مجله علمی پژوهشی «علوم و فناوری‌های پدافند نوین»
سال ششم، شماره ۲، تابستان ۱۳۹۴؛ ص ۱۴۴-۱۲۷

ارزیابی، مدل‌سازی و رتبه‌بندی ریسک برای تجهیزات شبکه برق در برابر خرابکاری‌های عمدی

رضا غفارپور[۱*]، علی‌اصغر پورموسی[۲]
۱- عضو هیات علمی دانشگاه امام حسین (ع)، ۲- کارشناس ارشد دانشگاه صنعتی امیرکبیر
(دریافت: ۹۳/۰۷/۰۴، پذیرش: ۹۴/۰۳/۰۴)

چکیده

شبکه‌های قدرت به عنوان یکی از زیرساخت‌های حیاتی، یک هدف استراتژیک برای حملات تروریستی می‌باشند. بنابراین ارائه راهکارهایی برای مقابله با این تهدیدات در ارزیابی امنیت سامانه امری ضروری به نظر می‌رسد. هدف از این مقاله ارائه روشی مبتنی بر ارزیابی ریسک است که به برنامه‌ریزان این امکان را می‌دهد تا امنیت سامانه قدرت را با در نظر گرفتن تهدیدات تروریستی احتمالی ارزیابی کنند. در این روش، ابتدا متغیرهای تأثیرگذار بر روی تصمیم گروه‌های تروریستی در حمله به سامانه قدرت مشخص شده و سپس با به‌کارگیری شبکه بیزین که منتج شده از تئوری احتمالات است، مدلی برای پیش‌بینی میزان احتمال حمله به تجهیزات شبکه قدرت و نتایج احتمالی آن پیشنهاد می‌شود. در نهایت با تعیین میزان آسیب ناشی از حمله به شبکه برق، مدل پیشنهاد شده به منظور محاسبه ریسک ناشی از حملات به تجهیزات سامانه قدرت مورد استفاده قرار می‌گیرد. همچنین به منظور ارزیابی کارایی روش پیشنهاد شده، میزان ریسک برای مؤلفه‌های یک شبکه خاص محاسبه شده و تجهیزات این شبکه بر اساس میزان ریسک رتبه‌بندی می‌شوند.

کلید واژه‌ها: سامانه قدرت، ارزیابی امنیت، تهدیدات تروریستی، تئوری احتمالات، ارزیابی ریسک، شبکه بیزین.

Risk Assessment, Modeling, and Ranking for Power Network Facilities Regarding to Sabotage

R. Gaffarpour[*], A. A. Pourmoosa
Imam Hossein University
(Received: 20/07/2014; Accepted: 04/08/2015)

Abstract

The power networks as a critical infrastructures are strategic targets for terrorist attacks. Therefore, providing solutions to deal with these threats is necessary for security assessment. This paper presents a method based on the risk assessment by which the planners are able to evaluate the power network security regarding to terrorist attacks. In this way, first, the variables affecting the terrorist groups decision-making for attacking the power systems are determined, and then by employing the Bayesian network which is derived from the probability theory, a model is proposed to estimate the probability of the attack against the power network facilities and its possible consequences. Finally, by determining the extend of damage caused by the attack on power network, the proposed model is used to calculate the risk of the attack on power system facilities. Also, in order to validate the effectiveness of the proposed method, the risk value for a specific network is estimated and its facilities are ranked according to the level of risk.

Keywords: Power Network, Terrorist Attacks, Probabilities Theory, Risk Assessment, Bayesian Network.

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

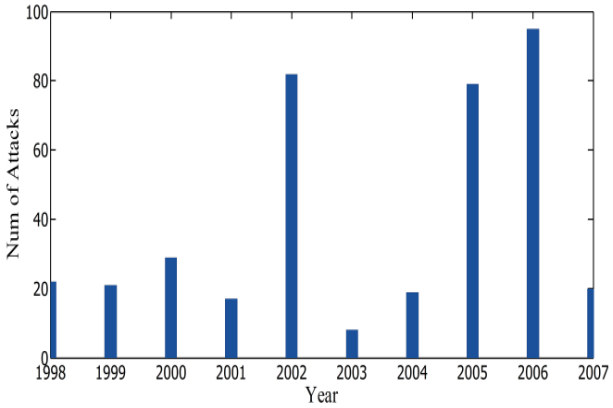
۱. مقدمه

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[1] 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 گردد. اختلال بر اثر عوامل طبیعی، خطای انسانی، خطای تجهیزات و حملات فیزیکی و سایبری[2] توسط گروه‌های تروریستی از مهم‌ترین عواملی هستند که باعث آسیب‌پذیری سامانه قدرت می‌شوند. از میان عوامل فوق، حمله تروریستی که به صورت سازمان‌یافته و با هدف ایجاد بیشترین آسیب به تجهیزات سامانه قدرت صورت می‌گیرد از اهمیت بسیار بالایی برخوردار است.

میزان حملات تروریستی صورت گرفته بر روی سامانه قدرت در نقاط مختلف جهان در شکل (۱) نشان داده شده است. بر اساس این شکل، تعداد حملات صورت گرفته بیانگر اهمیت بالای این زیرساخت حیاتی برای گروه‌های تروریستی بوده و شواهد و مدارک موجود نشان می‌دهد که تجهیزات شبکه قدرت در برابر این حملات بسیار آسیب‌پذیر می‌باشند [۱]. بنابراین، افزایش تعداد حملات تروریستی در نواحی مختلف جهان نشان می‌دهد که در ارزیابی امنیت شبکه قدرت که بیانگر میزان توانایی شبکه در تحمل اختلالات ناگهانی و یا خرابی تجهیزات بدون ایجاد وقفه در سرویس‌رسانی به مشتریان است [۲]. علاوه بر عوامل طبیعی یا غیرعمدی، عوامل غیرطبیعی یا عمدی مانند تهدیدات تروریستی نیز باید در نظر گرفته شوند. در نتیجه، اتخاذ اقدامات مؤثر به منظور جلوگیری و یا محدود کردن این حملات امری ضروری به نظر می‌رسد. با این حال، مسئله مهمی که در زمینه ارزیابی امنیت سامانه قدرت با در نظر گرفتن حملات تروریستی وجود دارد بحث عدم قطعیت در این نوع حملات است [۳]. اولین عدم قطعیت، مربوط به رخ دادن حملات بر روی سامانه قدرت (میزان احتمال حمله) و دومین عدم قطعیت مرتبط با تأثیر حملات بر روی رفتار و عملکرد سامانه قدرت (نتیجه حمله) است. از طرفی دیگر، به دلیل گستردگی سامانه قدرت و همچنین محدود بودن امکانات و منابع مالی و انسانی، حفاظت از تجهیزات شبکه قدرت به طور کامل امکان‌پذیر نمی‌باشد. بنابراین، ارائه راهکارهایی به منظور شناسایی و رتبه‌بندی تجهیزاتی که دارای بالاترین میزان ریسک در برابر حملات تروریستی هستند، می‌تواند در این زمینه بسیار مفید باشد. همچنین رتبه‌بندی تجهیزات بر حسب میزان ریسک به برنامه‌ریزان سامانه قدرت این امکان را می‌دهد که بتوانند شاخصی برای سطح امنیت تجهیزات شبکه تعیین کرده و اقدامات لازم را به منظور کاهش آسیب‌پذیری تجهیزات در برابر حملات تروریستی اتخاذ نمایند.

در این مقاله به منظور ارزیابی امنیت شبکه قدرت و همچنین محاسبه میزان ریسک برای تجهیزات شبکه در برابر حملات تروریستی یک روش احتمالاتی که بر پایه عدم قطعیت استوار است ارائه شده است. در این روش با ارائه مدلی مبتنی بر شبکه بیزین میزان احتمال حمله به هر یک از تجهیزات شبکه قدرت و پیامدهای ناشی از این حملات تعیین می‌شود. سپس با به‌کارگیری نتایج حاصل از مدل‌سازی می‌توان تجهیزات مختلف سامانه قدرت را بر حسب میزان ریسک آن‌ها رتبه‌بندی کرد. بر همین اساس ساختار کلی مقاله به بخش‌های زیر تقسیم می‌شود:

در بخش اول پیشینه‌ای از تحقیقات صورت گرفته در زمینه ارزیابی امنیت سامانه قدرت ارائه می‌شود. در بخش دوم، روش محاسبه ریسک برای تجهیزات شبکه قدرت مورد بررسی قرار گرفته و روش مدل‌سازی ریسک ناشی از حملات تروریستی بر روی تجهیزات سامانه قدرت ارائه می‌شود. در انتهای این بخش، رتبه‌بندی تجهیزات مختلف سامانه قدرت بر حسب میزان ریسک ناشی از حملات تروریستی بر روی آن‌ها در بخش هفتم ارائه شده و یک الگوریتم کلی برای این رتبه‌بندی[3] پیشنهاد می‌شود. در بخش سوم به منظور ارزیابی و پیاده‌سازی الگوریتم پیشنهادی، ریسک ناشی از حملات تروریستی بر روی تجهیزات یک سامانه قدرت استاندارد محاسبه شده و تجهیزات این سامانه بر اساس میزان ریسک رتبه‌بندی می‌شوند. در بخش چهارم نتایج به‌دست آمده از بخش سوم مورد تجزیه و تحلیل قرار می‌گیرد. در نهایت، نتیجه‌گیری و ارائه پیشنهادها نیز در بخش پنجم ارائه می‌گردد.



شکل ۱. تعداد حملات تروریستی بر روی سامانه قدرت

۱-۱. پیشینه تحقیق

در زمینه حملات تروریستی به زیرساخت‌های الکتریکی تاکنون تحقیقاتی مختلفی انجام شده که این تحقیقات بیشتر بر روی حملات تروریستی سایبری متمرکز است. در مرجع [۴]، با استفاده از روش فازی[4] شاخصی برای امنیت سایبری زیرساخت‌های حیاتی از جمله زیرساخت‌های الکتریکی ارائه شده است. در مرجع [۵]، ارزیابی امنیت

[1] Critical Infrastructure
[2] Physical and Cyber Attacks
[3] Ranking
[4] Fuzzy Method

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. در نهایت راهکارهایی برای مقاوم‌تر کردن پست‌ها در برابر حملات تروریستی سایبری پیشنهاد شده است. در تحقیقی دیگر [۶]، آسیب‌های ناشی از حملات تروریستی بر روی سامانه قدرت بررسی شده و راهکارهایی برای حفاظت مؤثر از تجهیزات سامانه در برابر تهدیدات تروریستی ارائه شده است. در مرجع [۷]، 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. ارائه روشی برای ارزیابی امنیت شبکه‌های هوشمند[1] با استفاده از نظریه بازی‌ها[2] در مرجع [۸] نشان داده است. 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 استراتژی‌ها به منظور مقابله با حملات تروریستی برای کاهش ریسک ارائه می‌شود. در تحقیقی دیگر [۹]، 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.

۲. روش پیشنهادی

۲-۱. تعریف ریسک ناشی از حملات تروریستی بر روی تجهیزات سامانه قدرت

به دلیل گستردگی جغرافیایی شبکه قدرت و بزرگ بودن ابعاد آن و همچنین قابل پیش‌بینی نبودن فعالیت‌های تروریست‌ها، انجام تمام سناریوهای حمله به سامانه قدرت و ارزیابی نتایج آن غیرممکن است. یک راه حل منطقی برای غلبه بر این مشکل استفاده از روش‌های ارزیابی ریسک است که توسط آن می‌توان محتمل‌ترین سناریوهای حمله به تجهیزات شبکه را با استفاده از آن پیش‌بینی کرد.

مفهوم ریسک عبارت است از نتایج و پیامدهای مورد انتظار ناشی از تهدیدات صورت گرفته بر روی یک هدف مشخص و با در نظر گرفتن آسیب‌های وارده به آن هدف. به صورت ریاضی می‌توان ریسک را به صورت زیر تعریف کرد [۱۰]:

$$R = P(A) \times P(C \mid A) \times E(D \mid A,C) \quad (۱)$$

در فرمول بالا، $P(A)$ احتمال حمله به هدف مورد نظر، $P(C|A)$ احتمال نتیجه‌بخش بودن حمله در صورت وقوع آن و $E(D|A, C)$ میزان آسیب رسیدن به هدف در صورت وقوع حمله و نتیجه‌بخش بودن آن می‌باشد. فرمول بالا نشان می‌دهد که ریسک ناشی از حمله به تجهیزات سامانه قدرت به سه عامل احتمال حمله به آن تجهیزات، نتیجه‌ای که آن حمله می‌تواند در پی داشته باشد و میزان آسیبی[3] که بر اثر نتیجه‌بخش بودن حمله می‌تواند به سامانه وارد شود بستگی دارد.

در ادامه این مقاله با در نظر گرفتن عوامل مؤثر بر روی ریسک، روشی برای مدل‌سازی این عوامل ارائه شده و با استفاده از مقادیر احتمال به‌دست آمده میزان ریسک برای هر یک از تجهیزات شبکه قدرت محاسبه می‌شود و در نهایت این تجهیزات بر اساس میزان ریسک رتبه‌بندی می‌شوند.

