ВОПРОСЫ ВЫБОРА ТЕХНОЛОГИЙ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ ПРИ ПОСТРОЕНИИ «ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА»

А.Г. Сабанов

ЗАО «Аладдин Р.Д.»

Электронное взаимодействие, особенно в удаленном режиме, требует автоматической идентификации сторон. Созданию надежных механизмов идентификации и аутентификации (подтверждения подлинности предъявленного идентификатора) уделяется все больше внимания как за рубежом, так и в нашей стране. Согласно стратегическому плану развития, опубликованному на сайте Минкомсвязи России, к 2018 г. планируется охватить электронными госуслугами до 80% граждан. При этом одной из важнейших с точки зрения информационной безопасности является корректное решение задачи идентификации и аутентификации (ИА) граждан в удаленном режиме заказа и получения госуслуг.

Для решения задачи ИА для конкретной услуги необходимо сначала определить и четко зафиксировать цели выбора технологий для оказания данной услуги. Для реализации выбранных целей необходимо выработать критерии выбора (контрольные показатели) технологий, наиболее полно охватывающие условия реализации выбранных целей. Затем необходимо сравнить возможные альтернативные решения по выбранным контрольным показателям с точки зрения минимизации рисков.

В процессе выбора решений существенную роль может оказать классификация решений по их основным признакам. Множество реализаций применяемых в настоящее время средств идентификации и аутентификации можно классифицировать по целям, задачам и степени строгости (рис. 1).

Рис. 1

Фронтальная грань решений ИА на рис. 1 представляет классификацию по целям и задачам, верхняя грань отражает применяемые технологии, а боковая грань дает представление об участии сторон электронного обмена в процессе аутентификации. Например, при использовании для аутентификации многоразового пароля или одноразовых паролей (OTP – One Time Password) подтверждение подлинности предъявленного идентификатора (логина) производится только для клиентской стороны, т.е. производится односторонняя аутентификация. Примером двусторонней аутентификации является один из видов широко применяемого протокола SSL (Secure Socket Layer), когда в защищенном обмене производится проверка подлинности сервера и клиента. Примером трехсторонней аутентификации является почти повсеместно используемый в корпоративных сетях протокол Kerberos, в котором роль третьей доверенной стороны выполняет сервер KDC (Key Distribution Centre).

В целях понимания физической природы и области применения наиболее распространенных средств ИА на рис. 2 приводится классификация средств ИА по другому основному признаку – технологиям, на которых данные средства основаны.

Рис. 2

Классификация основных типов аутентификации в соответствии с №63-ФЗ «Об электронной подписи» представлена в таблице.

Табл.

Учетная запись пользователя	**Секрет (аутентификатор)**	**Тип аутентификации**
Логин	пароль	Простая
Логин	одноразовый пароль (технология OTP)	Усиленная
заданные поля сертификата X.509	закрытый ключ (в терминах №1-ФЗ)	Строгая

ПРИМЕНЕНИЕ ДВУХ ФОНОВЫХ ИЗОБРАЖЕНИЙ В ЗАДАЧЕ ОПРЕДЕЛЕНИЯ СТАЦИОНАРНЫХ ЗОН ПРИ ОБРАБОТКЕ ВИДЕОПОСЛЕДОВАТЕЛЬНОСТЕЙ

С.А. Минеев

Нижегородский госуниверситет

Современные системы видеонаблюдения все чаще реализуют функции автоматического обнаружения в зоне наблюдения: движущихся объектов, оставленных предметов, групп людей и т.п. Наиболее распространены алгоритмы обнаружения движения [1], как наиболее простые в реализации и проверке. Алгоритмов же обнаружения оставленных предметов известно лишь несколько реализаций [2, 3].

Предлагается выделить в алгоритмах обнаружения оставленных предметов уровень абстракции, в котором фигурируют стационарные и нестационарные зоны. Если перейти на данный уровень абстракции, то большинство реализаций алгоритмов обнаружения оставленных предметов можно описать блок-схемой, где процедуры выделения стационарных и нестационарных зон могут быть определены в терминах матричных операций над изображениями, а процедура анализа взаимосвязей стационарных и нестационарных зон как последовательность логических и топологических операций над геометрическими объектами.

Рассмотрим алгоритм выделения временно-стационарных зон. Для этого определим:

I_t как последовательность регистрируемых изображений, где t – номер кадра в изображении;

$B_t(l)$ как квазистационарный фон на момент прихода кадра с номером t, где l – количество кадров, из которых сформирован фон;

$B_{t-l}(l)$ как квазистационарный фон, задержанный относительно фона $B_t(l)$ на l кадров;

$O_{t'}$ как область кадра, соответствующая объекту, появившемуся в кадре с номером t' и остающемуся неподвижным на последующих кадрах;

$D_t=|B_t(l)–B_{t-l}(l)|$ как модуль разности двух фонов, где каждый цветовой канал обрабатывается независимо.

