

Protokoły i moduły bezprzewodowe dla IoT (1)

Rozwój technologii IoT wymaga wsparcia przez odpowiednie protokoły i oprogramowanie. Można tworzyć własne standardy i sieci sensorów, jednak jest to nieoptyczne, ponieważ – myśląc globalnie – pojawi się problem spięcia naszej sieci z całą „resztą świata”. Dlatego idąc w sukurs konstruktorom budującym urządzenia dla IoT firmy – producenci podzespołów wręcz prześcigają się tworząc różnego rodzaju udogodnienia. Do takich, moim zdaniem, należą moduły komunikacyjne sterowane za pomocą typowych komend AT z zaimplementowanymi stosami komunikacyjnymi.

Uczestnicząc w różnych seminariach organizowanych głównie przez producentów i dystrybutorów, wiele razy słyszałem pytanie – czy używać gotowego modułu, czy układu scalonego? Faktem jest, że wiele firm wytwarzających komponenty elektroniczne oferuje gotowe rozwiązania nie tylko linków radiowych, ale i rozbudowanych sieci. Jako przykład można wymienić firmę Texas Instruments, która od wielu lat promuje rozwiązanie sieciowe o nazwie Simplicity oferując nie tylko podzespoły, ale również oprogramowanie umożliwiające tworzenie elastycznych, energooszczędnych sieci. Wystarczy skorzystać i już. Czy aby na pewno?

Obecnie jako użytkownicy urządzeń rynku konsumenckiego oczekujemy, że będą one połączone bezprzewodowo, bo przecież kto chciałby bawić się z jakimiś przewodami? Dlatego liczba urządzeń łączących się bezprzewodowo pomiędzy sobą lub z jakimiś zasobami rośnie lawinowo. Starsi czytelnicy EP pamiętają, że niegdyś, aby zbudować wyzwalany drogą radiową mechanizm otwierania bramy garażowej wystarczyło wysłać nośną 433 MHz zmodulowaną amplitudowo sygnałem sinusoidalnym np. o częstotliwości 400 Hz. Aktualnie uruchamiany w ten sposób mechanizm otwierania bramy przypuszczalnie od czasu do czasu uruchomiłby napęd bez żadnego powodu, ponieważ używamy tysięcy urządzeń zaśmiecających środowisko elektromagnetyczne. Wymusiło to opracowanie norm kompatybilności elektromagnetycznej i to głównie z nimi będzie musiał zmagać się producent lub dystrybutor wprowadzający produkt na rynek.

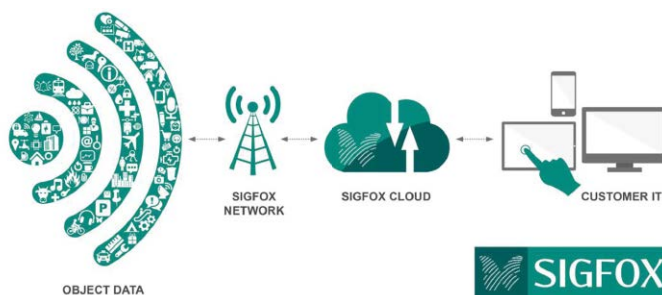
Kompatybilność elektromagnetyczna jest rozumiana jako możliwość poprawnej, niezakłóconej pracy urządzenia w otoczeniu innych urządzeń. Aby tego dokonać, urządzenie musi być odporne na czynniki zewnętrzne i samo nie może emitować zaburzeń ponad dozwoloną normę. Aby się o tym przekonać, niezbędne są pomiary na zgodność z normami. W przypadku urządzenia (interfejsu) radiowego są one bardzo czasochłonne i mogą być wykonane jedynie w specjalnej komorze. To jeszcze nie wszystko. Aby wprowadzić nasze urządzenie na rynek europejski, zależnie od rynku docelowego, będziemy jeszcze potrzebowali „podeprzeć się” opiniami odpowiednich organizacji (ISA, ETSI, inne?). Summa summarum, koszt certyfikacji naszego produktu, jeśli samodzielnie wykonamy interfejs radiowy, może sięgnąć 70-100 tysięcy euro. I teraz trzeba zastanowić się – czy mamy na to czas (bo nadanie certyfikatów potrwa) i czy nas na to stać? Czy nasz pomysł naprawdę jest taki genialny, że gdy np. za 2-3 lata skończy się procedura nadawania odpowiednich certyfikatów nadal będzie trafiał w potrzeby rynku?

