Sieci bezprzewodowe

W technikach łączności bezprzewodowej podstawową grupę stanowią systemy skoncentrowane na komunikacji nadajnik-odbiornik. Jednak najnowsze rozwiązania są optymalizowane, a czasami wręcz przeznaczone, do pracy w strukturze sieci bezprzewodowej.

W standardach połączeń bezprzewodowych Wi-Fi zajmuje szczególne miejsce. Rozwiązania sprzętowo-programowe Wi-Fi zapewniają podłączenie urządzeń do lokalnej sieci LAN i możliwość dostępu do Internetu. Każde urządzenie mobilne: smartfony, laptopy, tablety, od dawna jest wyposażane w ten standard. Dla smartfonów jest to jeden z dwu głównych kanałów dostępu do Internetu.

Dla konstruktorów urządzeń profesjonalnych duże znaczenie może mieć łatwość budowania i konfiguracji bezprzewodowych sieci lokalnych LAN. Duża popularność interfejsu powoduje, że bez trudu znajdziemy na rynku gotowe moduły z kompletną częścią radiową i wbudowaną anteną paskową lub złączem antenowym do podłączenia dopasowanej falowo anteny. W warstwie programowej wiele niezbędnych rozwiązań w tym biblioteki protokołów TCP/IP, jest dostępnych bezpłatnie.

Wi-Fi opiera się na modelu warstwowym i definiuje dolne warstwy: warstwę łącza danych, z podwarstwami LLC i MAC, oraz warstwę fizyczną warstwowego modelu OSI.

Amerykański Instytut Inżynierów Elektryków i Elektroników (Institute of Electrical and Electronics Engineers) opracował standard IEEE 802.11 przeznaczony do transferu danych w sieciach bezprzewodowych WLAN. Najbardziej znane są cztery wersje tego standardu: 802.11a, 802.11b, 802.11g i 802.11h (**tabela 1)**.

Najpopularniejsza z nich jest 802.11b umożliwiająca wymianę danych z teoretyczną prędkością 11 Mb/s. Wbudowany mechanizm *dynamic rate shirting* pozwala na dynamiczną zmianę szybkości transmisji w zależności od stanu kanału transmisyjnego. Wraz ze wzrostem dystansu pomiędzy nadajnikiem i odbiornikiem (spadek poziomu sygnału) lub ze wzrostem zakłóceń prędkość przesyłania danych jest zmniejszana do 5,5, 2 lub 1 Mb/s.

Równolegle rozwijany standard 802.11a, mimo że zapewnia prawie 5-krotny wzrost prędkości transferu, nie zdobył popularności w Europie. Po pierwsze pracuje w paśmie 5 GHz (UNII). W Unii Europejskiej to pasmo jest zarezerwowane do celów wojskowych i nie można go stosować do sieci bezprzewodowych bez ograniczeń. W Polsce może być używane tylko wewnątrz budynków. Po drugie nie jest w żaden sposób kompatybilny z 802.11b.

W 2003 roku został zatwierdzony standard 802.11g mający w założeniu łączyć zalety 802.11a i 802.11b: dużą prędkość transmisji przy odporności na zakłócenia oraz większy zasięg i pracę w paśmie 2,4 GHz. Znacząca różnica w prędkości wymusiła inne metody modulacji. 802.11b pracuje z modulacją CCK (*Complementary Code Keying*), a 802.11g z modulacją OFDM (*Orthogonal Frequency Division Multiplexing*). Oczywiście trudno oczekiwać w takiej sytuacji kompatybilności i trzeba stosować karty dwusystemowe. W dwusystemowych

Tabela 1. Najbardziej popularne standardy Wi-Fi

Standard	Prędkość transferu	Pasmo
802.11a	54 Mb/s	5 GHz
802.11b	11 Mb/s	2,4 GHz
802.11g	54 Mb/s	2,4 GHz
802.11h	54 Mb/s	5 GHz

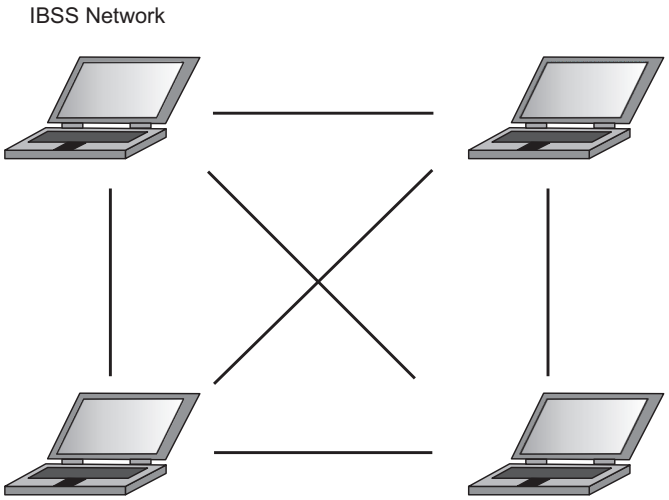
modułach Wi-Fi stosowany jest mechanizm protekcji wykrywający i przełączający moduł na dany typ modulacji.

Pasmo 2,4 GHz przydzielone do standardu 802.11b jest podzielone na 14 kanałów każdy o szerokości 22 MHz (**tabela 2**). Widać, że częstotliwości sąsiednich kanałów zachodzą na siebie nawzajem. Modulacja CCK pozwala na odseparowanie zakłóceń od nadajników pracujących na częściowo pokrywających się częstotliwościach. W praktyce dąży się do tego, aby stacje położone blisko siebie pracowały na tak odległych od siebie częstotliwościach, jak to tylko możliwe.

Topologia sieci Wi-Fi

Sieci Wi-Fi mogą pracować w dwu trybach: *Ad Hoc* lub *Infrastructure*.