۲-۲. مدل‌سازی ریسک ناشی از حملات تروریستی بر روی تجهیزات سامانه قدرت

مسئله اصلی در مواجهه با حملات تروریستی این است که این حملات از قبل برنامه‌ریزی می‌شوند. بنابراین حوادث ناشی از این حملات دارای درجه بالایی از عدم قطعیت می‌باشند. به طور کلی به‌کارگیری عبارت عدم قطعیت در مورد پدیده تروریسم به دلیل کمبود اطلاعات در مورد رفتار گروه‌های تروریستی است. در نتیجه اگر موارد قطعی‌ای به این گروه‌ها نسبت داده شود، در واقع احتمالات مربوط به رفتار گروه‌های تروریستی نادیده گرفته می‌شود که این امر ممکن است باعث بروز خطا در مدل‌سازی گردد. بنابراین در چنین مواردی می‌توان از روش‌هایی مانند شبکه بیزین[4] که مبتنی بر عدم قطعیت می‌باشد، استفاده کرد.

ساختار شبکه بیزین و نحوه پیاده‌سازی آن به منظور محاسبه ریسک [۱۱]: روش بیزین به ساده‌ترین شکل به صورت زیر تعریف می‌شود:

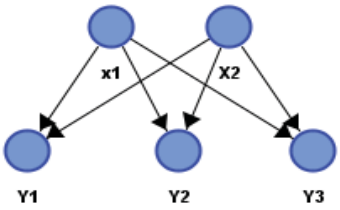
$$P(b \mid a) = \frac{P(a \mid b) \times P(b)}{P(b)} \quad (۲)$$

در این رابطه، $P(a)$ بیانگر احتمال وقوع پدیده a، $P(b|a)$ بیانگر احتمال وقوع پدیده b از میان احتمال وقوع پدیده a، $P(a|b)$ بیانگر احتمال وقوع پدیده a از میان احتمال وقوع پدیده b و $P(b)$ بیانگر احتمال وقوع پدیده b است.

در شبکه بیزین، هر یک از متغیرها به صورت یک گره[5] مدل می‌شود. برای هر گره نیز حالت‌های مختلفی وجود دارد که به هر یک از این حالت‌ها مقداری متناظر با میزان احتمال وقوع آن حالت اختصاص می‌یابد. گره‌ها توسط پیکان‌هایی که نشان دهنده جهت رابطه علت- معلولی است به هم متصل می‌شوند که این پیکان‌ها آرک[6] نامیده می‌شوند. شکل (۲) نمونه‌ای از یک شبکه بیزین را نشان می‌دهد. در این شکل گره‌هایی که پیکان از آن‌ها خارج می‌شود گره مادر (علت) و گره‌هایی که پیکان به آن‌ها وارد می‌شود گره فرزند (معلول) نامیده می‌شوند. نحوه تأثیرگذاری یک گره بر روی سایر

[1] Smart Grid
[2] Game Theory
[3] Damage
[4] Bayesian Network
[5] Node
[6] Arc

گره‌ها توسط جداول احتمال شرطی که برای هر گره فرزند به صورت جداگانه تعریف می‌شود مشخص می‌گردد که مقادیر آن بر اساس اطلاعات و تجارب پیشین و همچنین نظرات کارشناسان تعیین می‌شود. احتمال شرطی به طور کلی با نماد ریاضی $P(x|p_1, p_2, ..., p_n)$ نشان داده می‌شود. این عبارت بیانگر احتمال متغیر X در حالت x که توسط گره مادر P_1 در حالت p_1، گره مادر P_2 در حالت p_2 و گره مادر Pn درحالت p_n به‌دست می‌آید.



شکل ۲. نمایش گره‌ها و ارتباطات میان آن‌ها در روش بیزین

در این مقاله خروجی حاصل از تشکیل شبکه بیزین، یافتن مقادیر احتمال وقوع حمله به هر یک از تجهیزات سامانه قدرت و همچنین تعیین نتایج احتمالی این حمله با در نظر گرفتن متغیرهایی نظیر عوامل سیاسی، اقتصادی، اجتماعی، فنی، جغرافیایی و ... می‌باشد. به منظور تشکیل شبکه بیزین، فرضیات زیر در نظر گرفته می‌شود:

الف. هر متغیر در شبکه بیزین حالت‌هایی را اختیار می‌کند که مجموعه این حالت‌ها دوبه‌دو از یکدیگر مستقل هستند.

ب. وقوع یک حمله تروریستی مستقل از تعداد حملاتی است که در یک دوره زمانی معین توسط گروه‌های تروریستی رخ می‌دهد. به عبارتی دیگر، حملاتی که به طور قطعی توسط تروریست‌ها در یک بازه زمانی معین انجام می‌شود مد نظر ما نیست، بلکه منظور حملاتی است که از قبل پیش‌بینی نشده است.

جمع‌آوری اطلاعات: اولین گام در پیاده‌سازی شبکه بیزین، جمع‌آوری اطلاعات، داده‌ها، شواهد و مدارک می‌باشد. به طور کلی این اطلاعات را می‌توان در دسته‌های زیر طبقه‌بندی کرد:

الف. دسته اول شامل اطلاعاتی از ساختار کلی شبکه قدرت مورد نظر، تعداد تجهیزات سامانه، مشخصات فنی آن‌ها، موقعیت جغرافیایی تجهیزات، وضعیت شبکه قدرت در شرایط کاری مختلف، تعداد حملات صورت گرفته به شبکه در زمان‌های گذشته و ... می‌باشد.

ب. دسته دوم شامل اطلاعاتی از وضعیت کلی گروه‌های تروریستی شامل میزان فعالیت آن‌ها، امکانات و منابع تحت اختیار آن‌ها، محل استقرار این گروه‌ها، نواحی تحت تصرف آن‌ها، ساختار سازمانی آن‌ها، اطلاعاتی در مورد اقدامات گذشته این گروه‌ها، ایدئولوژی[1] و تفکرات حاکم بر این گروه‌ها و ... می‌باشد.

منابع جمع‌آوری اطلاعات برای تشکیل شبکه بیزین شامل موارد زیر می‌باشد:

- مدارک و شواهد موجود از حملات تروریستی در نقاط مختلف جهان.
- مطالعه و جمع‌آوری اطلاعات در مورد شبکه قدرت مورد نظر و شرایط مختلف عملکرد آن.
- استفاده از نرم‌افزار شبیه‌سازی سامانه قدرت.
- استفاده از نظرات متخصصین در حوزه‌های مختلف شامل حوزه تروریسم، روانشناسی، جامعه‌شناسی، برق و ...

متغیرهای مورد استفاده در شبکه بیزین: همان‌طور که قبلاً نیز اشاره شد، هدف از تشکیل شبکه بیزین در این مقاله، یافتن دو پارامتر اصلی تأثیرگذار بر روی میزان ریسک تجهیزات شبکه قدرت یعنی پارامتر "احتمال حمله[2]" و همچنین پارامتر "نتیجه حمله[3]" می‌باشد. بنابراین در ادامه ابتدا پارامتر "احتمال حمله" و متغیرهای تأثیرگذار بر روی آن مورد تحلیل و بررسی قرار گرفته و سپس متغیرهای تأثیرگذار بر روی پارامتر "نتیجه حمله" و چگونگی پیاده‌سازی آن در شبکه بیزین ارائه می‌شود. لازم به ذکر است که برای جمع‌آوری اطلاعات و تعیین متغیرهای شبکه بیزین، شبکه قدرت مورد نظر باید از قبل مشخص گردد. در این مقاله یک سامانه قدرت ۶ باسه با مشخصات نشان داده شده در بخش سوم برای این منظور در نظر گرفته شده است.

الف. احتمال حمله

با توجه به تجزیه و تحلیل اطلاعات و مدارک جمع‌آوری شده از شبکه قدرت و همچنین وضعیت گروه‌های تروریستی فعال در منطقه، مهم‌ترین متغیرهای تأثیرگذار بر روی پارامتر "احتمال حمله" به صورت زیر می‌باشد [۱۲]:

انگیزه حمله[4]:اولین متغیر تأثیرگذار بر روی پارامتر "احتمال حمله" متغیر "انگیزه حمله" می‌باشد. این متغیر نشان دهنده میزان تمایل تروریست‌ها به هدف قرار دادن مؤلفه خاصی از سامانه قدرت می‌باشد. این متغیر خود نیز به چندین متغیر وابسته است که شامل موارد زیر می‌باشد:

– **میزان فعالیت:** حالات مختلف مربوط به میزان فعالیت گروه‌های تروریستی را می‌توان به صورت زیر طبقه‌بندی کرد:

- **فعالیت زیاد:** در این حالت گروه‌های تروریستی توانسته‌اند با استفاده از ظرفیت‌های موجود، بخش‌های قابل توجه‌ای از یک ناحیه را تصرف کرده و سلاح‌ها و مهمات خود را در آنجا مستقر کنند. این فعالیت گروه‌های تروریستی می‌تواند حتی بیشتر هم باشد زمانی که منطقه تصرف شده توسط آن‌ها و محل استقرار آن‌ها نزدیک به یک کشور همسایه باشد که از این گروه‌ها طرفداری می‌کند. در این صورت این گروه‌ها می‌توانند از کمک‌های کشور همسایه به منظور گسترش فعالیت خود استفاده نمایند.

[1] Ideology

[2] Attack Probability
[3] Consequence of the Attack
[4] Motivation of the Attack

• **فعالیت نسبتاً زیاد:** در صورتی می‌توان گفت که حضور و فعالیت گروه‌های تروریستی نسبتاً زیاد است که این گروه‌ها بتوانند مناطقی از یک کشور اما کوچک‌تر از حالت قبل را در اختیار خود گرفته و ادوات جنگی و سلاح‌های مورد نیاز خود را در آنجا پیاده‌سازی کنند. البته در این حالت نیز ممکن است محل استقرار آن‌ها به مناطق مرزی نزدیک باشد. اما در این حالت برخورداری این گروه‌ها از کمک‌های کشورهای دیگر به‌راحتی حالت قبل نیست.

• **فعالیت کم:** فعالیت کم گروه‌های تروریستی به این معناست که آن‌ها نتوانسته‌اند مناطق قابل‌توجهی را به کنترل خود درآورند. در این حالت این گروه‌ها قادر نیستند اقدامات قابل‌توجهی انجام دهند چراکه از نظر حوزه فعالیت و برخورداری از کمک‌های احتمالی کشورهای دیگر دارای محدودیت گسترده‌ای می‌باشند.

– **وضعیت سیاسی:** تروریسم به طور ذاتی یک پدیده سیاسی است. انگیزه‌های سیاسی که منجر به تحریک گروه‌های تروریستی می‌شوند، متغیر می‌باشند. به عنوان مثال، رفتار یک حکومت، سخنرانی تحریک‌آمیز یک رهبر یا نماینده مذهبی یا سیاسی، تصمیمات غلط اقتصادی در سطح کلان از این نوع محرک‌ها می‌باشد. در شبکه بیزین، متغیر "وضعیت سیاسی" بیانگر این است که اداره یک کشور و یا یک ناحیه به چه اندازه در اختیار حکومت قانونی آن کشور و یا ناحیه می‌باشد. وضعیت‌های مختلف این متغیر در جدول (۱) نشان داده‌شده است.

–**میزان حساسیت**[1]: این متغیر بیانگر این است که اگر یکی از تجهیزات سامانه قدرت بر اثر آسیب ناشی از حملات مشکلی در عملکرد آن به وجود آید تا چه اندازه می‌تواند بر روی عملکرد کل سامانه تأثیرگذار باشد.حالات مختلف میزان حساسیت تجهیزات سامانه قدرت را می‌توان به صورت زیر طبقه‌بندی کرد:

• **بالا:** از دست رفتن این نوع تجهیزات در عملکرد سامانه بسیار مهم بوده و تعمیر و بازیابی آن نیز بسیار هزینه‌بر و زمان‌بر خواهد بود. اگر این نوع از تجهیزات آسیب ببینند، قابلیت اطمینان سامانه شدیداً کاهش یافته و حتی ممکن است باعث فروپاشی بخشی و یا کل شبکه مورد نظر گردد.

• **متوسط:** در این حالت از بین رفتن تجهیزات باعث وقفه در سرویس‌رسانی به مصرف کنندگان برای مدت نه‌چندان زیاد شده و در برخی موارد ممکن است با ایجاد شرایط اضطراری شدید در شبکه باعث از دست رفتن بخش‌هایی از سامانه قدرت گردد.

• **کم:** در این حالت، تجهیزات آسیب دیده تأثیر کمی بر روی سامانه داشته و بخش بسیار کوچکی از شبکه را تحت تأثیر قرار می‌دهند.

متغیر "انگیزه حمله" خود نیز دارای حالت‌های مختلف می‌باشد که در جدول (۱) نشان داده است.

[1] Criticality

قابلیت و قدرت تروریست‌ها[2]: دومین متغیر تأثیرگذار بر روی پارامتر "احتمال حمله" متغیر "قابلیت و قدرت تروریست‌ها" می‌باشد. قابلیت و قدرت گروه‌های تروریستی نشان دهنده سطح امکانات مالی و نظامی و همچنین به معنای توانایی این گروه‌ها در برنامه‌ریزی، سازمان‌دهی و انجام حملات می‌باشد. متغیرهای تأثیرگذار بر روی قابلیت و قدرت تروریست‌ها شامل موارد زیر است [۱۲ و ۱۳]:

–**ساختار سازمانی:** این متغیر نشان دهنده ویژگی‌های بدنه اصلی تشکیل دهنده گروه‌های تروریستی می‌باشد. به عبارتی دیگر متغیر "ساختار سازمانی" بیانگر این است که تعداد نفرات گروه‌های تروریستی چه اندازه می‌باشد؟ آیا گروه‌ها به صورت پراکنده‌اند و یا اینکه در یک مکان به صورت متمرکز قرار دارند. افراد تشکیل دهنده گروه دارای چه تفکراتی می‌باشند؟ رهبری آن‌ها چگونه است؟ آیا رهبر آن‌ها واحد می‌باشد و یا اینکه به صورت شورایی اداره می‌شود؟ حالات مختلف متغیر "ساختار سازمانی" در جدول (۱) نشان داده شده است.