Dlatego odpowiedź na pytanie postawione na początku nie jest łatwa. Jasne, że mając układ scalony interfejsu radiowego zbudujemy go w sposób najlepiej pasujący do naszych potrzeb, zajmujący najmniej miejsca i najtańszy, ale produkt musi być ponadczasowy i albo bardzo drogi, albo produkowany w dużych ilościach po to, aby nam się to ostatecznie opłaciło. Dla produkcji w małych lub

średnich woluminach nie traciłbym czasu na odpowiedź, ale skupił się na wyborze odpowiedniego protokołu komunikacyjnego i modułu transmisyjnego spełniającego potrzeby.

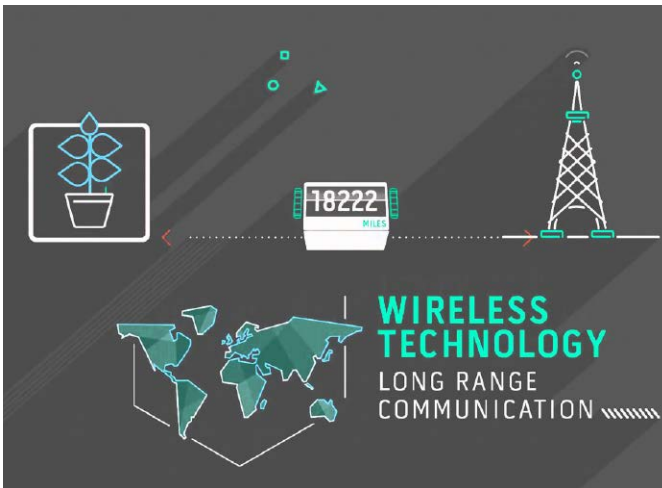
Sieci rozległe – WAN

Aplikacje IoT są specyficzne. Spodziewamy się, że większość urządzeń zostanie połączona siecią o topologii *mesh* (krata) i że będą w niej przesyłane raczej niewielkie komunikaty, o objętości nieprzekraczającej 2 kB. Ze względu na to, że będą to głównie sensory, to będzie ich bardzo dużo (zgodnie z szacunkami spodziewamy się, że do 2020 r. w sieci IoT będzie około 25 miliardów urządzeń), będą one zasilane z baterii lub akumulatora i dla wydłużenia czasu pracy bez konieczności wymiany źródła zasilania – będą okresowo wyprawiane z trybu czuwania w celu przesłania wyników pomiaru. A więc protokół/moduł przeznaczony dla IoT powinien umożliwiać szybkie nawiązanie łączności po aktywowaniu oraz wymagać jak najkrótszego czasu na wykonanie zadania. Przyjrzymy się głównym standardom, które w ostatnich latach wysunęły się na czoło i wydają się podbijać rynek aplikacji IoT.



Sigfox Nazwa standardu wywodzi się od nazwy firmy – twórcy i pomysłodawcy. Jest nią francuska firma Sigfox, która jest nie tylko pomysłodawcą, ale i operatorem sieci.

Sieć Sigfox została pierwotnie opracowana z myślą o połączeniu urządzeń przesyłających niewielkie pakiety danych. Struktura sieci jest zbliżona do sieci telefonii komórkowej. Urządzenia komunikują się z wykorzystaniem technologii transmisji wąskopasmowej UNB (Ultra Narrow Band) – podobnej do używanej przez łodzie podwodne – w nielicencjonowanym pasmie 868 MHz. Intencją twórców było wykorzystanie pasma o jak najdłuższej długości fali, co umożliwia uzyskanie jak największego zasięgu bez konieczności stosowania urządzeń pośredniczących. Firma deklaruje, że komunikaty przesyłane przez urządzenia Sigfox w idealnych warunkach mogą przebyć drogę do 1000 kilometrów, a każda stacja bazowa może obsłużyć do miliona obiektów pobierając jedynie 1/1000 energii wymaganej przez typową stację bazową stosowaną w telefonii komórkowej.



Podstawową różnicą pomiędzy Sigfox a rozwiązaniami oferowanymi przez operatorów telekomunikacyjnych jest to, że ta sieć od początku była opracowana z myślą o małych pakietach danych, podczas gdy inne sieci z definicji są nastawione na transmisję dużych ilości danych przy jak najbardziej optymalnym wykorzystaniu zasobów. Firma podaje w materiałach źródłowych, że stacje bazowe Sigfox mogą obsługiwać komunikaty o długości 12 bajtów, nie więcej niż 140 komunikatów dziennie przesyłanych przez pojedyncze urządzenie. Nie jest to dużo, ale spójrzmy na długość komunikatu z innej strony.

