

dr inż. Piotr Dudek
prof. dr hab. inż. Edward Wantuch
Politechnika Krakowska

SIECI BEZPRZEWODOWE ZIGBEE W ZASTOSOWANIACH PRZEMYSŁOWYCH

Technologie sieci bezprzewodowych znajdują obecnie szerokie zastosowanie w wielu różnorodnych obszarach, takich jak zbieranie i przesyłanie danych pomiarowych, automatyka domowa, monitorowanie i automatyka przemysłowa. Wśród wielu standardów sieci bezprzewodowych coraz większe zainteresowanie wzbudza nowy standard ZigBee. W artykule przedstawiona jest charakterystyka tej technologii bezprzewodowej oraz jej zalety.

WIRELESS ZIGBEE NETWORK FOR THE INDUSTRY

The wireless communication technologies are rapidly spreading to many new areas, including the automation and the importance of the use of wireless technologies in the data acquisition, building control, monitoring systems and automation of manufacturing processes will grow. From the existing wireless standards seems very promising the new international standard ZigBee. The article describes this wireless technology and it's benefits.

WSTĘP

Zastosowanie łączności bezprzewodowej w systemach przemysłowych z roku na rok staje się coraz bardziej powszechne. Systemy bezprzewodowe rozwiązują powszechne problemy związane z położeniem kabla, oszczędzają czas, materiał i koszty instalacji. Najczęściej stosowanymi technologiami bezprzewodowymi w systemach M2M (Man-to-Machine) są rozwiązania oparte na modułach GSM. Ich popularność szybko rośnie ze względu na wygodę stosowania, szybko malejące ceny oraz coraz większe możliwości. Również coraz częściej stosuje się aplikacje oparte na sieciach WLAN (IEEE 802.11), zapewniających prędkość transmisji danych do 54 Mb/s jak również technologie Bluetooth, HomeRF, czy też moduły działające w pasmach ISM (*Industrial, Scientific, Medical*) 433MHz, 868 MHz i 2,4 GHz. Z technologiami tymi zaczyna powoli konkurować nowoczesne rozwiązanie, działające w paśmie 2,4 GHz, zapewniające niezawodną transmisję danych z prędkościami do 250 kb/s na odległości do ok. 70 metrów. Technologia ZigBee (IEEE 802.15.4) zapewnia elastyczność konfiguracji sieci, zminimalizowanie poboru energii przez urządzenia, uproszczenie implementacji stosu obsługującego protokół oraz możliwość działania dużej liczby urządzeń w sieci. W artykule został przedstawiony protokół ZigBee, możliwości jego zastosowania, jego perspektywy, jak również ograniczenia.

1. CZYM JEST ZIGBEE?

Technologia ZigBee została zaprojektowana specjalnie z myślą o wykorzystaniu w produkcji różnego rodzaju czujników i urządzeń sterujących, bądź monitorujących. Ratyfikowany w maju 2003 r., IEEE 802.15.4 jest prostym lecz silnym protokołem pakietowym, zapewniającym dużą niezawodność poprzez potwierdzanie odbioru, sprawdzanie błędów, transmisję z widmem rozproszonym (sekwencja bezpośrednia), zdolność zmieniania częstotliwości dla uniknięcia interferencji i możliwości wyboru przez użytkownika poziomu bezpieczeństwa. Urządzenia te nie wymagają dużej szerokości pasma, natomiast opóźnienie

przy ich wykrywaniu oraz zużycie energii powinno w ich przypadku być zminimalizowane. Kwestia kosztów samego urządzenia również nie pozostaje bez znaczenia. Przewidywane obszary zastosowań obejmują bardzo różne dziedziny od przemysłu, rolnictwa, ochrony środowiska, automatyzacji budynków, poprzez ochronę zdrowia, obsługę sprzętów domowych po gry i zabawki.

