ПРИМЕНЕНИЕ АЛГОРИТМА ВЫДЕЛЕНИЯ СООБЩЕСТВ В ИНФОРМАЦИОННОМ ПРОТИВОБОРСТВЕ В СОЦИАЛЬНЫХ СЕТЯХ

Чесноков В.О.[1]

Социальные сети в настоящее время являются площадкой для информационного противоборства. При этом большинство существующих систем мониторинга ориентированы лишь на отслеживание количественных характеристик, поэтому они уязвимы для «вбросов» и «накручиваний» тем. Данная деятельность обычно осуществляется с помощью виртуальных пользователей (ботов), автоматических и автоматизированных. В статье представлен краткий обзор существующих методов обнаружения ботов, основанных на статистическом и семантическом анализе текстов, поведенческом анализе и теоретико–графовом подходе. Кроме того, указан пример применения алгоритма выделения сообществ для решения сопутствующей задачи — поиска лидеров общественного мнения. Предлагается новый подход обнаружения ботов, основанный на анализе сообществ графа ближайшего окружения пользователя. Предложенный метод был опробован на двух выборках виртуальных пользователей из социальной сети Livejournal: управляемых ботов и ботов, собранных вручную одним из пользователей. Для проверки использовалась выборка из 700 легитимных пользователей. Эксперименты показали высокие значения точности, полноты и меры F1 обнаружения виртуальных пользователей. Разработанный метод может быть использован как часть системы обнаружения ботов и при широком применении может существенно повысить стоимость создания правдоподобных аккаунтов виртуальных пользователей для злоумышленника.

***Ключевые слова**: информационное противоборство, безопасность коммуникаций, социальная сеть, социальный граф, выделение сообществ, боты, виртуальные пользователи, лидеры общественного мнения, виртуальные пользователи*

DOI: 10.21681/2311-3456-2017-1-37-44

Введение

Веб 2.0 стал новой формой потребления контента. Если раньше контент в интернете распространялся «по подписке», т.е. создавался владельцами сайта, его редакторами или журналистами, а посетители сайта были лишь его пассивными потребителями, то теперь контент создают сами пользователи. У них появилась возможность взаимодействия между собой и с контентом путем установления связей, оценок, комментариев, распространения информации и т.п. Ярчайший пример Веб 2.0 — онлайновые социальные сети.

На данный момент интернетом по всему миру пользуется более 3,3 миллиарда человек[2], в то время как число пользователей самой популярной в мире сети, Facebook, уже превышает полтора миллиарда[3]. При этом данное количество продолжает расти. В России, согласно данным ВЦИОМ[4],большинство россиян пользуются социальными сетями. Пользователи самостоятельно предоставляют о себе массу данных: пол, возраст, место проживания, место учебы и работы, предпочтения в литературе и музыке, хобби; связи с другими пользователями — дружественные и родственные; свои мнения и т.д.

Социальные сети стали альтернативными СМИ. Многие пользователи доверяют информации, полученной из социальных сетей («сарафанному радио») больше, чем традиционным источникам новостей — телевидению и газетам[5,6]. Косвенно данный факт подтверждается недавно принятым федеральным законом № 97-ФЗ от 5 мая 2014 года, приравнивающим крупных блогеров к СМИ.

Почти каждая крупная компания имеет представительство в нескольких социальных сетях, а некоторые мелкие представлены только таким образом. В последнее время все больше становится популярным мониторинг социальных сетей с точки зрения рейтинга какого-либо продукта или бренда[7,8]. На основе данных, автоматически собранных из социальных сетей, проводится оценка популярности и востребованности продукта или

1 Чесноков Владислав Олегович, МГТУ им. Н.Э.Баумнана, Москва, v.o.chesnokov@yandex.ru

2 http://www.internetlivestats.com/internet-users/

3 http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

4 http://wciom.ru/index.php?id=236&uid=115294

5 http://www.interfax.ru/russia/485226

6 http://www.forbes.ru/sobytiya/vlast/92590-kak-vlasti-chita-yut-vashi-blogi-rassledovanie-forbes

7 http://www.cossa.ru/149/17590/

8 http://www.likeni.ru/analytics/upravlenie-reputaciej-v-seti-avtomatizirovannij-i-ruchnoj-monitoring/

услуги, а также реакции потребителей на проведенные акции и специальные предложения[9].