12 bajtów pozwala na zakodowanie liczby z zakresu 0...296. Jeśli uznamy, że pojedyncza liczba to kod sterujący lub wynik pomiaru, to daje to ogromną liczbę możliwości. Kodom mogą towarzyszyć parametry związane np. z aplikacjami śledzącymi, monitorującymi,

parkingowymi, płatniczymi i innymi. Firma deklaruje, że używane w ten sposób moduły transmisyjne mogą pracować do 20 lat (!) przy zasilaniu z dwóch baterii – paluszków AA.

Ekspansja sieci Sigfox rozpoczęła się od Francji. Aktualnie firma ma tam 1200 stacji bazowych obejmujących swoim zasięgiem teren całego kraju. Do nich dołączyło 1300 stacji bazowych w Hiszpanii. Aktualnie sieć obejmuje pokryciem niemal całą Europę Zachodnią, a prace są prowadzone również w Warszawie i w Moskwie. Zapewne to tylko kwestia czasu, gdy będzie z niej można korzystać również w Polsce i w Rosji (<https://goo.gl/DXtFd5>). Firma rozpoczęła również inwestycje w Stanach Zjednoczonych (w paśmie 900 MHz) i planuje tam budowę w 2016 r. 1600 stacji bazowych.

Neul Jednym z głównych konkurentów Sigfox są sieci Neul i LoRa. Są to o tyle ważne standardy, że stoją za nimi potężne koncerny – we wrześniu 2014 r. brytyjska, wywodząc się ze słynnej Uniwersytetu Cambridge, firma Neul została kupiona przez koncern Huawei. Aktualnie nie ma zbyt wielu materiałów dostępnych na temat oferowanej technologii i możemy podzielić się jedynie strzępami docierających do nas informacji. Zgodnie z nimi, tuż po zakupie ustalono pewną strategię działania – Huawei zbuduje infrastrukturę, dla której układy scalone zaprojektuje i dostarczy Neul. Po tej zapowiedzi zauważyliśmy wiadomość na stronie internetowej o tym, że w 2015 r. wybrano nowego prezesa Neul i że firma Huawei otwarła biuro w Parku Technologicznym w Cambridge, i na razie tyle nowości.



REKLAMA

► **POLECANA FIRMA**



Zapewniamy pełne spektrum

- ✓ Bluetooth Low Energy, WiFi, 802.15.4/mesh, 6LoWPAN, ZigBee, Sigfox, GSM/3G/LTE;
- ✓ Atmel-Microchip, Gemalto, Redpine, dresden elektronik, ICP-DAS;
- ✓ Układy scalone, certyfikowane moduły, terminale, gatewaye, accespointy, repeatery;
- ✓ Akcesoria: anteny, przewody, złącza SIM, zasilanie;
- ✓ Rozwiązania security;
- ✓ Doradztwo i szkolenia;

**ZAPISZ SIĘ
NA BEZPŁATNY KURS
NA STRONIE WWW**



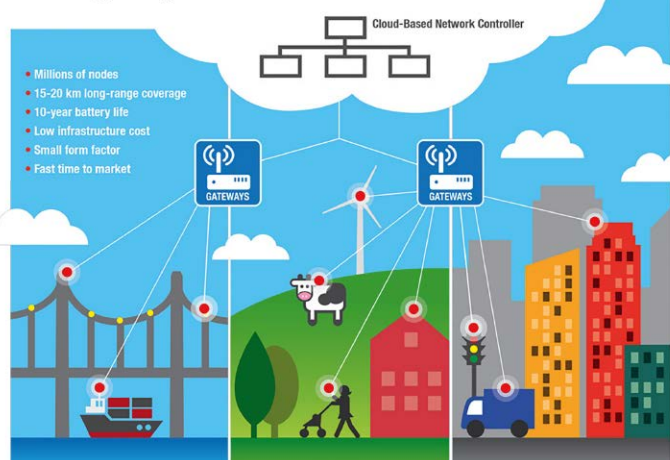
JM elektronik sp. z o.o. • 44-100 Gliwice • ul. Karolinki 58 • tel. 32 3396901 • sprzedaz@jm.pl • www.jm.pl



Zgodnie ze słowami byłego prezesa Stana Bolanda, firma Neul opracowuje dla Huawei wąskopasmowy standard transmisji IoT pracujący z wykorzystaniem pasm „zwolnionych” przez operatorów telefonii komórkowej, to jest częstotliwości z zakresu 450 MHz, 850 MHz i 900 MHz. W trakcie późniejszych prac miano się również zająć pasmami 1,8 GHz i 1,9 GHz używanymi przez LTE. Typowo, transmisja w sieci Neul ma zajmować 200 kHz, a zasada działania urządzeń jest zbliżona do Sigfox.