–**منابع:** منابع مورد نیاز برای گروه‌های تروریستی شامل منابع مالی و فیزیکی می‌باشد. تأمین منابع مالی یکی از دغدغه‌های بزرگ گروه‌های تروریستی می‌باشد. تروریست‌ها می‌توانند با داشتن پول کافی، تجهیزات بیشتر و پیشرفته‌تر خریداری کنند، افراد مختلفی را برای جاسوسی و به‌دست آوردن اطلاعات لازم به‌کار گیرند و حتی مقداری از پول‌ها را برای فراهم کردن امکانات بهتر برای اعضای خود به منظور راضی نگه‌داشتن آن‌ها صرف کنند. منابع فیزیکی نیز شامل تجهیزات جنگی، انواع سلاح‌ها، وسایل حمل و نقل ادوات جنگی و ... می‌باشد. این منابع نقش مهمی در تعیین اهدافی دارند که تروریست‌ها امیدوارند حملات موفقیت‌آمیزی بر روی آن‌ها انجام دهند. وضعیت‌های مختلف متغیر "منابع" در جدول (۱) نشان داده شده است.

متغیر "قابلیت و قدرت تروریست‌ها" خود نیز دارای حالت‌های مختلف می‌باشد که در جدول (۱) نشان داده است.

آسیب‌پذیری تجهیزات[3]: سومین متغیر تأثیرگذار بر روی پارامتر "احتمال حمله" متغیر "آسیب‌پذیری تجهیزات" سامانه قدرت می‌باشد. این متغیر نیز خود به چندین متغیر وابسته است که در ادامه مورد بررسی قرار می‌گیرد [۱۳ و ۱۴]:

–**مشاهده‌پذیری**[4]: این متغیر بیانگر این است که تجهیزات سامانه قدرت تا چه اندازه در دیدرس گروه‌های تروریستی بوده و موقعیت نسبی تروریست‌ها نسبت به تجهیزات (مؤلفه‌ها) مختلف شبکه قدرت چگونه است. حالات مختلف مربوط به متغیر "مشاهده‌پذیری" را می‌توان به صورت زیر طبقه‌بندی کرد:

[2] Capability
[3] Vulnerability
[4] Visibility

• **مشاهده‌پذیری بالا:** این حالت زمانی اتفاق می‌افتد که اهداف مورد نظر کاملاً در دیدرس گروه‌های مهاجم بوده و این گروه‌ها می‌توانند با کمترین میزان جابه‌جایی از محل استقرار خود حملاتی را بر روی هدف مورد نظر ترتیب دهند.

• **مشاهده‌پذیری متوسط:** در این حالت، اهداف نسبت به حالت قبل در فاصله بیشتری از محل استقرار تروریست‌ها قرار دارد. در این صورت این گروه‌ها می‌توانند از محل استقرار خود حملات موشکی بر روی اهداف مورد نظر انجام دهند اما به دلیل دور بودن اهداف این حملات دارای تأثیر کمتری نسبت به حالت قبل است.

• **مشاهده‌پذیری پایین:** این حالت زمانی اتفاق می‌افتد که اهداف مورد نظر به راحتی قابل مشاهده نبوده و در فاصله دوری از محل استقرار گروه‌های تروریستی قرار دارد. در این صورت این گروه‌ها مجبورند با جابه‌جایی نفرات و ادوات جنگی خود را به اهداف مورد نظر نزدیک‌تر کنند که این خود میزان ریسک را برای این گروه‌ها افزایش می‌دهد، چراکه ممکن است توسط نیروهای حکومتی غافل‌گیر شوند.

-**دسترس‌پذیری**[1]: این متغیر نشان دهنده محل استقرار تجهیزات سامانه قدرت در موقعیت‌های جغرافیایی مختلف و میزان دسترسی تروریست‌ها به این تجهیزات می‌باشد. حالات مختلف مربوط به متغیر "دسترس‌پذیری" را می‌توان به صورت زیر طبقه‌بندی کرد:

• **دسترس‌پذیری بالا:** در این حالت، تجهیزات سامانه قدرت در مناطقی دور افتاده و دور از نواحی شهری قرار دارند. بنابراین میزان دسترسی تروریست‌ها به این تجهیزات بالا بوده و اگر خطری این تجهیزات را تهدید کند به دلیل موقعیت این تجهیزات، نیروهای امنیتی قادر نخواهند بود خطر را به‌سرعت دفع کنند.

• **دسترس‌پذیری متوسط:** در این حالت، تجهیزات سامانه قدرت نسبت به حالت قبل در فواصل نزدیک‌تری به مناطق شهری و دارای جمعیت قرار دارند ولی فاصله آن‌ها آن‌قدر هم نزدیک به مناطق شهری نیست که بتوان حفاظت کامل از آن را به عمل آورده و در هنگام بروز خطر نیروهای امنیتی به منظور دفع خطر به سرعت وارد عمل شوند. در این شرایط میزان دسترسی تروریست‌ها به تجهیزات سامانه به راحتی حالت قبل نیست.

• **دسترس‌پذیری پایین:** در این حالت، تجهیزات سامانه قدرت در نواحی شهری و یا حومه شهر قرار دارند، سطح حفاظت و امنیت آن‌ها نسبتاً قابل قبول و در برخی موارد بسیار خوب بوده و در صورت بروز خطر، نیروهای امنیتی به سرعت وارد عمل می‌شوند.

-**سطح امنیت و حفاظت:** میزان امنیت و سطوح حفاظتی تجهیزات شبکه قدرت می‌تواند برنامه‌ریزی صورت گرفته توسط گروه‌های تروریستی را تحت‌الشعاع قرار داده و یا حتی تصمیم آن‌ها را در حمله به یک هدف خاص تغییر دهد. گروه‌های تروریستی معمولاً به اهدافی حمله می‌کنند که سطوح حفاظت و امنیت آن‌ها پایین است.

وضعیت‌های مختلف متغیر سطح حفاظت و امنیت در جدول (۱) نشان داده شده است.

-**روش حمله**: متغیر دیگری که بر روی آسیب‌پذیری تجهیزات تأثیرگذار است متغیر "روش حمله" می‌باشد. گروه‌های تروریستی می‌توانند به دو روش به هدف مورد نظر حمله نمایند [۱۳]:

• **حمله مستقیم:** در این روش، گروه‌های تروریستی مستقیماً و با به‌کارگیری انواع سلاح‌ها به هدف مورد نظر حمله می‌کنند. این روش نیز می‌تواند به دو روش تقسیم شود. در روش اول گروه‌های تروریستی به صورت گروه‌های مجزا که هر واحد می‌تواند از تعداد معدودی از نفرات تشکیل شود، به هدف مورد نظر حمله می‌کنند. در روش دوم، تروریست‌ها به صورت واحدهای منسجم و یکپارچه وارد عمل می‌شوند. این حالت ممکن است زمانی رخ دهد که گروه‌های تروریستی به دلیل ریسک بالا امکان پراکنده شدن و به صورت گروه‌های مجزا درآمدن را نداشته باشند.

• **حمله غیرمستقیم:** در این روش، هدف مورد نظر به طور مستقیم مورد حمله قرار نمی‌گیرد بلکه آسیب رساندن به هدف با استفاده از حمله به تجهیزات دیگر صورت می‌گیرد. به عنوان مثال در مورد یک نیروگاه، گروه‌های تروریستی می‌توانند با هدف قرار دادن تانکرها و یا لوله‌های انتقال سوخت، عملاً عملکرد نیروگاه را که قلب تپنده سامانه قدرت می‌باشد، تحت تأثیر قرار دهند.

متغیر "آسیب‌پذیری تجهیزات" خود نیز دارای حالت‌های مختلف می‌باشد که در جدول (۱) نشان داده است.

ارزش تجهیزات: چهارمین متغیر تأثیرگذار بر روی پارامتر "احتمال حمله" متغیر "ارزش تجهیزات" سامانه قدرت می‌باشد. ارزش تجهیزات خود به نوع تجهیزات، سطح فناوری به‌کار رفته در آن‌ها و ... بستگی دارد. به عنوان مثال واضح است که نیروگاه‌ها نسبت به پست‌ها از ارزش بسیار بالاتری برخوردارند. در نگاه اول ممکن است به نظر برسد که هر چه ارزش تجهیزات بیشتر باشد احتمال حمله به آن بیشتر است. این دیدگاه در حالت کلی درست نیست. به عنوان مثال خطوط انتقال دارای ارزش کمتری نسبت به نیروگاه‌ها می‌باشند اما به دلیل گستردگی خطوط انتقال بیشترین حملات بر روی این مؤلفه‌ها صورت می‌گیرد. حالت‌های مختلف متغیر "ارزش تجهیزات" در جدول (۱) نشان داده است.

با در نظر گرفتن تمامی متغیرهای تأثیرگذار بر روی پارامتر "احتمال حمله" حالت‌های مختلف این پارامتر در جدول (۱) نشان داده شده است. با توجه به حالت‌های مختلف جدول (۱)، احتمال حمله به هر یک از تجهیزات سامانه قدرت به صورت زیر محاسبه می‌شود:

$$P(A) = P(L) + P(M) + P(H) \qquad (۳)$$

[1] Accessibility

در فرمول بالا $P(L)$, $P(M)$, $P(H)$ به ترتیب مقدار احتمال حمله مربوط به حالت‌های پایین، متوسط و بالا می‌باشند.

ب. نتیجه (شدت) حمله

این پارامتر بیانگر این است که اگر حمله‌ای به یکی از مؤلفه‌های سامانه قدرت صورت پذیرد، نتیجه آن حمله و شدت تأثیر آن بر روی سامانه قدرت تا چه اندازه می‌باشد. عوامل تأثیرگذار بر روی پارامتر "نتیجه حمله" شامل موارد زیر می‌باشد:

-**احتمال حمله**: اولین متغیر تأثیرگذار بر روی نتیجه حمله، احتمال حمله می‌باشد. این در واقع یک امر بدیهی می‌باشد زیرا تا زمانی که حمله‌ای صورت نگیرد، نتیجه‌ای حاصل نخواهد شد.

-**ارزش تجهیزات**:دومین متغیر تأثیرگذار بر روی نتیجه حمله متغیر "ارزش تجهیزات" می‌باشد. در واقع هرچه هدف مورد نظر دارای ارزش بالاتری باشد، شدت تأثیر آن بر روی سامانه قدرت بیشتر بوده و آسیب بیشتری به شبکه وارد می‌کند.

شرایط سامانه قدرت: سومین متغیر تأثیرگذار بر روی پارامتر "نتیجه حمله" شرایطی است که سامانه قدرت پس از وقوع حمله در آن شرایط قرار می‌گیرد. حالت‌های مختلف این متغیر در جدول (۱) نشان داده شده است. در این جدول، شرایط اضطراری کنترل شده شرایطی است که سامانه دچار ناپایداری موقت می‌شود اما می‌توان با کنترل به موقع سامانه را از این حالت خارج کرد و البته در برخی مواقع ممکن است سامانه از این حالت به حالت اضطراری شدید تغییر وضعیت دهد. حالت اضطراری شدید یک حالت شدیداً ناپایدار است و حتی ممکن است شدت ناپایداری به حدی باشد که منجر به فروپاشی سامانه شود. بنابراین ممکن است در برخی مواقع برای جلوگیری از فروپاشی کامل شبکه، تولید را کاهش داده و یا بارهایی از سامانه خارج شود. حالت غیرقابل‌کنترل زمانی اتفاق می‌افتد که شدت حمله به سامانه قدرت بالا بوده و به بخش‌های حساس و بسیار حیاتی شبکه قدرت آسیب جدی وارد شود. در این صورت کنترل سامانه قدرت تقریباً ناممکن است [۱۵]. با در نظر گرفتن متغیرهای تأثیرگذار بر روی پارامتر "نتیجه حمله" حالت‌های مختلف این پارامتر در جدول (۱) نشان داده است.

در نهایت با در نظر گرفتن تمامی متغیرهایی که تاکنون مورد بررسی قرار گرفته‌اند، ساختار نهایی شبکه بیزین مربوط به مدل‌سازی ریسک ناشی از حملات تروریستی بر روی تجهیزات سامانه قدرت به صورت شکل (۳) پیاده‌سازی می‌شود.

