بسم الله الرحمن الرحيم

دانشگاه تربیت مدرس

دانشکده فنی و مهندسی

پایان‌نامه‌ی دوره کارشناسی ارشد مهندسی کامپیوتر - نرم‌افزار

راستی‌آزمایی حین‌اجرای برنامه‌های واکنشی بی‌درنگ با رویکرد منطق بی‌درنگ

مهدی میرزاآقایی

استاد راهنما :

دکتر سعید جلیلی

زمستان ۱۳۸۵

بسمه تعالی

تاییدیه هیات داوران

آقای مهدی میرزاآقایی پایان نامه ۹ واحدی خود را با عنوان راستی آزمایی حین اجرای برنامه های واکنشی بی درنگ بارویکرد منطق بی درنگ در تاریخ ۱۳۸۵/۱۱/۸ ارائه کردند.

اعضای هیات داوران نسخه نهایی این پایان نامه را از نظر فرم و محتوا تایید کرده و پذیرش آنرا برای تکمیل درجه کارشناسی ارشد مهندسی برق - مهندسی کامپیوتر-نرم افزار پیشنهاد می کنند.

اعضای هیات داوران	نام و نام خانوادگی	رتبه علمی	امضا
استاد راهنما	دکتر سعید جلیلی	استادیار	
استاد ناظر	دکتر نصراله مقدم چرکری	استادیار	
استاد ناظر	دکتر محمدتقی حمیدی بهشتی	استادیار	
استاد ناظر	دکتر - میریان		
مدیر گروه (یا نماینده گروه تخصصی)	دکتر نصراله مقدم چرکری	استادیار	

این نسخه عنوان نسخه نهایی پایان نامه مورد تایید است.

دستور العمل حق مالکیت مادی و معنوی در مورد نتایج پژوهشهای علمی دانشگاه تربیت مدرس

مقدمه:با عنایت به سیاست های پژوهشی دانشگاه در راستای تحقق عدالت وکرامت انسانها که لازمه شکوفایی علمی و فنی است و رعایت حقوق مادی ومعنوی دانشگاه و پژوهشگران لازم است اعضای هیات علمی دانشجویان دانش آموختگان و دیگر همکاران طرح درمورد نتایج پژوهشهای علمی که تحت عناوین پایان نامه وساله و طرحهای تحقیقاتی با هماهنگی دانشگاه انجام شده است موارد ذیل را رعایت نمایید:

ماده۱: حقوق مادی و معنوی پایان نامه‌ها / رساله های مصوب دانشگاه متعلق به دانشگاه است و هر گونه بهره‌برداری ازآن باید با ذکر نام دانشگاه و رعایت آیین‌نامه‌ها و دستورالعمل‌های مصوب دانشگاه باشد.

ماده ۲- انتشار مقاله یا مقالات مستخرج از پایان نامه/ رساله به صورت چاپ در نشریات علمی و یا ارائه در مجامع علمی می‌باید به نام دانشگاه بوده و استاد راهنما نویسنده مسئول مقاله باشند.

تبصره: در مقالاتی که پس از دانش آموختگی بصورت ترکیبی از اطلاعات جدید و نتایج حاصل از پایان‌نامه/ رساله نیز منتشر می‌شود نیز باید نام دانشگاه درج شود.

ماده۳- انتشار کتاب حاصل از نتایج پایان‌نامه/ رساله و تمامی طرحهای تحقیقاتی دانشگاه باید با مجوز کتبی صادره از طریق حوزه پژوهشی دانشگاه و بر اساس آیین‌نامه‌های مصوب انجام می‌شود.

ماده ۴- ثبت اختراع و تدوین دانش فنی و یا ارائه در جشنواره های ملی، منطقه‌ای و بین المللی که حاصل نتایج مستخرج از پایان‌نامه/ رساله و تمامی طرح های تحقیقاتی دانشگاه باید با هماهنگی استاد راهنما یا مجری طرح از طریق حوزه پژوهشی دانشگاه انجام گیرد.

ماده ۵- این دستورالعمل در ۵ ماده و یک تبصره در تاریخ ۱۳۸۴/۴/۲۵ در شورای پژوهشی دانشگاه به تصویب رسیده و از تاریخ تصویب لازم الاجرا است و هر گونه تخلف از مفاد این دستورالعمل، از طریق مراجع قانونی قابل پیگیری خواهد بود.

