**Beata KRUPANEK**

Politechnika Śląska, Katedra Metrologii, Elektroniki i Automatyki

doi:10.15199/48.2018.11.11

# Przegląd protokołów przeznaczonych do transmisji danych w systemach Internetu Rzeczy

***Streszczenie.*** *W niniejszej publikacji zebrano podstawowe informacje związane z transmisją danych w systemach Internetu Rzeczy. Począwszy od technologii niskopoziomowych definiujących parametry fizyczne* sygnału tj ZigBee, Bluetooth poprzez protokoły routingu (RPL, ADOV, TORA) oraz protokoły pośredniczące w transmisji (6LowPAN, Thread), *aż po protokoły warstwy najwyższej – aplikacji (MQTT, CoRE). Celem artykułu jest przedstawienie mnogości możliwych rozwiązań tego typu systemów objętych wspólną ideą Internetu Rzeczy.*

***Abstract****. This publication gathers basic information related to data transmission in IoT systems. Starting from low-level technologies defining physical parameters of the signal ie ZigBee, Bluetooth through routing protocols (RPL, ADOV, TORA) and protocols mediating in transmission (6LowPAN, Thread) up to the top layer protocols - applications (MQTT, CoRE). The aim of the article is to present a multitude of possible solutions for this type of systems covered by the common idea of the Internet of Things. (**Transmission protocols in IoT systems**).*

**Słowa kluczowe**: Internet Rzeczy, transmisja danych, protokoły komunikacyjne, chmura.
**Keywords**: Internet of Things, data transmission, transmission protocols, cloud.

## Wstęp

Termin Internet Rzeczy został po raz pierwszy użyty w 1999 roku przez Kevina Ashtona z Auto-ID Center w Massachusetts Institute of Technology, współtwórcy globalnego systemu identyfikacji wyrobów w standardzie RFID (ang. Radio Frequency IDentification) [1]. Istnieje wiele definicji Internetu Rzeczy [1 ,2, 3]. Termin ten, według Pawła Kolendy, dyrektora ds. badań IAB Polska, oznacza w uproszczeniu ekosystem, w którym wyposażone w sensory przedmioty komunikują się z komputerami [1]. Z kolei według rekomendacji ITU-T Y.2060 IoT to globalna infrastruktura na potrzeby społeczeństwa informacyjnego, pozwalająca na świadczenie zaawansowanych usług przez połączenie (fizyczne i logiczne) rzeczy bazując na istniejących i ewoluujących technikach informacyjnych i komunikacyjnych. Rzeczy rozumiane są tu jako obiekty świata fizycznego (urządzenia, dobra fizyczne, czujniki, aktuatory itp.) lub wirtualnego (kojarzone z przechowywaną i przetwarzaną informacją), które można zidentyfikować i zintegrować z siecią komunikacyjną. Rzeczy są także jednoznaczne z informacją, która może zmieniać się dynamicznie.

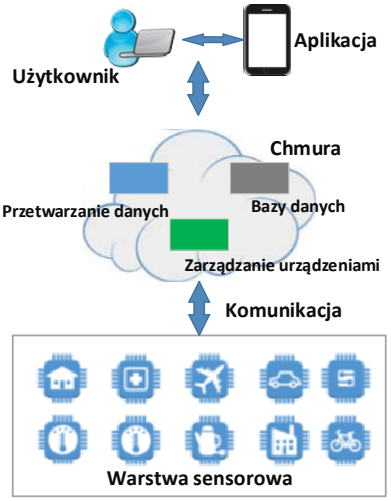
Według Internet Society termin Internet Rzeczy odnosi się do sytuacji, w których łączność w sieci oraz przetwarzanie danych rozszerza się na obiekty, sensory i rzeczy codziennego użytku (nie tylko komputery) pozwalając tym urządzeniom na generowanie i wymianę danych przy minimalnej interwencji człowieka.

Agencja IAB Polska szacuje, że skala zastosowania rozwiązań IoT jest ogromna: od miniaturowych dodatków do odzieży, poprzez inteligentne sprzęty domowe, automatykę budynkową i inteligentne miasta, po gospodarkę wodną czy systemy obronne. W Polsce Internet Rzeczy jest jeszcze w fazie rozwojowej.