Многие политики имеют свои страницы в социальных сетях, а некоторые их записи вызывали большой резонанс. Социальные сети могут повлиять на исход выборов за счет влияния на общественное мнение [1]. В свою очередь, события «арабской весны» наглядно продемонстрировали, что социальные сети могут играть серьезную роль в развитии политических событий и являться площадкой для информационного противоборства [2,3].

Информационное противоборство в социальных сетях

Разумеется, рост активности использования социальных сетей не может быть оставлен в стороне различными исследователями. Еще в конце 90-х начался поиск и изучение различных моделей взаимодействий в социальных сетях. Подробный обзор представлен в [4]. Однако существующие системы мониторинга (по крайней мере, предоставляющие информацию о своих возможностях), по большей части не используют богатое разнообразие математических моделей [5]. В основном мониторинг представляет собой сбор количественных показателей, таких как количество записей по теме, количество лайков к ним и т.п. Часто применяется анализ эмоционального окраса сообщений и строится тренд количественных характеристик[10].

Традиционно считается, что социальные сети почти не регулируются государством [2]. Однако еще в 2012 году служба внешней разведки России разместила заказ на разработку системы мониторинга и влияния на социальные сети[11]. В основном интерес спецслужбы состоял в мониторинге подозрительной активности в социальных сетях, создании систем раннего предупреждения о различных угрозах и формировании общественного мнения путем «вбросов» через сеть ботов. В середине этого года должны завершиться испытания системы мониторинга СМИ и социальных сетей Министерства обороны, предназначенной для отслеживания и анализа военно-политической, социально-экономической и общественно-политической обстановки в России и за рубежом[12]. Подобные системы имеются у МВД, ФСБ[13], у администрации президента, следственного комитета РФ и многих других федеральных служб РФ.

В США разведка на основе открытых источников (OSINT) является одной из основных разведывательных дисциплин. Бывший глава Разведуправления минобороны США считает, что до 90% разведданных управление получало из открытых источников[14]. Пропаганда в интернете производилась британскими и американскими спецслужбами по поводу событий в Афганистане, Ираке и Пакистане. В 2011 году DARPA объявило тендер на разработку SMISC — системы для отслеживания пропаганды против США и помощи в ведении контрпропаганды. На мониторинг социальных сетей был заказ и у ФБР. В бюро отметили, что «социальные сети стали основным источником разведывательной информации, так как в них можно найти первую реакцию на ключевые события»[15].

В последние годы Россия находится в состоянии информационной войны с США, считает председатель следственного комитета РФ Александр Бастрыкин[16], указывая в качестве основных приемов радикализацию идеологии и разжигание межэтнической розни и приводя в качестве примера вооруженный конфликт в Сирии. В качестве одной из мер противодействия он предлагает введение жесткого цензурирования Интернета по примеру Китая. Однако данная мера может быть довольно затратной и ненадежной: способы обхода блокировок постоянно совершенствуются (прокси, VPN, Tor, obfsproxy, передача информации по спутниковому телевидению в MPEG[17] и т.д.). Возможно, более продуктивным будет мониторинг с оперативным реагированием на информационные воздействия.

В Доктрине информационной безопасности РФ в качестве одной из угроз конституционным правам и свободам человека и гражданина указано «вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур». ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности.

9 http://www.cossa.ru/149/117540/
10 http://www.bbc.com/russian/russia/2015/12/151224_smj_sledcom_integrum
11 http://kommersant.ru/doc/2009256
12 https://lenta.ru/news/2015/01/28/monitor/
13 http://www.svoboda.org/content/article/24689413.html
14 http://vpk-news.ru/articles/7324
15 http://www.bbc.co.uk/russian/international/2012/01/120127_fbi_social_networks.shtml
16 http://kommersant.ru/doc/2961578
17 https://geektimes.ru/post/274827/

Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий» указывает достоверность информации как одно из свойств, подлежащих защите. Губанов и др. [4] выделяют задачу анализа и обеспечения информационной безопасности социальных сетей как двойственную к задаче информационного управления и манипулирования.

