Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej Nr 59

L Międzyuczelniana Konferencja Metrologów

MKM 2018

Szczecin - Kopenhaga, 10-12 września 2018

doi: 10.32016/1.59.24

WĘZŁY KOŃCOWE SYSTEMÓW INTERNETU RZECZY

Beata KRUPANEK, Ryszard BOGACZ

1. Miejsce pracy: Politechnika Śląska, Wydział Elektryczny
   tel.: 32 237 12 41 e-mail: beata.krupanek@polsl.pl
2. Miejsce pracy: Politechnika Śląska, Wydział Elektryczny
   tel.: 32 237 12 41 e-mail: ryszard.bogacz@polsl.pl

Streszczenie: Innowacyjność i rozwój w dziedzinie technologii komputerowych i sieciowych doprowadziły w ostatnim dziesięcioleciu do szybkiego rozwoju i poszerzenia oferty marketingowej związanej z nowoczesnymi urządzeniami (smartfony, tablety itd.) dostępnymi dla przeciętnego odbiorcy. Rosnąca oferta możliwości sieci oraz dostępnych aplikacji stała się początkiem idei połączenia w ramach sieci Internet różnych urządzeń także takich, które nie są kojarzone z technologią komputerową jak czujniki, urządzenia AGD, elementy wykonawcze, a nawet ubrania czy książki. Taki rozwinięty system złożony z wielu elementów wyposażony w odpowiednie oprogramowanie sterujące i aplikacyjne nazywa się Internetem Rzeczy (ang. Internet of Things, w skrócie IoT). Artykuł przestawia przegląd głównych cech technologii IoT oraz ogólną charakterystykę węzłów podłączanych do takiego systemu.

Słowa kluczowe: Internet Rzeczy, IoT, platforma w chmurze, czujniki, komunikacja bezprzewodowa.

1. INFORMACJE OGÓLNE

1.1. Internet Rzeczy - wprowadzenie

Termin Internet Rzeczy został po raz pierwszy użyty w 1999 roku przez Kevina Ashtona z Auto-ID Center w Mas-sachusetts Institute of Technology, współtwórcy globalnego systemu identyfikacji wyrobów w standardzie RFID (ang. Radio-Frequency IDentification) [1]. RFID to ogólny termin używany, aby opisać technologię, która umożliwia automatyczną identyfikację obiektu przy użyciu fal radiowych. Istnieje wiele definicji Internetu Rzeczy [1 ,2, 3]. Istnieje wiele definicji Internetu rzeczy. Termin Internet Rzeczy, według Pawła Kolendy, dyrektora ds. badań IAB Polska, oznacza w uproszczeniu ekosystem, w którym wyposażone w sensory przedmioty komunikują się z komputerami [1]. Każdy przedmiot w systemie IoT musi być indywidualnie identyfikowany, w celu gromadzenia danych, zdalnego monitorowania, podejmowania decyzji i prowadzenia procesów optymalizacji we wszystkich obszarach od produkcji, poprzez infrastrukturę po opiekę medyczną. 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.

Począwszy od 2013 roku, wizja Internetu Rzeczy zmieniała się znacznie z powodu istnienia wielu technologii, począwszy od komunikacji bezprzewodowej w Internecie do systemów mikro-elektromechanicznych (MEMS) wykorzystywanych w tradycyjnych dziedzinach sterowania i automatyki, w tym w gospodarstwie domowym i w budownictwie [3]. Ogólna koncepcja Internetu Rzeczy zakłada, że każdy obiekt ma swój własny identyfikator np. adres IP oraz jest podłączony do globalnego systemu jakim jest Internet. Urządzenia mogą komunikować się ze sobą za pomocą dostępnej dla nich platformy programowej. Użytkownik systemu ma możliwość komunikacji bezpośrednio z każdym urządzeniem, może sprawdzić jego stan, a także nim zdalnie sterować używając platformy.

