علوم رایانش و فناوری اطلاعات
نشریه علمی انجمن کامپیوتر ایران
مجلد ۱۷، شماره ۲، ۱۳۹۸
صفحات ۱۴- ۱
مقاله عادی

ارزیابی کمّی معیارهای مرتبط با انتشار خطا مابین مؤلفه‌های سیستم‌های هیبرید

آرمان سان احمدی[۱]، محمد عبداللهی ازگمی[۲*]

*نویسنده مسئول، دریافت: ۹۸/۰۵/۱۲، بازنگری: ۹۸/۰۷/۲۵، پذیرش: ۹۸/۱۰/۰۱

[۱] دانشجوی دکتری، شبکه‌های کامپیوتری، دانشگاه علم و صنعت ایران، تهران، ایران
[۲] دانشیار، دانشکده مهندسی کامپیوتر ، دانشگاه علم و صنعت ایران، تهران، ایران

چکیده

امروزه سیستم‌های هیبرید در بخش‌های مختلفی مانند ماشین‌های خودران، کارخانه‌های صنعتی، ابزارهای کنترل سلامت بیمار و غیره کاربرد فراوانی دارد. با توجه به کاربرد حساس این سیستم‌ها وقوع خطا در یک بخش سیستم می‌تواند به سایر بخش‌ها انتشار پیدا کند و خسارات مالی و جانی زیادی را به همراه داشته باشد. سیستم‌های هیبرید از دو بخش پیوسته و گسسته تشکیل شده‌اند. این بخش‌ها به‌منظور انجام هدف سیستم با همدیگر همکاری می‌کنند. وقوع یک خطا در بخش فیزیکی یا سایبری می‌تواند عملکرد کل سیستم را مختل کند. با توجه به کاربرد حساس این سیستم‌ها و هزینه‌بر بودن فرایند ساخت آن‌ها، لازم است قبل از طراحی و بهره‌برداری از آن، در یک محیط ایمن و کم‌هزینه به مدل‌سازی انتشار خطا سیستم پرداخته شود. در این مقاله روشی برای مدل‌سازی انتشار خطا بر اساس شبکه‌های فعالیت تصادفی ارائه شده است. بر اساس این مدل می‌توان با تزریق خطا در بخش‌های مختلف سیستم به شناسایی نقاط حساس سیستم، رفتار خرابی مؤلفه‌ها و تأثیر یک خطا و فعال شدن آن بر سایر مؤلفه‌های سیستم پرداخت. مدل ارائه شده بر روی یک زیرساخت حیاتی متشکل از سه لایه مختلف اعمال شده است و نتایج شبیه‌سازی و ارزیابی کمّی آن آورده شده است.

کلمات کلیدی: مدل‌سازی، انتشار خطا، سیستم‌های هیبرید، شبکه‌های فعالیت تصادفی، ارزیابی کمّی

۱- مقدمه

امروزه سیستم‌های هیبرید در بخش‌های مختلفی اعم از حمل‌ونقل خودکار، کارخانه‌های صنعتی، هواپیما و ابزارهای کنترل سلامت بیمار کاربرد فراوانی دارد. این سیستم‌های از چندین مؤلفه فیزیکی و رایانشی مختلف ساخته شده است. تمامی این مؤلفه‌ها به‌منظور انجام هدف سیستم با همدیگر همکاری می‌کنند[۱، ۲]. وقوع خطا در یک مؤلفه سیستم می‌تواند به سایر مؤلفه‌ها انتشار پیدا کند و منجر به خسارات مالی و جانی فراوانی شود. منبع خطا[۱] می‌تواند عوامل مختلفی همچون نقص فنی، استفاده از قطعات نامناسب و حملات عمدی باشد [۳].

خطا می‌تواند داخل یک مؤلفه غیرفعال باشد و سپس به دلیل شرایط مختلف سیستم این خطا فعال شود و به یک اشکال[۲] تبدیل گردد، اشکال ایجاد شده می‌تواند با انحراف عملکرد مؤلفه از حالت صحیح خود منجر به خرابی در مؤلفه و درنهایت کل سیستم شود [۴].

بررسی چگونگی انتشار خطا[۳] در بین مؤلفه‌های مختلف سیستم و بررسی پارامترهای مختلف آن همچون اتکاپذیری[۴]، در محیط واقعی، هزینه‌بر و غیرممکن است [۵، ۶]. بهتر است قبل از طراحی و ساخت سیستم‌های هیبرید ،از طریق مدل انتشار خطا می‌توان به مشاهده پارامترهای اتکاپذیری سیستم و شناسایی مؤلفه‌های حساس سیستم پرداخت. درنهایت با استفاده از نتایج مدل‌سازی می‌توان ادامه فرایند ساخت سیستم را دقیق‌تر انجام داد [۷].

تاکنون کارهای زیادی در حوزه مدل‌سازی انتشار خطای سیستم‌ها انجام گرفته است. اما به‌طورکلی هیچ‌یک از این مدل‌ها را نمی‌توان به طیف وسیعی از سیستم‌ها نگاشت کرد یا در صورت امکان پارامترهای کافی جهت استخراج نتایج دقیق در نظر گرفته نشده. به‌عنوان‌مثال بسیاری از کارهای انجام شده در این حوزه فقط قطع ارتباط دو مؤلفه را معیار انتشار خرابی در مؤلفه‌ها در نظر گرفته‌اند. برخی از این کارها فقط ارتباط ورودی و خروجی مؤلفه‌ها را در نظر گرفته‌اند و برخی دیگر،

پارامترهای دیگری مثل ارتباط غیرمستقیم مؤلفه‌ها را مدنظر نداشته‌اند. برخی از این مدل‌ها که دید سطح پایین‌تری دارند بسیار خاص‌منظوره هستند.

در روش پیشنهادی این مقاله وابستگی غیر داده‌ای بین مؤلفه‌ها در مدل‌سازی انتشار خطا در نظر گرفته شده است. ابتدا بر اساس همبندی[۵] و مشخصات سیستم، گراف داده‌ای و گراف غیر داده‌ای استخراج می‌شود. همچنین عبارت‌های احتمالی مربوط به رفتار هر یک از مؤلفه‌ها در شرایط مختلف به‌صورت احتمالی مشخص می‌شود. سپس قوانین تبدیلی ارائه خواهد شد که با استفاده از این قوانین می‌توان گراف‌های ساخته شده در مرحله قبل و عبارت‌های احتمالی را به مدل شبکه‌های فعالیت تصادفی تبدیل کرد. درنهایت با استفاده از صورت‌بندی تکرار-الحاق[۶]، مؤلفه‌های مختلف سیستم با همدیگر الحاق می‌شوند و مدل نهایی سیستم به دست خواهد آمد. درنهایت با اجرای سناریوهای مختلف به ارزیابی انتشار خطا سیستم پرداخته می‌شود.

۲- مفاهیم پایه

در این بخش مفاهیم پایه‌ای که در حوزه این مقاله لازم است، توضیح داده شده است.

۲-۱- آسیب‌شناسی خرابی

خطا به نقصی گفته می‌شود که در داخل سیستم وجود دارد. خطا می‌تواند عوامل مختلفی ازجمله: مشخصه‌سازی نادرست سیستم، طراحی نادرست، استفاده از ابزار نامناسب و عامل‌های بیرونی داشته باشد. اشکال به خطایی گفته می‌شود که فعال شده باشد. درواقع علت یک اشکال، همان خطا است. اشکال بخشی از وضعیت کل سیستم است که می‌تواند منجر به خرابی کل سیستم شود. اشکال‌ها می‌توانند آشکار یا پنهان باشند. حالت سیستم مجموعه‌ای از حالت‌های تک‌تک مؤلفه‌ها است. هنگامی‌که یک اشکال درون یک مؤلفه وجود دارد تا زمانی که آن اشکال به یک حالت خارجی آن مؤلفه انتقال پیدا نکند نمی‌تواند باعث خرابی کل سیستم شود [۴].

یک سیستم دچار خرابی شده است هرگاه خدمات مربوط به این سیستم از حالت صحیح آن انحراف داشته باشد. درواقع یک اشکال در صورت انتشار به محیط خارج از مؤلفه باعث ایجاد خرابی می‌شود. به‌طور مثال هنگامی‌که از یک خانه‌ی حافظه که یک بیت آن یک شده است استفاده شود و استفاده از آن باعث ایجاد خرابی در متغیرهای کنترلی و غیره شود مؤلفه دچار خرابی می‌گردد. خرابی‌ها در سیستم را می‌توان از طریق چهار دیدگاه مختلف شامل، دامنه‌ی خرابی، قابل تشخیص بودن، پایداری خرابی و تأثیر خرابی بر روی محیط دسته‌بندی کرد.

۲-۲- شبکه‌های فعالیت تصادفی

شبکه‌های فعالیت تصادفی یک بسط احتمالی برای شبکه پتری است. شبکه فعالیت تصادفی برای ارزیابی کارایی، اتکاپذیری و انجام‌پذیری ایجاد شد و ابزارهای زیادی برای کار با این مدل توسعه داده شده است. با توجه به قابلیت‌های این مدل، می‌توان طیف گسترده‌ای از سیستم‌ها را با استفاده از آن مدل کرد [۸].

هر شبکه فعالیت تصادفی را می‌توان به‌صورت یک ۱۲-تایی تعریف کرد $SAN^{۷} = (P, A, I, O, \gamma, \tau, i, o, \mu_0, C, F, G)$ است. تعریف هر یک از این نمادها عبارتند از:

P: مجموعه متناهی از مکان‌ها.

A: مجموعه‌ای متناهی از فعالیت‌ها.

I: مجموعه متناهی از دروازه‌های ورودی.

O: مجموعه متناهی از دروازه‌های خروجی.

γ: نشان‌دهنده تعداد اقدام‌های احتمالی متفاوت برای هر فعالیت است.

τ: مشخص‌کننده نوع هر فعالیت است (فوری یا زمانی).

i: نگاشت‌کننده دروازه‌های ورودی به فعالیت‌ها است.

o: نگاشت‌کننده دروازه‌های خروجی به فعالیت‌ها است.

μ_0: نشانه‌گذاری اولیه است که باید پایدار باشد.

C: تابع تخصیص توزیع‌های احتمالی مربوط به اقدام‌های احتمالی فعالیت‌ها است.

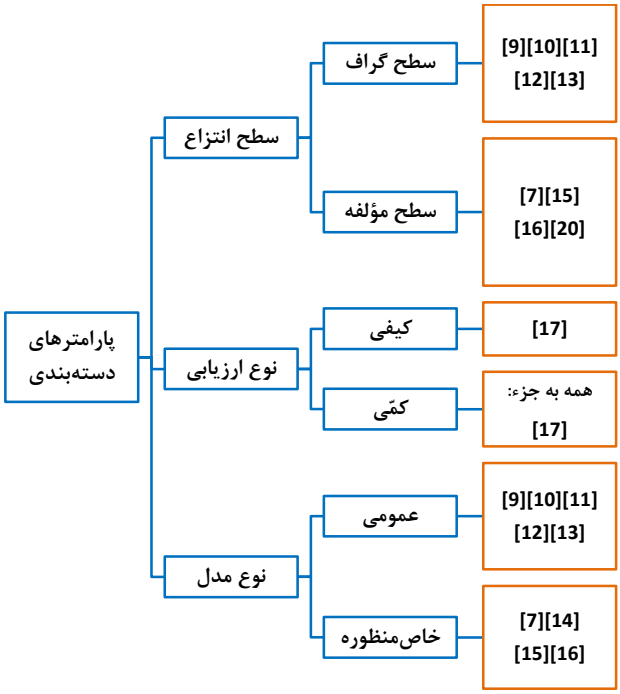
F: تابع تخصیص نرخ‌های احتمالی فعالیت‌ها است.

G: تابع تخصیص فعال‌سازی مجدد فعالیت‌ها است.

