



دانشگاه تهران
پردیس دانشکده‌های فنی
دانشکده مهندسی برق و کامپیوتر



توضیح خطا در شبکه‌های مبتنی بر نرم‌افزار با استفاده از استدلال مبتنی بر علیت

پایان‌نامه برای دریافت درجه کارشناسی ارشد در رشته مهندسی کامپیوتر
گرایش نرم‌افزار

امیرحسین صیحانی

اساتید راهنما

دکتر حسین حجت و دکتر محمدرضا موسوی

شهریور ۱۴۰۱

چکیده

واژگان کلیدی

فهرست مطالب

۳	فصل ۱: مقدمه
۳	۱.۱ موضوع پژوهش
۵	۲.۱ اهداف پژوهش
۵	۳.۱ ساختار فصل‌ها
۷	فصل ۲: تعاریف و دانش پیش‌زمینه
۷	۱.۲ مقدمه
۷	۲.۲ شبکه‌های مبتنی بر نرم‌افزار
۸	۳.۲ نت‌کت
۸	۱.۳.۲ دستور زبان نت‌کت
۹	۲.۳.۲ مدل معنایی نت‌کت
۱۲	۳.۳.۲ توصیف رفتار شبکه با نت‌کت
۱۴	۴.۳.۲ درستی‌سنجی برنامه‌های نت‌کت
۱۵	۴.۲ نت‌کت پویا
۱۵	۱.۴.۲ دستور زبان نت‌کت پویا
۱۶	۲.۴.۲ معنای عملیاتی نت‌کت پویا
۱۸	۳.۴.۲ توصیف برنامه‌ها در نت‌کت پویا
۲۰	۵.۲ ساختمان رویداد
۲۲	۶.۲ مدل علی
۲۵	۱.۶.۲ علت واقعی

۲۷	۲.۶.۲	پیدا کردن علت واقعی در مسائل
۲۸	۳.۶.۲	مدل تعمیم‌یافته
۲۹	۴.۶.۲	علت واقعی بدون شرط
۳۱	فصل ۳:	مروری بر کارهای پیشین
۳۱	۱.۳	تخمین پوشش
۳۲	۲.۳	علت خطا در مثال نقض
۳۳	۳.۳	چک کردن علیت
۳۴	۴.۳	علت واقعی در خودکاره‌های زمان‌دار
۳۴	۵.۳	چارچوب علیت بر اساس رد سیستم
۳۵	۶.۳	استدلال مبتنی بر علیت در HML
۳۶	۷.۳	جمع‌بندی
۳۷	فصل ۴:	روش و راه‌حل پیشنهادی
۳۷	۱.۴	مقدمه
۳۷	۲.۴	مدل معنایی عبارات نکت پویا در قالب ساختمان رویداد
۴۱	۱.۲.۴	معنای عبارات نکت پویای نرمال
۴۲	۳.۴	مدل علی برای ساختمان رویداد
۴۵	۴.۴	پیدا کردن علت خطا در نکت پویا
۴۷	مراجع	
سوم	واژه‌نامه فارسی به انگلیسی	
پنجم	واژه‌نامه انگلیسی به فارسی	

فهرست کارهای باقیمانده

فصل ۱

مقدمه

در این فصل به صورت اجمالی به موضوع و اهداف مورد انتظار این پژوهش پرداخته می‌شود و ساختار و محتوای فصول این نوشتار توضیح داده می‌شود.

۱.۱ موضوع پژوهش

شبکه‌های کامپیوتری یکی از مهم‌ترین اجزای زیرساخت سیستم‌های کامپیوتری هستند [۸]. شبکه‌های مبتنی بر نرم‌افزار^۱ با متمرکز کردن رفتار کنترل‌کننده‌ی شبکه و ساده‌تر کردن عناصر شبکه در سطح داده^۲ تست و درستی‌سنجی شبکه‌ها را تسهیل کرده‌اند. با این وجود به دلیل اینکه هر شبکه‌ی کامپیوتری ذاتاً یک سیستم توزیع‌شده و ناهمگام^۳ است اطمینان از درستی شبکه‌های مبتنی بر نرم‌افزار همچنان فرآیندی پیچیده و سخت است. اما این همه‌ی ماجرا نیست. درستی‌سنجی^۴ و تست یک شبکه‌ی مبتنی بر نرم‌افزار یا به طور کلی یک نرم‌افزار کامپیوتری قدم اول در فرآیند اشکال‌زدایی^۵ آن است. روش‌های درستی‌سنجی نرم‌افزار در صورتی که سیستم مورد آزمون ویژگی^۶ مورد نظر را برآورده نکند یک مثال نقض^۷ پیدا کرده و کاربر بر می‌گردانند. به جز

¹Software Defined Network

²Data Plane

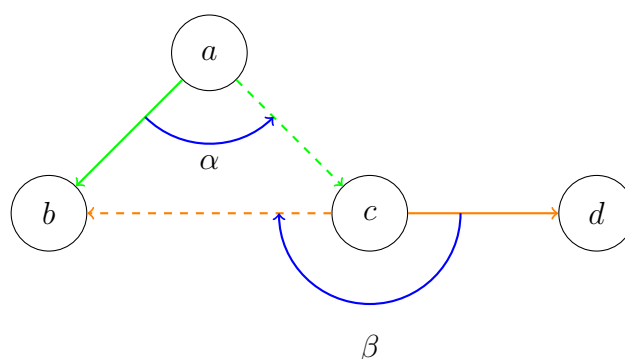
³Asynchronous

⁴Verification

⁵Debug

⁶Property

⁷Counterexample



شکل ۱.۱

این مثال نقض اطلاعات دیگری به کاربر داده نمی‌شود و در نتیجه برای رفع مشکل سیستم کاربر مجبور است تا با روش‌های ابتکاری و با استفاده از دانش و شهود خود در مورد سیستم منشا مشکل را پیدا، آن را برطرف و فرآیند درستی‌سنجی را تکرار کند. انگیزه اصلی این پژوهش جایگزین کردن بخش انسانی این فرآیند با روش‌های خودکار است. در واقع در این پژوهش به دنبال پیدا کردن علت واقعی رخ دادن خطا در یک شبکه‌ی مبتنی بر نرم‌افزار هستیم.

به عنوان مثال شبکه‌ی رسم‌شده در شکل ۱.۱ را در نظر بگیرید. در این شبکه امکان انجام دو به‌روز رسانی α و β وجود دارد که به ترتیب مسیرهای سبز و نارنجی پررنگ را با مسیرهای خط‌چین جایگزین می‌کنند. فرض کنید که ویژگی مورد انتظار در این شبکه نرسیدن بسته^۸ a به d باشد. پس از درستی‌سنجی می‌توان به مثال نقضی برای این ویژگی دست‌یافت که در آن ابتدا به روزرسانی α انجام می‌شود و سپس یک بسته از a به d ارسال می‌شود. این مثال نقض ساده و کوچک است ولی در نگاه اول و بدون بررسی بیشتر کمک چندانی به اشکال‌زدایی این شبکه نمی‌کند. با بررسی بیشتر این شبکه می‌توان دریافت که انجام شدن به روز رسانی α پیش از تکمیل شدن به روز رسانی β سبب به وجود آمدن مسیر بین a و d و در نتیجه بروز خطا می‌شود. هدف از انجام این پژوهش پیدا کردن چنین عواملی (مثلاً در اینجا ترتیب رخ دادن به‌روز رسانی‌ها) به عنوان علت واقعی رخ دادن خطا است.

^۸Packet

۲.۱ اهداف پژوهش

شبکه‌های مبتنی بر نرم‌افزار به دلیل اینکه ذاتاً توزیع شده و ناهمگام هستند مورد استفاده‌ی خوبی برای پیدا کردن علت واقعی خطا و تسهیل فرآیند رفع اشکال هستند. به همین دلیل در این پژوهش این دامنه از مسائل مورد بررسی قرار گرفته‌اند. برای توصیف این شبکه‌ها از زبان نت‌کت پویا^۹ [۴] استفاده شده است که یک زبان مینیمال و ساده بر پایه‌ی زبان نت‌کت^{۱۰} [۱] که توصیف به‌روز رسانی‌های شبکه و استدلال در مورد چندین بسته موجود در شبکه را فراهم کرده است. هدف اصلی این پژوهش ارائه‌ی یک فرمولاسیون از علت واقعی^{۱۱} بر اساس تعریف ارائه شده در [۱۲] برای برنامه‌های توصیف شده در زبان نت‌کت پویا و بررسی کارایی علت‌های واقعی پیدا شده در فرآیند اشکال‌زدایی از شبکه است.

۳.۱ ساختار فصل‌ها

در فصل دوم تعاریف و دانش پیش‌زمینه‌ی مورد نیاز برای بقیه فصول بیان می‌شود. فصل سوم روش ترجمه‌ی یک برنامه‌ی توصیف شده در زبان نت‌کت پویا به یک مدل علی^{۱۲} بیان می‌شود. فصل چهارم شامل به کارگیری روش ارائه شده در این پژوهش برای پیدا کردن علت خطا در چند دسته از ویژگی‌های رایج در شبکه است. در این فصل بررسی می‌شود که علت واقعی پیدا شده تا چه میزان با شهود موجود از مساله تطابق دارد و این فرمولاسیون تا چه حد موفق عمل می‌کند. فصل پنج شامل جمع‌بندی کارهای انجام شده در این پژوهش و بحث در مورد کاستی‌های آن و کارهای پیش‌رو است. در نهایت در فصل ششم مروری بر کارهای پیشین و مرتبط با این پژوهش انجام شده است.

^۹DyNetKAT

^{۱۰}NetKAT

^{۱۱}Actual Cause

^{۱۲}Causal Model

فصل ۲

تعاریف و دانش پیش زمینه

۱.۲ مقدمه

در این فصل مفاهیم مورد نیاز و استفاده در این پروژه مورد بررسی قرار می گیرند. این فصل شامل ۵ بخش است. ابتدا مفاهیم کلی شبکه های مبتنی بر نرم افزار بررسی می شوند. سپس زبان های نت کت و نت کت پویا که زبان های مورد استفاده در این تحقیق هستند شرح داده می شوند. در ادامه تعاریف اولیه ساختمان رویداد^۱ که به عنوان مدل معنایی در این تحقیق استفاده می شود شرح داده می شود. در بخش آخر مدل علّی^۲ که در این تحقیق برای پیدا کردن علت واقعی خطا مورد استفاده قرار می گیرد توصیف شده است.

۲.۲ شبکه های مبتنی بر نرم افزار

شبکه های کامپیوتری یکی از زیرساخت های حیاتی سیستم های کامپیوتری هستند. با وجود اینکه نیازمندی های این شبکه ها بسیار بیشتر و پیشرفته تر نسبت به گذشته شده است تکنیک ها و متدهای مدیریت و ساخت آنها همچنان مانند گذشته است. این مساله مدیریت آنها را در استفاده های امروزی پیچیده و مستعد خطا می کند. حتی شرکت های بزرگی مانند، Amazon Github یا GoDaddy مرتباً مشکلاتی در شبکه های خود پیدا می کنند

¹Event Structure

²Causal Model

[۸]. شبکه‌های مبتنی بر نرم‌افزار یک پارادایم جدید برای طراحی و پیاده‌سازی شبکه‌های کامپیوتری هستند که علاوه بر اینکه مدیریت و درستی سنجی آن‌ها را با روش‌های اصولی‌تر امکان‌پذیر می‌کنند، انعطاف بالایی هم دارند. به صورت خلاصه در یک شبکه‌ی مبتنی بر نرم‌افزار رفتارهای کنترلی (تغییر و به‌روز رسانی قوانین ارسال^۳) از عناصر شبکه مانند سویچ‌ها یا روترها جدا می‌شوند و توسط یک کنترل‌کننده‌ی مرکزی انجام می‌شوند. به عنوان مثال در زبان OpenFlow [۱۹] رفتار سویچ‌های شبکه تنها توسط تعدادی قانون به شکل تطبیق^۴ و اجرا^۵ توصیف می‌شود. قوانینی به این شکل ابتدا بررسی می‌کنند که بسته با قانون تطابق داشته باشد و اگر تطابق وجود داشت عملیات توصیف شده در قانون اجرا می‌شود. با ساده شدن عناصر شبکه، تمامی به‌روز رسانی‌ها و تغییرهای لازم در شبکه توسط یک کنترل‌کننده مرکزی انجام می‌شود. متمرکز شدن رفتار کنترلی سیستم باعث می‌شود تا استدلال و درستی سنجی در مورد رفتار شبکه آسان‌تر شود.

۳.۲ نتکت

نتکت، یک زبان برای توصیف شبکه‌های مبتنی بر نرم‌افزار است [۱]. این زبان با وجود دستور زبان^۶ ساده‌ای که دارد، بر اساس KAT [۱۶] بنا شده و به همین دلیل یک سیستم معادلاتی صحیح و کامل^۷ دارد. این سیستم معادلاتی کمک می‌کند تا با استفاده از روش‌های جبری و اثبات تساوی برنامه‌های توصیف شده در این زبان بتوان در مورد آن‌ها استدلال کرد.

۱.۳.۲ دستور زبان نتکت

در نتکت هر بسته به عنوان یک نگاشت از یک مجموعه از فیله‌های f_1, f_2, \dots, f_n به اعداد طبیعی با تعداد ارقام ثابت در نظر گرفته می‌شود. آی‌پی^۸ های مبدا و مقصد، نوع بسته، پورت^۹ های مبدا و مقصد مثال‌هایی از

³Forwarding Rule

⁴Match

⁵Action

⁶Syntax

⁷Sound and Complete

⁸IP

⁹Port

این فیلدها هستند. دستور زبان نت‌کت به صورت زیر تعریف می‌شود:

$$a, b ::= 1 \mid 0 \mid f = n \mid a + b \mid a \cdot b \mid \neg a$$

$$p, q ::= a \mid f \leftarrow n \mid p + q \mid p \cdot q \mid p^* \mid dup$$

در این گرامر عبارت‌های a, b عملاً معادل با تست‌های زبان کت^{۱۰} هستند. عبارت‌های p, q عبارت‌های نت‌کت را تعریف می‌کنند که نسبت به دستور زبان کت جمله‌هایی به شکل $f \leftarrow n$ و dup به آن اضافه شده است.