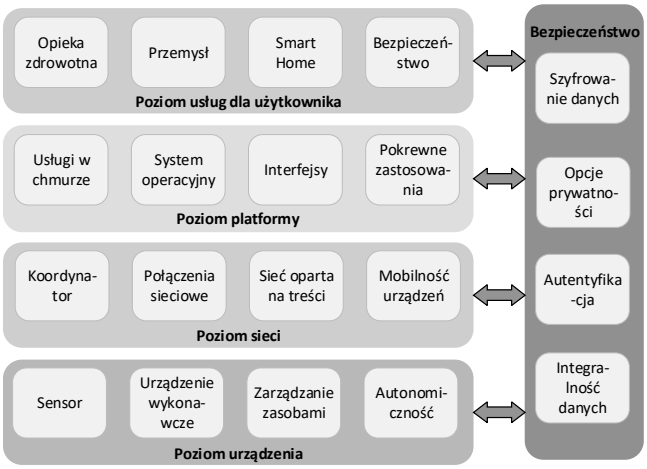
W celu sprawnego zarządzania usługami świadczonymi przez system IoT jego struktura musi być właściwie zaprojektowana. Istnieją jednak pewne ograniczenia budowy takiego systemu. Po pierwsze wielu producentów sprzętu oraz twórców niektórych fragmentów rozwiązań dla IoT nie stosuje standardowych technologii tylko rozwiązania autorskie, które trudno zaimplementować do innego systemu. Ponadto nie istnieje standardowy protokół transmisyjny dla IoT, najczęściej używa się popularnych standardów takich jak ZigBee, Wi-Fi, LTE, nie ma również urządzeń, które byłyby zdolne komunikować się przy użyciu każdego z nich [4, 5]. Z tego też względu urządzenie w sieci IoT pełniące rolę koordynatora (ang. gateway) jest kluczowe do utworzenia sieci. Kolejnym problemem, który zazwyczaj pojawia się przy tworzeniu takich systemów jest pojawiająca się ogromna ilość danych (Big Data), które powinny być przetworzone, przesłane do chmury, przeanalizowane i powinny być podstawą do wygenerowania raportów, statystyk oraz informacji sterujących elementami wykonawczymi.

1.2. Struktura systemu IoT

W ogólnym modelu systemu Internetu Rzeczy można wyróżnić cztery warstwy uwidocznione na rysunku 1. Jest to warstwa usług, warstwa platformy w chmurze, warstwa komunikacji (sieci) oraz warstwa urządzenia.

Warstwa użytkownika (ang. user service layer) stanowi interfejs, przez który użytkownik końcowy może otrzymywać dane pochodzące z systemu oraz nim sterować. Przykładowymi usługami świadczonymi przez IoT są:

zaawansowana opieka zdrowotna (zwłaszcza tzw. telemedycyna), samochody autonomiczne, inteligentny przemysł (np. Industry 4.0), inteligentne miasta (ang. Smart Cities), spersonalizowane urządzenia itp. Opis warstwy usługowej zazwyczaj jest realizowany w odniesieniu do usługi i typu gromadzonych danych [6, 7, 8].

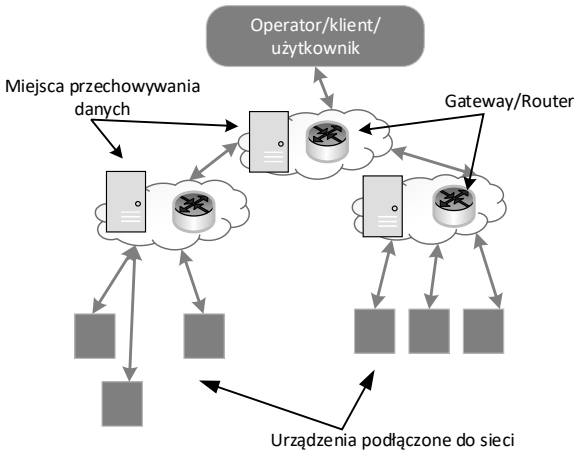


Rys. 1. Struktura systemu IoT

Poziom platformy w chmurze jest zlokalizowany poniżej poziomu użytkownika (usług świadczonych użytkownikowi końcowemu odbiorcy), a jego głównym zadaniem jest dostarczanie rozwiązań programowych i bazodanowych dla wspierania warstwy usługowej [9]. Istnieje bardzo wiele rozwiązań platform IoT włączając w to platformy sprzętowe, platformy ukierunkowane na analizę danych i usługowe. Często potrzeba wdrożenia kilku rodzajów platform w danym rozwiązaniu. Przykładowo platforma zorientowana sprzętowo umożliwia stworzenie środowiska do sterownia obiektami. Platforma do analizy danych pozwala na dopasowanie się do typu rejestrowanych danych, ich analizę, predykcję zmienności wielkości oraz zamianę postaci danych na język zrozumiały dla mikrokontrolera. Najistotniejszym aspektem związanym z platformą jest dobry interfejs programisty (ang. Application Programming Interface API) pozwalający na oprogramowanie systemu. Obecnie wiele firm z rynku IT posiada w swojej ofercie platformę IoT np. Microsoft, Google, IBM, Intel, Cisco, Oracle. Część z nich to platformy komercyjne, a część to platformy otwarte. Zazwyczaj warstwę tę opisuje się modelem wydawca/subskrybent (ang. publisher / subscriber) [9, 10, 11]

