Сведения о выполненных работах в 2017 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 Нина Владимировна

В 2017 г. продолжены исследования по разработке масштабируемых методов для обеспечения критериев безопасности, надежности и доверия SaS, в соответствии с техническим заданием на проект (по рабочим пакетам WP 1-5). Кроме того, в отчетном периоде мы рассмотрели еще один тип сервисов, а именно, сервисы, направленные на эффективную обработку, передачу и хранение информации.

В рамках рабочего пакета ***WP1***, посвященного эффективным манипуляциям с конечно автоматными моделями, в 2017 году научная группа ТГУ остановилась на масштабируемом синтезе последовательностей, идентифицирующих состояния автоматов, с использованием квантифицированных булевых формул (QBF), большинство решателей для которых основаны на логических схемах, а также на получении теоретических результатов по упрощению входо-выходных полуавтоматов и временных автоматов с целью дальнейшего синтеза экспериментов, решения задач тестирования и верификации и др. Были получены следующие основные результаты.

1) Теоретические и экспериментальные результаты по синтезу установочных последовательностей на основе квантифицированных булевых формул, для которых было проведено экспериментальное исследование четырех QBF решателей, а именно, DepQBF, RAReQS, QELL и 2QBF решателя, встроенного в систему ABC. Построение адаптивной установочной/синхронизирующей последовательности опирается на эффективный синтез установочных тестовых примеров для каждой пары состояний, и, принимая во внимание результаты экспериментов по синтезу установочных последовательностей на основе QBF решателей, мы предлагаем совместить два подхода. Мы предлагаем проверить на выполнимость соответствующую QBF формулу только для пар состояний, что должно быть значительно эффективнее, чем проверять такую формулу сразу для всех состояний.

2) Предложен метод синтеза адаптивных синхронизирующих последовательностей для детерминированных неприведенных автоматов.

3) Методы построения установочных и синхронизирующих последовательностей для автоматов адаптированы для построения установочных и синхронизирующих последовательностей для входо-выходных полуавтоматов.

4) С использованием конечно автоматной абстракции предложен метод минимизации детерминированного временного автомата, который является автоматом, приведенным по состояниям и времени. Показано, что минимальная форма

детерминированного полностью определенного временного автомата единственна (с точностью до изоморфизма), т.е. может рассматриваться в качестве канонической формы такого автомата для временных автоматов.

5) Усовершенствованы программные пакеты BALM-II и FSMTest, которые используются при организации работ по пакетам WP 1–5; в пакеты добавлены новые команды и новые программные реализации, осуществляющие манипуляции над автоматами.

В отчетном году по рабочему пакету ***WP2*** было продолжено исследование корреляции между тестами для логических схем, построенными на различных уровнях абстракции, а также проведено экспериментальное исследование качества тестов, построенных на основе расширенного и временного автоматов относительно проектно-ориентированных мутантов. В 2017 году мы также рассмотрели еще один тип сервисов, а именно, сервисы, направленные на эффективную обработку, передачу и хранение информации, и исследовали подходящие в данном случае модели неисправности. Эта часть исследований (начаты в 2017 г.) относится к тестированию и верификации программируемых сетей, которые формируют «сервис по требованию» (service-on-demand). Были получены следующие основные результаты.

1) В результате проведенных экспериментов для схем из пакета ITC’99 было показано, что для логических схем тесты, построенные конечно автоматными методами, являются достаточно качественными; более того, тест, основанный на поиске кратчайшей различающей последовательности для двух схем, спецификации и мутанта, после минимизации оказался даже длиннее, чем тест, основанный на выборе псевдослучайной (различающей) последовательности. Наиболее эффективным (в смысле длины построенного теста с гарантированной полнотой) является комбинированный подход, в котором на первом этапе запускается случайная генерация; далее тест «достраивается» различающими последовательностями для обнаружения не обнаруженных ранее неисправностей.

2) В отчетном году мы использовали расширенный автомат для тестирования бизнес-параметров сервиса, предоставленного компанией Loymax, которая занимается автоматизацией программ лояльности, направленных на реализацию комплекса маркетинговых мероприятий для привлечения новых клиентов и других видов потенциального прибыльного развития. Для протокола взаимодействия кассового ПО с системой Loymax был построен расширенный автомат, по конечно автоматному срезу которого обходом графа переходов был построен тест. Анализ результатов тестирования позволил обнаружить ряд ошибок и несоответствий тестируемой реализации спецификации протокола, некоторые из которых оказались критическими, в смысле возможных финансовых убытков компаний. Отметим, что тестируемая система на момент ее анализа лишь подготавливалась к релизу; соответственно, обнаруженные ошибки были устранены до ее реализации на реальных серверах.