## Model komunikacji w IoT

Internet Rzeczy, to w założeniach ogromna liczba urządzeń, które są zdolne do pozyskiwania, gromadzenia danych oraz ich częściowego analizowania i ich transmisji. Zazwyczaj są to różnego rodzaju czujniki i aktuatory, których możliwości są determinowane głównie przez konieczność zmniejszania poboru prądu ze źródła zasilania (zwykle baterii) i ich niewielkimi możliwościami obliczeniowymi (rys. 1). Wszystkie te urządzenia wraz z odpowiednimi interfejsami komunikacyjnymi (np. WiFi, Bluetooth, ZigBee, Z-Wave, Wavenis) tworzą warstwę sensorową trójwarstwowego modelu systemów IoT (rys. 2).

Przechowywanie oraz przetwarzanie danych pochodzących z urządzeń musi być realizowane w wyspecjalizowanym środowisku (chmurze), które zapewnia odpowiednie funkcje, aplikacje, skalowalność i bezpieczeństwo. Zadaniem chmury jest także zapewnienie interfejsu pomiędzy warstwą niższą czyli urządzeniami a usługami warstwy wyższej, aplikacjami typu M2M (ang. Machine-to-Machine) i końcowymi użytkownikami [1].

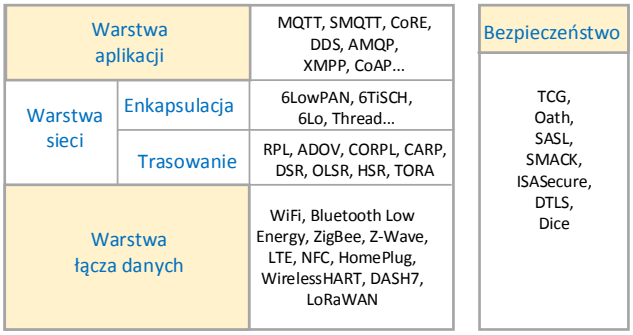



Rys. 1. Ogólna struktura systemu IoT

Omawiany model komunikacji w systemach IoT przedstawiono na rysunku 2. Obecnie funkcjonują jeszcze modele zbudowane z 4 i 5 warstw [4, 5]. Brak standaryzacji w zakresie Internetu Rzeczy skutkuje brakiem na chwilę obecną pewnych jednolitych rozwiązań. Nie ma jednego uniwersalnego standardu technologicznego, który byłby używany do komunikacji pomiędzy urządzeniami w ramach M2M. W praktyce używa się wielu standardów. Największe wyzwania prawne wiążą się z tymi kanałami komunikacji, które są elementem regulowanego i nadzorowanego rynku. Dotyczy to w szczególności używania kanałów komunikacji opartych na bezprzewodowych sieciach komórkowych.

Funkcjonujące w warstwie drugiej protokoły można podzielić na zapewniające trasowanie pakietów (np. RPL, OLSR, ADOV) oraz protokoły zapewniające opakowanie danych z warstwy łącza danych w nagłówki zawierające adres IPv6, którego stosowanie jest konieczne w systemach IoT. W warstwie aplikacji działają zazwyczaj

„lekkie” protokoły przeznaczone do transmisji danych z sensorami np. rozrusznikami serca. Zazwyczaj protokoły takie działają na zasadzie wydawca-subskrybent, co oznacza, że wiadomości wysyłane przez nadawców (ang. publisher) trafiają do serwera pośredniczącego (ang. broker), a nie bezpośrednio do odbiorców (ang. subscriber). Odbiorca otrzymuje wiadomości, którymi faktycznie jest zainteresowany, ale nie wie nic na temat jej nadawcy.




Rys. 2. Stos protokołów używany w systemach Internetu Rzeczy

Często w modelach komunikacji IoT [6] uwzględnia się dodatkowo warstwę związaną z przechowywaniem i zarządzaniem danymi (ang. Sorage and Management) oraz warstwę usług (ang. Services). Można znaleźć także modele 7-warstwowe na wzór modelu ISO/OSI [7]. W celu zapewnienia odpowiedniego poziomu bezpieczeństwa transmisji danych część naukowców proponuje wdrożenie dodatkowej warstwy z nim związanej (ang. Security) umiejscowionej pomiędzy warstwą najniższą, czyli samymi urządzeniami a warstwą łącza danych [8].