Определение ботов и лидеров общественного мнения

В условиях информационного противоборства можно выделить две задачи, которые можно решить с помощью анализа структуры социальной сети. Это задачи выявления лидеров общественного мнения – персон, которые имеют наибольшее влияние на других пользователей социальной сети – и виртуальных пользователей (ботов), которые могут влиять на численные показатели систем мониторинга путем создания большого количества сообщений с определенной тематикой. Обе задачи являются задачами бинарной классификации.

Выделению лидеров общественного мнения посвящено множество исследований. Например, в социальной сети Twitter исследователи выделяют более 75 различных метрик влияния пользователей [6], среди которых заслуживают отдельного упоминания PageRank [7], промежуточность и близостная центральность (closeness centrality). Стоит обратить внимание на то, какой граф нужно анализировать. Очевидно, что проводить анализ графа всей сети затратно и нецелесообразно, как минимум потому, что эксперт в одной области может совершенно не разбираться в другой. Обычно рассматривается подграф, соответствующий некоторой теме или событию, вершинами которого являются участники обсуждения. Известно, что мнения агентов в рамках одной группы (сообщества) сходятся и практически не поддаются внешнему влиянию [4]. Поэтому в некоторых задачах помимо лидеров темы, имеет смысл предварительно определить в графе темы группы пользователей, имеющих одно мнение, с помощью алгоритма выделения сообществ и определить лидеров мнений в каждом сообществе независимо. Например, если тема биполярна, таким образом обнаруживаются лидеры мнения противника, на которых следует попробовать оказать влияние.

Разработка универсального метода обнаружения ботов, по крайней мере в ближайшее время, не представляется возможной, поскольку виртуальные пользователи, управляемые человеком, могут быть практически неотличимы от реальных пользователей. В свою очередь, поведение новых или малоактивных пользователей порой очень схоже с поведением ботов. Кроме того, иногда реальные пользователи (обычно несовершеннолетние или малообеспеченные) готовы за небольшую плату или безвозмездно выполнять задачи ботов, используя свой реальный аккаунт в социальных сетях: накрутку постов, накрутку количества подписчиков, троллинг других пользователей и т.п. Тем не менее, необходимо постоянное совершенствование методов обнаружения ботов, что позволит существенно сократить количество виртуальных пользователей и повысить стоимость их создания, оставив возможность поддержания таких пользователей лишь единичным субъектам [8]. Отметим некоторые из основных таких способов.

Во-первых, это поведенческий анализ. Его используют преимущественно сами социальные сети как один из внутренних механизмов. В основном таким образом происходит обнаружение пользователей, нарушающих тем или иным образом пользовательское соглашение социальной сети. Резкое изменение активности обычно ведет к появлению CAPTCHA; при получении неверного ответа происходит блокировка или заморозка аккаунта. Точные механизмы обнаружения подозрительной активности обычно составляют тайну, хотя при планомерном исследовании методом проб и ошибок злоумышленник может найти методы обхода данных ограничений. Извне проводить подобный анализ довольно затруднительно, однако так можно вычислить очень простых автоматических ботов. Например, некоторые из них проявляют свою активность по расписанию и их легко будет обнаружить по временному профилю активности [9].

Другой подход заключается в статистическом и семантическом анализе текстов [10]. В случае, если группа ботов управляется одним человеком и идет активное обсуждение некоторой темы, тексты управляемых пользователей могут быть схожи между собой или даже идентичны друг другу [11]. Кроме того, у каждого человека есть характерные особенности речи и лексикона, что позволяет на основе анализа корпуса текстов пользователя ставить ему в соответствие уникальный идентификатор. При мониторинге, охватывающем достаточно большую часть социальной сети возможно найти пользователей с одинаковым идентификатором. С большой вероятностью можно утверждать, что часть или все такие пользователи будут ненастоящими (ботами или «фейками»). В некоторых исследованиях с помощью анализа тональности

сообщений составляется профиль эмоций пользователя [10]. Боты, предназначенные для «вбросов» обычно не обладают целостным профилем эмоций. Помимо этого, производится анализ количества ссылок в сообщениях и количества ответов другим пользователям [12].