۲.۳.۲ مدل معنایی نت‌کت

برای اینکه امکان استدلال در مورد مسیرهای طی شده توسط یک بسته در شبکه وجود داشته باشد، از مفهومی به نام تاریخچه‌ی بسته^{۱۱} استفاده می‌شود. هر تاریخچه‌ی بسته، یک دنباله از بسته‌ها است که بسته نخست دنباله، به عنوان بسته‌ی فعلی در نظر گرفته می‌شود. به صورت شهودی عبارت‌های ۱ و ۰ به ترتیب به معنای ارسال^{۱۲} و رها کردن^{۱۳} بدون شرط بسته هستند. عبارت $f = n$ در صورتی بسته را عبور می‌دهد که مقدار فیلد f آن برابر با n باشد. عبارت $f \leftarrow n$ مقدار n را به فیلد f بسته اختصاص می‌دهد. عبارت‌های dup باعث می‌شوند تا یک کپی از بسته‌ی فعلی ایجاد شود و به تاریخچه‌ی بسته‌ها اضافه شود. این عبارات در رفتار شبکه تأثیری ندارند اما امکان استدلال در مورد تمامی تغییرات ایجاد شده در حین جابه‌جایی بسته در شبکه را فراهم می‌سازند. به صورت دقیق،

¹⁰KAT

¹¹Packet History

¹²Forward

¹³Drop

معنای هر عبارت^{۱۴} نتکت با استفاده از معادلات زیر تعریف می شود:

$$\llbracket p \rrbracket H \in \mathcal{P}(H) \quad (۱.۲)$$

$$\llbracket 1 \rrbracket h \triangleq \{h\} \quad (۲.۲)$$

$$\llbracket 0 \rrbracket h \triangleq \{\} \quad (۳.۲)$$

$$\llbracket f = n \rrbracket (pk :: h) \triangleq \begin{cases} \{pk :: h\} & \text{if } pk.f = n \\ \{\} & \text{otherwise} \end{cases} \quad (۴.۲)$$

$$\llbracket \neg a \rrbracket \triangleq \{h\} \setminus (\llbracket a \rrbracket h) \quad (۵.۲)$$

$$\{f \leftarrow n\}(pk :: h) \triangleq \{pk[f := n] :: h\} \quad (۶.۲)$$

$$\llbracket p + q \rrbracket h \triangleq \llbracket p \rrbracket h \cup \llbracket q \rrbracket h \quad (۷.۲)$$

$$\llbracket p \cdot q \rrbracket h \triangleq (\llbracket p \rrbracket \bullet \llbracket q \rrbracket)h \quad (۸.۲)$$

$$\llbracket p^* \rrbracket h \triangleq \bigcup_{i \in \mathbb{N}} F^i h \quad (۹.۲)$$

$$F^0 h \triangleq \{h\} \quad (۱۰.۲)$$

$$F^{i+1} h \triangleq (\llbracket p \rrbracket \bullet F^i)h \quad (۱۱.۲)$$

$$(f \bullet g)x \triangleq \bigcup \{g(y) \mid y \in f(x)\} \quad (۱۲.۲)$$

$$\llbracket dup \rrbracket (pk :: h) \triangleq \{pk :: (pk :: h)\} \quad (۱۳.۲)$$

در معادلات بالا فرض می شود که H مجموعه‌ی تمامی تاریخچه‌های ممکن است. معادله‌ی ۱.۲ بیان می کند که معنی هر عبارت نتکت روی یک تاریخچه‌ی بسته یک مجموعه از تاریخچه‌ی بسته‌های حاصل از اعمال این عبارت روی تاریخچه‌ی ورودی است. معادله‌ی ۲.۲ بیان می کند که عبارت ۱ بسته را بدون شرط عبور می دهد. در مقابل معادله‌ی ۳.۲ رها شدن بسته را با خروجی یک مجموعه‌ی خالی مدل می کند. معادله‌ی ۴.۲ بسته‌ی نخست ورودی را بررسی می کند و اگر مطابق با عبارت نبود بسته رها می شود. معادله‌ی ۶.۲ مقدار n را به فیلد

¹⁴Expression

f بسته‌ی نخست تاریخچه اختصاص می‌دهد. در معادله‌ی ۹.۲ حاصل اپراتور ستاره‌ی کلین^{۱۵} معادل با اجتماع اعمال عبارت به تعداد دلخواه روی تاریخچه‌ی ورودی در نظر گرفته شده است. در نهایت معادله‌ی ۱۳.۲ یک کپی از بسته‌ی نخست ورودی را به ابتدای خروجی اضافه می‌کند.

نکته علاوه بر اصول موضوعه‌ی KAT^{۱۶} اصول موضوعه‌ی زیر را هم شامل می‌شود تا دستگاه معادلاتی صحیح و کامل^{۱۷} داشته باشد:

$$f \leftarrow n \cdot f' \leftarrow n' \equiv f' \leftarrow n' \cdot f \leftarrow n, \text{ if } f \neq f' \quad (۱۴.۲)$$

$$f \leftarrow n \cdot f' = n' \equiv f' = n' \cdot f \leftarrow n, \text{ if } f \neq f' \quad (۱۵.۲)$$

$$\text{dup} \cdot f = n \equiv f = n \cdot \text{dup} \quad (۱۶.۲)$$

$$f \leftarrow n \cdot f = n \equiv f \leftarrow n \quad (۱۷.۲)$$

$$f = n \cdot f \leftarrow n \equiv f = n \quad (۱۸.۲)$$

$$f \leftarrow n \cdot f \leftarrow n' \equiv f \leftarrow n' \quad (۱۹.۲)$$

$$f = n \cdot f = n' \equiv 0, \text{ if } n \neq n' \quad (۲۰.۲)$$

$$\sum_i f = i \equiv 1 \quad (۲۱.۲)$$

اصل‌های ۱۴.۲، ۱۵.۲، ۱۶.۲ خواص جابه‌جایی^{۱۸} عملیات‌ها را بیان می‌کنند. اصل ۱۷.۲ بیان می‌کند که اختصاص مقدار n به یک فیلد و سپس فیلتر کردن بر روی این فیلد با همین مقدار معادل با عملیات اختصاص^{۱۹} به تنهایی است. مشابه همین اصل برای یک فیلتر و سپس یک اختصاص هم در اصل ۱۸.۲ مشخص شده. اصل ۱۹.۲ بیان می‌کند که در دنباله‌ای از اختصاص مقادیر به یک فیلد مشخص، تنها آخرین اختصاص تاثیر دارد. در اصل ۲۰.۲ مشخص شده است که مقدار یک فیلد نمی‌تواند دو مقدار متفاوت داشته باشد. در نهایت اصل ۲۱.۲ بیان می‌کند که عملیات مجموع فیلترها به ازای هر مقدار ممکن برای یک فیلد مشخص برابر عنصر همانی^{۲۰} است.

¹⁵Kleene Star

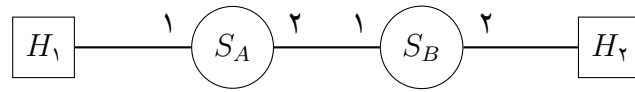
¹⁶Axiom

¹⁷Sound and Complete

¹⁸Commutative

¹⁹Assignment

²⁰Identity



شکل ۱.۲: مثال شبکه

۳.۳.۲ توصیف رفتار شبکه با نت‌کت

در ادامه نحوه‌ی توصیف یک شبکه با استفاده از نت‌کت بیان می‌شود. در شکل ۱.۲ شبکه شامل دو سویچ ۲۱ و A و B و دو هاست ۲۲ می‌باشد. هر سویچ دو پورت دارد که با شماره‌های ۱ و ۲ مشخص شده‌اند. در این شبکه هدف این است که امکان جابه‌جایی همه‌ی بسته‌ها به غیر از بسته‌هایی که از نوع SSH هستند وجود داشته باشد. عبارت نت‌کت زیر را در نظر بگیرید:

$$p \triangleq (dst = H_1 \cdot pt \leftarrow 1) + (dst = H_2 \cdot pt \leftarrow 2)$$

این عبارت همه‌ی بسته‌هایی که مقصد آن‌ها هاست ۱ باشد را به پورت ۱ و همه‌ی بسته‌هایی که مقصد آن‌ها هاست ۲ باشد را به پورت شماره‌ی ۲ می‌فرستد. این سیاست ۲۳ به سادگی رفتار سویچ‌ها را در نت‌کت تعریف می‌کند. در ادامه می‌توان با اضافه کردن یک فیلتر به این عبارت، ویژگی دسترسی کنترل ۲۴ را به این سیاست اضافه کرد تا همه‌ی بسته‌های از نوع SSH رها شوند:

$$p_{AC} \triangleq \neg(typ = SSH) \cdot p$$

اما استفاده از عبارت بالا به تنهایی برای توصیف رفتار شبکه شکل ۱.۲ کافی نیست. برای تکمیل این عبارت لازم است تا رفتار توپولوژی ۲۵ شبکه هم به آن افزوده شود. در نت‌کت توپولوژی شبکه به عنوان یک گراف جهت‌دار در نظر گرفته می‌شود و رفتار آن در قالب اجتماع رفتار هر یک از پیوندهای ۲۶ آن توصیف می‌شود. برای شبکه‌ی

²¹Switch

²²Host

²³Policy

²⁴Access Control

²⁵Topology

²⁶Link

شکل ۱.۲ می‌توان از عبارت زیر برای توصیف توپولوژی شبکه استفاده کرد:

$$\begin{aligned} t \triangleq & (sw = A \cdot pt = 2 \cdot sw \leftarrow B \cdot pt \leftarrow 1) + \\ & (sw = b \cdot pt = 1 \cdot sw \leftarrow A \cdot pt \leftarrow 2) + \\ & (sw = b \cdot pt = 2) \end{aligned}$$

در نکت در صورتی که سیاست و توپولوژی شبکه در قالب عبارت‌هایی توصیف شده باشند، رفتار کل شبکه در واقع دنباله‌ای از اعمال این عبارت‌ها به صورت یکی در میان است. به عنوان مثال در شکل ۱.۲ یک بسته از هاست ۱ ابتدا توسط سویچ A پردازش شده، سپس روی لینک بین دو سویچ جا به جا می‌شود و در نهایت توسط سویچ B پردازش می‌شود. در نکت می‌توان این رفتار را به صورت $p_{AC} \cdot t \cdot p_{AC}$ توصیف کرد. با استفاده از همین شهود، رفتار کل شبکه را می‌توان در قالب عبارت زیر توصیف کرد:

$$(p_{AC} \cdot t)^*$$

در توصیف بالا فرض شده است که بسته‌ها می‌توانند به هر طریق ممکن وارد شبکه و از آن خارج شوند، اما این رفتار همیشه مورد قبول نیست. به عنوان مثال در شبکه شکل ۱.۲ اگر مکان‌های ورودی و خروجی شبکه را در قالب عبارت زیر توصیف کنیم:

$$e \triangleq sw = A \cdot port = 1 \vee sw = B \cdot port = 2$$

می‌توانیم رفتار انتها به انتهای^{۲۷} شبکه را به شکل زیر توصیف کنیم:

$$p_{net} \triangleq e \cdot (p_{AC} \cdot t)^* e$$

در حالت کلی‌تر، نیازی به توصیف ورودی و خروجی‌های شبکه در قالب یک عبارت نیست. پس اگر فرض شود که مکان‌های ورودی شبکه توسط عبارت in و مکان‌های خروجی شبکه در قالب عبارت out توصیف شده باشند،

²⁷End to End

رفتار یک شبکه در نت کت به صورت زیر تعریف می شود:

$$in \cdot (p \cdot t)^* \cdot out$$

که عبارت p سیاست شبکه و عبارت t توپولوژی شبکه است.

۴.۳.۲ درستی سنجی برنامه‌های نت کت

درستی سنجی یک شبکه و بررسی خواص آن در نت کت با استفاده از بررسی تساوی عبارت یک شبکه با عبارت‌های دیگر انجام می شود. به عنوان مثال در شبکه‌ی شکل ۱.۲ برای بررسی اینکه همه‌ی بسته‌ها با نوع SSH از هاست ۱ رها می شوند کافی است تا تساوی زیر را ثابت کنیم:

$$\left(\begin{array}{l} type = SSH \cdot sw = A \cdot pt = 1 \cdot \\ (p_{AC} \cdot t)^* \cdot \\ sw = B \cdot pt = 2 \end{array} \right) \equiv 0$$

از طرفی برای بررسی یک خاصیت در شبکه، مثلاً امکان فرستاده شدن همه‌ی بسته‌هایی که از نوع SSH نیستند از هاست ۱ به هاست ۲ می توان به جای بررسی تساوی دو عبارت از نامساوی $p \leq q$ استفاده کرد. این نامساوی که خلاصه شده‌ی تساوی $p + q \equiv q$ است بیان می کند که رفتار عبارت p بخشی از رفتار عبارت q است. بنابراین برای بررسی این مساله که شبکه‌ی شکل ۱.۲ بسته‌های غیر SSH از هاست ۱ را عبور می دهد کافی است تا درستی نامعادله‌ی زیر را بررسی کرد:

$$\left(\begin{array}{l} \neg (type = SSH) \cdot sw = A \cdot pt = 1 \cdot \\ sw \leftarrow B \cdot pt \leftarrow 2 \end{array} \right) \leq (p_{AC} \cdot t)^*$$

۴.۲ نتکت پویا

نتکت پویا^{۲۸} برای رفع برخی از کاستی‌های نتکت ارائه شده است [۴]. به صورت دقیق‌تر نتکت پویا، امکان توصیف به‌روزرسانی سیاست‌های شبکه و همچنین رفتار شبکه در مقابل چندین بسته را ممکن می‌سازد.

