УДК 651. 34

А.С. Семенова, М.В. Бартош

Национальный технический университет «ХПИ», Харьков

ОЦЕНКА УСТОЙЧИВОСТИ СЕТИ INTERNET OF THINGS С ПОМОЩЬЮ ПОКАЗАТЕЛЕЙ ЦЕНТРАЛЬНОСТИ СВЯЗЕЙ

На основе результатов исследования существующих уязвимостей компьютерных сетей INTERNET OF THINGS (IoT) в статье определены ряд перспективных направлений дальнейшего совершенствования методов и средств обеспечения безопасности данных. В рамках одного из перспективных направлений проведен анализ основных показателей центральности связей компьютерной сети IoT. Определено сопоставимость результатов использования как уже известных, так и новых (усовершенствованных) показателей при оценке устойчивости сетей к злоумышленным атакам. Также выявлена эффективность использования усовершенствованного показателя Local Vector Centrality при оценке устойчивости сети к межосевым атакам.

Ключевые слова: *INTERNET OF THINGS, показатели центральности (централизации) связей, компьютерная сеть, устойчивость, безопасность.*

Введение

Постановка проблемы. Интернет вещей (IoT) одно из новых направлений современных информационных технологий. Это направление имеет своей стратегической целью компьютеризацию и автоматизацию процессов управления в широком диапазоне сфер обслуживания. Обеспечивается это повсеместной связью между различными техническими цифровыми устройствами с минимизацией включения человеческого фактора. Это существенно расширяет границы применимости компьютерной и другой цифровой техники и является в свою очередь своеобразным двигателем прогресса в различных отраслях экономики. На рис. 1 представлена обобщенная концепция построения общей структуры IoT.

