No. F-15-AAA-0000

ارزیابی قابلیت اطمینان شبکه هوشمند با در نظرگیری ارتباط غیرمستقیم شبکه سایبری بر شبکه قدرت درحضورمنابع تولید پراکنده

امیررضا حسنی آهنگر، حسین عسکریان ابیانه، همایون حائری

دانشکده مهندسی برق

دانشگاه صنعتی امیرکبیر

تهران

hassaniahangar@aut.ac.ir, askarian@aut.ac.ir, haeri@tavanir.org.ir

چکیده — استفاده از زیرساخت‌ها و تجهیزات مخابراتی در شبکه‌های هوشمند توزیع انرژی الکتریکی سبب شده است تا سیستمی متشکل از شبکه قدرت و شبکه سایبری (شبکه‌های کنترل، مانیتورینگ و حفاظت) ایجاد شود. در شبکه هوشمند، عملکرد سیستم قدرت بستگی زیادی به سیستم‌های مخابراتی دارد. این تجهیزات شامل سیستم‌های مانیتورینگ و حفاظت بوده که در شبکه‌های فوق توزیع نقش مهمی را ایفا می‌کنند. هرکدام از این تجهیزات می‌توانند اثرات متفاوتی بر روی شبکه قدرت داشته باشند. ارتباط این سیستم‌ها با شبکه قدرت به‌صورت ارتباط مستقیم و غیرمستقیم تقسیم‌بندی می‌شوند. در ارزیابی قابلیت اطمینان شبکه هوشمند باید روشی مورداستفاده قرار گیرد که شامل عملکرد مناسب هر دو سیستم سایبری و قدرت باشد. در این مقاله روشی نوین برای ارزیابی شاخص‌های قابلیت اطمینان شبکه‌های هوشمند با در نظرگیری ارتباط و خطاهای غیرمستقیم شبکه سایبری بر روی شبکه قدرت بر اساس روش تحلیلی ارائه می‌گردد. در این نوع ارتباط، در اثر عدم عملکرد تجهیز سایبری نرخ خرابی عناصر شبکه قدرت تغییر خواهد کرد. هم‌چنین یک مدل به‌روزرسانی حالات ارائه خواهد شد تا قابلیت اطمینان شبکه‌های سایبر- قدرت را تحت ارتباط غیرمستقیم ارزیابی کند. روش پیشنهادی بر روی شبکه هوشمند نمونه که یک پست H فشارقوی می‌باشد اعمال خواهد شد تا اثرات روش پیشنهادی را نشان دهد. هم-چنین در حضور منابع تولید پراکنده و بار مصرفی متغیر (منحنی بار) نیز به بررسی روش ارائه‌شده و تحلیل متناسب با آن پرداخته خواهد شد.

واژه‌های کلیدی — شبکه هوشمند، قابلیت اطمینان، ارتباط شبکه سایبری (شبکه کنترل، پایش و حفاظت) و قدرت، انرژی توزیع نشده مورد انتظار، تولیدات پراکنده.

۱.مقدمه

در سالیان اخیر با استفاده از منابع تولید پراکنده (DG) و رشد روزافزون آن‌ها در سیستم‌های قدرت، این نوع منابع مورد توجه بسیاری قرارگرفته است. از محاسن استفاده از منابع تولید پراکنده می‌توان به کاهش تلفات، آزادسازی ظرفیت انتقال و به تاخیرانداختن طرح‌های انتقال اشاره نمود [۱]. DG ها علاوه بر عملکرد عادی خود و متصل به شبکه قدرت، می‌توانند در زمان‌هایی که قسمتی از شبکه توزیع دچار قطعی می‌شود به‌صورت جزیره‌ای وارد عمل شوند و خاموشی‌های تحمیلی به مشترکین را به مقدار قابل‌ملاحظه‌ای کاهش دهند [۲].

با توجه به پیچیدگی‌های استفاده از منابع تولید پراکنده در شبکه‌های توزیع استفاده از شبکه‌هایی با قابلیت‌های رؤیت پذیری، پایش، کنترل و حفاظت هوشمند اجتناب‌ناپذیر است.

شبکه هوشمند انرژی الکتریکی شبکه‌ای است که جریان دوسویه انرژی الکتریکی و اطلاعات را با کمک بسترهای مخابراتی با قابلیت جمع‌آوری اطلاعات، پایش، پردازش و کنترل فراهم می‌کند. از اهداف ایجاد این شبکه کاهش هزینه‌ها و افزایش راندمان است. هم‌چنین افزایش قابلیت اطمینان هم از موارد مهم در این نوع شبکه‌ها بوده و توجه ویژه‌ای به این موضوع می‌شود. از مزایای شبکه هوشمند می‌توان به قابلیت خودترمیمی، مشارکت

مصرف‌کنندگان و کاهش آلودگی‌های زیست‌محیطی بر اساس امکان استفاده حداکثری از منابع تولید پراکنده تجدید پذیر اشاره نمود [۳].

فنّاوری‌های شبکه هوشمند استفاده از اتوماسیون و ارتباط داده‌ها را از طریق تجهیزات مخابراتی هوشمند در سیستم‌های بزرگ قدرت فراهم می‌سازند. شبکه هوشمند یک شبکه سایبر– قدرت (Cyber-power) است که از دو جز متمایز شبکه سایبری و شبکه قدرت تشکیل‌شده است. هر شبکه استانداردها و پروتکل‌های خاص خود را دارد و به‌وسیله قوانین فیزیکی مربوط به خود اداره می‌شود [۴].

درصورتی‌که به‌کارگیری از شبکه سایبری در سیستم‌های قدرت افزایش یابد، خرابی‌های مربوط به تجهیزات هوشمند و تأثیر آن‌ها بر روی سیستم قدرت به یک مسئله جدی تبدیل می‌شود. گزارش خاموشی‌ها تأیید می‌کند که عملکرد نادرست تجهیزات شبکه سایبری مانند کنترل، پایش و حفاظت عوامل مهمی در پایین آمدن سطح قابلیت اطمینان و پایداری شبکه قدرت هستند. ازاین‌رو در مطالعات ارزیابی ریسک شبکه‌های هوشمند باید راهکارهایی در نظر داشت که اثرات خطاهای شبکه سایبری بر روی شبکه قدرت پوشش داده شود [۵].

