УДК 004.75

Тіменко А.В.
Запорізький національний технічний університет

Шкарупило В.В.
Національний університет біоресурсів і природокористування України

АНАЛІЗ ПІДХОДІВ ДО ОРКЕСТРУВАННЯ IOT-СЕРВІСІВ

У статті досліджуються підходи до оркестрування IoT-сервісів. Розглядаються технології, на яких ґрунтується функціонування IoT-систем. Характеризується поточний стан і поширення Інтернету речей. Оркестрування IoT-сервісів розглядається як основоположна складова частина організації узгодженої взаємодії компонентів IoT-системи шляхом централізованого координування. Підходи до оркестрування аналізуються з позиції специфіки застосування.

Ключові слова: *IoT, SDN, SOA, координування, оркестрування, програмна система, сервіс.*

Постановка проблеми. Нині відзначається стрімке зростання кількості електронних пристроїв, що взаємодіють, обмінюються даними (годинників, мобільних телефонів, холодильників тощо). Такі пристрої прийнято називати «розумними» [1]. Водночас гостро постає питання побудови успішно функціонуючих систем на їх основі у різних сферах застосування: «розумного будинку» (smarthome) – керування освітленням, перемикачами живлення, індикаторами задимлення тощо [2]; «розумного міста» (smartcity) – керування постачанням електроенергії, тепла тощо [3] та ін. Стверджується, що у 2020 р. очікується функціонування близько 20 млрд «розумних» пристроїв [4].

Враховуючи вищесказане, варто зазначити, що канонічний підхід до побудови, обслуговування та реконфігурування комп'ютерних мереж, на основі яких би будувалася успішно функціонуюча та масштабована інфраструктура взаємодіючих «розумних» пристроїв, не є задовільним – з урахуванням потенційної кількості таких пристроїв. Шляхом вирішення цього питання є адаптація принципів програмно-конфігурованих мереж (SDN, Software Defined Networking) – підходу, що полягає у розмежуванні рівнів керування і даних [5]. Завдяки цьому значно спрощується процес вирішення задач, пов'язаних із реконфігуруванням та обслуговуванням мережі. Це можливо за рахунок того, що відповідні дії пропонується вирішувати на програмному, а не на апаратному рівні. З цією метою вводиться поняття «контролера» – програмної системи для автоматизації процесів централізованого координування, моніторингу, реконфігурування мережі тощо. Водночас постає питання: яким саме чином здійснювати озвучене координування в масштабах усієї розподіленої системи взаємодіючих пристроїв? У цьому аспекті можна провести аналогію із сервіс-орієнтованою архітектурою (SOA, Service-oriented Architecture), де функціонування розподіленої системи ґрунтується на взаємодії – координуванні – веб-сервісів. Подібні системи прийнято називати композитними веб-сервісами (композиціями веб-сервісів) [6]. Безпосередньо координування, зазвичай, здійснюється централізовано – згідно з моделлю оркестрування [7].

Під оркеструванням розумітимемо централізоване координування компонентів розподіленої програмної системи з метою організації їх узгодженої взаємодії для досягнення бажаного ефекту – виконання заданого потоку робіт для реалізації відповідного бізнес-процесу. Окремий бізнес-процес розглядатимемо у контексті певного сценарію предметної сфери: наприклад, моніторинг та обробка показників датчиків вологості у приміщенні з метою створення сприятливих умов для функціонування і розвитку певної екосистеми тощо. Поняття «оркестрування» пропонується відобразити з контексту веб-сервісів у контекст сервісів, що функціонують на основі технологій поверх програмно-конфігурованих мереж. Дослідження наявних підходів до оркестрування таких сервісів дозволить охарактеризувати актуальний стан відповідних напрацювань і виявити перспективні напрями подальших досліджень.

Аналіз останніх досліджень і публікацій. Для реалізації взаємодії «розумних» пристроїв у глобальному масштабі широко використовується концепція Інтернету речей поверх технології SDN [8], що ґрунтується на імплементації механізму M2M-взаємодії (machine-to-machine):