۳- کارهای مرتبط

در این بخش کارهای انجام‌شده در حوزه انتشار خطا مورد بررسی قرار گرفته است. کارهای انجام شده بر اساس سه مشخصه مدل دسته‌بندی شده است. این دسته‌بندی در شکل ۱ نشان داده شده است. مشخصه‌های در نظر گرفته‌شده عبارت‌اند از:

- نوع ارزیابی مدل
- سطح انتزاع مدل‌سازی
- نوع مدل (عمومی یا خاص‌منظوره)



شکل ۱- دسته‌بندی کارهای مرتبط

۳-۱- مدل‌های با سطح انتزاع گراف

در کار شماره [۹] به مدل‌سازی انتشار خطا بین زیرساخت‌های حیاتی و وابسته به هم پرداخته شده است. سیستم‌های حیاتی معمولاً از چندین زیرساخت مرتبط به هم ساخته شده است. وقوع خطا در یک زیرساخت می‌تواند به سایر بخش‌ها انتشار پیدا کند و عملکرد کل سیستم را مختل کند. به‌طور مثال وقوع خطا در سیستم توزیع برق ایتالیا در سال ۲۰۰۳ منجر به خاموشی گسترده و قطعی در سایر بخش‌ها مانند اینترنت شد. در مقاله [۹] برای مدل‌سازی انتشار خطا، یک چارچوب زنجیره مارکوف[۸] با وابستگی متقابل ارائه شده است. این‌گونه زنجیره مارکوف‌ها به این صورت است که ابتدا زنجیره مارکوف مرتبط به هر بخش ایجاد می‌شود سپس با توجه به ساختار سیستم این زنجیره مارکوف‌ها به همدیگر متصل می‌گردد. در مقاله اثبات شده است که زنجیره مارکوف ایجاد شده ارگودیگ است. با توجه به وابستگی این زنجیره مارکوف‌ها به همدیگر وقوع یک انتقال در یک زنجیره مارکوف می‌تواند بر

روی سایر زنجیره‌ها نیز تأثیرگذار باشد. مدل ارائه شده بیشتر برای شبکه‌های زیرساختی همچون شبکه‌های انتقال برق مناسب است و قابلیت گسترش به هر سیستمی را ندارد، همچنین در این مدل تفاوتی بین مؤلفه‌های رایانشی و فیزیکی لحاظ نشده است. همین افراد در مقاله [۱۰] پارامتر جدیدی تحت عنوان خطای انسانی را به مدل خود اضافه کردند.

در مقاله [۱۱] روشی بر مبنای تحلیل گرافی به‌منظور مدل‌سازی انتشار خطا در نظر گرفته شده است. با توجه به اینکه سیستم‌های هیبرید از دو بخش رایانشی و فیزیکی تشکیل شده است، در این مدل دو زیرشبکه با نام A و B نیاز است. ابتدا بر اساس همبندی سیستم ارتباط بین گره‌های A و B کشیده می‌شود. سپس هنگامی‌که یک گره از یک زیرشبکه خراب می‌شود تمامی یال‌هایی که از آن گره به سایر گره‌های زیرشبکه داخلی یا خارجی وصل شده است، حذف می‌گردد. پس از حذف یال‌های مربوطه، هر یک از زیر شبکه‌های A و B را می‌توان به چندین خوشه[۹] تبدیل کرد. در اینجا منظور از خوشه مجموعه گره‌هایی است که فقط با خود ارتباط دارند و با سایر گره‌های موجود در زیرشبکه خود ارتباطی ندارند. درصورتی‌که یالی در یک زیرشبکه وجود داشته باشد که بین دو خوشه متفاوت کشیده شده باشد آن یال نیز حذف خواهد شد. بعد از حذف یال‌ها درصورتی‌که گره‌ای ایجاد شد که با هیچ گره دیگری ارتباط ندارد آن گره نیز حذف خواهد شد. این فرایند آن‌قدر ادامه پیدا خواهد کرد تا شبکه به یک حالت پایدار برسد و دیگر نتوان گره یا یالی را حذف کرد. مشکلی که این روش دارد این است که حذف گره‌ها و ارتباط آن با سایر گره‌ها بر اساس یک منطق ساده و در سیستم‌های هیبرید به این صورت نمی‌توان در مورد خرابی یک مؤلفه نظر داد. البته این نحوه‌ی مدل‌سازی بیشتر برای سیستم‌های هیبرید تورین مثل شبکه‌های توزیع برق و انرژی کاربرد دارد. در مدل‌های سیستم‌های تورین تمامی گره‌ها یکسان فرض می‌شود و مدل انتشار خطای آن معمولاً با تحلیل‌های شبکه‌های پیچیده[۱۰] انجام می‌شود. درواقع برای سیستم‌هایی که همبندی آن‌ها یک شبکه پیچیده است می‌توان از این مدل استفاده کرد.

در مقاله [۱۲] به ارزیابی انتشار خرابی در سیستم‌های سایبر-فیزیکی[۱۱] پرداخته شده است. در این مقاله ارتباط بین گره رایانشی و فیزیکی بیشتر مورد توجه قرار گرفته است. در این روش یک قانون وجود دارد که هر گره محاسباتی باید توسط یک گره فیزیکی پشتیبانی شود، یعنی یک گره محاسباتی در صورتی خراب فرض می‌شود که ارتباط خود را با بخش فیزیکی از دست بدهد. یک گره محاسباتی در طول حیات خود می‌تواند با چندین گره فیزیکی مختلف ارتباط داشته باشد. تحلیل شبکه‌ای وقوع خطا در این مدل به این صورت است که در هر مرحله یک گره به‌صورت تصادفی حذف می‌شود. هنگام حذف یک گره تمامی پیوندهای آن نیز حذف می‌شود. سپس بزرگ‌ترین زیرشبکه را در هریک از شبکه‌های سایبری و فیزیکی در نظر گرفته می‌شود و سایر زیرشبکه‌ها نیز حذف می‌گردد.

در مقاله [۱۳] همانند مقاله قبلی روشی برای ارزیابی انتشار خطا در سیستم‌های سایبر-فیزیکی ارائه شده است. در این روش سیستم‌های سایبر-فیزیکی را به‌صورت دو شبکه فیزیکی و سایبری وابسته به هم در نظر گرفته است. در این روش کل سیستم به‌صورت یک شبکه متشکل از مؤلفه‌های سیستم در نظر گرفته می‌شود و هر یال بین دو مؤلفه نشان‌دهنده وابستگی دو مؤلفه است. هنگامی‌که یک گره دچار خرابی شود، آن گره همراه با یال‌های متصل به آن حذف خواهد شد. سایر گره‌ها درصورتی‌که یالی به آن وصل نباشد حذف خواهد شد روش ارزیابی مدل به‌صورت قابلیت اطمینان مرتبه k است. قابلیت اطمینان مرتبه k به این معنا است که درصورتی‌که یکی از شبکه‌های سایبری یا فیزیکی بیشتر از k گره سالم داشته باشد آن شبکه می‌تواند به عملکرد خود ادامه دهد. نحوه خرابی گره‌ها در این روش به‌صورت تصادفی است و منطق خاصی را دنبال نمی‌کند. یعنی ابتدا گراف شبکه کشیده می‌شود سپس یک یا چند مؤلفه به‌صورت تصادفی از آن حذف خواهد شد و تأثیر حذف آن و انتشار آن خرابی بر روی شبکه مشاهده خواهد شد. یکی از مشکلات این روش این است که پیچیدگی سیستم‌های سایبر-فیزیکی، تفاوت مؤلفه‌های آن‌ها و ارتباط پیچیده آن‌ها مخصوصاً ارتباط بین مؤلفه‌های سایبری و فیزیکی درست دیده نشده و مدل بسیار سطح بالا و دور از واقعیت است.

۳-۲- مدل‌های با انتزاع مؤلفه

در مقاله [۱۴] با استفاده از آتاماتای هیبرید به مدل‌سازی انتشار خطا در سیستم‌های هیبرید پرداخته شده است. ابتدا مدل هر مؤلفه به‌صورت جداگانه ساخته می‌شود، سپس بر اساس چهار نوع وابستگی این مدل‌ها به همدیگر متصل می‌شوند. انواع وابستگی در این مدل به‌صورت زیر است:

- **وابستگی فیزیکی:** عملکرد یک مؤلفه وابسته به عملکرد یک مؤلفه دیگر است.
- **وابستگی سایبری:** هنگامی‌که بین دو مؤلفه تبادل سیگنال صورت گیرد.
- **وابستگی جغرافیایی:** مؤلفه‌ها در یک منطقه جغرافیایی قرار داشته باشند (خطر زلزله).
- **وابستگی منطقی:** تصمیم‌های انسانی و سیاست‌های کاری بر روی آن تأثیرگذار باشد.

در مقاله [۷] روشی بر اساس درخت خطا حالت/رخداد ارائه شده است. از مدل ایجادشده به‌منظور ارزیابی ایمنی و امنیت سیستم‌هایی که از چندین مؤلفه مختلف تشکیل شده، استفاده شده است. درخت خطا حالت/رخداد ترکیب درخت خطا و مدل‌های حالت است. این مدل‌ها این امکان را فراهم می‌آورند که فضای حالت قطعی و رفتار خرابی احتمالی را در کنار یکدیگر در یک مدل قرار بگیرند. در این روش هر مؤلفه با مشخصه‌های مربوط به خود به‌صورت جداگانه مدل‌سازی می‌شود. این مشخصه‌ها شامل نرخ خرابی، نرخ تعمیر و غیره است. ارتباط مؤلفه‌ها در این روش از طریق رخدادهای متفاوت بین آن‌ها است. این رخدادها از طریق درگاه‌های موجود بر روی مؤلفه‌ها انتقال پیدا می‌کنند. مشکل این روش پیچیدگی طراحی و نیاز به پیش‌بینی مسیرهای خطا است که با توجه به پیچیده بودن سیستم‌های هیبرید، شناسایی این مسیرها سخت و غیرممکن است. همچنین مشکل دیگر این مدل ساختار ایستای آن است. در صورت ایجاد تغییر در یک ویژگی سیستم ممکن است بخش عظیمی از مدل تغییر کند

از مشکلات دیگر این روش وارد کردن تمام جزییات سیستم در مدل است. این مشکل فرایند مدل‌سازی را سخت و پیچیده می‌کند. همچنین این مدل زمان اجرای بالایی دارد.

در مقاله‌های [۱۵، ۱۶] روشی برای مدل‌سازی انتشار اشکال در سیستم‌های مکاترونیک ارائه شده است. در این روش دو پارامتر جریان داده و کنترل داده در مؤلفه‌های سیستم در نظر گرفته شده و بر اساس این دو پارامتر فرایند انتشار خطا ارزیابی شده است.

در مقاله [۱۷] حاشیه‌نویسی خرابی برای هر مؤلفه تولید می‌شود. این حاشیه‌نویسی‌ها نشان‌دهنده نحوه خرابی مؤلفه‌ها در برابر خطاهای گوناگون است. با استفاده از این حاشیه‌نویسی‌ها درخت خطای مؤلفه‌ها تولید می‌شوند که می‌تواند برای تحلیل انتشار خطا استفاده گردد. مشکلی که این مقاله دارد این است که ساختار آن ایستا است همچنین در مدل نهایی باید رخداد نهایی مشخص باشد. مشکل دیگر این روش تصادفی و احتمالی نبودن آن است که نمی‌توان تحلیل کمّی بر روی آن انجام داد.

در مقاله [۱۸] روشی برای ارزیابی ریسک با توجه به انتشار خطا در سیستم‌های سایبر-فیزیکی ارائه شده است. در این روش پارامترهای مختلفی ازجمله نقش انسان در آن در نظر گرفته شده است. روش ارائه‌شده در این مقاله روشی خوبی برای ارزیابی ریسک با توجه به انتشار خطا است. این روش خاص سیستم‌های الکتریکی و توزیع برق است.

۴- روش پیشنهادی

در این روش بر اساس سیستم موردمطالعه، گراف وابستگی داده‌ای و غیرداده‌ای استخراج می‌شود. سپس درصورتی‌که هریک از مؤلفه‌ها دارای رفتار احتمالی باشد، عبارت‌های احتمالی مربوط به آن اضافه می‌شود. درنهایت این گراف‌ها توسط روشی که در ادامه توضیح داده خواهد شد به مدل شبکه‌های فعالیت تصادفی هر مؤلفه تبدیل می‌شود. مدل هر یک از این مؤلفه‌ها با استفاده از صورت‌بندی تکرار/الحاق به همدیگر متصل می‌شوند. برای ارزیابی مدل پس از ساخت آن با توجه به نوع آزمایش، در یک یا چندین مؤلفه خطاهایی تزریق می‌شود و نحوه‌ی انتشار آن در کل سیستم و تأثیری که بر روی مؤلفه‌های دیگر می‌گذارد، مورد ارزیابی قرار می‌گیرد.