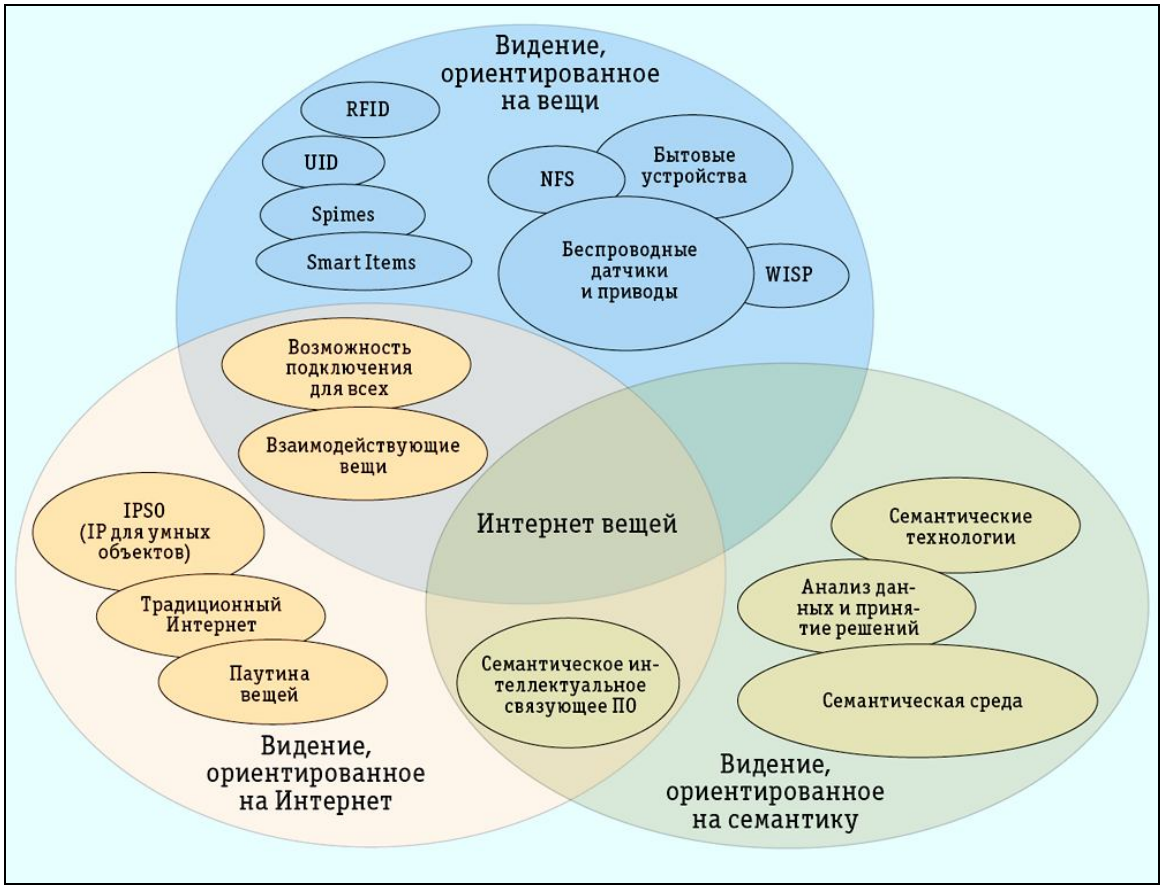

Рис. 1. Схема основных составляющих обобщенной концепции построения общей структуры IoT

В то же время, как показали исследования [1, 5], функциональность и операции IoT в значительной степени зависят от топологии и базовой структуры подключения к сети. Данный факт неизбежно вызывает проблемы безопасности в связи с возможностью незаметного подключения и автоматизированной интеграции между различными видами приложений. Например, злоумышленник может использовать взаимосвязанные устройства для распространения вредоносных программ. Проблема усугубляется разнородностью аппаратно-программных средств обеспечивающих функционирование IoT. Поэтому именно в последнее время этому вопросу начали уделять большое внимание. Так на базе Стэндфордского университета США была сформирована группа специалистов для разработки унифицированных предложений защиты данных в IoT [7].. А департамент США по энергетике (DOE) приступил к разработке предложений защиты от активных атак на уровне топологии.

Анализ литературы показал, что одним из недостатков и факторов, снижающих эффективность (в том числе и безопасность) функционирования компьютерных сетей IoT является стратегия на централизованной управление облачными ресурсами.

Это подтверждается фактами успешно проведенных злоумышленных атак на ключевые узлы коммутации IoT. Поэтому ряд фирм [5] предлагают альтернативные решения, связанные с созданием полностью децентрализованной экосистемы Интернета вещей, работающей независимо от центральных авторитетов.

В такой среде устройства смогут самостоятельно обнаруживать другие устройства, безопасно подключаться к ним и устанавливать с ними доверительные отношения с помощью контрактов.

Возможно, устройства даже смогут передавать друг другу ценности – например, платить за доступ к сенсорам или аренду вычислительной мощности.

Следует заметить, что создание децентрализованного IoT – сложная задача. Необходимо разработать протоколы обнаружения устройств, безопасности и управления идентичностью, реализовать схемы доверия, интегрировать в сеть криптовалюты и решить многие другие задачи.

Проведенные исследования показали, что одной из первоначальных задач в перечне является разработка оптимальной топологической структуры компьютерной сети IoT.

Для ее решения необходимо предварительно провести анализ и исследования существующих показателей централизации (децентрализации) узлов сети и степень влияния их возможного выхода из строя на общий показатель безопасности компьютерной сети IoT.

Проведенный анализ литературы [2-7] показал, что в настоящее время существует ряд основных показателей центральности (централизации) связей сети.

Так в источниках [2, 4] определено, что это показатели степень связности (degree centrality); степени близости к другим узлам (closeness centrality); степени посредничества (betweenness centrality) и влиятельности (eigenvector centrality). Кроме этого в последнее время представлено ряд новых, усовершенствованных разработок, в которых этот список расширяется.

