

ارائه شاخصی برای ارزیابی امنیت شبکه قدرت با استفاده از تئوری مجموعه فازی

رضا غفارپور^{۱*}، علی اصغر پورموسی^۲، علی محمد رنجبار^۳

۱- مربی دانشگاه امام حسین(ع) ۲- کارشناسی ارشد دانشگاه صنعتی امیرکبیر ۳- استاد دانشگاه صنعتی شریف

(دریافت: ۹۴/۰۱/۲۴، پذیرش: ۹۴/۱۰/۳۰)

چکیده

هدف از این مقاله، ارائه شاخصی برای ارزیابی امنیت شبکه قدرت بعد از حملات تروریستی بر روی تجهیزات شبکه با استفاده از تئوری مجموعه فازی می‌باشد. برای رسیدن به این هدف، از یک روش مبتنی بر تئوری احتمال و تئوری امکان استفاده شده است. در گام اول، با استفاده از روش بی‌زین که یک روش مبتنی بر تئوری احتمالات است، میزان احتمال حمله و همچنین میزان ریسک ناشی از فعالیت‌های تروریستی بر روی تجهیزات سامانه قدرت محاسبه شده و تجهیزات سامانه بر اساس این میزان ریسک رتبه‌بندی شدند. در گام دوم، با به‌کارگیری پخش بار فازی و یافتن پارامترهای فازی مرتبط با عملکرد شبکه، میزان تأثیر از دست رفتن هر یک از تجهیزات رتبه‌بندی شده در گام اول بر روی شبکه قدرت مورد بررسی قرار گرفت. در نهایت با محاسبه میزان ریسک ناشی از حمله به تجهیزات شبکه، شاخصی برای ارزیابی امنیت سامانه قدرت ارائه شده است. همچنین به منظور ارزیابی کارایی روش پیشنهاد شده، شاخص امنیت برای یک شبکه خاص محاسبه شد.

کلید واژه‌ها: شبکه قدرت، ارزیابی امنیت، تئوری احتمال، تئوری امکان، شبکه بی‌زین، پخش بار فازی

Presenting an Index for Evaluation of Power Network Security Using Fuzzy Set Theory

R. Gaffarpour^{*}, A. A. Pourmusa, A. M. Ranjbar

Imam Hossein University

(Received: 13/04/2015; Accepted: 20/01/2016)

Abstract

The purpose of this paper is to present an index for evaluation of power network security after terrorist attacks against the network facilities using fuzzy set theory. In order to achieve this goal, a method based on probability and possibility theory is used. In the first step, by using Bayesian network which is a method based on probability theory, the probability of the attack as well as the risk value caused by terrorist activities against the power network facilities was calculated and the network facilities were ranked according to the level of the risk. In the second step, by employing fuzzy load flow and finding the fuzzy parameters related to network performance, the impact of the loss of each component ranked in the first step on power network was investigated. Finally, having calculated the risk value caused by terrorist attacks against the network facilities, an index was provided for evaluating power network security. Also, in order to validate the effectiveness of the proposed method, security index for a specific network was calculated.

Keywords: Power Network, Security Assessment, Probabilities Theory, Possibility Theory, Bayesian Network, Fuzzy Load Flow

* Corresponding Author E-mail: rghaffarpour@ihu.ac.ir

۱. مقدمه

سامانه قدرت شامل مجموعه‌ای از شبکه‌ها و تجهیزات است که علاوه بر ارائه خدمات به مشتریان در سطح گسترده، برای یک جامعه و اقتصاد آن ضروری و حیاتی است. به دلیل وابستگی مراکز و زیرساخت‌های حیاتی^۱ یک کشور به شبکه برق، هر عاملی که باعث ایجاد اختلال در این شبکه شود می‌تواند باعث بروز خسارت‌های عمده به سایر زیرساخت‌های حیاتی یک کشور شود. اختلال بر اثر عوامل طبیعی، خطای انسانی، خطای تجهیزات و حملات فیزیکی و سایبری^۲ توسط گروه‌های تروریستی از مهم‌ترین عوامل هستند که باعث آسیب‌پذیری سامانه قدرت می‌شوند. از میان عوامل فوق، حمله تروریستی که به صورت سازمان یافته و با هدف ایجاد بیشترین آسیب به تجهیزات سامانه قدرت صورت می‌گیرد از اهمیت بسیار بالایی برخوردار است.

در مطالعات مربوط به امنیت سامانه قدرت، معمولاً پیش‌بینی دقیق تولید و تقاضای بار به دلیل اینکه به طور مستقیم یا غیرمستقیم از عوامل مختلفی که دارای درجات مختلف عدم قطعیت هستند تأثیر می‌پذیرد، مشکل است. این عدم قطعیت می‌تواند ناشی از عدم پیش‌بینی دقیق تقاضای بار ناشی از شرایط آب و هوایی، جمعیت منطقه، تولید ناخالص ملی، تعرفه برق و یا به دلیل آسیب رسیدن به تجهیزات شبکه قدرت ناشی از حوادث گوناگون مانند تهدیدات نظامی به ویژه وقوع حملات تروریستی باشد که این امر ضرورت در نظر گرفتن مسئله عدم قطعیت در میزان تولید و مصرف بار را نشان می‌دهد. بنابراین، اگر در مطالعات مربوط به امنیت شبکه برق، مقادیر تولید و تقاضای بار به صورت قطعی در نظر گرفته شود مانند آنچه که در روش‌های احتمالاتی انجام می‌شود، در این صورت تمام حالت‌های عدم قطعیت مربوط به این مقادیر نادیده گرفته شده و در نتیجه ممکن است منجر به بروز خطا در مدل‌سازی سامانه قدرت شود.

به طور کلی برای مدل‌سازی شبکه برق در مطالعات مربوط به امنیت سامانه قدرت در هنگام وقوع حملات عمدی مانند حملات تروریستی دو روش می‌توان پیشنهاد کرد که هدف نهایی این روش‌ها محاسبه میزان ریسک ناشی از این حملات بر روی تجهیزات شبکه است. مورد اول، مبتنی بر تئوری احتمالات بوده که در آن با استفاده از روش‌های مختلف مانند شبکه بیزین، ابتدا احتمال وقوع حمله به هر یک از تجهیزات سامانه قدرت محاسبه شده و سپس با در نظر گرفتن تأثیر این حملات بر روی عملکرد شبکه قدرت و همچنین میزان خسارات وارده به سامانه ناشی از

این حملات، میزان ریسک برای هر یک از تجهیزات به طور جداگانه محاسبه می‌شود. بنابراین این روش این امکان را فراهم می‌کند که از میان تجهیزات گوناگون سامانه قدرت که می‌تواند مدنظر تروریست‌ها برای حمله باشد، مهم‌ترین این تجهیزات را شناسایی کرده و آن‌ها را بر اساس میزان ریسک یعنی میزان خطرات بالقوه‌ای که از جانب تروریست‌ها این تجهیزات را تهدید می‌کند رتبه‌بندی نماید. با این وجود، این روش که مبتنی بر احتمالات است روش کامل و جامعی برای تعیین مقدار ریسک نمی‌باشد، چرا که در روش مبتنی بر تئوری احتمالات، محاسبه میزان ریسک بر مبنای حساسیت و میزان تأثیرگذاری هر یک از تجهیزات شبکه بر روی سامانه قدرت که بر پایه احتمالات بوده و همچنین بر اساس تجربه اپراتورها و استفاده از روش‌هایی مانند آنالیز پخش بار صورت می‌گیرد. بنابراین، از آنجایی که پارامتر حساسیت در پروسه تعیین مقدار ریسک تأثیرگذار است، طبیعی است که مقدار به‌دست آمده برای میزان ریسک از دقت بالایی برخوردار نباشد.

روش دوم مبتنی بر تئوری امکان یا تئوری مجموعه فازی است. بر خلاف روش اول که در آن میزان تولید و مصرف بار شبکه در آنالیز پخش بار به صورت قطعی و مشخص در نظر گرفته می‌شود، در روش دوم، میزان تولید و مصرف دارای درجه‌ای از عدم قطعیت است. در این روش با استفاده از پخش بار فازی و با تعیین پارامترهای عملکردی سامانه بر اساس تئوری مجموعه فازی، میزان ریسک سامانه برای هر یک از حوادث پیش‌بینی نشده ناشی از حملات تروریستی که منجر به آسیب دیدن تجهیزات شبکه برق می‌گردد محاسبه می‌شود.

در زمینه مطالعات امنیت سامانه قدرت با استفاده از تئوری احتمال و تئوری فازی تاکنون تحقیقات مختلفی انجام شده است. ارزیابی امنیت زیرساخت‌های الکتریکی و به طور خاص پست‌های برق با تعریف سناریوهای مختلف حمله مورد بررسی قرار گرفته و روشی برای محاسبه میزان آسیب ناشی از این حملات ارائه شده است [۱]. در نهایت راهکارهایی برای مقاوم‌تر کردن پست‌ها در برابر حملات تروریستی سایبری پیشنهاد شده است. آسیب‌های ناشی از حملات تروریستی بر روی سامانه قدرت نیز بررسی شده و راهکارهایی برای حفاظت مؤثر از تجهیزات سامانه در برابر تهدیدات تروریستی ارائه شده است [۲]. از طرف دیگر، راهکارهایی پیشنهاد شده است که توسط آن‌ها اپراتورها قادرند تجهیزات سامانه را از نظر میزان ریسک اولویت‌بندی کرده و با ارائه روش‌هایی برای حفاظت تجهیزات در برابر حملات، میزان ریسک ناشی از این حملات را کاهش می‌دهد [۳]. روشی نیز

¹ Critical Infrastructure

² Physical and Cyber Attacks

ابتدا احتمال وقوع حملات به هر یک از مؤلفه‌های سامانه قدرت با استفاده از شبکه بیزین محاسبه شده و تجهیزات سامانه بر اساس میزان ریسک رتبه‌بندی (اولویت‌بندی) می‌شوند. سپس هر یک از این مؤلفه‌ها به ترتیب اولویت از شبکه خارج شده و برای باقی‌مانده شبکه، پخش بار فازی انجام می‌شود. با استفاده از این پخش بار، پارامترهای سامانه مانند دامنه ولتاژ، زاویه ولتاژ، پخش توان عبوری از خطوط و... در حالت فازی به دست می‌آیند. سپس با استفاده از نتایج پخش بار، پارامترهای عملکردی سامانه بر اساس تئوری مجموعه فازی تعیین شده و میزان ریسک برای هر یک از حالت‌های خروج مؤلفه‌ها از شبکه ناشی از حملات تروریستی محاسبه می‌شود. در نهایت با در نظر گرفتن میزان احتمال حمله به مؤلفه‌ها که توسط شبکه بیزین به دست آمده است، میزان ریسک نهایی که در واقع نشان‌دهنده شاخصی برای امنیت سامانه قدرت است، تعیین می‌گردد.

۱-۱. تئوری مجموعه فازی

در یک مجموعه فازی که مانند هر مجموعه دیگری شامل تعدادی عنصر می‌باشد، هر عنصر دارای یک درجه عضویت نسبت به این مجموعه است که این درجه عضویت متناظر با عددی بین صفر و ۱ است. بنابراین می‌توان گفت یک مجموعه فازی تابعی است که در آن هر عنصر مجموعه دارای یک درجه عضویت متناظر با آن عنصر می‌باشد. به طور کلی می‌توان یک مجموعه فازی را به عنوان تعمیمی از مفهوم مجموعه کلاسیک در نظر گرفت که در آن تابع عضویت تنها دو مقدار صفر یا ۱ را اختیار می‌کند. در مجموعه فازی هر چه درجه عضویت به عدد ۱ نزدیک‌تر باشد، میزان اطمینان (میزانی که به یقین نزدیک‌تر است تا احتمال) برای عنصری که در مجموعه قرار دارد بیشتر است و برعکس هر چه درجه عضویت به عدد صفر نزدیک‌تر باشد، این میزان اطمینان کمتر است. بر این اساس می‌توان مجموعه فازی \bar{a} را به صورت زیر تعریف کرد [۱۳]:

$$\bar{a} = \left\{ \left(x, \mu_{\bar{a}}(x) \right) \mid x \in X \right\} \quad (1)$$

در رابطه بالا، $\mu_{\bar{a}}$ تابع عضویت بوده و x دامنه این تابع است. باید توجه داشت که برخلاف مجموعه‌های مبتنی بر قطعیت که در آن هر عنصر می‌تواند به مجموعه تعلق داشته باشد یا نداشته باشد، در یک مجموعه فازی بخشی از عنصر می‌تواند متعلق به مجموعه باشد و در عین حال متمم (بخش باقی‌مانده) آن به مجموعه تعلق نداشته باشد.