Główną warstwą modelu systemu IoT z rysunku 1 jest warstwa sieci (często nazywana warstwą komunikacji). Warstwa sieci zapewnia transmisję danych pomiędzy wszystkimi elementami systemu: urządzeniami a platformą i użytkownikiem a także między użytkownikiem a urządzeniami wykonawczymi. Realizacja fizyczna tej warstwy powinna umożliwić przesyłanie i zarządzanie ogromnymi ilościami danych systemu Internetu Rzeczy często w czasie rzeczywistym. Warstwa komunikacji musi być integralną częścią węzła IoT. Wybrany standard transmisji danych powinien zapewniać odpowiednią szybkość, oszczędność energii a także w wielu przypadkach odpowiednio niewielkie rozmiary modułu komunikacyjnego, który powinien być zintegrowany z sensorem.

W wielu opracowaniach [6, 12, 13] dotyczących systemów IoT prognozuje się, iż nie powstanie nowa dedykowana architektura sieciowa dla tego typu systemów, a obecne i przyszłe rozwiązania będą korzystać z sieci WSN (ang. Wireless Sensor Network). Istotne jest to, że scentralizowana struktura takiej sieci nie jest wystarczająca dla systemów przetwarzających tak duże ilości danych. Proponowane są modyfikacje struktur WSN przy uwzględnieniu typu świadczonej usługi dla klienta czyli sieci zorientowane usługowo SON (ang. service-oriented networks). Najczęściej proponowanym modelem struktury takiej sieci jest model CDN (ang. content distribution network), gdzie dane pochodzące z różnych źródeł przechowywane są w sposób rozproszony w wielu miejscach (rys. 2) [6]. Takie podejście poprawia przepływ informacji w systemie, pozwala na zabezpieczenie danych przed ich utratą, ponieważ dane nie są przechowywane w jednym miejscu, które w razie awarii lub ataku hakera może zostać uszkodzone lub niedostępne. W wielu przypadkach takie podejście obniża również koszt systemu.



Rys. 2. Struktura sieci typu CDN

Istnieją różne rozwiązania sieci CDN ale głównie są to systemy oparte na „farmach serwerów" lub hybrydowe [14]. Różnią się możliwościami, sposobem zarządzania, synchronizacją sieci oraz możliwościami uczenia się sieci. Warstwa urządzeń z rysunku 1 obejmuje wszystkie obiekty niezbędne do zbierania danych, ale także te, które są zorientowane usługowo. Ponadto urządzenia powinny mieć możliwość komunikacji jedno z drugim oraz z siecią. Urządzenia powinny również zapewniać sobie oraz modułowi komunikacyjnemu zasilanie. Obecnie sugeruje się [1, 9, 15], aby urządzenia miały strukturę typu open-source oraz open-hardware co oznacza, że producenci tacy jak Arduino, ioBridge iota czy ARM dostarczają tylko rozwiązań bazowych, które mogą być modyfikowane na potrzeby konkretnego rozwiązania.

2. WĘZŁY KOŃCOWE SYSTEMU IOT

W celu przeanalizowania wymagań stawianych urządzeniom końcowym działającym w sieci Internetu Rzeczy niezbędne jest poznanie struktury takiej sieci, co uczyniono w poprzednim rozdziale. Natomiast z punktu widzenia samego węzła ważna jest implementacja modelu warstwowego (lub jego części) w węźle, stąd konieczne jest przedstawienie podstawowej, uniwersalnej architektury węzła IoT.

