

Предисловие

24-25 ноября 2014 года в Париже в Институте Мин-Телеком (Institut Mines-Télécom) состоялся совместный российско-французский семинар, посвященный вопросам верификации, тестирования и оценки качества программного обеспечения (Software Verification, Testing, and Quality Estimation). Семинар был приурочен к открытию совместной исследовательской лаборатории по проблемам оценки качества в открытом веб-пространстве, которую организовали Института Мин-Телеком (Франция), Институт системного программирования РАН и Томский государственный университет. Одним из направлений исследований лаборатории будет оценка качества веб-приложений – бурного растущего сектора программных приложений. Ключевое слово этого направления Quality, послужило основой для названия совместной лаборатории – Qualipso.¹

В открытии семинара приняли участие Д. Садек, директор по исследованиям Института Мин-Телеком, академик РАН В.П. Иванников, директор ИСП РАН и проректор ТГУ Д.В. Сухушин. Присутствующие официальные представители организаций-участников прокомментировали открытие совместной лаборатории.

Д. Садек, директор по исследованиям Института Мин-Телеком:

- Подписание настоящего соглашения в рамках развития международного сотрудничества позволяет нам консолидировать существующее совместное сотрудничество в образовательных и научно-исследовательских сферах, таким образом способствуя продвижению и усилению статуса Института Мин-Телеком в мире.

В.П. Иванников, директор Института системного программирования РАН:

- В настоящее время формальные методы активно используются на практике при разработке программного обеспечения. Исследователи Франции и России имеют богатый опыт в изучении формальных моделей и языков. Консолидация отношений между этими странами и учреждениями призвана стимулировать новые идеи для совместного франко-российского сотрудничества.

Д.В. Сухушин, проректор по Программам развития Томского государственного университета:

- Открытие лаборатории является итогом наших многолетних отношений и свидетельством взаимного доверия одновременно. Формат международной

¹ Проведение семинара и подготовка публикаций сотрудников и обучающихся ТГУ частично поддержаны проектом 739 госзадания МинОбрНауки РФ

сетевой лаборатории открывает для участников новые возможности по продвижению исследований в международном исследовательском сообществе. Интегрируя наши исследования, мы приобретаем конкурентное преимущество в стремлении к лидерству в приоритетном направлении исследований.

Первый доклад на семинаре сделал профессор А.К. Петренко. В своем докладе он рассмотрел современное состояние дел в области верификации операционных систем и представил стек инструментов и технологий ИСП РАН, при помощи которых ведется верификация различных операционных систем, начиная от микроядерных ОС реального времени и заканчивая модулями ядра ОС Linux и дистрибутив ОС Linux, включающих в себя до миллиона интерфейсов. Были представлены возможности различных техник верификации в контексте их применения к микроядрам размером около 10 тысяч строк на языке программирования, к модулям размером до 100 тысяч строк, к библиотекам в диапазоне размеров от тысячи до миллиона интерфейсов.

Профессор Ана Кавалли в своем докладе представила работы департамента вычислительных сетей университета Телеком Южный Париж в направлении тестирования и мониторинга веб-систем. Эта научная группа много лет работает в области использования формальных моделей для тестирования и оценки качества программного обеспечения и имеет большое количество интересных теоретических результатов и разработанных приложений. Одно из таких приложений, ММТ, созданное совместно с предприятием Монтимаж (Франция), используется в различных компаниях для мониторинга безопасности компьютерных систем.

Профессор Н.В. Евтушенко представила сообщение на тему «Nondeterministic FSMs in Model-Based Testing», в котором было отмечено, что в настоящее время для описания дискретных систем все чаще используются модели с недетерминированным поведением. Недетерминизм появляется в силу различных причин, таких как опциональность в спецификациях, уровень абстракции, ограниченные управляемость и наблюдаемость и др. В докладе были представлены различные модели неисправности на основе недетерминированных автоматов для синтеза проверяющих тестов с гарантированной полнотой относительно перечисленных моделей.

В докладе Д. Ривера, Н. Кушик, К. Фьюензалида, А. Кавалли, Н. Евтушенко «Расширенные конечные автоматы с таймаутами для оценки удовлетворенности пользователя ОТТ сервисом» авторы предлагают использовать временной расширенный автомат для оценки качества предоставляемого медиа сервиса. Используя эту модель, провайдер может найти «узкие места» в правилах распространения сервиса, а именно, в бизнес модели, и соответственно повысить свою прибыль.