Третий подход представляет собой анализ связей пользователя. Простейшие методы основаны на анализе количества связей пользователя и отношения количества входящих и исходящих связей [12]. Методы, используемые для определения ботнетов, подходят и для анализа социального графа. Зараженные сегменты сети можно определить с помощью алгоритма выделения сообществ [13, 14], примененного к графу взаимодействия узлов; боты определяются по аномальному трафику.

Объединяет данные подходы комбинированный метод, заключающийся в использовании нескольких одновременно. Зачастую он строится на машинном обучении [10, 12], и позволяет на основе многих факторов выносить решение об обнаружении бота с некоторой долей уверенности. Основная задача заключается в отборе значимых факторов, подборе классификаторов и обучении модели. Даже если не использовать машинное обучение, использование нескольких методов повышает вероятность обнаружения поддельных аккаунтов.

Стоит отметить, что описанные методы возможно использовать для выявления недобросовестных СМИ, которые занимаются цитированием друг друга и публикуют недостоверную информацию.

Метод обнаружения ботов с помощью выделения сообществ

Известно, что социальные связи человека имеют свои особенности. Например, число связей, которые человек может эффективно поддерживать, ограничено парой сотен. Данный предел был выведен антропологом Р.Данбаром [15] и назван в его честь. Человек естественным образом участвует в нескольких сообществах, соответствующих его сферам деятельности и интересам — у него есть одноклассники, коллеги по работе, родственники и т.д.

Таким образом, степень каждой вершины в графе социальной сети ограничена сверху. Поэтому целесообразно вместо анализа графа всей социальной сети провести анализ графов ближайшего окружения пользователей. Скорее всего, графы реальных людей будут сильно отличаться от графов виртуальных пользователей, ведь у последних граф будет сформирован искусственным образом.

Для проверки гипотезы были использованы три списка пользователей социальной сети Livejournal:

1. 668 пользователей из утекшего списка управляемых ботов18;
2. боты, отобранные вручную одним из пользователей сети с помощью аккаунта-приманки19(1366 профилей);
3. выборка из 700 случайно выбранных пользователей, которые считались не ботами.

Для каждого из пользователей был составлен граф ближайшего окружения, состоящий из всех друзей пользователя и связей между ними. Был использован граф сети Livejournal, полученный в работе [16], часть данных была собрана заново. После этого к каждому из графов был применен алгоритм выделения сообществ, основанный на максимизации модулярности.

На рис. 1 представлен график количества сообществ для каждой из трех групп. В основном обычные пользователи имеют около пяти сообществ, в то время как для многих ботов их либо меньше четырех, либо больше десяти. Некоторые боты вообще не имеют сообществ либо имеют только одно. При этом средний размер сообществ (см. рис. 2) у ботов обычно либо больше, чем у нормальных пользователей, либо представляет величину, меньшую 5. У большинства ботов из числа управляемых средний размер сообщества превышает 100 человек, при этом количество их «друзей» может исчисляться несколькими сотнями пользователей, как видно на рис. 3. У большинства нормальных пользователей количество друзей лежит в интервале от 50 до 200, что согласуется с числом Данбара.

Для определения ботов был использован набор из простых правил:

1. Если количество друзей пользователя больше максимального или меньше минимального, то пользователь — бот.
2. Сообщества размером меньше минимального не учитываются.
3. Если количество сообществ больше максимального или меньше минимального, то пользователь — бот.
4. Иначе пользователь не бот.

В качестве параметров правил были выбраны следующие значения: максимальное количество сообществ — 9,

18 http://www.svoboda.org/content/transcript/26899521.html
19 http://che-love-chek.livejournal.com/profile