2) На основе модели временного автомата были проведены эксперименты по качеству тестов, построенных конечно автоматными методами для проверки функциональных

и нефункциональных требований к (встроенному) программному обеспечению (кибер) физических систем, используемых в лазерных сервисных системах, которые позволяют наблюдать за удаленными объектами и процессами, осуществлять мониторинг на линии с высокой скоростью и др. Как показали проведенные эксперименты (с использованием мутационного тестирования), для сервисных систем «генераторного» типа, тесты, построенные по таким моделям, оказываются достаточно качественными.

3) Мы также рассмотрели ошибки в реализациях телекоммуникационных протоколов, соответствующие ошибкам переходов/выходов недетерминированного автомата-спецификации. Экспериментально показано, что мутанты, соответствующие реальным ошибкам в программных реализациях протокола, достаточно часто можно обнаружить тестами полиномиальной длины с использованием новой модели неисправности, основанной на наблюдаемых проекциях. Еще одна новая модель неисправности для недетерминированных автоматов основана на сокращении автомата-спецификации таким образом, чтобы в сокращенном автомате существовала адаптивные различающая и передаточные последовательности. Предложен метод выделения из исходного автомата близкого к максимальному подавтомату с такими свойствами.

4) Исследование платформы для виртуализации сервисов и функций предполагает, что все компоненты должны быть тщательно протестированы, что, в свою очередь, требует использования не только привычных (классических) моделей неисправности, но и введения новых моделей неисправности. В этом году мы сконцентрировались на проверке цепочек сервисных функций (SFCs), которые запрашивает пользователь, сформулировали цели и задачи тестирования и предложили модель неисправности, основанную на перечислении графов.

5) На первом этапе тестирования композиция взаимодействующих систем проверяется на возможность совместного функционирования, т.е. на отсутствие осцилляций и тупиковых ситуаций. Для компактного задания множества «неисправных» композиций мы используем мутационные автоматы, полученные в результате всевозможных доопределений неопределенных переходов в каждой компоненте. Данная модель неисправности использована для композиции автоматов с таймаутами, для которой проверяющий тест строится с использованием усовершенствованного пакета BALM-II.

7) Проверка возможного достижения критических состояний и/или критических значений переменных в расширенном автомате хорошо осуществляется с использованием различных верификаторов, таких как, например, JavaPathFinder (JPF). Для реализации расширенного автомата мы используем шаблонный перенос инструкций в Java код, сохраняя все контекстные переменные, предикаты, описывающие условия переходов, и состояния расширенного автомата, соответствующие рабочему режиму. Соответственно, достижимость критических значений и/или состояний сохраняется и в шаблонной реализации. Затем, используя верификатор JPF, предназначенный для проверки многопоточных программ, мы

можем автоматически проверить, могут ли произойти опасные ситуации в проверяемом веб-сервисе. Данный подход был предложен в рамках рабочих пакетов WP 2 и 3 и был опробован на специальной группе игровых сервисов.

В рамках рабочего пакета ***WP3*** мы продолжили разработку алгоритмов для проверки безопасности веб-приложений и мобильных сервисов, в том числе, для композиций автоматов с входными и выходными таймаутами. Кроме того, были исследованы методы построения композиций временных и расширенных автоматов, проблемы, возникающие при построении таких композиций, и предложены подходы к их решению. Были получены следующие основные результаты.

1) Полученные в 2016 г. условия для анализа возможности возникновения тупиков и осцилляций в бинарной параллельной композиции конечных автоматов переформулированы для автоматов с входными и выходными таймаутами.

2) С использованием верификатора javaPathFinder для мобильных приложений (JPF-mobile) были обнаружены уязвимости в мобильных приложениях.

3) Один из способов исследования уязвимостей в веб приложениях заключается в построении полуавтомата, представляющего «опасные» последовательности символов и соответствует решению полуавтоматного неравенства или уравнения относительно операции конкатенации. Решение неравенства может привести к ложным срабатываниям, что, вообще говоря, может привести к недовольству пользователей при дальнейшей санитизации, поскольку при санитизации будет удаляться то, что на самом деле вредоносным не является. При решении полуавтоматного уравнения возможны пропуски опасных пользовательских данных. Получены новые результаты по решению полуавтоматных уравнений/неравенств относительно конкатенации, сформулированы достаточные условия, при которых полуавтоматное уравнение/неравенство не имеет решений или имеет несколько попарно не эквивалентных решений.

4) Мы также отмечаем, что в результате выполнения работ по проекту в 2017 г. показано, что в ряде случаев для описания временным автоматом совместной работы временных автоматов недостаточно условий отсутствии осцилляций и наличия медленной внешней среды. Необходимы дополнительные условия, некоторые из которых уже исследованы, другие мы продолжаем исследовать.

В рамках рабочего пакета ***WP4*** научная группа Томского государственного университета продолжает исследования в области оценивания и предсказания уровня доверия для сервисных систем. В 2017 году основной упор был сделан на так называемые устройства с ограниченными вычислительными возможностями, причем с развитием «Интернета вещей» (IoT) возрастает актуальность исследования таких устройств. Были получены следующие основные результаты.