۴-۱- فرایند پیشنهادی برای مدل‌سازی انتشار خطا

ابتدا با استفاده از مشخصات سیستم، گراف‌های اولیه از سیستم تهیه می‌شود که این گراف‌ها عبارت‌اند از:

- **گراف وابستگی داده‌ای:** این گراف از همبندی سیستم به دست می‌آید که مشخص می‌کند هر مؤلفه‌ای از چه مؤلفه‌هایی ورودی می‌گیرد و به کدام مؤلفه‌ها خروجی می‌فرستد.
- **گراف وابستگی غیرداده‌ای:** این گراف مشخص می‌کند که خرابی یک مؤلفه بر روی کدام مؤلفه‌های دیگر تأثیرگذار خواهد بود. این وابستگی به خاطر ورودی و خروجی ناصحیح نیست بلکه به خاطر حضور یا عدم حضور یک مؤلفه است.

در ادامه بعد از ساخت گراف‌ها عبارت‌های احتمالی مربوط به هر یک از مؤلفه‌ها، استخراج می‌شود.

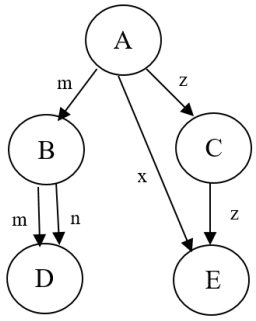
در ادامه قوانین برای تبدیل این گراف‌ها به مدل SAN ارائه شده است.

۴-۲- گراف وابستگی داده‌ای

مهم‌ترین ارتباطی که مؤلفه‌های یک سیستم باهمدیگر دارند، ارتباط ورودی و خروجی است. گراف وابستگی داده‌ای را می‌توان از همبندی شبکه به دست آورد. این گراف مشخص می‌کند که هر یک از مؤلفه‌های سیستم به کدام‌یک از مؤلفه‌های دیگر داده می‌فرستد و از کدام مؤلفه‌ها ورودی می‌گیرد. هنگام ساخت گراف داده‌ای درصورتی‌که یک مؤلفه چندین ورودی برای یک مؤلفه دیگر فراهم کند باید به تعداد ورودی‌ها میان آن‌ها یال کشیده شود. به‌طوری‌که هر یال نشان‌دهنده یک ارتباط است. شکل ۲ یک نمونه از گراف وابستگی داده‌ای را نشان می‌دهد. تعریف گراف وابستگی در فرمول ۱ آورده شده است.

$$\begin{gathered} G^{DF}=[N,D^{DF}] \\ N=\{n_1,\dots,n_t\} \\ D^{DF}=\{(n_i,n_j,V_{i,j}),\dots,(n_k,n_l,V_{k,l})\} \end{gathered} \quad (۱)$$

N مجموعه‌ای است که نشان‌دهنده رأس‌های گراف است. هر یک از این رأس‌ها، یک مؤلفه سیستم است. یال‌های بین آن‌ها که با مجموعه D^{DF} مشخص‌شده، ارتباط ورودی و خروجی مؤلفه‌ها است.

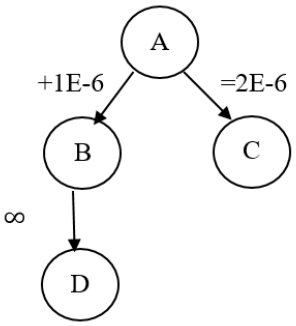


شکل ۲- یک نمونه گراف وابستگی داده‌ای

۴-۳- گراف وابستگی غیرداده‌ای

مؤلفه‌های یک سیستم ممکن است به‌صورت غیرمستقیم بر روی همدیگر تأثیر بگذارند. و این وابستگی بر روی مدل‌سازی انتشار خطا تأثیرگذار خواهد بود. گراف وابستگی غیرداده‌ای مشخص می‌کند که چه مؤلفه‌هایی به یکدیگر وابستگی دارند. در اینجا منظور از وابستگی تأثیری است که حضور یا عدم حضور یک مؤلفه بر نرخ خرابی یک مؤلفه دیگر می‌گذارد. به‌طور مثال خرابی مؤلفه خنک‌کننده باعث می‌شود نرخ خرابی یک مؤلفه دیگر بالاتر رود. در این گراف هر گره در صورت وجود وابستگی تنها یک یال به گره دیگر دارد. یک نمونه از گراف وابستگی غیرداده‌ای در شکل ۳ نشان داده شده است. این نوع وابستگی، پارامتری است که در کارهای پیشین دیده نشده است. درحالی‌که پارامتر مهمی بوده و در بسیاری از سیستم‌ها این وابستگی غیرمستقیم بین مؤلفه‌ها وجود دارد. نرخ خرابی با توجه به علامت ریاضی و مقداری که بر روی یال گراف قرار می‌گیرد تغییر می‌کند. تعریف گراف وابستگی غیرداده‌ای در فرمول ۲ نشان داده شده است.

$$\begin{gathered} G^{NDF}=[N,D^{NDF}] \\ N=\{n_1,\dots,n_t\} \\ D^{NDF}=\{(n_i,n_j,v_{i,j}),\dots,(n_k,n_l,v_{k,l})\} \end{gathered} \quad (۲)$$



شکل ۳- یک نمونه گراف وابستگی غیرداده‌ای

۴-۴- عبارت‌های احتمالی

مؤلفه‌هایی که ورودی دارند طبق روش‌های احتمالی FPTA[۱۲] که قبلاً در مقاله [۱۹] ارائه شده است. می‌توانند رفتار احتمالی داشته باشند. در این مقاله نیز از عبارت‌های احتمالی FPTA با تغییراتی جزئی استفاده شده است. در روش پیشنهادی ما، فرض شده است که هر ورودی یا خروجی دو حالت صحیح یا ناصحیح دارد. هر مؤلفه می‌تواند چندین ورودی داشته باشد. هریک از این ورودی‌ها می‌تواند صحیح یا ناصحیح باشد. رفتار مؤلفه با توجه به حالت‌های مختلفی که این ورودی‌ها دارند، می‌تواند احتمالی باشد. درواقع این عبارت‌ها نحوه‌ی انتشار خرابی از یک مؤلفه به مؤلفه‌های دیگر را به‌صورت احتمالی مشخص می‌کند. تمامی عبارت‌های احتمالی نیازی نیست که نوشته شوند و اگر فقط برای حالت‌هایی که خروجی صحیح است نوشته شود سایر عبارت‌های احتمالی قابل استنتاج است. بنابراین درصورتی‌که یک مؤلفه n ورودی و m خروجی مختلف داشته باشد به تعداد $2^n * 2^m$ عبارت احتمالی متفاوت نیاز داریم که 2^m حالت آن را می‌توان به‌صورت خودکار استخراج نمود. عبارت‌های احتمالی به‌صورت مجموعه معادله ۳ نشان داده می‌شود.

$$\begin{aligned} &1)\ \text{Input1.T, Input2.}\mathit{T} \rightarrow \text{Output1.T, 1.0} \\ &2)\ \text{Input1.}\mathit{F}\text{, Input2.T} \rightarrow \text{Output1.T, 0.6} \\ &3)\ \text{Input1.}\mathit{T}\text{, Input2.F} \rightarrow \text{Output1.T, 0.7} \\ &4)\ \text{Input1.}\mathit{F}\text{, Input2.F} \rightarrow \text{Output1.T, 0.02} \end{aligned} \quad (۳)$$

معادله‌های ۳ صحیح یا ناصحیح بودن خروجی مؤلفه در حالت‌های مختلفی که ورودی‌ها می‌توانند داشته باشند را نشان می‌دهد. به‌طور مثال با توجه به عبارت دوم هنگامی‌که ورودی اول ناصحیح باشد و ورودی دوم صحیح باشد این مؤلفه به‌احتمال

۰٫۶ خروجی صحیح تولید می‌کند و به احتمال ۰٫۴ مقدار خروجی این مؤلفه ناصحیح است.

۴-۵- تبدیل گراف وابستگی داده‌ای به مدل SAN

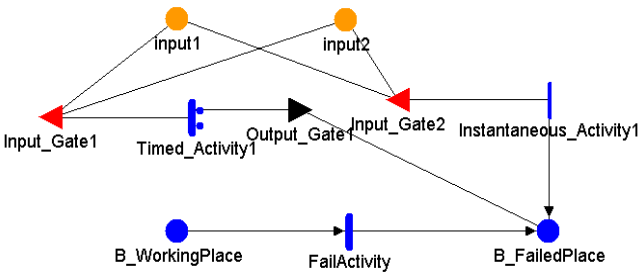
برای تبدیل این گراف به مدل SAN هرگاه از مؤلفه A به مؤلفه B یالی وجود داشته باشد، به معنای این است که A باید برای B ورودی ایجاد کند و آن را در اختیار B قرار دهد. این وابستگی از طریق یک مکان بسط‌یافته[۱۳] در مدل SAN ایجاد می‌گردد. در مدل SAN برای مکان‌های بسط‌یافته می‌توان ساختار داده تعریف کرد. ورودی‌ها و خروجی‌ها در مدل پیشنهادی می‌تواند دو حالت مختلف داشته باشد، حالتی که ورودی صحیح است و حالتی که ورودی ناصحیح است. بنابراین نشانه موجود در این مکان می‌تواند یک عدد صحیح باشد که عدد یک به معنای داده صحیح و عدد دو به معنای داده ناصحیح است. بنابراین به ازای هر جفت ورودی و خروجی باید یک مکان بسط‌یافته در مؤلفه A و B قرار داده شود. در ادامه برای تجمیع مدل نهایی از این مکان‌ها به‌عنوان مکان مشترک استفاده می‌شود.

$$O_i = \begin{cases} 1, & \text{مقدار خروجی ناصحیح باشد} \\ 2, & \text{مقدار خروجی صحیح باشد} \end{cases} \quad (۵)$$

$$I_i = \begin{cases} 1, & \text{مقدار ورودی ناصحیح باشد} \\ 2, & \text{مقدار ورودی صحیح باشد} \end{cases} \quad (۶)$$

همچنین می‌توان از مکان بسط‌یافته برای نشان دادن مقدار یک پارامتر استفاده کرد. به‌طور مثال برای نشان دادن تعداد کار انجام شده توسط یک پردازنده می‌توان از یک مکان بسط‌یافته برای شمارش این کارها استفاده کرد.

پس از ساخت مؤلفه‌های سیستم، هنگام الحاق مؤلفه‌ها به یکدیگر به‌منظور تشکیل مدل نهایی، مکان‌های بسط‌یافته مؤلفه‌هایی که به همدیگر وابستگی داده‌ای دارند باید به اشتراک گذاشته شود. در شکل ۴ مدل یک مؤلفه با ۲ ورودی مختلف نشان داده شده است.



شکل ۴- مؤلفه A با دو ورودی از سایر مؤلفه‌ها.

۴-۶- تبدیل گراف وابستگی غیرداده‌ای به مدل SAN

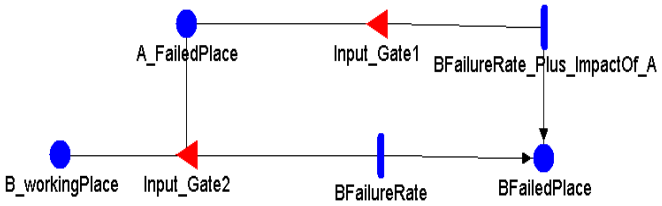
برای تزریق وابستگی غیرداده‌ای به مدل SAN باید به‌صورت زیر عمل کرد:

درصورتی‌که مؤلفه B به مؤلفه A وابستگی غیرداده‌ای داشته باشد باید حالت خرابی F مؤلفه A در مدل مؤلفه B قرار گیرد و این مکان بین این دو مؤلفه به اشتراک گذاشته شود. با استفاده از این مکان خرابی، زمانی که مؤلفه A خراب شد مؤلفه B از طریق این مکان متوجه خرابی مؤلفه A شود.

به ازای هر وابستگی غیرداده‌ای یک فعالیت جدید با نرخ جدیدی که از گراف وابستگی غیرداده‌ای محاسبه می‌شود در مدل مؤلفه قرار داده می‌شود.

به ازای هر فعالیت باید یک دروازه ورودی قرار داده شود که تابع شرطی آن با توجه به حالت خرابی مؤلفه A فعالیت مربوطه را فعال یا غیرفعال کند. به صورتی که قبل از خرابی مؤلفه A نرخ خرابی مؤلفه B از فعالیت اول پیروی کند و درصورتی‌که نشانه‌ای در مکان خرابی مؤلفه A قرار داده شد باید از فعالیت جدید پیروی کند. درآن‌واحد باید یکی از تابع‌های شرطی مربوط به دروازه‌های ورودی درست باشد و در هیچ حالتی دو تابع شرطی نباید هم‌زمان صحیح باشد.

در شکل ۵ یک نمونه مدل SAN مربوط به وابستگی غیرداده‌ای نشان داده شده است.



