АНАЛИЗ АЛГОРИТМОВ ВЫЧИСЛЕНИЯ УРОВНЯ ДОВЕРИЯ К ПОЛЬЗОВАТЕЛЮ В СОЦИАЛЬНОЙ СЕТИ

В.Н. Максименко, *доцент кафедры «Информационная безопасность» МТУСИ, к.т.н. vladmaks @yandex.ru;*
Н.Д. Долгова, *студент МТУСИ, sunnatal@mail.ru*

УДК 621.391

Аннотация. Статья посвящена анализу алгоритмов, вычисляющих уровень доверия к пользователю социальной сети. Представлены основные характеристики доверия пользователей в рамках компьютерных наук. Приведены зарубежные алгоритмы для вычисления уровня доверия между пользователями социальной сети, работа алгоритмов визуализирована на схемах. Описаны примеры использования выбранных алгоритмов. Произведен анализ и оценка различных алгоритмов определения степени доверия пользователей социальной сети к виртуальным друзьям.

Ключевые слова: алгоритмы вычисления уровня доверия; социальный граф; системы рекомендаций; безопасность в социальной сети; факторы доверия; социальный капитал.

ANALYSIS OF ALGORITHMS THAT CALCULATE THE LEVEL OF TRUST IN THE USER OF A SOCIAL NETWORK

Vladimir Maksimenko, *associate professor of the «Information security» MTUCI, candidate of technical sciences;*
Natalia Dolgova, *student MTUCI.*

Annotation. The article is devoted to the analysis of algorithms that calculate the level of trust in the user of a social network. The main characteristics of user confidence in computer science are presented. Foreign algorithms for calculating the level of trust between users of the social network are given; the work of the algorithms is visualized in the diagrams. Examples of using selected algorithms are described. The analysis and evaluation of various algorithms for determining the degree of trust of social network users to virtual friends has been made.

Keywords: algorithms for calculating the level of trust; social graph; recommendation systems; security in a social network; trust factors; social capital.

В зависимости от класса решаемых задач, контекста, расстояния и степени связности системы распределенной обработки информации могут быть отнесены к вычислительным, информационным, автоматизированным или социальным сетям, посредством которых субъекты информационных отношений решают не связанные, слабосвязанные или сильно связанные задачи [1-5]. Социальная сеть – это программно-техническая платформа для создания и функционирования социальных сообществ. Известно несколько наиболее распространенных социальных сетей, которых отдельные граждане (зарегистрированные пользователи социальной сети) или организации, в лице своих представителей, объединяются в социальные сообщества. Такие сообщества могут создаваться и устойчиво функционировать как на основе взаимных интересов отдельных членов сообщества, так и степени доверия к источникам информации. В настоящее время можно выделить три основных типа доверия: субъект-объект, объект-объект и субъект-субъект. В качестве «субъекта» выступает «человек», а «объектом» является «компьютер». Один из наиболее важных факторов, влияющих на отношения между людьми, является доверие. Доверие среди пользователей в социальных сетях представляет большой интерес не только в области информатики, но и в психологии и социологии. Поскольку социальные сети зачастую используют для распространения мнений

определенной направленности, что объясняется пониженной критичностью восприятия пользователями информации [6]. Знания о доверии в социальных сетях также могут использоваться в системах рекомендаций, что делает данную работу еще более интересной для исследователей.

Приведем наиболее распространенные характеристики доверия. Есть два основных типа доверия: прямое доверие и доверие к рекомендациям. Прямое доверие – доверие на основании личного опыта. Доверие к рекомендациям – доверие, основанное на мнении авторитета, группы людей, пропаганды (если *A* доверяет *B*, а *B* доверяет *C*, то *A* в некоторой степени тоже доверяет *C*) [7].

В настоящее время существует несколько различных подходов к определению доверия между пользователями в пиринговых (равноправных) сетях, а также в социальных сетях. В данной работе рассматривается доверие, которое является результатом неоднократных прямых взаимодействий между пользователями.

Существует три важных аспекта доверия: (a) доверие зависит от поведения пользователя, (б) доверие является динамичным и (c) доверие зависит от контекста.

Поведение пользователей (a): Социальное доверие зависит от поведения человека в социальных сетях. В контексте онлайн-сообщества, поведение человека зависит от его социального капитала (взаимодействия) в сообществе.

Важный элемент определения социального доверия – это контекст (b). Проиллюстрируем значение контекста на примере. Член *X* в сообществе доверяет рекомендациям другого члена *Y* по поводу автомобилей. Но в то же время, *X* не может доверять рекомендациям *Y* по поводу компьютерных игр или музыки. Это отражает реальность нашей жизни.