برای ارزیابی امنیت شبکه‌های هوشمند^۱ با استفاده از نظریه بازی‌ها^۲ ارائه شده است [۴]. در این روش، با به‌کارگیری تئوری گیم و با استفاده از روش‌های مدیریت ریسک و ترکیب آن با اقدامات حفاظتی، امنیت سامانه مورد ارزیابی قرار گرفته و در نهایت مناسب‌ترین راهبردها به منظور مقابله با حملات تروریستی برای کاهش ریسک ارائه می‌شود. در تحقیقی دیگر [۵]، با استفاده از تئوری بیزین-گیم و با طرح چندین سناریو مربوط به جمع‌آوری اطلاعات در مورد سامانه قدرت، به نقش اطلاعات و داده‌ها بر روی آنالیز ریسک ناشی از حملات بر روی سامانه قدرت پرداخته شده است. با استفاده از روش فازی^۳ شاخصی برای امنیت سایبری زیرساخت‌های حیاتی از جمله زیرساخت‌های الکتریکی ارائه شده است [۶]. با به‌کارگیری روش فازی، شاخصی برای پایداری گذرای سامانه قدرت به منظور ارزیابی امنیت آن پیشنهاد شده است [۷]. در تحقیقی دیگر [۸]، ارزیابی امنیت ولتاژ در شرایط دینامیکی با ارائه شاخص شدت با استفاده از تئوری مجموعه فازی انجام شده است. رتبه‌بندی حوادث پیش‌بینی نشده در سامانه قدرت برای ارزیابی امنیت شبکه برق مشخص شده است [۹]. همچنین، روشی برای ارزیابی امنیت شبکه قدرت با استفاده از روش فازی دینامیکی و تعریف شاخصی برای ریسک شبکه ارائه شده است [۱۰]. ارزیابی ریسک هنگام وقوع حوادث پی‌درپی در شبکه قدرت بر اساس تئوری مجموعه فازی مورد بحث و بررسی قرار گرفته است [۱۱]. در تحقیقی دیگر [۱۲]، الگوریتمی برای ارزیابی قابلیت اطمینان سامانه قدرت بر پایه روش فازی ارائه شده است.

روشی که در این مقاله برای محاسبه ریسک در مطالعات مربوط به امنیت سامانه قدرت پیشنهاد می‌شود، ترکیبی از تئوری احتمال و تئوری امکان است. بر اساس این روش، در گام اول با استفاده از روش بیزین که مبتنی بر تئوری احتمالات است، ابتدا میزان احتمال حمله به هر یک از تجهیزات سامانه قدرت محاسبه شده و سپس این تجهیزات بر اساس میزان ریسک ناشی از حملات تروریستی رتبه‌بندی می‌شوند. در گام دوم با استفاده از پخش بار فازی و با تعیین پارامترهای عملکردی سامانه بر اساس تئوری مجموعه فازی و همچنین با در نظر گرفتن میزان احتمال حمله که در گام اول به دست آمده است، شاخصی برای ریسک به منظور ارزیابی امنیت شبکه قدرت ارائه می‌شود. بنابراین، با در نظر گرفتن گام‌های فوق می‌توان روش پیشنهادی در این مقاله را به صورت زیر بیان کرد:

¹ Smart Grid
² Game Theory
³ Fuzzy Method

۱-۲. اعداد فازی

باید توجه داشت که ضرب دو عدد فازی LR را نمی‌توان به عنوان یک عدد فازی LR در نظر گرفت. بنابراین در اینجا از فرمول‌های تقریبی برای نشان دادن ضرب دو عدد فازی LR استفاده می‌شود. در نتیجه برای $\tilde{a}_1 \tilde{a}_2 > 0$ ، تقریب مماسی و متقاطع برای ضرب دو عدد فازی LR به ترتیب به صورت زیر بیان می‌شود:

$$\begin{aligned} \tilde{a}_1 \tilde{a}_2 &\approx (m_1 m_2, m_1 \alpha_2 + m_2 \alpha_1, m_1 \beta_2 + m_2 \beta_1)_{LR} \\ \tilde{a}_1 \tilde{a}_2 &\approx (m_1 m_2, m_1 \alpha_2 + m_2 \alpha_1 - \alpha_1 \alpha_2, m_1 \beta_2 + m_2 \beta_1 + \beta_1 + \beta_2)_{LR} \end{aligned} \quad (۴)$$

تئوری امکان^۳: به طور کلی اساس و پایه اعداد فازی و منطق فازی را تئوری امکان می‌نامند. تئوری امکان در واقع ابزاری برای مدل‌سازی عدم قطعیت می‌باشد. این تئوری اساساً به منظور ارزیابی و تجزیه و تحلیل موضوعاتی که اطلاعات ناقصی از آن‌ها در اختیار است مورد استفاده قرار می‌گیرد. اگر S مجموعه جهانی^۴ باشد و x یک توصیف نامشخصی از حالت یک مسئله باشد که مقداری را در S اختیار می‌کند، آنگاه برای هر مقدار s مربوط به متغیر x در حوزه S یک مقدار $\pi_x(s)$ وجود دارد که نشان دهنده درجه امکان گزاره $x=s$ است. همچنین، مقدار کمینه این توزیع برابر با عدد صفر و مقدار بیشینه آن برابر با عدد ۱ است. تابع $\pi_x(s)$ متناظر با میزان اطلاعات و دانش ما در مورد یک موضوع خاص می‌باشد. به عبارتی دیگر این تابع بیانگر این مطلب است که امکان وقوع یک حالت از امکان وقوع حالتی دیگر تا چه اندازه بیشتر یا کمتر می‌باشد. بنابراین می‌توان تابع $\pi_x(s)$ را به صورت زیر بیان کرد:

$$\begin{cases} \pi_x(s) = 0 & x = s \\ \pi_x(s) = 1 & x = s \end{cases} \quad (۵)$$

در رابطه بالا مورد اول بیان می‌کند که امکان وقوع پیشامد مورد نظر غیر ممکن است. رابطه دوم نیز بیانگر این مطلب است که امکان وقوع پیشامد مورد نظر به طور کامل وجود دارد.

توزیع امکان در واقع نوع خاصی از تئوری مجموعه فازی است. بر این اساس می‌توان یک توزیع امکان را با استفاده از اعداد فازی نشان داد. ارتباط بین تابع عضویت یک عدد فازی \tilde{a} و توزیع امکان به صورت زیر نشان داده می‌شود:

$$\mu_a(s) = \pi_x(s) \quad \forall s \in S \quad (۶)$$

درجه امکان وقوع پیشامد A که زیرمجموعه مجموعه S است به صورت زیر بیان می‌شود:

اعداد فازی^۱ در واقع یک مجموعه فازی \tilde{a} می‌باشد که بر اساس مقادیر تقریبی‌ای متناظر با اعداد حقیقی R بیان شده و این مقادیر در بازه صفر تا ۱ قرار دارند. این اعداد دارای شکل‌های مختلفی می‌باشند که این شکل‌ها متناظر با واقعیت حاکم بر مسئله می‌باشد. به عنوان مثال در مسئله مربوط به پخش بار، مقدار غیر قطعی پارامترهای سامانه می‌تواند با استفاده از عدد فازی نشان داده شود. به طور مثال می‌توان در مورد انتقال توان از خط انتقال یک سامانه قدرت به این صورت اظهار نظر کرد: مقادیر کمینه توان انتقالی از خط احتمالاً از ۵۰ مگاوات کمتر نمی‌شود و مقدار بیشینه آن نیز از ۸۰ مگاوات تجاوز نمی‌کند. همچنین بهترین تخمین برای توان عبوری از خط مورد نظر بین ۶۲ تا ۶۸ مگاوات خواهد بود.

پایاده‌سازی (مدل‌سازی) اعداد فازی: به طور کلی برای پایاده‌سازی اعداد فازی روش‌های مختلفی وجود دارد که در این بین می‌توان به اعداد فازی گسسته، اعداد فازی LR^2 ، اعداد فازی تجزیه شده، روش تبدیل و ... اشاره کرد. در این مقاله از اعداد فازی LR که نسبت به سایر روش‌ها دارای کاربرد بیشتری است استفاده می‌شود [۸-۶].

اعداد فازی LR : اعداد LR به عنوان طبقه‌ای از اعداد فازی هستند که در آن تابع عضویت توسط یک تابع افزایشی چپ (L) و یک تابع کاهش‌ی راست (R) شکل می‌گیرد. به طور کلی عدد فازی LR به صورت معادله زیر بیان می‌شود:

$$(m, \alpha, \beta) = \tilde{a}(x) = \begin{cases} L\left(\frac{m-x}{\alpha}\right) & x \leq m, \quad \alpha > 0 \\ R\left(\frac{x-m}{\beta}\right) & x > m, \quad \beta > 0 \end{cases} \quad (۷)$$

همان‌طور که مشاهده می‌شود، معادله بالا شامل دو تابع و سه مقدار اسکالر می‌باشد. در اینجا m نشان دهنده مقدار مد، α توزیع چپ و β توزیع راست است. اکنون با معلوم بودن دو عدد فازی LR و با استفاده از اصول بسط، عملگرهای جمع، تفریق و ضرب برای این اعداد به صورت زیر می‌باشد:

$$\begin{aligned} \tilde{a}_1 &= (m_1, \alpha_1, \beta_1)_{LR} & \tilde{a}_2 &= (m_2, \alpha_2, \beta_2)_{LR} \\ \tilde{a}_1 + \tilde{a}_2 &= (m_1 + m_2, \alpha_1 + \alpha_2, \beta_1 + \beta_2)_{LR} \\ -\tilde{a}_1 &= (m_1, \alpha_1, \beta_1)_{LR} \end{aligned} \quad (۸)$$

³ Possibility Theory

⁴ Universal Set

¹ Fuzzy Number

² Left-Right

بنابراین اگر بخواهید یک توصیف کلی از اعداد فازی داشته باشید می‌توان گفت که اعداد فازی در واقع اختصاص مقادیر صحیح مختلف به یک اظهار نظر کلی است. به عنوان مثال، تزریق توان در فرمول پخش بار می‌تواند بر اساس اعداد فازی مدل‌سازی شود. به عبارتی دیگر، می‌توان میزان بار شبکه را عددی مانند x یا مقدار پیک بار را عددی بین y و z در نظر گرفته و در این حالت آن‌ها را با استفاده از اعداد فازی مدل‌سازی و بر اساس توابع امکان بیان کرد. به عنوان یک نتیجه‌گیری کلی از این بخش می‌توان گفت که در مسائل مختلف، تئوری امکان زمانی جایگزین تئوری احتمال می‌شود که نیاز باشد وقوع یک پیشامد را در حالتی که اطلاعات چندان دقیقی از سامانه و گذشته آن در اختیار نیست و یا اینکه اطلاعات به صورت کمی کفایت اما از لحاظ کیفی چندان مطلوب نیست ارزیابی نماید.

تاکنون برای مدل‌سازی بحث عدم قطعیت در مورد میزان تولید و تقاضا، روش‌های مختلفی پیشنهاد شده‌اند که بیشتر بر پایه تئوری احتمال، تئوری امکان و اعداد فازی و برخی روش‌های ریاضی دیگر است. پخش بار مبتنی بر احتمال، اولین اقدام برای مدل‌سازی عدم قطعیت در زمینه تولید و تقاضا بود [۱۴]. در این روش از متغیرهای تصادفی با توزیع احتمال برای مدل‌سازی مسئله میزان تولید و تقاضا استفاده شد. نتایج به‌دست آمده از این روش توزیع احتمال مربوط به ولتاژ و پخش توان شبکه را نشان می‌دهد. روش دیگری که بعد از مدت‌ها ارائه شد، روش مبتنی بر پخش بار فازی بود که در این روش از اعداد فازی با تابع امکان^۱ مناسب برای مدل‌سازی مسئله میزان تولید و تقاضا استفاده شد. از مهم‌ترین این روش‌ها می‌توان به پخش بار فازی با استفاده از پخش بار DC [۱۵]، پخش بار AC فازی با استفاده از روش‌های مختلف مانند روش خطی، غیرخطی و چندخطی [۱۶] و [۱۷] اشاره کرد.

