هایی جداگانه مشخص می‌شود [۱۲]. ورودی هر بخش یک وسیله حفاظتی و یا یک کلید قدرت[۱۳] است. مطابق با شکل ۵ هر بخش تنها از یک رله تشکیل می‌شود. از این مفهوم ساده می‌توان استفاده نمود و بر اساس موقعیت قرارگیری تجهیزات حفاظتی و مفاهیم بخش‌بندی شبکه، تعداد نقاط بررسی شبکه را در اکثر موارد به تعداد بخش‌های شبکه کاهش داد. باید توجه داشت با استفاده از مفهوم بخش‌بندی شبکه، حجم محاسبات بسیار کاهش یافته و سرعت همگرایی به نتایج نهایی افزایش چشم‌گیری خواهد یافت.

درابتدا در این بخش از مفهوم بخش‌بندی کردن برای مشخص کردن احتمال حالت جزیره‌ای استفاده می‌شود. این مفهوم به این معنی است

در ادامه ، روش پیشنهادی بر روی شبکه نمونه معرفی شده در مراجع [۱۱، ۱۲] پیاده‌سازی می‌شود. نمایش تک خطی این شبکه در شکل ۶ قابل مشاهده است. شبکه مورد مطالعه یک شبکه توزیع با دو بخش بر اساس قرارگیری تجهیزات حفاظتی می‌باشد. در این شبکه دو نوع مولد تولید پراکنده بادی و دیزل ژنراتور نصب شده است. توان هر دیزل ژنراتور برابر ۲/۵ مگاوات و توان توربین بادی برابر ۱ مگاوات است.

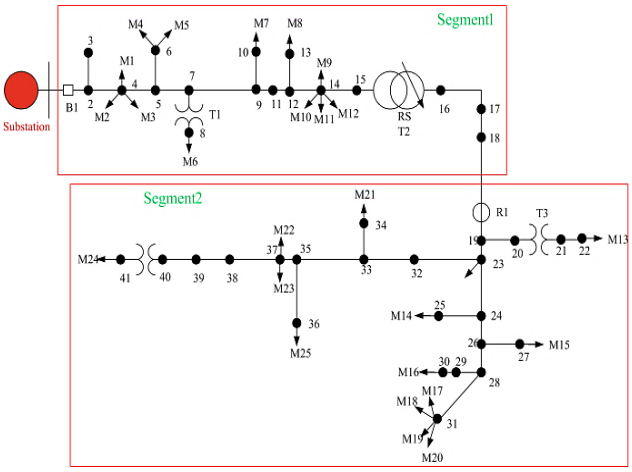


شکل ۴: نمایش تک خطی شبکه نمونه برای پیاده‌سازی روش پیشنهادی ارزیابی قابلیت اطمینان



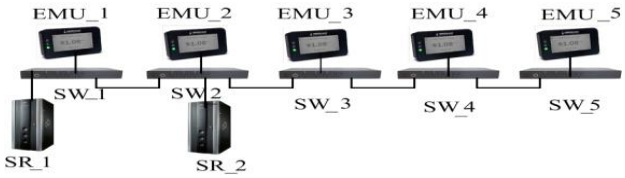
شکل ۵: مفهوم بخش‌بندی کردن [۱۱]

در شکل ۷ نیز شبکه سایبری مفروض برای این شبکه توزیع هوشمند درنظر گرفته شده است. با توجه به تمرکز بر اجزای کنترلی در مطالعه قابلیت اطمینان شبکه‌های هوشمند با درنظرگیری ارتباط‌های مستقیم سایبر- قدرت، واحدهای مدیریت انرژی به‌عنوان کنترل کننده شبکه، کلیدها و سرورها در شبکه سایبری غیر ایده‌آل در نظر گرفته شده است.



شکل ۶: نمایش تک خطی شبکه نمونه معرفی شده در مراجع [۱۱، ۱۲]

در جدول ۱، ارتباط‌های مستقیم سایبر- قدرت مورد مطالعه در شبکه نشان داده شده در شکل‌های ۶ و ۷ بیان شده است. در شکل ۷ آرایش شبکه سایبری که به‌صورت باس است نشان داده شده که ارتباط خطی میان تجهیزات سایبری را نشان می‌دهد.