ارتباط میان دو شبکه به‌طورکلی به این معناست که عملکرد صحیح و مناسب یکی از اجزای سیستم به وجود و کارکرد صحیح اجزای دیگر شبکه بستگی دارد. یک خرابی در شبکه سایبری ممکن است از جهات گوناگون بر شبکه قدرت تأثیرگذار باشد [۶]. ارتباط میان دو شبکه سایبری و قدرت می‌تواند به دو صورت مستقیم و غیرمستقیم تعریف شود که بر اساس چگونگی تأثیرگذاری بر روی اجزا شبکه قدرت بیان می‌شود.

تأثیر ارتباط غیرمستقیم بر روی قابلیت اطمینان سیستم قدرت متفاوت و پیچیده‌تر از ارتباط از نوع مستقیم است. ارتباط غیرمستقیم به معنای خرابی گروهی از المان‌ها در یک شبکه است که به‌طور آنی و مستقیم باعث خرابی و یا تغییر رفتار المان در شبکه دیگر نشوند. اما این خرابی بر روی عملکرد اجزا مدار در خرابی‌های احتمالی بعدی تأثیرگذار است. با توجه به این تعریف، خرابی‌های نامعلوم و پنهان جز ارتباط‌های غیرمستقیم قرار می‌گیرند [۷].

مرجع [۶, ۸] به بررسی و تعریف ارتباط میان شبکه سایبری و قدرت پرداخته است. در مقاله ذکرشده نیاز به شبکه سایبری در شبکه هوشمند را مورد بررسی قرار می‌دهد. سپس در ادامه حالت‌های مختلف نگاشت خطا از شبکه سایبری به شبکه قدرت را بیان می‌کند. بر این اساس چهار نوع ارتباط میان دو شبکه تعریف‌شده وجود دارد. البته لازم به ذکر است مراجع [۶, ۸] به بیان کیفی اصول و مفاهیم کلی ارتباط بین شبکه‌های سایبری و قدرت پرداخته و راه حلی برای محاسبه کمی شاخص‌های قابلیت اطمینان شبکه‌های هوشمند ارائه نکرده‌اند.

برای مطالعات کمی شاخص‌های ارزیابی ریسک شبکه‌های هوشمند با در نظرگیری خطاهای شبکه سایبری از مراجع [۷, ۹] می‌توان نام برد. روش بیان‌شده در این مراجع با یکدیگر مشابه بوده و تفاوت آن‌ها در نوع ارتباط میان دو شبکه سایبری و قدرت است. هم‌چنین منابع تولید پراکنده مورد استفاده در مراجع فوق از نوع قابل کنترل و با ظرفیت ثابت می‌باشد.

مرجع [۷] مفهوم ارتباط مستقیم را معرفی می‌کند و دو نوع از این ارتباط را بررسی می‌کند. اولین نوع ارتباط المان به المان مستقیم است که در نقاطی تعریف می‌شود که دو شبکه سایبری و قدرت را به هم متصل می‌کند. دومین ارتباط، ارتباط شبکه– المان است. این حالت زمانی رخ می‌دهد که خرابی در شبکه مخابراتی ویژگی‌های تجهیزات در شبکه قدرت را تغییر می‌دهد. نگاشت حالات که در این مقاله به آن اشاره شده است برای ارزیابی قابلیت اطمینان سیستم‌های Cyber-power که ارتباط مستقیم در آن‌ها مطرح است استفاده می‌شود.

۲.کاربردهای ارتباط غیرمستقیم در تجهیزات سیستم قدرت

در این بخش دو کاربرد از ارتباط غیرمستقیم در شبکه هوشمند که شامل مانیتورینگ (پایش) و حفاظت است معرفی خواهد شد.

۲.۱. سیستم‌های مانیتورینگ(پایش)

سیستم‌های مانیتورینگ (پایش) در شبکه قدرت به جمع‌آوری و گزارش دهی انواع داده‌ها به مراکز کنترل محلی و دور (Remote) سیستم قدرت می‌پردازد. این سیستم‌ها فرصت پیش‌بینی، دریافت، انجام عکس‌العمل‌های سریع در برابر خطاهای احتمالی را فراهم می‌آورد، درنتیجه این کار به کاهش نرخ خرابی و زمان تعمیر می‌انجامد [۱۰].

سیستم‌های مانیتورینگ شرایط سالم کار پایدار شبکه، وضعیت تجهیزات سیستم و ولتاژ باس‌ها را بررسی می‌کنند. هم‌چنین به تحلیل اطلاعات ثبت‌شده، فرستادن آن‌ها به مرکز کنترل و دریافت دستورات از سرورهای شبکه هوشمند می‌پردازند [۱۱].

۲.۲. سیستم‌های حفاظتی

خطاها در سیستم‌های قدرت شرایط نامطلوب را نشان می‌دهد که به دلیل خرابی تجهیز و یا حوادث طبیعی مانند صاعقه رخ می‌دهد. موضوعی

که حائز اهمیت بوده شناسایی و برطرف نمودن خرابی‌های سیستم است. هم‌چنین بتواند به‌طور مناسبی نسبت به آن عکس‌العمل نشان دهد. سیستم‌های حفاظت معمولاً از رله‌های حفاظتی و شبکه‌های مخابراتی داده تشکیل شده‌اند. که وجود آن‌ها برای عملکرد تجهیزات حفاظتی ضروری است [۱۲].