معادلات مربوط به مسئله پخش بار فازی معادلاتی غیر خطی هستند که شامل متغیرهای ورودی (توان اکتیو و راکتیو تزریقی به گره‌ها)، متغیرهای کنترلی (تولید توان اکتیو و دامنه ولتاژ در باس‌های PV ، تنظیم تپ ترانس، جبران‌سازی توان راکتیو و ...)، متغیرهای حالت (دامنه و فاز ولتاژ در باس‌های PQ و فاز ولتاژ تولیدی در باس‌های PV) و متغیرهای خروجی مانند پخش توان اکتیو و راکتیو می‌باشند. در پخش بار فازی، متغیرهای ورودی که شامل توان اکتیو و راکتیو تولیدی و مصرفی هستند به‌عنوان اعداد فازی می‌باشند که در واقع مدل‌کننده وجود عدم قطعیت در این متغیرها است. این مدل‌سازی می‌تواند به عنوان مثال، میزان انحراف این متغیرها از مقدار مرکزی را مدل کند. به همین

$$\Pi(A) = \sup_{s \in A} \pi_s(s) \quad \forall s \in S \quad (7)$$

لازم به یادآوری است که تئوری امکان وابسته به تئوری احتمال می‌باشد اما متفاوت با آن است. در تئوری احتمال وقوع یک پیشامد A دارای مقدار $p(A)$ است و بنابراین احتمال عدم وقوع پیشامد برابر با $1 - p(A)$ می‌باشد. این مسئله در مورد تئوری امکان صحیح نمی‌باشد. در واقع اگر امکان وقوع A را با $\pi(A)$ نشان دهید، آنگاه امکان عدم وقوع آن ممکن است از $1 - \pi(A)$ بیشتر باشد.

۲. روش پیشنهادی

۲-۱. پخش بار فازی

روش پیشنهادی در این مقاله، مبتنی بر پخش بار با به‌کارگیری روش فازی است که بر اساس آن عملکرد سامانه قدرت با در نظر گرفتن وقوع حملات تروریستی بر روی تجهیزات شبکه قدرت مورد ارزیابی قرار می‌گیرد. بر اثر هر یک از این حملات که منجر به آسیب به تجهیزات شبکه قدرت می‌گردد بالطبع نتایجی بر اثر از دست رفتن تجهیزات آسیب دیده برای شبکه قدرت در پی دارد. هدف ما از به‌کارگیری پخش بار فازی، بررسی نتایج ناشی از تأثیرات تجهیزات آسیب دیده بر اثر حملات تروریستی بر روی سامانه قدرت می‌باشد.

در واقع پخش بار فازی با در نظر گرفتن معیارهای عملکردی سامانه قدرت انجام می‌شود. این معیارها همان مواردی هستند که سامانه قدرت با توجه به این معیارها در حالت نرمال قرار دارد مانند حد مجاز ولتاژ و یا مقدار مجاز توان عبوری از یک خط. از طرفی دیگر، بحث عدم قطعیت در میزان تولید و تقاضا یکی از مهم‌ترین مسائل در مطالعات پخش بار است. بنابراین مدل‌سازی دقیق این عدم قطعیت به ما این امکان را می‌دهد که بتوان اثرات تولید و تقاضا را در عملکرد و توسعه سامانه قدرت و همچنین امنیت شبکه مورد ارزیابی قرار داد.

در مسئله پخش بار متداول، تزریق توان اکتیو و راکتیو در هر گره، با استفاده از مقادیر قطعی و معین مدل می‌شود. مسئله اصلی که در اینجا با آن مواجه هستید این است که، پیش‌بینی دقیق بار به دلیل اینکه به طور مستقیم یا غیر مستقیم از عوامل با درجات مختلف عدم قطعیت تأثیر می‌پذیرد، مشکل است. این عدم قطعیت می‌تواند ناشی از عواملی مانند شرایط آب و هوایی، مصرف بار روزانه و هفتگی، جمعیت منطقه، تولید ناخالص ملی، شاخص‌های قیمت، تعرفه برق و... باشد. در این میان، تئوری فازی چارچوبی است که توسط آن می‌توان انواع مسائل مربوط به عدم قطعیت را مدل‌سازی کرد. به ویژه منطق فازی این امکان را می‌دهد تا بتوان مواردی که از نظر عددی مبهم بوده و اطلاعات دقیقی از آن‌ها در اختیار ندارید را به خوبی مدل‌سازی کنید.

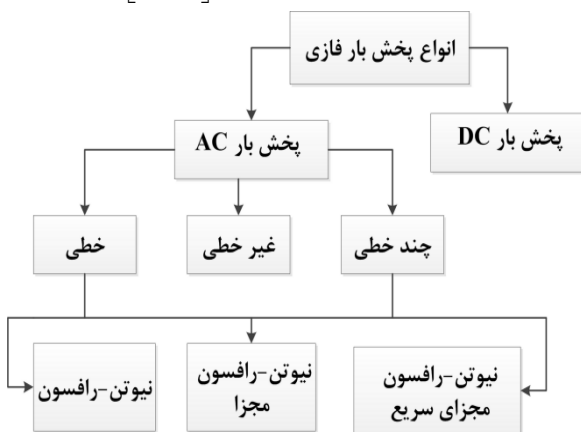
^۱ Possibility Function

تمامی این روش‌ها، اعداد فازی به برش‌های α تجزیه می‌شوند. در این مقاله از روش پخش بار AC استفاده می‌شود.

پخش بار AC فازی [۲۰ و ۲۱]: در این بخش، هدف از پخش بار AC فازی، مدل‌سازی عدم قطعیت مرتبط با توان اکتیو و راکتیو تزریقی به شبکه است. بنابراین طبیعی است که نتایج حاصل از این پخش بار که شامل دامنه و فاز ولتاژ، توان اکتیو و راکتیو عبوری از خط و ... است نیز به صورت فازی باشند. به طور کلی پخش بار AC فازی را می‌توان به صورت زیر پیاده‌سازی کرد:

الف. در گام اول، با استفاده از رابطه (۱۰)، مقدار پیش‌بینی شده (قطعی) برای توان اکتیو و راکتیو تزریقی به شبکه به‌دست می‌آید. در این معادله، CV اپراتوری است که بر اساس آن مقادیر میانی توان اکتیو P^{ctr} و راکتیو Q^{ctr} مربوط به توان فازی تزریقی به شبکه یعنی \bar{P} و \bar{Q} به‌دست می‌آید.

$$\begin{bmatrix} P^{ctr} \\ Q^{ctr} \end{bmatrix} = \begin{bmatrix} CV(\bar{P}) \\ CV(\bar{Q}) \end{bmatrix} \quad (10)$$



شکل ۳. انواع روش‌های پخش بار فازی

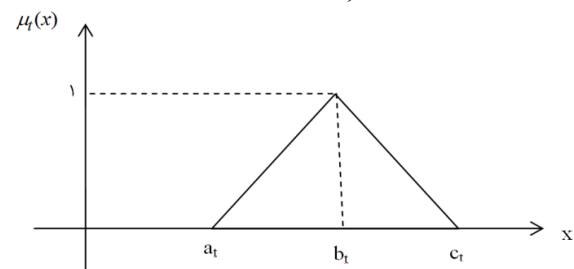
ب. با استفاده از مقادیر میانی به‌دست آمده در بخش (الف)، یک پخش بار معمولی (غیرفازی) با استفاده از روش نیوتون-رافسون انجام می‌شود. نتایج حاصل از این پخش بار، به‌دست آمدن مقادیر پیش‌بینی شده برای دامنه و فاز ولتاژ (V^{ctr} و δ^{ctr})، توان اکتیو و راکتیو عبوری از خط (P_{ij}^{ctr} و Q_{ij}^{ctr}) و ... است.

ج. با استفاده از ماتریس ژاکوبین که از آخرین تکرار پخش بار نیوتون-رافسون در بخش (ب) به‌دست آمده است، مقادیر فازی انحراف دامنه ولتاژ (ΔV) و انحراف فاز ولتاژ ($\Delta \delta$) مطابق با رابطه (۱۱) محاسبه می‌شود.

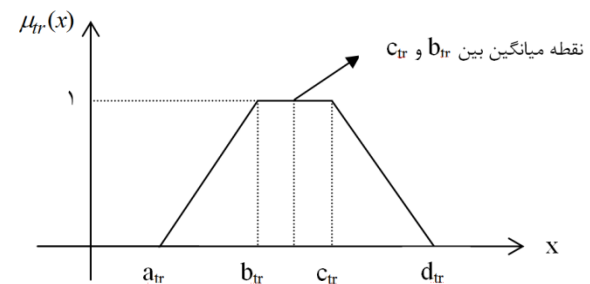
منظور، شکل‌های گوناگونی از اعداد فازی مانند تابع مثلثی^۱ (معادله ۸)، دوزنقه‌ای^۲ (معادله ۹) (شکل‌های ۱ و ۲) و ... می‌تواند مورد استفاده قرار گیرد [۱۸].

$$\mu_t(x, a_t, b_t, c_t) = \max\left(\min\left(\frac{x-a_t}{b_t-a_t}, \frac{c_t-x}{c_t-b_t}\right), 0\right) \quad (8)$$

$$\mu_{tr}(x, a_{tr}, b_{tr}, c_{tr}, d_{tr}) = \max\left(\min\left(\frac{x-a_{tr}}{b_{tr}-a_{tr}}, \frac{d_{tr}-x}{d_{tr}-c_{tr}}, 1\right), 0\right) \quad (9)$$



شکل ۱. تابع مثلثی



شکل ۲. تابع دوزنقه‌ای

از میان این روش‌ها، روش دوزنقه‌ای بیشتر از سایر روش‌ها مورد استفاده قرار می‌گیرد. مقادیر پارامترهای اعداد فازی بر اساس دانش و اطلاعات موجود از پخش بار سامانه حاصل می‌شود. به عنوان مثال، در بازه‌ای که شامل تمامی مقادیر ممکن برای تزریق توان به شبکه می‌باشد، مقدار پیش‌بینی شده برای تزریق توان یا نقطه میانگین نقطه‌ای است که تابع امکان در آن نقطه دارای مقدار ۱ است. این نقطه همان‌طور که در معادله‌های (۸) و (۹) نشان داده شده است، برای تابع مثلثی برابر با b_t و برای تابع دوزنقه‌ای برابر با مقدار میانگین بین b_{tr} و c_{tr} است [۱۹]. همچنین این نقاط در شکل‌های (۱) و (۲) نیز نشان داده است.

در پخش بار فازی، نتایج حاصل از پخش بار، بردار اعداد فازی مربوط به دامنه و فاز ولتاژ می‌باشند. در شکل (۳) انواع روش‌های ممکن برای پخش بار فازی نشان داده شده است. در

¹ Triangular

² Trapezoidal

بنابراین می‌توان با استفاده از بسط تیلور حول نقطه کار سامانه (مقدار قطعی‌ای که با استفاده از پخش بار به دست آمده است)، اعداد فازی این متغیرها را نیز به دست آورد.

روش پیشنهادی برای حل پخش بار فازی: در بخش قبلی، معادله‌های مربوط به پخش بار AC فازی مورد بحث و بررسی قرار گرفت. بنابراین، در این مرحله لازم است یک منطق فازی برای حل این معادله‌ها ارائه شود. در این مقاله از روش اعداد فازی LR برای حل مسئله پخش بار استفاده می‌شود. در روش اعداد فازی LR که در بخش قبل نیز توضیح داده شد، نیازی به گسسته‌سازی نبوده و در نتیجه لازم نیست که مسئله را در بازه‌های مختلف مورد بررسی قرار دهید. این روش بیشتر برای پخش بار DC و پخش بار AC خطی مورد استفاده قرار می‌گیرد. علاوه بر این، این نوع از اعداد فازی دارای محدودیت‌هایی نیز هستند. به عنوان مثال، هنگام جمع بستن، اعداد فازی باید دارای شکل‌های یکسان بوده و برای کم کردن اعداد فازی از یکدیگر، این اعداد باید تقریباً متقارن باشند.