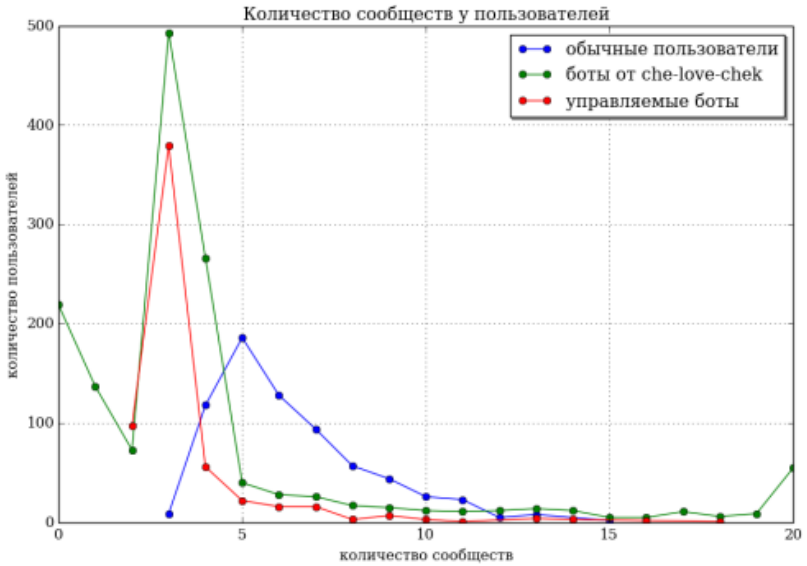

Рис. 1. *Количество сообществ у пользователей. Учитывалось не более 20 сообществ.*

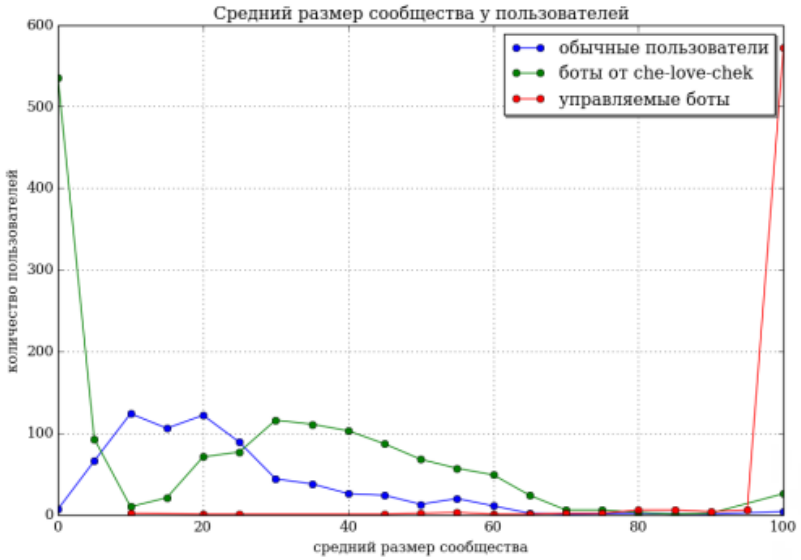

Рис. 2*. Средний размер сообществ у пользователей с шагом 5.*

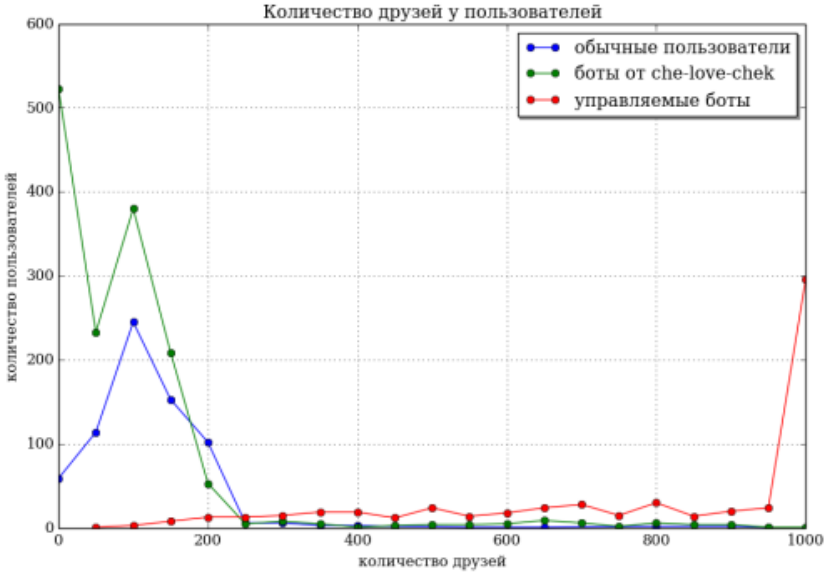

Рис. 3*. Количество друзей у пользователей с шагом 50.*

минимальный размер сообщества — 15, минимальное количество сообществ — 2, максимальное число друзей — 500, минимальное количество друзей — 30. Для каждой из выборок были рассчитаны значения