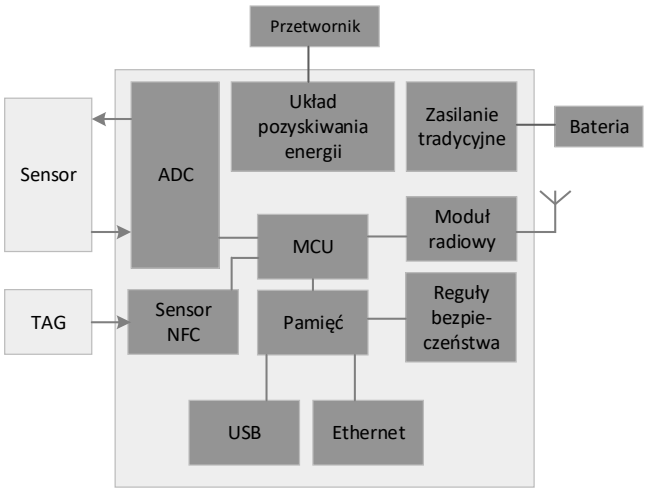
2.1. Architektura typowego węzła

Istnieje wiele różnorodnych struktur węzłów IoT zależnych miedzy innymi od profilu działania sieci,

aplikacji, topologii sieci, wybranego standardu komunikacyjnego oraz kosztów. Można wyróżnić w nich kilka wspólnych elementów, niektóre z nich przedstawiono na rysunku 3. Najważniejszym elementem węzła jest mikrokontroler (MCU) np. STM32 lub inny.

Kolejnym istotnym elementem jest jednostka komunikacyjna czyli moduł radiowy. Może on być zintegrowany z płytką węzła lub być dołączany w inny sposób. Obecnie jest wiele standardów transmisyjnych do wyboru np. ZigBee, WiFi, Z-Wave, UWB, Bluetooth, HomePlug, WirelessHART, LTE itd. Na rysunku wyszczególniono jeden z nich czyli NFC (ang. near-field communication). Jest to radiowy standard komunikacji pozwalający na bezprzewodową wymianę danych na odległość do 20 centymetrów, uważany obecnie za podstawę przyszłych systemów IoT, w których każdy przedmiot (ubranie, produkt spożywczy) będzie wyposażony w sensor pozwalający na pozyskanie o nim danych [6, 8, 15].

W skład węzła IoT wchodzi bardzo często moduł komunikacyjny USB oraz modem przewodowego Ethernetu. Ponadto, zgodnie ze strukturą CDN, węzeł ma pamięć pozwalającą na zapis wyników pomiarów, a także zapis różnego rodzaju reguł bezpieczeństwa.



Rys. 3. Ogólna struktura węzła IoT

Bardzo istotnym elementem węzła jest moduł zasilania, który w najnowszych rozwiązaniach jest dwuczłonowy. Z jednej strony to zasilanie tradycyjne bateryjne a z drugiej strony to układ pozyskiwania energii (ang. energy harvester). Pobieranie energii z rozmaitych źródeł, stało się zupełnie nową i bardzo obiecującą dziedziną, która pozwala na uniknięcie kłopotów z zasilaniem urządzeń bardzo małej mocy, których serwis jest utrudniony.

Układy pozyskiwania energii są często produkowane w postaci wydzielonych modułów. Działają na zasadzie samozasilania i pozostają zawsze w trybie aktywnym, gotowe do odbioru impulsów energii ze źródeł o różnej impedancji. Niektóre rozpoczynają pracę już przy zerowym napięciu zasilania, dzięki czemu nawet najmniejszy ładunek zostaje wykorzystany. Moduły są przystosowane do przechowywania ładunku bez strat, przez długi czas, aby energia mogła być wykorzystywana wtedy, gdy jest najbardziej potrzebna. Najczęściej tego typu moduły zbudowane są z ogniwa Peltiera oraz przetwornika DC-DC lub elementów termoelektrycznych lub mechanicznych [16].

Na rysunku 3 nie zamieszczono jeszcze wielu elementów, które mogą się pojawiać w rożnych konstrukcjach węzłów takich, jak: układ zarządzania zasilaniem, zewnętrzny oscylator, multimoduły komunikacyjnie, struktury typu MEMS, procesory DSP oraz opcjonalne elementy do sygnalizacji i wyświetlania danych.

Istotny z punktu widzenia konstruktora systemu Internetu Rzeczy jest podział obiektów w sieci na:
- aktywne - z funkcjami szybkiego wykrywania zdarzeń w ich otoczeniu, analizą i podjęciem autonomicznych działań;
- porównawcze – których struktura funkcjonalna bazuje na kategorii elementów aktywnych, a uzupełniona jest o możliwość interpretacji rejestrowanych sygnałów i danych z otoczenia oraz ich porównania z parametrami, wartościami predefiniowanymi w algorytmie węzła sieci;
- zorientowane procesowo - uwzględniające elementy dotyczące realizacji różnych zadań w obsługiwanym procesie, sterowania wybranym urządzeniem lub podsystemem infrastruktury systemu, sterowania obiektami w otoczeniu węzła sieciowego lub użytkownika.