Стефан Мааг в своем докладе «Тестирование MANETs на основе формальной модели» отметил, что тестирование реализаций на соответствие спецификации (тестирование конформности) является одним из необходимых этапов при разработке программного обеспечения в системах передачи информации. Применение формальных моделей позволяет автоматизировать процесс генерации тестовых последовательностей, которые будут использоваться при тестировании реальных реализаций. Однако несмотря на большое разнообразие методов в этой области, остается много нерешенных вопросов при использовании формальных моделей для тестирования протоколов маршрутизации мобильной связи (беспроводные самоорганизующиеся сети). Для понижения числа неопределенных вердиктов при пассивном тестировании, которые встречаются достаточно часто, Стефан Мааг предлагает использовать технологию, основанную на самоподобии вершин сети.

Доклады С. Прокопенко «Поиск неисправной компоненты в сети расширенных автоматов» и М. Форостьяновой «Метод синтеза тестов для программных реализаций телекоммуникационных протоколов на основе древовидных автоматов» посвящены возможности использования I -эквивалентов при построении проверяющих и диагностических тестов по модели расширенного автомата. Иными словами, для расширенного автомата строится древовидный конечный автомат, поведение которого совпадает с поведением исходного расширенного автомата на всех последовательностях длины не больше I . В докладе С. Прокопенко I -эквивалент строится для композиций мутационных расширенных автоматов, каждая из которых соответствует неисправностям в определенной компоненте. Построив диагностический эксперимент для таких I -эквивалентов, по реакции композиции, предъявленной для тестирования, достаточно часто можно определить, какая из компонент является неисправной, при условии, что неисправности возможны только в одной компоненте. В докладе М. Форостьяновой предлагается метод построения проверяющего теста на основе I -эквивалента эталонного расширенного автомата. Компьютерные эксперименты, проведенные с JAVA реализацией протокола TCP (Windows), показали, что полнота тестов для 8-эквивалента относительно мутаций mJAVA, практически совпадает с полнотой тестов, построенных известными конечно автоматными методами, которые, как известно, доставляют тесты высокого качества для протокольных реализаций.

На семинаре были представлены две тесно связанных между собой статьи И. Б. Бурдонова и А. С. Косачева «Построение прямого и обратного остова коллективом автоматов» и И. Б. Бурдонова, А. С. Косачева и В. В. Кулямина «Параллельные вычисления на графе с помощью обмена сообщениями», которые посвящены распределенным вычислениям на ориентированных графах на основе обмена сообщениями вдоль дуг между автоматами, находящимися в вершинах графа. Первая статья описывает

распределенный алгоритм извлечения структуры заранее неизвестного ориентированного графа в виде остовов для распространения сообщений от корневой вершины графа к любой другой его вершине и обратно. Во второй статье авторы предлагают алгоритм распределенного вычисления произвольной функции от мультимножества значений, которыми размечены вершины графа, использующий построенные первым алгоритмом остовы для эффективного обмена сообщениями.

В докладе Н.Г. Кушик были приведены результаты по способам понижения сложности задач, возникающих при верификации, тестировании и оценке качества программного обеспечения на основе конечных автоматов. Для понижения сложности использовались эвристики, масштабируемые представления и решение задач для определенных классов автоматов и полуавтоматов. Во второй части доклада были представлены результаты автора по понижению сложности задач, возникающих при оценке качества прикладного программного обеспечения, полученные совместно с Н. Евтушенко, Д. Парра, К. Фуензалида, Д. Ривера, Ж. Покхрел, В. Маллули.

В настоящее время активно развиваются методы синтеза тестов с гарантированной полнотой для систем, для которых важны временные аспекты, и доклады Александра Твардовский «К минимизации автоматов с таймаутами», (и М. Громова, Н. Евтушенко «К минимизации числа временных переменных во временных полуавтоматах» и Г. Кидяровой «О сравнении скорости функционирования двух временных автоматов» были посвящены анализу автоматов и полуавтоматов с временными ограничениями. В докладе А. Твардовского предложен метод минимизации автоматов с входными и выходными таймаутами. Если в некотором состоянии автомата входной символ не поступает в течение определенного времени (входного таймаута), то автомат может спонтанно перейти в другое предписанное состояние. Выходной таймаут определяет время выполнения перехода, т.е. задержку выдачи выходного символа относительно поданного входного символа. Предложенный метод доставляет приведенный автомат, т.е. автомат, в котором никакие два состояния не эквивалентны, эквивалентный исходному автомату с таймаутами. Именно для приведенных временных автоматов существуют методы синтеза тестов с гарантированной полнотой. Показывается, что в отличие от классических автоматов, автомат с таймаутами может иметь несколько приведенных форм, которые попарно не изоморфны. В докладе М. Громова были предложены достаточные условия для уменьшения числа временных переменных во временном полуавтомате без изменения его поведения. В докладе Г. Кидяровой было предложено масштабируемое представление для сравнения скорости функционирования двух временных автоматов.

