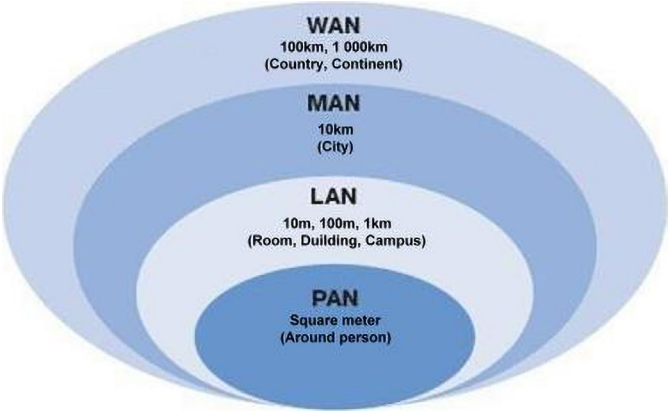
Aktualne standardy komunikacji radiowej

Ogromna popularność urządzeń przenośnych oraz rozwój IoT sprawiły, że nowoczesna elektronika nie może się obejść bez komunikacji radiowej. Co więcej, bardzo często nie wystarcza już zaimplementowanie tylko jednego ze standardów – potrzebnych jest kilka, by obsłużyć wszystkie potrzeby użytkowników. W artykule omawiamy aktualne standardy komunikacji radiowej, pokazujemy, czym się różnią i wskazujemy, kiedy sięgnąć po które z nich.

Komunikację radiową dzieli się na grupy, przede wszystkim w zależności od tego, na jaką odległość ma być prowadzona transmisja. W ogólności można wyróżnić sieci PAN, LAN, WAN i MAN, w których dominować będą określone rodzaje protokołów. Sieci PAN (Personal Area Network – sieć personalna) tworzy się z użyciem wszelkiego rodzaju interfejsów bezprzewodowych, których zasięg transmisji sięga kilku metrów. W obszarze tym dominuje Bluetooth, ale dzięki jego rozwojowi nowe wersje tego protokołu pozwalają także na tworzenie znacznie bardziej rozległych sieci. LAN (Local Area Network – sieć lokalna) pozwala łączyć ze sobą urządzenia zlokalizowane w jednym mieszkaniu lub budynku. Wśród rozwiązań bezprzewodowych najbardziej oczywistym protokołem dla takiej sieci będzie Wi-Fi, ale coraz częściej, szczególnie w przypadku małych, energooszczędnych urządzeń, korzysta się z nowych wersji standardów takich jak Bluetooth czy innych, lekkich interfejsów radiowych. WAN (Wide Area Network – sieć rozległa) zazwyczaj rozumiane jest jako interfejs internetowy. W typowych implementacjach do zapewnienia łączności



Rysunek 1. Sieci PAN, LAN, MAN, WAN

WAN stosuje się rozwiązania kablowe albo sieci komórkowe. Ani jedne, ani drugie nie będą omawiane w ramach niniejszego artykułu (sieci komórkowe i rozwiązania klasy 5G będą stanowić temat numeru lipcowego wydania EP), ale opiszemy sieci LoRaWAN i podobne (np. Sigfox), które można zakwalifikować do rozwiązań klasy WAN. W końcu mamy MAN (Metropolitan Area Network – sieci miejskie), które zatraciły już swój sens, głównie przez rozwój wcześniej wymienionych technologii. Ideą sieci MAN jest organizacja własnej komunikacji na obszarze wielu budynków lub nawet całego miasta, ale aktualnie, gdy zachodzi potrzeba wymiany informacji pomiędzy tak rozlegle rozmieszczonymi urządzeniami, bardziej opłaca się skorzystać z sieci komórkowych lub innych interfejsów, podłączających sprzęt do Internetu.

Bluetooth

Bluetooth to obecnie bardzo popularny protokół. Szacuje się, że każdego roku powstaje 4 mld urządzeń, kompatybilnych z tym standardem, a organizacja Bluetooth SIG łączy 34 tysiące firm. Choć początkowo twórcy Bluetootha postanowili, że nie będzie to protokół uniwersalny, aktualnie sytuacja wygląda dosyć odmiennie. Najpierw Bluetooth bazował na szeregu profili, ale dla obecnych wersji tego protokołu nie mają one już takiego znaczenia. Standard, nad którym pieczę trzyma organizacja Bluetooth Special Interest Group, ewoluował poprzez wersje 1.0, 1.2, 2.0, 2.1, 3.0, 4.0, 4.1, 4.2 i 5.0, a obecnie dostępna jest już wersja 5.1. Jest stosowany w bardzo różnych aplikacjach – w tym m.in. w roli sygnalizatorów przez ponad 80% lotnisk na świecie.

Bluetooth pracuje w paśmie ISM (Industrial, Scientific, Medical; nielicencjonowanym) na częstotliwościach około 2,4 GHz. Może służyć np. do przesyłu sygnałów audio do słuchawek lub z mikrofonów, komunikacji do klawiatur czy myszek z komputerami; wszystkie te funkcje wywodzą się jeszcze z dawnych czasów Bluetootha Classic, a więc z okresu przed wprowadzeniem zupełnie nowatorskiego rozszerzenia w postaci Bluetooth Low Energy, dostępnego od momentu pojawienia się wersji Bluetooth 4.0. To właśnie Low Energy (obecnie kryjące się pod nazwą Bluetooth Smart) sprawiło, że Bluetooth zapewnił sobie bezpieczną pozycję na rynku komunikacji bezprzewodowej. BT LE zerwało z zaszłościami z początków tego interfejsu. Zamiast tego sięgnięto po pomysły, jakie mieli twórcy konkurencyjnego rozwiązania – interfejsu Wibree, który w rzeczywistości nigdy się nie przyjął.

Bluetooth Low Energy/Smart

Bluetooth 4.0 LE rozwiązał dwa podstawowe problemy, z jakimi mierzyli się użytkownicy tego interfejsu i jakie sprawiały, że inżynierowie często zwyczajnie rezygnowali z jego implementacji albo szukali alternatyw takich jak np. ZigBee czy ANT. Przede wszystkim znacząco zmniejszono pobór prądu poprzez ograniczenie konieczności podtrzymywania połączenia, a dodatkowo zlikwidowano konieczność ciągłego parowania ze sobą połączonych już raz urządzeń. To sprawiło, że Bluetooth zaczął się nagle nadawać do zastosowania we wszelkiego rodzaju urządzeniach, które komunikują się jedynie raz na jakiś czas, przesyłając małe porcje informacji – a to właśnie taki sposób komunikacji jest typowy dla wielu urządzeń IoT. Bluetooth 4.0 LE sprawił, że producentom urządzeń elektronicznych przestało się opłacać tworzyć własnościowe technologie komunikacji i szukać alternatyw. Obecnie urządzenia wciąż muszą implementować obsługę profili BT, ale odbywa się to na znacznie prostszej zasadzie, w której w jednolity sposób poszczególne urządzenia Bluetooth deklarują świadczone przez siebie usługi. W efekcie krokomierz nowej generacji będzie w stanie komunikować się nie tylko z opaską tego samego producenta, ale z dowolną, która wspiera Bluetooth 4.0 LE lub nowszy. Gwoli wyjaśnienia warto dodać, że na rynku funkcjonuje jeszcze określenie Bluetooth Smart Ready, które obejmuje urządzenia najbardziej uniwersalne, a więc te, które potrafią się komunikować zarówno np. z zestawami słuchawkowymi, pracującymi zgodnie z Bluetooth Classic, jak i z sensorami Bluetooth Smart.