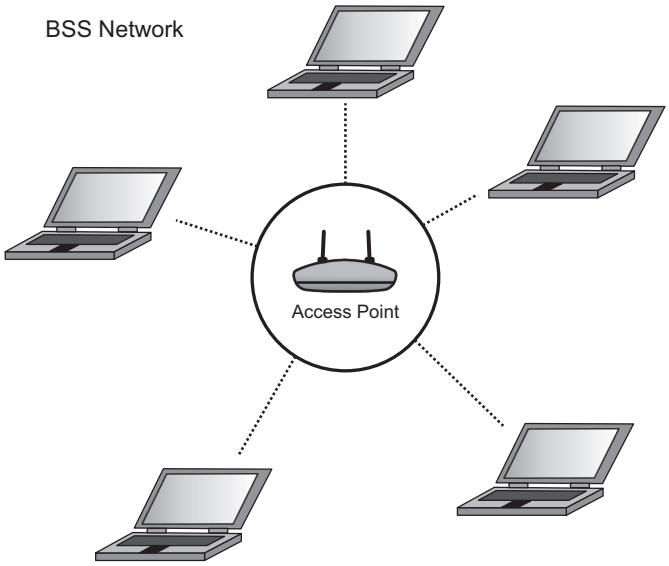
Tryb *Ad Hoc* odpowiada klasycznej sieci peer-to-peer i pozwala na tworzenie sieci radiowej wykorzystującej tylko komputery (urządzenia) wyposażone w interfejsy Wi-Fi. Taka topologia nazywana jest IBSS (*Independent Basic Service Set*). Każdy komputer może się komunikować bezpośrednio ze wszystkimi w sieci (**rysunek 1**).



Rysunek 1. Sieć IBSS (tryb Ad Hoc)

Tabela 2. Kanały standardu 802.11b

Kanał	Dolna częstotliwość kanału [GHz]	Środkowa częstotliwość kanału [GHz]	Górna częstotliwość kanału [GHz]
1	2,401	2,412	2,423
2	2,406	2,417	2,428
3	2,411	2,422	2,433
4	2,416	2,427	2,438
5	2,421	2,432	2,443
6	2,426	2,437	2,448
7	2,431	2,442	2,453
8	2,436	2,447	2,458
9	2,441	2,452	2,463
10	2,446	2,457	2,468
11	2,451	2,462	2,473
12	2,456	2,467	2,478
13	2,461	2,472	2,483
14	2,473	2,484	2,495



Rysunek 2. Sieć BBS (tryb *Infrastructure*)

Główną zaletą takiej sieci jest szybka i tania instalacja. Oprócz komputerów z kartami sieciowymi nic innego nie jest potrzebne. Ponieważ wszystkie komputery mogą się komunikować ze sobą, można w prosty sposób zwiększać zasięg sieci, bo część z nich może spełniać funkcję „stacji przekaźnikowych". Wadą takiej sieci jest mała liczba pracujących komputerów (max 8). Wyłączenie jednego z komputerów spełniających funkcję przekaźnika może spowodować utratę połączenia pomiędzy innymi komputerami w sieci.

Tryb *Infrastructure* wymaga przynajmniej jednego wydzielonego punktu dostępowego Access Point. Każdy komputer w sieci komunikuje się z punktem dostępowym i przez niego przechodzi cała transmisja danych. Komputery nie mogą się komunikować bezpośrednio jak to jest możliwe w sieci *Ad Hoc*. Wykorzystując tryb *Infrastructure* z przynajmniej jednym punktem dostępowym, tworzy się topologię sieci nazywaną BSS (*Basic Service Set*) (**rysunek 2**). Punktem dostępowym może być router z modemem ADSL i z funkcją Wi-Fi. Urządzenia tego typu są stosowane w domowych sieciach z dostępem do szerokopasmowego Internetu, dzielonym przez wszystkie urządzenia w sieci. Takie routery można też stosować do budowy lokalnej sieć LAN z połączeniami Wi-Fi i Ethernet bez dostępu do Internetu.

Zabezpieczenia sieci Wi-Fi

Każde połączenie radiowe jest podatne na ataki hakerskie. Bez silnych zabezpieczeń przed nieuprawnionym dostępem do połączenia trudno mówić o budowie sieci lokalnej nadającej się do czegokolwiek, a do poważnych zadań w szczególności. Standard IEEE 802.11 ma wbudowany szyfrowany mechanizm zabezpieczenia przed nieautoryzowanym podsłuchem i dostępem, nazwany WEP (*Wireless Equivalent Privacy*). Algorytm szyfrowania opiera się na kluczu o stałej długości 40, 64, 128, 152 i 256 bitów. Długość klucza jest wybierana przez użytkownika, a sam klucz jest generowany na podstawie podanego hasła. Co ważne, klucz nigdy nie jest przesyłany drogą radiową, ale zawsze tworzony lokalnie w każdym urządzeniu należącym do sieci, w tym również w punkcie dostępu. Ma to znacznie utrudnić podsłuchanie przesyłanych zaszyfrowanych danych.

W praktyce WEP okazał się bardzo słabym zabezpieczeniem. Klucz nie jest zmieniany w całym czasie posługiwania się hasłem i na dodatek łatwo go złamać dostępnym w Internecie oprogramowaniem. Sieci zabezpieczone WEP nie są uważane za bezpieczne.

Znacznie lepszym zabezpieczeniem jest inny standard – WPA (*Wi-Fi Protected Access*). W trakcie przesyłania danych klucze szyfrujące są dynamicznie zmieniane, dzięki czemu znacznie trudniej jest podsłuchać przesyłanie danych i włamać się do sieci. Autoryzacja w szyfrowaniu WPA może przebiegać na dwa sposoby. Pierwszy sposób

polega łączeniu z serwerem autoryzacji (np. *Radius – Remote Authentication Dial In User Service*). Drugi sposób wykorzystuje hasło użytkownika podobnie jak w WEP. Na jego podstawie tworzony jest klucz PSK (*Pre Shared Key*). WPA jest obsługiwany przez wszystkie obecnie używane Acces Point'y, a siec tak zabezpieczona jest uważana (na razie) za bezpieczną.

Kolejnym sposobem mającym za zadanie utrudnić Życie hakerom jest blokowanie rozgłaszania SSID (*Service Set Identifier*). SSID jest nazwą sieci, a wyłączenie jej rozgłaszania powoduje, że trudniej jest ją wykryć, bo nazwa nie pojawi się na liście dostępnych sieci.

Problem bezpieczeństwa powoduje, że szuka się innych metod zabezpieczania przed włamaniem. Z bardziej prostych znane jest filtrowanie adresów MAC kart sieciowych. Zabezpieczenie to kłopotliwe i również mało skuteczne, bo dzisiaj stosunkowo łatwo można zmienić programowo adresy MAC. Dużo lepiej wyglądają zabezpieczenia definiowane w normie IEEE 802.11i. Wykorzystywany jest tam algorytm silnego szyfrowania AES (*Advanced Encryption Standard*) z kluczami o długości 128, 192 lub 256 bitów, oraz uwierzytelnienie EAP i protokół dynamicznej zmiany klucza TKIP (*Temporal Key Integrity Protocol*). Niestety ta norma nie jest kompatybilna z IEEE 802.11b.