Временной фактор (c). Другим важным аспектом доверия является то, что оно зависит от времени. Распад социального капитала через какое-то время – это факт общественной жизни в социальных сетях. Взаимодействие, которое произошло в последнее время, может иметь большую ценность чем то, которое произошло некоторое время назад. Поэтому время является важным фактором для фиксации изменения в поведении индивида. Например, член *X* может иметь хорошие отношения с другим членом *Y* во время *t*, но эта связь может ослабевать, при отсутствии взаимодействия между ними.

Существует два типа взаимодействий: активный и пассивный. Пример активного взаимодействия включает в себя большое количество друзей, регулярные публикации, комментирование других членов и т. д. Однако не все члены сообщества – активные участники. Есть значительное количество членов, которые являются пассивными участниками сообщества. Взаимодействие пассивных членов в сообществе включает чтение статей, регулярные посещения сообщества и т. д. Эти члены могут не участвовать или не делиться своим опытом или чувствами, но они являются потребителями информации, что тоже очень ценно. Эти два типа взаимодействия коллективно создают **социальный капитал** сообщества и используются для оценки социального доверия.

Группы, где люди могут делиться своим опытом и личным мнением, а также получать богатый опыт и знания других членов называются сообщества. А для поставщиков услуг такие группы – отличная площадка для оперативной связи с клиентами. Но для успеха сообщества критическим фактором является доверие его членов друг к другу. Без доверия люди не захотят делиться своими знаниями и опытом из-за страха, что их публикации и идентификационные данные будут использованы неправильно или даже незаконно. Таким образом, актуальной становится задача построения сети доверия.

Алгоритм *STrust* [7, 8] находит пути для решения поставленной задачи. Алгоритм *STrust* для создания сообществ доверия в социальной сети, в котором участники доверяют друг другу, приведен на рис. 1.

Рисунок 1

Алгоритм *STrust* состоит из пяти шагов:

Шаг первый. Личный профиль: пользователь сначала регистрируется в социальной сети и создает учетную запись. Затем пользователь предоставляет личные данные, которыми он хотел бы поделиться с другими членами сообщества, такие как адрес электронной почты, дата рождения, хобби и т. д.

Шаг второй. Персональная идентификация: этот шаг предполагает представление личности пользователя. Например, выбор изображения или «аватара», выбор интересующих событий (подписаться на интересные страницы), определение списка друзей. Выбор друзей – это один из примеров установления личности пользователя в сообществе. Модель пользователя строится на основе личного профиля и персональной идентификации.

Шаг третий. Социальный капитал (социальная активность): пользователи строят свой социальный капитал, взаимодействуя друг с другом. Примеры взаимодействий: приглашение кого-то в друзья, ответ на приглашение дружить, давать комментарии по содержанию контента другим пользователям и т. д. Цель этого шага – создать среду для взаимодействия между пользователями.

Шаг четвертый. Социальное доверие: на этом этапе производится оценка доверия к отдельному пользователю или к сообществу в целом на основе социального капитала. Социальное доверие может также включать некоторую информацию о личности и профиле в зависимости от модели доверия, используемой для оценки. Социальная модель в данном алгоритме строится на основе первых двух шагов.

Шаг пятый. Рекомендация: последний шаг в рассматриваемом подходе является рекомендация. Данная структура поддерживает два типа рекомендаций: (а) рекомендации, основанные на контенте, который публикует пользователь на своей странице и (б) рекомендации, основанные на совместной фильтрации. Построение прогнозов предпочтений пользователя на основе известных предпочтений группы пользователей называется совместной фильтрацией.

(а) Рекомендации на основе контента (содержания) строятся на сходстве между двумя пользователями, хотя они могут и не взаимодействовать напрямую. Здесь используется модель пользователя (персональная идентификация и личный профиль) для поддержки таких рекомендаций.

(б) Рекомендации, основанные на совместной фильтрации, строятся на сходстве между двумя пользователями (на основе взаимодействий). Здесь используется социальная модель (социальный капитал и социальное доверие) для поддержки таких рекомендаций.

Цель рекомендаций – сделать онлайн-сообщество релевантным для его членов, чтобы мы могли увеличить социальный капитал и социальное доверие, которое, в свою очередь, используется в рекомендации, чтобы предлагать выполнение новых действий или контент. Этот цикл будет продолжаться до тех пор, пока не удастся построить сеть доверия.

В рассмотренной модели выделены различные типы взаимодействий между пользователями. Ясно прослеживается разница между доверием, основанном на личном опыте пользователя, и доверием на основе мнения других участников сообщества.