۲-۲. محاسبه پارامترهای عملکردی سامانه

در بخش قبلی، پخش بار فازی به منظور به دست آوردن اعداد فازی مربوط به ولتاژ باس‌ها و پخش توان خطوط پس از وقوع یک حمله تروریستی و جدا کردن مؤلفه آسیب دیده از شبکه مورد بحث و بررسی قرار گرفت. بر این اساس، با استفاده از نتایج حاصل از این شبیه‌سازی می‌توان پارامترهای عملکردی سامانه را با در نظر گرفتن شرایط مختلف محاسبه کرد. در این مقاله، عملکرد سامانه قدرت در حالت کاهش ولتاژ و اضافه بار خطوط مورد بررسی قرار می‌گیرد.

شرایط کاهش ولتاژ: تابع امکان مربوط به ولتاژ در هر باس به عنوان یک عدد فازی که توسط پخش بار فازی تعیین می‌شود، به صورت زیر بیان می‌شود:

$$\pi_V(x) = \mu_V(x), \quad \forall x \in X \quad (20)$$

در معادله بالا، X تمام مقادیر ممکن ولتاژ یک باس بوده و $\mu_V(x)$ درجه عضویت نسبت به عدد فازی \tilde{V} است. در این مقاله، مقادیر ممکن برای شرایطی که ولتاژ باس i پایین‌تر از مقدار مجازش باشد با رابطه (۲۱) نشان داده می‌شود:

$$\Pi_j^{LV}(x) = \max(\pi_{V_j}(x \leq 0.95)) \quad \forall x \in X \quad (21)$$

با استفاده از رابطه (۲۱)، بیشینه مقدار ممکن برای مقادیر ولتاژ کمتر از $0.95 pu$ می‌تواند به دست آید. مقدار $0.95 pu$ می‌تواند با توجه به شرایط سامانه قدرت و سایر عوامل متغیر باشد. برای محاسبه ریسک با استفاده از رابطه (۲۱)، لازم است که ابتدا یک تابع شدت به منظور مدل‌سازی مسئله کاهش ولتاژ شبکه قدرت

$$\begin{bmatrix} \Delta \tilde{\delta} \\ \Delta \tilde{V} \end{bmatrix} = [J]^{-1} \begin{bmatrix} \tilde{P} - P^{ctr} \\ \tilde{Q} - Q^{ctr} \end{bmatrix} \quad (11)$$

در نتیجه، تابع عضویت مربوط به مقادیر فازی دامنه ولتاژ (\tilde{V}) و فاز ولتاژ ($\tilde{\delta}$) توسط رابطه‌های (۱۲) و (۱۳) تعیین می‌گردد.

$$\begin{bmatrix} \tilde{\delta} \\ \tilde{V} \end{bmatrix} = \begin{bmatrix} \delta^{ctr} \\ V^{ctr} \end{bmatrix} + \begin{bmatrix} \Delta \tilde{\delta} \\ \Delta \tilde{V} \end{bmatrix} \quad (12)$$

$$\begin{bmatrix} \tilde{\delta} \\ \tilde{V} \end{bmatrix} = \begin{bmatrix} \delta^{ctr} \\ V^{ctr} \end{bmatrix} + \begin{bmatrix} \Delta \tilde{\delta} \\ \Delta \tilde{V} \end{bmatrix} \quad (13)$$

همان‌طور که از معادله‌های (۱۱) تا (۱۳) مشخص است، بر اثر انحراف موجود در مقادیر فازی توان تزریقی به شبکه، متناسب با آن، انحراف در دامنه و فاز ولتاژ به وجود آمده و در نتیجه مقادیر فازی‌ای برای دامنه و فاز ولتاژ به دست می‌آید.

د. گام بعدی، محاسبه توان اکتیو و راکتیو عبوری از خط است. توان عبوری از یک خط انتقال همان‌طور که در معادله‌های (۱۴) و (۱۵) نشان داده شده است، تابعی از دامنه و فاز ولتاژ در باس‌هایی است که ابتدا و انتهای آن خط به آن باس‌ها متصل است.

$$P_{ij} = G_{ij}V_i^2 - V_iV_j[G_{ij} \cos(\delta_i - \delta_j) - B_{ij} \sin(\delta_i - \delta_j)] \quad (14)$$

$$Q_{ij} = B_{ij}V_i^2 - V_iV_j[B_{ij} \cos(\delta_i - \delta_j) + G_{ij} \sin(\delta_i - \delta_j)] \quad (15)$$

در معادله‌های بالا، V_i و δ_i به ترتیب دامنه و فاز ولتاژ در گره i و V_j و δ_j به ترتیب دامنه و فاز ولتاژ در گره j بوده و G_{ij} و B_{ij} به ترتیب کاندوکتانس و سوسپتانس خط می‌باشد. همچنین میزان انحراف پخش توان در خط ij از میزان پیش‌بینی شده (قطعی) را می‌توان با استفاده از معادله‌های (۱۶) و (۱۷) بیان کرد:

$$\begin{aligned} \Delta P_{ij} &\approx \frac{\partial P_{ij}}{\partial V_i} \Big|_{V_i=V_i^{ctr}} \Delta V_i + \frac{\partial P_{ij}}{\partial V_j} \Big|_{V_j=V_j^{ctr}} \Delta V_j \\ &+ \frac{\partial P_{ij}}{\partial \delta_i} \Big|_{\delta_i=\delta_i^{ctr}} \Delta \delta_i + \frac{\partial P_{ij}}{\partial \delta_j} \Big|_{\delta_j=\delta_j^{ctr}} \Delta \delta_j \end{aligned} \quad (16)$$

$$\begin{aligned} \Delta Q_{ij} &\approx \frac{\partial Q_{ij}}{\partial V_i} \Big|_{V_i=V_i^{ctr}} \Delta V_i + \frac{\partial Q_{ij}}{\partial V_j} \Big|_{V_j=V_j^{ctr}} \Delta V_j \\ &+ \frac{\partial Q_{ij}}{\partial \delta_i} \Big|_{\delta_i=\delta_i^{ctr}} \Delta \delta_i + \frac{\partial Q_{ij}}{\partial \delta_j} \Big|_{\delta_j=\delta_j^{ctr}} \Delta \delta_j \end{aligned} \quad (17)$$

در نهایت، تابع عضویت مربوط به مقادیر فازی توان اکتیو (\tilde{P}_{ij}) و راکتیو (\tilde{Q}_{ij}) توسط رابطه (۱۸) و (۱۹) تعیین می‌شود.

$$\tilde{P}_{ij} = P_{ij}^{ctr} + \Delta \tilde{P}_{ij} \quad (18)$$

$$\tilde{Q}_{ij} = Q_{ij}^{ctr} + \Delta \tilde{Q}_{ij} \quad (19)$$

به طور مشابه، برای متغیرهای دیگر شبکه مانند تولید توان اکتیو در باس اسلک و توان راکتیو در باس‌های دارای ژنراتور نیز می‌توان روابطی غیر خطی بر حسب دامنه و فاز ولتاژ تعریف کرد.

$$\pi_p(x) = \mu_p(x), \quad \forall x \in X \quad (23)$$

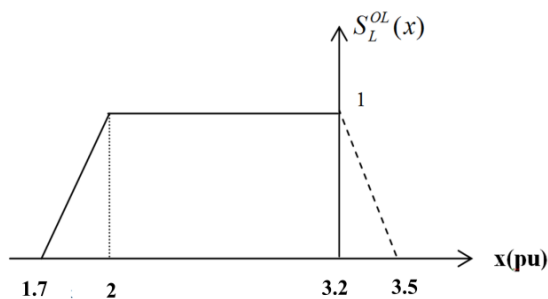
بنابراین، مقدار ممکن برای اضافه‌بار در خط L را می‌توان با معادله زیر بیان کرد:

$$\Pi_L^{OL}(x) = \max(\pi_{PL}(x \leq P_{\max})) \quad \forall x \in X \quad (24)$$

در این بخش، مانند حالت کاهش ولتاژ، عدد فازی مربوط به بارپذیری خط انتقال را با عدد فازی دوزنقه‌ای نشان داده می‌شود. بنابراین، اگر مقادیر توان عبوری از یک خط پس از وقوع یک حمله تروریستی را با X نشان داده شود، تابع شدت اضافه‌بار با استفاده از معادله (۲۵) بیان می‌شود:

$$S_L^{OL}(x) = \{\mu(1.7 pu, 2 pu, 3.2 pu, 3.5 pu, x) \quad \forall x \in X \quad (25)$$

همچنین عدد فازی مربوط شدت اضافه‌بار در شکل (۵) نشان داده شده است. با توجه به شکل (۵)، اگر توان عبوری از $2 pu$ بیشتر باشد، شدت اضافه‌بار برابر با یک در نظر گرفته می‌شود، اما در اینجا فرض می‌شود که توان عبوری از خط از $3/2 pu$ تجاوز نمی‌کند. همچنین مانند حالت قبل، یک بازه کوچک ($3/2 pu$ تا $3/5 pu$) که خارج از عملکرد سامانه است برای تکمیل عدد فازی دوزنقه‌ای در نظر گرفته می‌شود. لازم به ذکر است که برای مقادیر بیشتر از $3/2 pu$ ، معادله تأثیری در روند محاسبه شدت اضافه‌بار خط ندارد.



شکل ۵. عدد فازی شدت اضافه‌بار

۳-۲. شاخص ریسک برای ارزیابی امنیت

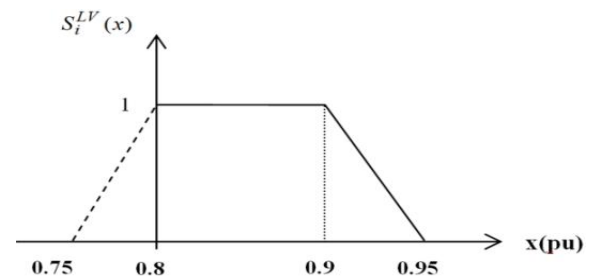
در بخش قبلی، پارامترهای عملکردی سامانه به منظور محاسبه ریسک نشان داده شده است. در این بخش، گام آخر برای یافتن شاخص ریسک به منظور ارزیابی عملکرد شبکه قدرت ارائه می‌شود. بر این اساس، در این بخش، دو شاخص یعنی شاخص مربوط به ریسک کاهش ولتاژ و شاخص مربوط به ریسک اضافه‌بار مورد بررسی قرار می‌گیرد.

شاخص ریسک کاهش ولتاژ: با فرض اینکه سامانه قدرت دارای n باس و L خط انتقال است، شاخص ریسک مربوط به کاهش ولتاژ در باس i ام و برای مؤلفه q ام سامانه قدرت با رابطه زیر داده می‌شود:

تعریف شود. در اینجا، عدد فازی دوزنقه‌ای که در شکل (۴) نشان داده شده است برای این کار پیشنهاد می‌شود. لازم به ذکر است که مقادیر نشان داده شده در شکل (۴) صرفاً به صورت یک پیشنهاد است و می‌توان مقادیر دیگری را به دلخواه برای این منظور مورد استفاده قرار داد. بنابراین اگر یک حمله تروریستی بر روی سامانه قدرت اتفاق بیافتد و بر اثر آسیب به هر یک از مؤلفه‌ها، شبکه دچار اختلال گردد، در این صورت اگر تمامی مقادیری که ولتاژ می‌تواند در حین وقوع این اختلال اختیار کند را با X نشان داده شود، آنگاه تابع شدت کاهش ولتاژ در باس Z را می‌توان با معادله (۲۲) نشان داد.

$$S_j^{LV}(x) = \left\{ \max \left(\min \left(\frac{x-0.75}{0.05}, \frac{0.95-x}{0.05}, 1 \right), 0 \right) \right\} \quad \forall x \in X \quad (22)$$

همان‌طور که از معادله (۲۲) مشخص است، این معادله یک مقدار صفر به تمامی مقادیر ولتاژ بالاتر یا مساوی $0.95 pu$ ، مقدار ۱ به تمامی مقادیر ولتاژ کمتر یا مساوی $0.75 pu$ و یک مقدار متناسب با معادله خطی $\frac{0.95-x}{0.05}$ برای مقادیر ولتاژ بین $0.75 pu$ و $0.95 pu$ اختصاص می‌دهد. این اعداد فازی در شکل (۴) نشان داده شده است. از آنجایی که عدد فازی دوزنقه‌ای در شکل (۲) دارای چهار عدد است، بنابراین یک بازه کوچک ($0.75 pu$ تا $0.8 pu$) که خارج از عملکرد سامانه است برای تکمیل عدد فازی دوزنقه‌ای در نظر گرفته می‌شود. لازم به ذکر است که برای مقادیر کمتر از $0.8 pu$ ، معادله تأثیری در روند محاسبه شدت کاهش ولتاژ ندارد.