Moduły Wi-Fi

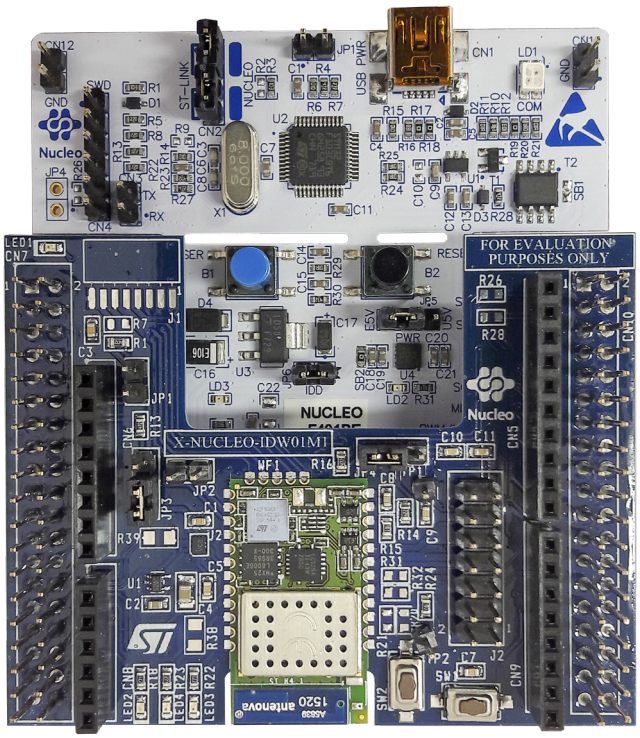
Jednym z przykładów modułu Wi-Fi jest SPWF01SA produkowany przez firmę ST. Najważniejsze właściwości SPWF01SA to:

- transceiver pracujący w paśmie 2,4 GHz zgodnie z IEEE 802.11 b/g/n,
- moduł radiowy spełnia wszystkie europejskie normy i dyrektywy w zakresie kompatybilności elektromagnetycznej,
- zintegrowana antena w wersji SPWF01SA.xy lub zintegrowane złącze antenowe w wersji SPWF01SC.xy,
- moc TX 18,3 DSSS DSM 1 dBm, 13,7 dBm przy 54 Mb/s OFDM,
- czułość RX –66 dBm przy 1 Mbps OFDM, –74,5 dBm przy 54 Mb/S OFDM,
- interfejs UART (Host),
- wbudowany mikrokontroler STM32 Cortex-M3 64 kB RAM i 512 kB Flash,
- zintegrowany stos TCP/IP: 8 jednoczesnych klientów TCP lub UDP i 1 socket server,
- 1 socket klient TLS/SSL wspierający protokół TLS1.2 z algorytmami szyfrowania AES, hash i algorytmy klucza publicznego (RSA, ECC),
- serwer internetowy obsługujący dynamicznie strony internetowe,
- szyfrowanie transmisji WEP/WPA/WPA2,
- możliwość aktualizacji firmware za pośrednictwem UART.

Obwody modułu z ekranowaną częścią radiową zostały umieszczone na płytce drukowanej z wyprowadzeniami przeznaczonymi do montażu powierzchniowego na płycie bazowej. To rozwiązanie dobrze się sprawdza w nowo projektowanych urządzeniach. Jednak, żeby można było przeprowadzić testy, chociażby w celu potwierdzenia przydatności w nowym projekcie, przygotowano moduł ewaluacyjny X-NUCLEO-IDW01M1 kompatybilny sprzętowo z modułami mikrokontrolerów serii STM32Nucleo.

Moduły ewaluacyjne NUCLEO (moduły mikrokontrolerów i płytek rozszerzeń) są sprzętowo zgodne ze standardem Arduino UNO R3, ale żeby wykorzystać wszystkie możliwości sprzętowe mikrokontrolerów płytki NUCLEO wyposażono w dodatkowe złącza nazwane ST Morpho i dużo większej liczbie wyprowadzeń niż to jest w przypadku Arduino UNO R3. X-NUCLEO-IDW01M1 można łączyć z modułem mikrokontrolera tylko za pomocą złącza Morpho. Na **fotografii 1** pokazano połączone moduły Wi-Fi X-NUCLEO-IDW01M1 i mikrokontrolera STM32 NUCLEO F401RE.

Moduł SPWF01SA ma wbudowany mikrokontroler z rodziny STM32 Cortex-M3 z zapisanym w pamięci Flash firmware. To firmowe oprogramowanie jest rozwijane i jest możliwość jego aktualizacji przez interfejs UART. Trzeba do pamięci mikrokontrolera



Fotografia 1. Połączone moduły X-NUCLEO-IDW01M1 i STM32 NUCLEO F401RE

modułu STM32 X-NUCLEO połączonego z X-NUCLEO-IDW01M1 wgrać skompilowany plik z katalogu FW_Upgrade_UART zawartego w paczce programowej z programami testowymi. Moduł mikrokontrolera STM32 Nucleo może się teraz łączyć z komputerem poprzez wirtualny UART via USB. Do komunikacji można użyć dowolnego programu terminalowego np. PuTTY, TeraTerm itp. Parametry transmisji – Baud: 115200 b/s, Data: 8 bit, Parity: None; Stop Bit: 1 bit, Flow Ctrl: None. Po wysłaniu komendy AT+S.STS moduł odpowie informacją o wersji firmware wgranej do mikrokontrolera modułu SPWF01SA. Na jej podstawie można podjąć decyzję o aktualizacji.

Zestaw programów demonstracyjnych oraz prostych programów pomocniczych pozwala użytkownikowi na konfigurowanie modułu SPWF01SA:

- do połączenia z punktem dostępowym Acces Point (AP),
- do pracy w trybach STA (*Station*), MiniAP (*mini Acces Point*), IBBS (pracy w konfiguracji *Ad Hoc*),
- do skanowania dostępnych sieci, wybór punktu dostępowego AP i połączenia z nim,
- do użycia połączenia TCP/UDP, do otwierania, zamykania oraz zapisywania/odczytywanie soketów.