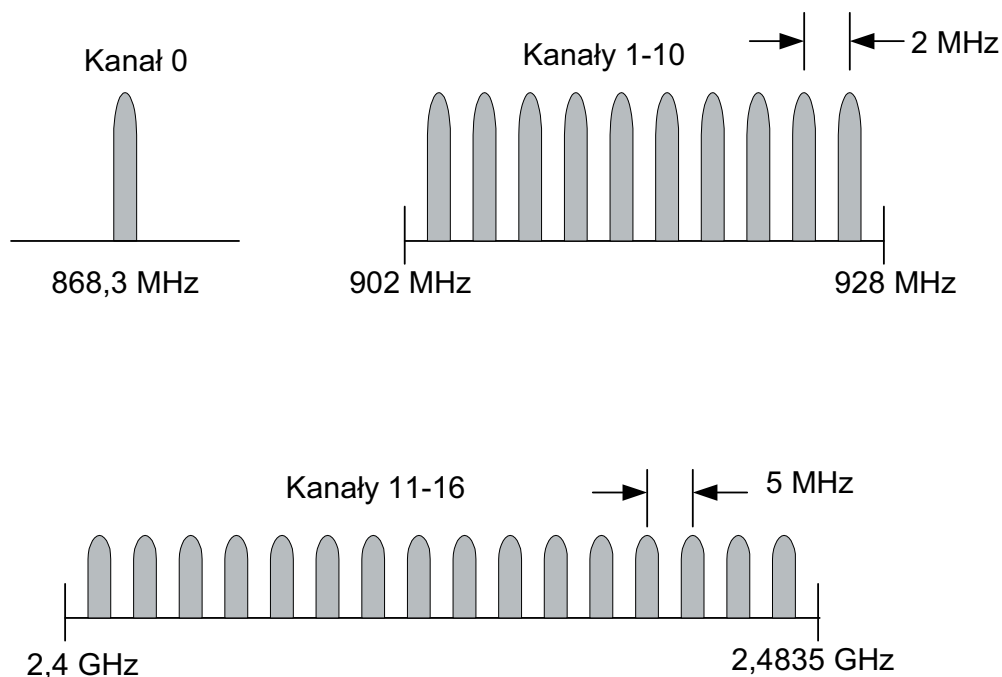
Technologia ta korzysta ze standardu łącza radiowego, zdefiniowanego przez IEEE 802.15.4, uzupełniając go o sieć logiczną oraz oprogramowanie związane z bezpieczeństwem i aplikacjami użytkownika. Zgodność ze standardem IEEE zapewnia dużą kompatybilność w współpracy między urządzeniami pracującymi w tej technologii. ZigBee aspiruje do pozycji globalnego standardu obsługującego sieci typu czujnik-system sterowania. Technologia ta została zaprojektowana tak, aby spełniać szereg wymagań:

- Mały pobór mocy. Baterie zasilające urządzenia używające tej technologii powinny wystarczać na okres miesięcy a nawet lat. Oszczędność energii pozostaje nie bez znaczenia nie tylko dla wygody użytkownika, ale również jest pożądana z ekologicznego punktu widzenia. Podstawowe radio ZigBee pracuje z mocą 1 mW, jeżeli urządzenie nie wysyła lub odbiera danych przełączane jest w tryb uśpienia, charakteryzującym się niskim poborem energii.
- Łatwość użycia. W przeciwieństwie do technologii Bluetooth, w której wybór trybu pracy zależy od wymaganego opóźnienia oraz poboru mocy, ZigBee ma tylko dwa tryby pracy: aktywny (wysyłanie/odbiór sygnału) oraz stan uśpienia. W ten sposób aplikacje nie muszą wybierać odpowiedniego trybu w zależności od potrzeb transmisji – dzieje się to niezależnie. Przełączenie do trybu aktywnego z trybu uśpienia następuje w czasie do 15 ms.
- Niskie koszty. Koszty urządzeń działających w technologii ZigBee są bardzo nieduże (kilkadziesiąt centów do kilku dolarów). Dzięki małemu zużyciu energii, ich eksploatacja również jest niedroga. Wbudowana konfiguracja powoduje, iż dodatkowe urządzenia sieciowe stają się niepotrzebne, co dodatkowo zmniejsza koszty.
- Możliwość obsługi dużej liczby urządzeń. Sieci ZigBee mogą obsługiwać 2^{64} urządzeń co w zupełności zaspokaja najbardziej możliwie rozbudowane projekty. Ma to zasadnicze znaczenie np. dla wielkich tablic czujników i sieci sterujących.
- Prosty protokół. Prostota kodu pozwala na łatwe współdziałanie oraz wspomniane już obniżenie kosztów. W szeregu istniejących opracowań konfiguracje modułów ZigBee można przeprowadzić poprzez komendy AT lub API producenta modułu. W porównaniu do innych technologii urządzenia te wymagają niewielu zasobów – od 4 kB do 32 kB – Bluetooth wymaga ok. 250 kB.
- Zasięg i omijanie zatorów komunikacyjnych. Sieci te pozwalają na zwielokrotnienie urządzeń/węzłów typu router pracujących jako przekaźnik informacji, co pozwala na zwiększenie obszaru pokrycia sygnałem bez konieczności wzmacniania sygnału. Jeżeli urządzenia nie mogą komunikować się po wyznaczonej trasie, automatycznie i dynamicznie wyznaczana jest nowa trasa.
- Globalna implementacja. Standard IEEE 802.15.4 implementowany przez ZigBee pozwala na pracę w pasmach 868 MHz w Europie, 915 MHz w Ameryce, Australii oraz 2.4 GHz – akceptowanym jako pasmo globalne niemal we wszystkich państwach. Najbardziej elastycznym oraz zapewniającym największe prędkości transmisji danych są rozwiązania pracujące w paśmie 2,4 GHz.

2. CHARAKTERYSTYKA ZIGBEE/IEEE 802.15.4

ZigBee pracuje w pasmach ISM 868 Mhz w Europie, 915 MHz w USA i 2,4 GHz – akceptowanym jako pasmo ogólnodostępne w większości państw na świecie. Metoda dostępu do medium to CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*). Dla pasm 868/915 MHz stosowana jest modulacja BPSK (*Binary Phase Shift Keying*), natomiast dla 2,4 GHz O-QPSK (*Orthogonal – Quadrature Phase Shift Keying*). Przewidziano 1 kanał w paśmie 868 MHz, 10 kanałów dla pasma 915 MHz a dla 2,4 GHz 16 kanałów o szerokości 5 MHz (rys. 1).

Rozwiązanie to przeznaczone jest dla aplikacji charakteryzujących się krótkim cyklem pracy – poniżej 0,1 % czasu. Na pobór mocy przez dany węzeł sieci składają się moce pobierane przez poszczególne podzespoły. Najwięcej energii zużywa nadajnik, odbiornik oraz mikrokontroler. Duży wpływ ma także częstotliwość pracy mikrokontrolera oraz liczba układów peryferyjnych, takich jak np. wzmacniacze mocy. Większość zasilanych z baterii węzłów w sieci ZigBee, tj. czujników i przełączników, znajduje się w stanie uśpienia przez 99,9 % czasu. Są one wzbudzane jedynie na kilka milisekund, aby dokonać odczytu czujnika lub skontaktować się z innymi elementami sieci. Całkowity pobór mocy takich węzłów jest bliski poborowi mocy w stanie uśpienia (rys 2).