جدول ۱. حالات مختلف متغیرهای شبکه بیزین

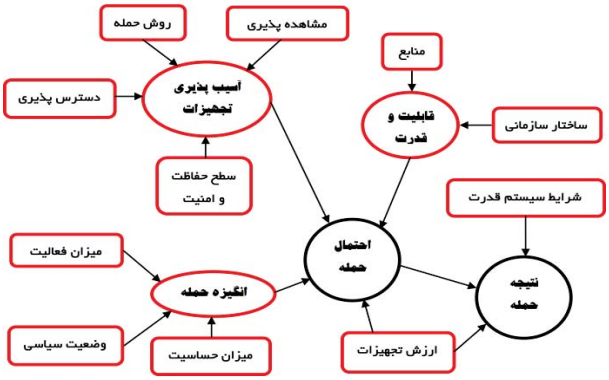
متغیر	حالت‌ها				
روش حمله	غیر مستقیم	مستقیم			
میزان فعالیت	کم	نسبتا زیاد	زیاد		
وضعیت سیاسی	آرام	نسبتا ناآرام	ناآرام		
منابع	ضعیف	متوسط	قوی		
شرایط سامانه قدرت	اضطراری کنترل شده	اضطراری شدید	غیر قابل کنترل		
میزان حساسیت	پایین	متوسط	بالا		
انگیزه حمله	پایین	متوسط	بالا		
قابلیت و قدرت	پایین	متوسط	بالا		
مشاهده پذیری	پایین	متوسط	بالا		
دسترس‌پذیری	پایین	متوسط	بالا		
سطح امنیت و حفاظت	پایین	متوسط	بالا		
ساختار سازمانی	پایین	متوسط	بالا		
آسیب‌پذیری	پایین	متوسط	بالا		
ارزش تجهیزات	پایین	متوسط	بالا		
احتمال حمله	بدون حمله	پایین	متوسط	بالا	
نتیجه حمله	بدون نتیجه	شدت کم	نسبتا شدید	شدید	فاجعه آمیز

اختصاص مقادیر احتمال به متغیرها: به منظور اختصاص مقادیر احتمال به هر یک از متغیرهای شبکه بیزین از نظرات متخصصان استفاده می‌شود. روشی که در این مقاله برای اختصاص مقادیر استفاده می‌شود به این صورت است که هر یک از متخصصان[1] بر اساس تجربه، داده‌ها و اطلاعات جمع‌آوری شده، شواهد و مدارک موجود مقدار احتمالی را به هر یک از حالت‌های متغیرهای شبکه بیزین اختصاص می‌دهد که این مقادیر می‌تواند عددی بین ۰ تا ۱ باشد. در نهایت با استفاده از مقدار میانگین اعداد اختصاص داده شده توسط همه متخصصان، می‌توان مقادیر احتمال مربوط به هر یک از متغیرها را تعیین نمود. ارزیابی متخصصان در مورد حالت‌های مختلف متغیرهای شبکه بیزین را می‌توان به فرم ماتریسی به صورت زیر نشان داد:

[1] Experts

$$A=\frac{1}{n}\begin{bmatrix} X_1 & X_2 & \dots & X_n \\ Y_1 & Y_1 & \dots & Y_n \\ Z_1 & Z_2 & \dots & Z_n \end{bmatrix}\begin{bmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{bmatrix} \quad (۴)$$

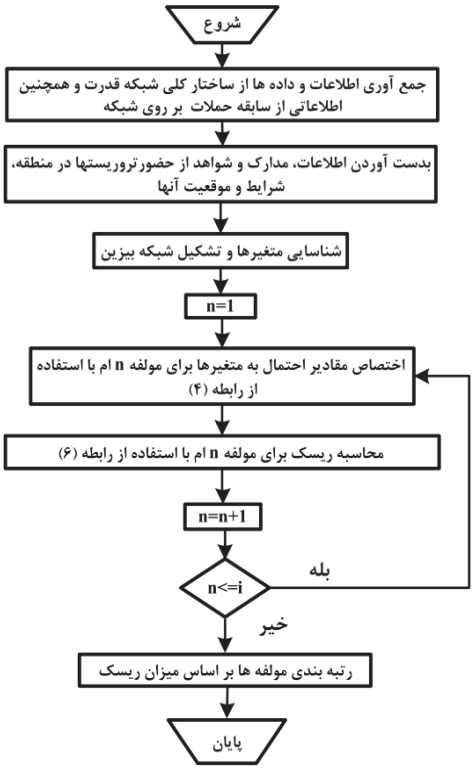
در رابطه بالا، X، Y و Z اعدادی هستند که هر یک از کارشناسان به سه حالت مختلف متغیرها اختصاص می‌دهند، n تعداد متخصصان و ω وزن مربوط به هر یک از متخصصان بوده و مقداری بین ۰ تا ۱ را اختیار می‌کند. این وزن بر اساس تجربه، سطح دانش و اطلاعات و همچنین سن متخصصان به هر یک از آن‌ها اختصاص می‌یابد. البته تعداد حالت‌های بعضی از متغیرهای شبکه بیزین در این مقاله کمتر یا بیشتر از سه حالت است که در این‌صورت تعداد سطرهای ماتریس معادله (۴) متناسب با تعداد حالت‌های متغیر مربوطه تغییر می‌کند.



شکل ۳. ساختار نهایی شبکه بیزین مربوط به مدل‌سازی ریسک ناشی از حملات تروریستی بر روی تجهیزات سامانه قدرت

۲-۳. محاسبه ریسک و رتبه بندی تجهیزات شبکه قدرت

بر اساس رابطه (۲)، میزان ریسک به دو پارامتر احتمال حمله و نتیجه حمله و همچنین میزان آسیب ناشی از نتیجه‌بخش بودن حمله وابسته است. مقادیر مربوط به پارامترهای احتمال حمله و نتیجه حمله را می‌توان با استفاده از شبکه بیزین تعیین کرد. پارامتر دیگری که بر روی محاسبه ریسک مؤثر است، میزان آسیب ناشی از حمله به تجهیزات سامانه قدرت است. این آسیب می‌تواند شامل آسیب‌های اقتصادی، زیست‌محیطی، جانی و ... باشد که در این مقاله فقط آسیب‌های اقتصادی برای محاسبه ریسک در نظر گرفته می‌شود. آسیب‌های اقتصادی نیز به دو دسته تقسیم می‌شوند. دسته اول مربوط به آسیب وارده به مؤلفه‌های شبکه و دسته دوم آسیبی است که به مصرف کنندگان برق براثر ایجاد اختلال ناشی از آسیب به هر یک از مؤلفه‌ها وارد می‌شود. در این مقاله هزینه تعمیر و یا تعویض مؤلفه آسیب دیده به عنوان معیاری برای نشان دادن میزان آسیب وارده به آن مؤلفه و همچنین درصد توان (بار) از دست رفته بر اثر آسیب به هر یک از تجهیزات، معادل با هزینه تحمیل شده و در نتیجه میزان آسیب وارده به مصرف کنندگان برق در نظر گرفته می‌شود.



شکل ۴. الگوریتم رتبه‌بندی ریسک ناشی از حملات تروریستی بر روی تجهیزات سامانه قدرت

بنابراین با در نظر گرفتن این هزینه‌ها، میزان آسیب ناشی از نتیجه‌بخش بودن حملات تروریستی به هریک از مؤلفه‌های شبکه قدرت را می‌توان به صورت زیر نشان داد:

$$D_T = F\left(C_F, C(P_L)\right) \quad (۵)$$

همان‌طور که از رابطه (۵) مشخص است، میزان آسیب تابعی از C_F هزینه تعمیر یا تعویض هر یک از مؤلفه‌ها و $C(P_L)$ هزینه تحمیلی به مصرف کنندگان به دلیل از دست رفتن بار ناشی از آسیب به هر یک از تجهیزات شبکه قدرت است. از طرفی دیگر باید در نظر داشت که در صورت وقوع یک حمله و نتیجه‌بخش بودن آن، میزان آسیب برای تمام حالت‌های پارامتر نتیجه حمله یکسان نبوده و لازم است این میزان متناسب با هر یک از حالت‌ها تعیین گردد. بر این اساس می‌توان فرمول نهایی محاسبه ریسک برای هریک از تجهیزات را به صورت زیر بیان نمود:

$$R = P(A)\sum_{i=1}^{4} P_i(C)\times D_{T_i} \quad (۶)$$

در رابطه (۶)، $P(A)$ میزان احتمال حمله به هریک از تجهیزات است که با استفاده از رابطه (۳) تعیین می‌شود، $P(C)$ میزان احتمال نتیجه‌بخش بودن حمله تروریستی و i نشان‌دهنده هر یک از حالت‌های پارامتر نتیجه حمله است.

به منظور رتبه‌بندی تجهیزات شبکه قدرت، ابتدا میزان ریسک برای هر یک از مؤلفه‌های شبکه با استفاده از رابطه (۶) محاسبه می‌شود. سپس مؤلفه‌ای را که دارای بیشترین میزان ریسک است به عنوان مبنا در نظر گرفته و با تعیین ریسک سایر تجهیزات نسبت به این

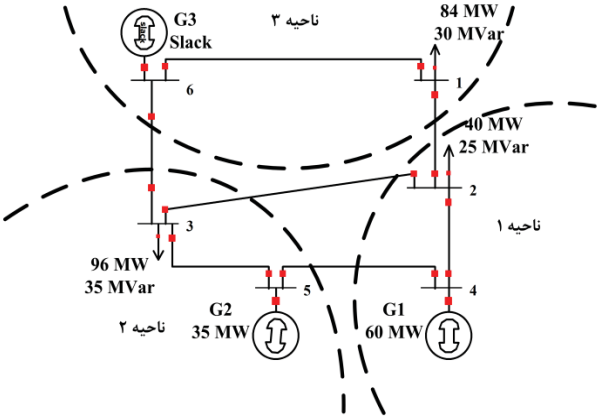
مبنا، تجهیزات مختلف شبکه بر حسب میزان ریسک از بالا به پایین رتبه‌بندی می‌شوند.

با در نظر گرفتن تمامی مراحل مدل‌سازی و محاسبه ریسک، الگوریتم رتبه‌بندی ریسک ناشی از حمله تروریستی به تجهیزات سامانه قدرت سامانه قدرت در شکل (۴) نشان داده است. در این الگوریتم، n تعداد مؤلفه‌های سامانه قدرت را نشان می‌دهد.

۳. مطالعه موردی

در این بخش الگوریتم پیشنهادی برای رتبه‌بندی ریسک، بر روی شبکه قدرت شش باسه که در شکل (۵) نشان داده است اعمال شده و نتایج حاصل از شبیه‌سازی مورد بحث و بررسی قرار می‌گیرد.

با توجه به شکل (۵)، این شبکه بر اساس میزان فعالیت تروریست‌ها و وضعیت سیاسی منطقه به سه ناحیه جداگانه تقسیم شده است. در ادامه پیاده‌سازی الگوریتم پیشنهادی بر روی سامانه قدرت مورد نظر به صورت گام‌به‌گام مورد بررسی قرار می‌گیرد.



شکل ۵. مشخصات سامانه قدرت و تقسیم‌بندی آن به نواحی مختلف

گام اول: اطلاعات، داده‌ها و مدارک به‌دست آمده از شبکه قدرت مورد نظر به صورت زیر است:

• **ساختار کلی سامانه:** همان‌طور که از شکل (۵) مشخص است.

سامانه مورد نظر دارای ۶ باس (پست)، ۷ خط انتقال و ۳ ژنراتور است باس ۶ به عنوان باس اسلک در نظر گرفته می‌شود.

• **مشخصات تجهیزات شبکه قدرت:** نیروگاه ۱ شامل ۴ واحد بخار، سیکل ترکیبی شامل ۴ واحد گازی و ۲ واحد بخار. نیروگاه ۲ شامل ۳ واحد بخار، سیکل ترکیبی شامل ۲ واحد گازی و ۱ واحد بخار. نیروگاه ۳ دارای ۱۰ واحد توربین آبی. پست ۱ دارای یک ترانس ۴۰۰/۲۳۰ کیلوولت، یک ترانس ۲۳۰/۱۳۲ کیلوولت و دو ترانس ۲۳۰/۶۳ کیلوولت. پست ۲ دارای یک ترانس ۴۰۰/۲۳۰ کیلوولت، یک ترانس ۲۳۰/۱۳۲ کیلوولت و دو ترانس ۱۳۲/۶۳ کیلوولت. پست ۳ دارای سه ترانس ۴۰۰/۱۳۲ کیلوولت و سه ترانس ۱۳۲/۶۳ کیلوولت. پست‌های ۴ و ۵ هرکدام دارای ۳ ترانس ۳۰/۴۰۰ کیلوولت و پست ۶ دارای ۴ ترانس ۳۰/۴۰۰ کیلوولت می‌باشند.

میزان حساسیت: بر اساس آنالیز پخش بار که توسط نرم‌افزار *power world* انجام شد، این نتایج برای نیروگاه‌ها، پست‌ها و خطوط انتقال استخراج شد: میزان حساسیت نیروگاه‌ها از بالا به پایین: نیروگاه ۳، نیروگاه ۱و نیروگاه۲. میزان حساسیت پست‌ها از بالا به پایین: پست ۶، پست۱، پست۴، پست۳، پست ۵ و پست۲.

میزان حساسیت خطوط از بالا به پایین: ۱-۶، ۶-۳، ۲-۴، ۵-۳، ۵-۴، ۳-۲، ۲-۱.

• **سطح حفاظت و امنیت:** در ناحیه ۱ ژنراتور ۱ و پست مربوط به آن دارای حفاظت متوسط است. پست ۲ نیز دارای حفاظتی نسبتاً متوسط بوده و خطوط انتقال در این ناحیه دارای حفاظت پایین می‌باشند. در ناحیه ۲ حفاظت ژنراتور ۲ و پست آن پایین، پست ۳ دارای حفاظت نسبتاً بالا و خط انتقال دارای حفاظت نسبتاً قابل قبول بوده و بعضاً گشت امنیتی هوایی در طول خط انتقال صورت می‌گیرد. در ناحیه ۳ ژنراتور ۳ دارای حفاظت بسیار خوب، پست مربوط به این ژنراتور نیز دارای حفاظت نسبتاً بالا و همچنین به طور دوره‌ای گشت امنیتی در اطراف نیروگاه و پست صورت می‌گیرد. بعضی از خطوط انتقال در این ناحیه دارای حفاظت تقریباً متوسط بوده و بعضی دیگر دارای حفاظت پایین می‌باشند.