Specyfikacja Bluetooth 4.0 pojawiła się w połowie 2010 roku i była stopniowo uaktualniana. Ważne jest, by dobierając moduł komunikacyjny, wziąć pod uwagę to, z którą wersją protokołu jest on zgodny. Niektóre z nich mają po prostu bardzo istotne, nowe funkcje, a niektóre mogą mieć ogromne znaczenie ze względu na specyfikę konkretnego projektu. Na rynku dostępne są jednocześnie moduły w różnych standardach, przy czym bywa, że producent deklaruje możliwość programowego uaktualnienia danego modułu tak, by w przyszłości był zgodny z nowszym standardem. Zdarza się też niemal odwrotnie – że moduł zostanie wyprodukowany zgodnie ze szkicem standardu, który nie jest jeszcze formalnie zatwierdzony. Pewną rolę odgrywa tu renoma producenta, gdyż przy obecnej mnogości dostawców łatwo trafić na firmę, której bardziej zależy na chwilowym zysku niż długotrwałym, dobrym imieniu.

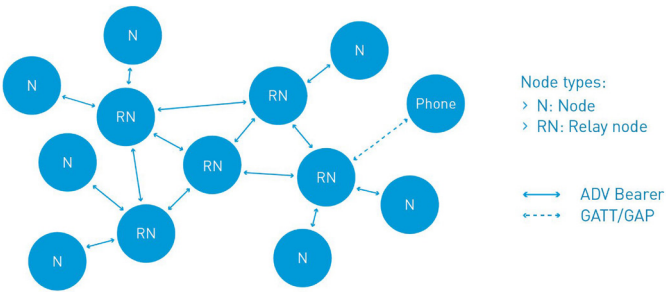
Wracając do poszczególnych wersji protokołu: w 2013 roku wypuszczono standard Bluetooth 4.1, który obejmował liczne zmiany programowe w protokole, ale żadne z nich nie były rewolucyjne. Do najważniejszych należą: ograniczenie interferencji z sieciami komórkowymi 4G, automatyczne włączanie i wyłączanie urządzeń oraz umożliwienie jednoczesnej pracy w trybie koncentratorów sieciowych i urządzeń peryferyjnych. Może mieć to znaczenie dla niektórych systemów IoT, gdyż dzięki tym modyfikacjom Bluetooth coraz bardziej można było nazywać prawdziwym protokołem sieciowym. Nieco większe zmiany, z punktu widzenia obecnych zastosowań, pojawiły się w wersji 4.2, którą opracowano właśnie pod kątem Internetu Rzeczy i opublikowano w 2014 roku. Wprowadzono mechanizmy ułatwiające komunikację urządzeń Bluetooth z Internetem, zwiększono 10-krotnie dopuszczalną wielkość pakietów, a przy okazji 2,5-krotnie zwiększono maksymalną szybkość transmisji.

Bluetooth w topologii kraty

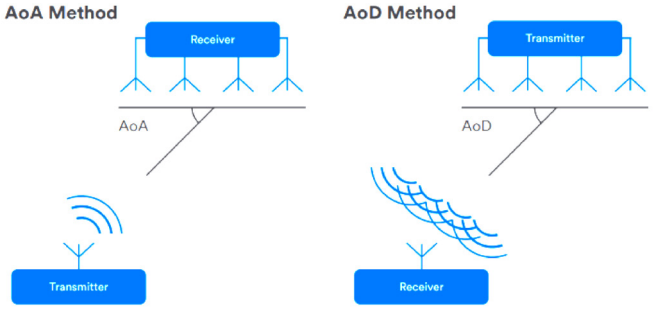
Trzy lata temu pojawił się standard Bluetooth 5.0, który już z łatwością można znaleźć w dostępnych na rynku modułach i układach sieciowych. Oprócz kolejnego zwiększenia przepustowości, powiększenia transferu i zmniejszenia opóźnień w transmisji, zaimplementowano obsługę sieci o topologii kraty. Tym samym zaimplementowano chyba ostatnią z funkcji, która mogła przekonywać część projektantów do sięgania po alternatywne rozwiązania. Obsługa sieci o topologii kraty (czasem nazywanej angielskim wyrazem „mesh") sprawiła, że Bluetooth stał się tym samym bardzo zaawansowanym protokołem sieciowym. Pozwala to też na ogromne wydłużenie zasięgu komunikacji. Wdrożenie Bluetootha 5.0 w grupie urządzeń rozmieszczonej w miarę równomiernie na dużej przestrzeni umożliwia prowadzenie komunikacji pomiędzy dowolnymi z nich, nawet jeśli odległości pomiędzy nimi przekraczają maksymalny zasięg bezpośredniej transmisji punkt-punkt. Co więcej, dane nie muszą już przechodzić przez żaden centralny koncentrator, tylko mogą biec najkrótszymi ścieżkami pomiędzy dowolną parą urządzeń. Przy okazji warto dodać, że zasięg transmisji nie tylko wzrósł, ale jeszcze może być indywidualnie konfigurowany. Projektant ma możliwość wyboru, czy preferuje ograniczyć pobór mocy i tym samym zmniejszyć zasięg, czy też wydłużyć odległość transmisji kosztem zwiększonego zużycia energii. To nie wszystko, bo na dopuszczalny dystans i pobieraną moc wpływ ma też przepustowość, którą w standardzie Bluetooth 5.0 również można manipulować.

Bluetooth 5.1

Najnowsze rozszerzenie, Bluetooth 5.1, zostało opublikowane na początku tego roku. Główną nowością jest wprowadzenie mechanizmów wykrywania orientacji w przestrzeni w oparciu na nadchodzących sygnałach radiowych. Moduł BT 5.1 ma być w stanie określać kąty, z których dochodzą sygnały radiowe, dzięki czemu urządzenia będą mogły nie tylko oceniać odległość, z jakiej dochodzi sygnał, ale też kierunek, w którym znajduje się drugie urządzenie. W idealnych warunkach połączenie tych funkcji ma pozwalać na pozycjonowanie



Rysunek 2. Topologia kraty w Bluetooth 5.0



Rysunek 3. Techniki AoA i AoD w Bluetooth 5.1

obiektów z dokładnością do centymetra. Będzie to jednak wymagało odpowiedniego zaprojektowania anten. Jedno z urządzeń musi bowiem być wyposażone w szereg anten i w zależności od tego, czy ma je nadajnik, czy odbiornik, stosowana będzie technika badania kątów przybywania sygnału (AoA – Angle of Arrival) lub emisji (AoD – Angle of Departure). Niewątpliwie, dobre wykorzystanie tych nowości będzie wymagało dużych umiejętności ze strony konstruktorów i zapewne warto będzie korzystać z gotowych modułów z poprawnie zaprojektowanymi antenami. Wtedy to Bluetooth powinien umożliwić dokładną nawigację w budynkach, takich jak np. centra handlowe.