Способ получения изображения D_t иллюстрируется на рисунке.

Интенсивность временно-стационарной зоны на изображении D_t с течением времени будет возрастать, начиная с момента t' появления и стабилизации объекта в кадре, вплоть до момента $t'–l$. Снижение интенсивности временно-стационарной зоны будет происходить по причине участия кадра $I_{t'}$ и последующих кадров в формировании задержанного фона, начиная с момента $t'–l$, а окончательно временно-стационарная зона исчезнет с изображения D_t в момент $t'–2l$. Таким образом, на бинарном изображении D_t высокий уровень будет соответствовать зонам, сохраняющим стационарность в статистическом смысле в течение интервала l.

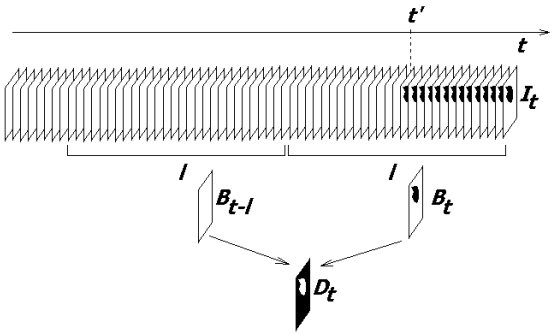

Рис.

На основе представленного алгоритма была разработана процедура обнаружения оставленных предметов, которая была протестирована на тестовых видеозаписях CAVIAR [4] и PETS [5]. Видеозаписи с размером кадра 655x524 и частотой следования 25 кадров/с обрабатывались в реальном времени на ПЭВМ с процессором Intel CORE i5 2500 МГц. Результаты тестирования показали высокую устойчивость алгоритма к таким помехам как изменение освещенности, частичное/полное кратковременное перекрытие оставленных предметов пешеходами.

К недостаткам алгоритма следует отнести значительный объем оперативной памяти, занимаемый двумя очередями изображений, по которым вычисляются текущее и задержанное фоновые изображения. Объем занимаемой памяти пропорционален интервалу задержки, размеру кадра, частоте следования кадров. В качестве базовой платформы систем видеонаблюдения на базе предложенного алгоритма рекомендуется применять 64-х разрядные операционные системы.

[1] Иванов В.А., Киричук В.С. // Автометрия. 2009. Т.45. № 5. С. 14.
[2] Иванов В.А., Киричук В.С., Орлов С.И. // Автометрия 2011. Т.47. № 1. С. 30.
[3] Bhargava M., Chen C.-C., Ryoo M.S., Aggarwal J.K. // Machine Vision and Applications. 2009. V.20. P. 271.
[4] CAVIAR Test Case Scenarios: http://homepages.inf.ed.ac.uk/rbf/CAVIARDATA1 (дата обращения 11.01.2013).
[5] PETS 2007 Benchmark Data: http://pets2007.net (дата обращения 11.01.2013).

СИСТЕМА ИДЕНТИФИКАЦИИ ДИКТОРОВ ПО ГОЛОСУ

Р.А. Васильев

Нижегородский государственный лингвистический университет

В работе предлагается метод фонетического анализа речи – выделение списка элементарных речевых единиц типа отдельных фонем из непрерывного потока

разговорной речи конкретного диктора. Описан практический алгоритм идентификации диктора – процесс определения говорящего из заданного набора дикторов.

В связи с возросшей информатизацией современного общества, увеличением числа объектов и потоков информации, которые необходимо защищать от несанкционированного доступа, а также необходимостью интеллектуализации всех форм взаимодействия пользователей автоматизированных систем управления с техническими средствами, все более актуальными становятся проблемы использования механизмов речевых технологий для разграничения доступа к информационно-вычислительным системам, в частности, проблема идентификации пользователей системы по голосу. Привлекательность данного метода – удобство в применении. Продукты с проверкой голоса сейчас предлагают более 20 компаний.

В поисках путей решения проблемы адекватной системы описания отдельных фонем само понятие «фонема» впервые было строго определено в теоретико-информационном смысле как «множество однородных минимальных звуковых единиц (МЗЕ), объединенных в кластер по критерию минимального информационного рассогласования (МИР) в метрике Кульбака-Лейблера. Условно говоря, человеческий мозг объединяет и запоминает в себе как нечто целое (в виде абстрактного образа) разные образцы (произношения) каждой отдельной фонемы в соответствующей «сфере» своей памяти вокруг абстрактного «центра» с заданным «радиусом» [1 – 3].