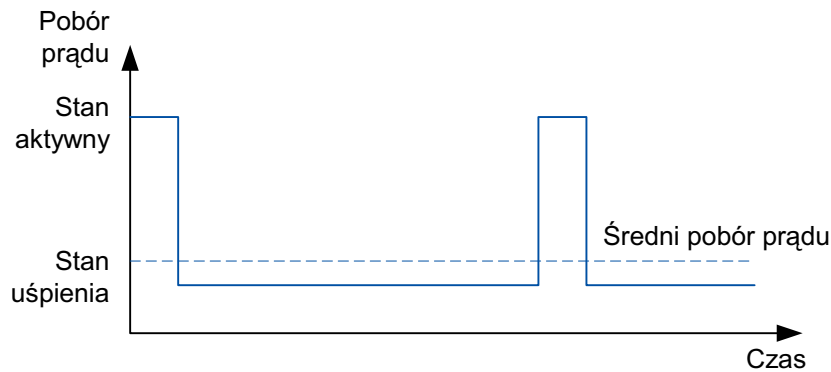


Rys. 1. Kanały i pasmo dla IEEE 802.15.4

Podczas transmisji danych stosowana jest złożona modulacja fazowa z rozpraszaniem widma metodą sekwencji bezpośredniej DSSS (*Direct Sequence Spread Spectrum*). W przypadku modulacji O-QPSK cztery kolejne bity informacyjne, tworzące tzw. symbol zastępowane są odpowiednio dobraną (1 z 16) sekwencją 32 bitów (*chips*). Daje to możliwość pracy przy słabym współczynniku S/N, wynikającym albo z powodu zakłóceń albo niskiej mocy nadajnika, co umożliwia zastosowanie tej technologii w środowisku charakteryzującym się dużym poziomem zakłóceń.

W odróżnieniu od technologii Bluetooth, transmisja danych odbywa się w jednym kanale, nie występuje tutaj tzw. *Frequency Hopping* – przeskakiwanie po kanałach. Mechanizm CCA

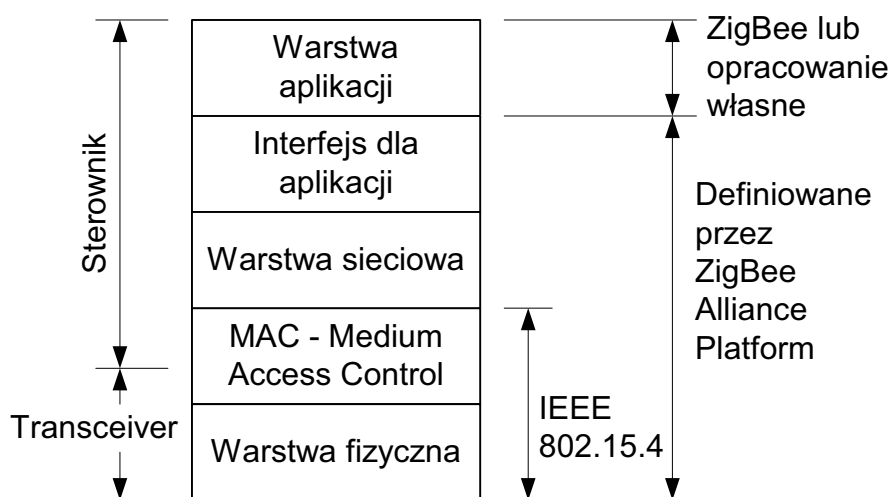
(*Clear Channel Assessment*), polegający na krótkotrwałym sprawdzaniu, czy inne urządzenia nie korzystają z danego kanału, pozwala uniknąć konfliktów z innymi sieciami. W warstwie fizycznej udostępniono takie procedury, jak detekcja odbieranej energii, badanie jakości łącza czy zmiana kanału. Standard nie definiuje algorytmów dynamicznej alokacji częstotliwości, lecz umożliwia ich wprowadzenie w warstwie sieciowej. Warstwa dostępu do medium zawiera funkcję skanującą wyszukującą urządzenie koordynujące. Poprzez wykorzystanie mechanizmu potwierdzania (protokół *handshake*) została zwiększona niezawodność transmisji danych.



Rys 2. Przykładowy pobór mocy przez mikrokontroler.