як поверх типового спектру технологій – TCP/IP, RFID (Radio Frequency Identification) [9] тощо, так і поверх нових технологій, таких як віртуалізація мережевих функцій (NFV, Network Functions Virtualization) – підхід, що полягає у відмежуванні мережевих функцій від фізичних пристроїв, на яких вони виконуються [10]. Концепція NFV реалізується за рахунок оперування мережевими функціями у віртуальному середовищі. Подібний підхід забезпечує гнучкість із позиції оперативності реагування на зміну вимог до мережевих конфігурацій, ресурсів, функцій. Під мережевими ресурсами зазвичай розуміють обчислювальні ресурси, обсяг пам'яті мережевих вузлів, різноманітні веб-додатки та сервіси. Названі ресурси можуть розміщуватися як у «хмарному» середовищі – згідно з концепцією хмарних обчислень (CC, Cloud Computing), так і у перспективному відгалуженні – «туманному» середовищі – за концепцією «туманних» обчислень (FC, Fog Computing). Відповідно до концепції CC мережеві ресурси розміщуються у розподіленому віртуальному середовищі – «хмарі» [11]. Ключові відмінні риси FC як еволюційної гілки від CC такі: територіальна розподіленість, гетерогенність, наявність значної кількості мережевих вузлів, мобільність, пріоритетність бездротового доступу [12]. FC – модель розподілених обчислень, що ґрунтується на розміщенні даних і засобів їх обробки якнайближче до джерела цих даних. Подібна концепція є особливо вагомою саме в контексті Інтернету речей, оскільки таким чином суттєво знижується обсяг даних, що передаються мережею, а також знижуються комунікаційні затримки. Озвучені риси формують сприятливе підґрунтя для розгляду технології FC як опорного базису для реалізації M2M-взаємодії територіально розподілених «розумних» пристроїв. Цей процес описується парадигмою Інтернету речей (IoT, Internet of Things) [13]. Варто враховувати такі аспекти: вимоги до незначного обсягу мережевого трафіку, малий обсяг оперативної пам'яті та незначні обчислювальні можливості пристроїв, обмеженість заряду батарей пристроїв тощо. Дотримання озвучених аспектів можливе як за рахунок залучення різноманітних «легких» протоколів обміну даними, наприклад, MQTT (Message Queue Telemetry Transport) [14], CoAP (Constrained Application Protocol) [15] тощо, так і за рахунок правильним чином організованого координування взаємодією пристроїв. Останній позиції і присвячена наша робота, а саме – аналізу наявних підходів до оркестрування IoT-сервісів, за рахунок якого здійснюється координування пристроїв.

Постановка завдання. У роботі ставиться і вирішується таке завдання: проаналізувати підходи до оркестрування IoT-сервісів. За результатами проведеного аналізу можливо виявити, окреслити й охарактеризувати специфіку застосування проаналізованих підходів; виявити перспективний напрям (напрями) подальших досліджень. IoT-сервіси (далі – сервіси) розглядаються як веб-сервіси, призначені до застосування в IoT-середовищі. Під IoT-системою розуміється сукупність сервісів, що взаємодіють згідно з моделлю оркестрування – шляхом централізованого координування. Як компонент такої системи може розглядатися як окремий атомарний (неподільний) сервіс, так і певна підсистема – композиція сервісів, що взаємодіють за визначеним сценарієм.

Виклад основного матеріалу дослідження. Попередньо зазначимо: композитні IoT-сервіси, зазвичай, охоплюють сенсори, пристрої, обчислювальні ресурси, а також інфраструктуру, яка сполучає названі складники [16]. Більше того, проводячи паралелі між SOA та IoT, варто зазначити, що така ключова концепція SOA, як динамічна композиція сервісів є характерною і для IoT [17]. Застосування сервісів із прив'язкою до певної визначеної предметної сфери має на меті сприяти підвищенню показників захищеності даних і надійності системи загалом – за рахунок того, що кожен окремий потік робіт (work flow) інкапсулюється у межах відповідного композитного сервісу. Оркестрування варто розглядати у контексті налаштування системи відповідно до вимог користувацьких запитів до неї. Проявом подібного оркестрування є певний потік робіт, який протікає за рахунок координування компонентів IoT-системи. Доречно враховувати складність системи з позиції значної кількості залучених мережевих вузлів, взаємодія яких здійснюється за рахунок координування сервісів. Постає низка задач, що потребують вирішення, зокрема одержання результату роботи композитного сервісу із задовільними показниками QoS-характеристик (Quality of Services), наприклад, із часовою затримкою не більше заданого значення. Складності додає і ad-hoc-режим функціонування системи, за якого конфігурація апаратного та / або програмного забезпечення мережі, топологія мережі змінюються динамічно. Оркестрування за ad-hoc-режиму пропонується будувати на основі потоково-орієнтованої парадигми програмування та відповідних методик [18]. Альтернативний підхід – розробка архітектури, що забезпечує динамічне оркестрування IoT-сервісів, побудованих на засадах SOA [19].