Для реализации исследований по идентификации дикторов по голосу, аспирантами и сотрудниками НГЛУ им Н.А. Добролюбова во главе с профессором Савченко В.В., был разработан лабораторный образец информационной системы фонетического анализа слитной речи (ИСФАР) [4]. Данная система представляет собой фонетический анализатор. Варианты применения такого анализатора можно привести из самых различных областей. Это может быть, например, задача анализа качества речи по ее фонетическому составу, как для отдельного диктора, так и для идентификации диктора по голосу. В качестве прикладной задачи можно привести текстонезависимую идентификацию разных дикторов по голосу в режиме реального времени.

В процессе эксперимента на сегментирование подавались фразы отдельных дикторов и производилась идентификация конкретного диктора посредством подсчета распознанных фонем. Решение о принадлежности произнесенной фразы конкретному диктору принималось автоматически после подсчета всех распознанных фонем и вычисления доминирующих фонем среди всех остальных.

По итогу эксперимента в произнесенной фразе было выделено 759 фонем, из них 609 фонем принадлежали определенному диктору, а 150 фонем были распознаны как «ложные» фонемы, похожие на фонемы других дикторов. Таким образом, по большему количеству принадлежащих определенному диктору фонем, можно идентифицировать того, кто произнес фразу. При этом в системе «ИСФАР» нет привязки к произнесенным командам и фразам, т.е. осуществляется автоматическая текстонезависимая идентификация диктора.

В ходе решения поставленной задачи были получены следующие результаты:

− благодаря применению минимальных звуковых единиц в задаче фонетического анализа речи (ФАР) удалось резко сократить вычислительную сложность решаемой задачи идентификации и одновременно в полной мере использовать оптимальные свойства решающей статистики МИР;

− проанализирован процесс речеобразования и исследована работа артикуляторного аппарата человека, в результате чего выработаны пути построения модели идентификации голосового сообщения;

− проведён обзор и анализ методов, которые могут использоваться при идентификации голосового сообщения: нейросети, частотные цифровые фильтры, Фурье-анализ, кепстральный анализ, методы машинного обучения, векторное квантование, гауссовы смеси и вейвлет-анализ. Показана предпочтительность выбора Фурье-анализа как основы построения модели;

− построена структурная схема модели идентификации голосового сообщения по фонемной составляющей и индивидуальным характеристикам голоса;

− спроектирована структура базы данных голосовых сообщений для тестирования и статистической оценки качества работы предложенной модели.

Исследования осуществлены в терминах универсального теоретико-информационного подхода и информационной теории восприятия речи. Их главная цель – создание необходимой методологической и программной базы для дальнейшей конструкторской разработки системы идентификации диктора по голосу.

[1] Савченко В.В. // Изв. вузов России. Радиоэлектроника. 2008. № 1. С. 24.
[2] Савченко В.В., Губочкин И.В. // Изв. вузов России. Радиоэлектроника. 2008. №1. С. 26.
[3] Савченко В.В. // Изв. вузов России. Радиоэлектроника. 2007. № 6. С. 3.
[4] Савченко В.В., Акатьев Д.Ю. Патент на полезную модель № 90251. Устройство для фонетического анализа и обучения речи. / Роспатент по заявке № 2009122158/22 от 09.06.2009.

РЕАЛИЗАЦИЯ АЛГОРИТМА ТРАССИРОВКИ ПУТЕЙ НА CUDA

Д.Р. Богров

Нижегородский госуниверситет

Алгоритмы на основе трассировки лучей генерируют изображение путем отслеживания взаимодействий лучей света с объектами сцены. Оригинальный вариант метода был впервые сформулирован в 1980 году Т. Уиттедом [1]. Однако реалистичная визуализация невозможна без расчета вторичного освещения, в результате которого одна поверхность освещается светом, отраженным от другой поверхности. Типичными примерами вторичного освещения служат явления переноса цвета между соседними поверхностями и каустики. Предложенная в 1986 году Джеймсом Кайя [2] трассировка пути, позволила учитывать все эффекты глобаль-

ного освещения, включающие все возможные взаимодействия между различными типами поверхностей.