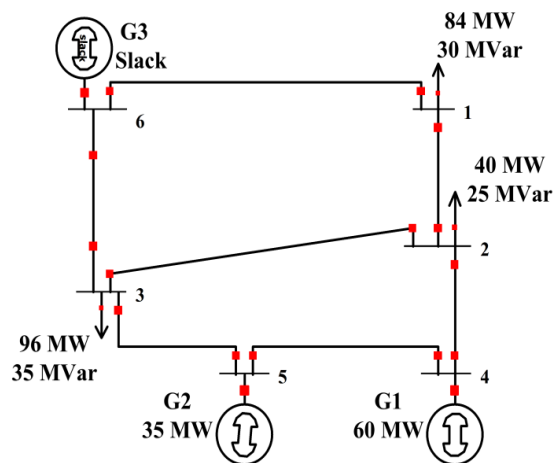


شکل ۴. عدد فازی شدت کاهش ولتاژ

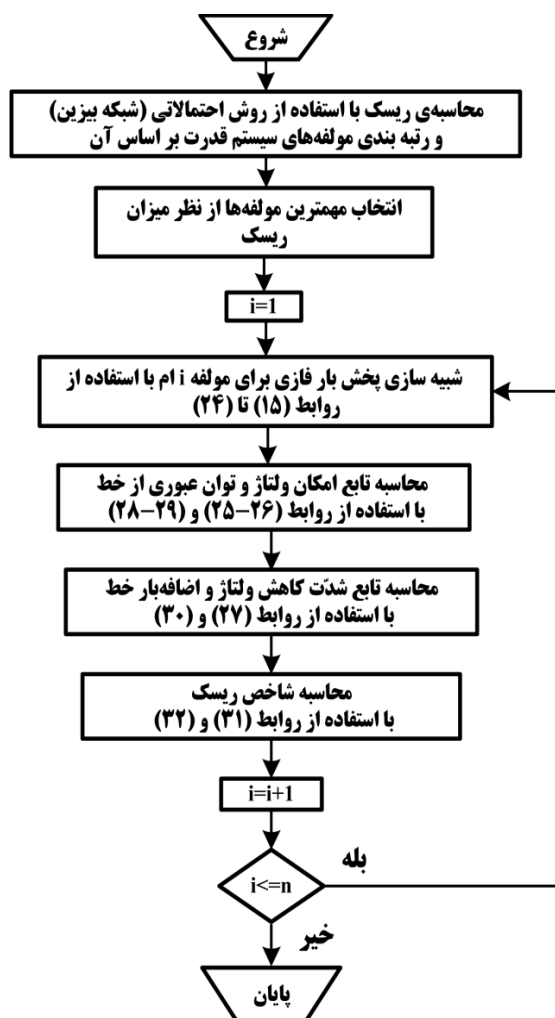
شرایط اضافه‌بار خط: اگر L یک خط انتقال باشد، آنگاه منظور از اضافه‌بار در این خط این است که توان عبوری از آن از حد مجاز فراتر رفته است. این مقدار مجاز برای هر خط مقدار مشخصی است که در واقع نشان دهنده محدودیت حرارتی برای سامانه قدرت می‌باشد.

تابع امکان برای توان عبوری از یک خط که توسط پخش بار فازی به دست می‌آید را می‌توان با رابطه (۲۳) نشان داد. در این رابطه، X مقدار ممکن برای توان عبوری از خط انتقال است.

گزارش شده است [۲۲]. پس از رتبه‌بندی، مؤلفه‌هایی را که میزان ریسک آن‌ها از مقدار ۰/۷ بیشتر است به عنوان مهم‌ترین مؤلفه‌ها برای ارزیابی امنیت در نظر گرفته می‌شوند که در جدول (۱) نشان داده شده است.



شکل ۶. شبکه شش‌باسه



شکل ۷. الگوریتم محاسبه شاخص ریسک برای ارزیابی امنیت سامانه قدرت

$$R_{i,q}^{LV}(x) = P(A_q) \cdot (\pi_{V_{i,q}}(x) \otimes S_{i,q}^{LV}(x)) \quad \forall x \in X \quad (26)$$

در رابطه بالا، $P(A_q)$ احتمال وقوع حمله به مؤلفه q ام سامانه قدرت که با استفاده از روش‌های احتمالاتی به دست می‌آید، $\pi_{V_{i,q}}(x)$ تابع امکان ولتاژ با در نظر گرفتن حمله تروریستی به مؤلفه q ام، $S_{i,q}^{LV}(x)$ تابع شدت کاهش ولتاژ و عملگر \otimes نشان دهنده ضرب فازی است. لازم به ذکر است که مقدار به دست آمده برای ریسک یک مقدار فازی می‌باشد.

شاخص ریسک اضافه‌بار خط: مشابه حالت قبل، شاخص ریسک مربوط به اضافه‌بار خط به صورت زیر تعریف می‌شود:

$$R_{L,q}^{OL}(x) = p(A_q) \cdot (\pi_{P_{L,q}}(x) \otimes S_{L,q}^{OL}(x)) \quad \forall x \in X \quad (27)$$

در رابطه بالا، $p(A_q)$ احتمال وقوع حمله به مؤلفه q ام سامانه قدرت که با استفاده از روش‌های احتمالاتی به دست می‌آید، $\pi_{P_{L,q}}(x)$ تابع امکان بارپذیری خط با در نظر گرفتن حمله تروریستی به مؤلفه q ام و $S_{L,q}^{OL}(x)$ تابع شدت اضافه‌بار خط است.

۳. مطالعه موردی

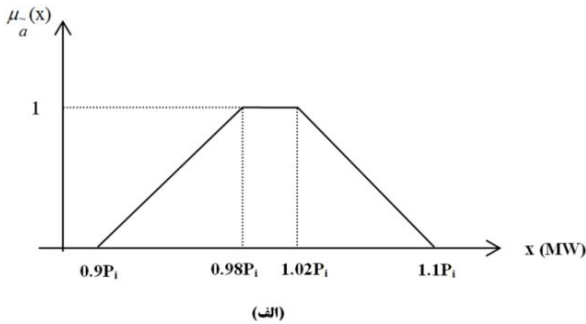
در این بخش، به منظور ارزیابی کارایی روش پیشنهاد شده، شاخص ریسک برای ارزیابی امنیت یک شبکه شش‌باسه که در شکل (۶) نشان داده شده است محاسبه می‌گردد. در ادامه مطابق با الگوریتم نشان داده شده در شکل (۶)، روش پیشنهادی بر روی شبکه شش‌باسه (از این پس به اختصار شبکه نامیده می‌شود) اعمال و شاخص ریسک برای مؤلفه‌های این شبکه محاسبه می‌شود و نتایج حاصل از آن مورد بحث و بررسی قرار می‌گیرد.

با توجه به مباحث صورت گرفته تاکنون، الگوریتم محاسبه شاخص ریسک برای ارزیابی امنیت سامانه قدرت در شکل (۷) نشان داده است.

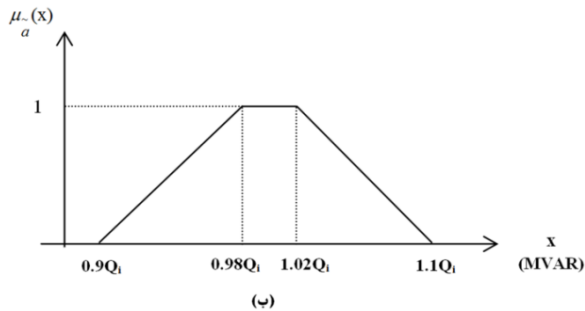
۳-۱. رتبه‌بندی مؤلفه‌های شبکه

گام اول در روش پیشنهادی شناسایی و رتبه‌بندی مؤلفه‌های شبکه از نظر بیشترین میزان ریسک است. به منظور پیاده‌سازی این گام، شبکه مورد نظر به نواحی مختلف تقسیم‌بندی شده و اطلاعات کاملی از سامانه قدرت و موقعیت گروه‌های تروریستی در این نواحی جمع‌آوری می‌شود. سپس با مشخص کردن مهم‌ترین پارامترهای تأثیرگذار بر روی احتمال حمله به سامانه قدرت و نتایج ناشی از آن و همچنین با استفاده از روش بیزین که مبتنی بر تئوری احتمالات است، میزان احتمال حمله به هر یک از مؤلفه‌های شبکه قدرت محاسبه شده و این مؤلفه‌ها بر حسب میزان ریسک رتبه‌بندی می‌شوند. جزئیات کامل این روش قبلاً

برای باس‌های دارای بار و باس‌های دارای ژنراتور که در واقع به عنوان متغیرهای ورودی مسئله پخش بار فازی در نظر گرفته می‌شوند در جدول (۲) نشان داده شده است. به همین منظور، برای به دست آوردن مقادیر ولتاژ فازی ابتدا با محاسبه میزان انحراف توان تزریقی به شبکه یعنی $(\tilde{P} - P^{ctr})$ برای توان اکتیو و $(\tilde{Q} - Q^{ctr})$ برای توان راکتیو و همچنین محاسبه معکوس ماتریس ژاکوبین، میزان انحراف ولتاژ با استفاده از معادله (۱۱) مشخص شده و در نهایت مقادیر ولتاژ فازی بر اساس رابطه (۱۳) استخراج می‌شود. جدول (۳) نتایج حاصل از شبیه‌سازی پخش بار فازی برای حالت پایه را برای ولتاژ باس‌ها نشان می‌دهد. همان‌طور که مشخص است، مقادیر ولتاژ فازی نشان داده شده در جدول (۳) برای سه باس از شش باس شبکه است، زیرا مقادیر ولتاژ باس اسلک (باس ۶) و باس‌های دارای ژنراتور (باس‌های ۴ و ۵) مقداری معلوم می‌باشد. با توجه به جدول (۳)، مشاهده می‌شود که ولتاژ تمامی باس‌ها در محدوده مجاز بوده و هیچ‌گونه اضافه یا کاهش ولتاژ مشاهده نمی‌شود. برای به دست آوردن مقادیر فازی توان عبوری از خط، ابتدا میزان انحراف توان عبوری از میزان پیش‌بینی شده با استفاده از معادله (۱۶) محاسبه شده و در نهایت با به کارگیری معادله (۲۲)، مقادیر فازی توان اکتیو عبوری (\tilde{P}_{ij}) برای هر یک از خطوط تعیین می‌شود. این مقادیر در جدول (۴) نشان داده شده است.