خرابی‌ها در بیشتر نقاط سیستم‌های حفاظت تا زمانی که اغتشاشی در شبکه قدرت رخ ندهد نامعلوم می‌ماند مانند اتصال کوتاه یا اضافه بار که در آن خرابی‌های پنهان مشخص می‌شود و باعث بیرون رفتن تجهیز مرتبط با آن می‌شود. وجود خرابی‌های پنهان در سیستم‌های حفاظت قابلیت اطمینان سیستم را کاهش می‌دهد [۱۳].

۲.۳. انواع ارتباط غیرمستقیم

۱. ارتباط غیرمستقیم المان به المان (IEEI): موقعی وجود خواهد داشت که خرابی‌ها بر روی تجهیزات شبکه سایبری که به‌طور فیزیکی به تجهیز قدرت متصل هستند رخ بدهد. به‌طور مثال اگر خرابی در تجهیز مانیتورینگ و یا حفاظت رخ دهد، باعث می‌شود عنصر قدرتی که به آن متصل است از کار بیفتد.

۲. ارتباط غیرمستقیم شبکه– المان (INEI): زمانی وجود خواهد داشت که خرابی‌ها بر روی المان‌های شبکه سایبری که به‌طور مستقیم به شبکه قدرت متصل هستند رخ نمی‌دهد. این نوع ارتباط در درون شبکه سایبری اتفاق می‌افتد و بر روی عملکرد المان قدرت در برابر خرابی احتمالی تأثیرگذار است. به‌طور نمونه اگر داده‌ی مخابراتی که حاوی اطلاعات از سرور مربوطه است به تجهیز مانیتورینگ و یا حفاظت نرسد منجر به عمل نکردن عنصر مربوطه در زمان لازم می‌شود [6].

بر این اساس روش تحلیلی ارزیابی قابلیت اطمینان برای این مسئله جهت مدل‌سازی ارتباط غیرمستقیم میان شبکه سایبری و قدرت پیشنهاد می‌شود. ایده و فرمولاسیون به‌روز رسانی حالت‌ها ناشی از خرابی‌ها در شبکه سایبری ارائه‌شده است. با درنظرگیری به‌روز رسانی حالات خرابی، تحلیل دو شبکه به‌هم‌پیوسته امکان‌پذیر می‌شود.

۳.فرمولاسیون مسئله

۳.۱. ارتباط سایبر– قدرت غیرمستقیم

در ارتباط غیرمستقیم، لینک سایبر– قدرت به‌وسیله رابطه (۱) نشان داده می‌شود.

$$\Gamma = (\gamma : \delta) \qquad (۱)$$

که نشان دهنده یک ارتباط غیرمستقیم میان عنصر سایبری γ و تجهیز شبکه قدرت δ است. رابطه (۱) به این معناست که اگر المان سایبری γعمل نکند و یا اطلاعات داده‌های ارسالی را دریافت نکند، بر روی عملکرد تجهیز قدرت در برابر خرابی احتمالی تأثیر خواهد گذاشت. در ابتدا فرض می‌شود که المان سایبری به‌طور مناسبی کار کند، در دسترس‌پذیری تجهیز قدرت با درنظرگیری عملکرد المان سایبری به‌صورت رابطه (۲) بیان می‌شود.

$$A_\delta = \frac{\mu_\delta}{\lambda_\delta + \mu_\delta} \qquad (۲)$$

که در آن λ_δ و μ_δ به ترتیب نرخ خرابی و نرخ تعمیر می‌باشند.

حال زمانی که ارتباط غیرمستقیم میان γ و δ وجود داشته باشد. اگر المان سایبری از کار بیفتد، نرخ خرابی و نرخ تعمیر المان قدرت δ به ترتیب برابر $\hat{\lambda}$ و $\hat{\mu}$ خواهد شد. با خرابی المان سایبری نرخ خرابی عنصر قدرت افزایش می‌یابد و مقدار نرخ تعمیر کم می‌شود. به طور مشابه، دردسترس پذیری المان قدرت δ بدون عملکرد عنصر سایبری γ در رابطه (۳) محاسبه‌شده است.

$$\hat{A}_\delta = \frac{\hat{\mu}_\delta}{\hat{\lambda}_\delta + \hat{\mu}_\delta} \qquad (۳)$$

به بیانی دیگر، ارتباط غیرمستقیم موجود میان عنصر سایبری γ و تجهیز قدرت δ در دسترس‌پذیری المان قدرت δ را در صورت عدم عملکرد صحیح المان سایبری γ از مقدار A_δ به $\hat{A}_\delta$ کاهش می‌دهد.

۳.۲. ارزیابی قابلیت اطمینان شبکه سایبر– قدرت با در نظرگیری ارتباط غیرمستقیم

روش پیشنهادی دارای سه مرحله است. در مرحله اول جدول احتمال حالات (P-table) تولید می‌شود. در مرحله دوم، به‌روز رسانی احتمال حالات مختلف با استفاده ار روش تحلیلی انجام می‌شود تا مقدار نرخ خرابی و نرخ تعمیر یک المان در شبکه قدرت متناسب با تأثیرپذیری آن از تجهیز

سایبری به‌روز شود. درواقع حالاتی که در آن‌ها ارتباط شبکه سایبری و قدرت وجود دارد احتمال آن‌ها تغییر می‌کند. بعد از این مرحله، مقدار بار قطع شده (LC) در سیستم قدرت برای تمامی حالات ممکن محاسبه می‌شود. بر اساس مقادیر بار قطع شده کل، شاخص‌های قابلیت اطمینان سیستم اندازه‌گیری می‌شوند. در ادامه هرکدام از این مراحل به‌صورت کامل توضیح داده می‌شود.