۱.۴.۲ دستور زبان نتکت پویا

در نتکت پویا، از رفتار انتها به انتها^{۲۹} ی توصیف‌های شبکه در قالب عبارات‌های نتکت استفاده می‌شود. به این معنا که در نتکت پویا تنها خروجی حاصل از اعمال عبارات نتکت روی بسته‌ها اهمیت دارد و مسیری که طی شده است در نظر گرفته نمی‌شود. به همین منظور دستور زبان نتکت پویا به صورت زیر تعریف می‌شود:

$$N ::= \text{NetKAT}^{-dup}$$

$$D ::= \perp | N; D | x?N; D | x!N; D | D \parallel DD \oplus D | X$$

$$X \triangleq D$$

در سینتکس بالا NetKAT^{-dup} قسمتی از زبان نتکت است که عبارات‌های dup از آن حذف شده است. عبارات‌های dup در توصیف‌های نتکت تأثیری در رفتار یک عبارت ندارند و هدف از استفاده از آن‌ها ثبت یک اثر از هر بسته پس از پردازش توسط یکی از عناصر شبکه است و امکان استدلال بر روی رفتار شبکه را ممکن می‌سازد. با توجه به این که در نتکت پویا رفتار انتها به انتهای یک عبارت نتکت مورد استفاده است، عبارت dup از دستور زبان کنار گذاشته شده است. نتکت پویا یک لیست از بسته‌های ورودی را پردازش می‌کند و یک لیست از مجموعه‌ی بسته‌های خروجی تولید می‌کند. اپراتور ترکیب متوالی^{۳۰} $N; D$ باعث می‌شود که یک بسته از لیست بسته‌های ورودی توسط سیاست N پردازش شود و سپس بسته‌ی توسط عبارت D پردازش شود. در نتکت پویا امکان ارتباط توسط عبارات‌هایی به شکل $x!N$ و $x?N$ توصیف می‌شوند که به ترتیب ارسال و دریافت یک عبارت نتکت را روی کانال x توصیف می‌کنند. ترکیب موازی^{۳۱} دو عبارت توسط $D \parallel D$ توصیف

²⁸DyNetKAT

²⁹End to End

³⁰Sequential Composition

³¹Parallel Composition

می‌شود. در نهایت رفتارهای غیرقطعی^{۳۲} توسط عبارت‌هایی به شکل $D \oplus D$ توصیف می‌شوند.

۲.۴.۲ معنای عملیاتی نکت پویا

معنای عملیاتی^{۳۳} نکت پویا با استفاده از عبارت‌هایی به شکل (d, H, H') تعریف می‌شوند که d عبارت نکت پویا فعلی است، H لیست بسته‌هایی که در ادامه باید پردازش شوند و H' لیست بسته‌هایی است که به صورت موفقیت‌آمیز توسط شبکه پردازش شده‌اند. در اینجا فرض می‌شود که $F = \{f_1, \dots, f_n\}$ یک مجموعه از فیلدهای بسته‌ها است. یک بسته به شکل یک تابع $F \rightarrow \mathbb{N}$ توصیف می‌شود. برای یک بسته مانند σ تساوی $\sigma(f_i) = v_i$ بیان می‌کند که مقدار فیلد f_i در بسته‌ی σ برابر با v_i است. یک لیست خالی از بسته‌ها با $\langle \rangle$ نمایش داده می‌شود. اگر l یک لیست از بسته‌ها باشد $l :: e$ لیستی است که حاصل از اضافه کردن بسته e به ابتدای لیست به دست می‌آید. برچسب هر قانون که با γ مشخص می‌شود به صورت یکی از شکل‌های $x!q, x?q, (\sigma, \sigma')$ یا $rcfg(x, q)$ تعریف می‌شود که $rcfg(x, q)$ به معنی انجام شدن $x!q$ و $x?q$ به صورت همگام^{۳۴} است. قوانین

³²Non-Deterministic

³³Operational Semantics

³⁴Synchronized

زیر معنای عملیاتی نتکت پویا را تعریف می‌کنند:

$$(cpol_{\neg}^{\gamma}) \frac{\sigma' \in \llbracket p \rrbracket (\sigma :: \langle \rangle)}{(p; q, \sigma :: H, H') \xrightarrow{(\sigma, \sigma')} (q, H, \sigma' :: H')} \quad (22.2)$$

$$(cpol_X) \frac{(p, H_0, H_1) \xrightarrow{\gamma} (p', H'_0, H'_1)}{(X, H_0, H_1) \xrightarrow{\gamma} (p', H'_0, H'_1)} X \triangleq p \quad (23.2)$$

$$(cpol_{\oplus}) \frac{(p, H_0, H'_0) \xrightarrow{\gamma} (p', H_1, H'_1)}{(p \oplus q, H_0, H'_0) \xrightarrow{\gamma} (p', H_1, H'_1)} \quad (24.2)$$

$$(cpol_{\oplus-}) \frac{(q, H_0, H'_0) \xrightarrow{\gamma} (q', H_1, H'_1)}{(p \oplus q, H_0, H'_0) \xrightarrow{\gamma} (p', H_1, H'_1)} \quad (25.2)$$

$$(cpol_{\parallel}) \frac{(p, H_0, H'_0) \xrightarrow{\gamma} (p', H_1, H'_1)}{(p \parallel q, H_0, H'_0) \xrightarrow{\gamma} (p' \parallel q, H_1, H'_1)} \quad (26.2)$$

$$(cpol_{\parallel-}) \frac{(q, H_0, H'_0) \xrightarrow{\gamma} (q', H_1, H'_1)}{(p \parallel q, H_0, H'_0) \xrightarrow{\gamma} (p \parallel q', H_1, H'_1)} \quad (27.2)$$

$$(cpol_{?}) \frac{}{(x?p; q, H, H') \xrightarrow{x?p} (q, H, H')} \quad (28.2)$$

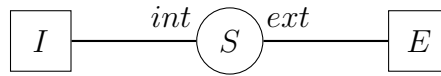
$$(cpol_{!}) \frac{}{(x!p; q, H, H') \xrightarrow{x!p} (q, H, H')} \quad (29.2)$$

$$(cpol_{!?}) \frac{(q, H, H') \xrightarrow{x!p} (q', H, H') (s, H, H') \xrightarrow{x?p} (s', H, H')}{(q \parallel, H, H') \xrightarrow{rcfg(x,p)} (q' \parallel s', H, H')} \quad (30.2)$$

$$(cpol_{?!}) \frac{(q, H, H') \xrightarrow{x?p} (q', H, H') (s, H, H') \xrightarrow{x!p} (s', H, H')}{(q \parallel, H, H') \xrightarrow{rcfg(x,p)} (q' \parallel s', H, H')} \quad (31.2)$$

قانون ۲۲.۲ انجام یک عملیات مانند (σ, σ') که به معنای پردازش بسته‌ی ابتدایی لیست ورودی توسط عبارت p و افزودن خروجی حاصل از آن مانند σ' به لیست خروجی است را مشخص می‌کند. قانون ۲۳.۲ بیان می‌کند که رفتار متغیر X که برابر با عبارت p است معادل با رفتار عبارت p است. قوانین ۲۴.۲ و ۲۵.۲ رفتار غیرقطعی را توصیف می‌کنند. قوانین ۲۶.۲ و ۲۷.۲ رفتار دو عبارت موازی را توصیف می‌کنند. قوانین ۲۸.۲ و ۲۹.۲ مشخص می‌کنند که ارسال یا دریافت پیام در نتکت پویا پردازشی روی بسته‌ها انجام نمی‌دهد. در نهایت همگام‌سازی^{۳۵} ارسال و دریافت پیام توسط قوانین ۲۸.۲ و ۲۹.۲ توصیف شده است.

³⁵Synchronization



شکل ۲.۲: مثال دیوار آتش

۳.۴.۲ توصیف برنامه‌ها در نکت پویا

در ادامه چگونگی توصیف یک دیوار آتش^{۳۶} وابسته به حالت^{۳۷} با استفاده از نکت پویا بیان می‌شود. شبکه‌ی شکل ۲.۲ را در نظر بگیرید. در این شبکه هدف این است که امکان ارتباط از داخل شبکه به بیرون فراهم باشد ولی امکان ارسال بسته از خارج شبکه ممکن نباشد. اما زمانی که یک بسته به خارج شبکه ارسال شد، دیوار آتش باید اجازه‌ی عبور بسته‌ها از بیرون را بدهد تا پاسخ بسته‌ها دریافت شوند. برای توصیف این شبکه می‌توان از عبارت نکت پویای زیر استفاده کرد:

$$Host \triangleq secConReq!1; Host \oplus secConEnd!1; Host$$

$$Switch \triangleq (port = int) \cdot (port \leftarrow ext); Switch \oplus$$

$$(port = ext) \cdot 0; Switch \oplus$$

$$secConReq?1; Switch'$$

$$Switch' \triangleq (port = int) \cdot (port \leftarrow ext); Switch' \oplus$$

$$(port = ext) \cdot (port \leftarrow int); Switch' \oplus$$

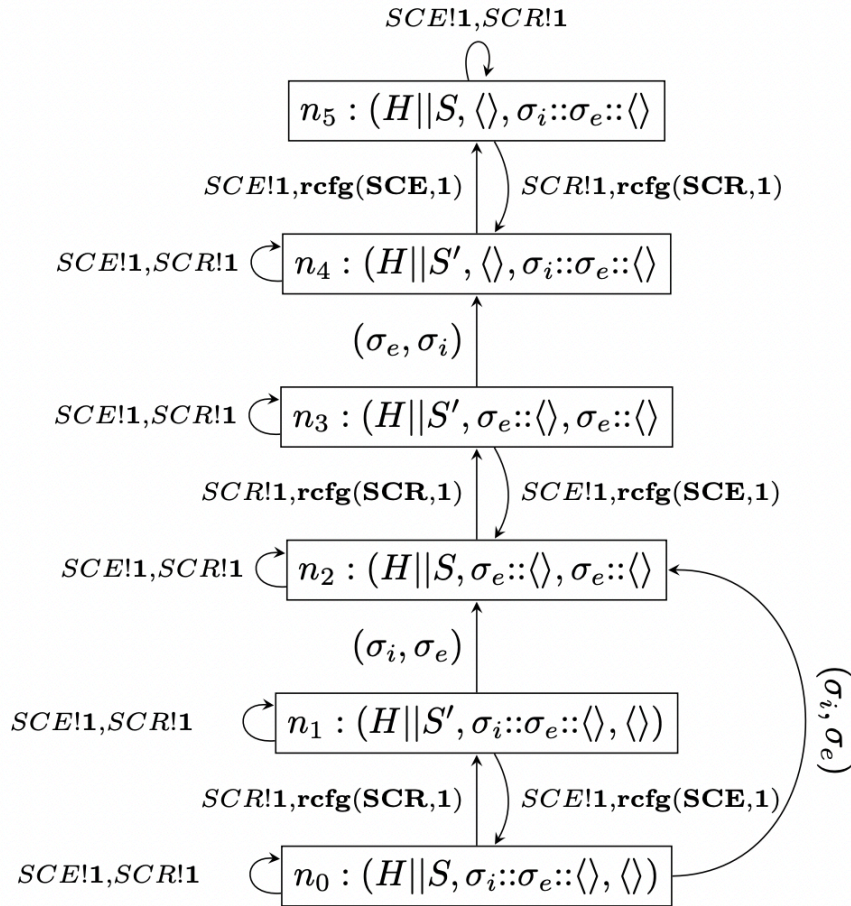
$$secConEnd?1; Switch$$

$$Init \triangleq Host \parallel Switch$$

در این توصیف عملیات $secConReq$ برای شروع ارتباط امن و $secConEnd$ برای خاتمه‌ی ارتباط امن در نظر گرفته شده‌است. بنابراین برنامه‌ی سوییچ پس از دریافت پیام برای شروع ارتباط امن تبدیل به برنامه‌ی $Switch'$ می‌شود که در آن اجازه‌ی ارسال بسته از پورت خارجی به پورت داخلی را می‌دهد. پس از دریافت پیام برای خاتمه‌ی ارتباط امن، برنامه به حالت اولیه‌ی خود بر می‌گردد و دوباره تمامی بسته‌های ورودی از پورت خارجی

^{۳۶}Firewall^{۳۷}Stateful

را رها می‌کند. در نهایت رفتار کل شبکه با استفاده از ترکیب موازی یک هاست و یک سویچ در حالت اولیه خود توصیف می‌شود. نمودار نمایش داده شده در شکل ۳.۲ سیستم انتقال برچسب‌دار^{۳۸} این شبکه را در حالتی



شکل ۳.۲: سیستم انتقال برچسب‌دار برای شبکه‌ی دیوار آتش

که یک بسته روی پورت ورودی و یک بسته روی پورت خروجی شبکه وجود دارد نشان می‌دهد. همانطور که در نمودار مشخص است، عملیات (σ_e, σ_i) که به معنای ارسال بسته از پورت ورودی به پورت خروجی است تنها در قسمتی از این سیستم انتقال قابل دسترسی است که پیش از آن یکی از عملیات‌های $SCR?1$ یا $rcfg(SCR, 1)$ انجام شده باشند. بنابراین در این حالت شبکه تنها در صورتی که بسته خارجی را به داخل ارسال می‌کند که پیش از آن پیام آغاز ارتباط امن دریافت کرده باشد.

³⁸Labeled Transition System

۵.۲ ساختمان رویداد

ساختمان رویداد ^{۳۹}[۲۱] یک مدل محاسباتی ^{۴۰} غیرجای‌گذاری شده ^{۴۱} برای پردازش‌های هم‌روند ^{۴۲} است. در این مدل، برخلاف مدل‌های جای‌گذاری شده ^{۴۳} مانند سیستم انتقال که هم‌روندی پردازش‌های موازی با انتخاب غیرقطعی مدل می‌شود، هم‌روندی پردازش‌ها به صورت صریح در مدل توصیف می‌شوند [۲۰].