شکل ۴- مدل مؤلفه B در صورت داشتن وابستگی غیرداده‌ای به مؤلفه A.

۴-۷- تزریق عبارت‌های احتمالی به مدل SAN

برای تزریق عبارت‌های احتمالی مربوط به یک مؤلفه در داخل مدل آن مؤلفه، می‌توان از فعالیت‌های احتمالی با چندین خروجی استفاده کرد. فعالیت‌های احتمالی به این صورت است که می‌توان مشخص کرد در صورت فعال بودن فعالیت، در p درصد مواقع نشانه را از طریق خروجی اول بفرستد و در 1-p درصد مواقع نشانه را از طریق خروجی دوم ارسال کند. هر فعالیت می‌تواند چندین خروجی مختلف داشته باشد ولی مجموع احتمال آن‌ها باید یک باشد. به ازای هر عبارت احتمالی و برعکس آن یک فعالیت چندتایی نیاز داریم و هر یک از این فعالیت‌ها به یک دروازه ورودی متصل می‌شود. با توجه به ورودی‌های مؤلفه مشخص می‌شود این فعالیت هم‌اکنون باید فعال باشد یا خیر.

در هرلحظه یکی از چندین فعالیت احتمالی باید فعال باشد. به‌طور مثال برای دو عبارت ۷ یک فعالیت احتمالی با ۲ خروجی نیاز داریم.

$$\begin{aligned} &1)\ \text{Input1}.F, \text{Input2}.T \rightarrow \text{Output1}.\text{T}, 0.6 \\ &2)\ \text{Input1}.F, \text{Input2}.\text{T} \rightarrow \text{Output1}.\text{F}, 0.4 \end{aligned} \quad (۷)$$

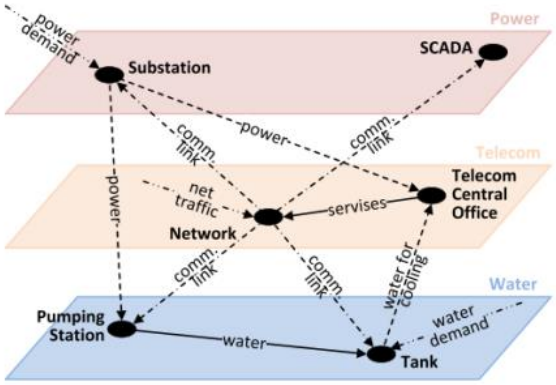
۴-۸- الحاق مؤلفه‌ها از طریق صورت‌بندی تکرار-الحاق

برای الحاق مؤلفه‌ها از صورت‌بندی تکرار-الحاق استفاده خواهد شد. طبق قوانینی که در بخش قبل توضیح داده شد، قوانین اتصال مؤلفه‌ها به یکدیگر به‌صورت زیر دسته‌بندی می‌شود:

- اتصال مؤلفه‌هایی که به همدیگر وابستگی داده‌ای دارند از طریق مکان‌های بسط‌یافته.
- اتصال مؤلفه‌هایی که به همدیگر وابستگی غیرداده‌ای دارند از طریق اشتراک مکان خرابی هر یک از مؤلفه‌ها.
- اتصال مؤلفه‌هایی که به‌منظور افزونگی در سیستم استفاده شده است از طریق اشتراک مکان خرابی مؤلفه‌های پیش‌نیاز.

۵- مطالعه موردی

در این بخش یک سیستم هیبرید متشکل از سه زیرساخت مختلف مدل‌سازی می‌شود. این سیستم شامل سه زیرساخت توزیع برق، زیرساخت آب‌رسانی و زیرساخت شبکه است. در زیرساخت آب‌رسانی یک پمپ آب و یک مخزن وجود دارد که وظیفه پمپ آب، تأمین آب موردنیاز مخزن آب است. همچنین در زیرساخت شبکه یک مجموعه تجهیزات شبکه و یک مرکز مخابرات وجود دارد این مرکز مخابراتی تجهیزات شبکه را مدیریت می‌کند. در زیرساخت سوم که زیرساخت توزیع برق است یک SCADA[۱۴] و ایستگاه برق وجود دارد که وظیفه ایستگاه برق تأمین برق موردنیاز پمپ آب و مرکز مخابراتی است. وظیفه SCADA نظارت بر توزیع برق است. شمای کلی این سیستم در شکل ۶ نشان داده شده است [۲۰].



شکل ۴- سیستم هیبرید متشکل از سه زیرساخت[۲۰]

۵-۱- سیستم هیبرید متشکل از سه زیرساخت

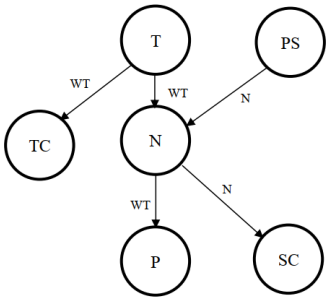
در این بخش به معرفی گراف‌ها و عبارات احتمالی مربوط به سیستم ترکیبی از چند زیرساخت پرداخته خواهد شد. با توجه به اینکه مؤلفه‌های این سیستم تمامی مؤلفه‌ها به‌صورت هم‌زمان مشغول به کار هستند و ترتیب اجرایی خاصی بین آن‌ها وجود ندارد. بنابراین در این مثال گراف ترتیب اجرایی وجود ندارد. اختصاراتی که در این مثال استفاده شده است در جدول ۱ نشان داده شده است.

جدول ۱: اختصارات اسامی مؤلفه‌های سیستم موردمطالعه.

نام مؤلفه	مخفف
پمپ آب	P
مخزن آب	T
ایستگاه برق	PS
SCADA	SC
مرکز مخابراتی	TC
شبکه	N

۵-۱-۱- گراف وابستگی داده‌ای سیستم موردمطالعه

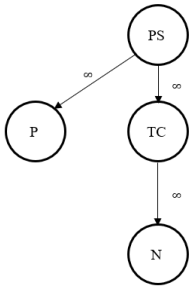
گراف وابستگی داده‌ای این سیستم در شکل ۷ نشان داده شده است. همان‌طور که در شکل ۷ مشخص است مخزن آب، سطح آب موجود در خود را به مرکز مخابراتی و شبکه ارسال می‌کند و شبکه این مقدار را برای پمپ ارسال می‌کند. همچنین ایستگاه برق مقدار برق توزیعی خود را برای شبکه ارسال کرده و شبکه این مقدار را برای SCADA می‌فرستد.



شکل ۷: گراف وابستگی داده‌ای سیستم موردمطالعه

۵-۱-۲- گراف وابستگی غیرداده‌ای سیستم موردمطالعه

در شکل ۸ گراف وابستگی غیرداده‌ای سیستم نشان داده شده است. همان‌طور که مشخص است در صورت خرابی ایستگاه برق، مرکز مخابراتی و پمپ آب نیز دچار خرابی می‌شوند و همچنین در صورت خراب شدن مرکز مخابراتی و عدم توانایی آن در ارائه سرویس، زیرساخت شبکه در عملکرد خود دچار مشکل می‌شود.



شکل ۸: گراف وابستگی غیرداده‌ای سیستم موردمطالعه

۵-۱-۳- عبارت‌های احتمالی مربوط به سیستم موردمطالعه

ایستگاه برق پس از دریافت دستورات کنترلی SCADA به‌عنوان ورودی، درصورتی‌که دستورات صحیح باشد در ۹۹ درصد مواقع ایستگاه برق به‌درستی دستورات را اعمال می‌کند. و درصورتی‌که دستورات اشتباه باشد قطعاً دستورات ناصحیح اعمال می‌شود. عبارت‌های احتمالی مربوط به آن در زیر نشان داده شده است:

$$SC.False \rightarrow PS.Fail, 0.99$$
$$SC.True \rightarrow C.Fail, 1 \qquad (۸)$$

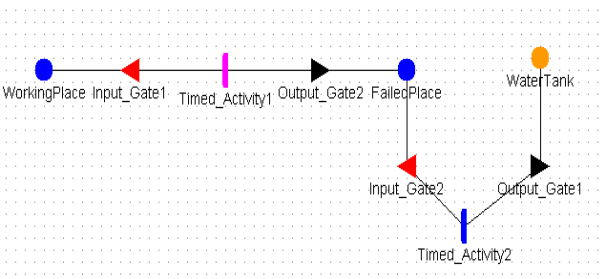
۵-۱-۴- طراحی مدل SAN مؤلفه‌های سیستم موردمطالعه

در این بخش هر یک از مؤلفه‌های سیستم سوخت‌رسان طراحی شده است. در طراحی هر یک از مؤلفه‌ها، نحوه‌ی استفاده از گراف‌های تولیدشده شرح داده است. تمامی متغیرهایی که برای نرخ خرابی یا تأثیر بر روی نرخ خرابی در نظر گرفته شده است در هنگام شبیه‌سازی مقداردهی می‌شود.

◘ مؤلفه مخزن آب

مدل SAN مربوط به مخزن آب در شکل ۹ نشان داده شده است. مخزن آب وقتی دچار خرابی می‌شود با یک نرخی که بعداً مقداردهی می‌شود نشتی می‌کند. با توجه به شکل مکان‌های مدل مؤلفه SAN به‌صورت زیر است:

- **WorkingPlace**: این مکان نشان‌دهنده سالم بودن مخزن آب است. هنگامی‌که یک نشانه داخل این مکان باشد یعنی مخزن عملکرد صحیحی دارد.
- **FailedPlace**: این مکان نشان‌دهنده خرابی مخزن آب است. هنگامی‌که یک نشانه داخل این مکان باشد یعنی مخزن دچار خرابی شده است و از این به بعد با یک نرخی مشخص نشتی دارد.
- **WaterTank**: این مکان نشان‌دهنده سطح آب داخل مخزن است که می‌تواند مقداری بین صفر تا ده داشته باشد.



شکل ۹: مدل SAN مؤلفه مخزن آب

جدول مربوط به دروازه‌های ورودی در جدول ۲ آمده است همچنین مشخصات دروازه‌های ورودی این مدل به این صورت است:

- **Input_Gate1**: این دروازه هنگامی اجازه شلیک به فعالیت Time_Activity1 را می‌دهد که مخزن سالم باشد و همچنین پس از شلیک، تعداد نشانه‌های داخل مکان WorkingPlace را برابر صفر قرار می‌دهد.
- **Input_Gate2**: این دروازه هنگامی اجازه شلیک به فعالیت Time_Activity2 را می‌دهد که مخزن خراب شده باشد.

جداول مربوط به دروازه‌های خروجی در جدول ۳ آمده است. همچنین نرخ فعالیت‌های این مؤلفه در جدول ۴ نشان داده شده است. تمامی نرخ‌ها از توزیع نمایی پیروی می‌کنند.

مشخصات دروازه‌های خروجی این مدل به‌صورت زیر است:

- **Output_Gate1**: هنگامی‌که فعالیت Time_Activity2 شلیک کند به معنی این است که مخزن خراب شده است و نشتی دارد بنابراین این دروازه ۲-واحد از آب موجود در مخزن را کم می‌کند.
- **Output_Gate2**: هنگامی‌که فعالیت Time_Activity1 شلیک کند این دروازه تعداد نشانه مکان FailedPlace را برابر صفر قرار می‌دهد.