تشکیل P-table:

اساس الگوریتم پیشنهادی پیدا نمودن بارزدایی پیش‌بینی‌شده در شبکه سایبر- قدرت است. به این منظور اطلاعات مورد نیاز باید از حالات مختلف سیستم جمع‌آوری‌شده و در P-table ثبت شود. جدول احتمال از سه جز تشکیل می‌شود: شاخص i، حالات سیستم ϕ_i و احتمال حالات Pr_{ϕ_i} . هر حالت ϕ_i یک آرایه باینری است که در آن هر المان در دسترس بودن و یا نبودن یک حالت تجهیز را در شبکه سایبری و قدرت بیان می‌کند. (رابطه۴)

$$\phi_i = (\phi_{i,1}, \phi_{i,2}, \ldots, \phi_{i,N_c}, \ldots, \phi_{i,N_c+N_p}) \qquad (۴)$$

که در آن $\phi_{i,k}$ وضعیت المان k در حالت i می‌باشد. اگر $\phi_{i,k}=0$ باشد، آنگاه المان k در حالت i در شرایط کارکرد صحیح خود است. اگر $\phi_{i,k}=1$ باشد، المان k در حالت i خراب (عدم عملکرد صحیح) است. با توجه به این‌که شبکه سایبر و قدرت به ترتیب دارای N_c و N_p المان است، طول ϕ_i برابر N_c+N_p است. زمانی که تمام المان‌ها دوحالته فرض شوند، احتمال حالت i ام از رابطه (۵) محاسبه می‌شود [۱۴].

$$Pr_{\phi_i} = \prod_{k=1}^{N_c+N_p} A_k^{(1-\phi_{i,k})} U_k^{\phi_{i,k}} \qquad (۵)$$

در رابطه بالا، A_k و U_k به ترتیب نشان دهنده در دسترس پذیری و در دسترس‌ناپذیری المان k ام می‌باشد.

به‌روز رسانی حالات

به‌روز رسانی حالات زمانی اتفاق می‌افتد که یک خرابی در یک المان شبکه سایبری بر روی عملکرد تجهیز قدرت در برابر خرابی‌های احتمالی در شبکه قدرت تأثیرگذار باشد.

زمانی که یک خرابی در عنصر مخابراتی رخ می‌دهد، مقادیر نرخ خرابی و نرخ تعمیر تجهیزات قدرت مربوط به آن تغییر می‌کنند و باید به‌روز رسانی شوند. در صورت عدم عملکرد یک عنصر در شبکه مخابراتی مقدار نرخ خرابی تجهیز قدرت بالا رفته و نرخ تعمیر پایین می‌آید. خرابی عنصر مخابراتی سبب می‌شود دو حالت مطابق جدول (۱) به‌وجود بیاید.

جدول ۱: حالات ارتباط غیرمستقیم شبکه سایبری و قدرت

ϕ_i	خرابی در هر دو عنصر شبکه سایبری و قدرت رخ داده است.	$\phi_{i,\gamma}=1$ ، $\phi_{i,\delta}=1$
ϕ_j	خرابی در عنصر شبکه سایبری رخ داده است ولی در شبکه قدرت رخ نداده است.	$\phi_{j,\gamma}=1$ ، $\phi_{j,\delta}=0$

اگر خرابی در عنصر سایبری تاثیری بر روی نرخ خرابی و تعمیر تجهیز شبکه قدرت نداشته باشد، احتمال حالتی که هر دو عنصر خراب شوند برابر است با:

$$Pr_{\phi_i} = U_\gamma \times \frac{\lambda_\delta}{\lambda_\delta + \mu_\delta} \qquad (۶)$$

که در رابطه بالا U_γ برابر عدم دسترس پذیری عنصر سایبری γ است. هم‌چنین احتمال حالت دوم نیز مطابق با رابطه (۷) بدست می‌آید.

$$Pr_{\phi_j} = U_\gamma \times \frac{\mu_\delta}{\lambda_\delta + \mu_\delta} \qquad (۷)$$

از طرفی دیگر زمانی که ارتباط غیرمستقیم میان المان سایبری و عنصر قدرت وجود داشته باشد، احتمال حالتی که هر دو عنصر به طور همزمان خراب باشند برابر است با:

$$Pr^{new}_{\phi_i} = U_\gamma \times \frac{\hat{\lambda}_\delta}{\hat{\lambda}_\delta + \hat{\mu}_\delta} \qquad (۸)$$

و

$$Pr^{new}_{\phi_j} = U_\gamma \times \frac{\hat{\mu}_\delta}{\hat{\lambda}_\delta + \hat{\mu}_\delta} \qquad (۹)$$

با مقایسه روابط (۶) و (۸) و با در نظرگیری $\hat{\lambda}_\delta > \lambda_\delta$ و $\hat{\mu}_\delta < \mu_\delta$ می‌توان نتیجه گرفت که $Pr^{new}_{\phi_i} > Pr_{\phi_i}$ است. هم‌چنین می‌توان گفت که احتمال خراب شدن دو عنصر γ و λ از دوشبکه، زمانی که ارتباط غیرمستقیم میان آن‌ها وجود دارد نسبت به زمانی که دو عنصر از هم مستقل هستند (رابطه‌ای میان آن‌ها وجود ندارد) محتمل‌تر است.

اختلاف میان دو رابطه (۶) و (۸) به وسیله به روز رسانی حالت مورد نظر مدل می‌شود.

$$Pr^{new}_{\phi_i} = Pr_{\phi_i} + \varsigma \times Pr_{\phi_j} \qquad (۱۰)$$

که در رابطه (۱۰)، پارامتر ς بیان کننده ضریب به روز رسانی حالت است. حال اگر در معادله بالا مقادیر هریک از طرفین را جایگذاری کنیم می‌توان معادله (۱۱) را بدست آورد.

$$U_\gamma \times \frac{\hat{\lambda}_\delta}{\hat{\lambda}_\delta + \hat{\mu}_\delta} = U_\gamma \times \frac{\lambda_\delta}{\lambda_\delta + \mu_\delta} + \varsigma \times U_\gamma \times \frac{\mu_\delta}{\lambda_\delta + \mu_\delta} \qquad (۱۱)$$

از معادله بالا می‌توان مقدار ς را بدست آورد.