Так, например в [3] предлагается рассматривать еще такой показатель, как эгоцентричность (Ego centrality), а в статье [6] рассматривается показатель локальной центральной плотности (Local Vector Centrality).

Результаты исследований

Рассмотрим более подробно следующие показатели:

1. Степень связности (degree centrality) – исторически первая и концептуально простая мера C_0 важности узлов в сети. Эта мера определяется как количество связей deg(v), инцидентных данному узлу v:

$$C_0(v) = \deg(v).$$

Степень связности узлов компьютерной сети IoT можно интерпретировать как меру активности узлов в процессе выполнения различных задач, характерных данному виду IoT.

2. Степень близости к другим узлам (closeness centrality) $C_c(v)$ – обратная величина суммы кратчайших путей $d(v_i, w_i)$ от узла v до других узлов w_i:

$$C_c(v) = \Big/ \sum_{i=1}^{|V|} d(v, w_i),$$

где $|V|$ – число всех узлов сети.

Таким образом, чем более важным является узел в соответствии с указанным показателем, тем меньше сумма кратчайших путей от него к другим узлам.

3. Степень посредничества (betweenness centrality) – характеристика узла, показывающая, насколько часто данный узел лежит на кратчайших путях между другими узлами.

Этот параметр вычисляется следующим образом

$$C_b(v) = \sum_{k \neq i} \sum_{j \neq i,\ j > k} \frac{\sigma_{kj}(v)}{\sigma_{kj}},$$

где σ_{kj} – количество кратчайших путей из узла k в узел j, а $\sigma_{kj}(v)$ – количество этих путей, проходящих через узел v.

Через узел с высокой степенью посредничества будет проходит большой объем данных, при условии что передача будет осуществляться по кратчайшим путям.

Это подразумевает большую уязвимость таких узлов к атакам злоумышленников.

4. Влиятельность (eigenvector centrality) – рекурсивная мера $C_e(v)$ важности узла, основанной на важности соседних узлов.

5. Чем более влиятельны узлы, с которыми связан узел, тем больше влиятельность самого узла:

$$C_e(v) = \frac{1}{\lambda}\sum_{i\in M(v)} C_e(t) = \frac{1}{\lambda}\sum_{i\in G} A_{v,t}C_e(t),$$

где $M(v)$ – множество соседних узлу v узлов; λ – константа; $A_{v,t}$ – элемент матрицы смежности (задается на основе связности узлов сети).

Значения $C_e(v)$ можно получить, решив уравнение

$$A_x = \lambda x,$$

где A – матрица смежности, λ и x – соответственно собственное значение и собственный вектор матрицы A.

6. Эгоцентричность (Ego centrality) – показатель, который можно описать следующим образом.

Пусть матрица смежности узла i – A_i имеет размерность $(d_i + 1)\times(d_i + 1)$.

Пусть I – единичная матрица.

Так как $\left|A^2(i)\right|_{kj}$ может задавать число двухходовых переходов между k и j, и

$$\left|A^2(i)\circ I - A(i)\right|_{kj} -$$

общее число кратчайших путей с двумя хопами между k и j для всех $k \neq j$, (символ $\circ$ обозначает матричное произведение), центральность $C_r(v)$ определяется как

$$C_r(v) = \sum_k \sum_{j>k} \Big/ \left|A^2(i)\circ I - A(i)\right|_{kj}^{1}.$$

В целом можно заметить, что данный показатель может рассматриваться как частный случай степени посредничества (betweenness centrality).

7. $C_{LVC}(i)$ (Local Vector Centrality (LVC)) – это показатель, характеризующий уязвимость компьютерной сети IoT к удалению узлов. Узел с более высоким LVC более важен для структуры сетевого соединения.

Пусть y – собственный вектор, связанный со вторым наименьшим собственным значением $\mu(L)$ матрицы Лапласса L.