To nie wszystko. Kolejną nowością jest zwiększenie ilości informacji przechowywanych w pamięci, a obejmujących cechy innych urządzeń Bluetooth, jakie znajdują się w okolicy. Dzięki temu można rzadziej przeprowadzać wykrywanie usług oferowanych przez urządzenia w otoczeniu, co jest zarówno nieco czasochłonne, jak i energochłonne. Usprawniono też mechanizm ogłaszania dostępności urządzenia, który w wersji 5.0 wymagał cyklicznego przechodzenia przez kanały 37, 38 i 39. W wersji 5.1 kolejność jest losowa, a więc znacząco maleje szansa, że dwa urządzenia będą się stale zakłócały podczas ogłaszania swojej dostępności. Co więcej, w protokole Bluetooth 5.0 urządzenie mogło przekazać drugiemu informacje o swoim harmonogramie rozgłaszania usług. Pozwala to ograniczyć nasłuchiwanie tych informacji do określonych okien czasowych i znacząco zaoszczędzić energię. Jednakże biorąc pod uwagę specyfikę i energooszczędność najmniejszych urządzeń IoT, w wersji 5.1 wprowadzono możliwość przekazywania informacji o harmonogramach urządzeń trzecich, a więc przykładowo smartfon może dowiedzieć się od jednego czujnika o tym, kiedy nasłuchiwać informacji o usługach drugiego czujnika.

ZigBee

Bezpośrednią alternatywą dla standardu Bluetooth w wersji 5.0 i nowszej jest ZigBee. Choć wywodzi się z 2002 roku, a pierwsze produkty zgodne z ZigBee pojawiły się w 2006 roku, standard ten funkcjonuje w dużej mierze na uboczu – poza głównym obszarem zainteresowania większości elektroników. Powodów ku temu jest wiele. Na przestrzeni kilkunastu lat ZigBee znalazło zastosowanie w inteligentnych domach, budynkach użyteczności publicznej, fabrykach, inteligentnych miastach oraz w innych dużych instalacjach i transporcie. Jednakże cały czas były to aplikacje bardziej przemysłowe, a te rządzą się swoimi prawami. W przemyśle wdrażanie nowych technologii elektronicznych przebiega wolniej niż na rynku konsumenckim, a do tego technologie bezprzewodowe zaczęły być akceptowane w środowisku przemysłowym znacznie później niż w urządzeniach, których niezawodność nie jest krytyczna. Natomiast w dobie IoT ZigBee wydaje się rewelacyjnym, gotowym już rozwiązaniem. Szczególnie korzystna jest możliwość pracy w sieciach o topologii kraty,

co pozwala na tworzenie bardzo rozległych i niezawodnych instalacji, bez ścisłego planowania architektury takiej sieci i zapewniania bezpośredniego połączenia z bramkami. Standard Bluetooth zyskał podobną możliwość dopiero w wersji 5.0, a to oznacza, że zdecydowana większość urządzeń na rynku, które korzystają z Bluetooth, nie może być wykorzystana do stworzenia kraty. W przypadku ZigBee można niejako podłączyć się do istniejącej sieci automatyki domowej i skorzystać z należących do niej bramek.

ZigBee w IoT

Ponadto aktualna wersja standardu, wprowadzona na początku 2016 roku i znana pod nazwą ZigBee 3.0 lub po prostu ZigBee, została bezpośrednio opracowana z myślą o aplikacjach IoT. Umożliwia projektantom produktów i właścicielom infrastruktury na wdrażanie niezawodnych sieci i wybór odpowiedniego stopnia równowagi pomiędzy złożonością zabezpieczeń a łatwością instalacji.

Przydatność ZigBee pod kątem IoT wynika po części z faktu, że jest to otwarty standard. Te same produkty mogą być wykorzystane praktycznie na całym świecie, co daje klientom duży wybór. Wielu dostawców współpracujących ze sobą elementów tego systemu sprawia, że nie są one ograniczone do żadnych konkretnych marek ani określonych producentów półprzewodników. ZigBee jest łatwe w instalacji i utrzymaniu, bo bazuje na samoorganizacji i samonaprawiającej się topologii sieciowej. Jest odporne na zakłócenia, niedrogie i łatwo się skaluje.

Maksymalna przepustowością danych w ZigBee wynosi około 250 kb/s na częstotliwości 2,4 GHz. Oznacza to, że ZigBee jest wolniejsze niż inne popularne standardy bezprzewodowe, takie jak Wi-Fi czy Bluetooth, ale nie ma to znaczenia w typowych aplikacjach IoT. ZigBee jest zaprojektowane do przesyłu małych pakietów danych we względnie długich odstępach czasowych, co jest zazwyczaj wystarczające do zbierania danych z czujników temperatury, sensorów bezpieczeństwa, systemów monitorowania jakości powietrza i podobnych podsystemów. W międzyczasie niska przepustowość wpływa na niską moc potrzebną do działania systemu, dzięki czemu węzły ZigBee mogą zazwyczaj pracować przez wiele lat na pojedynczej baterii.

Typowy zasięg transmisji pojedynczego urządzenia ZigBee to od ok. 10 do 15 metrów, gdy na drodze sygnału nie stoją żadne przeszkody. Można je jednak z łatwością ominąć, przekazując dane poprzez inne węzły sieciowe. ZigBee, szczególnie w wersji 3.0, jest także bezpieczne, a to dzięki wykorzystaniu szyfrowania danych, autentykacji i sprawdzania integralności za pomocą 128-bitowego algorytmu AES-CCM oraz dzięki wykorzystaniu innych algorytmów bezpieczeństwa.

Warto też wspomnieć o ZigBee Pro, które może jednocześnie pracować w dwóch pasmach ISM: 800–900 MHz, zgodnie z lokalnymi regulacjami prawnymi oraz 2,4 GHz – na całym świecie. Niższe pasmo ułatwia transmisję sygnału przez przeszkody, w budynkach. ZigBee Pro pozwala producentom przygotowywać urządzenia, które działają w ramach jednej sieci, ale pracującej w różnych pasmach, dzięki czemu lepiej radzą sobie z wyzwaniami, wynikającymi z ich otoczenia.

Z-Wave

Innym, dosyć starym już protokołem, ale zyskującym na popularności dopiero dzięki IoT, jest Z-Wave. Wywodzi się jeszcze z ubiegłego wieku, kiedy to został opracowany przez duńską firmę Zensys na potrzeby sterowania oświetleniem. Obecnie za rozwój protokołu odpowiada organizacja Z-Wave Alliance, przy czym za certyfikację techniczną odpowiada firma Silicon Labs.

W Z-Wave wykorzystywane są częstotliwości około 900 MHz, zależnie od kraju, w którym urządzenie ma pracować. Szybkość transmisji może wynosić do 100 kb/s, a jej zasięg to 40 metrów. Sieć ma topologię kraty, przy czym to źródło sygnału określa, którędy pakiety mają dotrzeć do celu. Rozwój Z-Wave cały czas trwa. W 2017 roku zwiększono poziom bezpieczeństwa protokołu. Szybko rośnie też liczba produktów zgodnych z Z-Wave. O ile dwa lata temu było ich 1700, o tyle obecnie liczba modeli urządzeń Z-Wave przekroczyła już 2600.

6LoWPAN i Thread

Na bazie warstwy MAC protokołu ZigBee powstały też inne rozwiązania, pomyślane do optymalizacji komunikacji urządzeń z Internetem. Jednym z nich jest 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks), który pozwala nadać każdemu urządzeniu adres IP. Sam protokół 6LoWPAN realizuje tylko jedną warstwę komunikacji i można na nim zbudować bardziej kompletne protokoły, czego przykładem jest Thread – standard bardzo podobny do ZigBee.