تقدیم به دیدگانم

به حامیان بزرگ زندگی‌ام

آنان که عاشقانه دوستشان دارم

تقدیم به پدرو مادر عزیزم

و خواهران مهربانم

تشکر و قدردانی

سپاس خداوند منان را که بار دیگر دری از درهای رحمت خود را بر من گشود و به من توفیق کسب علم، در راستای افزایش درک خویش از عظمت باری تعالی و شکوه جهان هستی مرحمت نمود. زیرا هر آنچه که بر انسان اتفاق می‌افتد بهانه‌ای است برای شناخت بهتر از جهان هستی و نزدیکی بیشتر با باری تعالی؛ این پژوهش نیز از این قاعده مستثنی نیست هر چند که در نگاه اول موضوع پژوهش چنین حسی را تداعی نمی‌کند.

در فرایند انجام این پژوهش از استاد گرانقدر جناب آقای دکتر سعید جلیلی درس‌های علمی و اخلاقی بی‌شماری را آموختم. از ایشان به دلیل این‌که طی مدت زمان انجام این پژوهش تجربیات ارزنده و چندین ساله‌ی خود را در اختیار اینجانب قرار دادند، نهایت تشکر را دارم.

حضور و نقش کلیدی پدر، مادر و خواهران عزیزم غیر قابل چشم پوشی است؛ زیرا اگر نبود زحمات و پشتیبانی‌های عاطفی آنها، انجام این پژوهش یا میسر نمی‌شد و یا با مشقت‌های فراوان انجام می‌شد. قدردان تمام حمایت‌های ایشان هستم.

از جناب آقای دکتر نصراله مقدم، به دلیل حمایت‌های بی‌دریغشان و اعضای محترم هیات داوران به دلیل صرف وقت برای ارزیابی این پژوهش، نهایت تشکر را دارم.

آخرین و نه کمترین سپاس من از آقایان غلامرضا شاه‌محمدی، مهدی آبادی، محرم منصوری‌زاده و سید مرتضی بابامیر به دلیل صرف وقت و راهنمایی‌هایشان است.

امید است، این پژوهش دریچه‌ای برای گام‌های وسیع‌تر باشد.

مهدی میرزاآقایی

۸۵/۱۱/۲

چکیده

رویکردهای متداول وارسی و اعتبارسنجی نرم‌افزار برای برنامه‌های واکنشی بی‌درنگ به اندازه کافی قابل اعتماد نیستند. باتوجه به پیچیدگی زیاد رویکرد وارسی رسمی و کامل نبودن رویکرد آزمون، رویکرد راستی‌آزمایی حین اجرا پیشنهاد شده است. این رویکرد، به‌علت این‌که در محیط واقعی اجرا می‌گردد، قادر به کشف خطاهایی است که تاکنون آشکار نشده‌اند. به‌عبارت دیگر، مکملی برای دو رویکرد فوق محسوب می‌شود.

در این پایان‌نامه، چارچوبی جهت راستی‌آزمایی حین اجرای برنامه‌های واکنشی بی‌درنگ ارائه شده است که علاوه بر مستقل بودن از زبان بیان ویژگی‌ها، توانایی اجرای همراه با برنامه تحت پایش را دارد و می‌تواند برنامه را در هنگام بروز وضعیت ناهنجار به حالت ایمنی ببرد. همچنین از رویکرد جنبه‌گرا برای ابزارآمایی ویژگی‌های ایمنی استفاده شده است. این چارچوب در سه فاز، عمل راستی‌آزمایی ویژگی‌ها را انجام می‌دهد. در فاز اول، ویژگی‌های ایمنی پس از استخراج از مسئولیت‌های برنامه با یک منطق‌زمانی بیان گردیده و رفتار تحمل‌پذیری برنامه در برابر نقض این ویژگی‌ها به آن اضافه می‌شود. راستی‌آزمای رفتار برنامه درحین اجرا که توسط جنبه‌های زمانی، عملیاتی و ضرب‌الاجل تحقق می‌یابد، به کدبرنامه بافته می‌شود و در محیط به‌همراه کد برنامه اجرا می‌گردد. راستی‌آزما، رفتار برنامه را در نقاط اتصال با توجه به ویژگی‌های ایمنی مربوطه، مورد بررسی قرارداده و در صورت تشخیص نقض ویژگی، رفتار مشخصی (تحمل پذیری در برابر نقض ویژگی) را از خود نشان داده و برنامه را به وضعیت ایمنی می‌برد که روش‌های متداول قادر به انجام این‌کار نیستند و تنها به رویدادنگاری بسنده می‌کنند.