Через каждый пиксель экранной плоскости испускается первичный луч, для которого определяется ближайшая точка соударения P (рис. 1). Яркость данного пикселя вычисляется из уравнения визуализации, для численного решения которого используется метод Монте-Карло:

$$L(P \to D_v) = L_e(P \to D_v) + \int_{\Omega} F_s(D_v, D_i) \,|\cos\theta\,| L(Y_i \to -D_i) dD_i ,$$

где $L(P \to D_v)$ – яркость излучаемая точкой поверхности P в направлении D_v, $L_e(P \to D_v)$ самостоятельно излучаемая яркость из точки P в направлении D_v, $F_s(D_v, D_i)$ – функция двунаправленной отражательной способности.

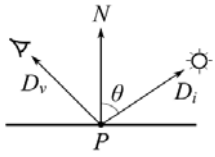

Рис. 1

Интеграл есть сумма всей энергетической яркости, приходящей в точку P со всех направлений, умноженной на коэффициент отражения материала и функцию двунаправленной отражательной способности. Заменяя интеграл выборками по методу Монте-Карло [3], можно при увеличении числа выборок приходящихся на один пиксель, сглаживать неровности финального изображения.

Расчет конечного изображения – процесс вычисления энергетической яркости, выполняющийся для каждого пикселя. Для реализации на CUDA (Compute Unified Device Architecture), процесс расчета изображения методом трассировки путей реализован по следующему конвейеру, содержащему несколько ядер (рис. 2).

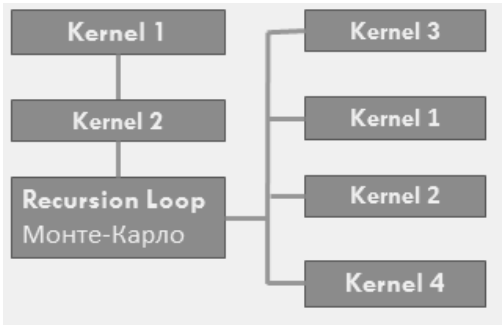

Рис. 2

1. Создает базовое изображение, визуализирует формы, находит ближайшие пересечения и присваивает соответствующий цвет. Это ядро устанавливает данные, хранящиеся в буфере: дистанцию ближайшего пересечения; идентификатор, тип и нормаль объекта; точки пересечения. Буфер хранит эти значения для каждого пикселя.

2. Производит тонирование и расчет теней изображения. Сначала генерируется теневой луч для каждого источника света и вычисляется область тени. Если луч находится не в тени, то ведется полный расчет освещения по модели затенения, т.е. рассчитывается первичное и вторичное освещение, если же луч оказывается в тени, то только вторичное. Результат записывается в буфере цвета.

3. Вызывается при рекурсии. Это ядро считывает вектор нормали объекта, определенный в буфере, и текущее направление камеры, и задает новый вектор для отраженного луча с использованием функции CUDA math, reflect.

4. Смешивает получившейся цвет с результатом цвета предыдущего прохода. Коэффициент смешивания определяется коэффициентом отражения материала.

Разработанная графическая система расчета глобального освещения является физически корректной: визуализация объектов происходит без смещения конечного изображения. Разработанная на основе программно-аппаратной архитектуры CUDA, данная система позволяет задействовать для расчетов графический процессор, выполняющий графический рендеринг. Для описания свойств поверхностей графическая система поддерживает различные модели освещения.

[1] Whitted T. // Comm. of the ACM**.** 1980. V. 23, No. 6. P. 343.
[2] Kajiya J.T. The Rendering Equation // Proc. of the SIGGRAPH. 1986. V.20, No.4. P.143.
[3] Dutre Ph., Bala K., Bekaert Ph. Advanced Global Illumination – Wellesley: A K Peters Ltd, 2006, 366 p.

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ОБНАРУЖЕНИЯ БЕСПРОВОДНЫХ ВТОРЖЕНИЙ

И.С. Исупов, А.А. Рябов

Нижегородский госуниверситет

Системы обнаружения беспроводных атак (Wireless Intrusion Detection System – WIDS) пока не настолько популярны, как их проводные аналоги, но современные тенденции позволяют предсказывать рост числа их внедрений. Положительным фактором является интеграция подобных программ с активным сетевым оборудованием и осознание руководством рисков, связанных с несанкционированным использованием беспроводных устройств. Последнее приводит к увеличению числа инсталляций WIDS даже в сетях, где беспроводные сети не используются. В связи с этим у специалистов в области безопасности возникает необходимость оценить не только качественные характеристики того или иного продукта, но и прогнозировать возможное негативное влияние от его внедрения на безопасность корпоративной сети.

Определим основные антропогенные источники угроз (см. рис.). К таким относятся внешние злоумышленники, взаимодействующие с системой через радиоэфир, внутренние злоумышленники, имеющие доступ к локальной сети, и операторы, обладающие некоторыми ограниченными возможностями по управлению компонентами системы.