$$\varsigma = \frac{\hat{\lambda}_\delta(\lambda_\delta+\mu_\delta)}{(\hat{\lambda}_\delta+\hat{\mu}_\delta)\mu_\delta} - \frac{\lambda_\delta}{\mu_\delta} \quad (۱۲)$$

با توجه به این که $\lambda_\delta << \mu_\delta$ و $\hat{\lambda}_\delta << \hat{\mu}_\delta$ می‌توان رابطه بالا را به صورت معادله (۱۳) بیان نمود.

$$\varsigma \approx \frac{\hat{\lambda}_\delta}{\hat{\mu}_\delta} - \frac{\lambda_\delta}{\mu_\delta} \quad (۱۳)$$

با توجه به رابطه بالا اگر خرابی در شبکه سایبری مقادیر نرخ تعمیر و خرابی درشبکه قدرت را تغییر ندهد، آنگاه $\varsigma = 0$ خواهد بود.

در نهایت $\Pr^{new}_{\phi_j}$ برابر می شود با:

$$\Pr^{new}_{\phi_j} = (1-\varsigma)\times \Pr_{\phi_j} \quad (۱۳)$$

در مرحله بعدی باید اتصال‌های عناصر مختلف با یکدیگر بررسی شود و حالات خرابی عناصر مخابراتی و چگونگی تاثیر آن‌ها بر روی تجهیزات قدرت مورد ارزیابی قرار گیرد. سپس بر اساس آن می‌توان عملیات مربوط به به‌روز رسانی حالات خرابی تجهیزات سیستم قدرت را انجام داد.

خرابی‌هایی که ناشی از سیستم مانیتورینگ (پایش) هستند اثرات متفاوتی نسبت به سیستم حفاظت دارند. در ادامه و در بررسی موردی شبکه نمونه این موارد مورد بحث قرار می‌گیرد.

در مرحله بعد میزان بارزدایی بارها باید لحاظ شود. با استفاده از تعادل تولید و مصرف می‌توان میزان بارزدایی را محاسبه نمود.

$$\sum P_G = \sum P_{load} \quad (۱۴)$$

در گام آخر می‌توان با استفاده از احتمال حالات و محاسبه میزان بارزدایی شاخص‌های قابلیت اطمینان سیستم را محاسبه نمود.

از دو شاخص LOLP و EENS جهت ارزیابی ریسک شبکه قدرت استفاده می‌شود. این شاخص‌ها به صورت زیر محاسبه می‌شوند [۷].

$$EENS = \sum_i P_{r_{\phi_i}} . LC_i^T \quad (۱۵)$$

$$LOLP = \sum_i P_{r_{\phi_i}} . \mathrm{sgn}(LC_i^T) \quad (۱۶)$$

در روابط بالا LC_i^T مجموع بارزدایی در حالات مختلف است.

EENS به معنای انرژی موردانتظار تامین نشده است. (برحسب مگاوات ساعت) LOLP به معنای احتمال از دست دادن بار(بر حسب درصد) است.

۴.پیاده‌سازی روش بر روی شبکه نمونه

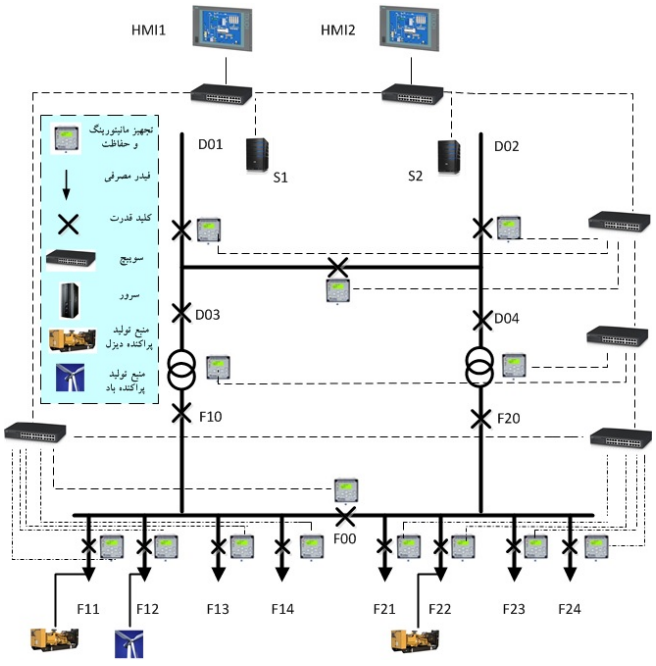
شکل(۱) یک پست فوق توزیع نمونه ۲۳۰/۶۳ کیلوولت با ساختار H را نشان می‌دهد [۱۱]. در این ساختار یک بریکر به هر کدام از خطوط ۲۳۰ کیلوولت و ترانس‌های مربوطه اختصاص داده می‌شود. در سطح ولتاژ ۶۳ کیلوولت، برای هر کدام از فیدرهای خروجی نیز یک بریکر درنظرگرفته می‌شود. جدول (۲) اجزای پست فوق توزیع را بیان می‌کند.

جدول ۲: اجزای پست فوق توزیع [۱۱]

بی (Bay)	معرفی
D01,D02	فیدر ورودی ۲۳۰ کیلوولت،۲۰۰MVA،۱۰۰km
D00	باس کوپلر ۲۳۰kv
D03,D04	کلید قدرت سمت HV ترانس
F10,F20	کلید قدرت سمت LV ترانس
F00	باس کوپلر۶۳ kv
F11,F12,F13,F14,F21,F22,F23,F24	فیدرهای خروجی ۶۳kv ، ۵۰MVA

تجهیزات مانیتورینگ در این پست نصب شده‌اند و تمامی اندازه‌گیری‌ها، حوادث و اغتشاشات به واحدهای پایش، کنترل و هم‌چنین حفاظت فرستاده می‌شوند.

