

Н. А. ЖУКОВА

Санкт-Петербургский федеральный исследовательский центр Российской академии наук, Санкт-Петербург

АУНГ МБОУ

Университет ИТМО, Санкт-Петербург

МОДЕЛЬ УПРАВЛЕНИЯ СБОРОМ ДАННЫХ В СИСТЕМЕ ИНТЕРНЕТА ВЕЩЕЙ НА ОСНОВЕ МЕТОДОВ АНАЛИЗА СОЦИАЛЬНЫХ СЕТЕЙ

В статье для решения проблем сбора данных в динамической сети интернета вещей (Internet of Things, IoT) предложен подход, предусматривающий использование моделей и методов анализа социальных сетей наряду с обычно используемыми методами кластеризации. Разработанная гибридная модель отслеживает контакты между узлами, которыми определяются так называемые «социальные отношения» каждого узла, и частоту этих контактов. Модель ограничивается работой только с узлами, связанными «дружбой». Учет «дружественных» отношений между узлами способствует повышению уровня безопасности сбора данных, а также обеспечивает снижение энергопотребления и уменьшение задержек при передаче данных.

Введение. Сбор данных в системах IoT становится все более сложной задачей, что в значительной степени обусловлено переходом от использования статических узлов к использованию множества мобильных узлов. При динамическом изменении топологии сети возникают сложности со сбором данных и определением надежности связей между узлами.

Для решения проблем сбора данных в условиях динамических изменений сети были разработаны модели на основе различных технологий. В работе [1] предложена модель сбора данных с использованием платформы «BeSmart», которая позволяет управлять сбором и обработкой разнородных данных, поступающих от узлов с ограниченными ресурсами. В работе [2] предложена линейная модель, которая основана на туманных (Fog) вычислениях. В работе [3] предложена модель сбора данных, основанная на кластеризации узлов. При использовании перечисленных подходов для сбора данных в динамических сетях выполняются только отдельные требования, предъявляемые к сбору данных в системах интернета вещей (снижение нагрузки на сеть и уменьшение задержки при сборе данных), а вопросам безопасности уделяется недостаточное внимание. Целью настоящего исследования было определение методов анализа социальных сетей, пригодных для применения в динамической сети IoT, отвечающих требованиям надежности и безопасности сбора данных, уменьшения энергопотребления и задержки при сборе данных. При использовании методов анализа социальных сетей в IoT возникло новое понятие – социальный интернет вещей (SIoT) [4].

Так, в SIoT узел i связан отношениями «дружбы» с узлами, которые подключаются к этому узлу i . Для установления отношений «дружбы» между устройствами (узлами) необходимо выполнить следующие действия: 1) определить частоту «встреч» (контактов) между устройствами; 2) установить максимальную степень «дружбы» для каждого устройства (степень «дружбы» узлов – это показатель количества связей, которые может установить данный узел с другими узлами); 3) собрать данные от всех «максимально дружественных» узлов при помощи методов кластеризации. Предлагаемая модель сбора данных основана на совместном использовании кластеризации, туманных вычислений и методов анализа социальных сетей, что позволяет повысить надежность и безопасность сбора данных в сети IoT.

Распределение степеней узлов (вершин графа) для повышения надежности и безопасности сбора данных. Многие естественно возникающие сети (социальные, коммуникационные, биологические и др.) хорошо моделируются безмасштабными графами. Поэтому для моделирования кластерных сетей, имеющих похожую на естественные сети топологию, наиболее подходящей моделью графа является модель безмасштабной сети.

Степень узла (т. е. число связей узла с другими узлами) можно рассматривать в качестве индикатора количества пакетов, полученных этим узлом. Рассмотрим одну из вершин графа – некоторый узел i . Для данного узла i полустепень захода $d + 1$ является числом дуг графа, входящих в вершину – сам этот узел i , тогда как полустепень исхода $d - 1$ является числом дуг графа, исходящих из вершины – узла i . То есть полустепень исхода показывает, на сколько узлов узел i может передавать данные, а полустепень захода определяет количество узлов, от

которых узел i может получать данные. Определяется максимальное количество соединений, которые могут установить центральные узлы кластера, чтобы избежать включения в кластер недопустимых (вредоносных) узлов. Вероятность связи нового узла с центральным узлом кластера s может быть определена следующим образом:

$$P_s = \left(1 - \frac{k_c}{k_{max}}\right) \frac{E_c k_c}{\sum_{i=1}^{N(t)} E_i k_i}, \quad (1)$$