Основу WIDS составляют сенсоры, выполняющие функцию сбора беспроводного трафика в режиме мониторинга. Сенсоры могут быть реализованы на базе операционной системы (ОС) семейства Windows или специализированных программно-аппаратных комплексов, в большинстве случаев базирующихся на ОС Linux. Сенсоры представляют собой достаточно интеллектуальные устройства,

поддерживающие семейство протоколов TCP/IP и обладающие развитыми интерфейсами управления.

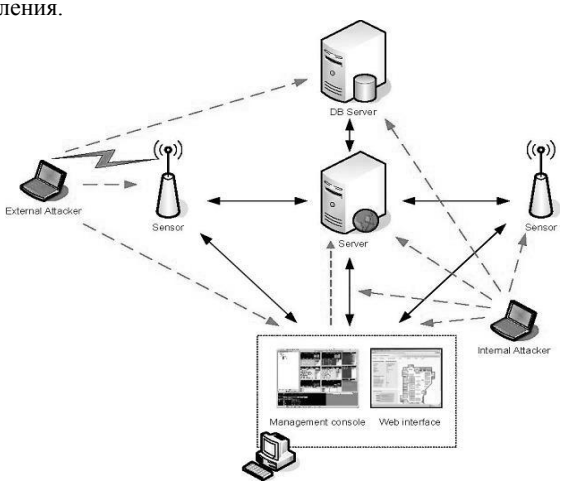

Рис.

В разрабатываемом приложении в качестве сенсоров предлагается использовать отдельно стоящие антенны, подключенные к одному компьютеру под управлением ОС Linux. Сервер обнаружения угроз обрабатывает все поступающие на него пакеты, собранные в зоне действия системы принимающих антенн. Таким образом, система обнаружения беспроводных вторжений содержит в себе всего один компьютер, занимающийся обработкой всех поступающих на него данных, и систему антенн.

В ходе обработки поступающей на сервер обнаружения угроз информации, им выполняются следующие задачи:

- принятие решений относительно беспроводных пользователей (внутри и вне сети);
- исследование работы пользователей в беспроводной сети (статистика использования ресурсов);
- в случае появления аномалий посылка оповещения администратору безопасности по электронной почте.

По сравнению с предыдущей версией приложения [2], был внесён ряд изменений в функциональные возможности приложения:

- программа занимается обработкой не только внешних, но и внутренних угроз;
- одна антенна заменена системой антенн для покрытия всей изучаемой области;
- появилась возможность использования нескольких беспроводных адаптеров для территориального разделения использующихся беспроводных устройств.

В ходе создания новой версии приложения было разработано несколько путей его развития. Важной особенностью станет возможность приложения в автоматическом режиме собирать статистику использования ресурсов беспроводной сети

пользователями. Для просмотра собранной статистики планируется подготовка наглядного вывода в виде графиков и диаграмм. Возможности программы будут расширены за счёт внедрения автоматической системы принятия решений для мгновенного реагирования, что позволит администраторам, которые отвечают за информационную безопасность, снизить собственную нагрузку по контролю над системой обеспечения безопасности: программа будет принимать начальные решения без операторов ПК. В дальнейшем администратор сети сможет эти решения изменить. Приложение фактически может работать автономно, лишь некоторые его параметры требуют настройки администратором.

В настоящее время продукт доступен только для UNIX-платформ, что создаёт некоторые неудобства для сетей, где используются Windows-машины. Исходя из этого планируется создание версии для ОС Windows и, возможно, для мобильных платформ. Кроссплатформенные приложения получают более широкое распространение из-за удобства их адаптации для любых условий использования.

[1] Исупов И.С., Рябов А.А. // В кн. Труды XVI научной конференции по радиофизике. /Под ред. С.М. Грача, А.В. Якимова. − Нижний Новгород: Изд-во ННГУ, 2012. С. 270.

ЭКСПЕРИМЕНТАЛЬНОЕ ОПРЕДЕЛЕНИЕ АЛГЕБРАИЧЕСКОЙ СТРУКТУРЫ МОДЕЛИ ПРОГНОЗИРУЮЩЕГО ОПЕРАТОРА НА ОСНОВЕ ГЕНЕТИЧЕСКИХ АЛГОРИТМОВ

А.А. Горбунов, А.О. Маченко

Нижегородский госуниверситет

Задача определения структуры и параметров математических моделей (ММ) процессов по их экспериментальным данным относится к проблематике идентификации объектов различной природы. В рамках математической модели генетической карты экспериментальных данных в качестве ММ источника участка стационарности (гена) текстовой последовательности введено понятие «прогнозирующего оператора» [1, 2], описываемое в общем случае выражением:

$$y(t) = f\big(y(t-1),\ldots,y(t-n),u(t),\ldots,u(t-n)\big), \qquad (1)$$

где $y(t)$ – выходная текстовая последовательность, f – q-значная функция, $u(t)$ – входная текстовая последовательность, t – дискретное время.