در سیستم قدرت تمامی بریکرها، ترانسفورمرها و خطوط انتقال دارای نرخ خرابی غیرصفر هستند. علاوه بر آن، در سیستم مخابراتی نیز تمامی سوییچ-ها، تجهیزات حفاظتی و پایش نیز دارای احتمال خرابی می‌باشند. در جدول (۳) و(۴) به طور نمونه و برای استفاده در شبیه سازی این قسمت مقادیر نوعی آورده شده است.



شکل ۱: پست فوق توزیع نمونه [۱۱]

مدارشکن‌ها نیاز به سیستم پایش جهت عملکرد مطمئن و جلوگیری از خرابی‌های احتمالی دارند. فشار گاز و تعداد دفعات عملکرد دو عامل مهمی هستند که نیاز به سیستم پایش و کنترل دارند [۱۱].

. جدول ۳: نرخ خرابی و تعمیر اجزای سیستم قدرت

تجهیزات	اختصار	نرخ خرابی	نرخ تعمیر
مدارشکن	-B	۰.۰۳۷	۲۹۲
ترانسفورمر	-T	۰.۰۶۸	۱۳۵.۹
فیدرهای خروجی	-L	۱	۳۹۲

جدول ۴: نرخ خرابی و تعمیر اجزای سیستم سایبری

تجهیزات	اختصار	نرخ خرابی	نرخ تعمیر
واحدهای حفاظتی	.P	۰.۵	۲۹۲
واحدهای پایش	.M	۱	۲۹۲
سوییچ	.C	۰.۵	۲۹۲

جدول (۵) دو لینک ارتباطی میان عنصر مخابراتی D04 و عنصر قدرت متناظر با آن مانند مدارشکن D04-B و ترانسفورمر D04-T را نشان می‌دهد. ارتباط‌های مشابهی می‌تواند میان بریکرها و ترانس‌های دیگر و تجهیزات مانیتورینگ متناظر با آن‌ها تعریف شود.

جدول ۵: ارتباط میان تجهیز مانیتورینگ و سیستم قدرت [۱۱]

$(\gamma:\delta)$	$\hat{\lambda}_\delta / \lambda_\delta$	$\hat{\mu}_\delta / \mu_\delta$
(D04.M:D04-B)	۸.۱۳	۰.۵۳
(D04.M:D04-T)	۱.۴۷	۰.۵۴

سیستم حفاظت برای خطوط و ترانسفورمرهای ۲۳۰ کیلوولت، رله‌های حفاظتی اصلی و پشتیبان درنظرگرفته می‌شوند. رله حفاظت اصلی فیدرهای خروجی ۶۳ کیلوولت را محافظت می‌کند. اگر یک خطایی رخ دهد، رله‌ها عمل کرده تا امنیت سیستم را تامین نمایند.

خرابی تجهیزات مانیتورینگ و حفاظت مربوط به رله‌ها باعث می‌شود رله پشتیبان و یا رله بالادستی عمل کند. در صورت عمل نمودن رله بالادستی، فیدرهای بیشتری از مدارخارج می‌شوند. بنابراین نرخ خرابی فیدرهای مجاور افزایش می‌یابد. برای مثال در شکل (۱) اگر یک اتصال کوتاهی در فیدر F23 رخ دهد و رله این فیدر از مدار خارج شده باشد، رله بالادستی آن یعنی F20 عمل خواهد کرد و بریکر سمت ثانویه ترانس را قطع می‌کند. در نتیجه تمامی فیدرهای مجاور F21,F22,F24 بی برق می‌شوند. این به معنای آن است که نرخ خرابی این فیدرها به طور غیرمستقیم به دلیل خرابی تجهیز حفاظتی فیدر دیگر افزایش یافته است. مشابه همین حالت F12.P ارتباط غیرمستقیمی با F11-L, F13-L, F14-L دارد. جدول (۶) ارتباط میان عناصر مخابراتی و تجهیز حفاظتی متناظر را نشان می‌دهد.

جدول ۶: ارتباط میان تجهیز حفاظتی و سیستم قدرت

$(\gamma:\delta)$	$\hat{\lambda}_\delta / \lambda_\delta$	$\hat{\mu}_\delta / \mu_\delta$
(F11.P:F12-L)	۲	۱
(F11.P:F13-L)	۲	۱
(F11.P:F14-L)	۲	۱

در نتیجه برای ارزیابی قابلیت اطمینان این شبکه سایبر– قدرت، ضریب به‌روز رسانی حالت ς برای تمامی حالات باید محاسبه شود. به طور مثال ضریب به روز رسانی برای حالتی که D04.M منجر به خرابی D04-B می‌شود به صورت زیر محاسبه می‌گردد.

با استفاده از رابطه اصلی (۱۲):

$$\varsigma = \frac{8.13*0.037*(0.037+292)}{(8.13*0.037+0.53*292)*292} - \frac{0.037}{292} = 0.001813$$

و با استفاده از رابطه تقریبی (۱۳):

$$\varsigma = \frac{8.13*0.037}{0.53*292} - \frac{0.037}{292} = 0.001817$$

با مقایسه اعداد بدست آمده از دو رابطه بالا تفاوت چندانی میان آن‌ها دیده نمی‌شود. به همین دلیل از رابطه تقریبی به دلیل سادگی محاسبات استفاده می‌شود.

ارزیابی قابلیت اطمینان سیستم مورد بحث در چند حالت عملکردی بررسی می‌شود و شاخص‌های تعریف شده برای آن‌ها محاسبه خواهد شد.

سناریو۱: این سناریو یک حالت پایه است که در آن سیستم قدرت به طور کامل از تجهیزات مانیتورینگ و حفاظت بهره می‌برد. در این حالت فرض می‌شود که این تجهیزات دارای نرخ خرابی نیستند.

سناریو۲: خرابی احتمالی تنها در سیستم مانیتورینگ درنظرگرفته می‌شود. تمامی بخش‌های دیگر شبکه مخابراتی بدون خرابی فرض می‌شوند.