**Protokoły łącza danych systemów IoT**

Sieci wchodzące w skład systemów Internetu Rzeczy można podzielić pod względem zasięgu terytorialnego na sieci osobiste oraz rozległe. Sieci osobiste czyli sieci PAN (ang. Personal Area Network) są zwykle stosowane do komunikacji pomiędzy urządzeniami umieszczonymi w niewielkiej odległości od siebie np. inteligentna lodówka, podłączone do sieci elementy monitorujące aktywność fizyczną, sterowane zdalnie rolety oraz termostaty domowe. Zazwyczaj protokoły transmisyjne stosowane w sieciach tego typu oferują wystarczająco duży zasięg przy niewielkim zużyciu energii [2, 3, 9].

Najczęściej stosowane w sieciach PAN protokoły w warstwie łącza danych to IEEE 802.15.4 (a na jego podbudowie działają m. in. ZigBee, Thread, MiWi, WirelessHART), IEEE 802.15.1 (Bluetooth), Wi-Fi (zwłaszcza IEEE 802.11ah dopasowany do Internetu Rzeczy) oraz Enocean i Z-Wave. Obecnie ciekawym rozwiązaniem zoptymalizowanym pod kątem oszczędzania energii jest właśnie protokół EnOcean, który pozwala na pozyskiwanie energii z otoczenia czyli na tzw. energy harvesting. Główne założenie tego typu sieci to bezbateryjne zasilanie węzłów nadawczych (tzw. samozasilające sensory bezprzewodowe). Do zasilania wykorzystuje się różne rozwiązania jak mikrogeneratory elektromagnetyczne, piezoelektryczne, baterie słoneczne czy termoogniwa lub energię mechaniczną uwalnianą podczas korzystania z wyłącznika światła w pomieszczeniu. Z kolei wadą takich technologii jak np. EnOcean jest niewielka przepływność (do 125 kbit/s) oraz bardzo uproszczony protokół dostępu do medium, co skutkuje wieloma kolizjami a w konsekwencji koniecznością powtarzania ramki danych [1, 2, 9, 10].

W tabeli 1 zostały zebrane podstawowe informacje i dane dotyczące wspomnianych protokołów transmisyjnych z uwzględnieniem tych parametrów, które najczęściej bierze się pod uwagę w systemach Internetu Rzeczy. Warto zwrócić uwagę, iż podany zasięg transmisji jest wartością katalogową zależną od konkretnego modemu transmisyjnego oraz od warunków w jakich będzie on pracował np. od obecności grubych ścian, zakłóceń elektromagnetycznych itp. Wartość katalogowa oraz wartość rzeczywista mogą się w tym przypadku znacznie różnić. Ponadto częstotliwość bezprzewodowego kanału komunikacyjnego została podana dla terytorium Unii Europejskiej.

Tabela 1. Porównanie wybranych protokołów transmisji danych stosowanych w IoT

| Nazwa | Zasięg | Często-tliwość | Topologia | Przepływność | Łatwość użycia | Pobór mocy |
|---|---|---|---|---|---|---|
| ZigBee na IEEE 802.15.4 | 10-300m | 868 MHz | Gwiazda, P2P, mesh | Do 250 kbps | duża | 50-100 mW |
| WiFi HaLow IEEE 802.11ah | >1000m | 900 MHz | One hop | Do 780 kbps | duża | 1mW – 100mW |
| Bluetooth IEEE 802.15.1 | 10m | 2.4 GHz | Gwiazda, P2P | Do 3 Mbps | duża | 30 mW |
| Z-Wave | 30m | 868 MHz | Mesh | 9.6 kbps | bardzo duża | 1 mW |
| EnOcean | 30m | 868 MHz | Gwiazda, P2P, mesh | 120 kbps | średnia | <1mW |
| Wavenis | 1000m | 868 MHz | Gwiazda, P2P, mesh | 19.2 kbps | średnia | <1mW |

Łatwość użycia (tab. 1) to parametr wyznaczony na podstawie pewnych subiektywnych przesłanek wynikających np. z łatwości konfiguracji modemu, z udostępnianego przez producenta oprogramowania, z szybkości tworzenia sieci przez węzły, z łatwości montażu modemu itp.