W zależności od typu węzła aplikacje dla niego mają inne funkcjonalności. Dla węzłów aktywnych będzie to aplikacja do szybkiego gromadzenia dużych ilości danych i ich analizy oraz generacji rozkazów dla elementów wykonawczych. Dla węzłów zorientowanych procesowo będą to algorytmy sterowania o charakterze kontekstowym, uwzględniające harmonogramy czasowe, sygnały przerwań od różnych czujników czy paneli sterowniczych itp.

2.2. Wymagania dla węzłów IoT

Z budowy węzła IoT przedstawionej na rysunku 3 wynika, iż najważniejszym elementem jest mikrokontroler a jego wybór jest najistotniejszy. Jednakże to wybrany układ zasilania decyduje o czasie życia całej sieci i determinuje w dużej mierze wybór układu radiowego. Uwzględnienie poboru mocy w systemach IoT jest kluczowe ponieważ większość węzłów pracuje przy użyciu zasilania bateryjnego, ponadto w wielu przypadkach serwisowanie urządzeń jest bardzo kłopotliwe.

Czas życia sieci L (ang. network lifetime) wyznaczany jest najczęściej ze wzoru [17]:

$$L = \frac{E_{początkowa}}{E_{całkowita}} \quad (1)$$

gdzie:
$E_{początkowa}$ jest sumaryczną początkową energią zgromadzoną przez wszystkie węzły sieci IoT,
$E_{całkowita}$ jest sumaryczną energią wydatkowaną prze węzeł na wysłanie oraz odebranie komunikatu i jest równa:

$$E_{całkowita} = E_{TX} + E_{RX} = q(E_{ele} + E_{wzm}) + qE_{ele} \quad (2)$$

E_{TX} - jest energią wydatkowaną przez sieć na wysłanie q bitów danych do następnego węzła,
E_{RX} - jest energią wydatkowaną przez sieć na odebranie q bitów danych od sąsiedniego węzła,
E_{ele} – jest energią wydatkowaną na działanie wszystkich układów elektronicznych związaną z przetwarzaniem danych, generacją nośnej itp.,
E_{wzm} – jest energią poświęconą na wzmocnienie sygnału do wysłania danych.

Z pomiarów przeprowadzonych dla ponad 40 elementowej sieci IoT mającej na celu rejestrację samochodów na parkingu wynika, że czas życia sieci jest stały do chwili, aż pierwsze węzły utracą możliwość zasilania bateryjnego. Kolejne węzły będą przejmować ich

funkcje oraz przekazywać większą ilość danych pracując jako rutery. Następnie czas życia sieci *L* wykładniczo maleje w czasie wielokrotnie krótszym niż czas przy pracy wszystkich węzłów przy użyciu zasilania bateryjnego (z przeprowadzonych pomiarów wynika, że jest to stosunek ok. 1:7 zależny od np. standardu transmisyjnego).

Typowe mikrokontrolery używane w systemach IoT (np. CortexM3) zużywają ok 15-30 mW (przy zasilaniu 3V, częstotliwości 12MHz i poborze prądu ok. 5-10 mA) a w stanie głębokiego uśpienia pobór mocy zmniejsza się nawet do około 3 µW. Moduł radiowy (w zależności od standardu) potrzebuje ok. 6-30 mA w celu wysłania ramki danych na poziomie 0 dBm. Zakładając, że węzeł pracuje (pobiera przejawy wielkości mierzonej, autoryzuje dane, wysyła dane, odbiera itd.) przez 20 ms co każde 2 minuty (średnie dane podyktowane przeprowadzonymi pomiarami dla różnych systemów) i pobiera prąd rzędu 10 mA przy zasilaniu 3 V wtedy pobiera moc rzędu 30 mW, tj. 600 µJ w czasie cyklu aktywności. W czasie gdy węzeł jest w stanie nieaktywnym pobiera około 2 µA (6 µW) co daje około 720 µJ. Oznacza to, że węzeł w czasie trybu nieaktywności (ang. sleep mode) może pobrać znaczenie większą energię niż pracując. Każde zmniejszenie poboru energii (za pomocą np. realizacji odpowiednich cykli aktywności i nieaktywności, wyłączeniu funkcji niepotrzebnych w danym momencie itp.) w czasie nieaktywności nawet o 3-5 µJ jest znaczące w perspektywie całego czasu życia sieci.