جدول ۲: جدول دروازه‌های ورودی مدل مؤلفه مخزن آب

Input_Gate1	**عبارت شرطی**
	WorkingPlace->Mark()==1 && FailedPlace->Mark()==0
	تابع ورودی
	WorkingPlace->Mark()=0;
Input_Gate2	**عبارت شرطی**
	FailedPlace->Mark()==1

جدول ۳: جدول دروازه‌های خروجی مدل مؤلفه مخزن آب

Output_Gate1	**تابع خروجی**
	if(WaterTank->Mark()>=3) { WaterTank->Mark() = WaterTank->Mark()-3; } else{ WaterTank->Mark() = 0; }
Output_Gate2	**تابع خروجی**
	FailedPlace->Mark()=1;

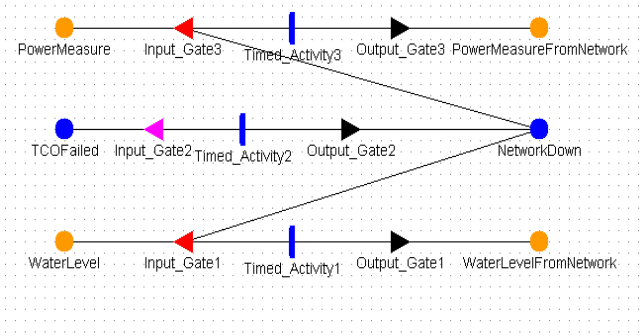
جدول ۴: نرخ فعالیت‌های مدل مؤلفه مخزن آب

نام فعالیت	نرخ شلیک
Time_Activity1	TankFailureRate
Time_Activity2	LeakRate

مؤلفه شبکه

زیرساخت شبکه به این صورت است که مقدار سطح آب و برق مصرفی را برای پمپ آب و SCADA می‌فرستد. همچنین این مؤلفه توسط مرکز مخابراتی کنترل می‌شود. و درصورتی‌که مرکز مخابراتی دچار اختلال شود این اختلال باعث خرابی این مؤلفه نیز می‌شود. مدل SAN مربوط به این مؤلفه در شکل ۱۰ نشان داده شده است. مکان‌های موجود در این مؤلفه به‌صورت زیر است:

- **PowerMeasure**: این مکان نشان‌دهنده مقدار برق توزیع‌شده توسط ایستگاه برق است. هنگامی‌که مقدار آن یک باشد یعنی مقدار برق توزیع‌شده درست اندازه‌گیری شده است و هنگامی‌که مقدار آن دو باشد یعنی مقدار آن نادرست اندازه‌گیری شده است. این مکان به دلیل وابستگی داده‌ای بین شبکه و ایستگاه برق، در این مؤلفه قرار داده شده است.
- **TCOFailed**: این مکان نشان‌دهنده خرابی مرکز خدماتی است و به دلیل وابستگی غیرداده‌ای بین این دو مؤلفه، در مدل مؤلفه شبکه قرار داده شده است.
- **WaterLevel**: این مکان نشان‌دهنده سطح آب داخل مخزن است. این مکان به دلیل وابستگی داده‌ای بین مخزن آب و شبکه، در این مؤلفه قرار داده شده است.
- **NetworkDown**: این مکان نشان‌دهنده خرابی این مؤلفه است.
- **PowerMeasureFromNetwork**: این مکان نشان‌دهنده مقدار برق توزیع‌شده از طریق ایستگاه برق است که توسط ایستگاه برق گزارش‌شده است.
- **WaterLevelFromNetwork**: این مکان نشان‌دهنده سطح آب مخزن است که از مؤلفه شبکه عبور کرده است.



شکل ۱۰: مدل SAN مؤلفه شبکه

جدول مربوط به دروازه‌های ورودی در جدول ۵ نشان داده شده است همچنین مشخصات دروازه‌های ورودی این مدل به‌صورت زیر است:

- **Input_Gate1**: این دروازه هنگامی اجازه شلیک به فعالیت Time_Activity1 را می‌دهد که شبکه سالم باشد.
- **Input_Gate2**: این دروازه هنگامی اجازه شلیک به فعالیت Time_Activity2 را می‌دهد که مرکز مخابراتی خراب شده باشد و شبکه سالم باشد.
- **Input_Gate3**: این دروازه هنگامی اجازه شلیک به فعالیت Time_Activity3 را می‌دهد که مقدار جدیدی در مکان PowerMeasure قرار بگیرد.

جدول ۵: جدول دروازه‌های ورودی مدل مؤلفه شبکه

Input_Gate1	**عبارت شرطی**
	NetworkDown->Mark()==0
	تابع ورودی
	;
Input_Gate2	**عبارت شرطی**
	NetworkDown->Mark()==0 && TCOFailed->Mark()==1
	تابع ورودی
	;
Input_Gate3	**عبارت شرطی**
	PowerMeasure->Mark() != PowerMeasureFromNetwork->Mark()
	تابع ورودی
	;

جدول مربوط به دروازه خروجی در جدول ۶ نشان داده شده است. همچنین نرخ فعالیت‌های این مؤلفه در جدول ۷ نشان داده شده است. تمامی نرخ‌ها از توزیع نمایی پیروی می‌کنند. مشخصات دروازه خروجی این مدل به‌صورت زیر است:

- **Output_Gate1**: هنگامی‌که فعالیت Time_Activity1 شلیک کند مقدار سطح آب را از طریق شبکه گزارش می‌دهد.
- **Output_Gate2**: هنگامی‌که فعالیت Time_Activity2 شلیک کند وضعیت شبکه را در حالت خراب تنظیم می‌کند.
- **Output_Gate3**: هنگامی‌که فعالیت Time_Activity3 شلیک کند درصورتی‌که شبکه خراب باشد، یک مقدار اشتباه و در غیر این صورت مقدار دریافت شده را در خروجی قرار می‌دهد.

جدول ۶: جدول دروازه‌های خروجی مدل مؤلفه شبکه

Output_Gate1	**تابع خروجی**
	WaterLevelFromNetwork->Mark() = WaterLevel->Mark();
Output_Gate2	**تابع خروجی**
	NetworkDown ->Mark()=1;
Output_Gate3	**تابع خروجی**
	if(NetworkDown->Mark()==0){ PowerMeasureFromNetwork->Mark() = PowerMeasure->Mark();} else{PowerMeasureFromNetwork->Mark()=2; }

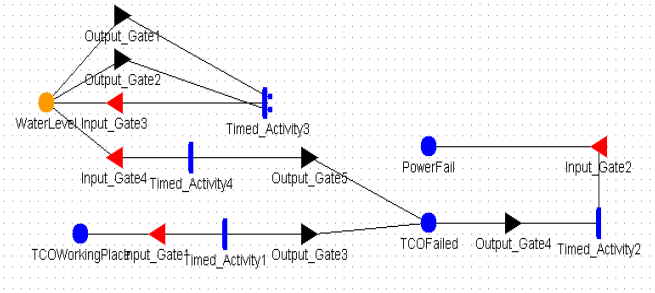
جدول ۷: نرخ فعالیت‌های مدل مؤلفه شبکه

نام فعالیت	نرخ شلیک
Time_Activity1	1
Time_Activity2	10
Time_Activity3	1

مؤلفه مرکز خدماتی

مرکز خدماتی وظیفه سرویس‌رسانی به شبکه را دارد. همچنین دارای یک خنک‌کننده است که از آب داخل مخزن آب استفاده می‌کند. مدل SAN این مؤلفه در شکل ۱۱ نشان داده شده است.

- **TCOFailed**: این مکان نشان‌دهنده خرابی مرکز خدماتی است.
- **WaterLevel**: این مکان نشان‌دهنده سطح آب داخل مخزن است. این مکان به دلیل وابستگی داده‌ای بین مخزن آب و مرکز خدماتی در این مؤلفه قرار داده شده است.
- **TCOWorkingPlace**: این مکان نشان‌دهنده سالم بودن مرکز خدماتی است.
- **PowerFail**: این مکان در صورت داشتن نشانه بیان‌گر قطعی برق است. این مکان به دلیل وابستگی غیرداده‌ای مرکز خدماتی و ایستگاه برق، در داخل مدل این مؤلفه قرار داده شده است.
- جداول مربوط به دروازه‌های ورودی در جدول ۸ آورده شده است. همچنین مشخصات دروازه‌های ورودی این مدل به این‌صورت است:
- **Input_Gate1**: این دروازه هنگامی اجازه شلیک به فعالیت Time_Activity1 را می‌دهد که مرکز خدماتی به‌صورت عادی خراب شود. یعنی مخزن آب خالی نباشد.
- **Input_Gate2**: این دروازه هنگامی اجازه شلیک به فعالیت Time_Activity2 را می‌دهد که برق قطع شده باشد.
- **Input_Gate3**: این دروازه هنگامی اجازه شلیک به فعالیت Time_Activity3 را می‌دهد که مخزن آب خالی نباشد.
- **Input_Gate4**: این دروازه هنگامی اجازه شلیک به فعالیت Time_Activity4 را می‌دهد که مخزن آب خالی باشد و مرکز خدماتی به‌صورت غیرعادی خراب شود.



شکل ۱۱: مدل SAN مرکز خدماتی

جدول ۸: جدول دروازه‌های ورودی مدل مؤلفه مرکز خدماتی

Input_Gate1	**عبارت شرطی**
	TCOWorkingPlace->Mark()==1 && WaterLevel->Mark()>0
	تابع ورودی
	TCOWorkingPlace->Mark()=0; TCOFailed->Mark()=1;
Input_Gate2	**عبارت شرطی**
	TCOWorkingPlace->Mark()==1 && PowerFail->Mark()==1 && TCOFailed->Mark()==0
	تابع ورودی
	TCOWorkingPlace->Mark()=0; TCOFailed->Mark()=1;
Input_Gate3	**عبارت شرطی**
	WaterLevel->Mark()>0 && TCOFailed->Mark()==0
	تابع ورودی
	;
Input_Gate4	**عبارت شرطی**
	WaterLevel->Mark()==0 && TCOWorkingPlace->Mark()==1
	تابع ورودی
	TCOWorkingPlace->Mark()=0; TCOFailed->Mark()=1;

جداول مربوط به دروازه‌های خروجی در جدول ۹ آورده شده است. همچنین مشخصات دروازه‌های ورودی این مدل به این‌صورت است:

- **Output_Gate1**: هنگامی‌که فعالیت Time_Activity3 شلیک کند مقدار سطح آب را یک واحد کاهش می‌دهد
- **Output_Gate2**: هنگامی‌که فعالیت Time_Activity3 شلیک کند مقدار سطح آب را دو واحد کاهش می‌دهد
- **Output_Gate3**: هنگامی‌که فعالیت Time_Activity1 شلیک کند وضعیت مرکز خرابی را خراب شده تعیین می‌کند.
- **Output_Gate4**: هنگامی‌که فعالیت Time_Activity2 شلیک کند وضعیت مرکز خرابی را خراب شده تعیین می‌کند.
- **Output_Gate5**: هنگامی‌که فعالیت Time_Activity4 شلیک کند وضعیت شبکه را در حالت خراب شده تنظیم می‌کند.

نرخ خرابی فعالیت‌های این مدل در جدول ۱۰ نشان داده شده است. تمامی نرخ‌ها از توزیع نمایی پیروی می‌کنند.

جدول ۹: جدول دروازه‌های ورودی مدل مؤلفه مرکز خدماتی

Output_Gate1	**تابع خروجی**
	WaterLevel->Mark() = WaterLevel->Mark()-1;
Output_Gate2	**تابع خروجی**

	if(WaterLevel->Mark()>1)
	WaterLevel->Mark()=WaterLevel->Mark()-2 ;
	else
	WaterLevel->Mark()=WaterLevel->Mark()-1 ;

Output_Gate3	**تابع خروجی**
	TCOFailed->Mark()=1;
Output_Gate4	**تابع خروجی**
	TCOFailed->Mark()=1;
Output_Gate5	**تابع خروجی**
	TCOFailed->Mark()=1;

جدول ۱۰: نرخ فعالیت‌های مدل مؤلفه مرکز خدماتی

نام فعالیت	نرخ شلیک
Time_Activity1	FailureRate
Time_Activity2	1
Time_Activity3	ConsumeRate
Time_Activity4	FailureRateWithoutWater

نحوه طراحی سایر مؤلفه‌ها در بخش پیوست مقاله آورده شده است. در ادامه به چگونگی الحاق این مؤلفه‌ها پرداخته شده است.

۵-۱-۵- الحاق مؤلفه‌های سیستم موردمطالعه

با توجه به روش مدل‌سازی که در بخش قبل توضیح داده شد برای الحاق مؤلفه‌ها با یکدیگر باید مکان‌ها به‌صورت زیر با یکدیگر به اشتراک گذاشته شوند.

- مکان‌های PowerMeasure در مدل مؤلفه‌های شبکه و ایستگاه برق (این اشتراک به دلیل وجود وابستگی داده‌ای است)
- مکان‌های PowerMeasureFromNetwork در مدل مؤلفه‌های SCADA و شبکه (این اشتراک به دلیل وجود وابستگی داده‌ای است)
- مکان‌های PowerFail در مؤلفه ایستگاه برق و مرکز مخابراتی و مکان SCADA_FailedPlace در مدل مؤلفه SCADA (این اشتراک به دلیل داشتن وابستگی غیرداده‌ای بین این سه مؤلفه است)
- مکان‌های SCADA_Output در مدل مؤلفه‌های SCADA و ایستگاه برق (این اشتراک به دلیل داشتن وابستگی داده‌ای بین این دو مؤلفه است)
- مکان‌های TCO_Failed در مدل مؤلفه‌های مرکز مخابراتی و شبکه (این اشتراک به دلیل داشتن وابستگی غیرداده‌ای بین این دو مؤلفه است)
- مکان‌های WaterLevel در مدل مؤلفه‌های شبکه، پمپ آب و مرکز مخابراتی و مکان WaterTank در مدل مخزن(این اشتراک به دلیل داشتن وابستگی داده‌ای بین این چهار مؤلفه است)
- مکان‌های WaterLevelFromNetworkدر مدل مؤلفه‌های شبکه و پمپ آب (این اشتراک به دلیل داشتن وابستگی داده‌ای بین این دو مؤلفه است)

۵-۱-۶- ارزیابی مطالعه موردی

برای مدل‌سازی و شبیه‌سازی روش پیشنهادی از سیستمی با پردازنده Core i7-3630QM، حافظه اصلی ۱۲ گیگابایتی و دیسک ۲۵۰ گیگابایتی SAMSUNG Evo850 استفاده شده است. همچنین نرم‌افزار Mobius در محیط ویندوز ۱۰ به‌منظور ابزار مدل‌سازی شبکه‌های فعالیت تصادفی مورد استفاده قرار گرفته است.