• **دسترس‌پذیری:** بخشی از تجهیزات سامانه قدرت در ناحیه ۱ در نزدیکی مناطق شهری قرار داشته و بخش کمتر آن نیز کمی از مناطق شهری دور می‌باشد. در ناحیه ۲، نیروگاه ۲ در منطقه مسکونی اما نسبتاً کم جمعیت قرار داشته و سایر تجهیزات در فاصله دوری از مناطق شهری قرار دارند. در ناحیه ۳ نیروگاه ۳ به دلیل اینکه یک نیروگاه آبی می‌باشد، در منطقه‌ای نسبتاً دور از شهر و نزدیک به مناطق کوهستانی قرار دارد. سایر تجهیزات نیز در فواصل نسبتاً دوری از مناطق شهری قرار دارند.

گام دوم: اطلاعات و شواهد به‌دست آمده از تروریست‌ها به صورت زیر می‌باشد:

• **میزان فعالیت و وضعیت سیاسی:** میزان فعالیت و همچنین وضعیت سیاسی نواحی مختلف در جدول (۲) نشان داده است.

جدول ۲. میزان فعالیت و وضعیت سیاسی نواحی مختلف

ناحیه	میزان فعالیت تروریست‌ها	وضعیت سیاسی
۱	گروه‌ها به صورت پراکنده بوده و فعالیت قابل‌توجهی مشاهده نمی‌شود.	درگیری‌هایی بین حکومت و مخالفان صورت گرفته ولی هنوز قسمت عمده این ناحیه در دست حکومت است.
۲	فعالیت نسبتاً زیاد است.	عمد تا از کنترل حکومت خارج‌شده است و اوضاع ناآرام می‌باشد.
۳	فعالیت گسترده‌ای مشاهده می‌شود.	آرام

• **ساختار سازمانی:** از نظر ساختار سازمانی، گروه‌های فعال در ناحیه ۱ به صورت پراکنده فعالیت داشته و رهبری منسجم ندارند. گروه‌های فعال در ناحیه ۲ به صورت چند زیر گروه می‌باشند که نزدیک به یکدیگر پراکنده شده‌اند و همچنین به صورت شورایی اداره شده و رهبری آن‌ها قوی می‌باشد. گروه‌های فعال در ناحیه ۳ در یک مکان متمرکز شده و بدنه اصلی این گروه‌ها را افرادی برجسته از نظر نظامی و جنگی تشکیل می‌دهند. رهبری گروه‌ها در این ناحیه به صورت فردی بوده و تصمیمات به صورت فردی اتخاذ می‌شود.

منابع: بر اساس اطلاعات به‌دست آمده، گروه‌های فعال در ناحیه ۱ از نظر مالی حمایت نسبی از آن‌ها صورت می‌گیرد، دارای ادوات جنگی سبک و بعضاً نیمه سنگین می‌باشند اما چون فعالیت‌های جنگی سبک، پراکنده و بعضاً نیمه سنگین می‌باشند، بیشتر از سلاح‌های سبک استفاده می‌کنند. در ناحیه ۲ به دلیل اینکه این ناحیه هم‌مرز با کشور همسایه می‌باشد، از طریق کشور همسایه حمایت مالی و پشتیبانی نسبتاً خوبی از آن‌ها صورت می‌گیرد. تجهیزات جنگی بسیار خوبی نیز در اختیار آن‌ها قرار دارد. گروه‌های فعال در ناحیه ۳ نیز دارای منابع مالی تقریباً متوسط بوده و

به دلیل متمرکز بودن در یک مکان بیشتر از سلاح‌های نیمه سنگین استفاده می‌کنند.

• **مشاهده‌پذیری:** در ناحیه ۱، موقعیت نسبی تروریست‌ها نسبت به نیروگاه و پست این ناحیه کمی دور می‌باشد ولی در موقعیت خوبی نسبت به خطوط انتقال قرار دارند. در ناحیه ۲، تروریست‌ها دارای موقعیت نسبتاً خوبی نسبت به کلیه تجهیزات می‌باشند. در ناحیه ۳، این گروه‌ها دارای موقعیت نسبتاً خوبی نسبت به پست و خطوط انتقال این ناحیه می‌باشند اما به دلیل موقعیت جغرافیایی نیروگاه آبی موقعیت نسبی آن‌ها نسبت به این نیروگاه نسبتاً دور می‌باشد.

گام سوم: متغیرهای تشکیل‌دهنده شبکه بیزین و حالت‌های مختلف آن‌ها در بخش ششم به طور کامل مورد بررسی قرار گرفته است. بنابراین شبکه بیزین مطابق با ساختار نشان داده شده در شکل (۴) تشکیل می‌شود.

گام چهارم: به منظور اختصاص مقادیر احتمال به متغیرها و همچنین تعیین مقادیر احتمال جداول شرطی، ۵ متخصص در هر زمینه که همگی دارای یک وزن می‌باشند برای این کار در نظر گرفته می‌شود. سپس اطلاعات و شواهد جمع‌آوری شده در اختیار این متخصصان قرار گرفته و آن‌ها مقادیری را به متغیرها اختصاص می‌دهند. در نهایت با استفاده از رابطه (۴) مقادیر احتمال متغیرهای شبکه بیزین تعیین می‌شود. این مقادیر در جدول (۱۱-۶) نشان داده‌شده است.

• **شبیه‌سازی شبکه بیزین:** پس از اختصاص مقادیر احتمال به متغیرها، خروجی شبکه بیزین با استفاده از شبیه‌سازی استخراج می‌گردد. در این مقاله از نرم‌افزار Netica برای این کار استفاده می‌شود. نرم‌افزار Netica یکی از بهترین نرم‌افزارها درزمینه شبیه‌سازی شبکه بیزین است. شکل (۷) نتایج شبیه‌سازی را برای ژنراتور ۱ در محیط نرم‌افزار نشان می‌دهد. همچنین نتایج شبیه‌سازی شبکه بیزین برای تمامی تجهیزات در جدول‌های (۱۲ و ۱۳) نشان داده است.

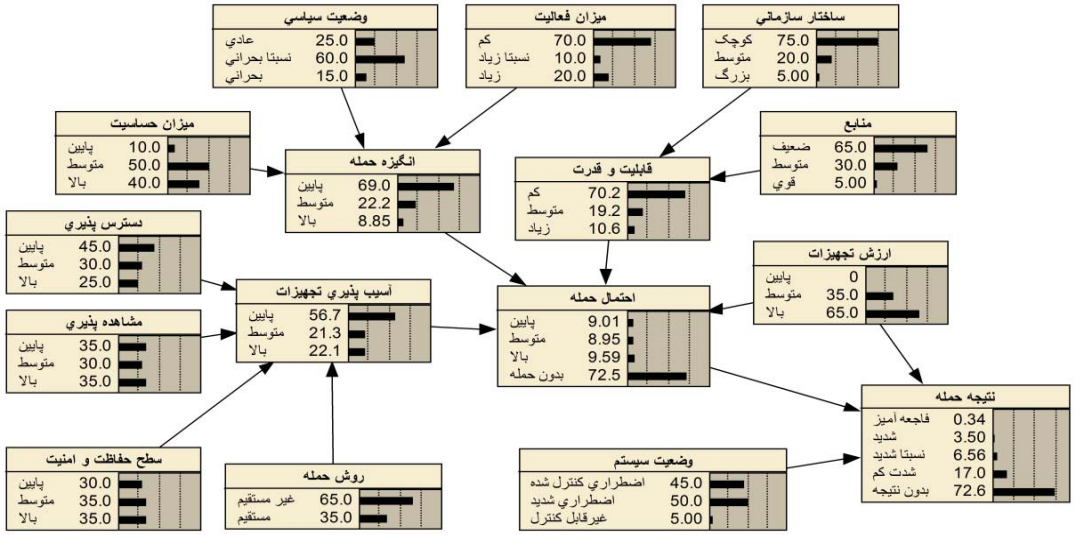
گام پنجم: برای محاسبه ریسک نیاز است که میزان آسیب ناشی از نتیجه‌بخش بودن حملات تعیین گردد. برای انجام این کار ابتدا باید معیاری را برای میزان آسیب به هر یک از مؤلفه‌ها با در نظر گرفتن هر یک از حالت‌های پارامتر نتیجه حمله تعریف کرد. بر این اساس، در این مقاله از معیار نشان داده در جدول (۳) استفاده می‌شود. بنابراین با در نظر گرفتن جدول (۳) و بر اساس مقایسه قیمت تجهیزات مختلف شبکه قدرت با استفاده از مراجع [۲۰-۱۶] و همچنین استفاده از آنالیز پخش بار به منظور تعیین میزان بار ازدست‌رفته ناشی از آسیب به هر یک از تجهیزات شبکه قدرت که معادل با هزینه تحمیلی به مصرف کنندگان می‌باشد، میزان آسیب ناشی از حمله به تجهیزات سامانه قدرت در جدول (۴) نشان داده شده است. با توجه به جدول (۴) مشاهده می‌شود که بیشترین میزان آسیب مربوط به از دست رفتن ژنراتور است که به عنوان مقدار مبنا و برابر با ۱ در نظرگرفته می‌شود.

لازم به ذکر است که برای هر نوع از تجهیزات، هزینه متوسط کل تجهیزات از همان نوع به عنوان مقدار هزینه نهایی در نظر گرفته شده است. به عنوان مثال هزینه مربوط به ژنراتورها در جدول (۴)، میانگین هزینه ۳ ژنراتور موجود در شبکه می‌باشد.

در نهایت با استفاده از نتایج حاصل از شبیه‌سازی شبکه بیزین و مقادیر داده شده در جدول (۴)، میزان ریسک هر یک از تجهیزات شبکه مورد نظر با استفاده از رابطه (۶) محاسبه شده و سپس تجهیزات شبکه بر اساس میزان ریسک رتبه‌بندی می‌شوند.

جدول ۳. معیار آسیب وارده به تجهیزات بر اثر نتیجه‌بخش بودن حمله

نوع تجهیزات	نتیجه حمله شدت کم	نتیجه حمله نسبتاً شدید	نتیجه حمله شدید	نتیجه حمله فاجعه‌آمیز
نیروگاه	از دست رفتن ۰ تا ۲۰ کل واحدها	از دست رفتن ۲۰ تا ۴۵ ٪ کل واحدها	از دست رفتن ۴۵ تا ۷۰٪ کل واحدها	از دست رفتن بیش از ۷۰ درصد کل واحدها
پست	از دست رفتن۰ تا ۲۵ ٪ کل تجهیزت	از دست رفتن ۲۵ تا ۵۰ ٪ کل تجهیزات	از دست رفتن ۵۰ تا ۷۵٪ کل تجهیزات	از دست رفتن ۷۵ تا ۱۰۰٪ کل تجهیزات
خط انتقال	از دست رفتن هر یک از خطوط با توجه به میزان حساسیت آن خط برای شبکه می‌تواند شامل یکی از حالت‌های فوق گردد.			



شکل ۶. نتایج شبیه‌سازی شبکه بیزین برای ژنراتور ۱ در محیط نرم‌افزار

جدول ۴. مقادیر پارامتر میزان آسیب بر اساس نتیجه حمله

	نتیجه حمله (فاجعه‌آمیز)	نتیجه حمله (شدید)	نتیجه حمله (نسبتاً شدید)	نتیجه حمله (شدت کم)
نوع مؤلفه	D_{T1}	D_{T2}	D_{T3}	D_{T4}
ژنراتور	۱	۰/۷۵	۰/۵	۰/۲۵
پست	۰/۶۵	۰/۵	۰/۳۵	۰/۲
خط	۰/۴۵	۰/۳۵	۰/۲۵	۰/۱۵

۴. نتایج و بحث

رتبه‌بندی میزان ریسک ناشی از حملات تروریستی بر روی تجهیزات شبکه قدرت مورد نظر در جدول (۵) نشان داده است. همان‌طور که از روی این جدول مشخص است، ژنراتور ۲ که در مقایسه با دیگر ژنراتورهای شبکه از نظر میزان توان تولیدی دارای پایین‌ترین رتبه می‌باشد، از نظر میزان ریسک ناشی از حملات تروریستی بالاترین رتبه را در بین کل مؤلفه‌ها به خود اختصاص می‌دهد. این امر می‌تواند به این دلیل باشد که این ژنراتور در ناحیه‌ای قرار دارد که از نظر وضعیت سیاسی بحرانی بوده و تروریست‌ها در این ناحیه فعالیت نسبتاً بالایی دارند که این خود انگیزه تروریست‌ها را برای حمله تقویت می‌کند. از طرفی دیگر، دسترس‌پذیری و مشاهده‌پذیری این مؤلفه نسبتاً بالا بوده و سطح حفاظت آن در حد قابل قبول نیست در نتیجه میزان آسیب‌پذیری این مؤلفه بالا می‌باشد. همچنین قابلیت و قدرت گروه‌های تروریستی ازنظر مالی و سلاح‌های پیشرفته در این ناحیه بسیار خوب می‌باشد. رتبه دوم از نظر میزان ریسک، مربوط به پست ۳ می‌باشد. این پست در همان ناحیه‌ای است که ژنراتور ۲ در آن قرار دارد. بنابراین طبیعی است که تروریست‌ها انگیزه خوبی برای حمله به این پست داشته باشند. از طرف دیگر نتایج آنالیز پخش بار نشان می‌دهد که این پست برای شبکه قدرت مورد نظر بسیار حساس می‌باشد چراکه با از دست رفتن این پست، فروپاشی ولتاژ در برخی از باس‌ها اتفاق می‌افتد که سامانه را از حالت پایدار خارج می‌سازد.