شکل ۸. اعداد فازی دوزنقه‌ای مربوط به تزریق توان اکتیو



شکل ۹. اعداد فازی دوزنقه‌ای مربوط به تزریق توان راکتیو

جدول ۱. میزان احتمال حمله به تجهیزات شبکه و رتبه‌بندی آن‌ها بر اساس میزان ریسک

نوع مؤلفه	احتمال حمله	ریسک
ژنراتور ۲	٪۴۰/۲	۱
پست ۳	٪۲۸	۰/۹۶
ژنراتور ۳	٪۳۰/۲	۰/۸۸
پست ۵	٪۴۰/۲	۰/۸۱
پست ۶	٪۳۳/۴	۰/۷۵
خط ۳-۶	٪۴۲/۵	۰/۷۱
خط ۱-۶	٪۴۰/۸	۰/۷۰

۳-۲. شبیه‌سازی پخش بار فازی

گام دوم، نشان دادن عدم قطعیت در توان تزریقی به شبکه و شبیه‌سازی پخش بار فازی است. همان‌طور که در بخش‌های قبلی نیز ذکر شد، در این مقاله از روش اعداد فازی LR برای حل پخش بار فازی استفاده می‌شود. همچنین، به منظور مدل کردن تزریق توان در همه باس‌ها اعداد دوزنقه‌ای که یک روش پرکاربرد بوده و پیاده‌سازی آن نیز ساده است مورد استفاده قرار می‌گیرد.

شبیه‌سازی برای حالت قبل از وقوع حمله تروریستی: در این بخش شبیه‌سازی پخش بار فازی برای حالت قبل از وقوع حمله (از این به بعد به اختصار حالت پایه نامیده می‌شود) مورد بحث و بررسی قرار می‌گیرد. همان‌طور که قبلاً ذکر شد به منظور مدل کردن تزریق توان در باس‌ها و همچنین بارهای شبکه از اعداد دوزنقه‌ای استفاده می‌شود. اعداد فازی دوزنقه‌ای مربوط به تزریق توان اکتیو و راکتیو در شکل‌های (۸) و (۹) نشان داده است. در این دو شکل، P_i و Q_i به ترتیب مقدار توان اکتیو و راکتیو پیش‌بینی شده (قطعی) ناشی از شبیه‌سازی پخش بار متداول هستند. لازم به ذکر است که این مقادیر پیش‌بینی شده برای توان $(P_i$ و $Q_i)$ همان مقادیر $(P^{ctr}$ و $Q^{ctr})$ مربوط به معادله (۱۰) می‌باشند. با توجه به شکل‌های (۸) و (۹)، در بازه $[0.98 P_i, 1.02 P_i]$ تابع عضویت برابر با عدد ۱ است. به عبارتی دیگر، میزان خطای توان تزریقی به شبکه در حالت معمول در حدود $\pm 2\%$ در نظر گرفته شده است. از طرفی دیگر، هرچه میزان انحراف توان بیشتر می‌شود، درجه عضویت به صورت خطی کاهش یافته و در صورتی که میزان انحراف از دو طرف (حد بالا و پایین) 10% مقدار پیش‌بینی شده یا بیشتر شود، درجه عضویت برابر با صفر است. لازم به ذکر است که اعداد فازی بارهای اکتیو و راکتیو نیز مانند اعداد فازی توان تزریقی به شبکه است. بنابراین، با توجه به مباحث فوق، مقادیر اعداد فازی دوزنقه‌ای

جدول ۲. مقادیر اعداد فازی دوزنقه‌ای برای متغیرهای ورودی

توان راکتیو (مگاوار)					توان اکتیو (مگاوات)					باس
۳۳	۳۰/۶	۳۰	۲۹/۴	۲۷	۹۲/۴	۸۵/۶۸	۸۴	۸۲/۳۲	۷۵/۶	۱
۲۷/۵	۲۵/۵	۲۵	۲۴/۵	۲۲/۵	۴۴	۴۰/۸	۴۰	۳۹/۲	۳۶	۲
۳۸/۵	۳۵/۷	۳۵	۳۴/۳	۳۱/۵	۱۰۵/۶	۹۷/۹۲	۹۶	۹۴/۰۸	۸۶/۴	۳
					۶۶	۶۱/۲	۶۰	۵۸/۸	۵۴	۴
					۳۸/۵	۳۵/۷	۳۵	۳۴/۳	۳۱/۵	۵

جدول ۳. ولتاژ فازی باس‌ها در حالت پایه

ولتاژ			توان تزریقی
باس ۳	باس ۲	باس ۱	
۰/۹۷۷۸	۱/۰۰۱۴	۱/۰۱۵۶	۰/۹P _i
۰/۹۸۶۱	۱/۰۰۵۳	۱/۰۱۸۵	۰/۹۸P _i
۰/۹۹۱۴	۱/۰۰۶۴	۱/۰۱۹۲	P _i
۰/۹۹۶۷	۱/۰۰۷۴	۱/۰۱۹۹	۱/۰۲P _i
۱/۰۰۵۲	۱/۰۱۱۱	۱/۰۲۲۸	۱/۱P _i

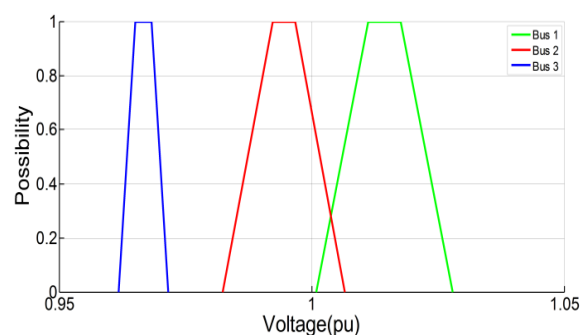
جدول ۴. توان فازی عبوری در حالت پایه

توان عبوری (pu)							توان تزریقی
خط ۲-۳	خط ۵-۳	خط ۴-۵	خط ۴-۲	خط ۱-۲	خط ۶-۳	خط ۶-۱	
۰/۰۸۷۳	۰/۲۳۸۷	۰/۰۴۹۷	۰/۲۷۸۹	۰/۰۶۷۸	۰/۴۲۷۱	۰/۸۹۲۸	۰/۹۹P _i
۰/۰۹۲۵	۰/۳۴۴۷	۰/۰۹۵۹	۰/۳۴۸۹	۰/۱۰۶۳	۰/۴۹۷۸	۰/۹۵۵۰	۰/۹۸P _i
۰/۱۱۰۱	۰/۳۸۵۲	۰/۱۱۶۱	۰/۳۸۴۲	۰/۱۲۱۱	۰/۵۲۰۲	۰/۹۷۲۵	P _i
۰/۱۲۷۵	۰/۴۲۵۵	۰/۱۲۷۳	۰/۴۱۹۵	۰/۱۳۵۹	۰/۵۴۲۶	۰/۹۹۰۰	۱/۰۲۱ P _i
۰/۴۰۲۱	۰/۵۳۱۴	۰/۱۷۳۵	۰/۴۸۸۸	۰/۱۷۴۴	۰/۶۱۳۷	۱/۰۵۲۲	۱/۱P _i

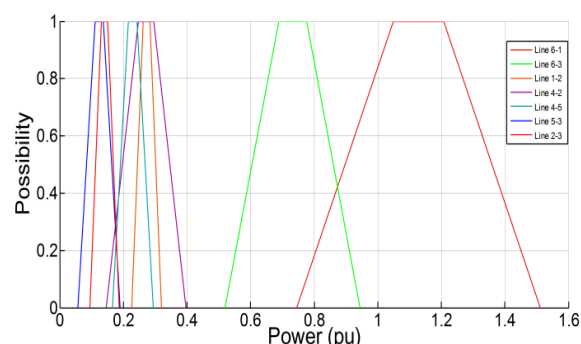
می‌گیرد. همچنین در هر یک از حملات تروریستی فرض می‌شود که نتایج حاصل از این حملات فاجعه‌آمیز است یعنی مؤلفه مورد نظر به طور کامل آسیب دیده و از شبکه جدا می‌شود.

سناریو ۱ "از دست رفتن ژنراتور شماره ۲": در این بخش فرض می‌شود که حمله‌ای به شبکه برق انجام شده و بر اثر آن ژنراتور شماره ۲ به طور کامل آسیب می‌بیند. نتیجه این حمله از دست رفتن تولید در باس ۵ است. نمای کلی شبکه پس از خروج ژنراتور شماره ۲ از سامانه ناشی از حمله به آن در شکل (۱۰) نشان داده است. همچنین، نتایج حاصل از شبیه‌سازی پخش بار فازی برای ولتاژ باس‌ها پس از وقوع این حمله در شکل (۱۱)

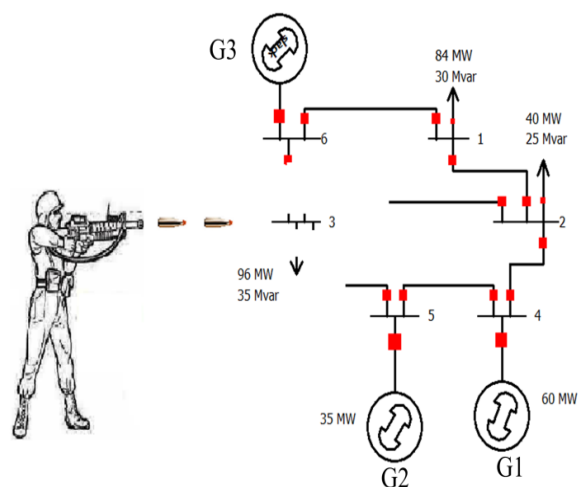
شبیه‌سازی برای حالت پس از وقوع حمله تروریستی: در این بخش، شبیه‌سازی پخش بار فازی برای حالت‌های مختلف حمله به شبکه قدرت مورد بررسی قرار می‌گیرد. همان‌طور که قبلاً نیز ذکر شد، شبیه‌سازی به ترتیب برای مؤلفه‌هایی صورت می‌گیرد که دارای بالاترین میزان ریسک به‌دست آمده توسط شبکه بی‌زین که در جدول (۱) نشان داده شده است، می‌باشند. در این بخش نیز مانند بخش قبلی از اعداد فازی نشان داده شده در جدول (۲) استفاده می‌شود. در ادامه شاخص ریسک به منظور ارزیابی امنیت شبکه برای هر یک از حالت‌های حمله به مؤلفه‌های شبکه بر اساس جدول (۱) ارائه شده و نتایج حاصل از آن مورد بحث و بررسی قرار



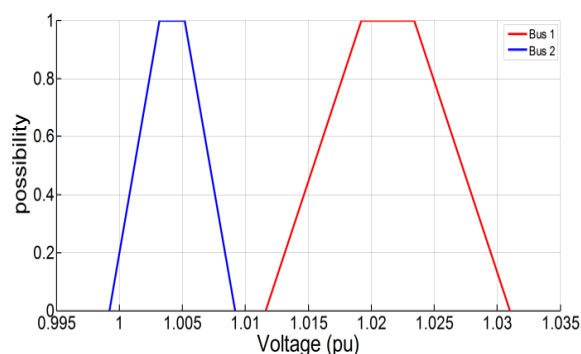
شکل ۱۱. میزان ولتاژ باس‌های شبکه پس از حمله به ژنراتور شماره ۲



شکل ۱۲. میزان توان عبوری از خطوط پس از حمله به ژنراتور شماره ۲



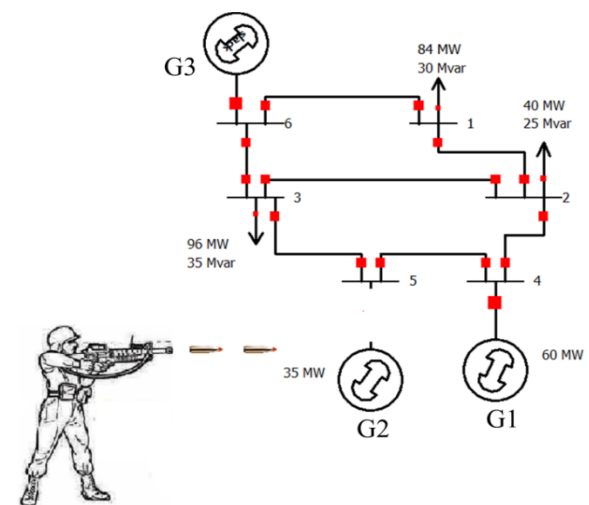
شکل ۱۳. حمله تروریستی به پست شماره ۳ و خروج آن از شبکه