این چارچوب با دو روش بیان ویژگی‌های RTL و ERL مدل‌سازی و اجرا گردید. RTL به‌علت این‌که توانایی بیان ویژگی‌های بی‌درنگ نظیر تاخیر، ضرب‌الاجل و چندین وقوع یک رخداد خاص را دارد، به‌راحتی می‌تواند در بیان ویژگی‌های زمانی برنامه‌های واکنشی بی‌درنگ بکار گرفته شود. ERL نیز به‌علت این‌که مختص برنامه‌های بی‌درنگ طراحی شده است و دارای بیان ساده و روانی می‌باشد، برای راستی‌آزمایی حین اجرا بکار گرفته شده است.

آزمایشات نشان می‌دهد که چارچوب پیشنهادی، نقض تمام ویژگی‌های تحت راستی‌آزمایی را تشخیص می‌دهد. سربار چارچوب پیشنهادی از ٤٪ تا ٣٣٪ می‌باشد که با توجه به تعداد و نوع ویژگی‌های مورد پایش و زبان بیان ویژگی‌ها تعیین می‌گردد. در ضمن مشخص شد که سربار چارچوب پیشنهادی با افزایش تعداد ویژگی‌ها بصورت خطی افزایش می‌یابد.

کلمات کلیدی: راستی‌آزمایی‌حین‌اجرا، برنامه واکنشی بی‌درنگ، منطق‌زمانی بی‌درنگ، منطق بی‌درنگ رویدادگرا، برنامه‌نویسی جنبه‌گرا.

فهرست مطالب

فهرست جداول

فهرست اشکال

فصل اول

کلیات

فصل اول
کلیات

۱-۱- مقدمه

امروزه نرم‌افزارها کاربردهای گسترده‌ای پیدا کرده‌اند که این گستردگی و دامنه استفاده، باعث افزایش پیچیدگی آن شده است. در کاربردهای خاصی مانند کنترل قطارها، کاربردهای پزشکی، فضاپیماها و غیره درصورتی که شکستی در نرم‌افزار بوجود بیاید هزینه‌های جبران ناپذیری مثل صدمات جانی و هزینه‌های مالی عظیمی خواهد داشت. بنابراین مقوله اعتبارسنجی نرم‌افزارها از اهمیت فوق‌العاده‌ای برخوردار است.

۱-۲- صورت مسئله

در دو دهه اخیر تلاش‌های زیادی برای تحلیل و اعتبارسنجی[1] برنامه‌های واکنشی بی‌درنگ انجام شده است. به‌علت ماهیت این‌گونه برنامه‌ها که معمولا حیاتی و حساس هستند، از روش‌های متداول برای اعتبارسنجی آنها استفاده نمی‌شود، چراکه زبان‌های برنامه نویسی رایج قابل اعتماد نیستند و اعتبارسنجی آن‌ها به طور کامل قابل انجام نیست[۱].

روش متداولی که برای آشکارسازی خطا در برنامه‌ها بکاربرده می‌شود، آزمون پیاده‌سازی برنامه توسط مجموعه ورودی‌های مشخص است. این رویکرد نمی‌تواند درستی پیاده‌سازی را برای تمام توالی‌های ورودی برنامه (که یک مجموعه نامحدود است) تضمین کند. بنابراین تضمینی برای عملکرد درست برنامه هنگام اعمال ورودی‌های داده نشده نمی‌دهد[۲, ۳]. بنابراین هیچگاه از طریق این رویکرد نمی‌توان بطورکامل به رفتار برنامه اطمینان پیدا کرد. علاوه بر آن تولید مجموعه ورودی‌ها برای برنامه‌های واکنشی بی‌درنگ بسیار مشکل‌تر از برنامه‌های عادی است[٤].در سال