Węzeł IoT powinien komunikować się w sposób bezprzewodowy z możliwie jak największą liczbą urządzeń i na jak największym obszarze. Niestety, zarówno systemy IoT jak i ich prekursor czyli sieci WSN nie mają predefiniowanego standardu łączności bezprzewodowej. Na rynku jest obecnie wiele standardów (częściowo wylistowanych w tabeli 1), które nie są ze sobą kompatybilne i nie pozwalają na bezpośrednie podłączenie węzła do Internetu, jedynie przez odpowiedniego gatewaya. Jeżeli węzeł ma możliwość komunikowania się w jednym nie będzie w stanie odebrać danych od innego urządzenia. Są tworzone różnego rodzaju rozwiązania łączące modemy bezprzewodowe kilku standardów (np. rozwiązanie firmy Digi integrujące modem ZigBee oraz WiFi), ale okazuje się, że takie urządzenie charakteryzuje się znacznie wyższym kosztem, większymi rozmiarami i często dużą złożonością aplikacyjną a także znacznie większym poborem prądu [1].

Tabela 1. Parametry modemów wybranych standardów transmisji bezprzewodowej

	LTE	**WiFi**	**ZigBee**	**Wireless HART**	**LPWA**
Zasięg	duży	<200 m	100m-1km	<250 m	1-10 km
Topologia	P2P	P2P / Mesh	Mesh	Mesh	P2P
I_{TX} (mA)	600-1100	19-400	34	28	<20
I_{sleep} (mA)	1,5 - 5,5	1,2	0,003	0,008	<0,005
Energy harvester	nie	nie	tak	tak	tak
L (aktywny)	2-3 h	4-8h	60 h	8-10 lat	10-20 lat
L (pasywny)	12 dni	50 h	2-3 lata	-	-
Pasmo	Lic.	ISM	ISM	ISM	ISM

LPWA – Low Power Wide Area.
I_{TX} – pobór prądu w czasie nadawania.
I_{sleep} – pobór prądu w czasie braku aktywności.

Przy wyborze modemu radiowego konieczne jest uwzględnienie nie tylko poboru energii, ale także częstotliwości pracy (pasmo ISM lub licencjonowane), kosztu modemu, rozmiarów oraz często dodatkowych, możliwych do wykorzystania wejść typu I/O i wbudowanych czujników. W systemach IoT istotne jest też, że moduł powinien pracować w standardzie IPv6, czyli musi być w stanie interpretować adresy IP 128- bitowe i tworzyć odpowiednio skonstruowaną ramkę danych. Obiecującymi standardami transmisji wydają się być DASH7 oraz Wi-Fi HaLow, pozwalające na tworzenie systemów, gdzie węzły mogą się poruszać z dużą prędkością [18]. Obecnie adresacja węzła jest dwustopniowa. Adresy IPv6 nadawane są urządzeniom dopiero przez właściwego gatewaya.

Kolejnym ważnym elementem systemu jest mikrokontroler. Jego wybór jest kluczowy w momencie, gdy węzeł systemu będzie musiał realizować częściowe przetwarzanie danych „in situ". Wybierając mikrokontroler do pracy w systemie IoT należy zwrócić uwagę na pobór mocy i możliwości jego zmniejszenia za pomocą trybów o obniżonym poborze prądu. Kolejnym istotnym parametrem mikrokontrolera jest rozdzielczość przetwornika AC/DC (zwykle 14 lub 16 bitów), dokładność przetwarzania oraz wielkość pamięci wewnętrznej (10kB – 1GB). Ważny jest także czas konwersji AC/DC, który ze względu na większe zużycie energii powinien być jak najmniejszy [1, 8, 15].

