Предаване на данни от интернет на обектите – подходи и протоколи

Л. Боянов

Data Communications in Internet of Things – Approaches and Protocols

L. Boyanov

Department of Information Technologies and Communications, University of National and World Economy, Sofia, Bulgaria, lboyanov@unwe.bg

Key Words: *Internet of Things; data transmission; communication protocols; big data.*

Abstract. *Communication models and protocols in Internet of Things (IoT) are relatively new field of research and use due to the fact, that connecting objects by digital means in Internet has occurred only in the last decade. However, the rapid grow of applications of this paradigm in almost all areas of human activity has led to enormous volume of data generated from all kind of sources (things) and transmitted all over the global digital network. This, in turn, has led to the creation of new models and protocols for data transmission in IoT. The paper gives an overview of the main approaches/models for communication in IoT. The requirement for scalability and simplicity is amongst the most important when IoT and Big data are involved. Four models are presented – the Push, Request/Response, Subscribe/Notify and Publish/Subscribe. A classification and layered approach is made for protocols used in IoT. Three of the most widely used for data transmission in IoT are taken for further investigation – MQTT, CoAP and AMQP. They are compared in terms of bandwidth, overhead, size of transmitted data, reliability and security. Then are compared with HTTP, which is well known and widely used on the Internet. The conclusions are that the most popular model for IoT and Big data communication is the Publish/Subscribe one, whether in regard to the use and recommendation for data protocol, one cannot point a clear leader at present (unlike the protocols in the TCP/IP stack for Internet), so there is the tendency that for the time being, different data protocols will be used in different IoT and big data applications.*

Увод

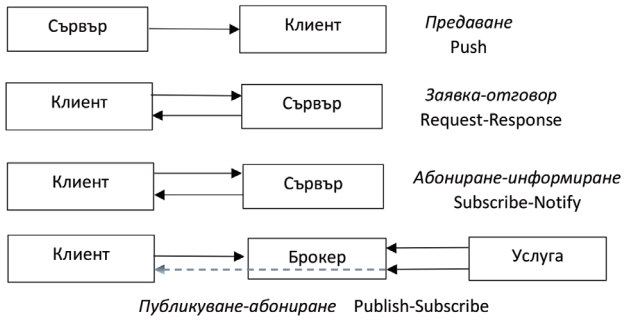
Интернет на обектите (Internet of Things – IoT, също и интернет на нещата) е система от електронно свързани механични обекти (включително машини) или живи същества (хора или животни с цифрови идентификатори), при която се осъществява обмен на данни. Основната разлика между ИнО и традиционния интернет е, че докато при последния в края на връзката най-често има човек или компютърна система, то при ИнО има просто устройство (например сензор или радиочестотен идентификатор – RFID), машина или живо същество. Макар и терминът *Internet of Things* да е предложен през 1999 г. [1], голямата еволюция на този модел става едва в края на първото десетилетие на 21-и век, когато броят на дигитално свързаните обекти в света става по-голям от броя на хората [2]. Днес десетки милиарди обекти се свързват в дигитални жични или безжични мрежи, което дава възможност на хора и автоматизирани системи да следят състоянието на обектите и в някои случаи – да им въздействат по определен начин. Примери за това са широко използваните умни часовници, телефони, умни домашни уреди, множеството сензори и индикатори в съвременните автомобили, системи в медицината, промишлеността, селското стопанство, образованието и т.н. Възможностите за следене на състоянието и идентификацията на произволен обект, откъдето могат да постъпват данни, обуславят изключителните възможности на ИнО като средство за мониторинг, обратна връзка и анализ на обектите от заобикалящата ни среда. От гледна точка на използваните протоколи за обмен на данни традиционният интернет се базира на множество протоколи, които се причисляват към стека TCP/IP. При ИнО има множество свързани разнородни физически обекти към сензорни или локални мрежи и съответно – към глобалния интернет. Поради тази специфика протоколите за обмен на данни и информация, използвани в ИнО, са много и различни.

С разширяване на размера и обхвата на ИнО растат и данните, които тази система генерира. Днес те са днес, разнообразни и от всякакъв вид. Терминът *големи данни* (Big Data) се използва за описанието на големи множества от данни, които се отличават по няколко показателя. На първо място това е техният голям обем. На второ – скоростта, с която те постъпват на мястото за обработка. На трето може да се посочи тяхното разнообразие. Тези три особености се представят често като трите V-та (Volume, Velocity, Variety) или V^3. Характерно за големите данни е, че в повечето случаи те не могат да бъдат обработвани с традиционните и утвърдени системи за управление на бази данни (СУБД). По-долу ще се обърне внимание на подходите за обмен на големите данни в ИнО и кои са най-често използваните комуникационни протоколи за предаване на данни към момента.