$$A = \frac{TP+TN}{TP+TN+FP+FN}, \quad (1)$$

$$P = \frac{TP}{TP+FP}, \quad (2)$$

$$R = \frac{TP}{TP+FN}, \quad (3)$$

$$F_1 = \frac{2PR}{P+R} = \frac{2TP}{2TP+FP+FN}, \quad (4)$$

где TP и TN — количество правильно определенных ботов и обычных пользователей соответственно; FP и FN — ошибки первого и второго рода; A — доля правильных ответов (accuracy); P — точность; R — полнота; F_1 — F-мера. Результаты для всех выборок представлены в табл. 1.

Таблица 1.
Точность определения ботов.

	A	**P**	**R**	**F_1**
управляемые боты	0.93	0.88	0.98	0.93
боты от che-love-chek	0.93	0.94	0.95	0.95
все боты	0.94	0.96	0.96	0.96

Таким образом, даже простой анализ, затрагивающий лишь количество сообществ и их размер, позволяет отделить простых ботов от реальных людей. Большинство создателей виртуальных пользователей не утруждают себя таким уровнем проработки, поскольку подобный анализ почти невозможен без привлечения автоматизированных средств. Повысить качество обнаружения возможно с помощью качественного анализа полученных сообществ: людей в сообществе обычно объединяет некоторый внешний фактор: общее место учебы или работы, схожие интересы или взгляды. Поскольку социальные сети характеризуются богатыми профилями, заполняемыми пользователями, а также позволяют создавать виртуальные сообщества по интересам, можно предположить, что для большинства выделенных сообществ образующий внешний фактор будет определяться по профилям пользователей. Соответственно, если у большей части сообществ некоторого пользователя невозможно выделить общий атрибут, то это повышает вероятность того, что данный пользователь является ботом.

Помимо этого, чтобы повысить достоверность результатов, аналогичные действия стоит произвести со всеми вершинами графа ближайшего окружения пользователя, т.е. с друзьями рассматриваемого пользователя. Очевидно, что большинство профилей друзей тоже должно соответствовать правилу: иначе, если большинство друзей пользователя боты, то и сам он скорее всего бот. Кроме того, если объединение всех графов ближайшего окружения друзей пользователей образует компоненту связности общего графа социальной сети или имеет малое количество связей с ней, то данное множество вершин состоит как минимум из подозрительных аккаунтов. Таким образом, сложность создания правдоподобного виртуального пользователя возрастает на несколько порядков: злоумышленник должен не только создать правдоподобный профиль одного пользователя, но и для всех его «друзей», а также установить двусторонние связи со многими существующими пользователями социальной сети. Если изначально злоумышленнику нужно создать N профилей (1 «главный» профиль и N-1 друзей), то теперь ему придется создать $O(N^d)$ друзей друзей, где N — среднее количество друзей пользователя, а d — диаметр анализируемого графа. При этом предлагаемый способ анализа не несет существенных дополнительных расходов при условии полномасштабного мониторинга социальной сети.

Заключение

Социальные сети завоевали доверие пользователей и стали для многих основным источником информации. В настоящее время социальные сети являются площадкой для информационного противоборства, и возникает необходимость выработки средств защиты от влияния и «вбросов» противника. Одна из основных задач заключается в поиске автоматических или автоматизированных виртуальных пользователей.

В данной статье был предложен метод выявления ботов на основе анализа сообществ графов их ближайшего окружения. Разработанный метод был опробован на двух выборках ботов из социальной сети Livejournal и показал высокие значения численных мер оценки качества алгоритмов бинарной классификации. Метод может быть использован как один из элементов подсистемы обнаружения виртуальных пользователей в системе мониторинга социальных сетей.

