Сведения о выполненных работах в 2016 году
по проекту **«Надежность, безопасность и доверие в системах, используемых в качестве сервисов: масштабируемые решения для эффективного анализа и менеджмента»,** поддержанному Российским научным фондом

Соглашение № 16-49-03012

Руководитель д-р техн. наук Евтушенко

В 2016 г. научная группа ТГУ исследовала параметры надежности, безопасности и доверия в сервисных системах или системах SaS, которые можно эффективно синтезировать и анализировать на основе классических и неклассических (полу)автоматных моделей. Основные результаты 2016 года сгруппированы по рабочим пакетам WP1-WP5.

WP1: исследованы отношения между «классическими» проблемами логического синтеза и верификации и существованием синхронизирующих, установочных и различающих последовательностей для классических и неклассических конечных (полу)автоматов. В рамках рабочего пакета WP1, посвященного эффективным манипуляциям с конечно автоматными моделями с целью синтеза умозрительных экспериментов с классическими и неклассическими (полу)автоматами, в 2016 году были получены следующие основные результаты.

1) Метод проверки существования и синтеза для детерминированных полностью определенных автоматов различающих, синхронизирующих и установочных последовательностей (если таковые существуют) с использованием масштабируемых представлений в виде логических схем.

2) Программная реализация части предложенных методов проверки существования и синтеза умозрительных экспериментов на основе логических схем и результаты компьютерных экспериментов с использованием разработанного программного обеспечения с серией контрольных примеров (бенчмарок) из пакета ITC'99. При синтезе различающих последовательностей рассматривались схемы-мутанты, построенные внесением неисправностей трех типов: одиночные константные неисправности, неисправности «перемычек» и трудно обнаружимые неисправности при замене единичного набора вентиля схемы. В результате экспериментов строились различающие последовательности для каждого класса неисправностей, и оценивалась их длина. Различающие последовательности для пары начальных состояний автоматов, реализуемых схемами из пакета ITC’99, оказались достаточно короткими. Коллеги из ИСП РАН провели эксперименты по качеству построенных различающих последовательностей для покрытия переходов исходного расширенного автомата. Эксперименты показали, что для исходного расширенного автомата построенные различающие последовательности «покрывают» почти все простые пути, т.е. множество различающих последовательностей, построенное на «уровне» логических схем, может быть применимо на более высоком уровне абстракции.

WP2: пакет посвящен исследованию параметров надежности для неклассических конечных (полу)автоматов и алгоритмам синтеза проверяющих тестов с гарантированной полнотой для недетерминированных, расширенных и временных автоматов. В рамках пакета WP 2 были получены следующие результаты.

1) Определен список основных параметров надежности систем SaS, которые могут быть проверены с использованием моделей с конечным числом переходов. К этим параметрам относятся: корректность функционирования, робастность системы, возможность восстановления системы после сбоя работы, чрезмерное потребление ресурсов реализацией сервисной системы.

2) Метод повышения полноты тестов, построенных по расширенному автомату. Полнота теста повышается за счет использования мутационного тестирования на основе инструмента mjava для программной реализации, выполненной по специальному шаблону. Предварительные эксперименты с рядом технических систем подтверждают, что такие тесты находят значительно больше функциональных ошибок в программных реализациях.

3) Метод построения адаптивной проверяющей последовательности для недетерминированных автоматов относительно редукции при условии, что автомат-реализация является детерминированным. Установлены достаточные условия, при которых предложенная адаптивная стратегия является исчерпывающей относительно всех возможных автоматов-реализаций.

4) Метод синтеза (адаптивных) проверяющих тестов с гарантированной полнотой для временных недетерминированных автоматов относительно редукции (для детерминированных автоматов относительно эквивалентности) в предположении, что известны максимальное число состояний проверяемого автомата и максимальная конечная граница для входных временных интервалов. Метод основан на построении соответствующей конечно автоматной абстракции временного автомата и дальнейшем использовании автоматных методов синтеза тестов с гарантированной полнотой. Показано, каким образом построенный тест можно существенно сократить, если все входные временные интервалы автомата-спецификации и автомата-реализации закрыты слева (или все интервалы закрыты справа). Дальнейшее сокращение проверяющего теста возможно за счет сокращения переходов в спецификации, т.е. за счет уменьшения степени недетерминизма спецификации. Несмотря на то, что в последнем случае построенный тест «перестает» быть полным относительно рассматриваемой модели неисправности, предварительные эксперименты показывают, что его полнота остается достаточно высокой.

WP3: исследованы параметры для масштабируемых представлений (неклассических) автоматов, влияющие на безопасность и робастность веб-приложений. В рамках пакета WP3 были получены следующие основные результаты.

1) Определен список параметров, влияющих на безопасность изолированного web-приложения, поведение которого может быть описано конечно автоматной моделью. К этим параметрам относятся: превышение максимально допустимого значения внутренней переменной; достижимость критических ситуаций, потеря запроса/ответа, робастность, устойчивость к угрозам (утечки памяти, SQL-инъекции и др.), состязания между пользователями. Сервисные системы могут быть адекватным образом промоделированы подходящими недетерминированными, возможно, ненаблюдаемыми автоматами; далее может быть синтезирован проверяющий тест для проверки корректной реализации критических (с точки зрения параметров безопасности) переходов.