Sieci rozległe zazwyczaj stosowane są tam, gdzie należy monitorować duże obszary geograficzne, a sieć złożona jest z tysięcy autonomicznych węzłów [11, 12, 13]. Odległości między węzłami też zazwyczaj są duże. Przykładem zastosowania tego typu sieci jest np. monitorowanie obszarów leśnych, pól uprawnych, samochodów na skrzyżowaniach itp. W sieciach rozległych zwykle występuje problem z okresowym serwisowaniem urządzeń związanym np. z wymianą baterii, co w sieciach rozległych może stanowić duży kłopot przy zastosowaniu rozwiązań z sieci osobistych PAN. Wymienione ograniczenia doprowadziły do powstania sieci rozległych Internetu Rzeczy czyli sieci WAN (ang. Wide Area Network). Sieci takie składają się zazwyczaj z węzłów o możliwie niewielkim poborze mocy, które komunikują się bezpośrednio z różnego rodzaju koncentratorami (np. stacje bazowe), których zapotrzebowanie na energię jest dużo wyższe [4, 9].

Przykładami systemów transmisyjnych funkcjonujących w sieciach rozległych są sieci komórkowe od GPRS do 5G. Wadą tego typu systemów w kontekście Internetu Rzeczy jest znaczny pobór prądu w momencie wysyłania lub odbierania komunikatów z sieci komórkowej. Wynika to z uwarunkowań dla jakich były tworzone sieci komórkowe a systemy IoT są generalnie nowym rozwiązaniem, które ma inne potrzeby. Ponadto w sieciach komórkowych istnieje ograniczenie co do liczby jednocześnie podłączonych urządzeń, a koszty transmisji danych są często nieadekwatne do kosztów budowy całego systemu.

Dlatego też opracowywana jest (przez konsorcjum NGMN) mobilna sieć telekomunikacyjna przeznaczona specjalnie dla Internetu Rzeczy, którą oznakowano jako 5G. Wielu polskich producentów (np. Nokia) już wdraża systemy pozwalające na testowanie i późniejsze działanie telefonii 5G. W sieciach 5G zmniejszono zużycie energii poszczególnych urządzeń końcowych w celu przesłania komunikatu, zwiększono liczbę jednoczesnych połączeń zapewniając komunikację z wieloma urządzeniami na raz oraz umożliwiono tworzenie sieci kratowych zmniejszając koszty transmisji danych [10, 13, 14].

Z kolei obecne sieci komórkowe, nienadające się do pracy w systemach IoT ze względu, chociażby, na limitowaną liczbę podłączonych urządzeń i wysokie koszty transmisji, spowodowały rozwój sieci WAN o niskim poborze mocy - LPWAN (ang. Low Power WAN). Sieci LPWAN bazują na protokołach, które kosztem gorszej przepustowości mają lepsze parametry w zakresie odporności na zakłócenia i zaniki sygnału. Część z tego typu sieci opiera się na topologii gwiazdy, gdzie węzły komunikują się z stacją bazową, czyli analogicznie jak w sieciach komórkowych. Węzły końcowe w sieciach LPWAN mogą pracować nawet do 20 lat na baterii AA co jest ich największą zaletą [10]. Przykładem takich sieci jest SigFox działający głównie na zachodzie Europy. Sieć Sigfox ogranicza komunikację do 140 komunikatów wysyłanych jednego dnia, każdy może zajmować do 12 bajtów i tylko 8 bajtów dla komunikatu zwrotnego. Opóźnienie transmisji sięga 3-5 ms. Predysponuje to SigFox do współpracy z aplikacjami, które stosunkowo rzadko się komunikują, takich jak na przykład rozproszone mierniki wysyłające co jakiś czas wyniki pomiaru. W Polsce technologia ta jest dostępna w części województw śląskiego oraz lubuskiego. Wybrane protokoły transmisyjne sieci LPWAN zostały zebrane w tabeli 2. Częstotliwość pracy została uwzględniona dla Europy, natomiast przepustowość podano dla łącza przeznaczonego do pobierania danych (ang. DL-down link).