Pomimo tego, że nadal nie natknąłem się na rozwiązania oferowane użytkownikom „pod klucz”, to jednak nie wolno lekceważyć potencjału, jaki ma Huawei. Może okazać się, że w pewnym momencie standard dosłownie zaleje Chiny, a później rozpocznie się jego ekspansja na inne kraje, ponieważ firma jest znanym producentem urządzeń telekomunikacyjnych używanych na całym świecie i zapewne ma udziały w wielu firmach telekomunikacyjnych. O przygotowaniach Huawei świadczą też inne zakupy: firmy CIP w Ipswich oraz utworzenie działu zajmującego się konstruowaniem procesorów w Bristolu.

LoRa™ End-Node Solution For Long Range and Low Power IoT Networks



LoRa Używając pełnej nazwy, LoRaWAN jest specyfikacją energooszczędnej sieci o dużym zasięgu (LPWAN), w której z założenia będą pracowały głównie urządzenia zasilane bateryjnie. Jako taka doskonale wpisuje się w potrzeby IoT. Architektura sieci LoRaWAN bazuje na topologii gwiazdy, w której bramki są transparentnymi pomostami zapewniającymi transmisję pomiędzy urządzeniami brzegowymi a serwerem centralnym. Bramki są dołączone do serwera za pomocą standardowych połączeń IP, natomiast urządzenia brzegowe wykorzystują do łączenia się z jedną lub wieloma bramkami technikę

rozproszonego widma, z różną prędkością transmisji. Komunikacja z punktami brzegowymi może być dwukierunkowa, co umożliwi nie tylko odbierania komunikatów, ale również kontrolowanie przesyłających je urządzeń lub aktualizowanie ich oprogramowania. Co ciekawe, prędkość transmisji jest zmieniana zależnie od długości komunikatu (technika ADR, Adaptive Data Rate) i mieści się w zakresie 0,3...50 kbps.

Sieć LoRa jest zabezpieczona przed nieautoryzowanym dostępem. Te zabezpieczenia obejmują:

- Unikatowy klucz dostępu do sieci (EUI64) uniemożliwiający nieautoryzowany dostęp do sieci.
- Unikatowy klucz aplikacji (EUI64) uniemożliwiający „poszycie się” pod urządzenie brzegowe.
- Specyficzny kod urządzenia (EUI128) identyfikujący rodzaj urządzenia w sieci. Warto dodać, że w sieciach LoRaWAN zdefiniowano klasy urządzeń końcowych spełniające potrzeby szerokiego zakresu aplikacji.

LoRa Alliance wywodzi się ze Stanów Zjednoczonych. W Internecie nie mogłem znaleźć klarownych danych na temat pokrycia terytoriów zasięgiem sieci. Dla Europy pokazane była jedynie mapki północnej części Belgii oraz południowej i centralnej części Niemiec.

LTE Advanced Operatorzy telefonii komórkowej również nie chcą tracić tak intratnego rynku usług, jakim rysuje się IoT – w jego potrzeby ma wpisać się technologia LTE Advanced oferowana w ramach istniejącej infrastruktury stacji bazowych.

W standardzie LTE Advanced (LTE-A) zwiększono efektywność spektralną transmisji oraz umożliwiono agregowanie częstotliwości nośnych, co umożliwia łączenie transmisji w 5 różnych częstotliwościach o maksymalnej szerokości pasma 20 MHz każda. Dzięki wspomnianym modyfikacjom teoretyczna szybkość transmisji osiągnięta w warunkach idealnych (użytkownik jest nieruchomy, znajduje się w zasięgu stacji bazowej o odpowiednio mocnym sygnale mającej wolne zasoby) w kierunku „down link” wynosi 1 Gb/s, a w kierunku „up link” 500 Mb/s

Obecnie, w niektórych większych miastach na świecie trwają testy sieci LTE Advanced, a w kilku wdrożono nawet próbne, komercyjne rozwiązania tego typu. Obsługa LTE Advanced została też wprowadzona do takich zintegrowanych procesorów, jak np. Qualcomm Snapdragon 800, w którym zaimplementowano m.in. agregację dwóch nośnych o szerokości 10 MHz każda, co ma teoretycznie pozwolić na transfer z szybkością do 150 Mb/s w sieci LTE-A. Pomimo, że urządzenia klienckie LTE Advanced muszą być w pełni kompatybilne ze standardem LTE, rozwiązania techniczne z LTE Advanced zostały też wprowadzone w 2011 r. do specyfikacji trzech nowych kategorii urządzeń LTE.