В случае линейной автономной модели прогнозирующего оператора одним из ее возможных представлений является детерминированная дискретная авторегрессионная модель

$$y(t) = \alpha_1 y(t-1) + \alpha_2 y(t-2) + \ldots + \alpha_n y(t-n). \qquad (2)$$

Алгоритм идентификации автономного источника текстовой последовательности в виде ММ (2) с возможностью регулирования алгебраической структуры (АС), описанный в [3], предполагает полный перебор возможных вариантов АС. В на-

стоящей работе рассматривается задача отбора с помощью генетических алгоритмов таких таблиц Кэли, описывающих операции с элементами алгебраической структуры, которые соответствуют экспериментальным текстовым последовательностям, порождаемым источником с моделью вида (2).

При отборе АС с помощью генетических алгоритмов, описанных в [4], понятие единичной особи включает в себя набор таблиц Кэли, отвечающих одной конкретной алгебраической структуре. Алгоритм выбора АС на основе генетических алгоритмов обладает рядом особенностей, позволяющих повысить эффективность его работы с точки зрения быстродействия и ресурсоемкости. Поиск решения осуществляется не путем улучшения одной АС, а путем использования сразу нескольких альтернатив на заданном множестве решений. Кроме того, генетические алгоритмы применяют не детерминированные, а вероятностные правила анализа оптимизационных задач [4].

Генетические алгоритмы выбора алгебраической структуры программно реализованы на языке C++ в среде разработки программного обеспечения Microsoft Visual Studio 2010. Реализованная компьютерная программа позволяет находить АС по критерию максимума средней длины гена текстовой последовательности при фиксированном значении параметра сложности n модели (2).

В реализованной программе также имеется возможность определять наилучшую АС в предположении о стационарности всей анализируемой текстовой последовательности. В этом случае оценивается степень различия между представленной выходной текстовой последовательностью и текстовой последовательностью, полученной с помощью прогнозирующего оператора ММ (2) при задании таблиц Кэли той или иной АС. Наилучшая АС отбирается, исходя из критерия минимизации различия между этими последовательностями.

Проведенные компьютерные эксперименты для ряда генетических текстовых последовательностей подтвердили уменьшение затраченного времени работы программы по отбору АС при использовании генетических алгоритмов в сравнении с использованием метода полного перебора всех возможных вариантов АС. Получены результаты выбора АС для ММ прогнозирующего оператора таких текстовых последовательностей, которые ранее, при использовании полного перебора вариантов АС, не определялись в силу ограниченности типичных ресурсов вычислительной техники, на которой проводились компьютерные эксперименты.

[1] Кирьянов К.Г. Генетический код и тексты: динамические и информационные модели сложных систем / Ред. Л.Ю. Ротков, А.В. Якимов. – Нижний Новгород: ТАЛАМ, 2002, 100 с.

[2] Кирьянов К.Г. // В кн. Труды III Международной конференции «Идентификация систем и задачи управления SICPRO'04». – М.: ИПУ РАН, 2004. С.187.

[3] Горбунов А.А., Коновалов А.С., Маченко А.О. // В кн. Труды XVI научной конференции по радиофизике /Под ред. С.М. Грача, А.В. Якимова. – Нижний Новгород: Изд-во ННГУ, 2012. С. 267.

[4] Гладков Л.А., Курейчик В.В., Курейчик В.М. Генетические алгоритмы. – Ростов-на-Дону: Ростиздат, 2004, 400 с.

АНАЛИЗ ЭФФЕКТИВНОСТИ ГИБРИДНОГО ОБЛАЧНОГО ЦЕНТРА

О.В. Хачинян

Нижегородский госуниверситет

Облачными системами называют системы, характеризующиеся динамическим выделением «бесконечного» числа виртуальных ресурсов, доступных по первому требованию пользователей. Одним из видов облачных вычислений является гибридное облако (hybrid cloud). Гибридное облако представляет собой такой вид облака (cloud computing), при котором часть собственной инфраструктуры компании выносится в дата-центр облачного провайдера, или в корпоративную инфраструктуру включатся внешние ресурсы и сервисы, потребляемые из облака внешнего поставщика [1].