شکل ۱۴. میزان ولتاژ باس‌های شبکه پس از حمله به پست شماره ۳

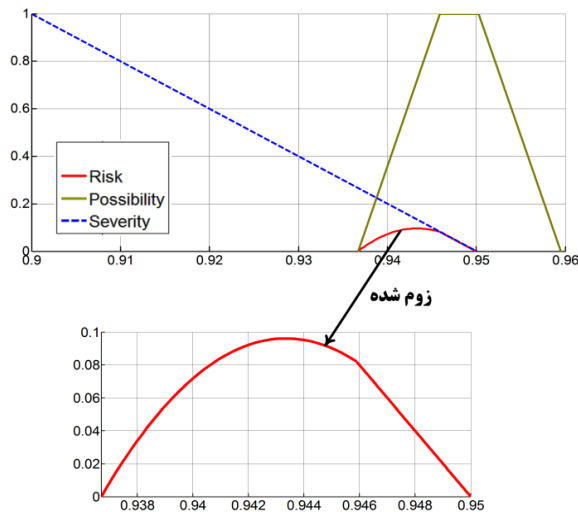
نشان داده است. لازم به ذکر است که روند شبیه‌سازی پخش بار فازی برای این حالت مانند حالت پایه بوده و تنها تفاوت، خروج ژنراتور شماره ۲ از شبکه است. با توجه به شکل (۱۱) تمامی مقادیر ولتاژ باس‌ها در محدوده مجاز بوده و در نتیجه تابع شدت بر اساس معادله (۲۲) برابر با صفر است. بنابراین، مطابق با رابطه (۲۶) شاخص ریسک ولتاژ برای تمامی باس‌ها صفر می‌باشد. همچنین، نتایج حاصل از شبیه‌سازی پخش بار فازی برای توان عبوری از خط پس از وقوع این حمله در شکل (۱۲) نشان داده است. در اینجا فرض می‌شود که توان پایه برای این شبکه 100 MVA بوده و اضافه‌بار تمام خطوط در 200 MVA یعنی 2 pu اتفاق می‌افتد. با توجه به شکل (۱۱)، از آنجایی که هیچ‌گونه اضافه‌باری در خطوط این شبکه مشاهده نمی‌شود در نتیجه براساس رابطه‌های (۲۵) و (۲۷) تابع شدت و در نتیجه شاخص ریسک اضافه‌بار برای تمامی خطوط صفر است.

سناریو ۲ "از دست رفتن پست شماره ۳": در این بخش فرض می‌شود که حمله‌ای به شبکه برق صورت گرفته و بر اثر آن پست شماره ۳ به طور کامل آسیب می‌بیند. نتیجه این حمله از دست رفتن بار در باس ۳ و خروج ۳ خط از شبکه است. نمای کلی شبکه پس از خروج پست شماره ۳ از سامانه ناشی از حمله به آن در شکل (۱۳) نشان داده است. همچنین، نتایج حاصل از شبیه‌سازی پخش بار فازی برای ولتاژ باس‌ها و همچنین توان عبوری از خط پس از وقوع این حمله در شکل‌های (۱۴) و (۱۵) نشان داده است. همان‌طور که در این شکل‌ها مشخص است، در این حالت نیز هیچ‌گونه کاهش ولتاژ و یا اضافه‌باری به ترتیب در ولتاژ باس‌ها و توان عبوری از خطوط مشاهده نمی‌شود و بنابراین شاخص ریسک ولتاژ و اضافه‌بار خط در این حالت نیز صفر است.



شکل ۱۵. حمله تروریستی به ژنراتور شماره ۲ و خروج آن از شبکه

به دست می آید. شاخص ریسک کاهش ولتاژ باس ها و اضافه بار خطوط در جدول (۵) نشان داده است.



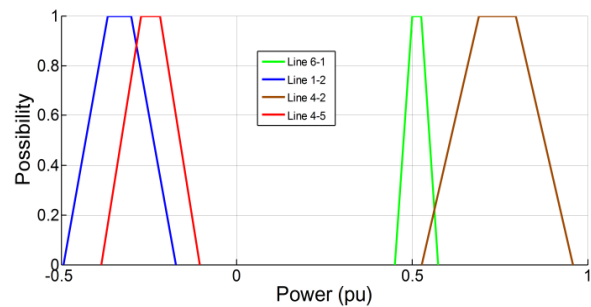
شکل ۱۹. ریسک کاهش ولتاژ در باس ۳ ناشی از حمله به پست شماره ۵

جدول ۵. شاخص ریسک ناشی از حمله به پست شماره ۵

باس	۱	۲	۳
شاخص ریسک ولتاژ	۰	۰	۰/۰۳۸۶
خط	۶-۱	۶-۳	۱-۲، ۴-۲، ۲-۳
شاخص ریسک اضافه بار	۰	۰	۰

سناریو ۵ "از دست رفتن پست شماره ۶": تأثیر از دست رفتن این مؤلفه بر روی شبکه ناشی از حمله تروریستی، مشابه سناریو ۳ است.

سناریو ۶ "از دست رفتن خط ۳-۶": در این بخش فرض می شود که حمله ای به شبکه برق انجام شده و بر اثر آن خط ۳-۶ از مدار خارج گردد. نمای کلی شبکه پس از خروج خط ۳-۶ از سامانه ناشی از حمله تروریستی در شکل (۲۰) نشان داده است. نتیجه این حمله از دست رفتن خطی از شبکه است که نقش اصلی را در تغذیه بار متصل به باس ۳ ایفا می کند. همچنین، نتایج حاصل از شبیه سازی پخش بار فازی برای ولتاژ باس ها و همچنین توان عبوری از خط پس از وقوع این حمله به ترتیب در شکل های (۲۱) و (۲۲) نشان داده است. با توجه به شکل (۲۱)، مشاهده می شود که ولتاژ باس های ۲ و ۳ از pu $0/95$ که مقدار مجاز برای ولتاژ شبکه می باشد کمتر است. در نتیجه می توان با روش پیشنهادی شاخص ریسک برای ولتاژ این دو باس را به دست آورد. بر این اساس، ابتدا با توجه به رابطه (۳۰)، با استفاده از حاصل ضرب تابع امکان (شکل ۲۱) و شدت کاهش ولتاژ (شکل ۴) ریسک اولیه برای این دو باس محاسبه می شود که در شکل های (۲۳) و (۲۴) نشان داده است. بر اساس

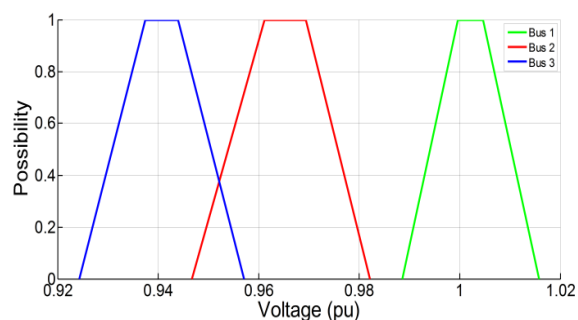


شکل ۱۵. میزان توان عبوری از خطوط پس از حمله به پست شماره ۳

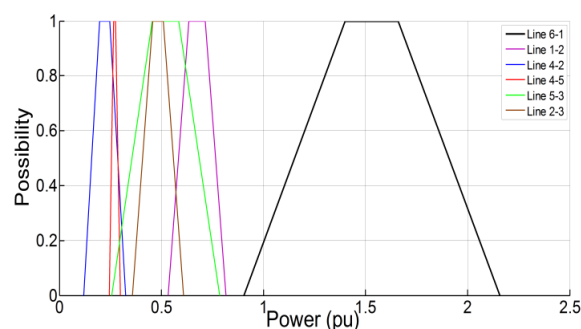
سناریو ۳ "از دست رفتن ژنراتور شماره ۳": فرض می شود حمله ای به ژنراتور شماره ۳ صورت گرفته و این مؤلفه شبکه به طور کامل تخریب شود. از طرفی دیگر، ژنراتور شماره ۳ به باس مرجع^۱ وصل بوده و بنابراین یک مؤلفه بسیار حیاتی برای شبکه قدرت است. اکنون اگر بر اثر حمله تروریستی این ژنراتور از شبکه خارج گردد، هر سه باس ۱، ۲ و ۳ دچار فروپاشی ولتاژ شده و در نتیجه Blackout در شبکه اتفاق می افتد. از آنجایی که مقدار ولتاژ باس ها در اثر حمله به این ژنراتور خارج از محدوده اعداد فازی (کمتر از $0/8 pu$) نشان داده شده در شکل (۴) است در نتیجه روش پیشنهادی در این مقاله نمی تواند برای ارزیابی امنیت در این حالت مورد استفاده قرار گیرد. با این وجود، مشخص است که سامانه در این حالت کاملاً ناپایدار است.

سناریو ۴ "از دست رفتن پست شماره ۵": در این حالت، بر اثر حمله تروریستی، پست شماره ۵ به طور کامل آسیب دیده و از شبکه خارج می شود. نتیجه این حمله از دست رفتن تولید در باس ۵ و خروج ۲ خط از شبکه است. نمای کلی شبکه پس از خروج پست شماره ۳ از سامانه ناشی از حمله به آن در شکل (۱۶) نشان داده است. همچنین، نتایج حاصل از شبیه سازی پخش بار فازی برای ولتاژ باس ها و همچنین توان عبوری از خط پس از وقوع این حمله در شکل های (۱۷) و (۱۸) نشان داده است. با توجه به شکل (۱۷)، مشاهده می شود که ولتاژ باس ۳ از pu $0/95$ کمتر است. بنابراین این باس در معرض ریسک ناشی از کاهش ولتاژ قرار دارد. مقدار این ریسک را می توان با استفاده از رابطه (۳۰) تعیین کرد. بر این اساس، با توجه به رابطه (۳۰) ابتدا با استفاده از حاصل ضرب تابع امکان (شکل ۱۷) و شدت کاهش ولتاژ (شکل ۴) ریسک اولیه محاسبه می شود که در شکل (۱۹) نشان داده است. مطابق با این شکل، مقدار بیشینه ریسک برابر با $0/096$ است. سپس ریسک نهایی که همان شاخص ریسک است بر اساس رابطه (۲۶) با ضرب بیشینه ریسک در میزان احتمال حمله به پست شماره ۵ که در جدول (۱) نشان داده است

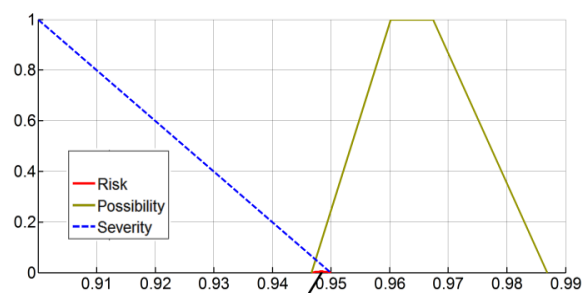
^۱ Slack Bus



شکل ۲۱. میزان ولتاژ باس‌های شبکه پس از حمله به خط ۳-۶



شکل ۲۲. میزان توان عبوری از خطوط پس از حمله به خط ۳-۶



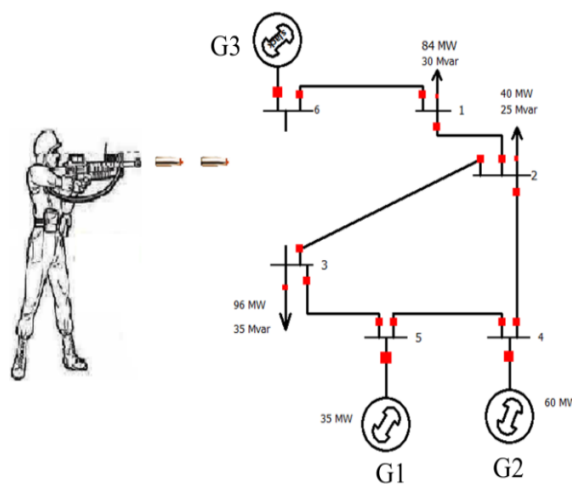
شکل ۲۳. ریسک کاهش ولتاژ در باس ۲ ناشی از حمله به خط ۳-۶