Największą wadą tej technologii w rozumieniu zastosowania w IoT jest jej przystosowanie do transmisji dużych ilości danych, konieczność ciągłego nasłuchiwanie komunikatów przesyłanych przez sieć, a przez to krótki czas pracy z zasilaniem bateryjnym. Dlatego moim zdaniem moduły LTE-A znajdą zastosowanie głównie w bramkach łączących urządzenia brzegowe z serwerem lub siecią korporacyjną lub w aplikacjach zasilanych stacjonarnie z zasilacza przyłączonego do sieci energetycznej.

Sieci lokalne – LAN i PAN

Oprócz transmisji na duże odległości np. z sieci czujników rozmieszczonych na terenie miasta, technologia IoT będzie też zapewne angażowała transmisję danych w sieciach lokalnych,





o małym zasięgu. Tu znajdują zastosowanie głównie standardy o ugruntowanej pozycji, wśród których wymienilibym głównie Wi-Fi, ZigBee 3.0 oraz Bluetooth 4.2. O ile sieć Wi-Fi jest bardzo dobrze znana z codziennych zastosowań, o tyle zmiany w standardach Bluetooth i ZigBee wymagają kilku słów komentarza.

ZigBee 3.0 Głównymi zaletami ZigBee są: niewielki pobór mocy, obsługa sieci o topologii kraty oraz fakt, że standard ten przyjęło wiele ważnych firm. Na przestrzeni lat, oprócz kolejnych wersji protokołu ZigBee (ZigBee 2004, ZigBee 2006 i ZigBee Pro), powstały też liczne profile aplikacji, podobnie jak w przypadku Bluetootha. Należą do nich m.in. ZigBee Home Automation, ZigBee Smart Energy, ZigBee Remote Control, ZigBee IP, ZigBee Retail Services, ZigBee Green Power czy ZigBee Light Link. Występują one w różnych, nie zawsze ze sobą kompatybilnych wersjach, a niektóre z nich bardzo znacząco się różnią. Przykładowo ZigBee Smart Energy 2.0 opiera się już o protokół IP, co ułatwia transmisję danych pomiędzy siecią ZigBee a Internetem.

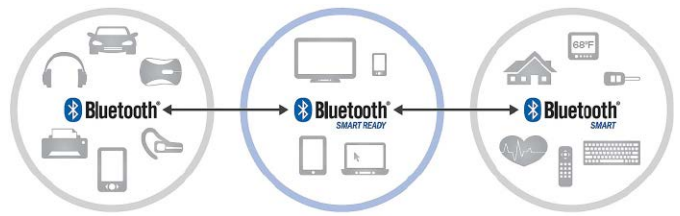
Aktualnie ZigBee znajduje zastosowanie aktualnie przede wszystkim w automatyce budynkowej. Oddzielny profil jest stosowany do komunikacji w ramach systemów oświetlenia, oddzielny do zarządzania i liczenia energii, a jeszcze inny do sterowania domowymi urządzeniami multimedialnymi. Ponieważ tworzy zmieszanie, zdecydowano się zunifikować te obszary zastosowań tworząc nową wersję standardu – ZigBee 3.0.

Nowy standard nie jest jeszcze gotowy – zgodnie z informacją podaną na stronie internetowej firmy Telegesis [12], nadal jest w fazie testowania. Zgodnie z założeniami, ma to być standard wstecznie kompatybilny, korzystający z częstotliwości 2,4 GHz i protokołu ZigBee Pro. Łącząc profile zdefiniowano w nim ponad 130 różnych urządzeń: automatyki domowej, oświetlenia, zarządzania energią, bezpieczeństwa, czujniki, urządzenia medyczne. Co ważne, dotychczasowe urządzenia, zgodne z najnowszymi profilami ZigBee będą poprawnie obsługiwane w sieciach ZigBee 3.0.

