

## ІНТЕЛЕКТУАЛЬНІ М2М-ШЛЮЗИ ДЛЯ БЕЗПРОВОДОВИХ ДОМЕНІВ ПРИЛАДІВ

**Кравчук С.О.**

*Інститут телекомунікаційних систем КПІ ім. І. Сікорського, Україна*

*E-mail:sakravchuk@ukr.net*

### **Smart M2M-gateways for wireless devices domains**

The approaches of smart M2M-gateways realization are presented, especially on the basis of RESTful.

В промисловій сфері часто виникають технічні завдання, де сенсорні системи повинні взаємодіяти не тільки між собою, а й з зовнішнім світом за допомогою того чи іншого вузла, для опису цих процесів використовуються два терміни: зв'язок машини з машиною (Machine to Machine - M2M) та Інтернет речей (IoT). Вони мають в основі єдину технологічну парадигму: інтелектуальні пристрої, підключені до Інтернету, дозволяють віддалено збирати і передавати дані [1-3]. Як показує сучасний досвід, аббревіатура IoT в більшій мірі відноситься до споживчого сектору, в той час як M2M має промислове забарвлення і краща при використанні обладнання промислового класу. Одним з найбільш важливих аспектів Інтернету речей є ефективна взаємодія розумних пристроїв один з одним і з хмарними застосуваннями.

Одним із ключових елементів архітектури M2M є шлюзи, які забезпечують пристроям M2M гарантовану міжмережну взаємодію і підключення до мережі і прикладного домену. Шлюз M2M може використовуватися для різних застосувань пристроїв M2M і функціонально може бути об'єднаний в одному модулі с пристроєм або групою пристроїв M2M.

M2M/IoT-шлюзи (рис. 1) дозволяють організувати двосторонній зв'язок польових пристроїв з хмарою, де збираються, зберігаються і обробляються дані за допомогою бізнес-застосувань. Крім того, шлюзи високого класу пропонують можливості з обробки та зберігання даних для надання послуг в автономному режимі, а при підключенні до хмарних застосувань забезпечують контроль і керування в реальному часі. Багатофункціональні IoT-шлюзи підходять для підключення датчиків, виконавчих механізмів і пристроїв комерційного підприємства в рамках M2M-застосувань. Крім того, вони включають в себе весь необхідний набір безпроводових інтерфейсів для організації надійного зв'язку, таких як стільниковий зв'язок, Wi-Fi, Bluetooth і Zigbee.

Реалізація інтелектуального M2M-шлюзу базується на задіянні веб-сервісів RESTful [4-10]. REST (скор. з англ. Representational State Transfer, «передача репрезентативного стану») — підхід до архітектури мережних протоколів, які забезпечують доступ до інформаційних ресурсів (рис. 2). При підході REST кількість методів і складність протоколу суворо обмежені, що призводить до того, що кількість окремих ресурсів має бути великою. Для веб-служб,

побудованих з урахуванням REST (тобто не порушують накладених їм обмежень), застосовують термін «RESTful». На відміну від веб-сервісів (веб-служб) на основі SOAP (Simple Object Access Protocol - протокол обміну структурованими повідомленнями в розподілених обчислювальних системах, базується на форматі XML), не існує «офіційного» стандарту для RESTful веб-API. Справа в тому, що REST є архітектурним стилем, в той час як SOAP є протоколом. Незважаючи на те, що REST не є стандартом сам по собі, більшість RESTful-реалізацій використовують стандарти, такі як HTTP, URL, JSON і XML.