تعریف ۱.۵.۲. ساختمان رویداد یک ساختمان رویداد یک سه‌تایی $(E, \#, \vdash)$ است که در آن:

۱. E یک مجموعه از رویدادها است

۲. $\#$ رابطه‌ی تعارض ^{۴۴}، یک رابطه‌ی دودویی متقارن و غیربازتابی بر روی مجموعه‌ی E است

۳. $\vdash \subseteq Con \times E$ رابطه‌ی فعال‌سازی ^{۴۵} است که شرط زیر را برقرار می‌کند:

$$X \vdash e \wedge X \subseteq Y \in Con \Rightarrow Y \vdash e$$

در رابطه‌ی بالا Con زیرمجموعه‌ای از مجموعه‌ی توانی رویدادها است که اعضای آن فاقد تعارض باشند. به صورت دقیق‌تر داریم:

$$Con = \{X \subseteq E \mid \forall e, e' \in X. \neg(e \# e')\}$$

تعریف ۲.۵.۲. به ازای هر ساختمان رویداد، می‌توانیم رابطه‌ی فعال‌سازی مینیمال را به صورت زیر تعریف کنیم:

$$X \vdash_{min} e \iff X \vdash e \wedge (\forall Y \subseteq X. Y \vdash e \Rightarrow Y = X)$$

³⁹Event Structure

⁴⁰Computational Model

⁴¹Non-Interleaving

⁴²Concurrent

⁴³Interleaving

⁴⁴Conflict

⁴⁵Enabling

همچنین در هر ساختمان رویدادی شرط زیر برقرار است:

$$Y \vdash e \Rightarrow \exists X \subseteq Y. X \vdash_{min} e$$

برای مشخص کردن وضعیت یک سیستم در هر لحظه از مفهومی به نام پیکربندی^{۴۶} استفاده می‌شود و و یک مجموعه شامل رویدادهایی است که تا آن لحظه در سیستم رخ داده‌اند.

تعریف ۳.۵.۲. اگر $E = (E, \#, \vdash)$ یک ساختمان رویداد باشد، یک پیکربندی آن یک زیرمجموعه از رویدادها $x \subseteq E$ است که شرایط زیر را داشته باشد:

$$1. x \in Con$$

$$2. \forall e \in x \exists e_0, \dots, e_n \in x. e_n = e \ \& \ \forall i \leq n. \{e_0, \dots, e_{i-1}\} \vdash e_i$$

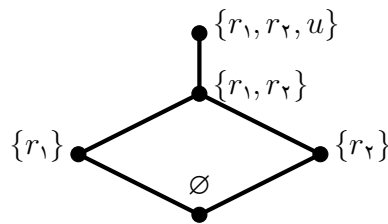
مجموعه‌ی همه‌ی پیکربندی‌های یک ساختمان رویداد مانند E با $\mathcal{F}(E)$ نمایش داده می‌شود. شبکه‌ی موجود در شکل ۵.۲ را در نظر بگیرید. در این شبکه دو هاست ۱ و ۲ به صورت هم‌روند یک بسته را به سویچ ارسال می‌کنند. این بسته‌ها شامل اطلاعات برای به روزرسانی مسیرهای دیگر در شبکه هستند، بنابراین سویچ پس از دریافت هر دوی این بسته‌ها آن‌ها را پردازش کرده و مسیرهای خود را به روزرسانی می‌کند. برای مدل کردن این شبکه می‌توانیم از یک ساختمان رویداد به صورت زیر استفاده کنیم:

$$E = (\{r_1, r_2, u\}, \emptyset, \{(\emptyset, r_1), (\emptyset, r_2), (\{r_1, r_2\}, u)\})$$

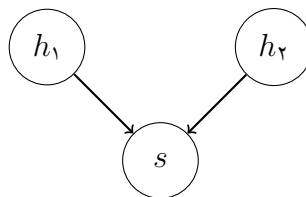
در این ساختمان رویداد، رویدادها به ترتیب دریافت یک بسته از هاست ۱، دریافت یک بسته از هاست ۲ و به روزرسانی سویچ را مدل می‌کنند. یکی از روش‌های رسم نمودار برای ساختمان رویداد، رسم نمودار هس^{۴۷} برای مجموعه‌ی پیکربندی‌های این ساختمان رویداد بر اساس رابطه‌ی زیرمجموعه است. برای مثالی که بیان شد می‌توان نموداری مطابق شکل ۴.۲ را رسم کرد.

⁴⁶ Configuration

⁴⁷ Hasse



شکل ۴.۲



شکل ۵.۲

۶.۲ مدل علی

پیدا کردن تعریفی برای علت واقعی^{۴۸} مبحثی است که مورد مطالعه و تحقیق بسیاری قرار گرفته است. این مساله به طور خاص در متون فلسفه مورد توجه قرار گرفته است. یکی از تعاریف علت واقعی که مورد توجه بسیاری قرار گرفته است، تعریفی مبتنی بر وابستگی خلاف واقع^{۴۹} است. مطابق این تعریف، رویداد الف علت رویداد ب است اگر در شرایطی که رویداد الف اتفاق نیافته باشد، رویداد ب هم اتفاق نیافتند. در اینجا اتفاق نیفتادن رویداد الف خلاف واقع است، چون در سناریوی واقعی (سناریو ای که واقعا اتفاق افتاده و مشاهده شده است) رویداد الف اتفاق افتاده است و در نظر گرفتن شرایطی که در آن رویداد الف اتفاق نیفتاده باشد بر خلاف واقعیت موجود است. اما این مدل به تنهایی امکان پیدا کردن علت مناسب را در همه‌ی موارد ندارد. به عنوان مثال سناریوی زیر را در نظر بگیرید که در آن سارا و بهرام هر کدام یک سنگ را برداشته و به سمت یک بطری شیشه‌ای پرتاب می‌کنند. در این سناریو، سنگ سارا زودتر از سنگ بهرام به بطری برخورد کرده و در نتیجه آن را می‌شکند. در این سناریو واضح است که پرتاب سنگ توسط سارا علت شکسته شدن بطری است. فرض کنید بخواهیم از علیت مبتنی بر خلاف واقع برای پیدا کردن این علت استفاده کنیم. بنابراین باید شرایطی را در نظر بگیریم که سارا سنگ خود را پرتاب نکند. اما مشکل اینجاست که در این شرایط همچنان بطری شکسته می‌شود،

^{۴۸}Actual Cause^{۴۹}Counterfactual

چون اگر سارا سنگ خود را پرتاب نکند، بهرام همچنان سنگ خود را پرتاب می‌کند و در نتیجه این بار سنگ بهرام به بطری برخورد کرده و آن را می‌شکند. بنابراین در این سناریو امکان تعریف پرتاب سنگ توسط سارا به عنوان علت شکسته شدن بطری با استفاده از استدلال مبتنی بر خلاف واقع وجود ندارد. هالپرن^{۵۰} و پزل^{۵۱} برای حل کردن مشکلاتی از این دست، تعریف جدیدی از علت واقعی [۱۲] ارائه کردند. مدل ارائه شده توسط آن‌ها به دلیل اینکه مبنای ریاضی دارد امکان استفاده از آن را در آنالیز و تحلیل سیستم‌های محاسباتی فراهم می‌کند. به همین دلیل این تعریف در مقالات زیادی در حوزه‌ی دانش کامپیوتر مورد استفاده قرار گرفته است. برای تعریف علت واقعی ابتدا برخی مفاهیم اولیه مورد استفاده در این تعریف توضیح داده می‌شوند. به صورت کلی فرض می‌شود که دنیای مورد تحلیل توسط تعدادی متغیر تصادفی مدل شده است. اگر X یک متغیر تصادفی باشد، یک رویداد به شکل $X = x$ تعریف می‌شود. برخی از این متغیرها بر روی یکدیگر تاثیر گذارند. این وابستگی‌ها در قالب مجموعه‌ای از معادلات ساختاری^{۵۲} مدل می‌شوند. هر یک از این معادلات در واقع یک مکانیزم یا قانون مشخص در این دنیا را مدل می‌کنند. متغیرها به دو دسته درونی^{۵۳} و برونی^{۵۴} تقسیم می‌شوند. متغیرهای برونی متغیرهایی در نظر گرفته می‌شوند که مقدار آن‌ها توسط عواملی که درون مدل نیستند تعیین می‌شوند. بنابراین در مدل فرض می‌شود که مقدار این متغیرها از قبل مشخص است. اما متغیرهای درونی متغیرهایی هستند که مقدار آن‌ها بر اساس معادلات ساختاری تعیین می‌شود. به صورت دقیق‌تر، امضای^{۵۵} یک مدل یک سه‌تایی $\mathcal{S} = (\mathcal{U}, \mathcal{V}, \mathcal{R})$ است که در آن \mathcal{U} مجموعه‌ی متغیرهای بیرونی \mathcal{V} مجموعه‌ی متغیرهای درونی و \mathcal{R} دامنه‌ی مقادیر ممکن برای هر یک از متغیرها را مشخص می‌کند. در این مدل فرض می‌شود که مجموعه‌ی متغیرهای درونی محدود است. مدل علی بر روی یک امضای \mathcal{S} یک دوتایی $\mathcal{M} = (\mathcal{S}, \mathcal{F})$ است که در آن \mathcal{F} به هر متغیر داخلی $X \in \mathcal{V}$ یک تابع $F_X : (\times_{U \in \mathcal{U}} \mathcal{R}(U)) \times (\times_{Y \in \mathcal{V} - \{X\}} \mathcal{R}(Y)) \rightarrow \mathcal{R}(X)$ اختصاص می‌دهد. هر تابع، معادله‌ی یک متغیر را به ازای مقادیر تمام متغیرهای دیگر مشخص می‌کند. به عنوان مثال اگر فرض کنیم $F_X(Y, Z, U) = Y + U$ اگر داشته باشیم $U = 2$, $Y = 3$ آنگاه مقدار X برابر ۵ خواهد شد. این معادلات امکان تفسیر آن‌ها بر اساس شرایط خلاف واقع را می‌دهند. به عنوان مثال در همین مدل اگر فرض کنیم که $U = u$ می‌توانیم نتیجه بگیریم که اگر مقدار متغیر Y برابر ۴ باشد آنگاه مستقل از اینکه مقدار بقیه‌ی متغیرها در دنیای واقعی چه مقداری دارند، مقدار

⁵⁰Halpern

⁵¹Pearl

⁵²Structural Equations

⁵³Endogenous

⁵⁴Exogenous

⁵⁵Signature

متغیر X برابر $u + ۴$ خواهد بود که به صورت $(X = u + ۴) \models [Y \leftarrow ۴]$ نوشته می‌شود. توابع ذکر شده فقط برای متغیرهای درونی تعریف می‌شوند و همانطور که پیش‌تر اشاره شد، برای متغیرهای بیرونی تابعی تعریف نمی‌شود و فرض می‌شود که مقدار آن‌ها از قبل مشخص شده است.

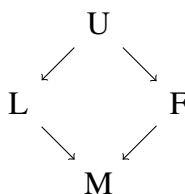
مثال ۱.۶.۲. یک جنگل را در نظر بگیرید که می‌تواند توسط رعد و برق یا یک کبریت رها شده دچار آتش سوزی شود. برای مدل کردن این سناریو از سه متغیر بولی^{۵۶} استفاده می‌کنیم:

- متغیر F که اگر جنگل دچار آتش سوزی شود مقدار آن درست است و در غیر این صورت مقدار آن غلط است
- متغیر L که اگر رعد و برق اتفاق افتاده باشد مقدار آن درست است و در غیر این صورت غلط است
- متغیر M که اگر یک کبریت در جنگل رها شده باشد مقدار آن درست است و در غیر این صورت غلط است

در این مثال فرض می‌کنیم که مقادیر متغیرهای برونی به گونه‌ای است که تمام شرایط لازم برای آتش سوزی جنگل در صورتی که رعد و برق اتفاق بیافتد یا کبریتی در جنگل رها شود را دارد (به عنوان مثال درختان جنگل به اندازه‌ی کافی خشک هستند و اکسیژن کافی در هوا وجود دارد). در این مدل تابع متغیر F را به گونه‌ای تعریف می‌کنیم که داشته باشیم: $F_F(\vec{u}, L, M) = L \vee M$. همانطور که پیش‌تر بیان شد، این مدل علی امکان بررسی معادلات بر اساس شرایط خلاف واقع را می‌دهد. به صورت دقیق‌تر اگر $M = (\mathcal{S}, \mathcal{F})$ یک مدل علی، \vec{X} یک بردار از متغیرهای درونی و \vec{x} برداری از مقادیر متغیرهای \vec{X} باشند مدل $M_{\vec{X} \leftarrow \vec{x}}$ را با امضای $S_{\vec{X}}$ $(\mathcal{U}, \mathcal{V} - \vec{X}, \mathcal{R}|_{-\vec{X}})$ یک زیرمدل^{۵۷} از M تعریف می‌کنیم. به صورت شهودی این مدل حاصل مداخله^{۵۸} ای در مدل M است که در آن مقادیر \vec{x} را به متغیرهای \vec{X} اختصاص داده‌ایم. به صورت دقیق‌تر تعریف می‌کنیم $M_{\vec{X} \leftarrow \vec{x}} = (\mathcal{S}_{\vec{X}}, \mathcal{F}^{\vec{X} \leftarrow \vec{x}})$ که $F_Y^{\vec{X} \leftarrow \vec{x}}$ از تابع F_Y که در آن مقادیر \vec{x} را به متغیرهای \vec{X} اختصاص داده‌ایم به دست می‌آید. به عنوان مثال اگر M مدل مثال ۱.۶.۲ باشد آنگاه در مدل $M_{L \leftarrow F}$ معادله‌ی متغیر F به $F = M$ تبدیل می‌شود. این معادله دیگر به متغیر L وابسته نیست بلکه با توجه به مقدار آن که در اینجا غلط است معادله‌ی جدیدی دارد. علاوه بر این توجه کنید که در مدل $M_{L \leftarrow F}$ دیگر معادله‌ای برای متغیر L وجود ندارد. توجه کنید که

^{۵۶}Boolean^{۵۷}Sub-Model^{۵۸}Intervention

در حالت کلی ممکن است یک بردار یکتا از مقادیر متغیرها برای یک مدل وجود نداشته باشد که همزمان تمامی معادلات را حل کند. در مدل علی یک بردار از مقادیر متغیرهای برونی \vec{u} یک هم‌بافت^{۵۹} نامیده می‌شود. در مدل‌های بازگشتی به ازای یک هم‌بافت مشخص همیشه یک راه‌حل یکتا برای تمامی معادلات مدل وجود دارد. در ادامه فرض می‌شود که مدل‌ها بازگشتی هستند. تعمیم مدل علی برای مدل‌های غیربازگشتی در [۱۲] توضیح داده است. برای یک مدل می‌توان یک شبکه‌ی علی ترسیم کرد. این شبکه یک گراف جهت‌دار است که به ازای هر متغیر یک گره در آن وجود دارد و یک یال بین دو گره وجود دارد اگر تابع متغیر دوم به متغیر اول وابسته باشد. به عنوان مثال شکل زیر شبکه‌ی علی مثال ۱.۶.۲ را نشان می‌دهد:



در ادامه برای سادگی رسم شبکه‌ی علی، متغیرهای برونی را از آن‌ها حذف می‌کنیم.