Ciekawą propozycją jest moduł ATWINC1500-MR210PB (**fotografia 2**) produkowany przez firmę Microchip. To kolejna konstrukcja, która najprawdopodobniej wywodzi się z przejętego Atmela. Cechą

Fotografia 2. Moduł Wi-Fi ATWINC1500

Tabela 3. Wybrane różnice pomiędzy standardami BLE

Parametr	BLE v4.2	BLE v5.0
Zasięg w pomieszczeniach	10 m	40 m
Zasięg na zewnątrz	40 m	200 m
Prędkość przesyłania danych	1 Mb/s	2 Mb/s
Ramka danych	ok. 32 bajtów	255 bajtów
Kodowanie i korekcja błędów	słabe	silne
Wsparcie IoT	nie	tak

charakterystyczną modułu jest niski poziom pobieranej mocy. Producent poleca go szczególnie do zastosowań w sieciach połączeń bezprzewodowych urządzeń IoT. Zapewniona jest zgodność ze standardem 802.11 b/g/n. Urządzenie ma niewielkie wymiary (21,7×14,7×2,1 mm) i podobnie jak wyżej opisywany moduł produkcji ST jest przeznaczony do montażu powierzchniowego. Do połączenia z hostem użyto portu szeregowego SPI.

Podstawowe cechy modułu:

- standard IEEE 802.11 b/g/n,
- pasmo ISM 2,4 GHz,
- zintegrowany przełącznik nadawanie/odbiór,
- zintegrowana antena paskowa PCB lub złącze FL dla anteny zewnętrznej,
- doskonała czułość i zasięg dzięki zaawansowanemu przetwarzaniu sygnału PHY,
- obsługa zabezpieczenia IEEE 802.11 WEP, WPA, WPA2,
- obsługa zabezpieczeń korporacyjnych za pomocą WPA/WPA2 (802.1X) (1),
- stos protokołów sieciowych IP zaimplementowany w mikrokontrolerze modułu (odciążenie hosta). Funkcje protokołów TCP, UDP, DHCP, ARP, HTTP, TLS i DNS,
- sprzętowe akceleratory zabezpieczeń WiFi i TLS.

Praca modułu jest wspierana przez biblioteki MPLAB Harmony.

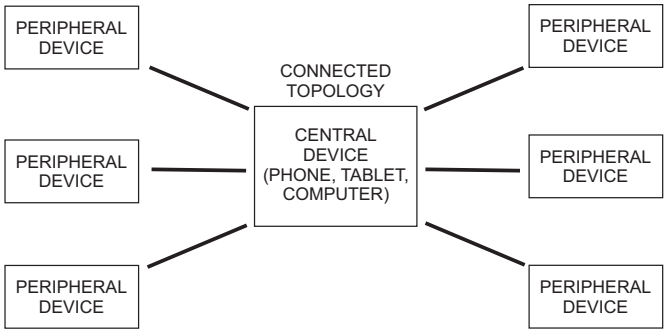
Bluetooth

Standard Bluetooth jest stosowany do transmisji danych na niewielkie odległości. Pierwsze wersje Bluetooth były optymalizowane do szybkiego przesyłania dużych ilości danych. Bluetooth 3.0 +HS zapewnia przepływność do 24 Mb/s. Niestety ta wersja standardu niezbyt dobrze radziła sobie z zarządzaniem poborem energii i trudno ją było stosować w urządzeniach zasilanych bateryjnie, na przykład w urządzeniach końcowych IoT. Dlatego w kolejnej wersji standardu (4.2) nazwanej Bluetooth Low Energy (BLE) priorytetem nie były duże prędkości transmisji danych, ale maksymalne ograniczenie poboru energii przez urządzenia łączące się przez Bluetooth.

Dalszy rozwój standardu zaowocował wersją BLE v5 zoptymalizowaną również do stosowania w sieciach urządzeń IoT. Podstawowe różnice pomiędzy tymi standardami pokazano w **tabeli 3**. Standard BLE v5 ma specjalny tryb pracy do połączeń na dłuższe dystanse nazwane BLE Long Range. Zwiększony zasięg uzyskuje się głównie przez zmniejszenie prędkości transmisji. Long Range jest szczególnie polecany do połączeń pomiędzy urządzeniami IoT.

BLE korzysta z pasma ISM 2,4 GHz podzielonego na 40 kanałów o szerokości 2 MHz. Kanały są logicznie podzielone na 2 grupy: 3 kanały advertising i 37 kanałów data. Kanały data są używane do dwukierunkowej transmisji danych pomiędzy urządzeniami w sieci. Kanały advertising biorą udział w procesie wyszukiwania urządzeń BLE znajdujących się w pobliżu, a potem w nawiązywaniu połączenia pomiędzy nimi.

Komunikacja w sieci BLE zaczyna się od rozgłaszania przez węzeł sieci (advertiser), informacji, że oczekuje na połączenia. Węzły sieci scanners odbierające komunikat żądania na połączenie wysyłają komunikat z żądaniem połączenia *connection request*. Ten komunikat musi zawierać dane niezbędne do zestawienia połączenia. Jeżeli połączenie zostanie nawiązane, to węzeł scanners staje się węzłem