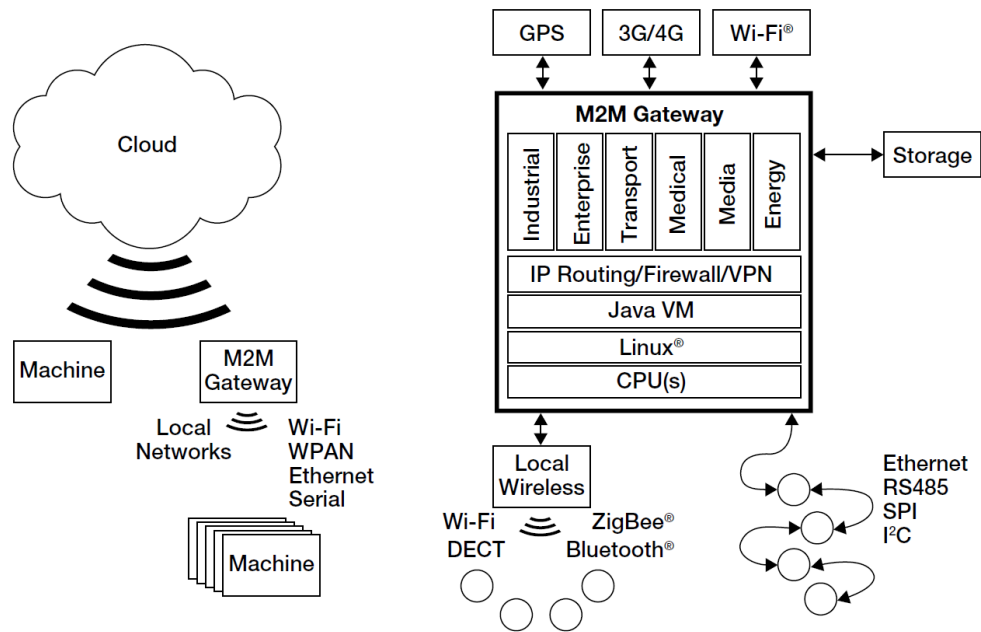


Рис. 1. Приклад M2M-шлюзу (M2M-Gateway).

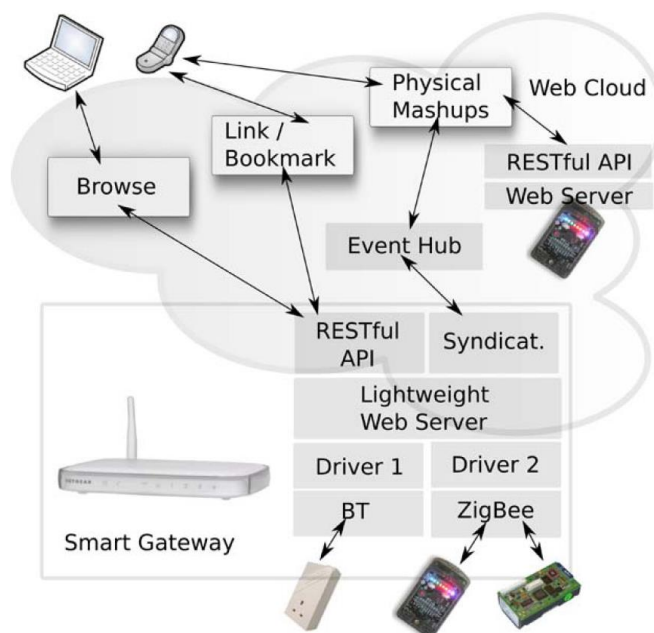


Рис. 2. Інтеграція Web і Інтернету за допомогою Smart Gateways і прямої інтеграції.

При цьому М2М-шлюз виконує трансляцію мережної адреси і фрагментацію/дефрагментацію пакетів.

Припускаємо, що працюємо в ієрархічній безпроводовій сенсорній мережі. Як тільки мережа розгортається, вузли організуються у вигляді ієрархічної моделі. Потім формуються ієрархічні кластери. Кожен кластер складається з великої кількості датчиків з низькою потужністю передачі і одного вузла датчика з високою потужністю передачі. Вузол передачі з високими рівнями потужності розглядається як заголовок кластера СН (cluster head). СН має канал зв'язку з точкою доступу (рівнем доступу).

Припускаємо набір  $S$  з  $K$  датчиків, які утворюють кластер. Кластер складається з вузла (голови кластера, СН), що передає з високими дискретними потужностями  $P_{\text{high}} = \{P_{\text{high } 1}, \dots, P_{\text{high } \max}\}$ , перекривати з вузлами, які передають з більш низькими дискретними потужностями передачі  $P_{\text{low}} = \{P_{\text{low } 1}, \dots, P_{\text{low } \max}\}$ . Передбачається, що датчики зафіксовані, і канал СН завжди підключений до вузла приймача (шлюз, який збирає дані з усіх вузлів і передає їх в центр обробки). Позначимо через  $P_i$  потужність передачі вузла  $i$ , яка передається на вузол  $j$  по радіоканалу. Якість радіоканалу, головним чином, залежить від відстані між передавачем і приймачем. Коли кадр передається вузлом  $i$  з  $P_i$ , він приймається на вузлі  $j$  з  $d_{ij}^{-\nu} P_i$ , де  $d_{ij}$  - відстань між вузлами  $i$  і  $j$ , а  $\nu$  - параметр загасання, який описує втрати на шляху поширення сигналу. Оскільки відстань між вузлами і параметр загасання є фіксованими, єдиний спосіб збільшити потужність прийому - це збільшити потужність передачі. Однак це також збільшує завади і, таким чином, знижує якість підключень безпроводових датчиків, яке вимірюється за допомогою відносини сигнал-завада-плюс-шум (SINR) наступним чином:

$$\gamma_{ij}(P) = \frac{d_{ij}^{-\nu} P_i}{\eta + \sum_{k \neq i} d_{kj}^{-\nu} P_k} .$$