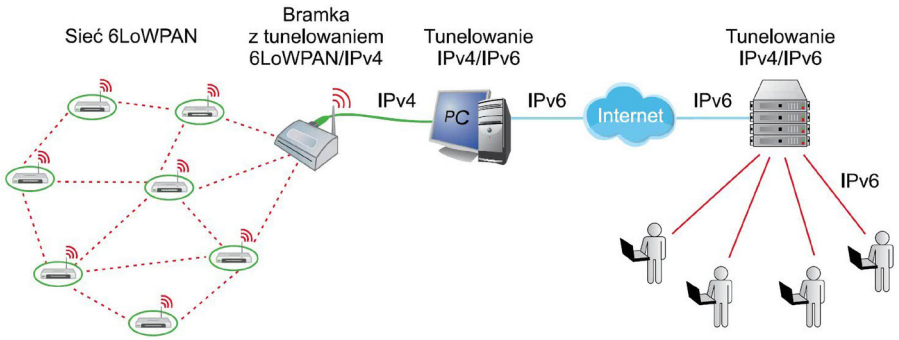
Zarówno Thread, jak i ZigBee pozwalają na tworzenie bezprzewodowych sieci LAN o topologii kraty, bazując na rozwiązaniach typowych dla sieci PAN. Korzystają z takiej samej warstwy MAC (IEEE 802.15.4) na częstotliwości 2,4 GHz, co oznacza, że często ten sam układ radiowy może posłużyć zarówno do ZigBee, jak i do obsługi Thread – wystarczy tylko zmiana oprogramowania. Oba standardy są otwarte i przeznaczone do podobnych zastosowań oraz pobierają podobną ilość energii. Są jednak pomiędzy nimi istotne różnice.

Thread korzysta z bardziej tradycyjnego sposobu adresowania urządzeń niż ZigBee. Wykorzystanie IPv6 w Thread sprawia, że adresem urządzenia można posługiwać się bezpośrednio w chmurze, zamiast tłumaczyć go na jakiś inny, lokalny identyfikator, dostępny pod adresem IP bramki. Ponadto ZigBee określa specyfikę warstwy aplikacji, która mówi o tym, jak aplikacje powinny się ze sobą komunikować. Jeśli naszym celem jest stworzenie urządzenia, które będzie pracować z innym urządzeniem ZigBee, oczywistym staje się sięgnięcie po ZigBee, ale jeśli nie ma takiej potrzeby, więcej możliwości da nam zastosowanie Thread. Nie definiuje on niczego w warstwie aplikacji. Przesyłane pakiety mogą zawierać dowolne informacje, bez z góry określonego formatu. To poniekąd sprawia, że stos programu Thread jest prostszy niż w przypadku ZigBee. Zresztą był to jeden z powodów opracowania tego protokołu. ZigBee ze względu na swoją złożoność działa nieco wolniej, zajmuje więcej pamięci i przez to może wymagać większego mikrokontrolera, który nie tylko zwiększy koszt aplikacji, ale też może podwyższyć pobór mocy.

Pisząc o koszcie, trzeba też wspomnieć o certyfikacji. Aby tworzone urządzenie było oficjalnie zgodne z ZigBee czy Thread, trzeba zdobyć odpowiedni certyfikat. Koszty tej operacji są różne i odpowiadają za nie inne organizacje. W przypadku ZigBee jest to ZigBee Alliance, a w przypadku Thread: Thread Group.

LoRa i LoRaWan

LoRa to protokół warstwy łącza, który świetnie sprawdza się w komunikacji bezprzewodowej P2P pomiędzy niewielkimi urządzeniami. Jest oparty na technologii rozpraszania widma CSS (Chirp Spread Spectrum). Technika ta była przez dekady stosowana w aplikacjach wojskowych i astronautyce. Jej kluczową zaletą jest możliwość uzyskania dużego zasięgu transmisji i odporność na interferencje. Transmisja prowadzona jest w nielicencjonowanych pasmach, na częstotliwości 868 MHz w Europie i 915 MHz w Ameryce Północnej. W praktyce LoRa jest stosowany przede wszystkim w ramach sieci LoRaWAN, której specyfikacja obejmuje też warstwę sieciową, a więc definiuje sposób wymiany informacji pomiędzy wieloma urządzeniami. LoRaWAN jest zoptymalizowany pod kątem minimalizacji poboru energii.



Rysunek 4. Zasada działania sieci 6LoWPAN

LoRaWAN określa się mianem sieci typu LPWAN (Low Power Wide Area Network), opartej na architekturze gwiazdy. Jest to znacząca różnica względem ZigBee i Thread. Podstawowym elementem infrastruktury tej sieci jest brama (gateway). Bezprzewodowo komunikuje się z węzłami końcowymi sieci, czyli np. modułami końcowymi IoT. Z drugiej strony, za pomocą bardziej standardowych protokołów (jak Ethernet, Wi-Fi lub 3G) łączy się z serwerami sieciowymi (chmurami). Dla węzłów końcowych bramki są przezroczyste – przekazują jedynie wiadomość pomiędzy urządzeniami a centralnym serwerem. Komunikacja pomiędzy węzłami a bramkami jest dwukierunkowa, możliwe jest jednak również wysyłanie wiadomości w trybie *multicast*, czyli do wielu odbiorców jednocześnie. Bezpieczeństwo danych gwarantuje szyfrowanie transmisji 128-bitowym kluczem AES128.

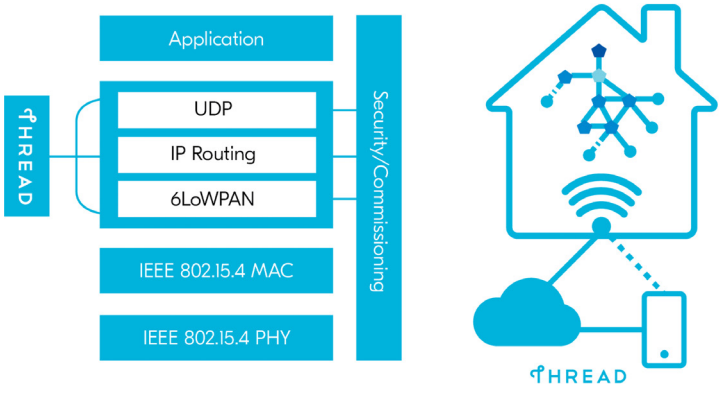
Architektura sieci LoRaWAN przypomina pod wieloma względami telefoniczne sieci komórkowe, które również oparte są na siatce rozmieszczonych na stałe w terenie stacji bazowych. Inaczej niż w przypadku GSM moduły LoRaWAN nie nawiązują jednak połączenia z jedną wybraną stacją bazową. Nadawany przez urządzenie końcowe sygnał trafia do wszystkich stacji w zasięgu transmisji i jest przez nie przetwarzany. Zwiększa to odporność sieci na błędy i awarie spowodowane uszkodzeniem pojedynczego elementu infrastruktury. Eliminację zduplikowanych pakietów wykonuje dopiero serwer sieciowy. Serwer, oprócz filtracji pakietów, zajmuje się również m.in. ustalaniem prędkości transmisji, kontrolą bezpieczeństwa oraz wyborem optymalnych bram do realizacji transmisji „w dół" (down-link).

Wśród głównych zalet LoRaWAN należy wymienić duży zasięg stacji bazowych – od ok. 15 km w terenach niezabudowanych do 2–5 km w terenach silnie zurbanizowanych. Jedna stacja bazowa może ponadto obsługiwać do 20 tysięcy urządzeń końcowych. Prędkość transmisji danych w sieci może być regulowana w zakresie od 0,3 kb/s do 50 kb/s, w zależności od dostępności medium komunikacyjnego.

LoRaWAN 1.1

W 2017 roku opublikowano specyfikację techniczną protokołu LoRaWAN 1.1, która zwiększyła atrakcyjność tego protokołu. Wprowadzono trzy duże zmiany: wsparcie dla przełączania połączeń pomiędzy sieciami (tzw. handover roaming), możliwość geolokalizacji modułów oraz nową klasę węzłów końcowych (klasa B).