شکل ۷: نمایش شبکه سایبری سیستم مورد مطالعه نشان داده شده در شکل ۱۱

جدول ۱: ارتباط‌های مستقیم سایبر- قدرت تجهیز به تجهیز شبکه نمونه نشان داده شده در شکل ۶

ردیف	تجهیز سایبری	تجهیز قدرت
۱	EMU_1	پست اصلی ۶۳/۲۰ کیلو ولت
۲	EMU_2	پست اصلی ۶۳/۲۰ کیلو ولت
۳	EMU_3	منبع تولید پراکنده شماره یک، بخش اول
۴	EMU_4	منبع تولید پراکنده شماره دو، بخش دوم
۵	EMU_5	منبع تولید پراکنده شماره سه، بخش دوم

بر اساس آسیب‌پذیر بودن و احتمال بروز خطا در شبکه قدرت و سایبری، می‌توان چهار سناریوی زیر را تعریف کرد که دو مورد (سناریو دوم و چهارم) از اهمیت بیش‌تری در مقایسه با سناریوهای دیگر برخوردار می‌باشند:

- سناریوی اول: شبکه سایبری و قدرت ایده آل بوده و عاری از خطا می‌باشند.
- سناریوی دوم: شبکه سایبری ایده‌آل و عاری از خطا بوده، ولی شبکه قدرت دارای خطا می‌باشد.
- سناریوی سوم: شبکه قدرت ایده‌آل و احتمال بروز خطا در شبکه سایبری وجود دارد.
- سناریوی چهارم: احتمال بروز خطا در شبکه سایبری و قدرت وجود دارد.

نتایج ارزیابی ریسک شبکه نشان داده شده در شکل ۶، در جدول ۲ بیان شده است. همان‌گونه که در این جدول مشاهده می‌شود، نتایج ارزیابی ریسک شبکه در شرایطی که شبکه سایبری ایده‌آل فرض گردد (سناریو دوم) بر اساس روش تحلیلی و همچنین مونت کارلو ارائه شده در [۱۲-۱۱] و همچنین روش پیشنهادی آورده شده است. اعداد و نتایج به‌دست آمده نشان می‌دهد که روش پیشنهادی برای ارزیابی سیستم دارای دقت مناسب بوده و نتایجی مشابه با نتایج روش مراجع [۱۲-۱۱] حاصل شده است.

همچنین نتایج ارزیابی شاخص‌های ریسک سیستم با درنظرگیری خطای شبکه سایبری نشان داده شده در سناریوی چهارم محاسبه گردیده است. نتایج به‌دست آمده نشان می‌دهد که ۸۳/۴۵٪ خطا و عدم دقت ناشی از درنظر گرفتن خطای شبکه سایبری در نتایج LOLE وجود دارد. در ضمن مقدار LOEE از ۲۴/۱۹ مگاوات‌ساعت در سال به ۳۵/۵۴ مگاوات ساعت در سال ناشی از خطاهای سایبری افزایش یافته است. افزایش مقدار انرژی از دست رفته مورد انتظار به‌سبب خطاهای شبکه سایبری با ارتباط مستقیم در حدود ۴۷٪ شده است. این نتایج نشان می‌دهد که نمی‌توان با استفاده از روش‌های مرسوم و این فرض ساده‌کننده که سیستم سایبری ایده‌آل بوده و خطایی در آن اتفاق نمی‌افتد، ارزیابی کاملاً دقیق از شاخص‌های ریسک سیستم داشت. بر اساس مقایسه‌های انجام‌شده می‌توان استدلال نمود که خطاهای شبکه سایبری دارای اهمیت ویژه در قابلیت اطمینان سیستم می‌باشند و همچنین استفاده از روشی که خطاهای شبکه سایبری را در معادلات ارزیابی ریسک شبکه‌های هوشمند وارد نماید ضروری است.

۹- تغییر در ساختار ماتریس ارتباطی میان کلیدها و کنترل‌کننده‌ها[۱۴] و تاثیرات آن بر روی شاخص‌های قابلیت اطمینان شبکه هوشمند

در این بخش با تغییر در ساختار ماتریس ارتباطی میان کلیدها و کنترل‌کننده روند تغییر در شاخص‌های قابلیت اطمینان شبکه هوشمند دنبال می‌شود. در تحلیل‌هایی که تا به حال انجام شد ساختار این ماتریس به این صورت فرض شده بود که مانند شکل ۲. الف هر

کنترل‌کننده (EMU) به یک کلید متصل بوده و منبع تولید پراکنده و بار مربوطه را تحت کنترل خود دارد. در این قسمت سه ساختار دیگر نیز بررسی می‌شود.