***Научный руководитель**: Ключарёв Петр Георгиевич, к.т.н., доцент кафедры «Информационная безопасность» МГТУ им. Н.Э.Баумана. pgkl@yandex.ru*

Литература

1. Jacob Ratkiewicz, Michael Conover, Mark Meiss et al. Detecting and Tracking Political Abuse in Social Media. In Proceedings of the 5th International AAAI Conference on Weblogs and Social Media (ICWSM). 2011.
2. Вельц С.В. Моделирование информационного противоборства в социальных сетях на основе теории игр и динамических байесовских сетей // Инженерный журнал: наука и инновации. Электронное научное техническое издание. 2013. № 11(23). С. 39.
3. Haque Khondker Habibul. Role of the New Media in the Arab Spring. Globalizations. 2011. Vol. 8. No. 5. pp. 675–679.
4. Губанов Д.А., Новиков Д.А., Чхартишвили А.Г. Модели информационного влияния и информационного управления в социальных сетях // Проблемы управления. 2009. № 5. С. 28-35.
5. Базенков Н.И, Губанов Д.А. Обзор информационных систем анализа социальных сетей // Управление большими системами: сборник трудов. 2013. № 41. С. 357-394.
6. Riquelme Fabian. Measuring user influence on Twitter: A survey. CoRR. 2015. No. abs/1508.07951.
7. Tang Lei, Liu Huan. Community Detection and Mining in Social Media. Synthesis Lectures on Data Mining and Knowledge Discovery. 2010. Vol. 2. No. 1. pp. 1-137.
8. Лыфенко Н.Д. Виртуальные пользователи в социальных сетях: мифы и реальность // Вопросы кибербезопасности. 2014. № 5(8). С. 17-20.
9. Ghosh Rumi, Surachawala Tawan, Lerman Kristina. Entropy-based Classification of ‹Retweeting' Activity on Twitter. CoRR. 2011. No. abs/1106.0346.
10. Dickerson John P., Kagan Vadim, Subrahmanian V. S. Using sentiment to detect bots on Twitter: Are humans more opinionated than bots? In Proceedings of the IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, 2014, Beijing, China, August 17-20, 2014. pp 620-627.
11. Yang Chao, Harkreader Robert Chandler, Gu Guofei. Recent Advances in Intrusion Detection. In Proceedings of the 14th International Symposium, 2011, Menlo Park, CA, USA, September 20-21, 2011. pp. 318-337.
12. Wang Alex Hai. Data and Applications Security and Privacy XXIV. In Proceedings of the 24th Annual IFIP WG 11.3 Working Conference, Rome, Italy, June 21-23, 2010. pp. 335-342.
13. Wang Jing, Paschalidis Ioannis Ch. Botnet Detection using Social Graph Analysis. CoRR. 2015. No. abs/1503.02337.
14. Qiang Cao, Michael Sirivianos, Xiaowei Yang et al. Aiding the Detection of Fake Accounts in Large Scale Social Online Services. In Proceedings of the 9th USENIX Symposium on Networked Systems Design and Implementation (NSDI 12), San Jose, CA: USENIX, 2012. pp. 197-210.
15. Dunbar R.I.M. Neocortex size as a constraint on group size in primates. Journal of Human Evolution. 1992. Vol. 22, No. 6. pp. 469-493
16. Ключарёв П.Г., Чесноков В.О. Исследование спектральных свойств социального графа сети LiveJournal // Наука и образование. Электронное научно-техническое издание. 2013. № 9. С. 391-400.

APPLICATION OF THE COMMUNITY ALLOCATION ALGORITHM IN THE INFORMATION CONFRONTATION IN THE SOCIAL NETWORKS

Chesnokov V.O.[20]

Abstract*.Social networks are currently a site for information confrontation. However, most of the available monitoring systems make a focus on tracking quantitative characteristics only, therefore they are vulnerable to a series of fibs and topic twisting. These activities are usually done by virtual users (bots), which are automatic and automated. The article provides a brief review of available methods of bot identification, which are based on static and semantic text analysis, behavioural analysis and theoretical graph approach. Moreover, it gives an example of applying community allocation algorithm to solve an accompanying problem – identification of the public opinion leaders. It suggests a new approach to bot identification, which is based on analysis of graph communities of the nearest user environment. The suggested method was tested on two samples of virtual users from Livejournal social network: managed bots and bots manually assembled by one of the users. The sample consisted of 700 legitimate users. The experiment had high values of accuracy, exhaustiveness and F1 measure of virtual user identification. The developed method can be used as a part of the bot identification system and, if applied widely, may significantly increase the cost of creating realistic virtual user accounts for the hackers.*