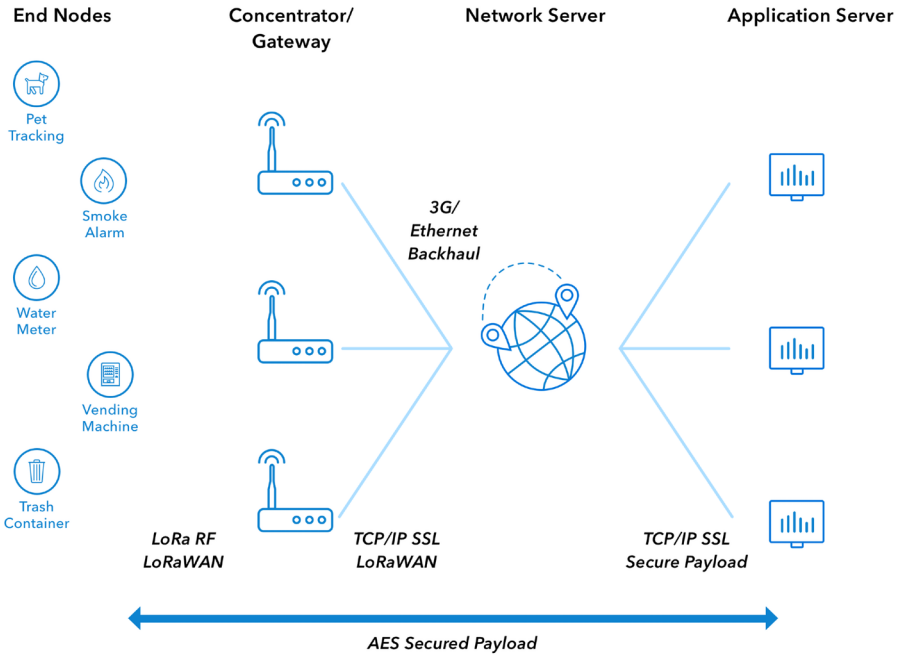
Nowy aktywny roaming jest alternatywą dla dotychczas używanego roaming pasywnego. Węzły końcowe sieci są bowiem przypisane do konkretnej sieci macierzystej. Jeśli znajdą się poza zasięgiem tej sieci, będąc jednocześnie w zasięgu innej sieci LoRaWAN, chcąc nawiązać połączenie, będą musiały użyć infrastruktury tej nowej sieci, czyli skorzystać z roamingu. Dotychczasowa specyfikacja LoRaWAN umożliwiała jedynie utrzymywanie sytuacji, w której kontrolę nad urządzeniem końcowym wciąż sprawował serwer sieci macierzystej i to do niego musiała być przekierowywana komunikacja z urządzeniem. Od wersji 1.1



Rysunek 5. Protokół Thread w modelu OSI

możliwe jest przekazanie zarządzania urządzeniem końcowym w całości do obcej sieci. Rolę serwera sieci macierzystej przejmuje serwer sieci obcej, co znacznie przyspiesza i upraszcza proces komunikacji – nie ma już konieczności ciągłej wymiany pakietów pomiędzy dwoma serwerami.

Wprowadzenie funkcji geolokalizacji było dosyć oczywistym krokiem, gdyż po prostu wykorzystano fakt, że w sieci LoRaWAN sygnał nadawany przez węzeł końcowy odbierany i przetwarzany jest przez wszystkie stacje bazowe w zasięgu. Do nadawanej przez moduły ramki dodano znacznik czasowy, na podstawie którego stacje bazowe, podobnie jak np. odbiorniki systemów nawigacji satelitarnej, mogą obliczyć różnicę pomiędzy czasem nadania a czasem odbioru ramki. Na tej podstawie, korzystając z odczytów z czterech stacji bazowych (mających zsynchronizowane zegary), serwer może precyzyjnie określić położenie modułu. Dzięki temu użycie sieci LoRaWAN pozwala poniekąd zrezygnować z odbiornika GNSS, o ile wymogi co do precyzji i dostępności lokalizacji są nieduże.



Rysunek 6. Architektura sieci LoRaWAN

Klasy i rodzaje urządzeń LoRaWAN

Warto też wspomnieć o podziale urządzeń LoRaWAN na klasy. Węzły sieci mogą należeć do jednej z trzech klas, w zależności od ich zastosowania. Klasy decydują o czasie nasłuchiwania, kiedy to urządzenie jest w stanie odebrać komunikat od stacji bazowej. Wydłużenie czasu nasłuchiwania transmisji zmniejsza opóźnienie, z jakim można skontaktować się z modułem, ale zwiększa zapotrzebowanie na energię elektryczną, przez co skraca czas pracy podczas korzystania z zasilania bateryjnego. Natomiast komunikacja w górę (od węzłów do stacji bazowej) inicjowana jest w każdym przypadku (niezależnie od klasy węzła) przez urządzenia końcowe, w zależności od ich potrzeb.

Klasa A obejmuje urządzenia najbardziej energooszczędne, tj. o najniższej dostępności. Nasłuchują one sygnałów jedynie bezpośrednio po zakończeniu własnej transmisji. Klasę tę stosuje się przede wszystkim do różnego rodzaju czujników.

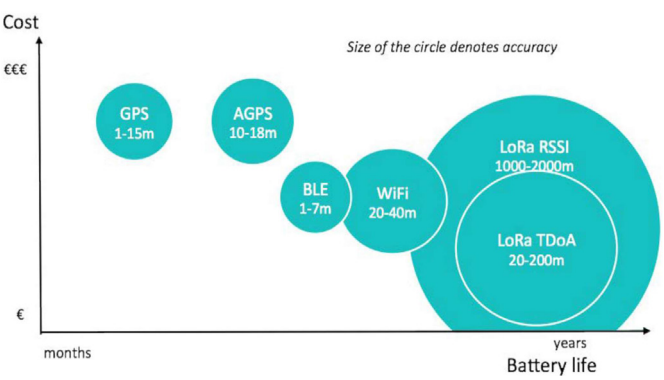
Klasa B została wprowadzona w protokole LoRaWAN 1.1. Urządzenia tej klasy, tak jak w przypadku klasy A, są zdolne do odbioru bezpośrednio po zakończeniu własnej transmisji, ale dodatkowo otwierają również okna odbiorcze w zaplanowanym wcześniej czasie. Aby stacja bazowa mogła skomunikować się z modułem podczas tego dodatkowego okna, konieczna jest synchronizacja czasowa pomiędzy urządzeniami.

Natomiast urządzenia **klasy C** są zdolne do odbioru sygnału prawie przez cały czas, z wyjątkiem momentów, w których same transmitują. Wiąże się to z najwyższym poborem energii elektrycznej, ale pozwala na natychmiastową dwustronną komunikację, bez żadnych dodatkowych opóźnień.