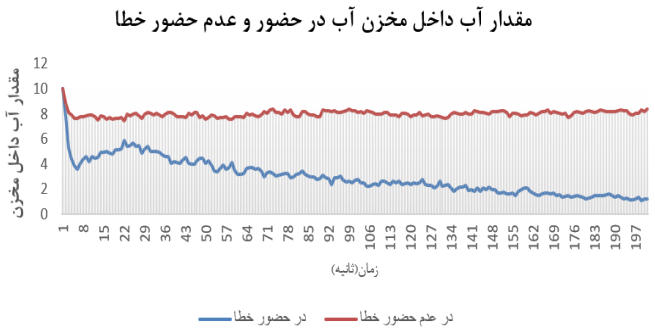
پس از الحاق مؤلفه‌های سیستم برای اجرای شبیه‌سازی ابتدا سیستم را بدون حضور هیچ خطایی اجرا می‌کنیم سپس با تزریق خطایی که منجر به خرابی مخزن آب شود شبیه‌سازی را اجرا می‌کنیم و نتایج این دو حالت را باهم مقایسه می‌کنیم. مقادیری که برای متغیرهای این مدل در نظر گرفته شده است در جدول ۱۱ نشان داده شده است. در هر آزمایش، مدل ۱۰۰ بار اجرا شده است و از مقادیر به‌دست‌آمده میانگین گرفته شده است.

جدول ۱۱: مقادیر متغیرهای مؤلفه‌های مدل در این آزمایش

نام متغیر	مقدار
ConsumeRate	1.0
FailureRate	1.0E-4
FailureRateWithoutWater	1.0
LeakRate	1.0
NormalFailureRate	1.0E-8
SCADA_FAilureRate	1.0E-8
TankFailureRate	1.0E-4
UnNormalFailureRate	1.0E-4
WorkingRate	2.0

◘ سطح آب داخل مخزن در حضور و عدم حضور خطا

هنگامی‌که مخزن آب سالم باشد تقریباً با استفاده از این پمپ آبی که استفاده شده است، سطح آب داخل مخزن بین ۷ تا ۸ تغییر می‌کند. ولی درصورتی‌که مخزن دچار خرابی شده باشد با یک شیب ملایم به سمت صفر میل می‌کند. نمودار میانگین آب داخل مخزن در شکل ۱۲ نشان داده شده است.



شکل ۱۲: مقدار آب داخل مخزن در حضور و عدم حضور خطا

◘ تحلیل رفتار مرکز مخابراتی در حضور و عدم حضور خطا

هنگامی‌که مخزن آب دچار خرابی شده باشد. در آب‌رسانی به مرکز خدماتی دچار مشکل می‌شود و این احتمال وجود دارد که زودتر دچار خرابی شود. نمودار رفتار خرابی این مؤلفه در شکل ۱۳ آورده شده است. همچنین درصورتی‌که مخزن آب دچار خرابی شده باشد. به‌طورقطع مرکز خدماتی در ثانیه ۴۰ام کاملاً خراب شده است و توانایی سرویس‌دهی ندارد.

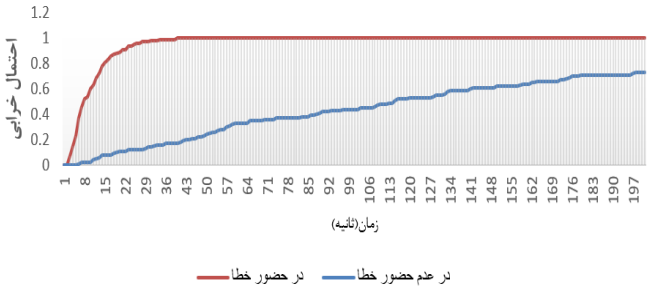
زمان خرابی مرکز خدماتی در حضور خطا در مخزن آب (سطح ۰,۷۵):

$T = 13s$

زمان خرابی مرکز خدماتی در عدم حضور خطا در مخزن آب (سطح ۰,۷۵):

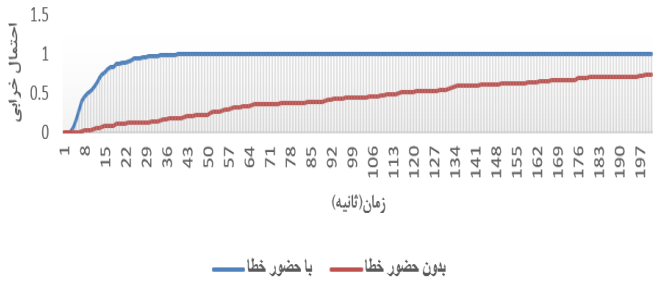
$T = 200s$

رفتار خرابی مرکز مخابراتی در حضور و عدم حضور خطا



شکل ۱۳: رفتار خرابی مرکز مخابراتی در حضور و عدم حضور خطا

رفتار خرابی شبکه در حضور و عدم حضور خطا



شکل ۱۴: رفتار خرابی مؤلفه شبکه زیرساخت در حضور و عدم حضور خطا

تحلیل رفتار شبکه در حضور و عدم حضور خطا

شبکه در صورتی می‌تواند که خدماتی همچون مقدار سطح آب را به پمپ آب گزارش دهد که مرکز خدماتی سالم باشد و توانایی سرویس‌رسانی را داشته باشد. در شکل ۱۴ نمودار رفتار خرابی این مؤلفه آورده شده است. درصورتی‌که مخزن آب دچار خرابی نشده باشد شبکه در ثانیه صدم به‌احتمال کمتر ۰,۴۴ صدم دچار خرابی شده است. بنابراین اگر زمان عملیات سیستم کمتر از ۱۰۰ ثانیه باشد این مقدار قابل‌اعتماد است.

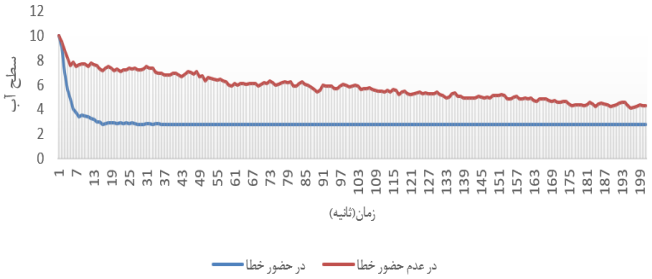
احتمال خرابی مؤلفه شبکه در حضور خطا:

$$P(F,100) = 1$$

احتمال خرابی مؤلفه شبکه در عدم حضور خطا:

$$P(F,200) = 0.44$$

سطح آب گزارش شده از طریق شبکه در حضور و عدم حضور خطا

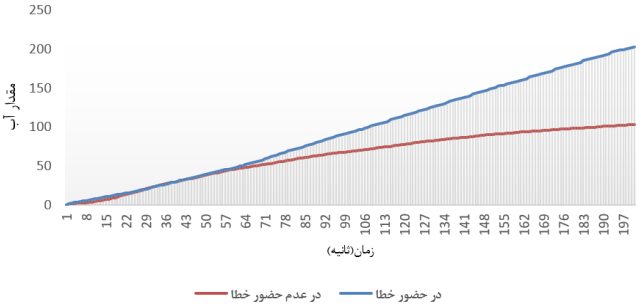


شکل ۱۵: سطح آب گزارش شده از طریق شبکه

سطح آب گزارش‌شده توسط شبکه در حضور و عدم حضور خطا

پمپ آب از سطح آب گزارش‌شده از طریق شبکه اطلاع دارد و درصورتی‌که شبکه دچار اختلال شده باشد این مقدار ممکن است صحیح نباشد. همان‌طور که در شکل ۱۵ نشان داده شده است. شبکه از ثانیه ۴۴ دچار خرابی شده و مقدار سطح آب را به‌صورت نادرست گزارش داده و باعث رخداد اشتباه در عملکرد پمپ آب شده است. این گزارش اشتباه باعث هدر رفتن آب در مخزن می‌شود. این رخداد به این دلیل اتفاق افتاده است که پمپ از مقدار آب واقعی داخل مخزن اطلاع ندارد و سرریز رخ داده است. نمودار مقدار آب سرریز شده در حضور و عدم حضور خطا نشان داده شده است.همان‌طور که شکل ۱۶ نشان داده شده است در صورت وجود خطا تقریباً دو برابر حالت عادی آب هدررفته است.

مقدار آب هدر رفته در حضور و عدم حضور خطا



شکل ۱۶: مقدار آب هدررفته در حضور و عدم حضور خطا

مقدار آب هدررفته در حضور خطا: 203L

مقدار آب هدررفته در عدم حضور خطا: 102L

احتمال قطعی برق در حضور و عدم حضور خطا

خرابی در مخزن آب باعث ازکارافتادن شبکه سیستم می‌شود بنابراین می‌تواند بر روی قطعی برق نیز تأثیرگذار باشد. همان‌طور که در شکل ۱۷ نشان داده شده است هنگامی‌که مخزن آب سالم نباشد احتمال قطعی برق در هرلحظه بیشتر است به‌طوری‌که احتمال قطعی برق در ثانیه ۲۰۰ام به‌صورت زیر است:

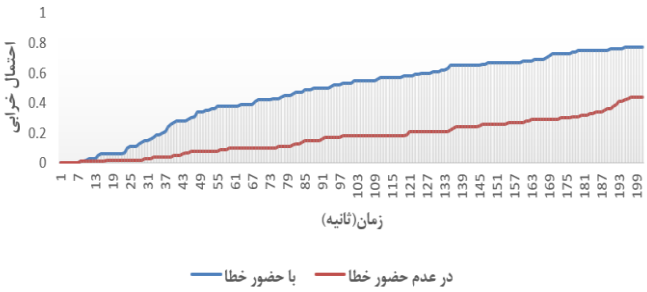
احتمال قطعی برق در ثانیه ۲۰۰ام در حضور خطا:

$$P(F) = 0.78$$

احتمال قطعی برق در ثانیه ۲۰۰ام در عدم حضور خطا:

$$P(F) = 0.44$$

قطعی برق در حضور و عدم حضور خطا



شکل ۱۷: احتمال قطعی برق در حضور و عدم حضور خطا

۵-۲- مقایسه روش پیشنهادی و نتیجه‌گیری

در این بخش روش پیشنهادی این پژوهش با مقاله‌های [۱۴] و [۲۰] مقایسه شده است. در ادامه مقایسه روش پیشنهادی از منظر پارامترهای مختلف با سایر روش‌ها آورده شده است.

۵-۲-۱- پارامترهای در نظر گرفته شده در مدل

روش‌های مقاله‌های پیشین به ارتباط مستقیم مؤلفه‌ها و نحوه‌ی ترکیب خطاها باهمدیگر پرداخته شده است. درحالی‌که پارامترهای دیگری در فرایند انتشار خطا می‌توانند مؤثر باشند. در روش پیشنهادی این مقاله علاوه بر در نظر گرفتن ارتباط مستقیم مؤلفه‌ها، پارامترهای دیگری در نظر گرفته‌شده‌اند که عبارت‌اند از ترکیب احتمالی خطاها و وابستگی غیرداده‌ای که بین مؤلفه‌ها وجود دارد.