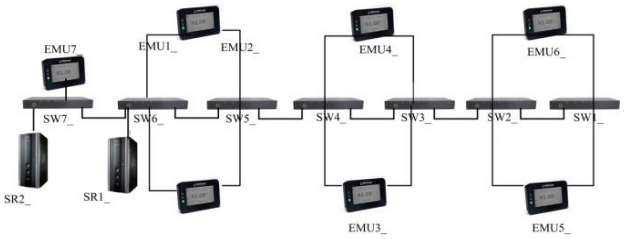
در ساختار دوم آرایش پیشنهادی به این صورت درنظر گرفته می‌شود که هر EMU به دو کلید ارتباطی متصل بوده و آن را کنترل می‌کند. همان‌طور که در شکل ۸ نشان داده شده است مزیت این ساختار این است که اگر یکی از کنترل‌کننده‌ها خراب شود و به‌درستی عکس‌العمل نشان ندهد کنترل‌کننده‌ی دیگر که به کلید مربوطه متصل است می‌تواند به عنوان جای‌گزین وارد شده و کلید مربوطه را تحت اختیار خود بگیرد.

در آرایش سوم نحوه ارتباط کلیدهای ارتباطی با کنترل‌کننده‌ها (EMU) به‌صورت شکل ۸ می‌باشد. در واقع هر کلید با کنترل‌کننده‌های کناری خود در ارتباط است و پیام‌های رسیده از سرورها را دریافت می‌کند. مزیت این آرایش این است که اگر یکی از EMU ها از کار بیافتد، کلید مرتبط با آن می‌تواند با کنترل‌کننده‌های دیگر ارتباط برقرار نماید. هم‌چنین در ساختار چهارم همه کلیدها به همه EMU ها متصل می‌باشند.

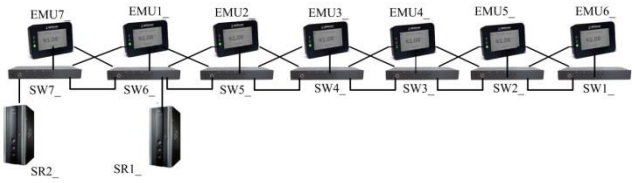
مقادیر شاخص‌های قابلیت اطمینان شبکه هوشمند مربوط به فیدر آیسین با توجه به ساختارهای متفاوت ارتباط میان کنترل‌کننده و کلیدها در جدول ۳ آمده است. با توجه به نتایج موجود در جدول می‌توان نتیجه گرفت که نحوه اتصال دو تجهیز کنترل‌کننده (EMU) و کلید تأثیر به‌سزایی در بهبود شاخص‌های قابلیت اطمینان شبکه هوشمند دارد. تا به حال ساختار پایه در شبیه‌سازی شبکه نمونه ساختار اول (پایه) بوده، با توجه به پرهزینه بودن ساختار چهارم که در شکل (۹) نشان داده شده است و لینک‌های ارتباطی بسیاری که باید در آن ایجاد شود، می‌توان از ساختار دوم و یا سوم نیز استفاده نمود.

جدول ۲: نتایج ارزیابی شاخص‌های ریسک شبکه نمونه نشان داده شده در شکل ۱۱

ردیف	شاخص‌های کفایت (adequacy)	سناریو دوم				سناریو چهارم	
		روش مراجع [۱۱، ۱۲]		روش پیشنهادی مرجع [۲۳]	روش پیشنهادی	روش پیشنهادی مرجع [۲۳]	روش پیشنهادی
		تحلیلی	مونت کارلو				
۱	LOLE (hr/year)	۱۰/۴۲۸۱	۹/۷۵۴۶	۱۰/۳۶۳۶	۱۰/۰۵	۱۹/۲۱	۱۸/۴۸
۲	LOEE (MWh/year)	۲۵/۵۵۴۴	۲۴/۴۳۵۱	۲۵/۳۶۱۲	۲۴/۱۹	۳۳/۵۴	۳۵/۵۴