---

[1] Validation

۲۰۰۲ گزارش RTI[1] به انستیتو ملی استاندارد و فناوری آمریکا مشخص ساخت که آزمون نرم افزار ۳۰٪-۹۰٪ از تلاش را برای تولید یک برنامه عملیاتی تشکیل می‌دهد. با این وجود، ۵٪ از تمام خطاهای پیداشده طی حیات نرم‌افزار، پس از انتشار نرم‌افزار کشف می‌شود. در سال ۱۹۹۹ هزینه تخمینی خطاهای نرم‌افزار تنها در صنعت هوانوردی ٦ میلیارد دلار بوده است[۵].

روش دیگری که برای حل مشکلات برنامه بکار می‌رود، شیوه‌های رسمی هستند که اجازه مدل‌سازی ریاضی و اثبات ویژگی‌های برنامه را می‌دهند. این روش‌ها که اثبات قضیه[2] و بازبینی مدل[3] نام دارند، باعث افزایش ضریب اطمینان رفتار برنامه می‌شوند. با این وجود، وارسی رسمی برنامه بطور کامل قابل انجام نیست. وجود شاخه‌های نامحدود در فرایند اثبات، در روش اثبات قضیه و مشکل انفجار فضای حالات[4] در روش بازبینی مدل، باعث غیرعملی شدن وارسی کامل برنامه‌های واکنشی بی‌درنگ می‌شود[٦]. در ضمن وارسی تمام حالات برنامه باعث پیچیدگی وارسی این‌گونه برنامه‌ها می‌شود. علاوه براین، وارسی برنامه تنها به مدل‌های رسمی این برنامه‌ها اعمال می‌گردد و هنوز درستی پیاده‌سازی و عوامل محیطی زمان اجرای آن‌ها بررسی نمی‌شود. بنابراین حتی اگر برنامه به‌صورت رسمی، قبل از پیاده‌سازی آن، وارسی گردد، با توجه به جزئی‌تر بودن پیاده‌سازی، هنوز اطمینان کاملی به درستی پیاده‌سازی عملی آن وجود ندارد[۷].

با توجه به مطالب بالا، زمانی‌که برنامه در حال اجرا است، تضمین این‌که برنامه بدون هیچ‌گونه خطایی به‌درستی اجرا شود، با بهره‌گیری از رویکرد آزمون و در صورت نیاز وارسی رسمی برنامه امکان‌پذیر نمی‌باشد. در اینجا است که رویکرد راستی‌آزمایی حین‌اجرای برنامه به‌منظور جبران کمبودهای این دو رویکرد می‌تواند بکار گرفته شود و مکملی برای این دو روش باشد[۷, ۸]. بنابراین پیشنهاد ما در این پژوهش استفاده از رویکرد آزمون و/یا وارسی رسمی است، اما از آنجا که نمی‌توان به رفتار برنامه بطور کامل اطمینان داشت، در نتیجه باقیمانده خطاهای موجود در برنامه از طریق رویکرد راستی‌آزمایی حین‌اجرا، شناسایی و از رفتار سوء برنامه پیش‌گیری شود.

هدف روش راستی‌آزمایی حین‌اجرای برنامه، مشاهده رفتار برنامه برای بررسی رفتار درست برنامه در حین اجرای آن می‌باشد. در حقیقت بررسی این‌که اجرای برنامه خصوصیات مشخصی را حفظ

---

[1] Research Triangle Institute
[2] Theorem Proving
[3] Model checking
[4] State Space Explosion

می‌کند یا خیر. تعاریف متفاوتی در متون علمی برای راستی‌آزمایی خطای حین اجرای برنامه ارائه شده است[٤]. تعریفی که در بین اکثر آن‌ها مشترک می‌باشد، عبارت است از:

"یک راستی‌آزما[1] برنامه‌ای است که رفتار برنامه را در حین اجرای آن راستی‌آزمایی کرده و تعیین می‌نماید آیا برنامه با ویژگی‌های داده شده همخوانی دارد؟"[٤].