۵-۲-۲- تفاوت در مدل انتخاب‌شده

در مقاله [20] برای مدل‌سازی از شبکه پتری و شبکه بیزی استفاده کرده است. این مدل‌ها با توجه به ساده بودن و امکانات کم آن‌ها فرایند مدل‌سازی را سخت و پیچیده می‌کند. این امکانات شامل مکان‌های بسط‌یافته، فعالیت‌های دارای چند حالت احتمالی و غیره است، که در مدل SAN وجود دارد. بنابراین درصورتی‌که یک سیستم را با این روش مدل‌سازی شود به دلیل قابلیت‌های کم مدل، مدل بسیار بزرگ و فرایند مدل‌سازی زمان‌بر و پیچیده می‌شود. همچنین در این روش باید قبل از مدل‌سازی همه‌ی خطاها را پیش‌بینی کرد و نحوه‌ی ترکیب آن‌ها برای انتشار در سایر مؤلفه‌ها را نیز در نظر گرفت. در روش مقاله [۱۴] از آتاماتای هیبریدی استفاده شده بود. برای مدل‌سازی با این روش باید تمامی جزییات مدل را در نظر گرفت. این جزییات شامل فرمول‌های مربوط به هر یک از مؤلفه‌ها نیز می‌شود. به‌طور مثال برای پر شدن مخزن آب باید دقیقاً فرمول نحوه‌ی پر شدن مدل را قرار داد و عملاً باید سیستم به‌صورت واقعی مدل شود. که این روش فرایند مدل‌سازی را بسیار پیچیده می‌کند.

در روش پیشنهادی این مقاله نیز به دست آوردن گراف وابستگی غیرداده‌ای می‌تواند بسیار زمان‌بر باشد. درواقع مدل‌ساز به‌منظور مدل‌سازی سیستم‌های بزرگ، باید زمان زیادی را صرف شناسایی ارتباطات غیرمستقیم بین مؤلفه‌های سیستم کند.

۵-۲-۳- نتایج به‌دست‌آمده از مدل

در روش پیشنهادی این مقاله با توجه به پویایی بالای مدل، می‌توان نتایج متنوعی را از مدل استخراج نمود. این نتایج می‌تواند قبل از طراحی سیستم جهت تصمیم مناسب در انتخاب مؤلفه‌های مختلف استفاده گردد. ازجمله نتایج قابل استخراج از مدل پیشنهادی عبارت‌اند از:

- ارزیابی قابلیت اطمینان کل سیستم
- احتمال خرابی هر مؤلفه در هرلحظه
- ترتیب خرابی مؤلفه‌ها
- نحوه انتشار خطا در سیستم
- مشخص کردن مؤلفه حیاتی
- میانگین زمان تا خرابی یک مؤلفه
- مشخص کردن مؤلفه‌های مناسب به‌منظور طراحی سیستم

۵-۲-۴- جامعیت و مقیاس‌پذیری

با توجه به رابط‌های ارائه شده برای مؤلفه‌های سیستم، هر مؤلفه‌ای شامل تعدادی ورودی و تعدادی خروجی است و نحوه نگاشت ورودی‌ها به خروجی‌ها را نیز می‌توان با عبارت‌های احتمالی مشخص کرد. مشخص است که هر مؤلفه‌ای در این ساختار می‌تواند قرار بگیرد و این موضوع جامعیت مدل را نشان می‌دهد.

با توجه به اینکه ارتباط تمامی مؤلفه‌ها در مدل ارائه شده این مقاله بر اساس ورودی و خروجی و ارتباط غیرداده‌ای است، درصورتی‌که چندین سیستم وجود داشته باشند که باهمدیگر ارتباط داشته باشند و بتوان آن‌ها را کنار هم قرار داد، به‌راحتی می‌توان ارتباط بین آن‌ها را با توجه به قوانین گفته‌شده فراهم کرد و مدل سیستم ترکیبی، متشکل از چند زیرسیستم را ایجاد نمود. بنابراین می‌توان نشان داد که مدل ارائه شده مقیاس‌پذیر نیز است.

۶- مراجع

[1] R. Alur, Principles of Cyber-Physical Systems, Massachusetts: MIT Press, 2015.

[2] S. Seshia and E. Lee, Introduction to Embedded Systems - A Cyber-Physical Systems Approach, MIT Press, 2017.

[3] M. Fan, Z. Zeng, E. Zio, R. Kang and Y. Chen, "A stochastic hybrid systems model of common-cause failures of degrading components," *Reliability Engineering & System Safety,* vol. 172, pp. 159-170, 2018.

[4] A. Avizienis, J.-C. Laprie, B. Randell and C. Landwehr, "Basic Concepts and Taxonomy of dependable and secure computing," *IEEE Transactions on Dependable and Secure Computing,* vol. 1, no. 1, pp. 11-33, 2004.

[5] R. Kang and Z. Li, "Strategy for reliability testing and evaluation of cyber physical systems," in *IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, Singapore, Dec 2015.

[6] G. Simko, T. Levendovszky, M. Maroti and J. Sztipanovits, "Towards a theory for cyber-physical systems modeling," in *Proceedings of the 4th ACM SIGBED International Workshop on Design, Modeling, and Evaluation of Cyber-Physical Systems*, Berlin, April 2014.

[7] R. Michael and P. Liggesmeyer, "Modeling and analysis of safety-critical cyber physical systems using state/event fault trees," in *International Conference on Computer Safety, Reliability and Security*, Toulouse, Sep 2013.

[8] W. H. Sanders and J. F. Meyer, "Stochastic activity networks: formal definitions and concepts," in *Lectures on formal methods and performance analysis*, New York, Springer, 2001, pp. 315 - 343.

[9] M. Rahnamay Naeini and M. M. Hayat, "Cascading Failures in Interdependent Infrastructures: An Interdependent Markov-Chain Approach," *IEEE Transactions on Smart Grid,* vol. 7, no. 4, pp. 1997-2006, 2016.

[10] R. A. Shuvro, Z. Wangt , P. Das, M. R. Naeini and M. M. Hayat, "Modeling cascading-failures in power grids including communication and human operator impacts," in *IEEE Green Energy and Smart Systems Conference*, Long Beach, Nov 2017.

[11] S. V. Buldyrev, R. Parshani, G. Paul, H. Stanley and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature,* vol. 464, pp. 1025-1028, 2010.

[12] Z. Huang and C. Wang, "Characterization of Cascading Failures in Interdependent Cyber-Physical Systems," *IEEE Transactions on Computers,* vol. 64, no. 8, pp. 2158-2168, 2015.

[13] Z. Zuyuan, W. An and S. Fangming, "Cascading Failures on Reliability in Cyber-Physical System," *IEEE Reliability Society,* vol. 65, no. 4, pp. 1745 - 1754, 2016.

[14] C. Heracleous, M. M.Polycarpou, G. Ellinas, C. G.Panayiotou and P. Kolios, "Hybrid systems modeling for critical infrastructures interdependency analysis," *Reliability Engineering & System Safety,* vol. 165, pp. 89-101, 2017.

[15] A. Morozov and K. Janschek, "Probabilistic error propagation model for mechatronic systems," *Mechatronics,* vol. 24, no. 8, pp. 1189-1202, 2014.

[16] A. Morozov and K. Janschek, "Dual Graph Error Propagation Model for Mechatronic System Analysis," *IFAC Proceedings Volumes,* vol. 44, no. 1, pp. 9893-9898, 2011.

[17] L. Grunske and B. Kaiser, "Automatic generation of analyzable failure propagation models from component-level failure annotations," in *Fifth International Conference on Quality Software*, Melbourne, Sep 2005.

[18] Y. Liu, D. Lu, L. Deng, T. Bai, K. Hou and Y. Zeng, "Risk assessment for the cascading failure of electric cyber-physical system considering multiple information factors," *IET Cyber-Physical Systems: Theory & Applications,* vol. 2, no. 4, pp. 155 - 160, 2017.

[19] X. Ge, R. F. Paige and J. A. McDermid, "Probabilistic Failure Propagation and Transformation Analysis," in *28th International Conference on Computer Safety, Reliability, and Security*, Berlin, 2009.
[20] S. Kabir, M. Walker and Y. Papadopoulos, "Dynamic system safety analysis in HiP-HOPS with Petri Nets and Bayesian Networks," *Safety Science,* vol. 105, pp. 55-70, 2018.

آرمان سان احمدی، تحصیلات دانشگاهی خود در مقطع کارشناسی در رشته مهندسی کامپیوتر-نرم‌افزار را در سال ۱۳۹۵ در دانشگاه رازی کرمانشاه و مقطع کارشناسی ارشد خود را در رشته مهندسی کامپیوتر-نرم افزار در سال ۱۳۹۷ در دانشگاه علم و صنعت ایران به پایان رسانده است. زمینه‌های تحقیقاتی مورد علاقه ایشان، مدل‌سازی و ارزیابی سیستم‌های سایبر-فیزیکی و اینترنت اشیاء است. ایشان هم‌اکنون دانشجوی مقطع دکتری مهندسی-کامپیوتر-شبکه و رایانش در دانشکده مهندسی کامپیوتر، دانشگاه علم و صنعت ایران است.

آدرس پست الکترونیکی ایشان عبارت است:
arman_sanahmadi@comp.iust.ac.ir

محمد عبداللهی ازگمی، دانش‌آموخته مقاطع کارشناسی، کارشناسی ارشد و دکتری در رشته مهندسی کامپیوتر-نرم‌افزار (به‌ترتیب در سال‌های ۱۳۷۱، ۱۳۷۵ و ۱۳۸۴) از دانشکده مهندسی کامپیوتر، دانشگاه صنعتی شریف است. زمینه‌های تحقیقاتی مورد علاقه ایشان، مدل‌سازی و ارزیابی سیستم‌های کامپیوتری و سایبری-فیزیکی و امنیت شبکه است. از ایشان تاکنون مقالات متعددی در مجلات و همایش‌های معتبر به چاپ رسیده است. دکتر عبداللهی ازگمی هم‌اکنون دانشیار گروه نرم‌افزار در دانشکده مهندسی کامپیوتر، دانشگاه علم و صنعت ایران است.

آدرس پست الکترونیکی ایشان عبارت است:
azgomi@iust.ac.ir

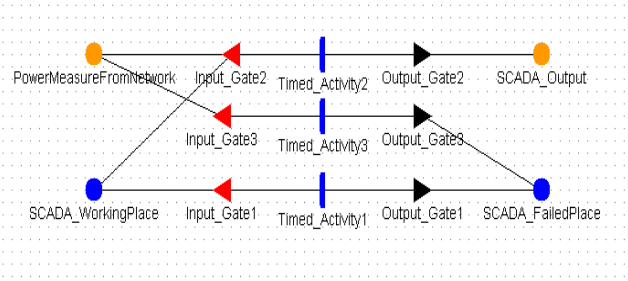
۷- پیوست

در این بخش مدل سایر مؤلفه‌ها آورده شده است.

۷-۱- مؤلفه SCADA

SCADA وظیفه کنترل ایستگاه برق را بر عهده دارد. مدل SAN این مؤلفه در شکل ۱۸ نشان داده شده است.

- **SCADA_WorkingPlace**: وجود یک نشانه داخل این مکان به معنای سالم بودن SCADA است
- **SCADA_FailedPlace**: وجود یک نشانه داخل این مکان به معنای خراب بودن SCADA است
- **SCADA_Output**: دستور کنترلی موردنظر ایستگاه برق داخل این مکان قرار می‌گیرد.
- **PowerMeasureFromNetwork**: وضعیت توزیع برق ایستگاه برق است که از طریق شبکه دریافت شده است. این مکان به دلیل وابستگی داده‌ای بین شبکه و SCADA در این مدل قرار داده شده است.



شکل ۱۸: مدل SAN مؤلفه SCADA

مشخصات دروازه‌های ورودی این مدل به‌صورت زیر است همچنین جدول مربوط به این دروازه‌ها در جدول ۱۳ داده شده است.

- **Input_Gate1**: این دروازه هنگامی اجازه شلیک به فعالیت Time_Activity1 را می‌دهد که SCADA سالم باشد.
- **Input_Gate2**: این دروازه هنگامی اجازه شلیک به فعالیت Time_Activity2 را می‌دهد که مقدار PowerMeasureFromNetwork تغییر کند.
- **Input_Gate3**: این دروازه هنگامی اجازه شلیک به فعالیت Time_Activity3 را می‌دهد که ایستگاه برق دچار خرابی شده باشد.
- مشخصات دروازه‌های خروجی این مدل به‌صورت زیر است. همچنین جداول مربوط به این دروازه‌ها در جدول ۱۴ نشان داده شده است.
- **Output_Gate1**: هنگامی‌که فعالیت Time_Activity1 شلیک کند وضعیت SCADA را به حالت خراب شده تغییر می‌دهد
- **Output_Gate2**: هنگامی‌که فعالیت Time_Activity2 شلیک کند درصورتی‌که SCADA سالم باشد مقدار یک و در غیر این صورت مقدار دو را در خروجی قرار می‌دهد.
- **Output_Gate3**: هنگامی‌که فعالیت Time_Activity3 شلیک کند وضعیت SCADA را به حالت خراب شده تغییر می‌دهد

نرخ خرابی فعالیت‌های این مدل در جدول ۱۵ نشان داده شده است. تمامی نرخ‌ها از توزیع نمایی پیروی می‌کند.