В докладе О.В. Кондратьевой, А. Кавалли и Н. Евтушенко «Решение автоматных уравнений для временных автоматов относительно параллельной

композиции» рассматривается параллельная композиция автоматов с таймаутами. Предлагается способ решения уравнения для такой композиции, и, в частности, формула для наибольшего (общего) решения. Отмечается, что для нахождения общего решения уравнения для автоматов с таймаутами понятие такого автомата необходимо расширить, допустив множество выходных таймаутов на переходах автомата. На основе решения уравнения можно частично управлять качеством синтезируемой компоненты в композиции веб сервисов, в частности, оптимизировать компоненту по времени обработки информации.

В докладе В. Х. Ла и А. Кавалли «Исследование отказоустойчивой маршрутизации в беспроводных сетях» отмечается, что в настоящий момент активно развиваются мобильные сенсорные сети. Экономия ресурсов в таких сетях ограничивает возможности безопасного проектирования и использование соответствующих, устойчивых к атакам, протоколов. С другой стороны, поскольку сенсорные датчики функционируют независимо и в достаточно сложных условиях, такие сети особенно склонны к отказам и уязвимы к преднамеренным атакам. Для надежного и безопасного функционирования таких сетей, необходимо исследовать и развивать устойчивость к потенциальным вторжениям. В докладе рассматриваются два таких устойчивых протокола маршрутизации, а именно, INSENS and ITSRLP, анализируются их свойства. Моделирование и анализ быстродействия показали, что оба протокола достаточно хороши с практической точки зрения. В докладе К. Тоуми, М. Ауди, А. Кавалли «Моделирование и тестирование безопасности при взаимодействии сервисов» авторы рассмотрели известные подходы к моделированию и тестированию безопасности взаимодействия веб сервисов с использованием формальных моделей. Были предложены оценки различных технологий активного и пассивного тестирования. Полученные результаты были продемонстрированы для реальной системы с использованием методов пассивного тестирования.

В большинстве методов построения проверяющих тестов по автоматной модели рассматривается инициальный конечный автомат, и соответственно проверяющие тесты строятся как набор входных последовательностей, перед каждой из которых подается сигнал СБРОС, переводящий автомат в начальное состояние. Если последний является достаточно дорогим, то имеет смысл попытаться построить одну последовательность, которая позволяет выяснить, является ли проверяемая реализация конформной спецификации. В докладе А. Ермакова «Построение проверяющих последовательностей для недетерминированных автоматов» предлагается алгоритм синтеза адаптивной проверяющей последовательности, при условии, что исходный автомат обладает разделяющей последовательностью и детерминированным сильно связным подавтоматом, что гарантирует, что только автомат, изоморфный некоторому подавтомату спецификации с тем же числом состояний, может быть редукцией автомата-спецификации. Кроме того, предполагается, что

процесс тестирования является адаптивным, т.е. следующий входной символ определяется по выходной реакции тестируемой реализации на предыдущие входные символы. За счет адаптивного подхода к тестированию длина теста может оказаться более короткой, чем длина тестовых последовательностей, построенных заранее до начала процесса тестирования. Кроме того, отмечается, что, поскольку проверяющая последовательность подается адаптивно, условия для автомата-спецификации могут быть ослаблены; в частности, вместо детерминировано достижимых состояний можно использовать определенно-достижимые состояния и соответствующие преамбулы, а вместо разделяющей последовательности - различающий тестовый пример, если таковые существуют в автомате-спецификации.

В докладе Х. Лопега, С. Маага, Ж. Моралеса «Масштабируемый метод оценки для систем управления доверием на основе распределенных систем онлайн мониторинга» рассматриваются многокомпонентные (композиционные) системы, которые становятся все более популярными, и требования к их взаимодействию постоянно повышаются. Соответственно, в таких системах можно разрешить выполнение только тех действий, которым можно доверять; причем решение, с кем и на каких условиях взаимодействовать, принимает каждая (под) система самостоятельно. В докладе авторы сфокусировались на вердиктах доверия, которые «выносятся» на основе поведения агентов и распределенного он-лайн мониторинга сети. Это дает возможность обеспечить управление доверием в системе с точки зрения опыта конкретной подсистемы, при условии, что анализируется так называемое «мягкое доверие». Предлагается масштабируемый метод для он-лайн оценки/анализа доверия с использованием дополнительной модели расширенного полуавтомата и методы понижения оценки времени на основе известных результатов.

В заключение семинара были обсуждены планы мероприятий, которые будут проводиться в рамках работ совместной исследовательской лаборатории Qualipso. Данный сборник содержит статьи, которые были написаны по результатам большинства представленных на семинаре докладов.

Заведующая кафедрой Информационных технологий
в исследовании дискретных структур ТГУ,
заведующая лабораторией Компьютерных наук,
профессор

Н.В.Евтушенко

Заведующая отделом Сетевого программирования
института Телеком, Южный Париж, профессор

Ана Р. Кавалли

Заведующий отделом Технологий
программирования ИСП РАН,
профессор

А.К.Петренко