Obecnie w wielu zastosowaniach wykorzystuje się platformę Ardiuno lub RaspberryPi. Wiele jednostek jest ukierunkowanych do pracy w określonych aplikacjach i zawiera zestaw obwodów peryferyjnych kompletny z punktu widzenia zastosowań aplikacyjnych. Przykładem mogą być układy z obwodami analogowymi przeznaczone do pracy w zasilaczach cyfrowych, jednostki z wbudowanym transceiverem do komunikacji bezprzewodowej (najczęściej WiFi) lub też mikrokontrolery o bardzo niskim poborze energii i z przetwornikiem A/C o wysokiej rozdzielczości, a także blokiem obliczeniowym do kalkulacji zużycia mediów. Wersje specjalizowane kierowane są także do motoryzacji, aplikacji przetwarzających sygnały (z DSP i koprocesorem matematycznym), ze sterownikiem ekranu lub przyciskami dotykowymi, kontrolerem wyświetlacza itd.

Najczęściej stosowaną architekturą mikrokontrolerów jest rodzina układów Cortex-M. W kolejności znajdują się producenci tacy jak: Atmel, Microchip, ST i TI. Dominują układy typu ARM. Szacuje się że jest to 95% rynku IoT. Nie bez znaczenia przy doborze jednostki centralnej jest wsparcie producenta w zakresie platformy w chmurze. Większość producentów np. Intel udostępnia własne środowiska IoT. W przypadku zastosowania układów starego typu niezbędne jest wykorzystanie bramek (ang. gateway) pozwalających na konwersję z platformy sprzętowej do platformy usługowej.

Zastosowania IoT niosą wiele korzyści, ale stwarzają także zupełnie nowe zagrożenia, wśród których najczęściej wymieniane są problemy z prywatnością danych, słabe punkty w systemach autoryzacji i uwierzytelnienia, niezabezpieczone interfejsy WWW, luki i błędy w oprogramowaniu. Dlatego kolejnym istotnym aspektem, który należy uwzględnić przy konstruowaniu węzła IoT jest zapewnienie odpowiedniego poziomu bezpieczeństwa przesyłanych danych. Internet Rzeczy, opierający się na chmurze obliczeniowej i urządzeniach połączonych milionami obsługujących ich aplikacji, nie tworzy

jednolitego środowiska i w związku z tym narażony jest na liczne zagrożenia. Niekontrolowana inwigilacja ludzi, zagrożenia wynikające z działalności hakerów oraz przejęcie kontroli nad urządzeniami to najważniejsze niebezpieczeństwa, które wraz z rozpowszechnieniem IoT staną się realnymi zagrożeniami dla bezpieczeństwa użytkowników. Wiele urządzeń umożliwiających odczytywanie zawartych w nich danych przy zastosowaniu technologii bezstykowej jest podatnych na podsłuchy i skimming, czyli nielegalne skopiowanie zawartości bez wiedzy jej posiadacza w celu utworzenia kopii i wykonywania nieuprawnionych transakcji. Istnieją firmy, które pomagają zabezpieczać systemy w obszarze produkcji, ale wywodzą się one bardziej z tradycyjnego podejścia do cyberbezpieczeństwa niż koncepcji IoT. Pojawiają się jednak również rozwiązania dedykowane np. firewalle warstwy 7 firmy Bayshore, testy penetracyjne i projektowanie zabezpieczeń dla IoT firmy Alutech czy Skkynet Cloud System pozwalający na bezpieczne przesyłanie danych w czasie rzeczywistym [1, 3, 6, 8, 15].

Dla poziomu bezpieczeństwa nie bez znaczenia jest wybór właściwego mikrokontrolera. Na potrzeby rynku IoT powinny to być mikrokontrolery ze zintegrowanym szyfratorem danych, co najmniej powinien to być AES128. Przykładem takiego rozwiązania jest mikrokontroler PIC32MZ z wbudowanym akceleratorem (Crypto Engine) na potrzeby związane z kryptografią danych przy użyciu AES, TDES, SHA i MD5. Niektóre procesory używają bardziej zaawansowanych metod ochrony danych jak np. MSP430FR firmy Texas posiadający pamięć FRAM do przechowywania programu i danych. Ze względu na dużą szybkość zapisu danych, do tego typu pamięci, danymi łatwiej zarządzać pomiędzy okresami aktywnym i pasywnym węzła IoT. Ponadto dostępne są zaawansowane funkcje ochrony pamięci, które eliminują możliwość dostępu do niej (lub wybranych segmentów) z zewnątrz. Tylko autoryzowane programy mogą uzyskać dostęp do tych segmentów pamięci, chroniąc wrażliwe dane przed zewnętrznymi atakami i włamaniami.