برای راستی‌آزمایی رفتار برنامه در حین اجرای آن با هدف اطمینان از اجرای درست آن با توجه به مسئولیت‌های بیان شده برنامه، ابتدا می‌بایست انواع ویژگی‌های قابل راستی‌آزمایی را مورد بررسی قرار داد. ویژگی‌های برنامه شامل دو نوع سلامت[2] و ایمنی[3] هستند که ویژگی‌های سلامت اتفاق خوبی که باید در برنامه رخ دهد را مشخص می‌کنند و با توجه به این‌که این نوع ویژگی‌ها خطرات جدی ندارند و تلاش می‌شود در روش‌های رسمی و آزمون نرم‌افزار این ویژگی‌ها حتی الامکان بررسی شوند و راستی‌آزمایی حین‌اجرای آن‌ها هزینه سربار بالایی دارد، لازم نیست که در زمان اجرا راستی‌آزمایی شوند[۹, ۱۰].

ویژگی‌های ایمنی نیز که در صورت نقض، باعث ناهنجاری رفتار برنامه می‌شوند از اهمیت فوق‌العاده‌ای در تمام برنامه‌های حساس به ایمنی برخوردارند. بنابراین در این پژوهش تنها ویژگی‌های ایمنی در زمان اجرا راستی‌آزمایی می‌شوند. البته اگر در برنامه‌ای سربار ناشی از راستی‌آزمایی حین‌اجرای ویژگی‌های سلامت قابل تحمل باشد، می‌توان تمامی یا تعدادی از ویژگی‌های سلامت را نیز حین‌اجرا راستی‌آزمایی نمود. ویژگی‌های ایمنی می‌توانند به روش‌های مختلفی مانند جبر، آتاماتاو منطق[۱۱] بیان شود که با توجه به نوع برنامه مورد راستی‌آزمایی تعیین می‌گردد[٤, ۱۲].

با توجه به این‌که برنامه‌های واکنشی بی‌درنگ، معمولا حیاتی هستند، درنتیجه در بیان این‌گونه برنامه‌ها نباید ابهام وجود داشته باشد. به‌همین دلیل از روش‌های رسمی برای بیان خصوصیات و رفتار این‌گونه برنامه‌ها استفاده می‌شود[۷]. روش بکارگرفته شده در این پژوهش، منطق بی‌درنگ[4] و منطق بی‌درنگ رویدادگرا[5] می‌باشد که به‌صورت رسمی ویژگی‌های ایمنی برنامه را بیان نموده و با

---

[1] Monitor
[2] Liveness
[3] Safety
[4] Real-Time Logic (RTL)
[5] Event-based Real-time Logic (ERL)

توجه به این‌که در زمان اجرا راستی‌آزمایی می‌شوند و تمامی پارامترهای ویژگی‌های ایمنی مقادیر ثابت است، قابل تصمیم‌گیری می‌باشند.

۱-۳- اهداف و نتایج حاصل از پژوهش

هدف از انجام این پژوهش فائق آمدن بر مشکلاتی است که روش‌های معمول وارسی و اعتبارسنجی برنامه‌ها دارند. این روش‌ها که شامل آزمون برنامه و وارسی رسمی (بازبینی مدل و اثبات قضیه) هستند، نمی‌توانند درستی اجرای برنامه را بطور کامل تضمین کنند. بنابراین برای این‌که اجرای درست برنامه بطور کامل تضمین شود، روشی برای راستی‌آزمایی حین‌اجرای برنامه‌های واکنشی بی‌درنگ تدوین و طراحی می‌گردد و با دو منطق زمانی RTL و ERL درستی این روش بررسی می‌شود. در این پژوهش، از رویکرد جنبه‌گرا[1] در بخش ابزارآمایی[2] برنامه‌های واکنشی بی‌درنگ برای راستی‌آزمایی حین‌اجرای این دسته از برنامه‌ها استفاده می‌شود.