سناریو۳: در این حالت خرابی احتمالی تنها در سیستم حفاظتی درنظرگرفته شده و بقیه تجهیزات بدون نرخ خرابی فرض می‌شوند.

سناریو۴: در سناریو آخر تجهیزات مانیتورینگ و حفاظت احتمال خرابی دارند و برای هر دو نرخ خرابی جداگانه تعریف می‌شود.

نتایج شبیه‌سازی در جدول (۷) محاسبه شده است.

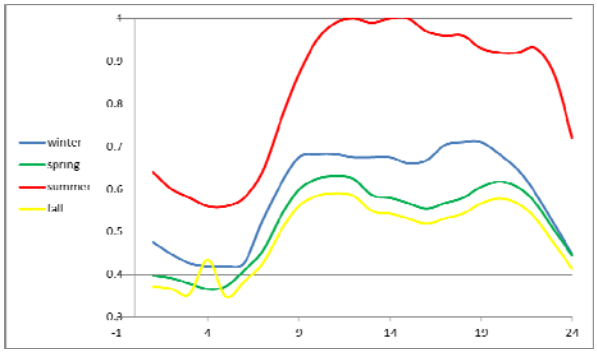
جدول ۷: شاخص‌های قابلیت اطمینان در شرایط مختلف

سناریو	LOLP(%)	EENS(P.U)	LOLP inc.%	EENS inc.%
۱ (سالم بودن)	۰.۲۲۸۰	۰.۰۲۳۶۵	–	–
۲ (خرابی در M)	۰.۲۳۳۲	۰.۰۲۴۰۸	۲	۱.۸
۳ (خرابی در P)	۰.۲۳۳۳	۰.۰۲۴۲۳	۲	۲.۴
۴ (خرابی در M و P)	۰.۲۳۸۵	۰.۰۲۴۷۵	۴.۶	۴.۵۶

با مقایسه نتایج در سناریوهای مختلف مشاهده می‌شود:

وجود تجهیزات مانیتورینگ و حفاظت برای سیستم های سایبر- قدرت امری ضروری به نظر می‌رسد و منجر به افزایش قابلیت اطمینان سیستم می-شود. خرابی در سیستم حفاظت نسبت به خرابی در سیستم مانیتورینگ شاخص EENS را بیشتر تحت تاثیر قرار می‌دهد. (وضعیت را بدتر می‌کند.) دلیل این امر آن است زمانی که سیستم حفاظتی از کار می افتد، خرابی‌ها در فیدرهای مجاور را نتیجه می‌دهد که این باعث بی برقی در مشترکین زیادی می‌شود. هم‌چنین خرابی در تجهیزات مانیتورینگ، LOLP را بیشتر خراب می‌کند. هم‌چنین ستون چهارم و پنجم از جدول (۷) میزان افزایش مقادیر شاخص‌ها را نسبت به حالت پایه که سناریو اول است نشان می‌دهد.

در مرحله بعدی DG های بادی و دیزلی را وارد مدار کرده و تحلیل قابلیت اطمینان را در حضور منابع تولید پراکنده انجام می‌دهیم. در این قسمت بارهای مصرفی را هم به صورت متغیر مطابق با منحنی بار ساعتی در یک شبانه روز درنظرگرفته می‌شود.



شکل ۲: منحنی بارگیری روزانه برای فصول مختلف در یک روز نمونه [۱۵]

منابع تولید پراکنده دیزلی دارای ظرفیت توانی ۹۰۰ کیلووات بوده که در فیدرهای F11 و F22 قرار دارند. این منابع دارای ظرفیت توانی ثابت بوده و دارای شاخصه احتمالاتی نیستند. منبع تولید پراکنده بادی نیز دارای توان نامی ۷۰۰ کیلووات بوده و دارای مشخصه توان احتمالاتی می‌باشد که مطابق با آنچه بیان شد میزان توان آن در ساعات مختلف محاسبه می‌شود. DG های ذکر شده خود دارای نرخ خرابی نیز هستند [۱۶, ۱۷].

مطابق با جدول (۸) در سه حالت مختلف می‌توان تحلیل قابلیت اطمینان را انجام داد. حالت اول تنها منبع دیزلی در مدار باشد. حالت دوم تنها منبع تولید پراکنده بادی در مدار وجود داشته باشد. در حالت آخر نیز از دو منبع فوق به صورت هیبریدی در شبکه استفاده می‌شود.

تحلیل نتایج جدول (۸) به صورت زیر می‌باشد.

۱.در حالتی که قرار است از منبع تولید پراکنده تجدیدپذیر مانند توربین بادی استفاده شود، به دلیل مشخصه احتمالاتی آن بهتر است از یک منبع با ظرفیت تولید ثابت مانند دیزل ژنراتور و با میکروتوربین نیز در کنار آن نصب شود تا قابلیت اطمینان سیستم در حد مطلوبی باقی بماند.

۲.استفاده از منابع تولید پراکنده قابل کنترل و تجدیدپذیر در سیستم قدرت که در این‌جا یک پست فوق توزیع مورد بررسی قرار گرفت، سبب می‌شود تا قابلیت اطمینان سیستم بهبود یابد.

جدول ۸: شاخص‌های قابلیت اطمینان در حضور DGها و بارمصرفی متغیر

حالت بهره‌برداری	EENS(P.U)	LOLP(%)
دیزل ژنراتور	۰.۰۷۳۶	۰.۱۹۲۷
توربین بادی	۰.۰۹۵۹	۰.۱۹۳۰
هیبریدی (دیزل+باد)	۰.۰۸۴۳	۰.۱۹۰۷

۵.نتیجه گیری:

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 روش جدیدی برای درنظرگیری ارتباط شبکه سایبری با شبکه قدرت پیشنهاد شده است. ارتباط ذکر شده میان این دو شبکه از نوع غیرمستقیم بوده و با مدل نمودن آن و به روز رسانی حالات جدید زمانی که خرابی در شبکه سایبری رخ می‌دهد می‌توان تحلیل قابلیت اطمینان سیستم قدرت را به نحو مطلوبی انجام داد. شبکه نمونه‌ای که بر روی آن روش پیشنهادی پیاده سازی شده است یک پست فوق توزیع می-باشد که خرابی‌های سیستم مانیتورینگ و حفاظت در آن درنظرگرفته شده است. نتایج نشان می‌دهند که خرابی در این سیستم ها قابلیت اطمینان سیستم قدرت را کاهش می‌دهد.