۱.۶.۲ علت واقعی

در ادامه فرمول‌های لازم برای تعریف علت واقعی توصیف می‌شوند. اگر $\mathcal{S} = (\mathcal{U}, \mathcal{V}, \mathcal{R})$ یک امضا باشد فرمول $X = x$ یک رویداد بدوی^{۶۰} نامیده می‌شود که $X \in \mathcal{V}, x \in \mathcal{R}(X)$. فرمول $[Y_1 \leftarrow y_1, \dots, Y_k \leftarrow y_k] \varphi$ یک فرمول علی پایه^{۶۱} نامیده می‌شود که در آن:

- φ یک ترکیب بولی از رویدادهای بدوی است

- Y_1, \dots, Y_k متغیرهای متمایز در \mathcal{V} هستند

- $y_i \in \mathcal{R}(Y_i)$

این فرمول به صورت خلاصه به شکل $[\vec{Y} \leftarrow \vec{y}] \varphi$ نوشته می‌شود و اگر $k = 0$ باشد آنگاه به صورت φ نوشته می‌شود. به صورت شهودی یک فرمول به شکل $[\vec{Y} \leftarrow \vec{y}] \varphi$ بیان می‌کند که در شرایط خلاف واقع ای که در آن

⁵⁹ Context

⁶⁰ Prime Event

⁶¹ Basic Causal Formula

مقادیر \vec{y} به متغیرهای \vec{Y} اختصاص داده شده است فرمول φ برقرار است. یک فرمول علی به صورت یک ترکیب بولی از فرمول‌های علی پایه تعریف می‌شود. برقراری فرمول علی ψ در مدل M تحت هم‌بافت \vec{u} را به صورت $(M, \vec{u}) \models \psi$ نشان می‌دهیم. به عنوان مثال $(M, \vec{u}) \models [\vec{Y} \leftarrow \vec{y}](X = x)$ برقرار است اگر مقدار متغیر X در راه حل معادلات مدل $M_{\vec{Y} \leftarrow \vec{y}}$ تحت هم‌بافت \vec{u} برابر x باشد.

تعریف ۲.۶.۲. فرمول $\vec{X} = \vec{x}$ علت واقعی φ (که تاثیر ^{۶۲} نامیده می‌شود) در (M, \vec{u}) است اگر شرایط زیر برای آن برقرار باشد:

$$1. (M, \vec{u}) \models (\vec{X} = \vec{x}) \wedge \varphi$$

۲. یک افزاز مانند (\vec{Z}, \vec{W}) از مجموعه متغیرهای \mathcal{V} با شرط $\vec{X} \subseteq \vec{Z}$ و مقادیر (\vec{x}, \vec{w}') برای متغیرهای (\vec{X}, \vec{W}) وجود داشته باشد که داشته باشیم $(M, \vec{u}) \models \vec{Z} = \vec{z}^*$ و شرایط زیر را برآورده کند:

$$(M, \vec{u}) \models [\vec{X} \leftarrow \vec{x}, \vec{W} \leftarrow \vec{w}'] \neg \varphi \quad (1)$$

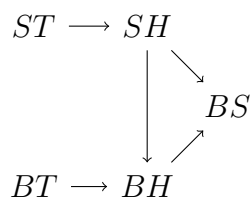
$$(ب) \quad \forall \vec{W}' \subseteq \vec{W}, \vec{Z}' \in \vec{Z}. (M, \vec{u}) \models [\vec{X} \leftarrow \vec{x}, \vec{W}' \leftarrow \vec{w}', \vec{Z}' \leftarrow \vec{z}^*] \varphi$$

۳. \vec{X} مینیمال باشد.

در این تعریف شرط اول بیان می‌کند که علت و تاثیر هر دو در شرایط واقعی برقرار هستند. شرط دوم به دنبال پیدا کردن شرایطی است که تحت آن تاثیر به صورت غیر واقع به علت وابسته باشد. این شرایط متغیرهای \vec{W} و مقادیری مانند \vec{w}' برای آن‌ها هستند. شرط ۲. الف بررسی می‌کند که تحت شرایطی که توسط $\vec{W} \leftarrow \vec{w}'$ به وجود می‌آید اگر علت مقداری متفاوت از مقدار خود در هم‌بافت واقعی داشته باشد اثر در مدل دیده نمی‌شود. شرط ۲. ب بررسی می‌کند که شرایط استفاده شده در ۲. الف عامل از بین رفتن اثر در ۲. الف نباشند. برای این منظور در شرایطی که علت مقدار واقعی خود را دارد در تمامی حالت‌هایی که متغیرهای شرایط می‌توانند داشته باشند بررسی می‌شود که اثر همچنان برقرار باشد. شرط سوم در واقع بیان می‌کند که زیرمجموعه‌ای از علت وجود نداشته باشد که همزمان شرایط ۱ و ۲ را برقرار کند. در تعریف بالا $(\vec{W}, \vec{w}', \vec{x}')$ یک شاهد ^{۶۳} بر اینکه $\vec{X} = \vec{x}$ علت φ است تعریف می‌شود.

⁶²Effect

⁶³Witness



شکل ۶.۲

۲.۶.۲ پیدا کردن علت واقعی در مسائل

در ادامه مثال سارا و بهرام که در ابتدای این بخش ذکر شده بود را بررسی می‌کنیم. برای مدل کردن این مساله متغیرهای زیر را در نظر می‌گیریم:

- BT : پرتاب سنگ توسط بهرام
- BH : برخورد سنگ بهرام به بطری
- ST : پرتاب سنگ توسط سارا
- SH : برخورد سنگ سارا به بطری
- BS : شکسته شدن بطری

ابتدا فرض می‌کنیم که متغیرهای BT, ST تنها به متغیرهای برونی وابسته‌اند. بطری در صورتی شکسته می‌شود که هر یک از سنگ‌های سارا یا بهرام با آن برخورد کنند. بنابراین برای شکسته شدن بطری معادله‌ی $BS = SH \vee BH$ را در نظر می‌گیریم. نکته‌ی اصلی در این مساله این است که سنگ سارا زودتر از سنگ بهرام به شیشه برخورد می‌کند، به همین دلیل لازم است تا این موضوع در مدل لحاظ شود. یک راه برای مدل کردن این مساله این است که معادله‌ی برخورد سنگ بهرام به شیشه را به گونه‌ای تعریف کنیم که تنها در صورتی که سنگ سارا به بطری برخورد نکرده باشد آنگاه سنگ بهرام به بطری برخورد کند. بنابراین می‌توانیم معادله‌ی $BH = BT \wedge \neg SH$ را تعریف کنیم. علاوه بر این معادله‌ی برخورد سنگ سارا را بدون وابستگی به برخورد سنگ بهرام تعریف می‌کنیم: $SH = ST$. با توجه به این تعاریف برای معادلات می‌توانیم گراف علی شکل ۶.۲ را برای این مدل رسم کنیم. در این مدل می‌توانیم $ST = T$ را به عنوان علت $BS = T$ تعریف کنیم. برای برقراری شرط ۲ در تعریف علت واقعی شرایط $\{BT\}$ و $\vec{W} = F$ و $w' = F$ را در نظر می‌گیریم. در این شرایط چون مقدار BH برابر F می‌شود،

مقدار BS تنها وابسته به مقدار SH و در نتیجه ST می‌شود. همچنین در این مدل $BT = T$ علت شکسته شدن شیشه نیست. مثلاً فرض کنید که شرایط $w' = F$, $\bar{W} = \{ST\}$ را در نظر بگیریم. در این شرایط اگر مقدار BT را به F تغییر دهیم مقدار BS هم غلط می‌شود. بنابراین شرط ۲.۱ الف برقرار است. اما به ازای $\bar{Z}' = \{BH\}$ شرط ۲.۲ ب برقرار نمی‌شود. در این حالت داریم: $(M, \bar{u}) \models [BT \leftarrow T, ST \leftarrow F, BH \leftarrow F]BS = F$. توجه کنید با وجود اینکه مقدار درست به BT اختصاص یافته اما چون مقدار BH به مقدار آن در هم‌بافت واقعی برگردانده می‌شود در نتیجه مقدار BS همچنان غلط می‌ماند.

مثال بالا نشان می‌دهد که این تعریف از علت واقعی برخی از مشکلات موجود در تعاریف ساده مبتنی بر خلاف واقع را برطرف می‌کند و می‌تواند توضیح مناسبی در برخی از این مثال‌ها پیدا کند. نکته‌ای که باید به آن توجه شود این است که هنوز روش یا معیاری برای این که چه تعریفی از علت واقعی تعریف مناسب است وجود ندارد. تنها روش ممکن مقایسه تعاریف مختلف استفاده از آن‌ها در مساله‌ها و سناریوهای مختلف و بررسی تطابق علت به دست آمده با استفاده از این تعریف‌ها با شهود موجود از مساله است.

۳.۶.۲ مدل تعمیم‌یافته

مدل علی تعمیم یافته^{۶۴} یک سه‌تایی $(S, \mathcal{F}, \mathcal{E})$ است که (S, \mathcal{F}) یک مدل علی است و \mathcal{E} یک مجموعه از مقداردهی‌های مجاز^{۶۵} برای متغیرهای درونی است. به صورت دقیق‌تر اگر متغیرهای درونی X_1, \dots, X_n باشند آن‌گاه $(x_1, \dots, x_n) \in \mathcal{E}$ اگر $X_1 = x_1, \dots, X_n = x_n$ یک مقداردهی مجاز است. یک مقداردهی دلخواه به یک زیرمجموعه از متغیرهای درونی مجاز است اگر امکان تعمیم به یک مقداردهی مجاز در \mathcal{E} را داشته باشد. هدف از این تعریف جلوگیری از در نظر گرفتن علت‌هایی است که شرایط رخ دادن آن‌ها غیر محتمل است. با توجه به تعریف مقداردهی مجاز، علت واقعی در یک مدل تعمیم یافته به گونه‌ای تعریف می‌شود که در شرط ۲ فقط امکان مقداردهی‌های مجاز وجود داشته باشد. در [۱۲] تعریف دقیق علت واقعی در مدل تعمیم یافته بیان نشده است. در بخش بعدی تعریفی از علت واقعی در مدل تعمیم یافته ارائه می‌شود.

⁶⁴Extended Causal Model

⁶⁵Allowable Settings

۴.۶.۲ علت واقعی بدون شرط

فرض کنید که $\vec{X} = \vec{x}$ یک علت واقعی برای φ در (M, \vec{u}) با استفاده از شاهد $(\emptyset, \emptyset, \vec{x}')$ باشد. با توجه به اینکه در اینجا \vec{W} یک بردار خالی است پس عملاً شرط ۲.ب به بررسی شرط زیر تبدیل می‌شود:

$$\forall \vec{Z}' \in \vec{Z}. (M, \vec{u}) \models [\vec{X} \leftarrow \vec{x}, \vec{Z}' \leftarrow \vec{z}^*] \varphi$$

با دقت در شرط بالا می‌توان دریافت که مقدار متغیرها در فرمول‌های $[\vec{X} \leftarrow \vec{x}, \vec{Z}' \leftarrow \vec{z}^*] \varphi$ با مقدار متغیرها در هم‌بافت اولیه تفاوتی ندارد زیرا مقدار آن‌ها به مقداری که در هم‌بافت اولیه داشته‌اند برگردانده می‌شود. بنابراین در شرط بالا می‌توان نتیجه گرفت:

$$(M, \vec{u}) \models [\vec{X} \leftarrow \vec{x}, \vec{Z}' \leftarrow \vec{z}^*] \varphi \iff (M, \vec{u}) \models \varphi$$

بنابراین شرط ۲.ب معادل با شرط ۱ می‌شود. با توجه به این موضوع می‌توان قضیه زیر را نتیجه گرفت:

گزاره ۳.۶.۲. اگر $\vec{X} = \vec{x}$ در (M, \vec{u}) با شاهی به شکل $(\emptyset, \emptyset, \vec{x}')$ شرط‌های ۱، ۲.الف و ۳ در تعریف ۲.۶.۲ را برای φ برآورده کند آنگاه $\vec{X} = \vec{x}$ یک علت واقعی برای φ در (M, \vec{u}) است.

فصل ۳

مروری بر کارهای پیشین

توضیح خطا^۱ و متمرکز کردن خطا^۲ روش‌هایی هستند که فرآیند رفع ایراد نرم‌افزار را تسهیل می‌کنند. توضیح خطا روش‌هایی را شامل می‌شود که به کاربر کمک می‌کند که با استفاده از یک مثال نقض یا یک دنباله از اجرای سیستم به ماهیت خطا و در نتیجه روش اصلاح خطا پی ببرد. در روش‌های متمرکز کردن خطا هدف مشخص کردن بخشی از سیستم است که عامل خطا بوده و امکان اندازه‌گیری کمی و مقایسه آن با دیگر بخش‌ها وجود دارد [۱۰]. یکی از روش‌های توضیح خطا پیدا کردن علت خطا بر اساس استدلال مبتنی بر خلاف واقع که توسط لوئیس در [۱۸] ارائه شده می‌باشد که در پژوهش‌هایی مانند [۲۲، ۱۰، ۱۱] استفاده شده است. هالپرن و پرل در [۱۲] تعریفی مبتنی بر استدلال خلاف واقع لوئیس ارائه کردند که توانسته است برخی از مشکلات تعریف لوئیس در پیدا کردن علت در سناریوهای پیچیده را بر طرف کند. در ادامه برخی از پژوهش‌هایی که از تعریف هالپرن و پرل برای توضیح خطا استفاده کرده‌اند را مورد بررسی قرار می‌دهیم.