Tabela 2. Porównanie wybranych protokołów transmisji danych na duże odległości - LPWAN

| Nazwa | Zasięg | Często-tliwość | Topologia | Przepu-stowość maks. | Wielkość ramki maks. | Bezpie-czeństwo |
|---|---|---|---|---|---|---|
| SigFox | 10/50 km | 868 MHz | gwiazda | 600 bps | 8B | Brak wsparcia |
| LoRa | 5/15 km | 433 MHz, 868 MHz | wielo-gwiazda | 37,5 kbps | 250B | AES 128 |
| DASH7 | 5 km | 433 MHz, 868 MHz | drzewo | 167 kbps | 8B | AES 128 +własne rozwiązania |
| Ingenu | 15 km | 2,4 GHz | gwiazda, drzewo | 19,5 kbps | 10KB | AES 256, 16B hash |
| Weithless-N | 3 km | 868 MHz | gwiazda | 100 bps | 20 b | AES 128 |

Konkurencyjnymi, dla SigFoxa, rozwiązaniami są LoRa, nWave czy Weightless Alliance. Przyszłościowym rozwiązaniem wydaje się być technologia LoRa, z której można skorzystać bez uiszczania opłat za transmisję danych; sama sieć nie jest też globalnie zarządzana. Wadą rozwiązania jest konieczność zakupu specjalizowanych modemów, które są obecnie produkowane przez tylko firmę Semtech (choć są prowadzone negocjacje nad zwiększeniem liczby producentów). Urządzenia LoRa pracują w paśmie SUB-GHz korzystając z techniki rozpraszania widma CSS (ang. Chirp Spread Spectrum). Prędkość transmisji jest zmienna i może sięgać 37,5 kbps w zależności od typu rozpraszania widma kanału. Zasięg LoRa zmierzony w warunkach testowych wynosi nawet 30 km przy wysokim współczynniku PDR (ang. Packet Delivery Ratio) – ponad 96%. Standardem, który obecnie jest uważany [5] za „przyszłość" transmisji w IoT jest DASH7, który w odróżnieniu od innych technologii LPWAN zapewnia połączenie urządzeń domyślnie w topologii drzewa bez urządzenia centralnego typu gateway. Skutkuje to większą złożonością wyższych warstw stosu protokołów jednakże dzięki badaniu stanu łącza przez wszystkie urządzenia końcowe i sensory zmniejszone zostały opóźnienia w transmisji. DASH7 zawiera mechanizmy korekcji błędów oraz kryptografii, ponadto węzły w sieci są stacjami ukrytymi, które stają się w sieci widoczne po przesłaniu odpowiedniego klucza [1, 10].

Dobierając protokół komunikacyjny do konkretnego zastosowania należy wziąć pod uwagę głównie pobór energii przez węzeł w momencie wysyłania i odbierania komunikatów, kompatybilność z innymi urządzeniami oraz koszt modemu. Kolejnymi wskazaniami do wyboru sposobu komunikowania się są odległość na jaką urządzenie może wysyłać dane, wspierany rodzaj topologii sieci (gwiazda, mesh itp.) oraz przepustowość, opóźnienia w transmisji i częstotliwość wysyłania danych z i do urządzenia. Generalnie jednostka centralna w sieci (koncentrator danych) nie powinna stanowić ograniczenia ponieważ w systemach Internetu Rzeczy powinna ona obsługiwać kilka rodzajów protokołów warstwy łącza danych.

Protokoły komunikacyjne można podzielić również, w dosyć oczywisty sposób na te, które używają pasma licencjonowanego oraz te, które pracują w paśmie ISM. Zarówno w sieciach PAN jak i LPWAN można korzystać z jednego jak i drugiego przedziału częstotliwości.

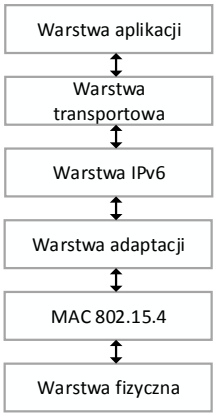
Komunikacja przewodowa w systemach Internetu Rzeczy jest coraz rzadziej wykorzystywana ze względu na ograniczenia jakie niesie ze sobą konieczność prowadzenia dedykowanego okablowania. Dlatego też najczęściej używane są protokoły pozwalające na transmisję danych z wykorzystaniem istniejących łączy energetycznych np. X10, Home Plug.

**Protokoły warstw wyższych**

W warstwie drugiej modelu systemów IoT znajdują się protokoły zapewniające trasowanie pakietów takie jak RPL, ADOV i inne [14]. Najczęściej w systemach Internetu Rzeczy stosowane są protokoły trasowania pochodzące z sieci typu ad-hoc. Wynika to z podobieństwa obu technologii w zakresie dużej liczby sensorów, które najczęściej wymagają tzw. „lekkich" protokołów routingu ze względu na niewielką moc obliczeniową urządzeń. Szerszy opis protokołów routingu można znaleźć w [14, 15, 16].