چارچوبی برای راستی‌آزمایی حین‌اجرای برنامه‌های واکنشی بی‌درنگ ارائه شده است، که کار راستی‌آزمایی حین‌اجرا را در سه فاز انجام می‌دهد. دو فاز اول قبل از زمان اجرا انجام می‌شوند، اما فاز سوم در حین اجرای برنامه انجام می‌گردد. فاز اول، ویژگی‌های ایمنی[3] را از مشخصات خواسته‌های برنامه استخراج می‌نماید و پس از استانداردسازی، به ازای هر ویژگی، رفتار تحمل پذیری[4] در برابر نقض آن تعیین می‌گردد. در فاز بعد، عمل ابزارآمایی ویژگی‌ها داخل کد برنامه انجام می‌شود. در این فاز، جنبه‌های عملیاتی، زمانی و ضرب‌الاجل تولید شده و توسط بافنده به کد برنامه افزوده می‌شوند. کد ابزارآمایی شده پس از ترجمه[5] در محیط اجرا می‌شود. در فاز سوم نیز راستی‌آزمایی حین‌اجرای برنامه در محیط انجام می‌گیرد.

نتایج حاصل از این پژوهش عبارتند از:

- چارچوب پیشنهادی، مستقل از زبان بیان ویژگی، زبان برنامه‌نویسی یا سیستم‌عامل می‌باشد. البته زبان بیان ویژگی‌ها باید نوعی از منطق‌زمانی باشد. این چارچوب با دو روش بیان ویژگی RTL و ERL بررسی شده است. RTL توانایی بیان قیدهای زمانی نظیر تاخیر و ضرب‌الاجل و

---

[1] Aspect Oriented Programming
[2] Instrumentation
[3] Safety Property
[4] Fault Tolerant
[5] Compile

مشخص سازی دفعات وقوع یک رخداد را دارد. علاوه بر این، RTL دارای قدرت تشریح بالا و سادگی فرمول‌نویسی است. از طرفی ERL دارای بیانی سطح بالا است به‌طوری‌که قیدهای منطق زمانی به‌راحتی با ERL بیان می‌شوند. این سادگی بیان، باعث شده است که فرمول‌های ERL به‌صورت کوتاه نوشته شوند. به‌عبارت دیگر، فرمول‌های ERL دارای قدرت خوانایی بسیار زیادی است.

- در چارچوب پیشنهادی، راستی‌آزما با برنامه تحت راستی‌آزمایی تجمیع شده و به‌صورت یک برنامه واحد اجرا می‌شود و در صورت نقض هرکدام از ویژگی‌های ایمنی، اجرای برنامه متوقف شده و برنامه به وضعیت امنی هدایت می‌شود.
- مشکل اصلی روش‌های جاری راستی‌آزمایی برنامه‌های واکنشی بی‌درنگ، به‌علت حیاتی و حساس بودن آن‌ها، عدم راهبری و هدایت به یک وضعیت امن بعد از تشخیص نقض ویژگی است، اما در چارچوب پیشنهادی علاوه بر تشخیص نقض ویژگی‌ها، عمل تحمل‌پذیری در برابر نقض ویژگی نیز انجام می‌شود.
- استفاده از رویکرد جنبه‌گرایی باعث کاهش پیچیدگی راستی‌آزمایی حین‌اجرای برنامه شده، در نتیجه تولید راستی‌آزما و نگهداری آن آسانتر شده است.

برای نشان دادن عملکرد درست روش ارائه شده، برنامه گذرگاه راه‌آهن پیاده‌سازی شد و روش ارائه شده روی آن اعمال شد. آزمایشاتی روی نمونه مدل‌سازی شده انجام گردید و با رویکردهای مشابه مقایسه شد. در آزمایشات که به‌صورت جداگانه انجام گرفته است، مشخص گردید که چارچوب ارائه شده سربار ٤٪ تا ٣٣٪ را به برنامه اضافه می‌کند که به‌راحتی با افزایش توان سخت‌افزاری قابل جبران است.

١-٤- مروری بر فصول پایان نامه

این پایان‌نامه مشتمل بر هفت فصل است که در فصل اول به بیان کلیاتی از پژوهش پرداختیم. مقدمه فصل ضرورت این پژوهش و کاربردهای آن‌را متذکر می‌شود. بخش بعد به بیان مسئله و مشکلات پیش روی اختصاص دارد. در این بخش روش‌های متداول اعتبارسنجی برنامه‌های واکنشی بی‌درنگ مورد بحث قرار گرفتند. سپس اهداف پژوهش مطرح شد. نتایج پژوهش نیز که شامل روش ارائه شده و ویژگی‌های این روش است، شرح داده شد.