Керування пристроями М2М і кінцевими точками ефективно здійснюється за допомогою шлюзу. Датчики підключені до проксі-входу, а виконавчі механізми підключені до проксі-виходу шлюзу. Всі елементи реалізовані з використанням окремих АРІ-інтерфейсів, доступні для клієнтів SCL (service capabilities layer) і мобільних клієнтів через північний інтерфейс. Повинна бути створена первісна конфігурація пристрою і його кінцевої точки. Це можна зробити за допомогою файлу XML або JSON, що містить статичний опис. Коли пристрій вперше підключається до шлюзу, цей АРІ читає файл конфігурації за допомогою запиту GET, або файл може бути переданий в нього. Файл конфігурації може бути створений і/або оновлений за допомогою мобільних клієнтів шляхом підключення до нього АРІ. Доступ до ресурсів пристроїв і кінцевих точок обмежений авторизованими клієнтами відповідно до прав доступу.

Розглянемо уявлення про взаємодію АРІ шлюзу з клієнтом через SCL архітектуру. Два пристрої М2М підключені до шлюзу на південному інтерфейсі і мобільний клієнт підключається до північного інтерфейсу (до шару доступу) через шар сервісних можливостей. АРІ розробляються на Java, а взаємодія з

пристроями і клієнтами M2M може здійснюватися з використанням XML/JSON. Вихідні файли конфігурації поміщаються в шлюз і розглядаються в API конфігурації ресурсів. Потім описи ресурсів пристрою, кінцевої точки і пристрою витягуються з цих файлів відповідними API і зберігаються в локальній базі даних. Після цього, коли мобільний клієнт видає GET-запит на отримання відомостей про пристрої, підключених до шлюзу, API опису ресурсів пристрою відповідає повним списком пристроїв і їх описами. З поля проксі-виходу і проксі-входу зрозуміло, чи має пристрій виконавчий механізм або датчик. Тепер, коли клієнт отримав інформацію про пристрої, він може вибрати пристрій і запитати у шлюзу відправити відомості про підключену кінцеву точку.

Конфігурація пристроїв і кінцевих точок можливо з мобільних клієнтів. Після того, як вони пов'язані зі шлюзом, клієнти можуть отримати доступ до файлу конфігурації пристрою, використовуючи запит GET. Ресурс API конфігурації надає тільки ті атрибути, які можуть бути створені або оновлені користувачами, наприклад, місце розташування.

## Література

1. Ільченко М.Ю., Кравчук С.О. Телекомунікаційні системи. – К.: Наукова думка, 2017.
2. Algorithm for clusterization, aggregation and prioritization of M2M devices in heterogeneous 4G/5G network / H. V. Beshley, M. O. Seliuchenko, I. A. Bernevek, S. I. Pushchuk, M. I. Beshley // *Visnyk Natsionalnoho universytetu "Lvivska politekhniky". Serie: Radioelektronika ta telekomunikatsii*, 2017-03-28. — Lviv : Vydavnytstvo Lvivskoi politekhniky, 2017. — No 874. — P. 95–102.
3. Тихвинский В.О., Терентьев С.В., Высочин В.П. Использование IMS-ПЛАТФОРМЫ для управления услугами в сетях M2M // *Электросвязь*. - 2011. - № 4. - С. 41-46.
4. Chen M., Wan J., Li F. Machine-to-Machine Communications: Architectures, Standards and Applications // *KSI TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS*. - 2012. - VOL. 6, NO. 2. – P. 480-497.
5. Datta S. K., Bonnet C. Smart M2M Gateway Based Architecture for M2M Device and Endpoint Management // *Published in IEEE International Conference on Internet of...* - 2014 (DOI:10.1109/iThings.2014.18).
6. Mouradian C., Jahromi N. T., Glitho R. H. NFV and SDN-Based Distributed IoT Gateway for Large-Scale Disaster Management // *Published in IEEE Internet of Things Journal* 2018 (DOI:10.1109/IIOT.2018.2867255).
7. Cheng B., Wei Z. M2M Gateway for Remote Wireless Monitoring for District Central Heating Networks // *Sensors* 2014, 14(12), 22447-22470; <https://doi.org/10.3390/s141222447>
8. Datta S. K., Bonnet C., Nikaiein N. An IoT Gateway Centric Architecture to Provide Novel M2M Services // *IEEE World Forum on Internet of Things (WF-IoT)*, pp. 514-519, 6-8 March 2014.
9. ETSI Technical Specification on Machine-to-Machine Communications; Functional Architecture, ETSI TS 102 690, V2.1.1 (2013-10).
10. *Architecting the Internet of Things* / Editors D. Uckelmann, M. Harrison, F. Michahelles. – Verlag, Berlin, Heidelberg: Springer, 2011. – 386 p.