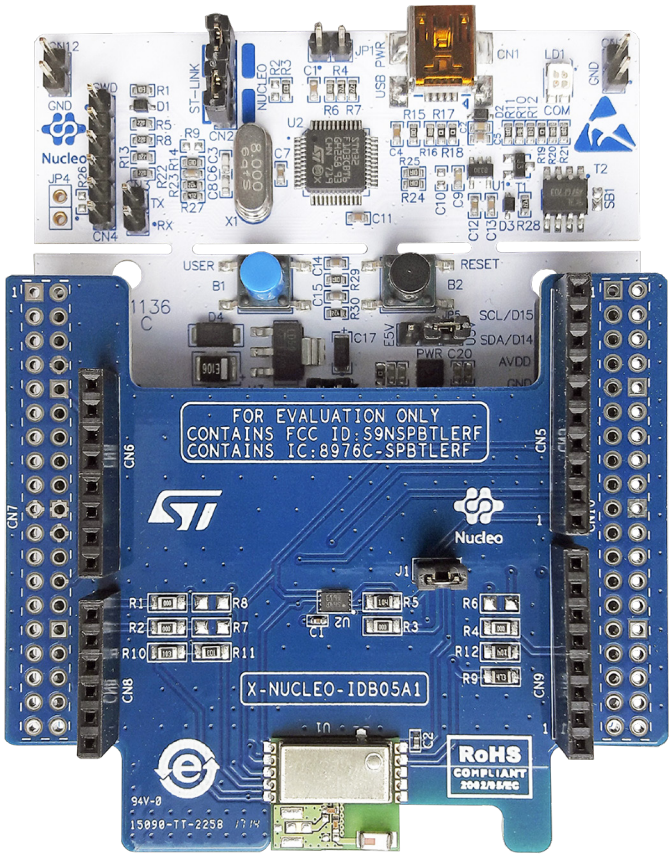


Rysunek 3. Podsieć BLE o topologii gwiazdy

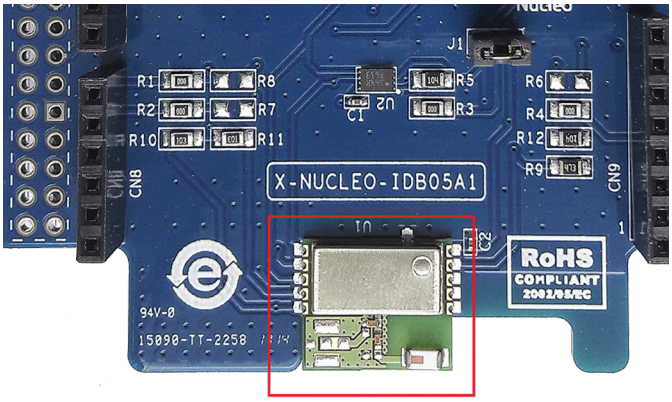
master, a węzeł rozgłaszający advertiser węzłem slave. Tworzy się w ten sposób podsieć pracująca w topologii gwiazdy, gdzie jest jeden master, mogący komunikować się z jednym lub więcej węzłów slave. Urządzenie pracujące jako węzeł master nazywane jest *Central Device*, a urządzenia slave *Pheriperial Device* (**rysunek 3**). Central Device to najczęściej komputer, smartfon, tablet, itp..

Transmisję zawsze inicjuje węzeł master. Węzeł slave musi przesłać w odpowiedzi informację zwrotną. Po nadaniu jednego pakietu danych musi minąć co najmniej 150 µs (*IFS Inter Frame Space*). Każdy z pakietów może zawierać wskaźnik MD (*More Data*) sygnalizujący konieczność przesłania kolejnych danych. Protokół BLE ma budowę warstwową i składa się z warstwy fizycznej psyhical layer, warstwy łącza danych link layer, oraz warstwy HCI (*Host Controller Interface*). W warstwach wyższych jest umieszczony GATT (*Generic Attribute Profile*) i GAP (*Generic Access Profile*).

Warstwa GATT jest zbudowana w oparciu o protokół ATT (*Atrribute Protocol*), który wykorzystuje dane GATT do określenia sposobu w jaki dwa urządzenia BLE wysyłają i odbierają standardowe wiadomości. GATT jest zbudowany w oparciu o role klienta i serwera. Układy Peripherial są serwerami GATT (maja zapisane definicje charakterystyk i serwisów), a układ Central pełni role klienta, bo wysyła



Fotografia 3. Płytka BLE X-Nucleo-IDB05A1 połączona z modułem Nucleo F-401RE



Fotografia 4. Moduł Bluetooth Low Energy SPBLE-RF SPBLE-RF

żądania do serwera. W specyfikacji GATT jest opisanych wiele profili w tym na przykład medyczne przeznaczone do pomiaru ciśnienia krwi, monitorowania poziomu glukozy, mierzenia rytmu serca, pomiaru temperatury ciała, itp.

Na rynku jest bardzo dużo modułów BLE. Do celów testowych warto skorzystać z gotowego rozwiązania na przykład z zestawu X-Nucleo-IDB05A1 będącego połączeniem modułu BLE z płytką 32-bitowego mikrokontrolera rodziny STM32 (**fotografie 3** i **4**) Połączenia przez BLE z tego zestawu można szybko przetestować dzięki udostępnieniu przez STM pakietowi programów demonstracyjnych X-CUBE-BLE1. Ze strony producenta trzeba pobrać spakowany program demonstracyjny en.X-Cube-BLE1. Po rozpakowaniu możemy korzystać z programów demonstracyjnych z gotowymi projektami dla środowisk projektowych:

- IDE Keil uVision,
- IAR EWARM,
- AC6.

Oprogramowanie demonstracyjne bazuje na warstwie abstrakcji sprzętu STM32CubeHAL dla mikrokontrolerów STM32. Aplikacja używa oprócz tego pakiet wsparcia BSP (*Board Support Package*) dla płytki Nucleo, oraz dla płytki rozszerzenia BlueNRG/BlueNRG-MS. Zastosowany tu procesor BLE BlueNRG-MS charakteryzuje się bardzo małym poborem mocy, a jego firmware jest zgodne ze specyfikacją Bluetooth 4.0/4.1. Warstwa sterowników (*Drivers*) zapewnia komponentom warstw wyższych (*Middleware*) dostęp do urządzenia BlueNRG-MS niezależnie od szczegółów sprzętowych. Inaczej mówiąc warstwy wyższe nie muszą znać budowy i szczegółów sterowania procesora BLE. Middleware Low Power Manager optymalizuje pobór mocy.

Pakiet oprogramowania zawiera szereg przykładowych aplikacji. Kiedy testowany układ pełni rolę układu peryferyjnego (*peripherial device–slave*), to wspierana jest obsługa profili specyfikacji GATT:

- Alert Notification Client,
- Blood Pressure Sensor,
- Find Me Locaqtor,
- Find Me Target,
- Glucose Sensor,
- Health Thermomenter,
- Heart Rate,
- Human Interface Device,
- Phone Alert Client,
- Proximity Monitor,
- Proximity reporter,
- Timer Server.

W przypadku pełnienia roli układu centralnego (*Central device–Master*) wpierana jest obsługa profili:

- Alert Notification Client,
- Blood Pressure Collector,
- Find Me locator,
- Glucose Collector,
- Health Thermometer Collector,
- Heart Rate Collector,
- Time Client.

Podobne moduły Bluetooth oferuje wielu producentów. Dla konstruktora najbardziej atrakcyjne jest połączenie modułu z mikrokontrolerem i oprogramowaniem. Takie rozwiązanie zostało pokazane wyżej na przykładzie zestawu STM. Również inni producenci w ten sposób promują swoje rozwiązania – połączenia własnych modłów radiowych Bluetooth z produkowanymi przez siebie mikrokontrolerami.

