был принят на 10 лет раньше от начала конкурса AES. Однако алгоритм «ГОСТ Р 28147-89» имеет, как минимум, два существенных недостатка:

• основные операции выполняются над 32-битными «полублоками». Алгоритм проигрывает в скорости в 4 раза байт-ориентированному «Rijndael» на 8-битных платформах;

• в тексте стандарта отсутствуют четкие критерии выбора узлов замены. Достаточно часто высказываются опасения, что существуют слабые узлы замены.

Рассмотрим устойчивость обоих алгоритмов к известным видам криптоанализа. Наиболее универсальными и эффективными для алгоритмов широкого класса являются дифференциальный и линейный виды криптоанализа. Дать оценку устойчивости алгоритма «ГОСТ Р 28147-89» к конкретным видам криптоанализа невозможно без спецификации узлов замен, так как качество этого шифра зависит от качества использованных узлов. Но исследования близких по архитектуре шифров с заданными таблицами подстановок показали, что криптоанализ шифра с 16 раундами в принципе осуществим, но требует очень большого числа исходных данных, а при 20-24 раундах становится теоретически бесполезным. Отечественный стандарт шифрования предусматривает 32 раунда шифрования, и этого количества хватает с запасом, чтобы успешно противостоять указанным видам криптоанализа.

По оценкам разработчиков шифра AES, уже на 4 раундах шифрования этот алгоритм приобретает достаточную устойчивость. Теоретической границей, за которой линейный и дифференциальный виды криптоанализа теряют смысл, является рубеж в 6 раундов. Согласно спецификации, в шифре предусмотрено 10-14 раундов. Следовательно, шифр AES также устойчив к указанным видам криптоанализа с определенным запасом. Таким образом, сравниваемые шифры обладают достаточной стойкостью к известным видам криптоанализа. В печати отсутствуют какие-либо сведения об успешных случаях вскрытия указанных шифров, а также описания процедур, которые теоретически позволили бы дешифровать сообщение с меньшими вычислительными затратами, чем полный перебор по всему ключевому пространству.

Рассмотренные алгоритмы обладают сопоставимыми характеристиками быстродействия при реализации на 32-битовых платформах. На 8-битовых платформах картина, вероятно, сходная. Что касается аппаратной реализации, то в отличие от «ГОСТ Р 28147-89», алгоритм шифрования AES позволяет достичь высокой степени параллелизма при выполнении шифрования, оперирует блоками меньшего размера и содержит меньшее число раундов, в силу чего его аппаратное воплощение может оказаться существенно более быстрым. Преимущество длины наибольшего пути в сетевом представлении примерно четырехкратное.

Проведенное выше сопоставление параметров российского стандарта шифрования и алгоритма шифрования AES, принятого за стандарт шифрования США, показало, что, несмотря на различие в архитектурных принципах этих шифров, их основные рабочие параметры сопоставимы. Исключением является тот факт, что «Rijndael»имеет значительное преимущество в быстродействии перед «ГОСТ Р 28147-89» при аппаратной реализации на базе одной и той же технологии. Очевидным шагом в оптимизации отечественного алгоритма шифрования, считаем, является переход байтовым заменам, что должно повысить стойкость алгоритма к известным видам криптоанализа.

Список литературы

1. Официальная страница NIST США [Электронный ресурс]. – 2015. – Режим доступа: http://csrc.nist.gov/archive/aes/index.html.

2. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Пер. с англ. / Б. Шнайер. – М.: Изд-во «Триумф», 2012. – 816 с.

3. Сонг Й. Ян. Криптоанализ RSA / Пер. с англ. Ю. Айдарова. – М.: Изд-во «Институт компьютерных исследований», 2011. – 312 с.

Секция «Проблемы моделирования, проектирования и разработки программных средств», научный руководитель – Рыбанов А.А., д-р техн. наук, профессор

ИССЛЕДОВАНИЕ МЕТОДОВ И РЕАЛИЗАЦИЯ АЛГОРИТМА МОДЕЛИРОВАНИЯ РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ В СОЦИАЛЬНЫХ СЕТЯХ

Айналимов Б.О., Короткова Н.Н.

Волжский политехнический институт, филиал ФГБОУ ВПО «Волгоградский государственный технический университет», Волжский, e-mail: batyr555@mail.ru

Анализ социальных данных стремительно набирает популярность во всём мире [1, 2] благодаря появлению в 1990-х годах онлайновых сервисов социальных сетей (SixDegrees, LiveJournal, Facebook, Twitter, YouTube и другие). Таким образом, социальные сети являются уникальным источником данных о личной жизни и интересах реальных людей. Это открывает беспрецедентные возможности для решения исследовательских и бизнес-задач. Такой бизнес-задачей может являться отправка отложенных и условных статусов (постов) в Twitter.

Постановка проблемы. Обработка социальных данных требует разработки соответствующих алгоритмических и инфраструктурных решений, позволяющих учитывать их размерность. К примеру, база данных социальной сети Twitter на сегодняшний день содержит более 1 миллиарда пользовательских аккаунтов и более 100 миллиардов связей между ними. Каждый день пользователи добавляют более 200 миллионов фотографий и оставляют более 2 миллиардов комментариев к различным объектам сети.