Oprócz urządzeń końcowych wyróżnia się też **bramki**, **serwery sieciowe** i **serwery aplikacyjne**. Bramki nazywane są też **modemami** i **punktami dostępu**, gdyż odbierają dane nadawane przez węzły końcowe za pomocą LoRaWAN. Wiadomości te są często konwertowane na pakiety, które można przesyłać za pomocą tradycyjnych sieci IP. Bramka jest więc podłączona do serwera sieciowego, do którego przesyła wszystkie wiadomości. Bramki są z założenia przezroczyste i mają ograniczoną moc obliczeniową. Wszystkie złożone operacje i inteligentne algorytmy są realizowane na serwerze sieciowym. To w nim następują bardziej skomplikowane procesy, związane z przetwarzaniem danych. Jest on odpowiedzialny za przekierowywanie i przekazywanie danych do odpowiednich aplikacji. Określa która z bramek jest najlepsza do skierowania wiadomości przesyłanej do wybranego węzła i usuwa zduplikowane wiadomości, jeśli zdarzyło się, że dane z węzła zostały przekazane do serwera przez więcej niż jedną bramkę. Co ważne, deszyfruje też wiadomości przesyłane z węzłów końcowych i szyfruje informacje przesyłane do węzłów. Bramki zazwyczaj łączą się z serwerem sieciowym za pomocą szyfrowanego połączenia IP (Internet Protocol). Sieć najczęściej zawiera interfejs do nadzorowania pracy i instalacji nowych bramek, pozwalając kontrolerowi sieci na zarządzanie nimi, rozwiązywanie problemów, wykrywanie usterek, monitorowanie pojawiających się alarmów itp.

Istniejące sieci LoRaWAN

Fakt istnienia stacji bazowych sprawia, że LoRaWAN może kojarzyć się z sieciami komórkowymi. I faktycznie – powstały już usługi, w ramach których użytkownicy mogą korzystać z gotowej infrastruktury, zamiast organizować ją sobie samodzielnie. Chyba najbardziej znaną siecią tego typu jest The Things Network. Jest ona tworzona przez społeczność – projektantów, którzy sami decydują się dołączyć tworzone przez siebie instalacje do tej globalnej sieci. Aktualnie, w chwili tworzenia tego artykułu, a więc na początku maja 2019 roku, The Things Network jest wspierane przez 70542 osoby ze 137 państw świata, do których łącznie należy 7188 bramek. Dokładną mapę ich lokalizacji można zobaczyć pod adresem: ***https://www.thethingsnetwork.org/***. Alternatywną siecią jest utrzymywana, wciąż niewielka sieć firmy Netemera. Obecnie pokrywa ona



Rysunek 7. Dokładność pozycjonowania względem czasu pracy na baterii z użyciem różnych technik geolokalizacji

Rysunek 8. Mapa stacji sieci The Things Network

podobno jedynie obszar Warszawy i okolic, ale firma planuje zbudować infrastrukturę także w 17 innych dużych miastach. Natomiast organizacja LoRa Alliance ogłosiła w marcu tego roku, że na świecie działa już ponad 100 komercyjnych sieci LoRaWAN.

Sigfox

Jeśli The Things Network wydaje się atrakcyjnym rozwiązaniem do tworzonej aplikacji, ale nie pokrywa obszaru, w którym projektowane urządzenia mają pracować, a budowa własnych stacji bazowych nie wchodzi w grę, warto zainteresować się siecią Sigfox. Jest to zarazem nazwa standardu, jak i francuskiej firmy, która taką sieć zaprojektowała i wdrożyła, a teraz świadczy za jej pomocą płatne usługi. 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) w nielicencjonowanym pasmie 868 MHz. Intencją twórców było wykorzystanie pasma o jak największej 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.

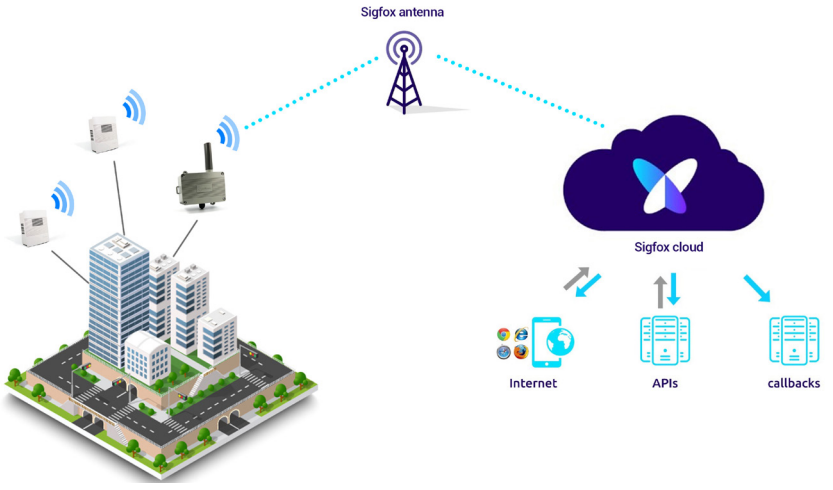
Sigfox – parametry

Podstawową różnicą pomiędzy siecią Sigfox a rozwiązaniami oferowanymi przez operatorów telekomunikacyjnych jest to, że od zawsze była ona opracowana z myślą o małych pakietach danych, podczas gdy inne sieci z definicji są nastawione na transmisję dużych ilości danych przy jak najlepszym wykorzystaniu zasobów. Stacje bazowe Sigfox mogą obsłużyć komunikaty o długości 12 bajtów, ale 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 zapisanie liczby całkowitej z zakresu od 0 do 4096. Jeśli uznamy, że pojedyncza liczba to kod sterujący lub wynik pomiaru, to takie ograniczenie nie będzie stanowić problemu. Ramka Sigfoxa razem z danymi potrzebnymi do kontroli transmisji ma nie więcej niż 26 bajtów. Dla porównania protokół IP ma 40-bajtowy nagłówek – nawet gdy przesyłane jest tylko 12 bajtów właściwych danych. Prowadzi to do mniejszego zużycia energii i wydłużenia czasu pracy na baterii. Firma deklaruje, że użytkowane w ten sposób moduły transmisyjne mogą pracować do 20 lat przy zasilaniu z dwóch baterii – paluszków AA.