Підходи до оркестрування IoT-сервісів розглянемо також із позиції залучення охарактеризованих вище основоположних технологій. Наприклад, ґрунтуючись на технологіях SDN та NFV, було запропоновано застосовувати пограничний SDN/NFV-придатний вузол, на якому мають бути розгорнуті віртуальні середовища для маніпулювання мережевими ресурсами [20]. Такий підхід відповідає принципам концепції FC, що має на меті зменшити обсяг трафіку, який циркулюватиме мережею внаслідок взаємодії сервісів, а також покращити часові затримки, пов'язані з комунікацією. Зазначений підхід також породжує низку нових питань, наприклад, яким чином забезпечити координування пограничних вузлів, як організувати їх взаємодію з позиції інтероперабельності – здатності до взаємодії з позиції підтримки різних протоколів, різної корпоративної належності тощо.

Більше того, оркестрування IoT-сервісів доречно розглядати також і з погляду цілісності даних, які циркулюють між сервісами. Попередньо вже було проведено масштабне дослідження на предмет встановлення та забезпечення цілісності зовнішніх щодо певної підсистеми IoT-системи даних [21]. За результатами цього дослідження відповідні напрацювання було узагальнено та систематизовано. Стверджено, що підходи до перевірки цілісності даних можна умовно згрупувати таким чином: підходи, напрямлені на підтвердження придатності даних до одержання (POR, Proof of Retrievability), та підходи, орієнтовані на підтвердження володіння даними (PDP, Provable Data Possession). Підходи першої групи ґрунтуються на формулюванні суджень стосовно цілісності даних на основі верифікації (перевірки) супутніх метаданих, другої групи – на основі верифікації вибіркових даних. Підходи і першої, і другої груп можна охарактеризувати як такі, що спрямовані на забезпечення цілісності даних із позиції попередження несанкціонованого доступу до них, підміни даних тощо. Прикладом відповідних рішень є система ContexIoT, яка за рахунок забезпечення контекстної цілісності даних, що циркулюють на рівні потоку керування та потоку даних, сприяє ефективному контролю доступу користувачів до ресурсів IoT-системи [22].

Для забезпечення цілісності даних під час передавання їх від сенсорів до підсистем обробки даних пропонується застосовувати цифрові підписи, які ґрунтуються на використанні еліптичних кривих (ECDSA, Elliptic Curve Digital Signatures) [23]. Це, в свою чергу, супроводжується додатковими споживанням пристроями енергії.

Отже, розглянуті підходи до оркестрування IoT-сервісів суттєво різняться за спрямованістю та характером реалізації. Варто відзначити нестачу підходів, які б адресували оркестрування IoT-сервісів із позиції інтероперабельності, адже саме цей аспект можна охарактеризувати як один із першочергових – враховуючи масштаб IoT-систем з погляду кількості залучених пристроїв, їх територіального розподілу та розмаїття корпоративної належності.

Висновки. Таким чином, у роботі було проведено аналіз підходів до оркестрування IoT-сервісів. За результатами проведеного аналізу встановлено, що названі підходи суттєво різняться як за спрямованістю, так і за характером реалізації. Було виявлено, що переважна більшість розглянутих підходів орієнтована на забезпечення та підтримку цілісності даних, що циркулюють між компонентами IoT-систем. Питання забезпечення узгодженості взаємодії компонентів IoT-систем при оркеструванні IoT-сервісів із позиції інтероперабельності, на нашу думку, потребують подальших досліджень.

Список літератури:

1. Conti M., Dehghantanha A., Franke K., Watson S. Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*. 2018. Vol. 78. Part 2. P. 544–546.

2. Sivaraman V., Gharakheili H.H., Vishwanath A., Boreli R., Mehani O. Network-level security and privacy control for smart-home IoT devices. *Internet of Things Communications and Technologies (IoT-CT)*: Proc. IEEE WiMoB Workshop, Abu Dhabi, United Arab Emirates, Oct. 19–21, 2015. P. 163–167.

3. Kyriazis D., Varvarigou T., White D., Rossi A., Cooper J. Sustainable smart city IoT applications: Heat and electricity management & Eco-conscious cruise control for public transportation. *A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*: Proc. 2013 IEEE 14th International Symposium, Madrid, Spain, June 4–7, 2013. P. 1–5.

4. Li S., Xu L.D., Zhao S. 5G Internet of Things: A survey. *Journal of Industrial Information Integration*. 2018. Vol. 10. P. 1–9.

5. Kreutz D. et al. Software-defined networking: a comprehensive survey. *Proceedings of the IEEE*. 2015. Vol. 103. № 1. P. 14–76.

6. Tan W., Fan Y., Ghoneim A., Hossain M.A., Dustdar S. From the Service-Oriented Architecture to the Web API economy. *IEEE Internet Computing*. 2016. Vol. 20. № 4. P. 64–68.

7. Peltz C. Web services orchestration and choreography. *Computer*. 2003. Vol. 36. № 10. P. 46–52.

8. Al-Fuqaha A., Guizani M., Mohammadi M., Aledhari M., Ayyash M. Internet of Things: A survey on enabling technologies protocols and applications. *IEEE Communications Surveys & Tutorials*. 2015. Vol. 17. № 4. P. 2347–2376.

