

Институт вычислительных технологий СО РАН

**XVIII Всероссийская конференция
молодых учёных
по математическому моделированию
и информационным технологиям**

Программа

Тезисы докладов

Алфавитный указатель участников

Иркутск

21–25 августа 2017 г.

УДК 004, 519.6
ББК 22.19, 32.81
М34

Материалы XVIII Всероссийской конференции молодых учёных по математическому моделированию. г. Иркутск, Россия, 21–25 августа 2017 г. — Новосибирск: ИВТ СО РАН, 2017. — 112 стр.

Целью конференции является обсуждение актуальных результатов исследований молодых научных сотрудников, аспирантов и студентов старших курсов в области вычислительной и прикладной математики и информатики. Участие в конференции дает возможность молодым ученым получить представление о результатах исследований в области современного математического моделирования, вычислительных и информационных технологий, установить научные контакты, а также познакомиться с широким кругом проблем, представленных в докладах участников.

В рамках работы конференции представлены следующие тематические направления: математическое моделирование; численные методы и методы оптимизации; высокопроизводительные и распределённые вычисления; информационные и геоинформационные системы; управление, обработка, защита и хранение информации; автоматизация и теория управления.

Организаторы конференции:

- Институт вычислительных технологий СО РАН
- Институт динамики систем и теории управления СО РАН
- Институт вычислительной математики и математической геофизики СО РАН
- Институт вычислительного моделирования СО РАН
- Новосибирский национальный исследовательский государственный университет
- Новосибирский государственный технический университет
- Сибирский государственный университет телекоммуникаций и информатики

Ответственные за выпуск: Есипов Д. В., Гусев О. И.

[3] МАССЕЛЬ Л. В., МАССЕЛЬ А. Г. Методы и средства ситуационного управления в энергетике на основе семантического моделирования // V Международная конференция OSTIS. Минск: БГУИР. — 2015. — С. 199–204.

2.32. Кулясов Н.В. Инструменты определения угроз безопасности информационных систем.

Последние несколько десятилетий идёт непрерывная интеграция информационных технологий в жизнь общества, этот процесс непосредственно взаимосвязан с расширением ИТ инфраструктуры, обеспечивающей хранение, обработку и и передачу увеличивающихся объёмов информации. Также этому сопутствует увеличение количества инцидентов, связанных с информационной безопасностью [1], исходя из чего исследования в области определения угроз являются актуальными.

Согласно исследованию лаборатории Касперского о тенденциях киберугроз информационной безопасности [2], одной из наиболее распространённых являются сетевые киберугрозы, рассмотрим их подробнее.

Для обнаружения сетевых угроз существуют различные методы и средства. Наиболее актуальные данные о методах обнаружения были получены в работе [3], автор разделил существующие методы на следующие группы: поведенческие методы; методы на основе знаний; методы машинного обучения; методы вычислительного интеллекта (нейронные сети); гибридные методы;

Основные средства обнаружения, которые поддерживают один и более методов, представлены следующими классами: межсетевые экраны (firewall); системы обнаружения вторжений (Intrusion Detection System); системы предотвращения вторжений (Intrusion Prevention System); системы управления событиями информационной безопасности (Security information and event management).

В ходе работы [4] были рассмотрены системы из каждого класса и установлена узкая специализация каждой. На основе этого был сделан вывод: комплексную защиту можно организовать только используя совокупность нескольких систем одновременно, это приводит к необходимости развертывания и администрирования нескольких программных продуктов, а зачастую и аппаратных сред, что отрицательно сказывается на надёжности и трудозатратности системы в целом.

Список литературы

- [1] Марков Р. А., Бухтояров В. В., Попов А. М., Бухтоярова Н. А. Исследование нейросетевых технологий для выявления инцидентов информационной безопасности // Молодой ученый. — 2015. — № 23, С. 55–60.
- [2] Киберугрозы и информационная безопасность в корпоративном секторе: тенденции в мире и в России.

Адрес доступа: http://www.kaspersky.ru/images/kaspersky_global_it_security_risks_survey2.pdf

- [3] Браницкий А. С. Анализ и классификация методов обнаружения сетевых атак // Тр. СПИИРАН. — 2016. — № 45, С. 207–244.
- [4] Кулясов Н. В. Система распознавания интернет угроз по журналам веб-сервисов // Молодой Учёный. — 2015. — № 11, С. 79–83.

2.33. Лисовская Е.Ю., Моисеева С.П., Галлилейская А.А. Моделирование процессов передачи данных с помощью СМО требований случайного объема

Системы массового обслуживания (СМО) требований случайного объема имеют применение при анализе современных телекоммуникационных и компьютерных сетей, и являются одним из основных аналитических инструментов оценки производительности сети. В частности, они используются для моделирования процессов, происходящих в узлах сетей [1]. Однако аналитические результаты были получены лишь в предположении, что входящий поток (в.п.) является пуассоновским.

При проектировании сетей передачи данных, инфокоммуникационных систем характеристики бесконечнолинейных СМО позволяют определить необходимое количество линий связи, чтобы избежать потери. Авторами данной работы проведено исследование таких систем с непуассоновскими в.п. (МАР, ММРР, рекуррентный). Для таких систем показано, что в условии высокой интенсивности в.п. суммарный объем требований в системе имеет гауссовское распределение [2]. Имитационное моделирование и численный анализ позволили определить область применимости аппроксимации [3].