Модель социального доверия, *STrust* определяет социальное доверие как твердое убеждение в компетентности субъекта действовать в соответствии с ожиданиями к нему, но это твердое убеждение не является фиксированным значением, связанным с объектом, оно применяется только в определенном контексте в любое данное время.

Следующий алгоритм для вычисления социального доверия *SocialTrust* [9], который предоставляет пользователям сообщества динамические значения для определения уровня доверия. В реализации алгоритма *SocialTrust* используются персонализированный механизм обратной связи для адаптации по мере развития сообщества и отслеживание поведения пользователей. *SocialTrust* поддерживает надежное установление уровня доверия даже при наличии крупномасштабного сговора со стороны злонамеренных участников сообщества. Цель *SocialTrust* – увеличение онлайн сообществ за счет предоставления рейтинга доверия для каждого пользователя.

Рассмотрим сценарий, в котором пользователь – инициатор взаимодействия, имеет информационную потребность (например, ищет работу в Москве или ищет хороший ресторан). Основной сценарий: пользователь просматривает свои отношения до некоторого радиуса поиска кандидатов; на основе анализа профилей (профилей друзей, друзья друзей и т.д.), он создает набор кандидатов, которые могут удовлетворить его потребность в информации; на основе предоставленного рейтинга доверия он выбирает топ наиболее доверенных кандидатов-пользователей; он спрашивает всех кандидатов из топа; если он удовлетворен ответами, он оставляет положительную обратную связь; в противном случае он оставляет негативный отзыв.

Настройка моделирования. Моделирование начинается с присвоения каждому пользователю в сети доверия по умолчанию. После этого пользователи выбираются случайным образом, чтобы начать просмотр сеанса для удовлетворения конкретной потребности в информации, пользователи поддерживают обратную связь с системой и через регулярные промежутки времени система рассчитывает уровень доверия для каждого пользователя в сети для использования в следующем цикле. Для каждого просмотра сессии моделируется большой обзор отношений, основанных на группе доверия с радиусом 7 узлов. В группе доверия осуществляется просмотр пользователей с использованием случайного выбора до восьми случайных соседей, выбранных на каждом шагу. Такая большая группа доверия выбирается намеренно (охватывает в среднем 26 тыс. пользователей), чтобы получить качественную оценку значения доверия, при выборе меньшей группы большое число «вредоносных» пользователей исказит результаты ответов в каждом сеансе просмотра.

Существует потребность в исходной информации от пользователя. Для этого используется запрос случайным образом выбранных пользователей из пространства всех профилей *MySpace*, взвешенный по количеству профилей, в которых он происходит. Профиль, встречающийся во время просмотра, считается кандидатом.

Поведение пользователя. Учитывается два типа пользователей: «вредоносные» пользователи, которые всегда предоставляют неверный ответ и обычные пользователи, которые только иногда случайно могут дать неверный ответ.

Расчет доверия: все расчеты доверия выполняются, используя метод Якоби [10] для 25 итераций и параметр смешивания $\lambda = 0{,}85$. Во всех экспериментах цикл состоит из 5000 сеансов просмотра. Есть 30 симуляторов циклов. Для каждого запроса пользователи обеспечивают обратную связь более 20 наиболее доверенных пользователей, с которыми они сталкиваются. Результаты отчета за последние 5000 сеансов просмотра – усредненные более пяти симуляций. Для компонента качества ссылок опираются на модель скользящего случайного блуждания с объемом $k = 3$ и экспоненциальный поправочный коэффициент с $\psi = 0{,}5$ и $\delta = 0{,}5$.

Рассмотренная модель прогнозирования доверия между пользователями интернет-сообществ, является примером, в котором используются только отношения между субъектами при определении уровня доверия. Здесь приводится анализ взаимодействий пользователей в конкретной социальной сети. Доверие вычисляется на основе этих взаимодействий.

Следующий алгоритм *TrustMail* [11] для сетей с рейтингом доверия, основанном на социальном графе. В данном алгоритме социальный граф состоит из узлов, представленных пользовательскими профилями и ребер, представленных социальными связями между профилями. Осуществляется построение рейтинговой схемы.

Описание модели *TrustMail*. Есть две переменные: g – процент хороших (доверенных) узлов и p_a – точность распознавания хороших узлов. Когда узел дает неточный рейтинг, он может оценивать хороший узел как не доверенный, или оценивать плохой узел как доверенный.

Информация из узлов с нулевыми рейтингами игнорируется, так как большое количество неправильной информации может быть получено, когда плохой узел неправильно оценивается как доверенный.