3. WNIOSKI KOŃCOWE

Niewątpliwie technologia Internetu Rzeczy jest bliską przyszłością. W skład systemów IoT wchodzi wiele elementów, które w dniu dzisiejszym nie są ze sobą kompatybilne lub mają niewystarczające zasoby i mają nieodpowiednie protokoły komunikacyjne oraz nieodpowiednią topologię sieci. Patrząc z punktu widzenia projektanta systemu IoT należy zwrócić szczególną uwagę na aspekty związane z zasilaniem systemu oraz z jego łącznością ze światem zewnętrznym. Bardzo istotną kwestią jest bezpieczeństwo systemu – znacznie istotniejszą niż częstotliwość pracy mikrokontrolera. Poza wymienionymi kryteriami ważnym parametrem systemu jest jego koszt całkowity uwzględniający kilkuletnie serwisowanie. Na wzrost kosztów ma wpływ dobór poszczególnych elementów – zwłaszcza modułu bezprzewodowego, którego cena może przewyższyć całkowity koszt wszystkich pozostałych elementów węzła.

4. BIBLIOGRAFIA

1. Internet Rzeczy w Polsce. Raport IAB Polska, red. naukowa P. Kolenda, 2015.
2. Vermesan O., Friess P.: Internet of Things - From Research and Innovation to Market Deployment. River Pub., 2014.
3. Brachman A.: Internet przedmiotów. Raport Obserwatorium ICT, Technopark Gliwice, 2013.
4. Yan Z., Niemi V., Yang L.T.: Key technologies for 5G, the next generation of mobile networks and services. Int. J. Commun. Syst., 29/2016, pp.2328-2329.
5. Zhao M.: Discrite Control in the Internet of Things and Smart Environments through a Shared Infrastructure. Ph.D. Thesis, 2015.
6. Lee S.K., Bae M., Kim H.: Future of IoT Networks: A Survey. Applied Sciences, 2017, pp. 1-25.
7. Singh K.J., Kapoor D.S.: Create Your Own Internet of Thinsg: A Survey of IoT Platforms. IEEE Consum. Ele. Mag., 6/2017, pp. 57-68.
8. Chui M., Loffler M., Roberts R.: The internet of things. McKinsey Q., 2/2010, pp. 1-9.
9. Cha S., Ruiz M.P., Wachowicz M., et.al.: The role of an IoT platform in the design of rel-time recommender systems. Proc.of IEEE 3rd World Forum on Internet of Things, USA, 2016, pp.448-453.
10. AllSeen Alliance: Open Source IoT to advance the Internet of Everythings. USA, 2014.
11. Happ D., Karowski N. et al.:Meeting IoT platform requirements with open pub/sub solutions. Ann Telecommun., 72/2017, pp. 41-52.
12. Ning H., Wang Z.: Future Internet of things architecture: Like mankind neural system or social organization framework. IEEE Commun. Lett., 15/2011, pp.461-463.
13. Gubbi J., Buyya R., Marusic S., Palaniswani M.: Internet of Things (IoT): A vision, architectural elements an future directions. Future Gener.Comp. Sys., 29/2013, pp.1645-1660.
14. Mellouk A., Hoceini S., Tran H.: Quality of experience vs. quality of service: Application for a CDN Architecture. Proc. 21st Int. Conf. on Software, Telecomm., and Comp Net. Croatia, 2013.
15. Guinard D., Trifa V.: Internet Rzeczy. Budowa sieci z wykorzystaniem technologii webowych i Raspberry Pi. Helion, 2017.
16. Lampi M.: Internet of Things. Ambient Energy Harvesting. www.wiki.aalto.fi
17. 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.
18. Shrestha H.: DASH7-Based Indoor Navigation System. Helsinki Metropolia Univ. of Applied Sciences, 2014.

IOT END NODES – STRUCTURE AND REQUIREMENTS

Innovation and development in the field of computer and network technologies have led in the last decade to rapid development and expansion of the marketing offer associated with modern devices (smartphones, tablets, etc.) for the average recipient. The growing offer of network possibilities and available applications has become the beginning of the idea of connecting various devices within the Internet network, also those that are not associated with computer technology such as sensors, household appliances, executive elements and even clothes or books. Such a developed system composed of many elements equipped with appropriate control and application software is called the Internet of Things (IoT for short). In order for an object to become part of such a system, a number of requirements related to its computing power, communication, routing etc. should be met. The article presents the main features of IoT technology and the general characteristics of nodes connected to such a system.

Keywords: Internet of Things, IoT, cloud platform, sensor, wireless communication.