Отзыв
на автореферат диссертации Терёхиной Ирины Юрьевны на тему: «Методы выявления аномалий в условиях смеси технологических процессов, сопровождающих наблюдаемый объект», представленной на соискание ученой степени кандидата физико-математических наук по специальности 2.3.6 — «Методы и системы защиты информации, информационная безопасность»

В диссертационной работе Терёхиной И. Ю. рассматривается задача обнаружения аномалий в функционировании технологических процессов. Задача обнаружения аномалий разбивается на две подзадачи: 1) построение модели процесса по журналам (логам) работы информационной системы — линейным последовательностям событий, которые задают допустимые исполнения процесса; 2) поиск аномалий, где под аномалией понимается несоответствие некоторого исполнения процесса уже построенной математической модели.

В рамках работы рассматриваются два крупных класса моделей, для которых были получены новые научные результаты:

1. Модели, заданные сетями Петри. Известно, что такие модели имеют множество применений в области распределенных систем, а также обладают большой выразительной мощностью. Тем не менее, как показано в работе, использование их в контексте рассматриваемой задачи весьма затруднительно. Данный результат вполне соотносится с интуитивным представлением о допустимых областях применения сетей Петри и практикой их использования. Тем не менее, формализация этого представления и строгое доказательство — один из результатов теоретической значимости, полученных в данной диссертации впервые.

2. Модели на базе ациклических ориентированных графов, на которые налагаются определенные условия (полноты, неизбыточности и минимальности). Научная новизна работы в разрезе данного класса моделей заключается в том, что впервые рассматривается существенное расширение результата, полученного ранее Р. Агравалом и др., которое позволяет моделировать поведение наблюдаемого объекта не только в сопровождении одного, а в сопровождении сразу нескольких процессов (смеси) в рамках одного журнала исполнений. Автором впервые построены эффективные алгоритмы решения сформулированных задач в рамках данной модели, для которых строго доказана оценка их вычислительной сложности.

Решение задачи, рассматриваемой в работе, представляется рецензенту актуальным с практической точки зрения. Дело в том, что данные результаты востребованы для разработки программных продуктов для обеспечения информационной безопасности информационных систем, таких как сетевые экраны для защиты веб-приложений (англ. WAF, web application firewall). Современные программные продукты данного класса обладают большим количеством функциональных возможностей, а некоторые отечественные решения даже обладают уникальными возможностями интеллектуального анализа функционирования приложений на уровне бизнес-логики. Тем не менее, даже глубокого структурного разбора отдельных запросов пользователей к защищаемому веб-приложению и соотнесение их с соответствующими бизнес-действиями недостаточно для обнаружения аномалий на более высоком уровне, учитывающем структуру процессов, реализуемых взаимодействием пользователей с веб-приложением.

Применимость работы в данной области наглядно демонстрирует диаграмма Хассе частичного порядка допустимых действий, совершаемых в многопользовательском приложении, представленная на рис. 9 в тексте диссертации, которая является типичным примером того, как может быть устроено допустимое взаимодействие пользователя с модельным веб-приложением на уровне абстракции, соответствующей бизнес-процессам.

Более того, востребованы именно эффективные алгоритмы решения данной задачи с точки зрения вычислительной сложности, поскольку обучение моделей по историческим данным и поиск аномалий в веб-трафике в реальном времени происходят в условиях существенного количества пользователей, суммарно выполняющих большое количество запросов в секунду.

Таким образом, результаты, полученные в работе Терёхиной И. Ю., во-первых, закрывают потребность в таких алгоритмах и анализе их вычислительной сложности (скажем, временная сложность алгоритма проверки трассы для модели на базе ориентированных ациклических графов, представленная в работе, является линейной относительно длины проверяемой трассы, что наилучшим образом подходит для анализа веб-трафика в реальном времени), а во-вторых, отсекают заведомо бесплодные попытки использования прочих известных моделей (в данном случае, сетей Петри) в рамках подобных предметных областей с присущими им особенностями и ограничениями.

К тексту автореферата имеется ряд замечаний:

1. Отсутствие замкнутости в формулировках некоторых теорем и лемм, часть контекста и условий приходится восстанавливать по обрамляющему тексту. Например, для понимания содержательного смысла теоремы 1 (соответствующей теореме 2.2 в тексте диссертации) требуется прочитать обрамляющий пояснительный текст.

2. Некоторые утверждения (теоремы 3, 5, 7, 9 и 11, а также теоремы 2, 4, 6 и 8) о вычислительной сложности алгоритмов имеют общую повторяющуюся структуру, что затрудняет их первоначальное чтение и понимание, поэтому было бы удобно либо реорганизовать текст таким образом, чтобы естественным образом устранить дублирование, либо же представить сводные результаты для различных случаев и ограничений в виде таблицы.

3. В тексте имеются незначительные опечатки, не искажающие смысл работы.

Перечисленные замечания носят редакционный характер, являются легко исправляемыми и не влияют на общую положительную оценку диссертации. Содержательно, работа Терёхиной И. Ю. представляет из себя научно-исследовательскую работу высокого качества, обладающую научной новизной, имеющую не только теоретическую, но и прикладную значимость.

Учитывая все вышеизложенное, считаю, что Терёхина Ирина Юрьевна заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 2.3.6 — «Методы и системы защиты информации, информационная безопасность».

Директор по разработке Хашаев Артур Акрамович
ООО «СолидСофт»

21 октября 2024 г.

Адрес: 17312, Россия, Москва, ул. Вавилова, д. 47А.
Тел.: +7 (499) 705-76-57, электронный адрес: info@solidwall.ru

Подпись Хашаева Артура Акрамовича заверяю.
Генеральный директор ООО «СолидСофт» Гамаюнов Д. Ю.