Комуникационни модели

В най-общ план може да се посочат четири комуникационни модела на обмен на данни. Първият е предаване-избутване (Push), вторият е заявка-отговор (Request/

Response), третият – абониране-информиране (Subscribe/Notify), а четвъртият – публикуване-абониране (Publish/Subscribe) – *фиг. 1*.



Фиг. 1. Модели за обмен на данни

При модела *Предаване* се осъществява еднопосочна комуникация – сървърът изпраща данни на предварително зададен клиент, който получава данните. Сървърът знае предварително адреса на клиента, а последният чака съобщения/данни от сървъра.

При модела *Заявка-отговор* сървърът получава заявка от клиента и след известно време изпраща отговор. През това време друг клиент може да изпрати заявка, която се слага в опашка/буфер и се обработва веднага след предишната.

При модела *Абониране-информиране* клиентът посочва интерес към дадена услуга, предоставяна от сървъра, към който се изпраща заявка за абонамент. Сървърът запазва заявката и адреса на клиента и когато се появят данни/информация по тази услуга, сървърът я изпраща на клиента.

При модела *Публикуване-абониране* има слабо свързване на комуникационните поредици. Услугите за предлагана информация се управляват от отделен модул, наречен брокер. Когато клиент(и) заяви(ят) своя интерес за определена информация, брокерът поема грижата за препредаване на заявения информационен поток между услугите и клиента/клиентите.

Моделът *Публикуване-абониране* е много разпространен при ИнО и при работа с големи данни. Подходът премахва ефективно излишни комуникационни обмени. Тук има и още една важна причина – значима част от крайните възли в ИнО не притежават сериозни хардуерни възможности. Така брокерът има за задача да намери получателя на съобщението. Този модел е удобен и за прекъснато подаване на данни, т.е. когато има значителни паузи във времето между отделните съобщения или ненадеждна междинна мрежа. Така се избягва честото *ръкостискане* (handshaking), използвано при синхронизацията на комуникациите.

Комуникационни протоколи

В областта на ИнО има множество стандарти, предназначени да обслужват търговски и индустриални приложения. Технологиите Zigbee [3]и Z-wave [4] обслужват редица приложения в умни домове и сгради. Друг често използван протокол за малък обхват през последните години е Bluetooth LE [5] (LE означава ниска консумация на енергия). В случаите, когато трябва да се обменят данни на по-големи разстояния, често са избирани Sigfox [6] или LoRa [7]. Тези стандарти в повечето случаи имат свои собствени транспортни механизми, мрежово свързване, връзки за данни (канално ниво за достъп до мрежата) и изисквания за физическия слой.

Съществуват класификации по различни признаци на протоколите, използвани в ИнО. Една от тях е по това дали протоколът е мрежови (network protocol), или пренася данни (data protocol). **Мрежовите протоколи** са проектирани с цел да свързват и извършват маршрутизацията на данните в мрежи, като често това става в рамките на интернет. Такива протоколи са LoRa, Bluetooth, Zigbee и други. Протоколите за **пренос на данни** са предназначени за комуникация между устройства с ниска мощност и ограничени ресурси. Устройствата могат да обменят данни и без свързване в интернет. Широко разпространени протоколи от този клас са MQTT, CoAP, AMQP, XMPP и други.

По подобие на TCP/IP модела е целесъобразно да се състави модел от протоколи по слоеве, използвани в ИнО. Тези слоеве могат да се дефинират по следния начин:

- Инфраструктурен (6LowPAN, IPv4/IPv6, RPL).
- Идентификационен (EPC, uCode, IPv6, URIs).
- Транспортен (WiFi, Bluetooth, LPWAN).
- Откриващ (Physical Web, mDNS, DNS-SD).
- Пренос на данни (MQTT, CoAP, AMQP, Websocket, Node).
- Управление на устройства (TR-069, OMA-DM).
- Семантичен (JSON-LD, Web Thing Model).

От споменатите по-горе протоколи повече внимание ще се обърне на три – MQTT, CoAP, AMQP, като впоследствие ще се направи сравнение с широко използвания HTTP, който е наложен като стандарт в интернет.