شکل ۸: ساختار شبکه سایبری-ساختار دوم



شکل ۹: ساختار شبکه سایبری- ساختار سوم

جدول ۳: شاخص‌های ریسک شبکه نمونه برای ساختارهای متفاوت شبکه سایبری

شاخص	LOEE(MWh/year)	LOLE (hr/year)
ساختار پایه (bus)	۷۲/۶۸	۵۸/۴۹
ساختار دوم	۶۱/۶۰	۵۴/۹۶
ساختار سوم	۵۸/۸۱	۵۴/۴۶
ساختار چهارم (mesh)	۴۳/۸۶	۴۴/۳۶

۱۰- بهینه‌سازی توپولوژی شبکه سایبری با دیدگاه بهبود قابلیت اطمینان شبکه‌های هوشمند

در این بخش هدف تغییر در ماتریس ارتباطی میان کلیدها (switch-switch) با یکدیگر است. با استفاده از تئوری گراف‌ها در این بخش به مدل‌سازی و شبیه‌سازی ماتریس ارتباطی میان کلیدها می‌پردازیم. بدین صورت که هر کلید یک گره فرض شده است که ارتباط میان آن‌ها با شاخه نشان داده می‌شود. همان طور که در بخش فرمولاسیون مسئله بیان شد، مطابق با روابط (۱۴) و (۱۵) ماتریس مجاورت مدل می‌شود.

تابع هدفی که برای این مسئله در نظرگرفته شده است یکی از شاخص‌های ارزیابی قابلیت اطمینان شبکه هوشمند است که در این‌جا از EENS استفاده شده است. قیودی که در بهینه‌سازی مذکور درنظرگرفته شده است به‌صورت زیر است:

۱. گراف مورد نظر پیوسته باشد. به عبارتی دیگر اتصال میان همه گره‌های گراف برقرار باشد (connectivity).
۲. شرط دو اتصالی نیز برقرار باشد. یعنی هر گره حداقل به دو شاخه متصل باشد. این قید به این علت قرار داده شده که اطمینان حاصل کنیم داده‌های مورد نظر به گره‌های دیگر می‌رسند (two-connectivity).

۳. هزینه ایجاد شبکه که به‌صورت حاصل ضرب یک عدد ثابت (هزینه ایجاد هر شاخه) در تعداد شاخه‌ها درنظرگرفته می‌شود کمینه شود.

برای درنظرگیری شرط هزینه که برابر با حاصل ضرب یک ضریب ثابت در تعداد شاخه‌ها می‌باشد، می‌توان تنها تعداد شاخه‌ها را درنظرگرفت. با کمینه نمودن تعداد شاخه‌ها می‌توان هزینه ایجاد شبکه را نیز کمینه نمود.

برای حل این مسئله در این مقاله، از دو روش بهینه‌سازی استفاده می‌شود. ابتدا از الگوریتم ژنتیک که روشی شناخته شده در مراجع است استفاده نموده و با استفاده از آن ساختار بهینه توپولوژی شبکه سایبری را با توجه به آنچه از قبل تعریف شده به‌دست آورده می‌شود. نتیجه حاصله از الگوریتم ژنتیک در جدول ۴ آمده است. شکل ۱۰ ساختار شبکه سایبری را پس از بهینه‌سازی نشان می‌دهد. ساختاری که در شکل ۱۰ نشان داده شده است ارتباط میان کلیدهای ارتباطی را نشان می‌دهد که قیود ذکرشده در قسمت فرمولاسیون مسئله را برآورده می‌نماید. می‌توان گفت با این آرایش به بهترین حالت از لحاظ قابلیت اطمینان و کمینه‌ترین هزینه می‌رسیم.