Тогда $C_{LVC}(i)$ можно рассчитать как

$$C_{LVC}(i) = \sum_{j\in N_i}\left(y_i - y_j\right)^2.$$

Следует заметить, что хоть $C_{LVC}(i)$ – это и обобщенная центральная мера, ее можно точно аппроксимировать локальными вычислениями и передачей сообщений с использованием метода распределенной мощности для вычисления вектора y.

При оценке устойчивости сети по показателям централизации к различным атакам мы можем сравнить количество выведенных из строя узлов, необходимых для успешной атаки.

Это необходимо для уменьшения наибольшего размера показателя до определенного значения, например, количества узлов, необходимых для уменьшения размера наибольшего компонента до 10% от исходного размера.

На рис. 2 представлены результаты исследования показателя устойчивости сети IoT (графики зависимости нормализированных значений выбранных показателей централизации от количества выведенных из строя узлов сети IoT) в соответствии с базой данных GTS-CE [4].

Рассматривался практический случай когда сеть состоит из 149 узлов и 193 соединительных линий.

Как видно из графика в представленной сети IoT межосевые атаки и атаки LVC имеют сопоставимую эффективность, что приводит к снижению на 20% наибольшего количественного показателя путем удаления 10 узлов из сети.

Выводы

В результате проведенных анализа литературы и исследований были определены наиболее информативные показатели централизации сети IoT.

Проведены исследования возможности их использования для анализа устойчивости компьютерной сети IoT к атакам злоумышленников, направленных на выведение из строя центральных, наиболее ванных узлов.

Результаты показали в целом сопоставимость результатов в рассмотренном конкретном случае, и преимущество до 20% п показателя Local Vector Centrality при удалении 10 узлов.

Дальнейшие исследования будут направлены на построение топологически защищенной компьютерной сети IoT.

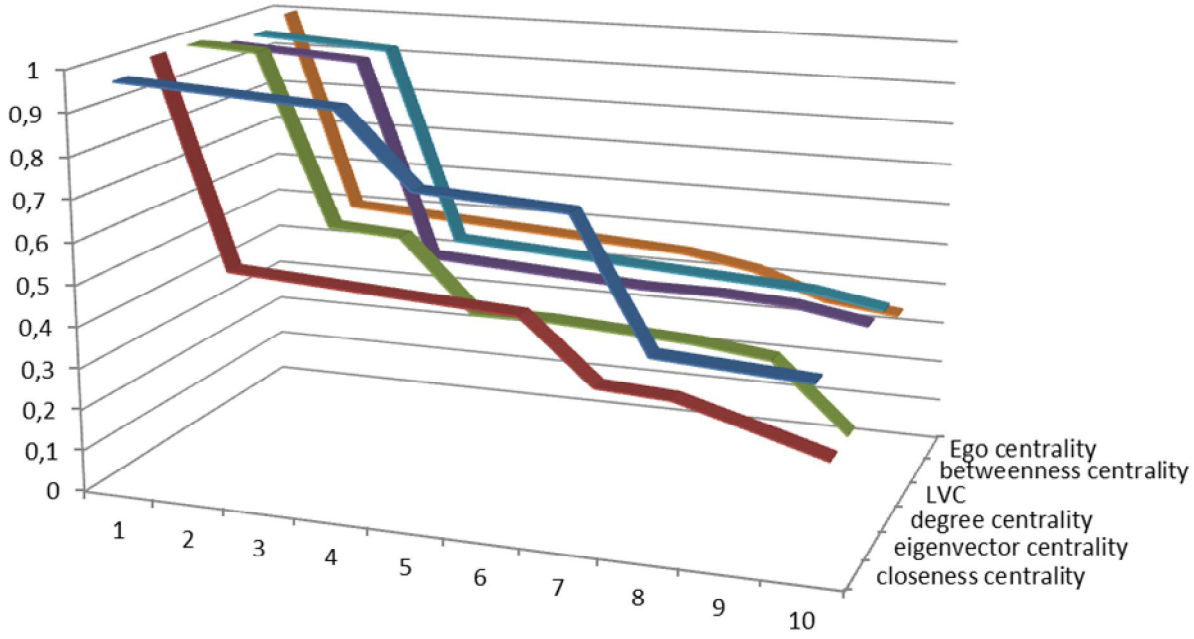

Рис. 2. Графики зависимости нормализированных значений выбранных показателей централизации от количества выведенных из строя узлов сети IoT