1) Адаптация метода предсказания доверия на основе логических схем с использованием известных методов и средств машинного обучения. Предлагается при синтезе логической схемы, оценивающей уровень доверия и имеющей один выход, на

котором появляются булевы константы 0 (не доверяю) и 1 (доверяю), «консультироваться» с некоторой «идеальной» или «золотой», но недостаточно масштабируемой самообучающейся моделью, что позволит существенно усовершенствовать процесс проектирования логической схемы.

2) Выявление критических параметров для мобильных приложений и устройств с целью проектирования логической схемы для оценки уровня доверия для мобильных приложений и смартфонов с ограниченными вычислительными возможностями.

В отчетном году мы остановились на следующих динамических параметрах мобильных приложений: 1) размер «кучи» – размер занимаемой приложением памяти при ее динамическом распределении; 2) размер стека – размер памяти, занимаемой выделенным потоком приложения; 3) загрузка процессора – загрузка приложением ЦП, исчисляемая в процентах; 4) загрузка (использование) диска – пространство, занимаемое данными приложения; 5) потребление энергии – количество энергии, потребляемой приложением.

Для моделирования различных комбинаций значений параметров при вычислении уровня доверия мобильному приложению мы предлагаем использовать самообучающиеся модели. Более того, поскольку мы рассматриваем смартфоны с ограниченными вычислительными возможностями, предлагается использовать масштабируемые представления таких моделей, а именно, логические схемы. Проведенные нами предварительные эксперименты свидетельствуют, что для определенных выше параметров и ограничений на их значения описанный выше подход представляет интерес.

При оценке/прогнозировании QoE (рабочий пакет ***WP5***) мы используем масштабируемые представления, такие как логические схемы, а также различные булевы выражения, которые описываются такими схемами. Исследованы свойства логических схем, которые можно использовать для повышения их способности к предсказанию уровня удовлетворенности пользователей композитных сервисов. Кроме того, в этом году мы рассмотрели новые типы сетевых сервисов, направленных на организацию хранения и передачи информации, и определили ряд параметров, которые влияют на качество обслуживания при использовании таких сервисов. Получены следующие основные результаты.

1) Часть недостатков интервального доопределения логической схемы при прогнозировании уровня QoE (результаты 2016 г.), как и в случае прогнозирования уровня доверия, может быть устранена за счет «консультирования» при синтезе логической схемы с некоторой «идеальной» или «золотой» технологией обучения (или подходящей, но недостаточно масштабируемой самообучающейся моделью). Для двух выбранных «эталонных», но недостаточно масштабируемых самообучающихся моделей, используемых для предсказания значения QoE, мы предлагаем построить и совместить параллельно такие логические схемы. Выходные значения, снимаемые со схем-компонент, подаются на схему, вычисляющую минимальное (максимальное) значение двух целых чисел. Построенная таким

образом схема гарантирует, что предсказываемое значение QoE будет не ниже (не выше), чем значение, возвращаемое каждым из «оракулов».

2) Были также исследованы и другие возможности совмещения двух логических схем, в зависимости от их «предсказательных» способностей, при условии, что каждая из этих схем детерминирована в сторону фиксированного ответа QoE. В этом случае значение QoE параллельно вычисляется на обеих логических схемах; на выходе схемы-композиции выдается значение лишь одной из них, и для этого можно воспользоваться подходящим мультиплексором для «снятия» значений с требуемых выходов, а также переключателем для указания ситуаций, при которых выходная реакция должна «сниматься» с той или иной схемы.

3) В отчетном году мы кратко рассмотрели параметры (запросов), влияющие на качество обслуживания и, как следствие, удовлетворенность пользователя / клиента сервисами специального типа, а именно, сервисами для эффективной обработки, передачи и хранения информации. Мы идентифицируем основные параметры запросов, которые влияют на качество обслуживания пользователя, и рассматриваем функциональные или логические параметры и параметры, относящиеся к распределению ресурсов. Значения параметров первой группы проверяются с использованием масштабируемых операций над булевыми матрицами; параметры второй группы можно проверить с помощью соответствующей системы логических выражений. Для проверки качества запросов, направляемых на одну из платформ по виртуализации, мы провели эксперименты с парсером, «разбирающим» запросы в языке TOSCA, чтобы убедиться, что в настоящий момент парсер «пропускает» запросы, для которых невозможно обеспечить требуемое качество обслуживания; более того, некоторые запросы угрожают безопасности системы.

Выполнение работ по Российско-Тайваньскому проекту полностью соответствует заявленному плану исследований. Результаты, полученные в процессе выполнения работ по проекту, опубликованы в 15 работах (одна публикация совместно с научной группой Национального Университета Тайваня), в том числе, 8 – в журналах и периодических изданиях (5 входят в международные базы цитирования Scopus и Web of Science и 3 – в Перечень ВАК), 7 – в трудах международных конференций (все входят в международные базы цитирования Scopus или Web of Science); защищена 1 кандидатская диссертация (под руководством руководителя проекта РНФ).