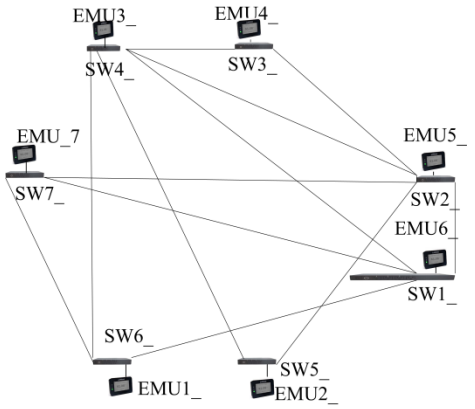
در ادامه از یک الگوریتم نسبتاً جدید به نام ALO (بهینه‌سازی شیرمورچه) استفاده شده که در سال ۲۰۱۵ در مرجع [۲۴] ارائه شده است. نتایج حاصله از شبیه‌سازی این الگوریتم در جدول ۵ نشان داده شده است که مقدار شاخص را مشابه الگوریتم ژنتیک به‌دست آورده است ولی ساختار بهینه به‌صورت شکل ۱۱ نشان داده شده است.در این شکل ارتباط میان کلیدهای ارتباطی را به صورت متفاوتی از شکل ۱۰ نشان می‌دهد که تعداد شاخه‌ها را کم‌تر از حالت قبلی نشان می‌دهد. این الگوریتم روشی الهام‌گرفته از طبیعت است که از مکانیزم شکار شیرمورچه در طبیعت پیروی می‌کند. در واقع الهام‌بخش این الگوریتم، رفتار شکار شیرمورچه‌ها و به دام انداختن مورچه‌ها در دام‌هایشان می‌باشد. ویژگی متمایز این الگوریتم قابلیت جست‌وجوی بالا و نرخ همگرایی بالا است [۲۴].

جدول ۴: نتایج بهینه‌سازی توپولوژی شبکه سایبری با روش الگوریتم ژنتیک (GA)

تعداد تکرار	تعداد جمعیت	جواب بهینه (تابع هدف)-EENS	متغیرها	تعداد شاخه‌ها
۲۰	۲۰	۰/۰۰۶۱۷	ماتریس ارتباطی کلید- کلید	۱۲

جدول ۵: نتایج بهینه‌سازی توپولوژی شبکه سایبری با روش بهینه‌سازی شیرمورچه[۱۵]

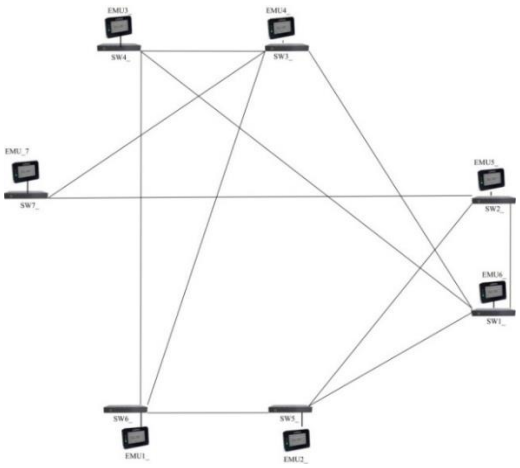
تعداد تکرار	تعداد جمعیت	جواب بهینه (تابع هدف)-EENS	متغیرها	تعداد شاخه‌ها
۲۰	۲۰	۰/۰۰۶۱۷	ماتریس ارتباطی سوییچ - سوییچ	۱۱



شکل ۱۰: ساختار شبکه سایبری منتجه از بهینه‌سازی با روش GA (شبکه واقعی)

ماتریس ارتباطی میان کلیدها که توسط بهینه‌سازی به‌دست آمده به‌صورت زیر است.

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix} \quad (۱۸)$$



شکل ۱۱: ساختار شبکه سایبری منتجه از بهینه‌سازی با روش ALO (شبکه واقعی)

۱۱- نتیجه‌گیری

با توجه به پیشرفت‌های اخیر در تجهیزات و فناوری‌های شبکه‌های هوشمند، خرابی‌های شبکه سایبری و تاثیرات آن بر روی شبکه قدرت باید در نظرگرفته شوند. در این مقاله روشی تحلیلی و جدید برای ارزیابی قابلیت اطمینان شبکه هوشمند ارائه شده است که ارتباط مستقیم میان شبکه سایبری و قدرت را درنظرمی‌گیرد. تحلیل قابلیت اطمینان شبکه هوشمند بدون درنظرگیری ارتباط میان شبکه سایبر-قدرت با خطای زیادی همراه است زیرا شبکه‌های مخابراتی و سایبری در معرض خرابی‌های متعددی قرار دارند. با استفاده از یک روش پیشنهادی

مرحله‌ای که بر مبنای ارتباط میان عناصر و تعریف ماتریس‌هایی میان تجهیزات مختلف است محاسبه قابلیت اطمینان شبکه موردنظر انجام شد. روش پیشنهادی بر روی فیدر آیسین (یکی از شبکه‌های شرکت توزیع نیروی برق بندرعباس) که یکی از شبکه‌های بحرانی و پربار بوده پیاده‌سازی و تحلیل شد با مقایسه نتایج می‌توان دریافت که دقیق نبودن نتایج قابلیت اطمینان بر اساس روش‌های مرسوم مهم است. به همین دلیل می‌بایست اثرات و ارتباطات این دوشبکه را درنظرگرفت. در ادامه نیز جهت بهبود قابلیت اطمینان به بررسی آرایش‌های مختلف شبکه سایبری و هم‌چنین بهینه‌سازی ساختار این شبکه با استفاده از دو الگوریتم ژنتیک و ALO پرداخته شد.