В настоящее время авторами проводится исследование двухфазных СМО требований случайного объема. Такие СМО представляют собой последовательную обработку требований (после окончания обслуживания на первой фазе требование переходит на вторую).

Исследование выполнено при частичной финансовой поддержке РФФИ в рамках научного проекта № 16-31-00292.

Список литературы

- [1] ТИХОНЕНКО О., КЕМРА W.M. Performance evaluation of an M/G/n-type queue with bounded capacity and packet dropping // International Journal of Applied Mathematics and Computer Science. — 2016. — Vol. 26, No 4, P. 841–854.
- [2] Колбасова В. А., Лисовская Е. Ю., Моисеева С. П. Суммарный объем заявок в бесконечнолинейной системе массового обслуживания с рекуррентным входящим потоком // Материалы Девятой международной научной конференции «Распределенные компьютерные и телекоммуникационные сети: управление, вычисление, связь (DCCN-2016)»: в 3 томах. — 2016. — С. 248–255.

[3] Лисовская Е. Ю., Paganò M. Имитационное моделирование системы массового обслуживания требований случайного объема // Труды 12-й Международной Азиатской школы-семинара «Проблемы оптимизации сложных систем». — 2016. — С. 352–357.

2.34. Лычев А.В., Проничкин С.В. Динамические сетевые модели анализа среды функционирования организационных систем

Сложные организационные системы состоят из множества взаимосвязанных элементов. Оценка эффективности таких систем с учетом их динамических и комплексных характеристик является актуальной в экспертных и интеллектуальных системах поддержки принятия решений [1]. Существующие подходы к разработке моделей оценки эффективности сложных систем, основанные на принципах моделирования среды их функционирования [2], ограничены общностью их моделирования.

В настоящее время существует два основных подхода к разработке динамических сетевых моделей анализа среды функционирования, а именно прямой и обратный. Обратный подход основан на специальных сетевых срезах информации [3], который является очень чувствительным к искажениям данных и весьма трудоёмок с вычислительной точки зрения, и таким образом он менее распространен на практике, чем прямой подход.

Прямой подход более устойчив к искажениям данных, находит более широкое применение и обладает свойствами вычислительной эффективности. Тем не менее, существующие прямые и обратные методы, по-прежнему нуждаются в предварительном наборе весовых коэффициентов показателей эффективности, что создает определенные трудности для лиц, принимающих решения.

На основе проведенного исследования существующих подходов к оценке эффективности сложных динамических организационных систем на основе методологии анализа среды функционирования предложен более адекватный подход к моделированию их эффективности.

В отличие от существующих подходов предлагаемый не зависит от набора заданных весов, используемых в свертках отдельных оценок эффективности компонентов сложных систем. В нашем подходе набор весов генерируется эндогенно на основе статистических данных различных перспектив развития системы с несколькими элементами и периодами функционирования. Такой подход к моделированию существенно отличается от существующих, поскольку представляет пост-декомпозицию общей эффективности на основе эндогенной взаимосвязи между переменными, связанными с ограничениями компонентов и системными ограничениями. В частности, в отличие от подхода субъективной агрегации, в котором важность отдельных компонентов системы определяется с помощью предварительно задан-

ных весов, в нашем случае используется объективная декомпозиция, которая определяет приоритеты элементов интегрированной системе без предварительно заданных весовых коэффициентов.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 17-06-00237.

Список литературы

- [1] LYCHEV A. V., KRIVONOZLIKO V. E., UTKIN O. B., SAFIN M. M. On some generalization of the DEA models // Journal of the Operational Research. — 2009. — Vol. 186, P. 1518–1527.
- [2] KAO C. Network data envelopment analysis: a review // European Journal of Operational Research. — 2014. — Vol. 239, No 1, P. 1–16.
- [3] TONE K., TSUTSUI M. Dynamic DEA: a slacks-based measure approach // Omega: The International Journal of Management Science. — 2010. — Vol. 38, No 3, P. 145–156.

2.35. Лях Т.В., Зюбин В.Е. Метод разработки и верификации промышленных алгоритмов управления на языке Reflex

На сегодняшний день существуют несколько подходов к разработке алгоритмов управления сложными технологическими объектами. Перспективным направлением для программирования таких систем управления видится использование предметно-ориентированных языков. Эти языки позволяют в узких терминах решаемой задачи создавать специализированные алгоритмы управления.

Одним из таких языков программирования является процесс-ориентированный язык Рефлекс. Язык Рефлекс предназначен для создания управляющих алгоритмов в области промышленной автоматизации и робототехнике. Язык Рефлекс базируется на модели гиперпроцесса [1]. Код на языке Рефлекс организован в виде набора взаимодействующих процессов. Процессы исполняются параллельно, способны запускать друг друга, останавливать и отслеживать текущее состояние других процессов. Это позволяет вести параллельную обработку сигналов, поступающих от оборудования, обслуживать временные задержки и события, а также отслеживать действия, одновременно происходящие на объекте. В языке предусмотрены удобные средства для операций с временными интервалами и средства описания связей с датчиками и управляющими элементами промышленного объекта. Язык Рефлекс доказал свою адекватность для разработки промышленных алгоритмов управления в ряде успешных проектов [2].

Однако при всем удобстве использования языка Рефлекс остаётся вопрос о тестировании и верификации разработанного алгоритма управления. Запуск неотлаженного алгоритма на объекте управления чреват нештатными ситуациями или даже авариями на объекте. В то же время, так как промыш-