۱.۳ تخمین پوشش

در [۷] نویسندگان از مدل HP برای تخمین میزان پوشش^۳ سیستم توسط یک توصیف در فرآیند واریسی مدل استفاده کرده‌اند. معیارهای پوشش معمولاً در فرآیند تست سیستم استفاده می‌شوند و مشخص‌کننده درصدی از

^۱Fault Explanation

^۲Fault Localization

^۳Covering

اجزا یا حالت‌های سیستم هستند که توسط مجموعه‌ی تست‌ها مورد استفاده یا بازدید قرار می‌گیرند. در فرآیند واریسی مدل همه‌ی حالت‌های سیستم بررسی می‌شوند به همین دلیل در این شرایط اگر تغییر یک حالت منجر به نقض ویژگی توصیف شده شود این حالت پوشش داده شده توسط ویژگی تعریف می‌شود. با استفاده از مفهوم مسئولیت^۴ که در [۱۳] تعریف شده است، نویسندگان این پژوهش به جای در نظر گرفتن مقدار ۰ و ۱ برای پوشیده شدن یا نشدن از درجه‌ی مسئولیت استفاده می‌کنند. همانطور که مشخص است این پژوهش به اصلاح و بهبود توصیف ویژگی کمک می‌کند و نه پیدا کردن علت خطا. در این پژوهش همانند پژوهش جاری به شکل مستقیم از تعریف HP استفاده شده است.

۲.۳ علت خطا در مثال نقض

در [۲] نویسندگان سیستم را به صورت یک سیستم انتقال^۵ در نظر می‌گیرند که در آن هر حالت یک نگاشت از یک مجموعه‌ی متغیرهای بولی به مقادیر درست و غلط است. در این پژوهش با استفاده از تعریف علت واقعی در یک مثال نقض یک ویژگی توصیف شده در LTL^۶ یک دوتایی متغیر و حالت به عنوان علت واقعی در نظر گرفته می‌شود. در همین پژوهش یک الگوریتم تقریبی برای پیدا کردن همه‌ی علت‌ها در یک مثال نقض داده شده ارائه شده است و ابزاری برای نمایش این علت‌ها به صورت گرافیکی به کاربر توسعه داده شده و در ابزار درستی‌سنجی PE RuleBase متعلق به IBM گنجانده شده است. تصویر ۱.۳ رابط کاربری ابزار RuleBase PE را پس از پیدا کردن یک مثال نقض برای ویژگی زیر نشان می‌دهد:

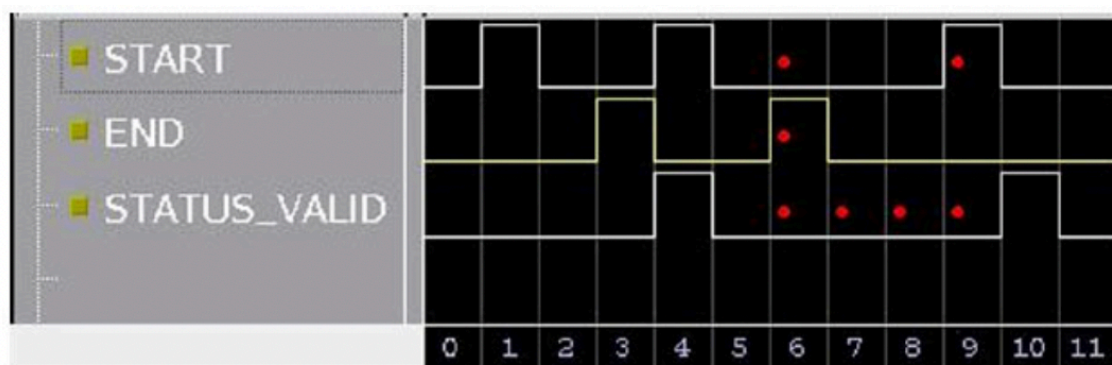
$$G((\neg \text{START} \wedge \neg \text{STATUS_VALID} \wedge \text{END}) \rightarrow [\neg \text{START} \vee \text{STATUS_VALID}])$$

در این تصویر نقاط قرمز علت‌های واقعی هستند که با الگوریتم تقریبی پیاده‌سازی شده پیدا شده‌اند. این پژوهش یکی از کاربردی‌ترین استفاده‌ها از توضیح خطا و پیدا کردن علت خطا را نشان می‌دهد. در این پژوهش سعی شده است تا علت خطا در یک مثال نقض پیدا شود و به همین دلیل مقدار متغیرها در حالت‌ها به عنوان علت پیدا می‌شوند در حالی که در پژوهش جاری هدف پیدا کردن علت خطا در کل سیستم است و در واقع ساختارهای

^۴Responsibility

^۵Transition System

^۶Linear Temporal Logic



شکل ۱.۳: رابط کاربری ابزار PE RuleBase

سیستم، مثلاً وجود یا عدم وجود روابط تعارض یا فعال‌سازی به عنوان علت خطا پیدا می‌شوند. اما همانند پژوهش جاری در این پژوهش هم به شکل مستقیم و بدون تغییر از تعریف HP استفاده شده است.

۳.۳ چک کردن علیت

در پژوهش [۱۷] نویسندگان تعریفی از علت واقعی که الهام گرفته از تعریف HP است ارائه می‌کنند و الگوریتم آن‌ها بر اساس این تعریف در حین اجرای فرآیند واریسی مدل^۷ علت‌ها را پیدا کرده و در نتیجه در انتهای واریسی مدل اگر سیستم ویژگی مورد نظر را نقض کرد به جای برگرداندن یک مثال نقض، رویدادهایی که علت رخداد خطا بوده‌اند را بر می‌گرداند. در این پژوهش یک منطق برای توصیف یک دنباله از رویداد عملیات‌های سیستم ارائه شده است و فرمول‌های این منطق به عنوان علت خطا در نظر گرفته می‌شوند. این پژوهش هم همانند [۲] سعی بر پیدا کردن همه‌ی علت‌های بروز خطا دارد و علت‌ها عملاً دنباله‌هایی از اجرای سیستم هستند. تفاوت اصلی این کار با پژوهش جاری در این است که در این پژوهش علت خطا در رفتارهای سیستم جستجو می‌شود در حالی که در پژوهش جاری علت خطا در میان عناصر ساختاری سیستم جستجو می‌شود. این روش تنها برای ویژگی‌های دسترس‌پذیری ارائه شده است. در [۳] نویسندگان این روش را برای ویژگی‌های دلخواه توصیف شده توسط LTL تعمیم دادند.

^۷Model Checking

۴.۳ علت واقعی در خودکاره‌های زمان‌دار

در [۱۵] نویسندگان از تعریف HP برای پیدا کردن علت خطا در خودکاره‌های زمان‌دار^۸ استفاده کرده‌اند. در درستی سنجی خودکاره‌های زمان‌دار یک ابزار واریسی مدل بلا درنگ نقض ویژگی را در قالب یک رد تشخیصی زمان‌دار^۹ که در واقع یک مثال نقض است بر می‌گرداند. یک TDT در واقع یک دنباله متناوب از انتقال تاخیر^{۱۰} و انتقال عملیات^{۱۱} ها است که در آن مقدار تاخیرها به صورت سمبلیک مشخص شده‌اند. هدف این پژوهش پیدا کردن مقادیری یا دامنه‌ای از مقادیر برای این تاخیرهای سمبلیک است که بروز خطا را اجتناب ناپذیر می‌کنند یا به عبارت دیگر علت واقعی هستند. در این پژوهش اما به صورت مستقیم از تعریف HP استفاده نشده است و بر اساس آن تعریفی برای علت واقعی نقض ویژگی در یک TDT بیان شده است.

۵.۳ چارچوب علیت بر اساس رد سیستم

در [۹] نویسندگان این مساله را مطرح می‌کنند که تعریف ارائه شده توسط هالپرن و پرل ذاتاً یک مدل بر اساس منطق گزاره‌ای^{۱۲} است و به همین دلیل برای درستی سنجی پردازنده‌ها ایده‌آل نیست. در این پژوهش یک فرمالیسم و تعریف جدید برای علیت بر اساس تعریف HP ارائه می‌شود که در آن از رد^{۱۳} های سیستم به جای متغیرها در مدل HP استفاده می‌شود و امکان ترکیب^{۱۴} چند مدل با یکدیگر را فراهم می‌کند.

⁸Timed Automata

⁹Timed Diagnostic Trace

¹⁰Transition Delay

¹¹Delay Transition

¹²Propositional Logic

¹³Trace

¹⁴Composition

۶.۳ استدلال مبتنی بر علیت در HML

در [۵] نویسندگان از مفهوم استدلال مبتنی در سیستم انتقال برچسب‌دار^{۱۵} و HML^{۱۶} [۱۴] استفاده کرده‌اند. در این پژوهش سیستم با استفاده از یک سیستم انتقال برچسب‌دار مدل می‌شود و رفتار ناامن توسط یک فرمول در قالب HML توصیف می‌شود. سپس یک تعریف جدید که برگرفته شده از تعریف HP است با استفاده از این مدل‌ها برای علت واقعی بیان می‌شود. در این تعریف از مفهومی به نام عدم وقوع^{۱۷} رویدادها که پیش‌تر در [۱۷] مطرح شده بود استفاده می‌شود. شهود کلی مفهوم عدم وقوع در علیت این است که در کنار اینکه رخ دادن برخی از رویدادها منجر به خطا می‌شود، رخ ندادن رویدادها هم می‌تواند به عنوان علت در نظر گرفته شود. در تعریف ارائه شده در این پژوهش مجموعه‌ای از محاسبه^{۱۸} های سیستم به عنوان علت برقراری یک فرمول HML در سیستم که رفتار نا امن^{۱۹} را توصیف می‌کند تعریف می‌شود. هر محاسبه شامل یک دنباله از عملیات‌های سیستم در کنار تعدادی عملیات دیگر، که عدم وقوع آن‌ها هم جزئی از علت است، در نظر گرفته می‌شود. به عبارت دیگر یک محاسبه را می‌توان شامل دو جز در نظر گرفت. جز اول یک اجرای سیستم است که منجر به خطا می‌شود. جز دوم مجموعه‌ای از اجراهای سیستم است که منجر به خطا نمی‌شوند و حاصل جایگذاری^{۲۰} برخی از عملیات‌ها در جز اول این محاسبه هستند. عملیات‌های جایگذاری شده عملیات‌هایی هستند که عدم وقوع آن‌ها به عنوان علت بروز خطا در نظر گرفته می‌شود. در این تعریف علت واقعی به گونه‌ای تعریف شده است که محاسباتی که منجر به فعال شدن فرمول HML در سیستم می‌شوند به عنوان علت در نظر گرفته می‌شوند. در این تعریف شروطی مشابه با شروط موجود در تعریف HP در نظر گرفته شده است. در [۶] نویسندگان تعریف خود را بهبود دادند تا تطابق بیشتری با تعریف HP داشته باشد. علاوه بر این در این پژوهش ثابت شده است که این تعریف از علت در سیستم‌هایی که ارتباط همگام^{۲۱} شده دارند قابل ترکیب نیست ولی در حالتی که سیستم‌ها ارتباط همگام نداشته باشند امکان ترکیب یا شکستن آن وجود دارد. نتایج حاصل از این پژوهش یکی از انگیزه‌های اصلی پژوهش جاری بود برای اینکه با انتخاب یک مدل معنایی یا تعریف علیت متفاوت امکان ترکیب آن برای سیستم‌های همگام شده بررسی شود. در ادامه به بررسی شباهت‌ها و تفاوت‌های این پژوهش و پژوهش جاری

¹⁵Labeled Transition System

¹⁶Hennesy Milner Loigc

¹⁷Non-Occurrence

¹⁸Computation

¹⁹Unsafe Behavior

²⁰Interleaving

²¹Synchronized

می‌پردازیم. اولاً در این پژوهش تعریف جدیدی از علت واقعی ارائه شده است که در پژوهش جاری مستقیماً از تعریف ارائه شده در [۱۲] استفاده شده است. در پژوهش جاری تمرکز بر پیدا کردن یک علت برای بروز خطا در سیستم است که در این پژوهش همه‌ی علل خطا مورد بررسی قرار می‌گیرند. پژوهش جاری علل خطا را در ساختارهای سیستم جستجو می‌کند که در حالی که این پژوهش در میان رفتارهای سیستم به دنبال علل خطا می‌گردد.

۷.۳ جمع‌بندی

همان‌طور که بررسی شد پژوهش‌های متعددی در زمینه‌ی توضیح خطا ارائه شده است که نشان از اهمیت این مساله در فرآیند درستی سنجی و اشکال‌زدایی دارد. همچنین تعریف HP هم مورد توجه زیادی برای پیدا کردن علت خطا قرار گرفته است. یکی از مهم‌ترین تمایزهای پژوهش جاری با پژوهش‌های پیشین در المان‌هایی است که در آن علت خطا پیدا می‌شود. همان‌طور که بررسی شد در تمامی پژوهش‌های پیشین در این زمینه علت خطا در میان رفتارهای سیستم جستجو می‌شود. اما در پژوهش جاری رویکردی متفاوت استفاده شده است و علت خطا در میان ساختارهای سیستم، مثلاً هم‌روند بودن یا نبودن پردازش، انجام می‌شود. مساله‌ی دیگری که باید به آن اشاره شود این است که در پژوهش جاری همانند [۲، ۷] به شکل مستقیم و بدون تغییر از تعریف HP استفاده می‌شود.