где k_c – количество связей центрального узла; k_{max} – максимальное число связей любого узла в кластере; E_c – энергия центрального узла; $N(t)$ – количество центральных узлов в момент времени t ; E_i – энергия узла i ; k_i – количество связей узла i . Большое значение $E_c k_c$ показывает возможность подключения нового узла к кластеру, поскольку центральный узел s имеет большой запас энергии. Из формулы (1) следует, что, если степень вершины – центрального узла достигает максимального предельного значения для числа соединений k_{max} , вероятность того, что новый узел сможет установить связь с центральным, станет нулевой. То есть узлы могут отличаться степенью вероятности включения в кластер в зависимости от таких свойств, как энергия и вычислительная мощность, что повышает надежность и безопасность сбора данных.

Выбор сетевых «дружеских» связей для повышения надежности и безопасности сбора данных. Использование методов анализа социальных сетей в IoT позволяет объектам автономно устанавливать так называемые «социальные отношения» [4]. Для таких сетей могут быть определены следующие возможные типы отношений: *отношения между объектами собственности* (Ownership Object Relationship, OOR) – это тип отношений между объектами, которые принадлежат одному пользователю; *социальные объектные отношения* (Social Object Relationship, SOR) – это отношения, которые устанавливаются между объектами, они отражают социальные действия, такие как «встречи» одних узлов с другими; *родительские объектные отношения* (Parental Object Relationship, POR) – устанавливаются между узлами, относящимися к однородными объектами, созданными одним производителем (например, товары одной компании); *объектные отношения совместного размещения* между узлами (Co-location Object Relationship, C-LOR) – это отношения между объектами, которые постоянно существуют в одном и том же месте [4].

Ограничивая «дружбу» с другими узлами числом k_{max} , узлы могут управлять «социальными отношениями». Так, сбор данных на основе кластеризации может выполняться с ограниченного количества «дружественных» узлов, не превышающего k_{max} , что отвечает требованиям безопасности к сбору данных в сети IoT.

Каждый узел управляет запросами «дружбы» с учетом следующих условий:

- каждый узел должен отклонить запрос о «добавлении в друзья» после достижения числа связей, равного k_{max} ;
- каждый узел должен отсортировать свой «список друзей» в порядке понижения степени «дружбы». Чтобы максимизировать количество «друзей», узел должен принять первых k_{max} «друзей»;
- каждый узел должен отсортировать свой «список друзей» в порядке повышения степени «дружбы». Чтобы свести к минимуму количество друзей, узел должен отклонить первых k_{max} «друзей».

Стратегия помогает мобильным узлам управлять «списком друзей» – формировать наилучший набор «друзей» k_{max} – и выбирать оптимальный путь для сбора данных.

Управление сбором данных на основе отношений «дружбы». Программное обеспечение на основе туманных вычислений является посредником для установления «дружеских» связей между узлами. При помощи туманных вычислений определяются отношения SOR (социальные объектные отношения) и OOR (отношения между объектами собственности) на основе набора данных некоторого «умного» города [5]. SOR устанавливаются при «случайных встречах» между устройствами. Отношения OOR устанавливаются для устройств, принадлежащих одному пользователю или организации. Поэтому отношения OOR устанавливаются на короткое время, а с течением времени увеличивается число отношений SOR.

При сборе данных предполагается, что алгоритмы на основе туманных вычислений собирают требуемые данные с узлов, между которыми установлены «дружеские связи» (SOR). Один узел может установить «социальную связь» с максимальным числом «друзей» k_{max} . В этом случае сбор данных указанными алгоритмами выполняется с помощью кластеризации. Пусть

200 узлов с одинаковой начальной энергией $2J$ расположены в области моделирования 300×300 м². Предполагается, что все узлы имеют одинаковую вычислительную мощность, максимальное число «друзей» k_{max} определяется как 50 узлов для каждого узла. Каждому из 50 узлов, входящих в одну «социальную группу», присваивается идентификатор для сбора данных на основе кластеризации (ID узла, местоположение в текущий момент времени). В одной группе максимальное количество узлов-участников – 50. На рис. 1 показаны идентификаторы узлов в различных группах. На рис. 2 изображен центральный узел кластера, который выполняет сбор данных с 50 узлов «дружбы». На каждой итерации сбора данных центральный узел кластера выбирается из числа этих узлов «дружбы». На рис. 3 и 4 показаны общее потребление энергии и общая задержка при передаче данных по сети соответственно.