نکته قابل توجه در نتایج به‌دست آمده این است که ژنراتور اسلک که یک مؤلفه بسیار حیاتی برای سامانه قدرت می‌باشد در رتبه سوم قرار دارد. این مؤلفه در ناحیه‌ای قرار گرفته است که تروریست‌ها دارای فعالیت نسبتاً خوبی می‌باشند اما از نظر وضعیت سیاسی ناحیه‌ای آرام می‌باشد که این خود انگیزه تروریست‌ها را برای حمله به این مؤلفه علی‌رغم حساسیت بالای آن کاهش می‌دهد. از طرفی دیگر این مؤلفه دارای دسترس‌پذیری متوسطی بوده و سطح حفاظت آن بسیار خوب می‌باشد.

نتیجه غیرقابل باور دیگر، قرار گرفتن ژنراتور ۱ در رتبه یازدهم می‌باشد. این ژنراتور ازنظر میزان تولید دومین ژنراتور مهم شبکه است. این مؤلفه در ناحیه‌ای قرار دارد که از نظر سیاسی نسبتاً بحرانی می‌باشد اما تروریست‌ها فعالیت قابل توجهی در این ناحیه ندارند. از طرف دیگر این مؤلفه یک مؤلفه نسبتاً حیاتی برای سامانه قدرت می‌باشد. همچنین میزان دسترس‌پذیری و سطح حفاظت این مؤلفه در حد متوسط است. اما نکته مهم‌تر اینکه در این ناحیه تروریست‌ها از نظر منابع مالی و امکانات جنگی در سطح ضعیفی می‌باشند. همچنین ساختار سازمانی آن‌ها (تعداد نفرات، افراد برجسته جنگی و رهبری قدرتمند) کوچک می‌باشد.

در بین خطوط انتقال، خطوط ۶-۳ و ۶-۱ به فاصله کمی از هم به ترتیب در رتبه ششم و هفتم قرار دارند. این رتبه‌ها حتی بالاتر از سه پست و یک ژنراتور شبکه است. در ناحیه‌ای که این دو خط قرار دارند تروریست‌ها دارای فعالیت بالا می‌باشند ولی جو سیاسی در این ناحیه آرام است. همچنین هر کدام از این دو خط برای سامانه قدرت دارای اهمیت ویژه‌ای است چراکه با از دست رفتن هر یک از آن‌ها در برخی از خطوط اضافه‌بار اتفاق می‌افتد که نتیجه آن از دست رفتن بخش

قابل توجهی از توان انتقالی شبکه می‌باشد. این دو مؤلفه دارای دسترس‌پذیری بسیار خوبی برای تروریست‌ها بوده و سطح حفاظت آن‌ها نیز به دلیل طولانی بودن پایین است اگرچه نسبت به خطوط دیگر شبکه بالاتر می‌باشند.

جدول ۵. رتبه‌بندی تجهیزات بر اساس میزان ریسک

نوع مؤلفه	ریسک (R)	R_N (ریسک نرمالیزه شده)
ژنراتور ۲	٪۵/۹۸	۱
پست ۳	٪۵/۷۴	۰/۹۶
ژنراتور ۳	٪۵/۲۸	۰/۸۸
پست ۵	٪۴/۸۴	۰/۸۱
پست ۶	٪۴/۴۷	۰/۷۵
خط ۶-۳	٪۴/۲۳	۰/۷۱
خط ۶-۱	٪۴/۱۸	۰/۷
خط ۲-۱	٪۴/۱۲	۰/۶۹
پست ۱	٪۳/۸۵	۰/۶۴
خط ۵-۳	٪۳/۶۸	۰/۶۲
ژنراتور ۱	٪۲/۸۸	۰/۴۸
پست ۴	٪۲/۵	۰/۴۲
پست ۲	٪۲/۲۱	۰/۳۷
خط ۴-۲	٪۱/۹۳	۰/۳۲
خط ۵-۴	٪۱/۸۶	۰/۳۱
خط ۳-۲	٪۱/۷۸	۰/۳

جدول ۶. مقادیر احتمال شرطی پارامتر"قابلیت و قدرت" (تمامی مقادیر برحسب درصد)

ساختار سازمانی	منابع	قابلیت و قدرت		
		پایین	متوسط	بالا
کوچک	ضعیف	۸۰	۱۵	۵
	متوسط	۷۰	۲۰	۱۰
	قوی	۴۰	۳۰	۳۰
متوسط	ضعیف	۶۷,۵	۲۲,۵	۱۰
	متوسط	۴۰	۳۵	۲۵
	قوی	۲۰	۲۵	۵۵
بزرگ	ضعیف	۶۵	۲۰	۱۵
	متوسط	۳۰	۲۵	۴۵
	قوی	۰	۵	۹۵

جدول ۷. مقادیر احتمال شرطی پارامتر"نتیجه حمله" (تمامی مقادیر بر حسب درصد)

وضعیت سامانه	ارزش تجهیزات	احتمال حمله	نتیجه حمله				
			فاجعه آمیز	شدید	نسبتاً شدید	شدت کم	بدون نتیجه
اضطراری کنترل‌شده	پایین	پ	۰	۰	۵	۹۰	۵
		م	۰	۰	۱۰	۸۷/۵	۲/۵
		ب	۰	۰	۱۵	۸۵	۰
		ب ح	۰	۰	۰	۰	۱۰۰
	متوسط	پ	۰	۰	۱۰	۸۷/۵	۲/۵
		م	۰	۰	۱۷/۵	۸۰	۲/۵
		ب	۰	۰	۲۵	۷۵	۰
		ب ح	۰	۰	۰	۰	۱۰۰
	بالا	پ	۰	۰	۲۰	۸۰	۰
		م	۰	۰	۲۷/۵	۷۲/۵	۰
		ب	۰	۰	۳۵	۶۵	۰
		ب ح	۰	۰	۰	۰	۱۰۰
اضطراری شدید	پایین	پ	۰	۱۰	۱۰	۸۰	۰
		م	۰	۲۲/۵	۱۲/۵	۶۵	۰
		ب	۰	۳۵	۲۰	۴۵	۰
		ب ح	۰	۰	۰	۰	۱۰۰
	متوسط	پ	۰	۱۵	۲۰	۶۵	۰
		م	۰	۲۰	۲۵	۵۵	۰
		ب	۰	۲۵	۳۰	۴۵	۰
		ب ح	۰	۰	۰	۰	۱۰۰
	بالا	پ	۰	۱۷/۵	۲۷/۵	۵۵	۰
		م	۲/۵	۲۲/۵	۲۵	۵۰	۰
		ب	۵	۳۰	۲۰	۴۵	۰
		ب ح	۰	۰	۰	۰	۱۰۰
غیرقابل کنترل	پایین	پ	۰	۳۷/۵	۲۷/۵	۳۵	۰
		م	۰	۴۵	۲۵	۳۰	۰
		ب	۲/۵	۵۰	۲۷/۵	۲۲/۵	۰
		ب ح	۰	۰	۰	۰	۱۰۰
	متوسط	پ	۵	۳۲/۵	۲۵	۳۷/۵	۰
		م	۱۰	۳۲/۵	۳۰	۲۷/۵	۰
		ب	۱۵	۴۰	۲۵	۲۰	۰
		ب ح	۰	۰	۰	۰	۱۰۰
	بالا	پ	۱۰	۳۵	۳۰	۲۵	۰
		م	۱۵	۴۰	۳۰	۱۵	۰
		ب	۲۵	۴۷/۵	۲۵	۲/۵	۰
		ب ح	۰	۰	۰	۰	۱۰۰

جدول ۸. مقادیر احتمال حالت‌های مختلف متغیرهای شبکه بیزین (تمامی مقادیر برحسب درصد)

مولفه	وضعیت سیاسی			میزان فعالیت			میزان حساسیت			دسترس‌پذیری			مشاهده‌پذیری			روش حمله	
	ناآرام	نسبتاً آرام	آرام	زیاد	نسبتاً زیاد	کم	بالا	متوسط	پایین	بالا	متوسط	پایین	بالا	متوسط	پایین	مستقیم	غیر مستقیم
ژنراتور ۱	۱۵	۶۰	۲۵	۲۰	۱۰	۷۰	۴۰	۵۰	۱۰	۲۵	۳۰	۴۵	۳۵	۳۰	۳۵	۳۵	۶۵
ژنراتور ۲	۸۰	۱۵	۵	۲۵	۶۰	۱۵	۳۰	۵۰	۲۰	۵۵	۳۵	۱۰	۵۵	۲۵	۲۰	۷۵	۲۵
ژنراتور ۳	۵	۱۰	۸۵	۷۰	۲۵	۵	۹۰	۱۰	۰	۳۵	۲۵	۴۰	۴۰	۲۵	۳۵	۶۵	۳۵
پست ۱	۵	۱۰	۸۵	۷۰	۲۵	۵	۶۰	۳۰	۱۰	۳۵	۴۰	۲۵	۵۵	۳۰	۱۵	۶۵	۳۵
پست ۲	۱۵	۶۰	۲۵	۲۰	۱۰	۷۰	۶۵	۲۰	۱۵	۳۰	۴۰	۳۰	۴۵	۲۵	۳۰	۳۵	۶۵
پست ۳	۸۰	۱۵	۵	۲۵	۶۰	۱۵	۸۵	۱۵	۰	۶۵	۲۵	۱۰	۷۰	۲۵	۵	۷۵	۲۵
پست ۴	۱۵	۶۰	۲۵	۲۰	۱۰	۷۰	۶۵	۲۰	۱۵	۳۰	۳۰	۴۰	۴۵	۳۵	۲۰	۳۵	۶۵
پست ۵	۸۰	۱۵	۵	۲۵	۶۰	۱۵	۵۵	۳۵	۱۰	۶۰	۳۵	۵	۶۵	۲۵	۱۰	۷۵	۲۵
پست ۶	۵	۱۰	۸۵	۷۰	۲۵	۵	۷۵	۲۵	۰	۴۵	۲۵	۳۰	۴۵	۳۰	۲۵	۶۵	۳۵
خط ۴-۲	۱۵	۶۰	۲۵	۲۰	۱۰	۷۰	۴۵	۴۰	۱۵	۵۵	۲۵	۲۰	۹۰	۱۰	۰	۳۵	۶۵
خط ۵-۴	۱۵	۶۰	۲۵	۲۰	۱۰	۷۰	۱۵	۵۵	۳۰	۷۵	۱۵	۱۰	۸۵	۱۵	۰	۳۵	۶۵
خط ۳-۲	۱۵	۶۰	۲۵	۲۰	۱۰	۷۰	۱۵	۵۰	۳۵	۹۰	۱۰	۰	۸۰	۱۵	۵	۳۵	۶۵
خط ۵-۳	۸۰	۱۵	۵	۲۵	۶۰	۱۵	۲۰	۶۰	۲۰	۹۰	۱۰	۰	۹۵	۵	۰	۷۵	۲۵
خط ۶-۱	۵	۱۰	۸۵	۹۵	۵	۰	۶۵	۳۵	۰	۸۰	۱۰	۱۰	۸۵	۱۰	۵	۶۵	۳۵
خط ۶-۳	۵	۱۰	۸۵	۹۵	۵	۰	۵۵	۴۵	۱۰	۹۰	۱۰	۰	۹۰	۱۰	۰	۶۵	۳۵
خط ۲-۱	۵	۱۰	۸۵	۷۵	۲۰	۵	۱۰	۴۰	۵۰	۱۵	۵۰	۳۵	۹۰	۱۰	۰	۶۵	۳۵

ادامه جدول ۸. مقادیر احتمال حالت‌های مختلف متغیرهای شبکه بیزین (تمامی مقادیر برحسب درصد)

مولفه	سطح حفاظت و امنیت			منابع			ساختار سازمانی			ارزش			وضعیت سامانه		
	بالا	متوسط	پایین	قوی	متوسط	ضعیف	بزرگ	متوسط	کوچک	بالا	متوسط	پایین	اضطراری کنترل شده	اضطراری شدید	غیرقابل کنترل
ژنراتور ۱	۴۵	۲۵	۳۰	۵	۳۰	۶۵	۵	۲۰	۷۵	۶۵	۳۵	۰	۴۵	۵۰	۵
ژنراتور ۲	۱۵	۲۰	۶۵	۸۰	۲۰	۰	۷۵	۲۰	۵	۵۵	۳۵	۱۰	۵۵	۴۰	۵
ژنراتور ۳	۷۵	۲۰	۵	۳۵	۵۰	۱۵	۵۵	۳۵	۱۰	۸۰	۲۰	۰	۰	۲۵	۷۵
پست ۱	۳۵	۲۵	۴۰	۳۵	۵۰	۱۵	۵۵	۳۵	۱۰	۷۵	۲۰	۵	۰	۴۰	۶۰
پست ۲	۳۰	۳۰	۴۰	۵	۳۰	۶۵	۵	۲۰	۷۵	۵۵	۲۵	۲۰	۴۰	۵۵	۵
پست ۳	۱۵	۳۵	۵۰	۸۰	۲۰	۰	۷۵	۲۰	۵	۶۵	۲۰	۱۵	۱۵	۳۵	۵۰
پست ۴	۴۰	۳۰	۳۰	۵	۳۰	۶۵	۵	۲۰	۷۵	۵۵	۴۵	۰	۴۰	۵۷/۵	۲/۵
پست ۵	۱۵	۲۰	۶۵	۸۰	۲۰	۰	۷۵	۲۰	۵	۵۰	۴۵	۵	۳۰	۶۵	۵
پست ۶	۶۰	۲۰	۲۰	۳۵	۵۰	۱۵	۵۵	۳۵	۱۰	۶۵	۳۵	۰	۰	۱۵	۸۵
خط ۴-۲	۲/۵	۱۰	۸۷/۵	۵	۳۰	۶۵	۵	۲۰	۷۵	۲۲/۵	۱۲/۵	۶۵	۸۵	۱۵	۰
خط ۵-۴	۲/۵	۱۰	۸۷/۵	۵	۳۰	۶۵	۵	۲۰	۷۵	۲/۵	۱۲/۵	۶۵	۹۰	۱۰	۰
خط ۳-۲	۲۵	۳۰	۴۵	۵	۳۰	۶۵	۵	۲۰	۷۵	۲۲/۵	۱۲/۵	۶۵	۸۷/۵	۱۲/۵	۰
خط ۵-۳	۶۰	۳۰	۱۰	۸۰	۲۰	۰	۷۵	۲۰	۵	۲۲/۵	۱۲/۵	۶۵	۷۵	۲۵	۰
خط ۶-۱	۱۵	۲۰	۶۵	۳۵	۵۰	۱۵	۵۵	۳۵	۱۰	۳۵	۱۰	۵۵	۰	۶۵	۳۵
خط ۶-۳	۱۰	۲۰	۷۰	۳۵	۵۰	۱۵	۵۵	۳۵	۱۰	۲۵	۱۵	۶۰	۵	۷۰	۲۵
خط ۲-۱	۲/۵	۱۰	۸۷/۵	۳۵	۵۰	۱۵	۵۵	۳۵	۱۰	۲۲/۵	۲/۵	۶۵	۹۰	۱۰	۰