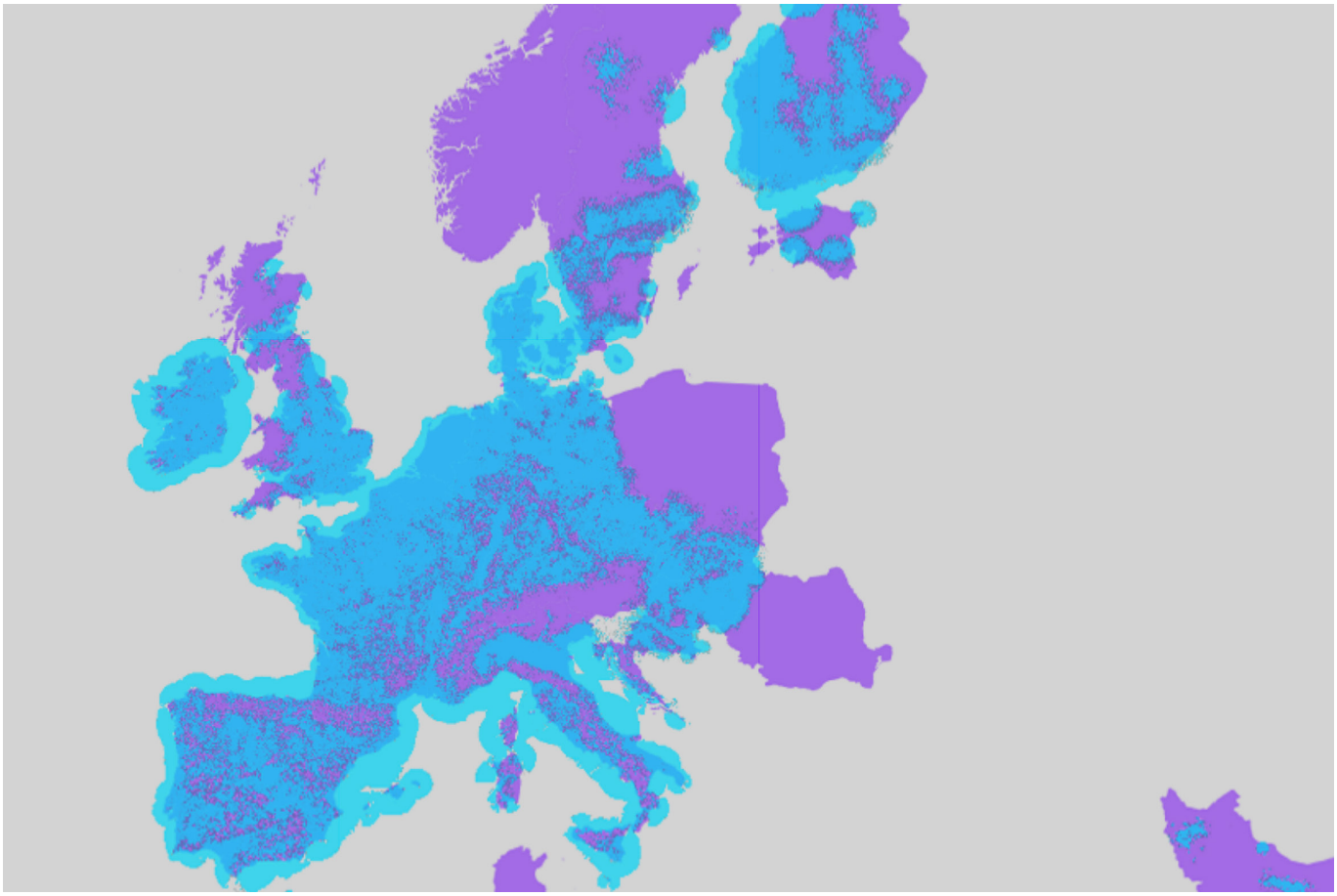
Zasięg Sigfoxa

Ekspansja sieci Sigfox rozpoczęła się od Francji. Aktualnie firma operuje w ponad 60 krajach na całym świecie, przy czym najwięcej stacji jest zlokalizowanych w Europie Zachodniej. W niektórych krajach działa nie bezpośrednio, a poprzez firmy trzecie, pełniące funkcję oficjalnych operatorów/pośredników. W Polsce Sigfox prowadził programy pilotażowe już około 2 lat temu, ale wciąż nie mamy działającego operatora. Wynika to zapewne z szybkiego rozwoju technologii komórkowych LTE dla małych urządzeń. Osoby, które chciałyby wdrożyć rozwiązanie oparte na sieci Sigfox w Polsce, mogą skorzystać z mikrostacji bazowych (Micro Base Station), jakie zaprezentowano pod koniec ubiegłego roku. Aktualną mapę zasięgu można zobaczyć pod adresem: ***www.sigfox.com/en/coverage***.

Model biznesowy przyjęty przez firmę Sigfox zakłada, że przedsiębiorstwo będzie operatorem sieci i jej serwerów. Urządzenia



Rysunek 9. Zasada działania sieci Sigfox



Rysunek 10. Mapa sieci Sigfox w Europie

użytkowane w sieci muszą być certyfikowane, a sam certyfikat można uzyskać łatwiej, jeśli skorzysta się z precertyfikowanych modułów. Wytwarza je kilku producentów. Przyjęta strategia ma spowodować, że ceny urządzeń współpracujących z siecią będą niewysokie, co przyciągnie użytkowników. Sama firma Sigfox zarabia jako operator sieci i serwerów, pobierając niewielką opłatę abonamentową od użytkowników sieci, co jednak przemnożone przez liczbę urządzeń ma dać odpowiedni wynik finansowy. Innymi słowy, Sigfox nie zajmuje się sprzętem sieciowym i nie chce na nim zarabiać, ale skupić się jedynie na swojej roli jako twórcy standardu i operatora sieci. Na skutek przyjęcia takiego modelu działania, każdy użytkownik chcący użyć sieci Sigfox w swojej aplikacji, musi pracować bezpośrednio z firmą Sigfox lub jej oficjalnym przedstawicielem – nie ma innej opcji. To istotna różnica względem technologii LoRa i sieci LoRaWAN.

Należy dodać, że usługi sieci Sigfox realizowane są w chmurze. Aby odebrać wiadomości, ale też by zarządzać obiektami w sieci, klienci i partnerzy Sigfoxa korzystają z chmury. Dostęp do danych, billingi, zarządzanie urządzeniami i użytkownikami, mapy oraz inne funkcje są dostępne w chmurze Sigfoxa za pomocą trzech interfejsów – portalu WWW, API umożliwiającego zautomatyzowany dostęp do wszelkich usług portalu za pomocą skryptów oraz funkcji zwrotnych, które pozwalają na automatyczne otrzymywanie informacji o nowych zdarzeniach w trybie PUSH.

Bezpośrednia konkurencja sieci Sigfox

Sigfox ma (lub raczej miał) bezpośrednią konkurencję. Jedną z firm, która starała się działać na podobnej zasadzie, była firma Neul, w której kluczową rolę odgrywał Huawei. Formalnie firma nadal istnieje, ale wszystko wskazuje na to, że zrezygnowała ze swoich działań na rzecz transmisji komórkowej 4G i 5G.

Inną firmą, która przedstawia się jako bezpośrednia konkurencja Sigfoxa, jest Link Labs. W Polsce jeszcze nie zyskała popularności, ale można już kupić moduły zaprojektowane specjalnie pod kątem tej sieci – rozwiązania określanego mianem Symphony Link. Jest ono reklamowane jako bardziej niezawodne niż Sigfox ze względu na 100-procentowe potwierdzenia wszystkich transmitowanych pakietów. Oczywiście jest to także tańsze i bardziej energooszczędne rozwiązanie niż korzystanie z sieci komórkowych, a komunikacja odbywa się na częstotliwościach 868 MHz lub 915 MHz.

Wi-Fi

Wszystkie opisane dotąd standardy koncentrowały się na niewielkim zużyciu energii, kosztem silnie ograniczonej przepustowości. Jeśli dostęp do prądu elektrycznego nie jest problemem albo aplikacja wymaga szybszych transferów, warto sięgnąć po Wi-Fi. Jest kilka generacji tego standardu, które równolegle funkcjonują na rynku. Najtańsze będą moduły zgodne ze standardem IEEE 802.11n i starszymi jego odmianami. Specyfikacja IEEE 802.11n została opublikowana w 2009 roku, ale wprowadzała na tyle wiele nowości i udało się ją całkiem dobrze dopracować, w związku z czym odniosła bardzo duży sukces. W efekcie, pomimo że ma już 10 lat, nadal cieszy się popularnością.

IEEE 802.11n występuje w kilku wersjach, w różnym stopniu korzystających z techniki MIMO. Zwielokrotnienie strumieni transmisji pozwala podnieść maksymalną, teoretyczną przepustowość ze 150 Mb/s przez 300 Mb/s, 450 Mb/s aż do 600 Mb/s. Oznacza to, że w zależności od konfiguracji anten, moduł zgodny z IEEE 802.11n będzie miał różną szybkość transmisji.

Oczywiście w praktyce takie przepustowości nie są realne, ale w dobrych warunkach można uzyskać transfery na poziomie nawet 100 Mb/s, czyli porównywalnym z tym, co w najbardziej popularnym Ethernecie przewodowym. Specyfikacja Wi-Fi n obejmuje też transmisję nie tylko w paśmie 2,4 GHz, ale i na częstotliwości 5 GHz.