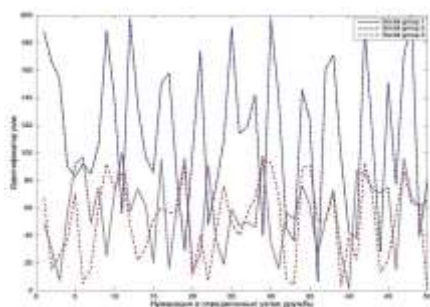


Рис. 1. Идентификаторы устройств определенной «социальной группы» устройств

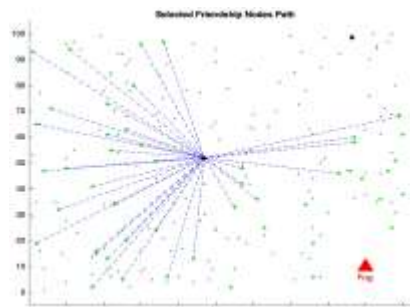


Рис. 2. Пути сбора данных между центральным узлом кластера и выбранными узлами «дружбы»

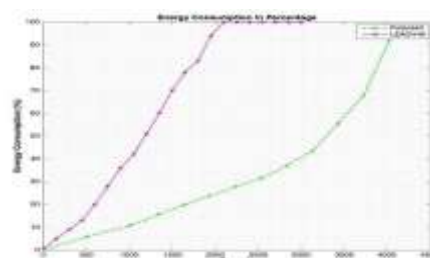


Рис. 3. Общее потребление энергии

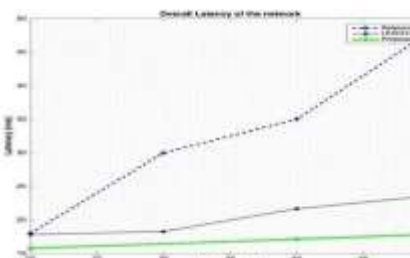


Рис. 4. Общая задержка при передаче данных

Заключение. В данной статье новая модель сбора данных скомбинирована с моделью «дружественных отношений», применяемой при анализе социальных сетей. Группируя узлы с «максимально дружественными» связями, модель помогает избежать использования вредоносных узлов, что способствует повышению безопасности и надежности сбора данных. Результаты экспериментов показали, что применение модели также может снизить энергопотребление и уменьшить задержки при передаче данных по сравнению с традиционными моделями. Планируется дальнейшая разработка предложенной модели с целью использования методов анализа социальных сетей для повышения эффективности управления сбором данных в сетях IoT.

ЛИТЕРАТУРА

1. Fotiou, Nikos et al. "Smart IoT Data Collection." 2018 IEEE 19th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM) (2018): 588-599.
2. Oma, Ryuji et al. An Energy-Efficient Model of Fog and Device Nodes in IoT. 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA) (2018): 301-306.
3. Fattoum, Marwa et al. A Two-Level Clustering based on Position, Data Correlation and Residual Energy in WSN. 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC) (2019): 961-966.
4. Atzori, Luigi et al. "SIoT: Giving a Social Structure to the Internet of Things." IEEE Communications Letters 15 (2011): 1193-1195.
5. Marche, Claudio et al. "A Dataset for Performance Analysis of the Social Internet of Things." 2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC) (2018): 1-5.

Zhukova Nataly (St. Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg), Aung Myo Thaw (ITMO University, St. Petersburg)

Model of Data Collection Control in the Internet of Things on the Basis of Social Networking Technologies

The paper deals the issues of data collection in a dynamic Internet of Things (IoT) network. An approach is proposed based on the use of compatible models and methods of social networks analysis along with clustering methods commonly used in this case. In this case Internet of Things (IoT) becomes so called Social Internet of Things (SIoT). The developed hybrid model determines frequency of contacts between nodes of the network thus creating social network relationships for each node. After defining friendly social network connections between nodes the model is limited to including into consideration only connections of friendship, taking into account at the same time their distribution by degrees of friendliness. Data collection based on clustering with limited friendship meets not only security requirements, but also helps to reduce energy consumption and data transfer delays. Simulations using the proposed model and comparison of results with those of traditional models shows the enhancement as regards energy saving and delay of data transfer.