Проблема заключается в том, что большинство существующих алгоритмов, позволяющих эффективно решать актуальные задачи, не способны обрабатывать данные подобной размерности за приемлемое время. В связи с этим, возникает потребность в новых решениях, позволяющих осуществлять распределённую обработку (с помощью операционной системы Corezoid) и хранение данных без существенной потери качества результатов (с помощью облачной базы данных Firebase), что подтверждает актуальность решенной в рамках данной работы задачи.

Цель данной работы: повышение эффективности взаимодействия менеджера рекламного агентства с большим количеством аккаунтов социальной сети Twitter при медиапланировании. Для достижения поставленной цели необходимо решения следующих исследовательских задач:

1) математическое описание методов и реализации алгоритма моделирования распространения информации в социальных сетях.

2) разработка алгоритмов и программная реализация web-ориентированной информационной системы условного и отложенного постинга в Twitter.

3) экспериментальная оценка эффективности предлагаемых критериев и алгоритмов.

Сравнительный анализ существующих методов и реализации алгоритма моделирования распространения информации в социальных сетях

Существует ряд методов, позволяющих находить решение задачи об отложенном постинге. При выборе алгоритма решения приходится выбирать между точными алгоритмами, которые не применимы для стеков большой размерности, и приближенными, которые работают быстро, но не обеспечивают оптимального решения задачи. Если перебирать всевозможные подмножества данного набора из n предметов, то получится решение сложности не менее чем $O(2^n)$. В настоящее время неизвестен (и, скорее всего, вообще не существует) алгоритм решения этой задачи, сложность которого является многочленом от n.

Доказывается, что жадный выбор на первом шаге не закрывает пути к оптимальному решению: для всякого решения есть другое, согласованное с жадным выбором и не хуже первого.

Показывается, что подзадача, возникающая после жадного выбора на первом шаге, аналогична исходной.

Рассуждение завершается по индукции.

Оптимальность для подзадач

Говорят, что задача обладает свойством оптимальности для подзадач, если оптимальное решение задачи содержит в себе оптимальные решения для всех её подзадач. Например, в задаче о выборе заявок можно заметить, что если A – оптимальный набор заявок, содержащий заявку номер 1, то $A' = A \setminus \{1\}$ – оптимальный набор заявок для меньшего множества заявок S', состоящего из тех заявок, для которых $s_i \leq f_1$ [4].

Программная реализация алгоритма моделирования распространения информации в социальной сети «Twitter».

Был разработан метод поиска неявных сообществ пользователей социальных сетей на основе социальных связей между ними. Предложенный алгоритм

Сравнительный анализ методов и алгоритмов

Метод	Тип алгоритма	Сложность	Плюсы	Минусы
Полный перебор	Точный	O(n!)	Простота реализации; Точное решение	Входные данные не велики; временная сложность
Метод ветвей и границ	Точный		Возможно значительное сокращение времени; простота реализации	Работает как полный перебор
Жадный алгоритм	Приближенный	O(n*log(n))	Высокая скорость; может работать с большими значениями n; простота реализации	Решение неточное
Генетический алгоритм	Приближенный		Высокая скорость; может работать с большими значениями n; независимость от вида исходных данных	Не гарантирует нахождение оптимального решения
Метод динамического программирования	Точный	O(w*n)	Независимость от вида исходных данных; точное решение	Большой объём вычислительной работы

Возможность быстрой реализации, высокой скорости работы и функционирования при работе с большими данными – это преимущества жадного алгоритма, который и был взят за основу для реализации распределенной информационной системы постинга.

Математическое описание алгоритма моделирования распространения информации в социальных сетях

Общего критерия оценки применимости жадного алгоритма для решения конкретной задачи не существует, однако, для задач, решаемых жадными алгоритмами, характерны две особенности: во-первых, к ним применим Принцип жадного выбора, а во-вторых, они обладают свойством Оптимальности для подзадач [5].

Принцип жадного выбора

Говорят, что к оптимизационной задаче применим принцип жадного выбора, если последовательность локально оптимальных выборов даёт глобально оптимальное решение. В типичном случае доказательство оптимальности следует такой схеме:

локально имитирует человеческое общение между парами индивидуумов, а глобально моделирует инфекционный процесс. Основой алгоритма является процесс обмена метками сообществ между вершинами в соответствии с динамическими правилами взаимодействия, в ходе которого поощряется объединение сообществ ближайших контактов отдельных пользователей в глобальные сообщества. Дополнительным шагом алгоритма является определение сообществ с недостаточной внутренней связанностью и разделение их на более связные подсообщества [6]. Разработанный метод обладает следующими особенностями:

• применимость к ориентированным и неориентированным графам;

• учёт весов на рёбрах;