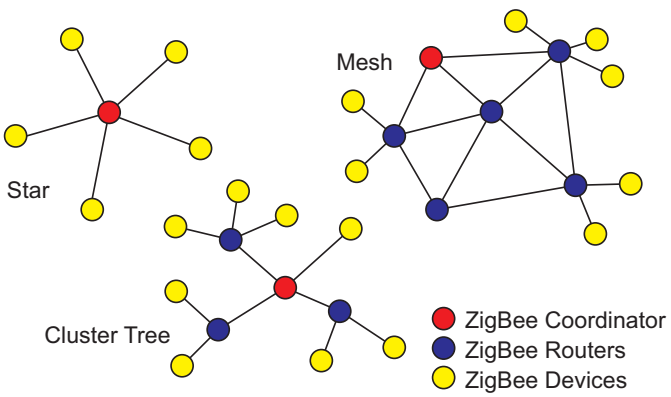
ZigBee

Jest to tani, energooszczędny, bezprzewodowy standard sieci kratowej przeznaczony dla urządzeń zasilanych bateryjnie pracujących w aplikacjach monitorowania i sterowania. Jedną z istotnych właściwości sieci jest zapewnienie przesyłania danych z małym opóźnieniem czasowym. ZigBee w założeniu ma być prostszy i tańszy niż sieci Bluetooth i Wi-Fi. Zastosowania obejmują bezprzewodowe włączniki światła, domowe monitory energii , zbieranie danych z urządzeń medycznych, systemy zarządzania ruchem oraz inne urządzenia konsumenckie i przemysłowe, które wymagają bezprzewodowego transferu danych o małym zasięgu i małej prędkości przesyłania danych.

W warstwie programowej ZigBee jest zestawem protokołów komunikacyjnych wysokiego poziomu wykorzystujących model warstwowy. Najniższe dwie warstwy sprzętową i MAC określa specyfikacja IEEE802.15.4 (podobnie jak opisywany już MiWi). Wyższe warstwy to warstwa sieci, warstwa aplikacji, obiekty ZigBee Device Objects (ZDO) i obiekty aplikacji zdefiniowane przez producenta. ZDO są odpowiedzialne za niektóre zadania, w tym śLEDzenie ról urządzeń, zarządzanie wnioskami o dołączenie do sieci, a także wykrywanie urządzeń w sieci i bezpieczeństwo.

ZigBee pracuje w pasmach ISM 2,4 GHz, chociaż niektóre urządzenia używają również częstotliwości 784 MHz w Chinach, 868 MHz w Europie i 915 MHz w Stanach Zjednoczonych i Australii, jednak nawet te regiony i kraje nadal używają 2,4 GHz dla większości komercyjnych urządzeń ZigBee do użytku domowego. Szybkość transmisji danych waha się od 20 kbit/s (pasmo 868 MHz) do 250 kbit/s (pasmo 2,4 GHz). Niska moc wyjściowa nadajników ogranicza bezpośredni zasięg do 10...100 m.

Warstwa sieciowa ZigBee natywnie obsługuje zarówno sieci w topologii gwiazdy (z punktem centralnym), klastrowe (drzewiaste) jak i sieci kratowe P2P (MESH). Każda sieć musi mieć jedno urządzenie koordynujące. W sieciach z topologią gwiazdy koordynatorem musi być węzeł centralny (**rysunek 4**). W sieciach kratowych stosuje się przekazywanie danych przez urządzenia pośredniczące pełniące funkcje routerów ZigBee. Pozwala to na rozszerzenie zasięgu komunikacji na poziomie sieci. Inną cechą definiującą ZigBee są urządzenia do prowadzenia bezpiecznej komunikacji, ochrony ustanawiania i transportu kluczy kryptograficznych, ram szyfrowania i urządzenia kontrolnego. Opiera się na podstawowej strukturze bezpieczeństwa zdefiniowanej w IEEE 802.15.4.



Rysunek 4. Topologie sieci ZigBee

W sieciach ZigBee pracują trzy rodzaje urządzeń:

1. Koordynator ZigBee (ZC). W każdej sieci jest tylko jeden koordynator. Jego funkcją jest pierwotne konfigurowanie sieci, przechowywanie informacji o konfiguracji, jest centrum zaufania i repozytorium kluczy bezpieczeństwa. Koordynator musi być urządzeniem o określonej wydajności (zazwyczaj wymaganej największej wśród urządzeń sieci) pozwalającej na wykonywanie przydzielonych zadań.
2. Router ZigBee (ZR). Oprócz funkcji urządzenia końcowego router może pełnić rolę routera pośredniego, przesyłając dane pomiędzy innymi urządzeniami.
3. Urządzenie końcowe ZigBee (ZED). Posiada wystarczającą funkcjonalność do komunikacji z węzłem nadrzędnym (koordynatorem lub routerem), ale nie może przekazywać danych z innych urządzeń. Urządzenie końcowe nie musi być cały czas w pełnej gotowości tak jak router i koordynator, dlatego kiedy nie wykonuje żadnych funkcji sieciowych lub aplikacyjnych (zbieranie danych, sterowanie) to przechodzi w stan uśpienia. Jest najtańszy w produkcji i może być zasilany bateryjnie.

Można wyróżnić dwie konfiguracje pracy sieci ze względu na ruch danych: z nawigacją (*beacon enabLED*) i bez nawigacji (*non beacon enabLED*). W sieciach bez sygnałów nawigacyjnych obsługiwany jest nieblokowany mechanizm CSMA/CA. Routery mają odbiorniki ciągle aktywne i wymagają niezawodnego zasilania. W sieciach nieobsługujących sygnałów nawigacyjnych pobór mocy jest zdecydowanie asymetryczny: niektóre urządzenia są zawsze aktywne, podczas gdy inne przez większość czasu są uśpione.

W sieciach z sygnałami nawigacyjnymi routery ZigBee przesyłają okresowe sygnały nawigacyjne potwierdzając swoja obecność w innych węzłach sieci. Okres ten wynosi od 15...40 milisekund do ok. 760 sekund. W czasie, kiedy sygnały nawigacyjne nie są wysyłane routery mogą przechodzić w stan uśpienia i ograniczać wydatnie zużycie energii.

Sieci Thread

Kolejnym rozwiązaniem przeznaczonym dla sieci bezprzewodowych są sieci Thread. Thread jest protokołem do budowania sieci bezprzewodowych o małej mocy, opartym na powszechnie obsługiwanym protokole internetowym (IP). Thread umożliwia komunikację urządzenie–urządzenie i urządzenie–chmura i zawiera niezbędne funkcje bezpieczeństwa. Stos protokołów podobnie jak ZigBee w najniższych warstwach sprzętowej i MAC jest oparty o specyfikację IEEE 802.15.4 zapewniającą niski pobór energii i małe opóźnienie przesyłania danych.