Дана общая точность прямых рейтингов, первоначально назначенных в сети ($g * p_a$). Назовем ее начальной точностью в сети и представляем с помощью переменной a. Первоначальная точность – это показатель того, насколько часто рейтинги у пользователей в сети согласуются с истинным значением в соответствии с источником (но это не показатель точности оценки пользователя в отношении его собственных убеждений).

Визуализация расчета рейтинга узлами (рис. 2). A – узел, для которого рассчитывается уровень доверия. Узел G – источник. Источник опрашивает каждого из соседей, которому он дал рейтинг с положительной репутацией.

Каждый из доверенных соседей источника вернет свой рейтинг для пользователя. Узлы B и C будут возвращать рейтинги, рассчитанные через узел D. A рейтинг репутации от узла D будет получен с учетом рейтингов от узлов E и F. Значения кэшируются, так как нам необходимо будет второй раз воспользоваться рейтингом репутации.

Далее источник будет оценивать полученные рейтинги и округлять конечное значение. Это округленное значение – выведенный результирующий рейтинг репутации от источника до пользователя.

Узел будет делать правильный вывод, если большинство его соседей вернет правильный рейтинг для пользователя. Поскольку плохие узлы всегда отвечают неверно, точность хороших узлов должна компенсироваться, чтобы получить правильный вывод от большинства голосов. Таким образом, чтобы получить правильный вывод, начальная точность должна быть равна менее 0,5.

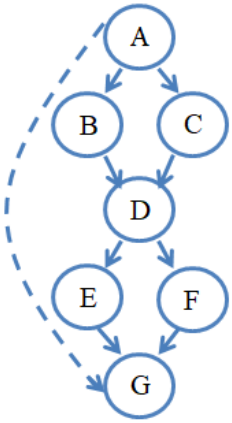

Рисунок 2

Пусть $a = g * p_a$. с n узлами, вероятность того, что большинство узлов будут правильно оценивать приемник, заданный биномиальным распределением. Биномиальное распределение может быть аппроксимировано нормальным распределением со средним по центру. Центральная предельная теорема гласит, что с ростом n биномиальная распределение становится все ближе и ближе к нормальному распределению. То есть, биномиальная вероятность любого события приближается к нормальной вероятности того же события.

Поскольку n увеличивается, стандартное отклонение нормального распределения уменьшается, следовательно, вероятность того, что большинство узлов составят правильные рекомендации, ближе к среднему a. Таким образом, при $a > 0,5$ (среднее значение больше 0,5) вероятность правильного вывода 1. Аналогично, при $a < 0,5$ вероятность правильного вывода равна 0.

Следовательно, если узлы точны не менее половины времени, вероятность того, что рекомендация правильна равна 1. Это критический момент. Пока $g * p_a$ больше чем 0,5, мы можем ожидать очень точного вывода.

Среднее значение доверия округляется на каждом шаге алгоритма. Точность оценки увеличивается на каждом новом уровне. Поскольку алгоритм движется от непосредственных соседей пользователя к источнику запросов среднее значение (a) будет варьироваться от узла к узлу, но будет увеличиваться на каждом уровне.

Начиная с равномерной точности 0,7 вероятность правильной классификации пользователя возрастает по мере того, как мы перемещаем дерево поиска от выбранного для оценки узла к источнику. После получения оценки от трех уровней узлов, источник получит верную классификацию пользователя с вероятностью в 96%.

Почтовый клиент *TrustMail* использует рейтинг доверия каждого отправителя в качестве оценки для сообщения. Затем пользователи могут сортировать сообщения в соответствии со своим значением доверия. *TrustMail* показывает, что когда мнение конкретного пользователя отличается от среднего общественного мнения, рекомендуемые рейтинги, основанные на доверии, более точны, чем в нескольких других общих методах совместной фильтрации.

Сравнение алгоритмов вычисления уровня доверия к пользователям в социальной сети приведено в табл. 1.

Особенности подхода к оценке доверия *SocialTrust*: во-первых, адаптация к изменениям уровня доверия с течением времени; во-вторых, основная метрика *SocialTrust* осуществляет поддержку персонализированной обратной связи через формирование персонифицированной группы доверия.