Список литературы

1. Черняк Л. Интернет вещей: новые вызовы и новые технологии [Электронный ресурс] / Л. Черняк // Открытые системы. СУБД 2013 № 04. Режим доступа: https://www.osp.ru/os/2013/04/13035551.

2. Юдина М.Н. Узлы в социальных сетях: меры центральности и роль в сетевых процессах / М.Н. Юдина // Омский научный вестник 2016, С. 161-165.

3. Everett Martin Ego network betweenness. / Martin Everett, Stephen P. Borgatti. // Social Networks, 27(1):31–38, 2005.

4. Knight Simon The Internet topology zoo. / Simon Knight, Hung X. Nguyen, Nickolas Falkner, Rhys Bowden, and Matthew Roughan. // IEEE J. Sel. Areas Commun., 29(9):1765–1775,October 2011.

Matviishyn Oleksandr Decentralization in the Internet of Things [Электронный ресурс] / Oleksandr Matviishyn. – Режим доступа: https://united.softser veinc.com/blog/decentralization-internet-of-things.

5. Pin-Yu Chen Local Fiedler vector centrality for detection of deep and overlapping communities in networks. /Yu Chen, Alfred O. Hero // IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pages 1120–1124, 2014.

6. Rethinking a Secure Internet of Things [Электронный ресурс]. – Режим доступа: http://iot.stanford.edu.

Надійшла до редколегії 1.02.2017

Рецензент: д-р техн. наук, проф. О.А. Серков, Національний технічний університет «ХПІ», Харків.

ОЦІНКА СТІЙКОСТІ МЕРЕЖІ INTERNET OF THINGS ЗА ДОПОМОГОЮ ПОКАЗНИКІВ ЦЕНТРАЛЬНОСТІ ЗВ'ЯЗКІВ

Г.С. Семенова, М.В. Бартош

На основі результатів дослідження існуючих вразливостей комп'ютерних мереж INTERNET OF THINGS (IoT) в статті визначено ряд перспективних напрямків подальшого вдосконалення методів і засобів забезпечення безпеки даних. В рамках одного з перспективних напрямків проведено аналіз основних показників центральності зв'язків комп'ютерної мережі IoT. Визначено порівнянність результатів використання як уже відомих, так і нових (удосконалених) показників при оцінці стійкості мереж до зловмисним атакам. Також виявлено ефективність використання вдосконаленого показника Local Vector Centrality при оцінці стійкості мережі до міжосьовим атакам.

Ключові слова: *INTERNET OF THINGS, показники центральності (централізації) зв'язків, комп'ютерна мережа, стійкість, безпеку.*

ESTIMATION OF THE STABILITY OF THE INTERNET OF THINGS NETWORK WITH THE INDICATORS OF CENTRALITY OF CONNECTIONS

H.S. Semenova, M.V. Bartosz

Based on the results of a study of the existing vulnerabilities of computer networks INTERNET OF THINGS (IoT), the article identifies a number of promising areas for further improvement of methods and tools to ensure data security. Within the framework of one of the prospective directions, the analysis of the main indicators of the centrality of the IoT network connections was carried out. The comparability of the results of using both known and new (improved) indicators in assessing the stability of networks for malicious attacks was determined. Also, the effectiveness of using the improved indicator of Local Vector Centrality in assessing the stability of the network to inter-axial attacks was revealed.

Keywords: *INTERNET OF THINGS, indicators of centrality (centralization) of communications, computer network, stability, security.*