IEEE 802.11ac i 802.11ax

Coraz większą popularnością cieszy się standard IEEE 802.11ac, który poprzez zastosowanie nawet 160-megahercowych kanałów i 8-krotnego MIMO teoretycznie pozwala na transfery do niemal 3,5 Gb/s, ale nie są to realne wartości do uzyskania w warunkach rzeczywistych. Kolejną generacją standardu jest wersja IEEE 802.11ax, określana też mianem Wi-Fi 6, o teoretycznej przepustowości przekraczającej 10 Gb/s, ale formalnie specyfikacja tego standardu nie została jeszcze zatwierdzona. Nie przeszkadza to jednak niektórym producentom układów na wprowadzanie na rynek nowych urządzeń, wstępnie zgodnych z IEEE 802.11ax. Podobnie zresztą było z Wi-Fi n i Wi-Fi ac, gdyż podstawowa charakterystyka standardu zazwyczaj nie zmienia się na długo przed jego ostatecznym zatwierdzeniem.

IEEE 802.11ah i 802.11af

Rozwój rynku IoT, którego potrzeby są inne niż w przypadku domowych sieci komputerowych, sprawił, że także i w ramach rodziny protokołów Wi-Fi pojawiły się energooszczędne warianty o małej przepustowości. Choć opisano je już jakiś czas temu, nadal mówi się o nich jako o przyszłości Wi-Fi. Sprowadzają się one do dwóch standardów:

- IEEE 802.11ah, nazywanego też HaLow i przeznaczonego do transmisji na duże odległości,
- IEEE 802.11af, nazywanego też White-Fi, przystosowanego do tych samych celów co HaLow, ale pracującego na niewykorzystywanych pasmach telewizyjnych.

Aby zwiększyć relatywnie krótki zasięg popularnych sieci Wi-Fi, HaLow pracuje na częstotliwości 900 MHz. Urządzenia działające w tym standardzie wybudzają się zgodnie z określonym harmonogramem, kiedy to mogą odbierać informacje.

Natomiast sieci 802.11af pracują na różnych częstotliwościach z zakresu od 54 MHz do 790 MHz. Tak nietypowy zakres sprawia, że trudno o międzynarodowe wykorzystanie tego standardu. Zajętość tych pasm będzie różna nie tylko w zależności od kraju, ale i regionu. W wielu krajach potrzeba licencji, by móc w nich transmitować takie fale radiowe.

ANT i ANT+

Zapotrzebowanie na energooszczędną komunikację radiową oraz możliwość (lub konieczność) pobierania (lub ponoszenia) opłat licencyjnych sprawiły, że na rynku pojawiło się wiele innych, mało popularnych standardów transmisji bezprzewodowej. Poszczególne z nich wywodzą się z różnych środowisk.

Przykładowo, na rynku konsumenckich opasek sportowych można się spotkać z protokołem ANT, opracowanym przez firmę ANT Wireless, należącą do koncernu Garmin. Komunikacja ANT odbywa się w paśmie 2,4 GHz i przypomina Bluetooth LE. Sieć może być zorganizowana w topologie punkt-punkt, gwiazdę, drzewo lub kratę. Odległość bezpośredniej transmisji sięga 30 metrów, a dopuszczalna przepustowość to 60 kb/s. Dostępna jest rozszerzona wersja ANT+, która jednak nie wiąże się z większą wydajnością, tylko obejmuje zmiany w warstwie aplikacji, by różne urządzenia mogły wspólnie przetwarzać dane z innych sensorów ANT+.

Obecnie urządzenia z interfejsem ANT produkuje ponad 170 firm.

MiWi

Osoby korzystające z modułów firmy Microchip mogą natomiast sięgnąć po protokół MiWi, który został opracowany, by ułatwić tworzenie niedrogich, komercyjnych i domowych sieci radiowych. Jest przeznaczony do zapewnienia komunikacji pomiędzy systemami HVAC i alarmami. W warstwie fizycznej przypomina ZigBee (bazuje na IEEE 802.15.4), ale może pracować na częstotliwościach 2,4 GHz i w paśmie ISM poniżej 1 GHz.

Stos protokołu MiWi jest jednak znacznie mniejszy niż w przypadku standardowych implementacji ZigBee i to pomimo wsparcia dla topologii kraty. W typowych przypadkach wystarczy jedynie 20 kB pamięci na kod programu.

DigiMesh

Na podobnej zasadzie jak MiWi działa i oferowany jest standard DigiMesh. Stanowi alternatywę dla ZigBee i jest dostępny w modułach firmy Digi. Od ZigBee różni się m.in. jednym rodzajem węzłów – wszystkie są sobie równorzędne i pracują w topologii kraty. Wyróżnikiem DigiMesh jest zastosowanie opcjonalne synchronizowanych cykli uśpienia, dzięki czemu urządzenia wybudzają się w tym samym czasie i nie muszą na siebie czekać, a więc dłużej pozostają w trybie pracy o bardzo niskim poborze energii.

EnOcean

Interesującą, ale mało popularną technologią jest EnOcean. Została ona przyjęta jako standard ISO 14543-3-10, jako metoda przesyłu danych na krótkie dystanse, zoptymalizowana pod kątem urządzeń pobierających energię z otoczenia. EnOcean została opracowana przez niemiecką firmę o tej samej nazwie. Dane przesyłane są na częstotliwościach 902 MHz, 928,35 MHz, 868,3 MHz i 315 MHz, w postaci pakietów o rozmiarze 14 bajtów, z szybkością 125 kb/s. W praktyce energia na potrzeby wyemitowania fal radiowych zużywana jest jedynie podczas przesyłu jedynek bitowych.

DASH7

Ostatnim ze standardów opisywanych w niniejszym artykule jest DASH7 Alliance Protocol (D7A), rozwijany przez organizację DASH7 Alliance i bazujący na ISO 18000-7. Jest to otwarty standard dla sieci czujnikowych, pracujący na częstotliwościach 433 MHz, 868 MHz i 915 MHz, a więc w paśmie nielicencjonowanym. Zasięg transmisji wynosi do 5 km, a główną zaletą tej technologii są krótkie opóźnienia, pomimo bardzo małego poboru energii. Z tego względu standard jest polecany do używania w urządzeniach poruszających się. Cechuje się otwartym, bardzo lekkim stosem protokołu, szyfrowaniem AES ze 128-bitowym kluczem oraz szybkością transmisji do 167 kb/s. Maksymalny rozmiar pakietów to 256 bajtów. Urządzenia mogą tworzyć sieci o topologii P2P, gwiazdy lub drzewa. Standard jest cały czas rozwijany – dwa i pół roku temu opublikowano wersję 1.1, w której zwiększono bezpieczeństwo komunikacji.

Podsumowanie

Liczba protokołów opisanych w artykule pokazuje, jak wiele oczekiwano od Internetu Rzeczy, gdyż bardzo dużo z tych standardów zostało opracowanych właśnie pod kątem IoT. Co więcej, nie są to wszystkie, jakie powstały – na przestrzeni lat pojawiły się jeszcze inne rozwiązania, takie jak Ingenu/Onramp, Weightless, WirelessHart, Insteon i Wi-Fi IEEE 802.11ad, które nie zyskały rozgłosu lub zupełnie straciły na znaczeniu. Warto też mieć na uwadze, że czasem najtańszym rozwiązaniem jest skorzystanie z autorskiego systemu komunikacji, w którym dysponujemy jedynie łączem radiowym, a zasady transmisji określamy samodzielnie. Na rynku są niedrogie moduły, które pozwalają na realizowanie także takich projektów.

Marcin Karbowniczek, EP