MQTT е т. нар. лек (lightweight) протокол за съобщения [8]. С него се изпращат данни от сензори към приложения. Той работи над стека TCP/IP и предоставя надеждни, прости потоци от данни. MQTT може да работи с всяка мрежа, която осигурява двупосочни връзки без загуби. Протоколът функционира с три важни елемента: абонат, издател и брокер. MQTT е добър избор за безжични мрежи, които изпитват ограничения за честотната лента или работят с ненадеждни връзки. Facebook използва MQTT във Facebook Messenger за споделяне на съобщения. Този протокол използва модела *Публикуване-абониране*. Неговите характеристики го правят много подходящ не само за ИнО комуникации, но и при свързване Machine to Machine (M2M), където има хардуерни ограничения за изпълнение на кода и/или мрежовата честотна лента е ограничена

CoAP е протокол от приложния слой, който се използва в ограничени откъм ресурси устройства [9]. Той е проектиран за лесна интеграция с HTTP, като същевременно отговаря на изисквания като многоадресна поддръжка, ниски режийни разходи и простота. Една от основните цели на CoAP е създаването на общ уеб протокол с изисквания

на среда с ограничения – спрямо енергията, автоматизацията на сградите и други приложения. Целта на CoAP не е да замести директно HTTP, а да реализира архитектурния подход за разпределени системи REST [10], често срещано при HTTP, но оптимизиран за M2M приложения.

AMQP е отворен протокол на приложния слой, ориентиран към съобщения за мидълуеър (middleware) [11]. Определящите характеристики на AMQP са надеждно предаване на съобщенията, маршрутизация (включително точка-точка и публикуване-абониране) и сигурност. Ключови характеристики на AMQP са неговите възможности на пренос на данни през:

- Организации – приложения в различни организации.
- Технологии – приложения на различни платформи.
- Време и пространство – възможно е някоя система да е спряна по различни причини и протоколът е направен да осигурява надеждност.

AMQP версия 1.0 поддържа различни брокерски услуги, които могат да се използват за получаване, нареждане в опашка, маршрутизиране и доставяне на съобщения.

По-долу са представени едни от най-широко разпространените протоколи за пренос на данни за ИнО според [12]. Разглеждат се MQTT, CoAP, AMQP и HTTP според няколко критерии за сравнение между протоколите.

1. **Размер на полезната информация спрямо служебната в едно съобщение.** При CoAP има най-малко служебна информация и най-малък размер на съобщения. Следват MQTT и AMQP. HTTP има най-много служебна информация, но позволява и най-голям размер на съобщенията.
2. **Енергията и ресурсите, необходими за генериране на едно съобщение с еднакво съдържание.** CoAP – ползва най-малко ресурси и има най-ниска консумация. След него са MQTT и AMQP, като при HTTP има най-голяма консумация на енергия и използвани ресурси.
3. **Използвана честотна лента и закъснение.** С най-тясна използвана честотна лента и забавяне е CoAP, следван от MQTT, AMQP. HTTP е с най-широка ползвана честотна лента и най-голямо закъснение.
4. **Качество на услугите (QoS) и надеждност, както и оперативна съвместимост**. MQTT предлага най-високо ниво на качество на услугите, но в същото време има най-малка оперативна съвместимост измежду четирите. В другият край е HTTP, при който има най-голяма оперативна съвместимост в мрежата, но в същото време няма надеждност на предаване на съобщенията, заложена като основна характеристика на протокола. Между тях са CoAP и AMQP.
5. **Сигурност.** AMQP има най-високото ниво на сигурност, докато MQTT е само протокол за съобщения и поддържа най-ниското ниво на сигурност. HTTP следва AMQP относно сигурност, а след него е CoAP. Освен TLS/SSL, MQTT има минимални функции за автентикация и разчита само на потребителско име и парола. CoAP използва методите DTLS и IPsec за автентикация и криптиране.

Представените наблюдения са обобщени в *таблицата*. Характеристиките на протоколите са без абсолютни стойности, защото освен собствени измервания са използвани и данни от други източници и са направени обобщения, които няма как да се изразят коректно в количествени стойности. Приложенията, за които всеки протокол би бил подходящ, зависи изключително много от условията, при които той се прилага. Например различни възли на едно приложение могат да имат различно захранване (даден възел да е на батерия, а друг – свързан към постоянен източник) или пък достъп до различна честотна лента (даден възел е на място с тясна честотна лента, а друг – с много широка). В този смисъл сравнението между протоколите дава насоката и най-важните съображения, които един проектант или разработчик трябва да има предвид и на тази база да прилага съответния протокол за съответен възел.