Sieci Thread oparte o protokół IP (IPv6) są idealne do łatwego połączenia urządzeń IoT z Internetem. Główne cechy protokołu to:

- bezpieczeństwo – wszystkie urządzenia w sieci są uwierzytelniane a transmisja jest szyfrowana,
- prostota – prosta instalacja, uruchomienia i obsługa,
- niezawodność – sieć kratowa ma właściwości samo naprawiania. Uszkodzone pojedyncze urządzenie nie ma wpływu na działanie sieci,
- energooszczędność – urządzania mogą pracować w stanie uśpienia przez wiele godzin.

W sieci pracują dwa typy urządzeń:

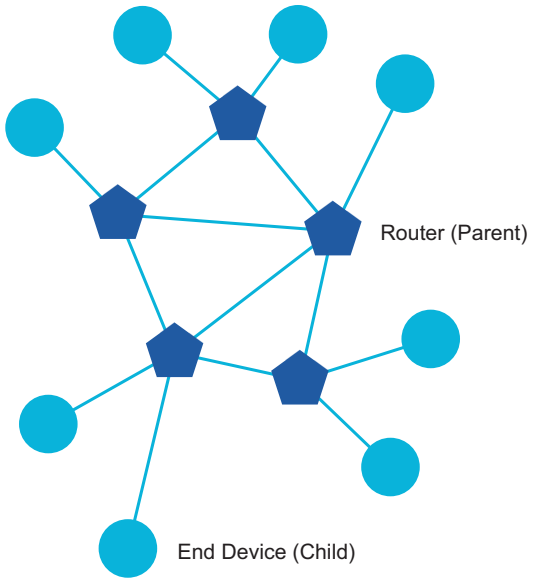
1. router (*parent*),
2. urządzenie końcowe (*child*).

Topologia sieci została pokazana na **rysunku 5**. Router to węzeł, który:

- przesyła pakiety danych do urządzeń sieciowych,
- zapewnia bezpieczne usługi uruchamiania dla urządzeń próbujących dołączyć do sieci,
- utrzymuje transceiver włączony przez cały czas.

Urządzenie końcowe (ED) to węzeł, który:

- przede wszystkim komunikuje się z jednym routerem,
- nie przesyła dalej pakietów dla innych urządzeń sieciowych,
- może wyłączyć swój transceiver w celu zmniejszenia poboru energii.



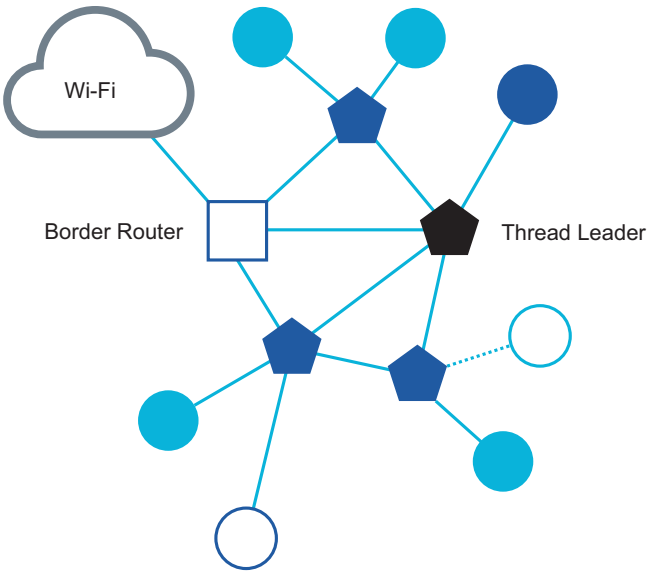
Rysunek 5. Topologia sieci Thread

Jeden z routerów pełni funkcję lidera (Leader). Jest odpowiedzialny za zarządzanie zestawem routerów w sieci. Jest dynamicznie wybierany automatycznie pod kątem odporności na uszkodzenia oraz agreguje i rozpowszechnia informacje o konfiguracji w całej sieci.

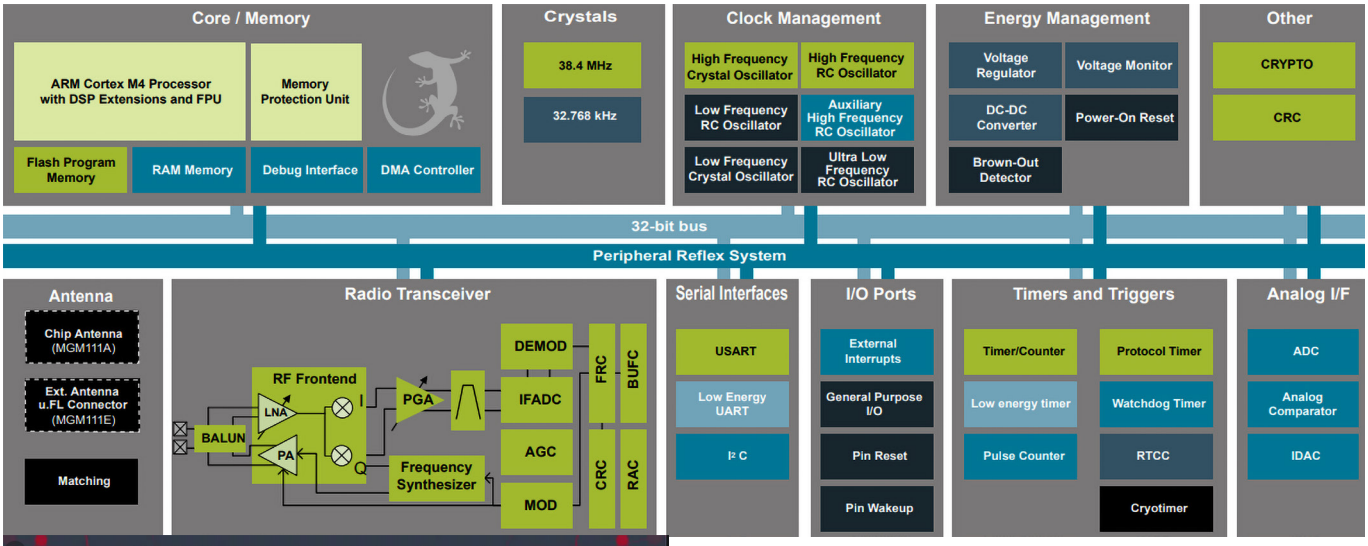
W sieci może też pracować Border Router. Jest to urządzenie, które może przekazywać informacje między siecią Thread a inną siecią (na przykład Wi-Fi) (**rysunek 6**). Konfiguruje także sieć Thread do połączeń zewnętrznych. Każde urządzenie może służyć jako router graniczny, jeżeli ma takie możliwości techniczne.