قابلیت اطمینان سیستم‌های قدرت با استفاده از به کارگیری تجهیزات مانیتورینگ و حفاظت بهبود می‌یابد. هر کدام از این تجهیزات می‌توانند اثرات متفاوتی بر روی شاخص‌های قابلیت اطمینان سیستم داشته باشند. به همین دلیل با استفاده از شاخص‌های عددی به ارزیابی بهبود چنین حالاتی پرداخته شد. هم‌چنین در حالتی که در شبکه قدرت منابع تولید پراکنده وجود داشته باشد و بار مصرفی متغیر در فیدرها درنظرگرفته شود، قابلیت

اطمینان سیستم بهبود یافته و تحلیل در سناریوهای مختلف نشان دهنده توجه به انواع مختلف DG ها در بهبود شرایط با درنظرگیری شبکه سایبری می‌باشد.

۶.منابع

[1] C. J. Dent, A. Hernandez-Ortiz, S. R. Blake, D. Miller, and D. Roberts, "Defining and Evaluating the Capacity Value of Distributed Generation," *Power Systems, IEEE Transactions on,* vol. PP, pp. 1-9, 2014.

[2] S. Elsaiah, M. Benidris, and J. Mitra, "Analytical approach for placement and sizing of distributed generation on distribution systems," *Generation, Transmission & Distribution, IET,* vol. 8, pp. 1039-1049, 2014.

[3] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart Grid; The New and Improved Power Grid: A Survey," *Communications Surveys & Tutorials, IEEE,* vol. 14, pp. 944-980, 2012.

[4] 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), IEEE 38th Annual*, , pp. 529-534, 2014.

[5] M. Al-Muhaini and G. T. Heydt, "Evaluating Future Power Distribution System Reliability Including Distributed Generation," *Power Delivery, IEEE Transactions on,* vol. 28, pp. 2264-2272, 2013.

[6] B. Falahati and F. Yong, "A study on interdependencies of cyber-power networks in smart grid applications," in *Innovative Smart Grid Technologies (ISGT), IEEE PES*, pp. 1-8, 2012.

[7] B. Falahati, F. Yong, and W. Lei, "Reliability Assessment of Smart Grid Considering Direct Cyber-Power Interdependencies," *Smart Grid, IEEE Transactions on,* vol. 3, pp. 1515-1524, 2012.

[8] Y. Yang, T. Littler, S. Sezer, K. McLaughlin, and H. F. Wang, "Impact of cyber-security issues on Smart Grid," in *Innovative Smart Grid Technologies (ISGT Europe), 2011 2nd IEEE PES International Conference and Exhibition on*, pp. 1-7, 2011.

[9] B. Falahati and F. Yong, "Reliability Assessment of Smart Grids Considering Indirect Cyber-Power Interdependencies," *Smart Grid, IEEE Transactions on,* vol. 5, pp. 1677-1685, 2014.

[10] O. Gomez, C. Portilla, and M. A. Rios, "Reliability Analysis of Substation Monitoring Systems Based on Branch PMUs," *Power Systems, IEEE Transactions on,* vol. 30, pp. 962-969, 2015.

[11] B. Falahati, F. Yong, and M. J. Mousavi, "Reliability Modeling and Evaluation of Power Systems With Smart Monitoring," *Smart Grid, IEEE Transactions on,* vol. 4, pp. 1087-1095, 2013.

[12] M. G. Lauby, J. J. Bian, and A. D. Slone, "State of bulk power system reliability," in *Power and Energy Society General Meeting (PES), IEEE*, pp. 1-5, 2013.

[13] "Reliability fundamentals of system protection," *NERC, Report to the Planning Committee,* Dec. 2010.

[۱۴] امیررضا حسنی اهنگر، حامد هاشمی، حسین عسکریان ابیانه, "آنالیز حساسیت تاثیر سیستم سایبری (کنترل، مانیتورینگ و حفاظت) نسبت به ضریب نفوذ منابع تولید پراکنده بر روی قابلیت اطمینان شبکه های هوشمند," نهمین کنفرانس تخصصی حفاظت و کنترل سیستم های قدرت, ۲۰۱۵.

[۱۵] امیررضا حسنی آهنگر، حامد هاشمی، حسین عسکریان ابیانه, "بررسی اثرات منفی احتمالی سیستم سایبری (کنترل، پایش و حفاظت) بر قابلیت اطمینان شبکه‌های هوشمند با افزایش ضریب نفوذ منابع تولید پراکنده تجدیدپذیر بادی*(EPDC)* ", بیستمین کنفرانس توزیع برق.۲۰۱۵.

[۱۶] ابوالفضل صدقی، محمد مهدی قاسمی‌پور، مریم رمضانی, "ارزیابی قابلیت اطمینان سیستم مستقل باد/فتوولتائیک/دیزل/ذخیره ساز در حضور خودروهای الکتریکی*(PSC)* "،بیست و هشتمین کنفرانس بین المللی برق.۱۳۹۲.

[۱۷] داریوش یزدان پناه، کاظم عاملی، مصطفی عیدیانی, "ارزیابی اثرات اضافه شدن ۵۰۰ مگاوات واحد جدید بادی در شبکه خراسان از نقطه نظر قابلیت اطمینان و پایداری شبکه ", *(PSC)*بیست و هشتمین کنفرانس بین المللی برق ۱۳۹۲ .