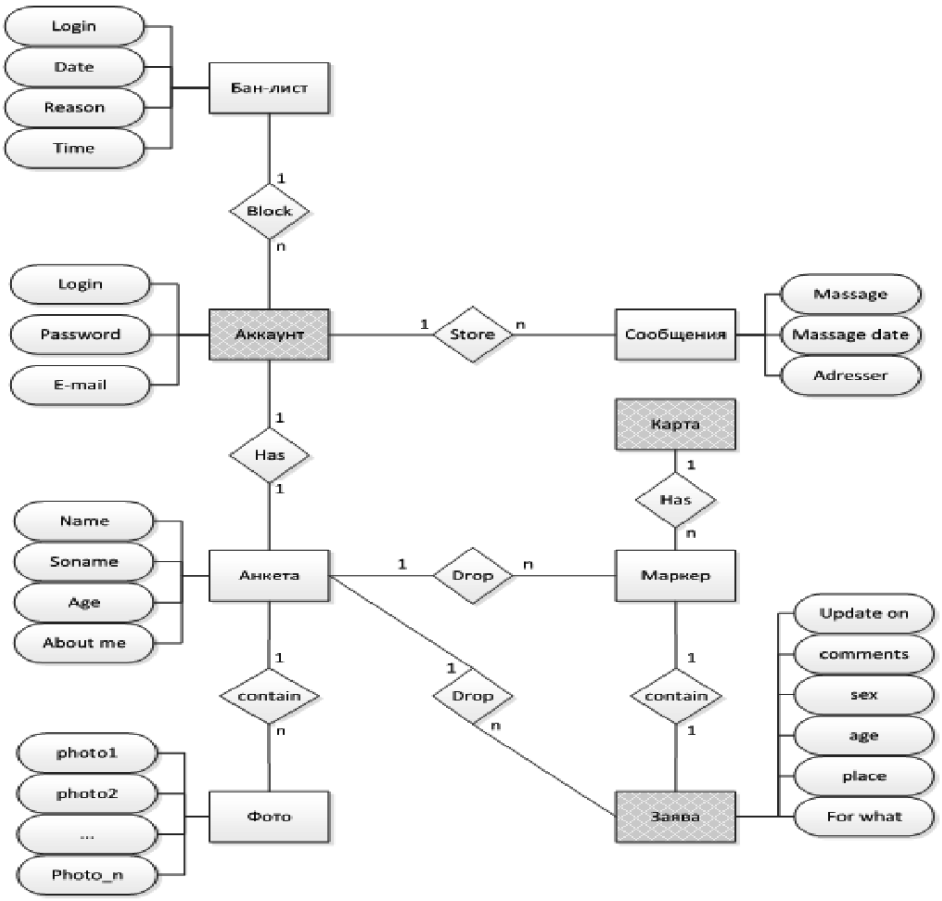
• поиск как пересекающихся, так и непересекающихся сообществ;

• поиск как локальных (среди ближайших контактов пользователя), так и глобальных сообществ;

• низкая вычислительная сложность;

• возможность распределённой реализации в рамках вычислительной модели Pregel [3].

ER-модель базы данных, интегрированной с алгоритмом показан на рисунке.



ER-модель базы данных

Заключение

Одной из доминирующих тенденций развития социальных сетей как социокультурного феномена является более глубокое понимание особенностей социального поведения человека и, как следствие, создание новых средств для самовыражения, а также обмена информацией и опытом. Разумно ожидать дальнейшего расширения пользовательской модели и функционала социальных сетей, что приведёт к появлению новых типов данных в виде объектов и связей социального графа и, как следствие, возможности более эффективно решать задачи, связанные с обработкой персональной информации.

Разработанное программное обеспечение упрощает взаимодействия менеджера рекламного агентства с социальной сетью Twitter при решении задачи медиапланирования.

Список литературы

1. Вестник Ленинградского государственного университета им. А.С. Пушкина. – №1. Т VII. –2013.
2. Труды Международного симпозиума «Надежность и качество». – Т I.– 2013.
3. International Journal of Open Information Technologies. – №1. Т II. – 2014.
4. Najork M., Wiener J. L. Breadth-first crawling yields high-quality pages. Proceedings of the 10th international conference on World Wide Web. – ACM, 2001. – С. 114-118.
5. Leskovec J., Faloutsos C. Sampling from large graphs. Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining. – ACM, 2006. – С. 631-636.
6. Gjoka M. et al. Practical recommendations on crawling online social networks. Selected Areas in Communications, IEEE Journal on. – 2011. – Т. 29. – №. 9. – С. 1872-1892.

МЕТОДЫ ЗАЩИТЫ ОТ ВРЕДОНОСНЫХ ПРОГРАММ НА ОСНОВЕ КОНТРОЛЯ ДОСТУПА К ФАЙЛАМ

Бальсина А.В., Короткова Н.Н.

Волжский политехнический институт, филиал Волгоградского государственного технического университета, Волжский, e-mail: anastasiybalsina@mail.ru

С появлением и развитием информационных технологий проблема хранения огромного количества данных разнообразного формата и содержания была решена. В этот момент и возникла новая проблема, важность которой трудно переоценить – как уберечь эти хранилища, носители и потоки данных от посягательства извне, которое может принести немалый вред. Основными методами защиты являются программные средства, что подразумевает защиту от потери самой информации, операционной системы, программного обеспечения или документа. Наибольшей