جدول ۹.مقادیر احتمال شرطی پارامتر"آسیب‌پذیری تجهیزات" (تمامی مقادیر برحسب درصد)

روش حمله	دسترس‌پذیری	سطح حفاظت و امنیت	مشاهده‌پذیری	آسیب‌پذیری		
				بالا	متوسط	پایین
غیر مستقیم	پایین	پایین	پ	۱۰	۱۰	۸۰
			م	۱۵	۱۵	۷۰
			ب	۲۰	۲۰	۶۰
		متوسط	پ	۱۰	۵	۸۵
			م	۱۰	۱۵	۷۵
			ب	۲۰	۱۵	۶۵
		بالا	پ	۱۰	۱۵	۷۵
			م	۱۵	۲۰	۶۵
			ب	۲۰	۲۵	۵۵
	متوسط	پایین	پ	۲۵	۱۵	۶۰
			م	۲۵	۲۵	۵۰
			ب	۳۰	۳۰	۴۰
		متوسط	پ	۱۰	۲۰	۷۰
			م	۱۵	۲۵	۶۰
			ب	۲۰	۳۰	۵۰
		بالا	پ	۵	۱۵	۸۰
			م	۵	۲۰	۷۵
			ب	۱۰	۲۵	۶۵
	بالا	پایین	پ	۳۲/۵	۲/۵	۶۵
			م	۴۰	۵	۵۵
			ب	۴۷/۵	۷/۵	۴۵
		متوسط	پ	۳۰	۵	۶۵
			م	۳۵	۱۰	۵۵
			ب	۴۰	۱۵	۴۵
		بالا	پ	۱۵	۱۰	۷۵
			م	۲۰	۱۵	۶۵
			ب	۳۰	۱۲/۵	۵۷/۵

ادامه جدول ۹.مقادیر احتمال شرطی پارامتر"آسیب‌پذیری تجهیزات" (تمامی مقادیر برحسب درصد)

روش حمله	دسترس‌پذیری	سطح حفاظت و امنیت	مشاهده‌پذیری	آسیب‌پذیری		
				بالا	متوسط	پایین
مستقیم	پایین	پایین	پ	۲۵	۲۵	۵۰
			م	۳۰	۳۰	۴۰
			ب	۴۰	۳۰	۳۰
		متوسط	پ	۵	۳۵	۶۰
			م	۱۰	۴۰	۵۰
			ب	۲۰	۴۰	۴۰
		بالا	پ	۲/۵	۴۲/۵	۵۵
			م	۵	۵۰	۴۵
			ب	۱۰	۵۵	۳۵
	متوسط	پایین	پ	۴۵	۱۵	۴۰
			م	۵۰	۲۰	۳۰
			ب	۵۵	۲۵	۲۰
		متوسط	پ	۲۵	۲۵	۵۰
			م	۳۰	۳۰	۴۰
			ب	۴۰	۳۰	۳۰
		بالا	پ	۱۰	۲۰	۷۰
			م	۱۰	۳۰	۶۰
			ب	۱۷,۵	۳۲,۵	۵۰
	بالا	پایین	پ	۶۰	۰	۴۰
			م	۶۵	۵	۳۰
			ب	۷۰	۱۰	۲۰
		متوسط	پ	۴۲,۵	۱۷,۵	۴۰
			م	۵۰	۲۰	۳۰
			ب	۵۷,۵	۲۵	۱۷,۵
		بالا	پ	۲۰	۳۰	۵۰
			م	۲۰	۴۰	۴۰
			ب	۲۷,۵	۴۵	۲۷,۵

جدول ۱۰. مقادیر احتمال شرطی پارامتر "انگیزه حمله" (تمامی مقادیر بر حسب درصد)

وضعیت سیاسی	میزان فعالیت	میزان حساسیت	انگیزه حمله		
			بالا	متوسط	پایین
آرام	کم	پ	۱۰	۱۰	۸۰
		م	۱۵	۱۵	۷۰
		ب	۲۰	۲۰	۶۰
	نسبتاً زیاد	پ	۱۰	۵	۸۵
		م	۱۰	۱۵	۷۵
		ب	۲۰	۱۵	۶۵
	زیاد	پ	۱۰	۱۵	۷۵
		م	۱۵	۲۰	۶۵
		ب	۲۰	۲۵	۵۵
نسبتا ناآرام	کم	پ	۲۵	۱۵	۶۰
		م	۲۵	۲۵	۵۰
		ب	۳۰	۳۰	۴۰
	نسبتا زیاد	پ	۱۰	۲۰	۷۰
		م	۱۵	۲۵	۶۰
		ب	۲۰	۳۰	۵۰
	زیاد	پ	۵	۱۵	۸۰
		م	۵	۲۰	۷۵
		ب	۱۰	۲۵	۶۵
ناآرام	کم	پ	۳۲/۵	۲/۵	۶۵
		م	۴۰	۵	۵۵
		ب	۴۷/۵	۷/۵	۴۵
	نسبتا زیاد	پ	۳۰	۵	۶۵
		م	۳۵	۱۰	۵۵
		ب	۴۰	۱۵	۴۵
	زیاد	پ	۱۵	۱۰	۷۵
		م	۲۰	۱۵	۶۵
		ب	۳۰	۱۲/۵	۵۷/۵

جدول ۱۱. مقادیر احتمال شرطی پارامتر "احتمال حمله" (تمامی مقادیر بر حسب درصد)

ارزش تجهیزات	آسیب‌پذیری تجهیزات	قابلیت و قدرت	انگیزه حمله	احتمال حمله			
				بدون حمله	پایین	متوسط	بالا
پایین	کم	پایین	پ	۸۷/۵	۵	۵	۲/۵
			م	۸۰	۷/۵	۷/۵	۵
			ب	۷۲/۵	۷/۵	۱۲/۵	۷/۵
		متوسط	پ	۸۵	۷/۵	۵	۱۲/۵
			م	۷۷/۵	۱۰	۷/۵	۵
			ب	۷۰	۱۰	۱۲/۵	۷/۵
		بالا	پ	۷۷/۵	۱۰	۷/۵	۵
			م	۷۰	۱۲/۵	۱۰	۷/۵
			ب	۶۲/۵	۱۲/۵	۱۵	۱۰
	متوسط	پایین	پ	۸۷/۵	۲/۵	۵	۵
			م	۷۷/۵	۷/۵	۷/۵	۷/۵
			ب	۷۲/۵	۷/۵	۷/۵	۱۲/۵
		متوسط	پ	۸۰	۵	۷/۵	۷/۵
			م	۷۰	۱۰	۱۰	۱۰
			ب	۶۵	۱۰	۱۰	۱۵
		بالا	پ	۷۲/۵	۷/۵	۱۰	۱۰
			م	۶۲/۵	۱۲/۵	۱۲/۵	۱۲/۵
			ب	۵۷/۵	۱۲/۵	۱۲/۵	۱۷/۵
	زیاد	پایین	پ	۷۷/۵	۲/۵	۱۲/۵	۷/۵
			م	۶۷/۵	۷/۵	۱۲/۵	۱۲/۵
			ب	۶۲/۵	۷/۵	۱۲/۵	۱۷/۵
		متوسط	پ	۷۰	۵	۱۵	۱۰
			م	۶۰	۱۰	۱۵	۱۵
			ب	۵۵	۱۰	۱۵	۲۰
		بالا	پ	۶۲/۵	۷/۵	۱۷/۵	۱۲/۵
			م	۵۵	۱۰	۱۷/۵	۱۷/۵
			ب	۵۰	۱۰	۱۷/۵	۲۲/۵

ادامه جدول ۱۱. مقادیر احتمال شرطی پارامتر"احتمال حمله" (تمامی مقادیر برحسب درصد)

ارزش تجهیزات	آسیب‌پذیری تجهیزات	قابلیت و قدرت	انگیزه حمله	احتمال حمله			
				بدون حمله	پایین	متوسط	بالا
متوسط	کم	پایین	پ	۸۷/۵	۷/۵	۲/۵	۲/۵
			م	۷۲/۵	۱۲/۵	۷/۵	۷/۵
			ب	۶۲/۵	۱۷/۵	۷/۵	۱۲/۵
		متوسط	پ	۸۰	۱۰	۵	۵
			م	۶۵	۱۵	۱۰	۱۰
			ب	۵۵	۲۰	۱۰	۱۵
		بالا	پ	۷۲/۵	۱۲/۵	۷/۵	۷/۵
			م	۵۷/۵	۱۷/۵	۱۲/۵	۱۲/۵
			ب	۴۷/۵	۲۲/۵	۱۲/۵	۱۷/۵
	متوسط	پایین	پ	۷۰	۱۰	۱۲/۵	۷/۵
			م	۵۷/۵	۱۲/۵	۱۷/۵	۱۲/۵
			ب	۴۲/۵	۱۷/۵	۱۷/۵	۲۲/۵
		متوسط	پ	۶۵	۱۰	۱۵	۱۰
			م	۵۰	۱۵	۲۰	۱۵
			ب	۳۵	۲۰	۲۰	۲۵
		بالا	پ	۵۷/۵	۱۲/۵	۱۷/۵	۱۲/۵
			م	۴۲/۵	۱۷/۵	۲۲/۵	۱۷/۵
			ب	۲۷/۵	۲۲/۵	۲۲/۵	۲۷/۵
	زیاد	پایین	پ	۷۷/۵	۲/۵	۷/۵	۱۲/۵
			م	۶۵	۵	۱۲/۵	۱۷/۵
			ب	۵۷/۵	۷/۵	۷/۵	۲۷/۵
		متوسط	پ	۷۰	۵	۱۰	۱۵
			م	۵۷/۵	۷/۵	۱۵	۲۰
			ب	۵۰	۱۰	۱۰	۳۰
		بالا	پ	۶۲/۵	۷/۵	۱۲/۵	۱۷/۵
			م	۵۰	۱۰	۱۷/۵	۲۲/۵
			ب	۴۲/۵	۱۲/۵	۱۷/۵	۳۲/۵

ادامه جدول ۱۱. مقادیر احتمال شرطی پارامتر"احتمال حمله" (تمامی مقادیر برحسب درصد)

ارزش تجهیزات	آسیب‌پذیری تجهیزات	قابلیت و قدرت	انگیزه حمله	احتمال حمله			
				بدون حمله	پایین	متوسط	بالا
بالا	کم	پایین	پ	۹۰	۲/۵	۵	۲/۵
			م	۷۷/۵	۷/۵	۷/۵	۷/۵
			ب	۶۲/۵	۲/۵	۷/۵	۲۷/۵
		متوسط	پ	۸۷/۵	۲/۵	۵	۵
			م	۷۰	۱۰	۱۰	۱۰
			ب	۵۵	۵	۱۰	۳۰
		بالا	پ	۸۰	۵	۷/۵	۷/۵
			م	۶۲/۵	۱۲/۵	۱۲/۵	۱۲/۵
			ب	۴۷/۵	۷/۵	۱۲/۵	۳۲/۵
	متوسط	پایین	پ	۶۷/۵	۵	۲/۵	۲۵
			م	۴۷/۵	۲/۵	۱۵	۳۵
			ب	۳۲/۵	۱۰	۵	۵۲/۵
		متوسط	پ	۶۲/۵	۲/۵	۵	۳۰
			م	۵۰	۵	۱۰	۳۵
			ب	۳۰	۱۰	۱۵	۴۵
		بالا	پ	۵۲/۵	۵	۷/۵	۳۵
			م	۳۷/۵	۷/۵	۱۵	۴۰
			ب	۳۰	۱۰	۱۰	۵۰
	زیاد	پایین	پ	۶۰	۵	۵	۳۰
			م	۴۷/۵	۵	۷/۵	۴۰
			ب	۳۲/۵	۷/۵	۱۰	۵۰
		متوسط	پ	۵۰	۱۰	۵	۳۵
			م	۳۵	۱۰	۱۰	۴۵
			ب	۳۰	۵	۱۰	۵۵
		بالا	پ	۴۰	۱۰	۱۰	۴۰
			م	۲۵	۱۰	۱۵	۵۰
			ب	۱۰	۵	۲۰	۶۵

جدول ۱۲. نتایج شبیه‌سازی شبکه بیزین (تمامی مقادیر بر حسب درصد)