2) Для совместной работы веб-приложений установлены достаточные условия для обнаружения тупиковых ситуаций и осцилляций в композиции конечных автоматов, если компоненты композиции являются детерминированными, возможно, частичными автоматами, и предложен двухэтапный алгоритм для определения тупиковых ситуаций. Предложен более простой подход, чем ранее известные, к построению композиций автоматов с таймаутами. После того как построена параллельная композиция подходящих автоматных моделей для SaS, композиция может эффективно анализироваться для проверки критических свойств безопасности.

WP4: исследованы параметры сервисных систем, которые влияют на поведение компоненты и методы синтеза тестов для формирования данных при прогнозировании уровня доверия на основе проверки функционирования. В рамках WP4 получены следующие основные результаты.

1) Предложен подход упреждающей оценки доверия, который содержит два основных этапа. Первый этап заключается в определении параметров, которые могут повлиять на доверие к системе (потенциально «чувствительные» параметры доверия, которые могут быть получены от экспертов). Второй этап основан на «извлечении» значений чувствительных параметров доверия по анализу исходного кода исследуемой системы и при подаче построенных тестов.

2) Для оценки доверия предложен подход на основе методов и средств активного тестирования. Идея предлагаемого подхода заключается в том, чтобы влиять на поведение тестируемой реализации за счет подачи конкретных входных сигналов, которые могут «заставить» тестируемую систему показать себя как не заслуживающую доверия. Тестовые наборы, на которых проверяется поведение тестируемой системы, могут быть получены различными способами, начиная от случайного моделирования, методов и средств статического анализа и заканчивая типовыми методами генерации тестов на основе формальных моделей.

WP5: исследованы параметры, необходимые для выполнения функциональных и нефункциональных требований и новые методы к доопределению систем частичных булевых функций для получения оптимальных (или близких к оптимальным)

логических схем (относительно предсказания уровня удовлетворенности конечного пользователя). В рамкахWP5 получены следующие основные результаты.

1) Исследованы параметры различных электронных сервисов, имеющих наибольшее влияние на удовлетворенность конечного пользователя. Отмечено, что параметры, необходимые для выполнения функциональных и нефункциональных требований, определяются индивидуально для каждого сервиса (или групп сервисов). Оценка удовлетворенности конечного пользователя QoE в мультимедийных системах обычно производится на основе сетевых параметров; к таким параметрам относятся, например, число потерянных пакетов при передаче данных (packet loss), а так же «дрожание» транслируемого изображения (jitter). Для OTT (Over-the-Top) сервисов, передающих по телекоммуникационной сети некоторое видео по требованию пользователя и не отвечающих за качество связи и другие сетевые параметры, критическими можно считать количество данных, передаваемых в единицу времени, или битрейт, время буферизации видео, «замерзание» изображения (freezing events), т.е. количество «заморозок» и общее/максимальное время такой «заморозки»/буферизации. С ростом развития концепции «Интернет вещей» (Internet of Things или IoT) все большее внимание уделяется нефункциональным параметрам, в частности, бизнес-параметрам, а также параметрам, связанным с влиянием на окружающую среду, в частности, потреблением ресурсов, и т.п.

2) Предложен метод доопределения системы частичных булевых функций для получения оптимальных (или близких к оптимальным) логических схем (относительно предсказания уровня удовлетворенности пользователя). Метод опирается на использование самообучающихся систем для предсказания/оценивания QoE, основанных на дереве решений (Decision Tree), одним из масштабируемых представлений которого являются логические схемы. Оптимизация логической схемы осуществляется за счет «оптимального» или близкого к нему доопределения системы частичных булевых функций, соответственно, в рамках WP5 был предложен метод такого доопределения (с использованием системы проектирования и верификации логических схем ABC). На основе предлагаемого подхода с использованием логических схем были продолжены эксперименты для предсказания результативности обучения иностранному языку по выбранной методике. Предварительные эксперименты с обучающей и тестовой выборками показали, что в 88% оценочные значения определились корректно с допустимой погрешностью предсказания, что свидетельствует о достаточно хороших перспективах использования описанных выше критериях оптимизации логических схем.

3) Предложен подход к оптимизации потребления энергии, затрачиваемой при использовании встроенного программного обеспечения, основанный на манипуляциях с моделями с конечным числом состояний/переходов, которые могут быть получены по исходному программному коду. В качестве критерия оптимизации рассматривается сетевая нагрузка при использовании различных программных реализаций сетевых компонентов, в частности, при различной реализации сетевых

протоколов. Соответственно, был предложен подход, основанный на оптимизации исходного кода с использованием модели взвешенного древовидного автомата (Weighted Tree Automata или WTA). Метод содержит правила выбора весов для переходов автомата с целью оптимизации сетевых обменов для снижения энергопотребления/нагрузки сети. После того, как все функции записи или чтения (на переходах WTA) сгруппированы, выбирается оптимальная последовательность доступных замен для регулярных цепочек. Предложенный подход может оказать существенное влияние на энергопотребление, например, при использовании аппаратных компонентов, реализующих алгоритмы шифрования.

При выполнении работ по проекту в 2016 г. сделаны 6 докладов на международных конференциях с публикацией докладов в изданиях, входящих в Scopus и Web of Science, опубликованы 4 журнальные статьи. Для эффективного обмена результатами, полученными при выполнении проекта в 2016 г., для их анализа и обобщения проведен совместный семинар (Национальный университет Тайваня, Тайбэй, 2-9 декабря, 2016).