فصل ۴

روش و راه حل پیشنهادی

۱.۴ مقدمه

در این فصل روش پیدا کردن علت خطا در یک برنامه‌ی توصیف شده در نتکت پویا توضیح داده می‌شود. در بخش اول مدل معنایی عبارات نتکت پویا با در قالب ساختمان رویداد تعریف می‌شود. در بخش دوم یک مدل علی برای توصیف ساختمان رویداد مطرح می‌شود. در نهایت در بخش سوم شامل استفاده از این چگونگی ترکیب این دو روش برای توضیح خطا در یک برنامه نتکت پویا توضیح داده می‌شود..

۲.۴ مدل معنایی عبارات نتکت پویا در قالب ساختمان رویداد

در این بخش ابتدا انواع ترکیب و محدودسازی ساختمان‌های رویداد تعریف می‌شود. سپس با استفاده از این تعاریف یک مدل معنایی برای عبارات نتکت پویا ارائه می‌شود.

تعریف ۱.۲.۴. فرض کنید $E = (E, \#, \vdash)$ یک ساختمان رویداد باشد. به ازای یک مجموعه‌ی $A \subseteq E$ ،

محدودیت ^۱ E به A یک ساختمان رویداد به شکل زیر است:

$$E[A = (A, \#_A, \vdash_A)]$$

که داشته باشیم:

$$X \subseteq \text{Con}_A \iff X \subseteq A \wedge X \in \text{Con}$$

$$X \vdash_A e \iff X \subseteq A \wedge e \in A \wedge X \vdash e$$

تعریف ۲.۲.۴. فرض کنید $E = (E, \#, \vdash)$ یک ساختمان رویداد و a یک رویداد باشد. ساختمان رویداد $aE = (E', \#', \vdash')$ به گونه‌ای تعریف می‌شود که داشته باشیم:

$$E' = \{(0, a)\} \cup \{(1, e) | e \in E\},$$

$$e'_0 \# e'_1 \iff \exists e_0, e_1. e'_0 = (1, e_0) \wedge e'_1 = (1, e_1) \wedge e_0 \# e_1$$

$$X \vdash' e' \iff e' = (0, a) \text{ or } [e' = (1, e_1) \wedge (0, a) \in X \wedge \{e | (1, e) \in X\} \vdash e_1]$$

تعریف ۳.۲.۴. یک ساختمان رویداد برچسب‌دار ^۲ یک پنج‌تایی به شکل $(E, \#, \vdash, L, l)$ است که در آن $(E, \#, \vdash)$ یک ساختمان رویداد، L یک مجموعه از برچسب‌ها (فاقد عنصر $*$) و l یک تابع به فرم $l: E \rightarrow L$ است که به هر رویداد یک برچسب اختصاص می‌دهد. یک ساختمان رویداد برچسب‌دار را به اختصار به صورت (E, L, l) نشان می‌دهیم.

تعریف ۴.۲.۴. در یک ساختمان رویداد رابطه‌ی \bowtie را به صورت زیر تعریف می‌کنیم:

$$e \bowtie e' \iff e \# e' \vee e = e'$$

تعریف ۵.۲.۴. فرض کنید (E, L, l) یک ساختمان رویداد برچسب‌دار و α یک برچسب باشد. $\alpha(E, L, l)$

¹Restriction

²Labeled Event Structure

را به صورت یک ساختمان رویداد برچسب‌دار به شکل $(\alpha E, L', l)$ تعریف می‌کنیم که در آن $L' = \{\alpha\} \cup L$ و به ازای هر $e' \in E'$ داشته باشیم:

$$l'(e') = \begin{cases} \alpha & \text{if } e = (0, \alpha) \\ l(e) & \text{if } e = (1, e) \end{cases}$$

تعریف ۶.۲.۴. فرض کنید $E_0 = (E_0, \#_0, \vdash_0, L_0, l_0)$ و $E_1 = (E_1, \#_1, \vdash_1, L_1, l_1)$ دو ساختمان رویداد برچسب‌دار باشند. مجموع این دو ساختمان رویداد $E_0 + E_1$ را به صورت یک ساختمان رویداد برچسب‌دار $(E, \#, \vdash, L, l)$ تعریف می‌کنیم که در آن داشته باشیم:

$$E = \{(0, e) | e \in E_0\} \cup \{(1, e) | e \in E_1\}$$

با استفاده از این مجموعه از رویدادها توابع $\iota_k : E_k \rightarrow E$ را به ازای $k = 0, 1$ به شکل زیر تعریف می‌کنیم:

$$\iota_k(e) = (k, e)$$

رابطه‌ی تعارض را به گونه‌ای تعریف می‌کنیم که داشته باشیم:

$$\begin{aligned} e \# e' &\iff \exists e_0, e'_0. e = \iota_0(e_0) \wedge e' = \iota_0(e'_0) \wedge e_0 \#_0 e'_0 \\ &\vee \exists e_1, e'_1. e = \iota_1(e_1) \wedge e' = \iota_1(e'_1) \wedge e_1 \#_1 e'_1 \\ &\vee \exists e_0, e_1. (e = \iota_1(e_0) \wedge e' = \iota_1(e_1)) \vee (e' = \iota_1(e_0) \wedge e = \iota_1(e_1)) \end{aligned}$$

رابطه ی فعال سازی را به گونه ای تعریف می کنیم که داشته باشیم:

$$X \vdash e \iff X \in Con \wedge e \in E \wedge$$

$$(\exists X_0 \in Con_0, e_0 \in E_0. X = \iota_0 X_0 \wedge e = \iota_0(e_0) \wedge X_0 \vdash_0 e_0) \text{ or}$$

$$(\exists X_1 \in Con_1, e_1 \in E_1. X = \iota_1 X_1 \wedge e = \iota_1(e_1) \wedge X_1 \vdash_1 e_1)$$

مجموعه ی برچسب ها را به صورت $L = L_0 \cup L_1$ و تابع برچسب گذاری را به شکل تعریف می کنیم:

$$l(e) = \begin{cases} l_0(e_0) & \text{if } e = \iota_0(e_0) \\ l_1(e_1) & \text{if } e = \iota_1(e_1) \end{cases}$$

تعریف ۷.۲.۴. فرض کنید که $E_0 = (E_0, \#_0, \vdash_0, L_0, l_0)$ و $E_1 = (E_1, \#_1, \vdash_1, L_1, l_1)$ دو ساختار رویداد برچسب گذاری شده باشند. حاصل ضرب آن ها $E_0 \times E_1$ را به صورت یک ساختمان رویداد برچسب گذاری شده $E = (E, \#, \vdash, L, l)$ تعریف می کنیم که در آن رویدادها به صورت زیر تعریف می شوند:

$$E_0 \times_* E_1 = \{(e_0, *) | e_0 \in E_0\} \cup \{(*, e_1) | e_1 \in E_1\} \cup \{(e_0, e_1) | e_0 \in E_0 \wedge e_1 \in E_1\}$$

با توجه به این مجموعه رویدادها توابعی به شکل $\pi_i : E \rightarrow_* E_i$ تعریف می کنیم که به ازای $i = 0, 1$ داشته باشیم: $\pi_i(e_0, e_1) = e_i$. در اینجا رابطه ی تعارض را به کمک رابطه ی \bowtie که پیش تر تعریف شد، به شکل زیر به ازای تمامی رویدادهای $e, e' \in E$ توصیف می کنیم:

$$e \bowtie e' \iff \pi_0(e) \bowtie_0 \pi_0(e') \vee \pi_1(e) \bowtie_1 \pi_1(e')$$

رابطه‌ی فعال‌سازی را به صورت زیر تعریف می‌کنیم:

$$X \vdash e \iff X \in Con \wedge e \in \mathcal{E}$$

$$(\pi_0(e) \text{ defined} \Rightarrow \pi_0 X \vdash_0 \pi_0(e)) \wedge (\pi_1(e) \text{ defined} \Rightarrow \pi_1 X \vdash_1 \pi_1(e))$$

مجموعه‌ی برچسب‌های حاصلضرب را به صورت زیر تعریف می‌کنیم:

$$L_0 \times_* L_1 = \{(\alpha_0, *) \mid \alpha_0 \in L_0\} \cup \{(*, \alpha_1) \mid \alpha_1 \in L_1\} \cup \{(\alpha_0, \alpha_1) \mid \alpha_0 \in L_0 \wedge \alpha_1 \in L_1\}$$

در انتها تابع برچسب‌گذاری را به صورت زیر تعریف می‌کنیم:

$$l(e) = (l_0(\pi_0(e), l_1(\pi_1(e))))$$

تعریف ۸.۲.۴. فرض کنید که $E = (E, \#, \vdash, L, l)$ یک ساختمان رویداد برچسب‌دار باشد. فرض کنید Λ یک زیرمجموعه از L باشد. محدودیت E به Λ را به صورت $E[\Lambda]$ و به شکل یک ساختمان رویداد برچسب‌گذاری شده به شکل $(E', \#', \vdash', L \cap \Lambda, l')$ که در آن $\{e \in E \mid l(e) \in \Lambda\}$ است و $(E', \#', \vdash') = (E, \#, \vdash)[\{e \in E \mid l(e) \in \Lambda\}]$ است و تابع برچسب‌گذاری معادل محدودسازی تابع l به دامنه‌ی $L \cap \Lambda$ است.

۱.۲.۴ معنای عبارات نتکت پویای نرمال

در ادامه ابتدا فرم نرمال عبارات نتکت پویا را تعریف می‌کنیم. فرض کنید که فیلدهای ممکن برای بسته‌ها f_1, f_2, \dots, f_k باشند. یک فیلتر کامل^۳ به صورت $\alpha = f_1 = n_1 \dots f_k = n_k$ و یک اختصاص کامل^۴ به صورت $\pi = f_1 \leftarrow n_1 \dots f_k \leftarrow n_k$ تعریف می‌شود. می‌گوییم یک عبارت q در $NetKAT^{dup}$ به فرم نرمال است اگر به شکل $\sum_{\alpha \cdot \pi \in \mathcal{A}} \alpha \cdot \pi$ باشد که داشته باشیم $\mathcal{A} = \{\alpha_i \cdot \pi_i \mid i \in I\}$. در عبارت قبل I مدل زبانی $NetKAT^{dup}$ می‌باشد. بر اساس لم ۵ در [۴] به ازای هر عبارت p در $NetKAT^{dup}$ یک عبارت p' به فرم نرمال وجود دارد که داشته باشیم: $p \equiv p'$.

³Complete Test

⁴Complete Assignment

تعریف ۹.۲.۴. زبان نتکت پویا نرمال را با دستور زبان زیر تعریف می‌کنیم:

$$F ::= \alpha \cdot \pi$$

$$D ::= \perp | F; D | x?F; D | x!F; D | D \parallel D | D \oplus D$$

با استفاده از این لم، در لم ۹ که در [۴] ثابت شده است، به ازای هر عبارت p در نتکت پویا یک عبارت معادل آن به فرم نرمال وجود دارد که داشته باشیم: $p \equiv q$. بنابراین در نهایت می‌توانیم هر عبارت نتکت پویا را به فرم یک عبارت نرمال با توجه به تعریف ۹.۲.۴ بنویسیم. در ادامه فرض کنیم که \mathcal{A} مجموعه‌ی الفبا شامل تمامی حروف به شکل $\alpha \cdot \pi, x?F, x!F$ باشد و داشته باشیم $\alpha \in \mathcal{A}, L \subseteq \mathcal{A}$. معنای عبارات نتکت پویای نرمال را با به صورت زیر تعریف می‌کنیم:

$$[\perp] = (\emptyset, \emptyset)$$

$$[\alpha; t] = \alpha([\![t]\!])$$

$$[t_1 \oplus t_2] = [t_1] + [t_2]$$

$$[t_1 \parallel t_2] = [t_1] \times [t_2]$$

$$[\delta_L(t)] = [t] \upharpoonright \mathcal{A} \setminus L$$

سمت چپ معادلات بالا عبارات نتکت پویای نرمال و در سمت راست ساختمان رویداد معادل هر یک مشخص شده است. در معادلات بالا (\emptyset, \emptyset) یک ساختمان رویداد که مجموعه‌ی رویدادها و مجموعه‌ی برچسب‌های آن تهی است را نشان می‌دهد.

۳.۴ مدل علی برای ساختمان رویداد

در ادامه نحوه‌ی توصیف یک ساختمان رویداد در قالب یک مدل علی مطابق تعریف HP را بیان می‌کنیم. فرض کنیم که $E = (E, \#, \vdash)$ یک ساختمان رویداد باشد. مدل علی این ساختمان رویداد را به صورت

$\mathcal{M} = (\mathcal{S}, \mathcal{F}, \mathcal{E})$ تعریف می‌کنیم که در آن $\mathcal{S} = (\mathcal{U}, \mathcal{V}, \mathcal{R})$. در این مدل فرض می‌کنیم همه‌ی متغیرها از نوع بولی هستند. همچنین در این مدل متغیر برونی در نظر نمی‌گیریم بنابراین داریم $\mathcal{U} = \emptyset$. اگر فرض کنیم مجموعه رویدادها به صورت $E = \{e_1, e_2, \dots, e_n\}$ باشد مجموعه‌ی متغیرهای درونی را به صورت زیر تعریف می‌کنیم:

$$\begin{aligned} \mathcal{V} = & \{C_{e_i, e_j} | 1 \leq i < j \leq n, e_i \in E \wedge e_j \in E\} \\ & \cup \{EN_{s, e} | s \in \mathcal{P}(E), e \in E, e \notin s\} \\ & \cup \{M_{s, e} | s \in \mathcal{P}(E), e \in E, e \notin s\} \cup \{PV\} \end{aligned}$$

به صورت شهودی به ازای هر عضو از رابطه‌های $\#, \vdash, \vdash_{min}$ یک متغیر درونی در نظر می‌گیریم که درست بودن این متغیر به معنای وجود عنصر منتظر با آن در رابطه است.