Таблица 1

Название алгоритма	Исследуемые в работах свойства доверия	Модель оценки доверия	Источник информации
TrustMail	*a)* Не учтен динамичный аспект доверия. *b)* Пропагандирующее свойство доверия, когда учитываются множественные рекомендации. *c)* Субъективный характер доверия для персонализации расчета доверия, где личные предпочтения участника имеют прямое влияние на вычисление доверия.	Граф социальных взаимодействий. Доверие к друзьям друзей на основе доверия к своим друзьям. Информация о доверии от разных друзей формирует окончательное решение об уровне доверия.	Определяет уровень доверия между пользователями на основании уже имеющегося опыта (как они взаимодействовали между собой, как часто).
SocialTrust	*a)* Уровень доверия может увеличиваться или уменьшаться со временем и новыми впечатлениями, взаимодействиями или наблюдениями. *b)* Не учтено пропагандирующее свойство доверия *c)* При расчетах не учитывается субъективный характер доверия.	Доверие рассчитывается на основании ответов на запросы к группе пользователей	Поведение на момент вычислений. Определяет уровень доверия между пользователями по их поведению в настоящее время (как они общаются между собой, как часто взаимодействуют)
STrust	*a)* Учтена зависимость уровня доверия от прошедшего времени после последних взаимодействий. *b)* Не учтено пропагандирующее свойство доверия. *c)* Учтен субъективный характер доверия	Доверие к отдельному участнику сообщества основывается на доверии к сообществу в целом.	Определяет уровень доверия между пользователями по их поведению в настоящее время (каким образом взаимодействуют, как часто взаимодействуют).

В *STrust* выделяют разные типы взаимодействий между пользователями и исследуют их. Подчеркнута разница между доверием, основанном на популярности члена сообщества, и доверием, основанном на личном опыте взаимодействий.

Отличие *TrustMail* заключается в предложенной функции композиции доверия, основанной на структуре доверительных отношений. Информация из нескольких цепочек доверия должна быть составлена для формирования окончательного решения об уровне доверия.

Заключение

Можно заключить, что алгоритмы дают значительные результаты и могут рассчитывать доверие между пользователем и его друзьями в социальной сети и в реальной жизни. Основанный на доверии подход является одним из наиболее перспективных направлений для поддержания относительной открытости сообществ, в то же время, предоставляя некоторую меру устойчивости к уязвимостям. Используя рейтинги доверия, пользователь может решить, с кем участвовать в новых социальных взаимодействиях, а с кем стоит вести себя с особой осторожностью. Это исследование является хорошей базой для будущей работы по этому вопросу, где более крупные наборы данных могут обеспечить лучшие результаты, и где могут быть оценены различные контексты доверия или комбинации алгоритмов доверия.

Литература

1. Артамонова Я.С., Максименко В.Н. Аналитическое моделирование ИК-услуг сетей NGN // Инновации и инвестиции, 2015. – № 6. – С. 136-142.
2. Максименко В.Н. Категорный подход к исследованию аспектов защиты информации и управления качеством сервисов и услуг в сетях сотовой подвижной связи // T-Comm: Телекоммуникации и транспорт, 2018. – Т. 12. – № 9. – С. 41-49.
3. Максименко В.Н., Васильев М.А. Методика расчета стандартизованных показателей качества дополнительных услуг на сетях подвижной связи // T-Comm: Телекоммуникации и транспорт, 2011. – Т. 5. – № 4. – С. 26-28.
4. Максименко В.Н. Услуга определения местоположения абонента как средство защиты в сети сотовой подвижной связи // Известия ЮФУ. Технические науки, 2007. – № 4 (76). – С. 151-155.
5. Максименко В.Н., Ясюк Е.В. Основные подходы к анализу и оценке рисков информационной безопасности // Экономика и качество систем связи, 2017. – № 2 (4). – С. 42-48.
6. Долгова Н.Д., Максименко В.Н. Анализ контента участника социальной сети для определения доверенного субъекта // в книге. XII международная научно-техническая конференция «Технологии информационного общества»: Сборник трудов – Т. 1. – М.: ИД Медиа Паблишер, 2018. – С. 331-333.
7. Sherchan, w., Nepal, s. and paris, C. 2013. A Survey of trust in social networks. ACM Comput. Surv. 45, 4, Article 47 (August 2013).
8. Nepal, S., Sherchan, W., and Paris, C. Strust: Atrust model for social networks. In Proceedings of the 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. (2011), 841-846.
9. Liu, H., Lim, E.-P., Lauw, H. W., Le, M.-T., Sun, A-, Srivastava, J. and Kim, Y. A. Predicting trusts among users of online communities: An epinions case study. In Proceedings of the 9th ACM Conference on Electronic Commerce. ACM Press, New York, (2008), 310-319.
10. Jacoby, C.G. « An easy method to numerically solve the equations found in the theory of secular disorders » (German). Crelle's Journal 30: 51-94.
11. Golbeck, J. A. Computing and applying trust in web based social networks. Ph.D. thesis, University of Maryland at College Park, MD., 2005.