جدول ۱۳: جدول دروازه‌های ورودی مدل مؤلفه SCADA

Input_Gate1	**عبارت شرطی**
	SCADA_WorkingPlace->Mark()==1
	تابع ورودی
	SCADA_WorkingPlace->Mark()=0; SCADA_FailedPlace->Mark()=1;
Input_Gate2	**عبارت شرطی**
	PowerMeasureFromNetwork->Mark() != SCADA_Output->Mark()
	تابع ورودی
	;
Input_Gate3	**عبارت شرطی**
	PowerMeasureFromNetwork->Mark()==2 && SCADA_WorkingPlace->Mark()==1 && SCADA_FailedPlace->Mark()==0
	تابع ورودی
	SCADA_WorkingPlace->Mark()=0;

جدول ۱۴: جدول دروازه‌های ورودی مدل مؤلفه SCADA

Output_Gate1	**تابع خروجی**
	SCADA_FailedPlace->Mark()=1;
Output_Gate2	**تابع خروجی**
	if(SCADA_WorkingPlace->Mark()==1) {SCADA_Output->Mark() = 1;} else if(SCADA_WorkingPlace->Mark()==0) {SCADA_Output->Mark() = 2 ;}
Output_Gate3	**تابع خروجی**
	SCADA_FailedPlace->Mark()=1;

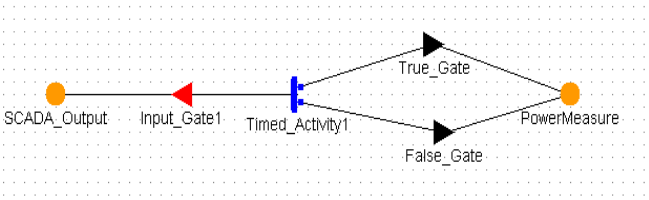
جدول ۱۵: نرخ فعالیت‌های مدل مؤلفه SCADA

نام فعالیت	نرخ شلیک
Time_Activity1	SCADA_FailureRate
Time_Activity2	1
Time_Activity3	0.01

۷-۲- مؤلفه ایستگاه برق

ایستگاه برق وظیفه توزیع برق به سایر مؤلفه‌ها را بر عهده دارد. هنگامی‌که SCADA درست عمل کند و دستورات صحیحی برای ایستگاه برق ارسال کند. ایستگاه برق در ۹۹ درصد مواقع درصد عمل می‌کند. مدل SAN این مؤلفه در شکل ۲۲ نشان داده شده است.

- SCADA_Output: دستورات مربوط به SCADA در این مکان قرار می‌گیرد. وجود این مکان به دلیل وابستگی داده‌ای بین مؤلفه SCADA و ایستگاه برق است.
- PowerMeasure: وضعیت برق توزیع‌شده در این مکان قرار می‌گیرد.
- مشخصات دروازه‌های ورودی این مدل به‌صورت زیر است همچنین جدول مربوط به این دروازه‌ها در جدول ۱۹ نشان داده شده است.
- Input_Gate1: این دروازه در تمامی شرایط اجازه شلیک به فعالیت Time_Activity1 را می‌دهد.



شکل ۱۹: مدل SAN مؤلفه ایستگاه برق

مشخصات دروازه‌های خروجی این مدل به‌صورت زیر است همچنین جدول مربوط به این دروازه‌ها در جدول ۱۷نشان داده شده است.

True_Gate: هنگامی‌که فعالیت Time_Activity1 شلیک کند درصورتی‌که ایستگاه برق درست عمل کند دستور صحیح مربوط به مؤلفه SCADA را انجام می‌دهد.

False_Gate: هنگامی‌که فعالیت Time_Activity1 شلیک کند درصورتی‌که ایستگاه برق سالم باشد مقدار ۲ را به‌صورت اشتباه در خروجی قرار می‌دهد. این اتفاق در یک درصد مواقع رخ خواهد داد.

نرخ خرابی فعالیت‌های این مدل در جدول ۱۸ نشان داده شده است. تمامی نرخ‌ها از توزیع نمایی پیروی می‌کند:

جدول ۱۶: جدول دروازه‌های ورودی مدل مؤلفه ایستگاه برق

Input_Gate1	**عبارت شرطی**
	SCADA_Output->Mark()==1 || SCADA_Output->Mark()==2
	تابع ورودی
	;

جدول ۱۷: جدول دروازه‌های ورودی مدل مؤلفه ایستگاه برق

True_Gate	**تابع خروجی**
	PowerMeasure->Mark() = SCADA_Output->Mark();
False_Gate	**تابع خروجی**
	PowerMeasure->Mark()=2;

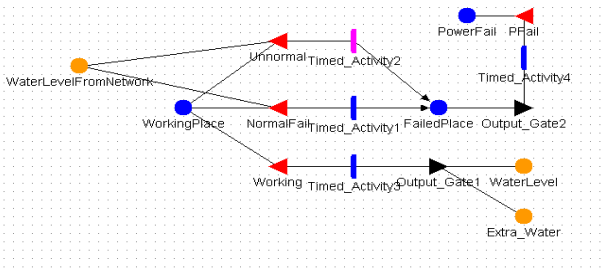
جدول ۱۸: نرخ فعالیت‌های مدل مؤلفه ایستگاه برق

نام فعالیت	نرخ شلیک
Time_Activity1	1

۷-۳- مؤلفه پمپ آب

زیرساخت شبکه به این صورت است که مقدار سطح آب و برق مصرفی را به ترتیب برای پمپ آب و SCADA می‌فرستد. همچنین این مؤلفه توسط مرکز مخابراتی کنترل می‌شود. و درصورتی‌که مرکز مخابراتی دچار اختلال شود این اختلال باعث خرابی این مؤلفه نیز می‌شود. مدل SAN مربوط به این مؤلفه در شکل ۲۰ نشان داده شده است. مکان‌های موجود در این مؤلفه به‌صورت زیر است:

- **PowerMeasure**: این مکان نشان‌دهنده مقدار برق توزیع‌شده است.
- **WorkingPlace**: این مکان نشان‌دهنده سالم بودن پمپ آب است.
- **PowerFail**: این مکان بیان‌گر قطعی برق است.
- **FailedPlace**: این مکان نشان‌دهنده خرابی این مؤلفه است.
- **WaterLevel**: این مکان بیان‌گر سطح آب واقعی داخل مخزن است.
- **Extra_Water**: این مکان نشان‌دهنده آب سرریز شده مخزن است.(وجود این مکان الزامی نیست)
- **WaterLevelFromNetwork**: این مکان نشان‌دهنده سطح آب مخزن است که از مؤلفه شبکه عبور کرده است.
- مشخصات دروازه‌های ورودی این مدل به‌صورت زیر است همچنین جدول مربوط به این دروازه‌ها در جدول ۱۹ نشان داده شده است.
- **Unormal**: این دروازه هنگامی اجازه شلیک به فعالیت Time_Activity2 را می‌دهد مخزن کمتر از نصف ظرفیت خود آب داشته باشد.
- **NormalFail**: این دروازه هنگامی اجازه شلیک به فعالیت Time_Activity1 را می‌دهد مخزن بیشتر از نصف ظرفیت خود آب داشته باشد.
- **Working**: این دروازه هنگامی اجازه شلیک به فعالیت Time_Activity3 را می‌دهد که پمپ آب سالم باشد.
- **PFail**: این دروازه هنگامی اجازه شلیک به فعالیت Time_Activity4 را می‌دهد که برق قطع شده باشد.



شکل ۲۰: مدل SAN پمپ آب

مشخصات دروازه‌های خروجی این مدل به‌صورت زیر است همچنین جدول مربوط به این دروازه‌ها در جدول ۲۰ نشان داده شده است.

Output_Gate2: هنگامی‌که فعالیت Time_Activity4 شلیک کند حالت پمپ آب را خراب شده تنظیم می‌کند.

نرخ خرابی فعالیت‌های این مدل در جدول ۲۱ نشان داده شده است. تمامی نرخ‌ها از توزیع نمایی پیروی می‌کند:

جدول ۱۹: جدول دروازه‌های ورودی مدل مؤلفه پمپ آب

عبارت شرطی	**Unormal**
WaterLevelFromNetwork->Mark()>5 && WorkingPlace->Mark()==1	
تابع ورودی	
WorkingPlace->Mark()=0; FailedPlace->Mark()=1;	
عبارت شرطی	**NormalFail**
WaterLevelFromNetwork->Mark()<=5 && WorkingPlace->Mark()==1	
تابع ورودی	
WorkingPlace->Mark()=0; FailedPlace->Mark()=1;	
عبارت شرطی	**Working**
PowerMeasure->Mark() != PowerMeasureFromNetwork->Mark()	
تابع ورودی	

if(WaterLevel->Mark()==10 &&
WaterLevelFromNetwork->Mark()>5)
{Extra_Water->Mark() = Extra_Water->Mark() + 1;}
else if(WaterLevel->Mark()==10 &&
WaterLevelFromNetwork->Mark()<=5)
{Extra_Water->Mark() = Extra_Water->Mark() + 2;}
else if(WaterLevelFromNetwork->Mark()<10 &&
WaterLevelFromNetwork->Mark()>5){
if(WaterLevelFromNetwork->Mark()<=9)
{WaterLevel->Mark()=WaterLevel->Mark()+1; }
else
{WaterLevel->Mark()=10 ;}
if(waterLevel->Mark()>10){
Extra_Water->Mark() = Extra_Water->Mark() +
WaterLevel->Mark() – 10;
WaterLevel->Mark()=10;}} ;
else if(WaterLevelFromNetwork->Mark()<=5){
if(WaterLevelFromNetwork->Mark()<=8)
WaterLevel->Mark()=WaterLevel->Mark()+2;}
else
{WaterLevel->Mark()=10; }
if(waterLevel->Mark()>10){
Extra_Water->Mark() = Extra_Water->Mark()
+ WaterLevel->Mark() – 10;
WaterLevel->Mark()=10 ;}}	

عبارت شرطی	**PFail**
WorkingPlace->Mark()==1 && FailedPlace->Mark()==0 && PowerFail->Mark()==1	
تابع ورودی	
;	

جدول ۲۰: جدول دروازه‌های خروجی مدل مؤلفه پمپ آب

تابع خروجی	**Output_Gate2**
FailedPlace->Mark()=1; WorkingPlace->Mark()=0;	
تابع خروجی	**Output_Gate1**
;	

جدول ۲۱: نرخ فعالیت‌های مدل مؤلفه پمپ آب

نام فعالیت	نرخ شلیک
Time_Activity1	NormalFailureRate
Time_Activity2	UnNormalFailureRate
Time_Activity3	WorkingRate
Time_Activity4	1

[1] Fault
[2] Error
[3] Fault Propagation
[4] Dependability
[5] Topology
[6] Replication/Join
[7] Stochastic Activity Network
[8] Markov chain
[9] Cluster
[10] Complex Network
[11] Cyber-Physical Systems
[12] failure *propagation* and transformation analysis
[13] Extended Place
[14] Supervisory Control and Data Acquisition

The CSI Journal on Computing Science and Information Technology

The CSI Journal on
Computing Science and
Information Technology
Vol. 17, No.2, 2020

Quantitative Evaluation of Fault Propagation Measures among the Components of Hybrid Systems

Arman Sanahmadi, Mohammad Abdollahi Azgomi

School of Computer Engineering, Iran University of Science and Technology, Tehran, Iran.

Abstract

Todays, hybrid systems are widely used in various fields such as autonomous cars, industrial plants, health control utilities and so on. Due to the critical applications of these systems, the occurrence of faults in one part of the system can propagate to other parts and cause significant damages. Hybrid systems consist of two continuous and discrete parts. These parts work together to achieve the system goal. A fault in either physical or cyber part can disrupt the overall operation of the system. In this paper, a method for modeling fault propagation for these systems is presented. This modeling method can be used to inject faults in various parts of the system to identify the critical points of the system, the component failure behavior and the effect of a fault on other components of the system. The proposed model helps to reduce the costs of system construction and identifying system weaknesses. To evaluate the proposed model, it is applied to a critical infrastructure consisting of three different layers, the results of which are presented in this paper.

Keywords: Modeling, fault propagation, hybrid systems, stochastic activity networks (SANs), quantitative evaluation.