به ازای $x, y \in \mathcal{P}(E)$ پوشیده شدن^۵ x توسط y را که با $x < y$ نمایش می‌دهیم به صورت زیر تعریف می‌کنیم:

$$x \subseteq y \wedge x \neq y \wedge (\forall z. x \subseteq z \subseteq y \Rightarrow x = z \text{ or } y = z)$$

همچنین به ازای هر متغیر $X \in \mathcal{V}$ بردار \vec{V}_X را بردار شامل همه‌ی متغیرهای درونی به غیر از X تعریف می‌کنیم. با استفاده از این تعاریف توابع متغیرهای درونی را به صورت زیر تعریف می‌کنیم:

$$F_{C_{e, e'}}(\vec{V}_{C_{e, e'}}) = \begin{cases} true & \text{if } e \# e' \\ false & \text{otherwise} \end{cases}$$

$$F_{M_{s, e}}(\vec{V}_{M_{s, e}}) = \begin{cases} Min(s, e) \wedge Con(s) & \text{if } s \vdash_{min} e \\ false & \text{otherwise} \end{cases}$$

⁵Covering

$$F_{EN_{s,e}}(\vec{V}_{EN_{s,e}}) = \left(M_{s,e} \vee \left(\bigvee_{s' < s} EN_{s',e} \right) \right) \wedge Con(s)$$

که در آن‌ها داریم:

$$Con(s) = \left(\bigwedge_{1 \leq j < j' \leq n \wedge e_j, e_{j'} \in s} \neg C_{e_j, e_{j'}} \right)$$

$$Min(s, e) = \left(\bigwedge_{s' \subseteq E, (s' \subset s \vee s \subset s') \wedge e \notin s'} \neg M_{s', e} \right)$$

فرض کنید که \mathbb{E} مجموعه‌ی تمامی سه‌تایی‌ها به فرم $(E, \#', \vdash')$ باشد که داشته باشیم:

$$\#' \subseteq E \times E$$

$$\vdash' \subseteq \mathcal{P} \times E$$

یک تابع به فرم $ES : \times_{V \in \mathcal{V} \setminus \{PV\}} \mathcal{R}(V) \rightarrow \mathbb{E}$ تعریف می‌کنیم که به صورت شهودی ساختمان رویداد حاصل از مقدار فعلی متغیرها در مدل علی را به دست می‌دهد. فرض کنیم \vec{v} برداری شامل مقادیر متغیرهای $\mathcal{V} \setminus \{PV\}$ باشد. به ازای هر متغیر مانند $V \in \mathcal{V}$ مقدار آن در \vec{v} را با $\vec{v}(V)$ نمایش می‌دهیم. تابع ES را به گونه‌ای تعریف می‌کنیم که اگر $ES(\vec{v}) = (E, \#', \vdash')$ آنگاه داشته باشیم:

$$\forall e, e' \in E. e \#' e' \wedge e' \#' e \iff \vec{v}(C_{e,e'}) = T$$

$$\forall s \in \mathcal{P}(E), e \in E. s \vdash' e \iff \vec{v}(EN_{s,e}) = T$$

در ادامه فرض می‌کنیم که رفتار نا امن^۶ سیستمی که در قالب ساختمان رویداد مدل شده است، در قالب تابع متغیر PV توصیف شده است و در صورتی که رفتار نا امن در سیستم وجود داشته باشد مقدار آن درست و در غیر این صورت غلط است. در نهایت مقداردهی‌های مجاز \mathcal{E} را مجموعه‌ی مقداردهی‌هایی مانند \vec{v} در نظر می‌گیریم که خروجی تابع ES به ازای آن‌ها یک ساختمان رویداد باشد.

برای پیدا کردن علت واقعی در این مدل از تعریف زیر که در واقع سازگار شده‌ی تعریف برای مدل علی تعمیم

^۶Unsafe Behavior

یافته است استفاده می‌کنیم:

تعریف ۱.۳.۴. اگر $M = (\mathcal{S}, \mathcal{F}, \mathcal{E})$ یک مدل علیّی تعمیم یافته و \vec{V} برداری از متغیرهای $\mathcal{V} \setminus PV$ باشد، فرمول $\vec{X} = \vec{x}$ علت واقعی φ در (M, \vec{u}) است اگر شرایط زیر برای آن برقرار باشد:

$$(M, \vec{u}) \models (\vec{X} = \vec{x}) \wedge \varphi \quad ۱.$$

۲. یک افزاز مانند (\vec{Z}, \vec{W}) از مجموعه‌ی متغیرهای \mathcal{V} با شرط $\vec{X} \subseteq \vec{Z}$ و مقادیر (\vec{x}, \vec{w}') برای متغیرهای (\vec{X}, \vec{W}) وجود داشته باشد که داشته باشیم $(M, \vec{u}) \models \vec{Z} = \vec{z}^*$ و شرایط زیر را برآورده کند:

$$(M, \vec{u}) \models [\vec{X} \leftarrow \vec{x}', \vec{W} \leftarrow \vec{w}'] \neg \varphi \wedge \vec{V} = \vec{v} \wedge \vec{v} \in \mathcal{E} \quad (I)$$

$$\forall \vec{W}' \subseteq \vec{W}, \vec{Z}' \in \vec{Z}. (M, \vec{u}) \models [\vec{X} \leftarrow \vec{x}, \vec{W}' \leftarrow \vec{w}', \vec{Z}' \leftarrow \vec{z}^*] \vec{V} = \vec{v} \wedge \vec{v} \in \mathcal{E} \Rightarrow \varphi \quad (ب)$$

۳. \vec{X} مینیمال باشد.

در این تعریف برای اینکه تنها مقداردهی‌های مجاز برای پیدا کردن علت واقعی در نظر گرفته شوند شرط ۲ تغییر یافته است. بند اضافه شده به شرط ۲. الف بیان می‌کند که تغییرات ایجاد شده در مدل یک مقداردهی مجاز باشند. بند اضافه شده در ۲. ب باعث می‌شود این شرط تنها در حالت‌هایی بررسی شود که مقداردهی داده شده مجاز باشد.

۴.۴ پیدا کردن علت خطا در نت‌کت پویا

با استفاده از تعاریف بخش‌های قبلی در این بخش به چگونگی پیدا کردن علت خطا در یک برنامه توصیف شده در نت‌کت پویا می‌پردازیم.

فرض می‌کنیم که یک عبارت نت‌کت پویا p در اختیار داریم. ابتدا عبارت p را به فرم نرمال مطابق تعریف ۹.۲.۴ در می‌آوریم. فرض کنیم عبارت q فرم نرمال عبارت p باشد. اکنون فرض کنیم $E = \llbracket q \rrbracket$ ساختمان رویداد معادل q باشد. اکنون مدل علیّی \mathcal{M} را بر اساس E می‌سازیم و رفتار نا امن را در قالب تابع متغیر PV این مدل و به شکل یک شرط بر روی مجموعه‌ی پیکربندی‌های مدل علیّی توصیف می‌کنیم. در نهایت کافی است برای پیدا کردن علت واقعی رفتار نا امن، علت واقعی $PV = T$ در \mathcal{M} را بر اساس تعریف ۱.۳.۴ پیدا کنیم. توجه کنید

که در اینجا محدودیتی برای چگونگی تعریف رفتار نا امن وجود ندارد و یان تعریف می‌تواند هر شرطی بر روی مجموعه‌ی پیکربندی‌های مدل علی باشد.

مثلا اگر مجموعه‌ای از مثال‌های نقض سیستم در قالب پیکربندی‌های ساختمان رویداد وجود داشته باشد (مثلا مجموعه‌ی C)، می‌توان رفتار نا امن را وجود یکی از این پیکربندی‌ها در سیستم توصیف کرد:

$$F_{PV}(\vec{V}_{PV}) = \bigvee_{\forall c \in C} c \in \mathcal{F}(ES(\vec{v}))$$

در مثالی دیگر اگر رفتار نا امن در قالب یک شرط unsafe روی برچسب‌های سیستم توصیف شده باشد می‌توان رفتار نا امن را وجود یک پیکربندی که شامل یک رویداد که شرط unsafe را برآورده می‌کند توصیف کرد:

$$F_{PV}(\vec{V}_{PV}) = \exists c \in \mathcal{F}(ES(\vec{v})). \exists e \in c. \text{unsafe}(l(e))$$

مراجع

- [1] Anderson, Carolyn Jane, Foster, Nate, Guha, Arjun, Jeannin, Jean-Baptiste, Kozen, Dexter, Schlesinger, Cole, and Walker, David. Netkat: Semantic foundations for networks. *Acm sigplan notices*, 49(1):113–126, 2014. [5](#), [8](#)
- [2] Beer, Ilan, Ben-David, Shoham, Chockler, Hana, Orni, Avigail, and Trefler, Richard. Explaining counterexamples using causality. *Formal Methods in System Design*, 40(1):20–40, Feb 2012. [32](#), [33](#), [36](#)
- [3] Caltais, Georgiana, Guetlein, Sophie Linnea, and Leue, Stefan. Causality for general ltl-definable properties. *Electronic Proceedings in Theoretical Computer Science*, 286:1–15, Jan 2019. [33](#)
- [4] Caltais, Georgiana, Hojjat, Hossein, Mousavi, Mohammad, and Tunc, Hunkar Can. Dynetkat: An algebra of dynamic networks. *arXiv preprint arXiv:2102.10035*, 2021. [5](#), [15](#), [41](#), [42](#)
- [5] Caltais, Georgiana, Leue, Stefan, and Mousavi, Mohammad Reza. (de-)composing causality in labeled transition systems. *Electronic Proceedings in Theoretical Computer Science*, 224:10–24, Aug 2016. [35](#)
- [6] Caltais, Georgiana, Mousavi, Mohammad Reza, and Singh, Hargurbir. Causal reasoning for safety in hennessy milner logic. *Fundamenta Informaticae*, 173(2–3):217–251, Mar 2020. [35](#)
- [7] Chockler, Hana, Halpern, Joseph Y., and Kupferman, Orna. What causes a system to satisfy a specification? *ACM Transactions on Computational Logic*, 9(3):1–26, Jun 2008. [31](#), [36](#)
- [8] Foerster, Klaus-Tycho, Schmid, Stefan, and Vissicchio, Stefano. Survey of consistent software-defined network updates. *IEEE Communications Surveys & Tutorials*, 21(2):1435–1461, 2018. [3](#), [8](#)

- [9] Gössler, Gregor and Le Métayer, Daniel. A general trace-based framework of logical causality. In *International Workshop on Formal Aspects of Component Software*, pages 157–173. Springer, 2013. [34](#)
- [10] Groce, Alex, Chaki, Sagar, Kroening, Daniel, and Strichman, Ofer. Error explanation with distance metrics. *International Journal on Software Tools for Technology Transfer*, 8(3):229–247, 2006. [31](#)
- [11] Groce, Alex and Visser, Willem. What went wrong: Explaining counterexamples. In *International SPIN Workshop on Model Checking of Software*, pages 121–136. Springer, 2003. [31](#)
- [12] Halpern, Joseph Y. and Pearl, Judea. Causes and explanations: A structural-model approach, part i: Causes. *arXiv:cs/0011012*, Nov 2005. arXiv: cs/0011012. [5](#), [23](#), [25](#), [28](#), [31](#), [36](#)
- [13] Halpern, Joseph Y. and Pearl, Judea. Causes and explanations: A structural-model approach, part ii: Explanations. *The British journal for the philosophy of science*, 56(4):889–911, 2005. [32](#)
- [14] Hennessy, Matthew and Milner, Robin. On observing nondeterminism and concurrency. In *International Colloquium on Automata, Languages, and Programming*, pages 299–309. Springer, 1980. [35](#)
- [15] Kölbl, Martin, Leue, Stefan, and Schmid, Robert. Dynamic causes for the violation of timed reachability properties. In *International Conference on Formal Modeling and Analysis of Timed Systems*, pages 127–143. Springer, 2020. [34](#)
- [16] Kozen, Dexter. Kleene algebra with tests. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 19(3):427–443, 1997. [8](#)
- [17] Leitner-Fischer, Florian and Leue, Stefan. Causality checking for complex system models. In *International Workshop on Verification, Model Checking, and Abstract Interpretation*, page 248–267. Springer, 2013. [33](#), [35](#)
- [18] Lewis, David. *Counterfactuals*. Wiley, 1973. [31](#)
- [19] McKeown, Nick, Anderson, Tom, Balakrishnan, Hari, Parulkar, Guru, Peterson, Larry, Rexford, Jennifer, Shenker, Scott, and Turner, Jonathan. Openflow: enabling innovation in campus networks. *ACM SIGCOMM computer communication review*, 38(2):69–74, 2008. [8](#)
- [20] Sassone, Vladimiro, Nielsen, Mogens, and Winskel, Glynn. Models for concurrency: Towards a classification. *Theoretical Computer Science*, 170(1-2):297–348, 1996. [20](#)

- [21] Winskel, Glynn. *Event structures*, volume 255 of *Lecture Notes in Computer Science*, page 325–392. Springer Berlin Heidelberg, Berlin, Heidelberg, 1987. [20](#)
- [22] Zeller, Andreas. *Why programs fail: a guide to systematic debugging*. Elsevier, 2009. [31](#)

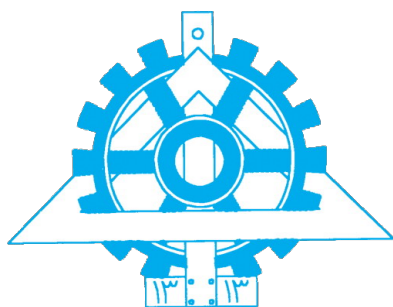
واژه‌نامهٔ فارسی به انگلیسی

واژه‌نامه انگلیسی به فارسی

Abstract

This thesis studies on writing projects, theses and dissertations using tehran-thesis class. It ...

Keywords Writing Thesis, Template, \LaTeX , \Xy Persian



University of Tehran
College of Engineering
Faculty of Electrical and
Computer Engineering



Explaining Failures in Software-Defined Networks Using Casual Reasoning

A Thesis submitted to the Graduate Studies Office
In partial fulfillment of the requirements for
The degree of Master of Science
in Computer Engineering - Software Engineering

By:

Amir Hossein Seyhani

Supervisors:

Dr. Hossein Hojjat and Dr. Mohammad Reza Mousavi

Advisor:

First Advisor

September 2022