W warstwie drugiej modelu z rysunku 2 znajduje się podwarstwa związana z enkapsulacją adresów sieciowych. Pracują w niej protokoły zapewniające implementację adresu w wersji IPv6 do danych przesyłanych przez protokoły warstwy łącza danych. Każde urządzenie IoT musi posiadać własny, unikatowy adres, do zapewnienia czego nie wystarczy standardowa adresacja IPv4. Jednym z protokołów, który ją zapewnia to 6LoWPAN (ang. IPv6 over Low Power Wireless Personal Area Networks), który pozwala na wysyłanie i odbieranie pakietów IPv6 przez sieci korzystające z protokołu IEEE 802.15.4 [17]. Protokół ten optymalizuje również wielkość pakietów pod kątem ich transmisji pomiędzy urządzeniami o ograniczonych zasobach. Stos protokołu 6LoWPAN przedstawiono na rysunku 3. Działając na podbudowie warstwy fizycznej i łącza danych protokołów z rodziny 802.15 (np. MiWi,

ZigBee itp.) pozwala na konwersję pakietu danych zaadresowanego przez warstwy niższe do formatu adresu obowiązującego w systemach IoT. Konwersja ta jest niezbędna ze względu na ograniczoną liczbę bajtów pakietu IEEE 802.15.4, która wynosi 128 bajtów, przy czym efektywnie na dane warstw wyższych przypada jedynie 102 bajty. Biorąc pod uwagę to, iż nagłówek protokołu IPv6 składa się z minimum 40 bajtów, a prawie 40 kolejnych bajtów należy łącznie zarezerwować na poczet protokołów bezpieczeństwa i transmisyjnych okazuje się, że na dane aplikacji pozostaje mniej niż 20 bajtów, co jest wartością zbyt małą, aby prowadzić efektywną transmisję danych. Protokół 6LoWPAN zapewnia skrócenie nagłówka protokołu IPv6 do zaledwie 6-10 bajtów w zależności od docelowego adresu danych [17]. Ponadto definiuje możliwości dzielenia danych na mniejsze fragmenty oraz wspiera komunikację w sieci mesh.




Rys. 3. Stos protokołu 6LoWPAN

Zadaniem protokołów warstwy najwyższej (aplikacji) jest tworzenie połączenia pomiędzy urządzeniami, tworzenie zapytań i nasłuchiwanie w celu wychwytywania komunikatów wysyłanych przez inne urządzenia. Protokoły te nadzorują komunikację typu „jeden do wielu" i „wielu do wielu" oraz komunikację z bazą danych. Część z tych protokołów współdziała z protokołem IP np. XMPP (ang. Extensible Messaging and Presence Protocol), AMQP (ang. Advanced Message Queuing Protocol) oraz MQTT (ang. Message Queuint Telemetry Transport). Obecnie promowany jest protokół HomeKit firmy Apple oraz Google Wave. Istotną kwestią związaną z warstwą aplikacji jest gwarancja jakości usług i terminowego dostarczenia pakietu danych czyli QoS, często zapewniana na trzech poziomach [1, 2, 4].

Obecnie powszechnie używa się protokołu MQTT (łączenie z chmurami Amazon Web Services czy Microsoft Azure). Jest on oparty o wzorzec wydawca-subskrybent. W takiej architekturze wiadomości wysyłane przez nadawców trafiają do serwera pośredniczącego, a nie bezpośrednio do odbiorców. Odbiorca otrzymuje wiadomości, którymi faktycznie jest zainteresowany, nie wie nic na temat ich nadawcy. Nadawca także nie wie, który z obiorców otrzyma wiadomość. Serwer pośredniczący musi posiadać odpowiednie zasoby, aby pełnić rolę interfejsu między serwerem danych a urządzeniami końcowymi. Nagłówek protokołu MQTT zajmuje 2 bajty dzięki czemu m.in. nazywany jest „lekkim" protokołem. Ponadto MQTT pozwala na zapewnienie jakości usług na 3 poziomach [18].