جدول ۶. شاخص ریسک ناشی از حمله به خط ۳-۶

باس	۱	۲	۳
شاخص ریسک ولتاژ	۰	۰/۰۰۱۸	۰/۱۰۷۱
خط	۶-۱	۲-۳	۱-۲, ۴-۲, ۲-۳, ۵-۳
شاخص ریسک اضافه بار	۰/۱۴۹۶	۰	۰

شکل‌های (۲۳) و (۲۴)، مقدار بیشینه ریسک برای باس ۲ و ۳ به ترتیب برابر با ۰/۰۰۴۲ و ۰/۲۵۲ است. سپس شاخص ریسک مطابق با رابطه (۲۶) با ضرب بیشینه ریسک در میزان احتمال حمله به خط ۳-۶ که در جدول (۱) نشان داده است حاصل می‌شود. از طرفی دیگر، با در نظر گرفتن معیار اضافه‌بار خطوط یعنی $2 pu$ ، شکل (۲۲) نشان می‌دهد که خط ۱-۶ دچار اضافه‌بار شده است. بنابراین با روش پیشنهادی می‌توان شاخص ریسک مربوط به این اضافه‌بار را نیز تعیین نمود. در این حالت نیز همانند روند محاسبه شاخص ریسک برای کاهش ولتاژ، ابتدا با توجه به رابطه (۲۷)، با استفاده از حاصل ضرب تابع امکان (شکل ۲۲) و شدت اضافه‌بار (شکل ۵) ریسک اولیه برای اضافه‌بار این خط محاسبه می‌شود که در شکل (۲۵) نشان داده است. بر اساس شکل (۲۵)، مقدار بیشینه ریسک برای این خط برابر با ۰/۳۵۲ است. سپس مطابق با رابطه (۲۷) با ضرب بیشینه ریسک در میزان احتمال حمله به خط ۳-۶ که در جدول (۱) نشان داده شده است شاخص ریسک برای اضافه‌بار این خط محاسبه می‌شود. شاخص ریسک کاهش ولتاژ باس‌ها و اضافه‌بار خطوط در جدول (۶) نشان داده است.

سناریو ۷ "از دست رفتن خط ۱-۶": بر اثر حمله تروریستی به خط ۱-۶، ولتاژ باس‌های ۱ و ۲ دچار فروپاشی شده و ولتاژ باس ۳ نیز در مرز ناپایداری قرار می‌گیرد. بنابراین، در این حالت نیز شبکه به شدت ناپایدار بوده و از آنجایی که مقادیر ولتاژ باس‌ها در خارج از محدوده اعداد فازی (کمتر از $0.8 pu$) نشان داده شده در شکل (۴) است در نتیجه روش پیشنهادی در این مقاله نمی‌تواند برای ارزیابی امنیت در این حالت مورد استفاده قرار گیرد. با این وجود، مشخص است که سامانه در این حالت کاملاً ناپایدار است.

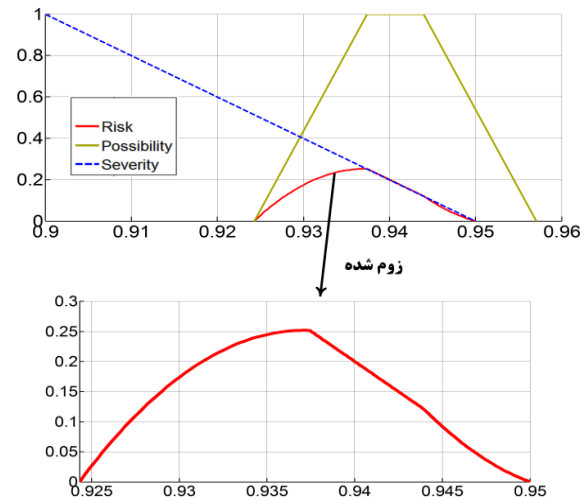


شکل ۲۰. حمله تروریستی به خط ۳-۶ و خروج آن از شبکه

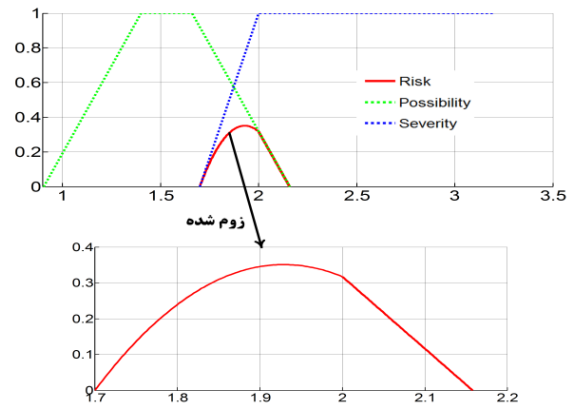
تابع امکان برای ولتاژ باسها و توان عبوری از خطوط محاسبه می‌شود. سپس با در نظر گرفتن دو پارامتر مرتبط با امنیت سامانه قدرت یعنی پارامترهای کاهش ولتاژ و اضافه بار خطوط، یک تابع شدت برای هر یک از این پارامترها تعیین می‌شود. در نهایت با استفاده از توابع امکان محاسبه شده و همچنین توابع شدت تعریف شده، شاخص ریسک برای کاهش ولتاژ باسها و اضافه بار خطوط ناشی از حمله تروریستی به شبکه ارائه می‌شود. لازم به ذکر است که شاخص به دست آمده مربوط به ریسک کل شبکه نمی‌باشد بلکه برای هر باس و یا یک خط شبکه به طور مجزا محاسبه می‌شود که بر اساس آن برنامه ریزان سامانه قدرت می‌توانند از این شاخصها برای برنامه ریزی آینده سامانه و همچنین ارزیابی امنیت شبکه استفاده نمایند.

۵. مراجع

- [1] Alami, H. "Modeling the Reliability of Electric Power of an Energy Hub in Critical Situation"; J. Passive Defence Sci. Tech. 2015, 5, 278-285 (In Persian).
- [2] Taylor, C.; Krings, A.; Alves-Foss, J. "Risk Analysis and Probabilistic Survivability Assessment (RAPSA): An Assessment Approach for Power Substation Hardening"; Proc. of ACM Workshop on Scientific Aspects of Cyber Terrorism (SACT), U. S., 2002.
- [3] McClintock, J.; Saxon, M.; Forsythe, J.; Rascoe, J.; Risser, J. "Development of the Adaptable, GIS-Based, Multi-Threat Detection System"; Proc. of IEEE Int. Conf. on Tech. for Homeland Security, 2011, 507-511.
- [4] Biringer, B. "Risk Assessment Methodology for Electric Power Transmission, RAM-TSM"; Proc. of IEEE Int. Carnahan Conf. on Security Tech., 2004, 99-105.
- [5] Law, Y. W.; Alpcan, T.; Palaniswami, M. "Security Games for Risk Minimization in Automatic Generation Control"; IEEE Trans. on Power Syst. 2014, 30, 223-232.
- [6] Bompard, E.; Ciwei, G.; Napoli, R.; Russo, A.; Masera, M.; Stefanini, A. "Information Impact on the Risk Analysis of the Malicious Attack Against Power System"; Proc. of IREP Symposium on Bulk Power System Dynamics and Control, 2007, 1-8.
- [7] Göztepe, K. "Designing a Fuzzy Rule Based Expert System for Cyber Security"; Int. J. Inform. Secur. Sci. 2006, 1, 1-12.
- [8] Machias, A. V.; Souflis, J. L.; Dialynas, E. N. "A Fuzzy Transient Stability Index in Power System Security Evaluation"; IEEE Control Systems Society 2002, 34, 662-666.
- [9] Tso, S. K.; Zhu, T. X.; Zeng, Q. Y.; Lo, K. L. "Dynamic Voltage Security Assessment Using a Fuzzy Severity Index"; Engineering Applications of Artificial Intelligence 1995, 8, 657-664.
- [10] Hsu, Y. Y.; Kuo, H. C. "Fuzzy-Set Based Contingency Ranking [Power System Security]"; IEEE Trans. on Power Syst. 1992, 7, 1189-1196.
- [11] Ming, Z.; Ding, S.; Song, X.; Tian, K. "Indices System and Methods for Power Grid Security Assessment Based on Dynamic Fuzzy"; Proc. of IEEE Int. Conf. on Electrical and Control Eng. (ICECE), 2010, 3830-3833.
- [12] Huan, H.; Xiaoshi, D.; Chen X.; Zhao, F.; Xiangning L.; Zhiqian B. "Risk Assessment of Cascading Failure in Power Systems Based on Uncertainty Theory"; IEEE Power and Energy Society General Meeting 2011, 1-5.



شکل ۲۴. ریسک کاهش ولتاژ در باس ۳ ناشی از حمله به خط ۳-۶



شکل ۲۵. ریسک اضافه بار خط ۶-۱ ناشی از حمله به خط ۳-۶

۴. نتیجه گیری

در این مقاله برای ارزیابی امنیت سامانه قدرت با در نظر گرفتن عدم قطعیت در تزیق توان به شبکه یک روش ترکیبی مبتنی بر تئوری احتمال و تئوری امکان ارائه شد. بر همین اساس، در گام اول، با استفاده از تئوری احتمال، مهم‌ترین مؤلفه‌های سامانه قدرت که میزان ریسک ناشی از حملات تروریستی به آنها از سایر مؤلفه‌ها بیشتر است شناسایی شده و میزان احتمال حمله به هر یک از این مؤلفه‌ها نیز محاسبه می‌شود. لازم به ذکر است که استفاده از تئوری احتمال در این مقاله به دو دلیل دارای اهمیت است. اول این که با استفاده از این تئوری، میزان احتمال حمله به مؤلفه‌های شبکه قدرت مشخص می‌شود. دلیل دوم این است که، با به کارگیری این تئوری و شناسایی مهم‌ترین مؤلفه‌های سامانه قدرت از نظر میزان ریسک حمله به آنها تعداد شبیه‌سازی‌ها در گام بعدی کاهش خواهد یافت. در گام دوم، با به کارگیری تئوری امکان به عنوان ابزاری برای مدل‌سازی عدم قطعیت و همچنین استفاده از شبیه‌سازی پخش بار فازی، ابتدا

- [18] Saraiva, J. T.; Miranda, V.; Matos, M. A. "Generation and Load Uncertainties Incorporated in Load Flow Studies"; Proc. of Electrotechnical Conf., 6th Mediterranean MELECON, 1991, 2, 1339-1342.
- [19] Saraiva, J. T.; Fonseca, N.; Matos, M. A. "Fuzzy Power Flow - An AC Model Addressing Correlated Data"; Proc. of IEEE Int. Conf. on Probabilistic Methods Applied to Power Syst. 2004, 843-849.
- [20] Miranda, V.; Saraiva, J. T. A. "Fuzzy Power Flow - An AC Model Addressing Correlated Data"; IEEE Trans. on Power Syst. 1992, 7, 223-232.
- [21] Sun H.; Yu D. C.; Xie Y. "Application of Fuzzy Set Theory to Power Flow Analysis with Uncertain Power Injections"; Proc. of IEEE Power Eng. Society, 2000, 2, 1191 - 1196.
- [22] Gaffarpour, R.; Pourmoosa, A. "Risk Assessment, Modeling, and Ranking for Power Network Facilities Regarding to Sabotage"; J. Passive Defence Sci. Tech. 2015, 6, 128-144 (In Persian).
- [13] Abdelaziz, A. R. "A Fuzzy-Based Power System Reliability Evaluation"; Electric Machines & Power Syst. 1999, 27, 271-278.
- [14] Dubois, D. J. "Fuzzy Sets and Systems: Theory and Applications (Mathematics in Science & Engineering)"; New York, NY, Academic Press (HBJ), 1980.
- [15] Hatziargyriou, N. D.; Karakatsanis, T. S. "Probabilistic Load Flow for Assessment of Voltage Instability"; IEE Proceedings of Generation, Transmission and Distribution, 1999, 145, 196-202.
- [16] Dimitrovski, A.; Tomsovic, K. "Boundary Load Flow Solutions"; IEEE Trans. on Power Syst. 2003, 19, 348-455.
- [17] Hao, L.; Shi, G.; Xu, Y. "Study on the Fuzzy AC Power Flow Model"; Proc. of Intelligent Control and Automation. Hangzhou, P. R. China, 2004, 5092-5096.