Keywords*: information warfare, social network, social graph, ego–network, community detection, bots, virtual users, public opinion leaders.*

20 Vladislav Chesnokov, Bauman Moscow State Technical University, Moscow, v.o.chesnokov@yandex.ru

References

1. Jacob Ratkiewicz, Michael Conover, Mark Meiss et al. Detecting and Tracking Political Abuse in Social Media. In Proceedings of the 5th International AAAI Conference on Weblogs and Social Media (ICWSM). 2011.
2. Vel'ts S.V. Modelirovanie informatsionnogo protivoborstva v sotsial'nyh setyah na osnove teorii igr i dinamicheskih bajesovskih setej // Inzhenernyj zhurnal: nauka i innovatsii. Elektronnoe nauchnoe tehnicheskoe izdanie. 2013. № 11(23), p. 39.
3. Haque Khondker Habibul. Role of the New Media in the Arab Spring. Globalizations. 2011. Vol. 8. No. 5, pp. 675–679.
4. Gubanov D.A., Novikov D.A., CHhartishvili A.G. Modeli informatsionnogo vliyaniya i informatsionnogo upravleniya v sotsial'nyh setyah // Problemy upravleniya. 2009. № 5, pp. 28-35.
5. Bazenkov N.I, Gubanov D.A. Obzor informatsionnyh sistem analiza sotsial'nyh setej // Upravlenie bol'shimi sistemami: sbornik trudov. 2013. № 41, pp. 357-394.
6. Riquelme Fabian. Measuring user influence on Twitter: A survey. CoRR. 2015. No. abs/1508.07951.
7. Tang Lei, Liu Huan. Community Detection and Mining in Social Media. Synthesis Lectures on Data Mining and Knowledge Discovery. 2010. Vol. 2. No. 1, pp. 1-137.
8. Lyfenko N.D. Virtual'nye pol'zovateli v sotsial'nyh setyah: mify i real'nost' // Voprosy kiberbezopasnosti. 2014. № 5(8), pp. 17-20.
9. Ghosh Rumi, Surachawala Tawan, Lerman Kristina. Entropy-based Classification of ‹Retweeting' Activity on Twitter. CoRR. 2011. No. abs/1106.0346.
10. Dickerson John P., Kagan Vadim, Subrahmanian V. S. Using sentiment to detect bots on Twitter: Are humans more opinionated than bots? In Proceedings of the IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, 2014, Beijing, China, August 17-20, 2014. pp 620-627.
11. Yang Chao, Harkreader Robert Chandler, Gu Guofei. Recent Advances in Intrusion Detection. In Proceedings of the 14th International Symposium, 2011, Menlo Park, CA, USA, September 20-21, 2011, pp. 318-337.
12. Wang Alex Hai. Data and Applications Security and Privacy XXIV. In Proceedings of the 24th Annual IFIP WG 11.3 Working Conference, Rome, Italy, June 21-23, 2010, pp. 335-342.
13. Wang Jing, Paschalidis Ioannis Ch. Botnet Detection using Social Graph Analysis. CoRR. 2015. No. abs/1503.02337.
14. Qiang Cao, Michael Sirivianos, Xiaowei Yang et al. Aiding the Detection of Fake Accounts in Large Scale Social Online Services. In Proceedings of the 9th USENIX Symposium on Networked Systems Design and Implementation (NSDI 12), San Jose, CA: USENIX, 2012, pp. 197-210.
15. Dunbar R.I.M. Neocortex size as a constraint on group size in primates. Journal of Human Evolution. 1992. Vol. 22, No. 6, pp. 469-493
16. Klyucharev P.G., CHesnokov V.O. Issledovanie spektral'nyh svojstv sotsial'nogo grafa seti LiveJournal // Nauka i obrazovanie. EHlektronnoe nauchno-tehnicheskoe izdanie. 2013. № 9, pp. 391-400.