9. Landt J. The history of RFID. *IEEE Potentials*. 2005. Vol. 24. № 4. P. 8–11.

10. Mijumbi R. et al. Network function virtualization: state-of-the-art and research challenges. *IEEE Communications Surveys & Tutorials*. 2016. Vol. 18. № 1. P. 236–262.

11. Armbrust M.A view of cloud computing. *Communications of the ACM*. 2010. Vol. 53. № 4. P. 50–58.

12. Bonomi F., Milito R., Zhu J., Addepalli S. Fog computing and its role in the Internet of Things. *MCC workshop on Mobile cloud computing*: proceedings of the first edition, Helsinki, Finland, August 13–17, 2012. P. 13–16.

13. Atzori L., Iera A., Morabito G. The Internet of Things: a survey. *Computer Networks*. 2010. Vol. 54. № 15. P. 2787–2805.

14. Singh M., Rajan M.A., Shivraj V.L., Balamuralidhar P. Secure MQTT for Internet of Things (IoT). *Communication Systems and Network Technologies*: Proceedings 2015 Fifth International Conference, Gwalior, India, April 4–6, 2015. P. 746–751.

15. Rahman R.A., Shah B. Security analysis of IoT protocols: A focus in CoAP. *Big Data and Smart City (ICBDSC)*: 2016 3rd MEC International Conference, Muscat, Oman, March 15–16, 2016. P. 1–7.

16. Wen Z., Yang R., Garraghan P., Lin T., Xu J., Rovatsos M. Fog orchestration for internet of things services. *IEEE Internet Computing*. 2017. Vol. 21. № 2. P. 16–24.

17. Miorandi D., Sicari S., De Pellegrini F., Chlamtac I. Internet of things: vision, applications and research challenges. *Ad Hoc Networks*. 2012. Vol. 10. № 7. P. 1497–1516.

18. Kortuem G., Kawsar F., Sundramoorthy V., Fitton D. Smart objects as building blocks for the internet of things. *IEEE Internet Computing*. 2010. Vol. 14. № 1. P. 44–51.

19. Guinard D., Trifa V., Karnouskos S., Spiess P., Savio D. Interacting with the SOA-based Internet of Things: discovery, query, selection, and on-demand provisioning of web services. *IEEE Transactions on Services Computing*. 2010. Vol. 3. № 3. P. 223–235.

20. Vilalta R. et al.End-to-end SDN orchestration of IoT services using an SDN/NFV-enabled edge node. *Optical Fiber Communication Conference*: proceedings, Anaheim, California United States, March 20–22, 2016.

21. Liu C., Yang C., Zhang X., Chen J. External integrity verification for outsourced big data in cloud and IoT: A big picture. *Future Generation Computer Systems*. 2015. Vol. 49. P. 58–67.

22. JiaY. J. et al. Contex loT: Towards providing contextual integrity to appified IoT platforms. *Network and Distributed System Security*: proceedings of 24th Annual Symposium, NDSS 2017, San Diego, California, USA, February 26–March 1, 2017. P. 1–15.

23. Bauer J., Staudemeyer R.C., Pöhls H.C., Fragkiadakis A. ECDSA on things: IoT integrity protection in practise. *Information and Communications Security*: proceedings of 18th International Conference, ICICS 2016, Singapore, Singapore, November 29 – December 2, 2016. P. 3–17.

АНАЛИЗ ПОДХОДОВ К ОРКЕСТРОВКЕ IOT-СЕРВИСОВ

В статье исследуются подходы к оркестровке IoT-сервисов. Рассматриваются технологии, на которых основывается функционирование IoT-систем. Характеризуется текущее состояние и распространенность Интернета вещей. Оркестровка IoT-сервисов рассматривается как основополагающая составляющая организации согласованного взаимодействия компонентов IoT-системы путем централизованного координирования. Подходы к оркестровке анализируются с позиции специфики применения.

Ключевые слова: *IoT, SDN, SOA, координирование, оркестровка, программная система, сервис.*

ANALYSIS OF THE APPROACHES TO IOT-SERVICES ORCHESTRATION

The scientific article is devoted to investigation of the approaches to IoT-services orchestration. The core technologies the functioning of IoT-systems is built upon are considered. Current state of the IoT actuality and dissemination is characterized. The orchestration of IoT-services is considered as the main building block of providing the consistent communication between the components of IoT system by way of centralized coordination. The approaches to orchestration are analyzed from the applicability specifics perspective.

Key words: *IoT, SDN, SOA, coordination, orchestration, software system, service.*