Ponieważ protokoły ZigBee i Thread są oparte o specyfikację IEEE 802.15.4, to w warstwie sprzętowej mogą być identyczne. Dlatego często spotyka się sprzętowe rozwiązania, które są wspólne, a jedynie różnią oprogramowaniem wyższych warstw protokołów. Spotykane są również moduły, które do tych dwu dołączają tez protokół BLE.

Przykładem takiego rozwiązania jest moduł MGM111 Mighty Gecko Mesh Networking Module (**rysunek 7**). MGM jest oparty o rozwiązanie Silicon Labs EFR32 Mighty Gecko SoC i łączy energooszczędny, wieloprotokołowy bezprzewodowy SoC ze sprawdzoną konstrukcją transceivera RF z układem antenowym.



Rysunek 6. Sieć Thread połączona z siecią Wi-Fi poprzez Border Router



Rysunek 7. Moduł MGM111

Moduł pracuje w paśmie 2,4 GHz i wspiera transmisję radiową dla wykorzystujących standard IEEE 802.15.4 sieci typu ZigBee i Thread. Prędkość transmisji wynosi 250 kb/s. Zastosowano przetwarzanie bezpośredniego widma rozpraszającego DSSS i modulację przesunięcia kwadraturowego przesunięcia fazowego (OQPSK) określoną przez IEEE 802.15.4. Moc wyjściowa jest programowana i osiąga +10 dBm. Czułość odbiornika wynosi –99 dBm. Wbudowany akcelerator sprzętowy obsługuje algorytmy szyfrowania transmisji AES, ECC i SHA.

Innym przykładowym rozwiązaniem są mikrokontrolery rodziny STM32WB. STM32WB to połączenie uniwersalnego wydajnego rdzenia ARM Cortex-M4 zoptymalizowanego dla małego zużycia energii z rdzeniem ARM-Cortex M0+ i modułem transceiver'a radiowego pracującego w paśmie 2,4 GHz, zgodnego z normą IEEE 802.15.4. Jak się łatwo domyśleć mikrokontrolery STM32WB są przeznaczone do stosowania w układach, w których istnieje potrzeba użycia łącza radiowego ze szczególnym naciskiem na standard Bluetooth 5.0 (BLE), Thread i ZigBee. Radiowy układ nadajnika jest oparty o bezpośrednią modulację nośnej w kanale nadawczym TX. Układ odbiornika wykorzystuje przemianę częstotliwości z niską częstotliwością pośrednią IF. Dzięki wbudowanemu w strukturę modułu transformatorowi w.cz. antenę o impedancji ok. 50 Ω można dołączyć bezpośrednio do wyprowadzenia RF1 mikrokontrolera (jednożyłowe połączenie SE). Naturalna charakterystyka pasmowa transformatora w pewnym stopniu filtruje szkodliwe częstotliwości harmoniczne i eliminuje zakłócenia zewnętrzne.

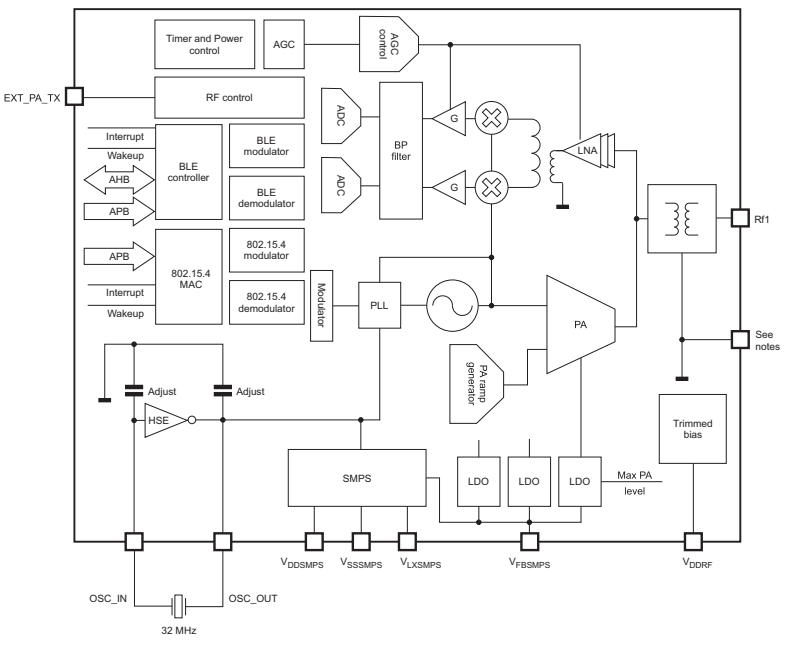
Moc wyjściowa TX jest regulowana przez programowe ustawianie napięcia wyjściowego stabilizatora LDO zasilającego nadajnik transceivera. Odbiornik może pracować w programowanych trybach z dużą wydajnością lub ograniczonym poborem mocy. Wbudowana w układ odbiornika automatyczna regulacja wzmocnienia ARW obejmuje zarówno tor wzmocnienia wielkiej częstotliwości jak i tor pośredniej częstotliwości. Źródłem sygnału zegarowego taktującego moduł RF jest oscylator kwarcowy o częstotliwości 32 MHz z wbudowanymi wewnętrznymi kondensatorami o programowanej pojemności. Rezonator 32 MHz oraz prosty dodatkowy układ filtrów w.cz. są jedynymi elementami zewnętrznym potrzebnymi do pracy. Antena może być wykonana ma płytce PCB. Można również dołączyć przez złącze RF antenę zewnętrzną na pasmo 2,4 GHz. Układ antenowy powinien posiadać na wejściu filtr pasmowo przepustowy lub dolnoprzepustowy ograniczający pasmo sygnału wejściowo/wyjściowego, oraz układ kompensacji niedopasowania impedancji.

Dla mikrokontrolerów STM32WB dostępne są biblioteki protokołów BLE, ZigBee i Thread dystrybuowane przez środowisko STM32CubeMX.

Podsumowanie

W zależności od przeznaczenia, komponenty sieci bezprzewodowych optymalizuje się pod kątem dużej przepustowości, oszczędności energii czy zasięgu. Trzeba znać wszystkie oferowane technologie, aby móc wybrać optymalne rozwiązanie.

Tomasz Jabłoński, EP



Rysunek 8. Schemat blokowy modułu radiowego