مراجع

[1] P. P. Varaiya, F. F. Wu and J. W. Bialej, “Smart operation of smart grid: risk-limiting dispatch,” Proc. IEEE, vol. 99, no. 1, pp. 40-57, Jan. 2011.

[2] F. Aminifar, M. Fotuhi-Firuzabad, M. Shahidehpour and A. Safadarian, "Impact of WAMS malfunction on power system reliability assesment," IEEE Trans. on Smart Grid, vol. 3, no. 3, pp. 1302-1309, 2012.

[3] A. G. Bruce, "Reliability analysis of electric utility SCADA systems," IEEE Trans. Power Syst., vol. 13, no. 3, pp. 844-849, 1998.

[4] D. Kirschen and F. Bouffard, “Keep the lights on and the Information Flowing, a new framework for analyzing power system security,” IEEE Power Energy Mag., pp. 50–60, Jan.–Feb. 2009.

[5] H. Tram, “Technical and operation considerations in using smart metering for outage management,” in Proc. IEEE/PES Transm. Distrib. Conf. Expo. 2008, pp. 1–3, 2008.

[6] L. Pereira, “Cascade to black [system blackouts],” IEEE Power Energy Magazine, vol. 2, no. 3, pp. 54–57, May–Jun. 2004.

[7] Fang, S. Misra, X. Gue and D. Yang, "Smart grid- the new and improved power grid: a survey," Communications surveys and tutorials, IEEE, vol. 14, no. 4, pp. 944-980, 2012.

[8] B. Falahati and Y. Fu, “Reliability assessment of smart grid considering direct cyber-power interdependencies,” IEEE Trans. Smart Grid, vol. 3, no. 3, pp. 1515-1524, 2012.

[9] B. Falahati and Y. Fu, “Reliability assessment of smart grid considering indirect cyber-power interdependencies,” IEEE Trans. Smart Grid, vol. 5, no. 4, pp. 1677-1685, 2014.

[10] C. Singh, A. Sprintson, and A. , “Reliability assurance of cyber-physical power systems,” in Power Energy Society Gen. Meet., 2010 IEEE, pp. 1–6, Jul. 25–29, 2010.

[11] Y. M. Atwa and E. F. El-Saadany, A.-C. Guise, “Supply adequacy assessment of distribution system including wind-based DG during different modes of operation,” IEEE Trans. Power Syst., vol. 25, no. 1, pp. 78-86, Feb. 2010.

[12] Y. M. Atwa and E. F. El-Saadany, M. M. A. Salama, R. Seethapathy, M. Assam, S. Conti, “Adequacy evaluation of distribution system including wind/solar DG during different modes of operation,” IEEE Trans. Power syst., vol. 26, no. 4, pp. 1945-1952, Nov. 2011.

[13] H. Hashemi-Dezaki, H. Askarian-Abyaneh, M. Garmrudi, H. Mahdinia and K. Mazlumi, “A novel approach based on reliability sensitivity analysis to allocate protective devices,” Turk J Elec Eng & Comp Sci., vol. 22, no. 2, pp. 315-324, 2014.

[14] H. Hashemi-Dezaki, S. H. Hosseinian, H. Askarian-Abyaneh and S. M. Mousavi Agah, “Optimized operation and maintenance costs to improve system reliability by decreasing the failure rate of distribution lines”, Turk. J. Elec. Eng. & Comp. Sci., vol. 21, no. 2, pp. 2191-2204, Dec 2013.

[15] H. Hashemi-Dezaki, H. Askarian-Abyaneh, G. B. Gharehpetian and H. Nafisi, “Optimized allocation of DGs to improve system reliability based on loading effects,” Arab. J. Sci. Eng., vol. 39, no. 5, pp. 3907-3915, 2014.

[16] B. Falahati and Y. Fu, "Faults and failures in cyber-power interdependent networks," in T&D Conference and Exposition, 2014 IEEE PES, 2014, pp. 1-5.