نوع مؤلفه	آسیب‌پذیری			قابلیت و قدرت			انگیزه حمله		
	پایین	متوسط	بالا	کم	متوسط	زیاد	پایین	متوسط	بالا
ژنراتور ۱	۵۶/۶	۲۱/۳	۲۲/۱	۷۰/۲	۱۹/۲	۱۰/۶	۶۹	۲۲/۱۵	۸/۸۵
ژنراتور ۲	۳۶/۵	۱۸/۹	۴۴/۶	۱۱/۷	۱۳/۵	۷۴/۸	۴۲/۶	۳۲/۵	۲۴/۹
ژنراتور ۳	۵۱/۹	۲۹/۸	۱۸/۳	۳۲/۷	۲۲/۱	۴۵/۲	۴۷/۱	۳۴/۶	۱۸/۳
پست ۱	۴۳/۶	۲۴/۸	۳۱/۶	۳۲/۷	۲۲/۱	۴۵/۲	۵۲/۲	۳۲/۲	۱۵/۶
پست ۲	۵۳/۱	۲۰/۷	۲۶/۲	۷۰/۲	۱۹/۲	۱۰/۶	۶۶/۹	۲۲/۹	۱۰/۲
پست ۳	۳۴/۴	۲۰/۷	۴۵/۹	۱۱/۶	۱۳/۶	۷۴/۸	۳۴/۲	۳۳/۷	۳۲/۱
پست ۴	۵۳/۹	۲۲/۲	۲۳/۹	۷۰/۲	۱۹/۲	۱۰/۶	۶۶/۸	۲۲/۹	۱۰/۳
پست ۵	۳۳/۹	۱۹	۴۷/۱	۱۱/۶	۱۳/۶	۷۴/۸	۳۸/۷	۳۳	۲۸/۳
پست ۶	۴۷/۸	۲۷/۲	۲۵	۳۲/۷	۲۲/۱	۴۵/۲	۴۹	۳۳/۸	۱۷/۲
خط ۴-۲	۳۹/۷	۱۶/۹	۴۳/۴	۷۰/۲	۱۹/۲	۱۰/۶	۶۹	۲۲	۹
خط ۵-۴	۳۹	۱۳/۵	۴۷/۵	۷۰/۲	۱۹/۲	۱۰/۶	۷۳/۹	۱۹/۳	۶/۸
خط ۳-۲	۴۱/۵	۱۵/۸	۴۲/۷	۷۰/۲	۱۹/۲	۱۰/۶	۷۴/۴	۱۸/۸	۶/۸
خط ۵-۳	۳۳	۲۹/۶	۳۷/۴	۱۱/۷	۱۳/۵	۷۴/۸	۴۳/۷	۳۲/۳	۲۴
خط ۶-۱	۳۳/۵	۱۷/۲	۴۹/۳	۳۲/۷	۲۲/۱	۴۵/۲	۵۰/۲	۳۳/۳	۱۶/۵
خط ۶-۳	۳۲/۹	۱۶/۲	۵۰/۹	۳۲/۷	۲۲/۱	۴۵/۲	۵۱/۳	۳۲/۹	۱۵/۸
خط ۲-۱	۳۴/۲	۲۴/۵	۴۱/۴	۳۲/۷	۲۲/۱	۴۵/۲	۶۳/۹	۲۶/۴	۹/۷

جدول ۱۳. مقادیر احتمال پارامترهای تأثیرگذار بر روی ریسک حاصل از شبیه‌سازی شبکه بیزین و میزان ریسک هریک از مولفه‌های شبکه قدرت (تمامی مقادیر بر حسب درصد)

نوع مؤلفه	بدون حمله	احتمال حمله پایین	احتمال حمله متوسط	احتمال حمله بالا	نتیجه حمله				
					فاجعه آمیز	شدید	نسبتاً شدید	شدت کم	بدون نتیجه
ژنراتور ۱	۷۲/۴	۹	۹	۹/۶	۰/۳۴	۳/۵	۶/۶۶	۱۷	۷۲/۶
ژنراتور ۲	۵۹/۸	۱۰/۸	۱۲/۹	۱۶/۵	۰/۴۵	۴/۵	۹/۲	۲۵/۸	۶۰
ژنراتور ۳	۶۹/۸	۹/۸	۱۰/۵	۹/۹	۳/۴۵	۱۰/۶	۸/۱۵	۸	۶۹/۸
پست ۱	۶۸/۱	۹/۳	۱۰/۹	۱۱/۷	۲/۹	۱۰/۵	۸/۳	۱۰/۲	۶۸/۱
پست ۲	۷۲	۷/۸	۸/۶	۱۱/۶	۰/۳	۴/۲	۶/۲	۱۷/۲	۷۲/۱
پست ۳	۵۹/۸	۱۰	۱۳	۱۷/۲	۲/۷	۱۱/۶	۱۰/۱	۱۵/۹	۵۹/۷
پست ۴	۷۰/۱	۹/۷	۹/۴	۱۰/۸	۰/۲۶	۴	۷/۱۴	۱۸/۴	۷۰/۲
پست ۵	۵۹/۲	۱۱/۲	۱۳/۲	۱۶/۴	۰/۵۶	۶/۷۵	۹/۷۴	۲۳/۶	۵۹/۳
پست ۶	۶۶/۶	۱۰/۶	۱۱/۱	۱۱/۶	۳/۹۴	۱۱/۹	۹	۸/۵۶	۶۶/۶
خط ۴-۲	۶۶/۷	۶/۳	۷/۷	۱۹/۳	۰/۰۲	۱/۴	۵/۵	۲۶/۰۸	۶۷
خط ۵-۴	۶۷	۶/۲	۷/۶	۱۹/۲	۰/۰۲	۰/۸۹	۵/۳۹	۲۶/۴	۶۷/۳
خط ۳-۲	۶۷/۸	۶/۲	۷/۵	۱۸/۵	۰/۰۲	۱/۱	۵/۲۸	۲۵/۵	۶۸/۱
خط ۵-۳	۵۲/۷	۸/۸	۱۱/۶	۲۷	۰/۰۵	۳/۲	۷/۸۵	۳۵/۹	۵۳
خط ۶-۱	۵۹/۲	۷/۹	۱۰/۴	۲۲/۵	۱/۴	۱۳/۸	۹/۳	۱۶/۴	۵۹/۱
خط ۶-۳	۵۷/۵	۸/۱	۱۰/۳	۲۴/۱	۰/۷۶	۱۲/۴	۸/۹۴	۲۰/۳	۵۷/۶
خط ۲-۱	۵۹/۸	۷/۸	۹/۵	۲۲/۹	۰/۰۲	۱/۰۸	۶/۵	۳۲/۲	۶۰/۲

۵. نتیجه‌گیری

در ایـن مقالـه ابتـدا بحـث تروریسـم و خطـرات ناشـی از حمـلات تروریستی بر روی امنیت شـبکه قـدرت مـورد بحـث و بررسـی قـرار گرفت. یکی از مسائل اصلی در مواجهه با موضوع حملات تروریسـتی، وجود عدم قطعیت به دلیل فقـدان اطلاعـات کـافی در زمینـه رفتـار گروه‌های تروریستی است. بنابراین لازم است از روش‌های احتمـالاتی که بر مبتنی بر عدم قطعیت است برای مدل‌سازی حملات تروریستی بر روی شبکه قدرت استفاده شود. در این مقاله از شـبکه بیـزین کـه

منتج شده از تئوری احتمالات است برای ارزیابی امنیت شبکه استفاده می‌شود.

این مدل‌سازی قادر است علاوه بر تعیین میزان احتمال حمله به هر یک از تجهیزات، نتیجه احتمالی این حملات را نیز پیش‌بینی نماید. همچنین با استفاده از نتایج شبکه بیزین، فرمولی برای محاسبه ریسک ناشی از حمله به تجهیزات سامانه قدرت پیشنهاد شد که توسط آن می‌توان تجهیزات مختلف سامانه قدرت را بر اساس میزان ریسک هر یک از آن‌ها رتبه‌بندی کرد. رتبه‌بندی تجهیزات بر حسب میزان ریسک، این امکان را برای بهره‌برداران سامانه قدرت فراهم می‌کند که با پیش‌بینی محتمل‌ترین سناریوهای حمله به تجهیزات شبکه، شاخصی برای ارزیابی سطح امنیت سامانه قدرت تعیین کرده و اقدامات لازم را به منظور کاهش آسیب‌پذیری تجهیزات در برابر این حملات اتخاذ نمایند. همچنین به منظور ارزیابی کارایی روش پیشنهادی برای رتبه‌بندی ریسک، میزان ریسک برای مؤلفه‌های یک شبکه قدرت ۶ باسه محاسبه شده و نتایج آن مورد بحث و بررسی قرار گرفت. ممکن است در ابتدا تصور شود که نتایج حاصل از اعمال روش پیشنهادی برای رتبه‌بندی ریسک سامانه ۶ باسه تقریباً قابل پیش‌بینی بوده و در نتیجه نیازی به استفاده از روش پیشنهادی نمی‌باشد که البته این تصور به دلیل اینکه شبکه مورد نظر یک شبکه کوچک با تعداد محدودی از تجهیزات است تا حدودی درست بوده و در نتیجه رتبه‌بندی برخی از تجهیزات این شبکه بدون استفاده از روش پیشنهادی نیز امکان‌پذیر است. اما اگر شبکه قدرت یک شبکه بزرگ با گستره جغرافیایی وسیع و شامل تجهیزات بسیار زیاد باشد، در این صورت بدیهی است که بدون استفاده از روش‌های احتمالاتی مانند روش پیشنهاد شده در این مقاله پیش‌بینی میزان ریسک و در نتیجه رتبه‌بندی تجهیزات سامانه غیرممکن است. بنابراین می‌توان ادعا کرد که روش پیشنهاد شده در این مقاله قادر است میزان ریسک ناشی از حمله به یک شبکه قدرت بزرگ و با حجم وسیعی از تجهیزات را به خوبی پیش‌بینی نماید. البته در این حالت مدل‌سازی شبکه به دلیل افزایش تعداد مؤلفه‌ها پیچیده‌تر است. همچنین روش پیشنهادی می‌تواند بدون تغییرات قابل‌توجهی برای تعیین میزان ریسک و رتبه‌بندی تجهیزات سایر زیرساخت‌های حیاتی نیز مورد استفاده قرار گیرد.

۶. مراجع

[1] National Memorial Institute for the Prevention of Terrorism in the US (www.MIPT.org).

[2] Sharada, C. R.; Ajjampur, S.; Raikar, S.; Prakash, M. N. “To Study the Adequacy Assessment of Generation System”; International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering 2014, 3, 1-1.

[3] Nilsen, T.; Aven, T. “Models and Model Uncertainty in the Context of Risk Analysis”; Reliability Eng. & Syst. Safety 2003, 79, 309-317.

[4] Göztepe, K. “Designing a Fuzzy Rule Based Expert System for Cyber Security”; Int. J. Inform. Secur. Sci. 2006, 1, 1-12.

[5] Taylor, C.; Krings, A.; Alves-Foss, J. “Risk Analysis and Probabilistic Survivability Assessment (RAPSA): An Assessment Approach for Power Substation Hardening”; In Proc. of ACM Workshop on Scientific Aspects of Cyber Terrorism (SACT), U.S.A, 2002.

[6] McClintock, J.; Saxon, M.; Forsythe, J.; Rascoe, J.; Risser, J. “Development of the Adaptable, GIS-Based, Multi-Threat Detection System”; In Proc. of IEEE Int. Conf. on Tech. for Homeland Security 2011, 507-511.

[7] Biringer, B. “Risk Assessment Methodology for Electric Power Transmission, RAM-T^{SM}”; In Proc. of IEEE Int. Carnahan Conf. on Security Tech. 2004, 99-105.

[8] 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.

[9] 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”; In Proc. of IREP Symposium on Bulk Power System Dynamics and Control, 2007, 1-8.

[10] Willis, H. H. “Guiding Resource Allocations Based on Terrorism Risk”; Int. J. Uncertainty 2007, 27, 597-606.

[11] Heckerman, D. “A Tutorial on Learning with Bayesian Networks”; Microsoft Corporation, Advanced Technology Devision, 1995.

[12] Ackerman, G.; Abhayaratne, P.; Bale, J.; Bhattacharjee, C.; Blair, C.; Hansell, L. “Assessing Terrorist Motivations for Attacking Critical Infrastructure”; Monterey Institute of Int. Studies, California, 2007.

[13] Leson, J. “Assessing and Managing the Terrorism Threat”; U.S. Department of Justice, 2005.

[14] Griffith, T. E. “Strategic Attack of National Electrical System”; Thesis, School of Advanced Air power Studies, Maxwell Air Force Base, Alabama, 1994.

[15] Chakrabarti, A.; Halder, S. “Power System Analysis: Operation and Control”; Third Ed., New Delhi, 2008.

[16] Howard, S. “Technical Comparison of AIS v GIS Substation Options”; Int. ESBI Energy Innovation, Ireland, 2011.

[17] Mason, T.; Curry, T.; Wilson, D. “Capital Costs for Transmission and Substations”; Western Electricity Coordinating Council, 2012.

[18] Sterling, M. J. “Electricity Transmission Costing Study”; Institution of Engineering & Technology (IET), 2012.

[19] Yli-Hannuksela, J. “The Transmission Line Cost Calculation”; University of Applied Sciences, Finland, 2011.

[20] “Updated Capital Cost Estimates for Utility Scale Electricity Generating Plants”; U.S. Department of Energy, 2013.