Одним из главных параметров эффективности облачного центра является его время ответа. Оно прописывается в соглашении об уровне обслуживания SLA (Service Level Agreement). Облачный провайдер должен знать минимально требуемые облачные ресурсы для определенных вычислительных узлов или виртуальных машин.

В данной работе рассматривается аналитическая модель, позволяющая определить минимально необходимое число виртуальных машин для удовлетворения критерия SLA по времени ответа.

Рассмотрим модель облачного центра. Обработка входящих запросов происходит следующим образом: запросы поступают на LB (Load Balancer), который распределяет нагрузку равномерно между m виртуальными машинами. Будем считать протекающие в системе процессы марковскими. Пусть входящие запросы подчинены распределению Пуассона с интенсивность поступления заявок λ [2]. Запросы обслуживаются в соответствии с правилом FCFS (First Come First Served) − первый пришел, первый обслуживается. Среднее время обслуживания запроса LB равно $1/r$, а виртуальной машиной − $1/\mu$ соответственно. Предположим, что $r \geq m\mu$. В противном случае LB должен быть повторно масштабирован.

Состояние системы описывается графом состояний (см. рис. 1).

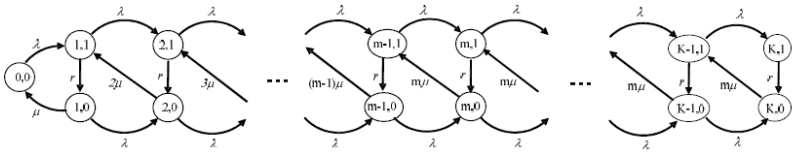

Рис. 1

Нахождение системы в состоянии $(0,0)$ означает, что система свободна. Состояние $(k,1)$ соответствует тому, что заявка находиться в LB, $(k,0)$ – обслуживается виртуальной машиной (k – чис-

ло заявок в системе). Состояние $(K,0)$ соответствует полной занятости системы.

Вероятность нахождения в состоянии $q_{0,0}$, $q_{1,0}$, $q_{1,1}$ может быть найдена как:

$$\begin{aligned} &-\lambda q_{0,0} + \mu q_{1,0} = 0, \\ &-(\lambda+\mu) q_{1,0} + r q_{1,1} = 0, \\ &-(\lambda+r) q_{1,1} + \lambda q_{0,0} + 2\mu q_{2,0} = 0. \end{aligned} \quad (1)$$

Вероятность нахождения в состоянии $(k,1)$:

$$\begin{aligned} &-(\lambda+r) q_{k,1} + \lambda q_{k-1,1} + (k+1)\mu q_{k+1,0} = 0, \ \text{если} \ 2 \le k < m-1 \\ &-(\lambda+r) q_{k,1} + \lambda q_{k-1,1} + m\mu q_{k+1,0} = 0, \ \text{если} \ k \ge m \end{aligned} \quad (2)$$

Вероятность нахождения в состоянии $(k,0)$:

$$\begin{aligned} &-(\lambda+k\mu) q_{k,0} + r q_{k,1} + \lambda q_{k-1,0} = 0, \ \text{если} \ 2 \le k < m-1 \\ &-(\lambda+m\mu) q_{k,0} + r q_{1,1} + \lambda q_{k-1,0} = 0, \ \text{если} \ k \ge m \end{aligned} \quad (3)$$

Тогда из уравнений (1)-(3) может быть найдена средняя пропускная способность γ: $\gamma = \mu \sum_{k=1}^{K} q_{k,0}$.

Вероятность отказа в обслуживании соответствует нахождению системы в состоянии $(K,0)$ или $(K,1)$

$$P = q_{K,0} + q_{K,1}.$$

Среднее число занятых виртуальных машин

$$\overline{K} = \sum_{k=1}^{K} k\left(q_{K,0} + q_{K,1}\right).$$

По формуле Литта среднее время ответа

$$W = \frac{\overline{K}}{\gamma} = \frac{1}{\gamma}\sum_{k=0}^{K-1} k\left(q_{k,0} + q_{k,1}\right) + \frac{K}{\gamma}\left(q_{K,0} + q_{K,1}\right).$$

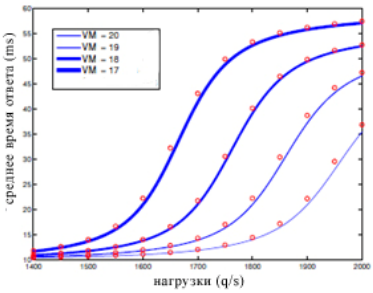

Рис. 2

Результаты вычислений для K=100, r =0,2 мс, m = 10 мс представлены на рис. 2.