[17] S. Wei-Liang, C. Chung-Shiuan, K. C. J. Lin, and K. A. Hua, "Autonomous Mobile Mesh Networks," Mobile Computing, IEEE Transactions on, vol. 13, pp. 364-376, 2014.

[18] M. N. Albasrawi, N. Jarus, K. A. Joshi, and S. S. Sarvestani, "Analysis of Reliability and Resilience for Smart Grids," in Computer Software and Applications Conference (COMPSAC), 2014 IEEE 38th Annual, pp. 529-534, 2014.

[۱۹] حسین شکری، سجاد نجفی، "حل مسئله مشارکت بهینه واحدهای نیروگاهی در حضور منابع انرژی تجدیدپذیر"، مجله مهندسی برق دانشگاه تبریز, دوره ۴۵، شماره ۱، بهار ۱۳۹۴.

[۲۰] رضا قربانی, کاظم مظلومی, "جایابی و تعیین ظرفیت بهینه محدودساز جریان خطا با لحاظ عدم قطعیت در توان تولیدی توربین بادی", مجله مهندسی برق دانشگاه تبریز, دوره ۴۶، شماره ۴، زمستان ۱۳۹۵.

[21] A. H. Ahangar, H. A. Abyaneh, and G. B. Gharepetian, "Negative effects of cyber network (control, monitoring, and protection) on reliability of smart grids based on DG penetration," in Computer and Knowledge Engineering (ICCKE), 2015 5th International Conference on, pp. 54-60, 2015.

[22] L. Jikeng, W. Xudong, Q. Ling, “Reliability evaluation for the distribution system with distributed generation,” Euro. Trans. Electr. Power, vol. 21, no. 1, pp. 895–907, 2011.

[۲۳] حامد هاشمی دزکی، " مدیریت ریسک شبکه‌های هوشمند انرژی الکتریکی در شرایط عدم قطعیت پارامترهای سیستم،" رساله دکتری، دانشکده مهندسی برق، دانشگاه صنعتی امیرکبیر، ۱۳۹۴.

[24] S. Mirjalili, "The Ant Lion Optimizer," Advances in Engineering Software, vol. 83, pp. 80-98, 2015.

علائم و اختصارات

S_i	i امین ماتریس حالت سیستم	A_k	در دسترس پذیری المان k ام
$s_{i,j}$	متغیر باینری معرف دسترس‌پذیری j امین تجهیز در i امین ماتریس حالت سیستم	U_k	در دسترس ناپذیری المان k ام
N_C	تعداد اجزای شبکه سایبری	λ_k	نرخ خرابی
N_P	تعداد اجزای شبکه قدرت	μ_k	نرخ تعمیر
$P_{r_{S_i}}$	احتمال حالت i ام	P_G	توان تولیدی
LOLP[۱۶]	احتمال از دست رفتن بار	LOLE[۱۷]	تعداد ساعات از دست رفتن بار
LOEE[۱۸]	انرژی مورد انتظار از دست رفته	sgn	تابع علامت
v_m	میانگین سرعت	σ	انحراف معیار
v_{ci}	سرعت قطع ابتدایی	v_{ct}	سرعت قطع انتهایی

P_{Load}	توان بار	k	پارامتر شکل
P_{Loss}	توان تلفاتی	c	پارامتر مقیاس
$P_{MainSub.}$	توان تولیدی پست	P_{rated}	توان نامی باد
LC_i^T	مجموع بارزدایی در حالات مختلف	v_r	سرعت نامی
EENS[۱۹]	انرژی مورد انتظار تأمین نشده		

زیرنویس‌ها

[1] Supervisory Control And Data Acquisition
[2] Interdependent Cyber-System
[۳] Cyber-Power
[4] Direct Element Element Interdependency
[5] Direct Network Element Interdependency
[۶] Indirect Element Element Interdependency
[۷] Indirect Network Element Interdependency
[۸] Mesh
[۹] Energy Management Unit (EMU)
[۱۰] State Matrix
[۱۱] Adjacency Matrix
[۱۲] State Matrix
[۱۳] Circuit breaker
[۱۴] Switch-EMU
[۱۵] Ant-Lion Optimizer
[16] Loss Of Load Probability
[17] Loss Of Load Expected
[18] Loss Of Energy Expected
[19] Expected Energy Not Served