Сравнение на характеристики на протоколи за пренос на данни в ИнО

Протокол	Полезна информация	Служебна информация	Енергия	Използвана честотна лента	Надеждност	Сигурност	Разпространение
MQTT	Средно	Малко	Средно	Широка	Висока	Ниска	Високо
AMQP	Средно	Средно	Много	Средна	Висока	Висока	Средно
CoAP	Малко	Малко	Малко	Много широка	Средна	Средна	Високо
HTTP	Много	Много	Много	Тясна	Ниска	Висока	Ниско

Заключение

От разгледаните модели на комуникация в ИнО най-широко приложими на този етап са протоколите, които ползват модела *Публикуване-абониране*. Това е разбираемо, защото този протокол е силно скалируем, а при работа с ИнО и с големи данни това е от ключово значение.

Съществуват огромно количество мрежови протоколи, като за къси разстояния в последно време се налага Bluetooth LE, а Lora е предпочитан за градска среда. Поради сравнително краткото време от началото на използване на комуникационни протоколи в ИнО все още няма изтъкнат протокол за обмен на данни, който да отговаря в еднаква степен на най-важните изисквания – ефективност, ниска

енергоемкост, честотна лента, надеждност и сигурност. Въпреки това при свързване със сензори и идентификатори, както и за редица приложения MQTT, AMQP и CoAP са много разпространени – всеки със своите предимства и недостатъци. Ясно е, че проектантите трябва да се съобразяват с изискванията, произтичащи от техните приложения, за да могат да избират и най-подходящия протокол за обмен на данни от ИнО.

Литература

1. Ashton, K. That 'Internet of Things' Thing. RFID JOURNAL, Jun. 22, 2009. Accessed: Feb. 12, 2021. [Online]. Available: https://www.rfidjournal.com/that-internet-of-things-thing.

2. Evans, D. The Internet of Things How the Next Evolution of the Internet Is Changing Everything. Cisco, Apr. 2011. Accessed: Feb. 13, 2021. [Online]. Available: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

3. Zigbee Protocol. Zigbee, Zigbee Alliance. https://zigbeealliance.org/solution/zigbee/ (Accessed Jul. 14, 2021).

4. Z-Wave. Z-Wave - Better and Safer Smart Homes are Built on. Z-Wave. https://www.z-wave.com (Accessed Jul. 14, 2021).

5. Bluetooth Wireless Technology. Bluetooth Technology Overview, Bluetooth® Technology Website. https://www.bluetooth.com/learn-about-bluetooth/tech-overview/ (Accessed Jul. 14, 2021).

6. Sigfox. SIGFOX, THE 0G NETWORK. https://www.sigfox.com/en (Accessed Jul. 14, 2021).

7. What is LoRa?|Semtech LoRa Technology Semtech. https://www.semtech.com/lora/what-is-lora (Accessed Jul. 14, 2021).

8. Hillar, G. C. MQTT Essentials a Lightweight IoT Protocol: the Preferred IoT Publish-subscribe Lightweight Messaging Protocol. 2017. Accessed: Feb. 25, 2021. [Online]. Available: https://learning.oreilly.com/library/view/-/9781787287815/?ar.

9. The Constrained Application Protocol (CoAP). rfc7252, CoAP. https://datatracker.ietf.org/doc/html/rfc7252 (Accessed Jul. 13, 2021).

10. REST API. What is REST, REST API Tutorial. https://restfulapi.net/ (Accessed Jul. 14, 2021).

11. Advanced Message Queuing Protocol. Home|AMQP, AMQP. https://www.amqp.org/ (Accessed Jul. 13, 2021).

12. Naik, N. Choice of Effective Messaging Protocols for IoT Systems: MQTT, CoAP, AMQP and HTTP, in 2017 IEEE International Systems Engineering Symposium (ISSE), Vienna, Austria, Oct. 2017, 1–7. doi: 10.1109/SysEng.2017.8088251.

За контакти:
Доц. д-р **Любен Боянов**
Катедра „Приложна информатика и комуникации"
Университет за национално и световно стопанство
e-mail: lboyanov@unwe.bg