Teoretycznie, wprowadzenie ZigBee 3.0 ma pozwolić twórcom aplikacji na szybkie korzystanie z funkcji urządzeń ZigBee innych producentów, gdyż w zależności od typu i funkcji pełnionej przez dany sprzęt, będzie on udostępniał konkretne, określone przez standard parametry. Wszystkie urządzenia, które będą pozwalać na włączanie czegoś, będą przyjmowały identyczną komendę, niezależnie od tego, czym sterują itd. Ma to zdecydowanie zwiększyć możliwości wzajemnej współpracy urządzeń, czyli ułatwić tworzenie aplikacji pasujących do trendu IoT.

Bluetooth 4.2 Obszerne informacje na temat Bluetooth w wersjach wcześniejszych od 4.2 publikowaliśmy w majowym wydaniu EP z 2015 r. [8]. Nie będziemy ich powtarzali, jedynie skupiając się na różnicach pomiędzy interfejsem w wersji 4.1 a 4.2.

Specyfikacja Bluetooth 4.2 obejmuje szereg ważnych zmian związanych z zastosowaniem w IoT. W protokole komunikacyjnym wprowadzono szereg zmian mających na celu podwyższenie



poziomu bezpieczeństwa oraz prędkości transmisji danych. Umożliwiono przy tym korzystanie z adresowania IPv6 oraz protokołu Bluetooth over Internet dla uzyskania bezpośredniego dostępu do sieci Internet. Zachowano przy tym wsteczną kompatybilność ze starszymi wersjami standardu – można powiedzieć, mającymi „4” z przodu, obejmującą opcje obniżonego poboru energii. Dla potrzeb urządzeń IoT zaimplementowano:

- Protokół komunikacyjny Low Power IP (IPv6/6LoWPAN).
- Profil GATT (Bluetooth Smart Internet Gateway).
- Wydłużono długość pakietów danych (LE Data Packet Length Extension).
- Zaimplementowano filtrowanie w warstwie sieciowej.
- Zabezpieczenia LE Privacy 1.2, LE Secure Connections.

Prędkość transmisji w porównaniu do poprzednich wersji standardu z „4 z przodu” wzrosła 2,5-krotnie i wynosi 650 kb/s.

Standard Bluetooth na dobre zagościł w użytkowanych przez nas urządzeniach i jest dobrze znany konstruktorom. Wszystko wskazuje na to, że w wersji 4.2 poprawiono funkcjonalność i nie wykonano jakiegoś karkołomnego kroku, więc ten standard ma bardzo duże szanse na zastosowanie w IoT (w praktyce – jest już stosowany), a liczba urządzeń łączących się za pomocą Bluetooth może dramatycznie wzrosnąć, bo oprócz naszych laptopów i smartfonów będą go też używały np. lodówka i lampka na stole.

Na koniec

Szansę na „przebiecie się” w trudnym rynku IoT – zwłaszcza w sieciach lokalnych – mają też inne standardy. Należą do nich wspomniany Simplicity oferowany przez Texas Instruments lub MiWi promowany przez Microchip. Niewykluczone też, że w wielu zastosowaniach będą służyły moduły pracujące w nielicencjonowanym paśmie ISM służące jako link radiowy pomiędzy sensorem a bramką.

W artykule omówiono najbardziej popularne protokoły radiowe, o których dużo mówi się i słyszy w kontekście IoT i które są implementowane przez różnych producentów. W kolejnym zaprezentujemy przykładowe, popularne moduły, których już można użyć we własnym urządzeniu lub po prostu po to, aby nauczyć się nowych umiejętności.

Jacek Bogusz, EP

Bibliografia:

- [1]. <https://goo.gl/hzN8qd>
- [2]. <https://goo.gl/Etu3xb>
- [3]. <http://goo.gl/qltjiN>
- [4]. <https://goo.gl/6CBFwo>
- [5]. <https://goo.gl/CbTvIj>
- [6]. <https://goo.gl/wG9FPX>
- [7]. <http://goo.gl/xPtYmZ>
- [8]. M. Karbowniczek „Moduły interfejsów bezprzewodowych sieci lokalnych i osobistych”, *Elektronika Praktyczna* 5/2015 (<http://goo.gl/ttV29I>)
- [9]. <https://goo.gl/B4DPlp>
- [10]. <http://goo.gl/hNEDs2>
- [11]. <http://goo.gl/9fwmnR>
- [12]. <http://goo.gl/uXHkAV>