**Podsumowanie**

Transmisja danych, poza chmurą obliczeniowo-usługową, jest najbardziej dynamicznie rozwijającą się częścią IoT. W systemach Internetu Rzeczy współistnieje dużo różnych protokołów związanych z komunikacją między urządzeniami i maszynami (D2D, M2M Communication) – począwszy od protokołów definiujących częstotliwość transmisji, poprzez protokoły adaptacyjne do wymagań IoT aż po specjalizowane protokoły aplikacji. Obecnie nie sposób stwierdzić, które z nich zostaną uznane jako część standardu technologii IoT, ponieważ konkurencja na tym rynku jest znaczna. W dużej mierze przyszłość IoT zależy od operatów sieciowych i dostępnej infrastruktury dla konstruktorów oraz programistów systemów IoT.

***Autorka**: dr inż. Beata Krupanek, Politechnika Śląska, Katedra Metrologii, Elektroniki i Automatyki, ul. Akademicka 10, 44-100 Gliwice, E-mail: beata.krupanek@polsl.pl;*

LITERATURA

[1] Trifa V., Guinard D.: Internet Rzeczy. Budowa sieci z wykorzystaniem technologii webowych i Raspberry Pi, Helion, 2017.
[2] Mendes T., Godina R., Rodrigues E., Matias J., Catalão J.: Smart Home Communication Technologies and Applications: Wireless Protocol Assessment for Home Area Network Resources, *Energies* 8 (2015), 7279-7311.
[3] Moinuddin K., Srikantha N., Narayana A., KS L.: A Survey on Secure Communication Protocols for IoT Systems, *IJECS* 6 (2017), Issue 6, 21802-21807.
[4] Sethi P., Sarangi S.: Internet of Things: Architectures, Protocols, and Applications, *Journal of Electrical and Computer Engineering*, Volume 2017.
[5] Rahmani R., Kanter T.: Layering the Internet-of-Things with Multicasting in Flow-Sensors for Internet-of-Services, *International Journal of Multimedia and Ubiquitous Engineering,* Vol.10, No.12 (2015), pp.37-52
[6] Rahmani R., Kanter T.: Layering the Internet-of-Things with Multicasting in Flow-Sensors for Internet-of-Services, *International Journal of Multimedia and Ubiquitous Engineering*, Vol.10, No.12 (2015), pp.37-52
[7] The Internet of Things Reference Model, © 2014 Cisco and/or its affiliates.
[8] Aldosari H.: Proposed Security Layer for the Internet of Things Communication Reference Model, International Conference on Communication, *Procedia Computer Science* 65 (2015), 95–98.
[9] Horyachyy O.: Comparison of Wireless Communication Technologies used in a Smart Home: Analysis of wireless sensor node based on Arduino in home automation scenario. *Faculty of Computing*, Blekinge Institute of Technology, SE-371 79 Karlskrona, Sweden.
[10] Raza U., Kulkarni P., Sooriyabandara M.: Low Power Wide Area Networks: An Overview, *IEEE Communications Surveys & Tutorials*, 19 (2017), Issue: 2.
[11] Abidoye A.P., Obagbuwa I.C.: Models for integrating wireless sensor networks into the Internet of Things. *IET Wirel. Sens. Sys*, 7 (2017), pp. 65-72.
[12] Vermesan O., Friess P.: Internet of Things - From Research and Innovation to Market Deployment. River Pub., (2014).
[13] Hassan S., Syed S., Hussain F.: Communication Technologies in IoT Networks, Internet of Things, Building Blocks and Buisness Models, Springer, (2017).
[14] Alameri I.: MANETS and Internet of Things System: A Development of Data Routing Algorithm, *Engineering, Technology and Applied Science Research*, 2 (2018).
[15] Zikira Y., Ishmanov F., Afzal M., Yu H.: A survey on routing protocols supported by the Contiki Internet of things operating system, *Future Generation Computer Systems*, 12 (2017).
[16] Sankaran S., Sridhar R.: Modeling and Analysis of Routing in IoT Networks, 2015 Intl. Conference on Computing and Network Communications (CoCoNet'15), Dec. 16-19, (2015), Trivandrum, India.
[17] Gee Keng Ee, Chee Kyun Ng, Nor Kamariah Noordin Borhanuddin Mohd. Ali: A Review of 6LoWPAN Routing Protocols, *Proceedings of the Asia-Pacific Advanced Network,* 30 (2010), p. 71-81.
[18] Stanford-Clark A., Truong H.L.: MQTT For Sensor Networks (MQTT-SN) Protocol Specification, International Business Machines Corporation, (2013).