[1] http://www.ibm.com/developerworks/ru/library/cl-cloudstorage/index.html
[2] Kleinrock L. Queueing Systems: Vol. I. Theory. – New York: Wiley Interscience, 1975, 417 p.

ПРОВЕДЕНИЕ ЭКСПЕРТИЗ ПО ПРЕСТУПЛЕНИЯМ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

С.М. Авдонин, Д.В. Демьяненко, А.А. Рябов

Нижегородский госуниверситет

При внедрении информационных технологий в самые разнообразные сферы жизнедеятельности общества возрастает количество преступлений, связанных с компьютерной информацией, а их общественная опасность становится все более очевидной.

Уголовный кодекс Российской Федерации [1] в главе 28 четко определяет преступления в сфере компьютерной информации:

- неправомерный доступ к компьютерной информации (ст. 272);
- создание, использование и распространение вредоносных компьютерных программ (ст. 273);
- нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274).

Однако ряд уголовно наказуемых деяний по своему составу вплотную сопрягается с преступлениями в сфере компьютерной информации. Это обусловлено тем, что при использовании компьютерной информации в качестве средства совершения другого преступления, она сама становится предметом общественно опасного деяния, например:

- нарушение авторских и смежных прав в отношении программ для ЭВМ и баз данных, а также иных объектов авторского и смежного права, находящихся в виде документов на машинном носителе (ст. 146);
- клевета, то есть распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию, с использованием информационно-телекоммуникационных сетей (ст. 128.1.);
- незаконный оборот специальных технических средств, предназначенных для негласного получения информации (ст. 138.1) и т.д.

Расследование и судопроизводство по данным преступлениям весьма трудно осуществить без использования экспертных познаний в области современных информационных технологий. Как правило, во всех перечисленных случаях производство экспертизы заключается в исследовании носителей информации. При этом основной задачей эксперта является объективное описание содержимого носителей информации. Выводы по результатам анализа вышеозначенного содержимого зависят от поставленных перед экспертом вопросов.

Накопленный авторами опыт позволяет сформулировать некоторые методические рекомендации при проведении экспертиз носителей информации.

При производстве экспертизы необходимо указать сведения об аппаратном и программном обеспечении рабочего места, с которого осуществлялось исследование. Это позволит повторить полученные результаты в случае назначения повторной экспертизы, а также поможет при анализе их достоверности.

Если на экспертизу предоставляется компьютер (или иное средство вычислительной техники), необходимо провести внешний осмотр поступившего объекта исследования, проверить комплектность, выявить его недостатки и внешние дефек-

ты. В случае, если выявленные недостатки и дефекты способны нарушить работоспособность объекта исследования, то об этом необходимо уведомить дознавателя, следователя или суд. Далее необходимо определиться с алгоритмом проведения всего экспертного исследования, применяемыми методиками и используемым оборудованием и лишь после этого удостовериться в работоспособности представленного на исследование оборудования.

При производстве экспертизы очень важным является принцип неизменности вещественных доказательств. Он подразумевает, что информация на представленном на исследование носителе данных не должна быть изменена. В случае, если носителями информации являются оптические (CD, DVD, Blu-ray) диски, внесение экспертом искажений в содержащуюся на них информацию маловероятно. При исследовании других носителей (НГМД, НЖМД, флэш-диски и т.п.) нужно использовать другой подход. Как правило, непосредственное изучение информации с таких носителей производится после создания двоичного образа с применением различного инструментария, предназначенного для подобных целей. Но такой подход не всегда возможен. В таких случаях есть аппаратные средства, предоставляющие возможность исследовать носители в режиме запрета модификации их содержимого (аппаратные и программные блокираторы).

В некоторых случаях встает задача о подтверждении работоспособности программного обеспечения, установленного на исследуемых носителях. Такую проверку практически невозможно сделать без модификации содержимого исследуемых носителей. В этом случае лучше использовать виртуальную машину (например, VMware Player), позволяющую исследовать программное обеспечение без модификации содержимого носителя.

Несоблюдение данного принципа может повлечь за собой фатальные изменения на уровне данных (стирание или модификация значимой информации). В связи с этим важно особо отметить, что согласно ст. 57 Уголовно-процессуального кодекса Российской Федерации [2] эксперт не вправе проводить без разрешения дознавателя, следователя, суда исследования, могущие повлечь полное или частичное уничтожение объектов, либо изменение их внешнего вида или основных свойств.

[1] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 23.07.2013)
[2] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 23.07.2013)