3. ARCHITEKTURA STOSU ZIGBEE

Jak wspomniano wcześniej, najważniejszą zmierzoną cechą charakterystyczną dla sieci ZigBee był niski koszt wdrożenia systemu i jego eksploatacji - co w tym przypadku oznacza zasilanie bateryjne wystarczające na miesiące lub lata. Aby spełnić te warunki konieczne jest zastosowanie prostych protokołów transmisyjnych działających na prostych urządzeniach. Stos protokołów standardu IEEE 802.15.4 wykorzystany w interfejsie radiowym ZigBee został przedstawiony na rysunku 3. Warstwa fizyczna (PHY) oraz warstwa dostępu do mediów (MAC) zostały opracowane przez IEEE. Podczas projektowania warstwy fizycznej wzięto pod uwagę żądanie niskich kosztów i możliwość produkcji urządzeń jako układów scalonych o dużej skali integracji.



Rys. 3. Stos protokołów standardu IEEE 802.15.4 i ZigBee

Dla wszystkich zakresów częstotliwości, w jakich pracuje protokół IEEE 802.15.4 wspólna jest struktura jednostki danych protokołu warstwy fizycznej PDU (*Physical Protocol Data Unit*) (Rys. 4). Zaczyna się ona od 32-bitowej preambuły wykorzystywanej do określenia częstotliwości pracy, taktowania sekwencji pseudolosowej oraz przepływności symbolowej. Natomiast maksymalny rozmiar pola danych użytecznych wynosi 127 bajtów i decyduje o nim wartość siedmiu bitów nagłówka oddzielonego od preambuły specjalnym ogranicznikiem ułatwiającym analizę ramki.



Rys. 4. Struktura jednostki danych warstwy fizycznej

Zgodnie z zasadami dotyczącymi rozwiązań 802 przyjętymi przez IEEE w warstwie łącza danych wyróżniamy podwarstwę dostępu do medium MAC (*Media Access Control*), współpracującą z różnymi implementacjami warstwy fizycznej, oraz podwarstwę logicznej kontroli łącza LLC (*Logical Link Control*), która została zdefiniowana w standardzie 802.2 i jest wspólna dla Ethernetu, Wi-Fi oraz Bluetooth.

Warstwa MAC jest odpowiedzialna m.in. za zarządzanie dostępem do kanału, kontrolą i potwierdzaniem odebranych ramek. Współpraca z logiczną kontrolą łącza zgodną z 802.2 typ 1 może odbywać się poprzez specjalną podwarstwę zbieżności SSCS (*Service-Specific Convergence Sublayer*) lub LLC odwołuje się bezpośrednio do usług podwarstwy MAC. Pomimo prostoty struktura jednostki danych protokołu MAC jest bardzo elastyczna i pozwala uwzględnić stosowanie różnych topologii oraz aplikacji w warstwach wyższych. Oprócz pola danych ramka składa się z trzech zasadniczych części. W skład nagłówka wchodzi pole kontrolne odpowiedzialne za określenie typu i zawartości przesyłanej ramki, formatu pola adresowego. Kolejny bajt zawiera numer sekwencji wykorzystywany przy potwierdzaniu poprawnego odbioru ramki. Ostatnim polem nagłówka jest adres. Protokół pozwala przysyłać dane użyteczne o różnej długości, jednakże ograniczeniem od góry jest maksymalny rozmiar całej ramki wynoszący 127 bajtów. Ramkę kończy 16-bitowa sekwencja CRC sprawdzająca integralność danych. Ponieważ pole danych jest ma co najwyżej 104 bajtów długości, to dane o większej objętości muszą być podzielone na ponumerowane porcje i przesyłane sekwencyjnie jako oddzielne komunikaty w osobnych ramach. Urządzenie odbiorcze za pomocą numerów sekwencyjnych zapisanych w kolejnych ramach będzie mógł złożyć transmitowane dane w całość.

Warstwa MAC protokołu IEEE 802.15.4 zawiera cztery typy ramek transmisyjnych:

- ramka znacznika (*beacon frame*), którą wykorzystuje koordynator sieci w celu wysyłania znaczników do urządzeń w sieci,
- ramka danych,
- ramka potwierdzenia (*acknowledgment frame*), która zawiera potwierdzenie odebrania komunikatu,
- ramka rozkazu MAC (*MAC command frame*), używana do przesyłania pojedynczych rozkazów.

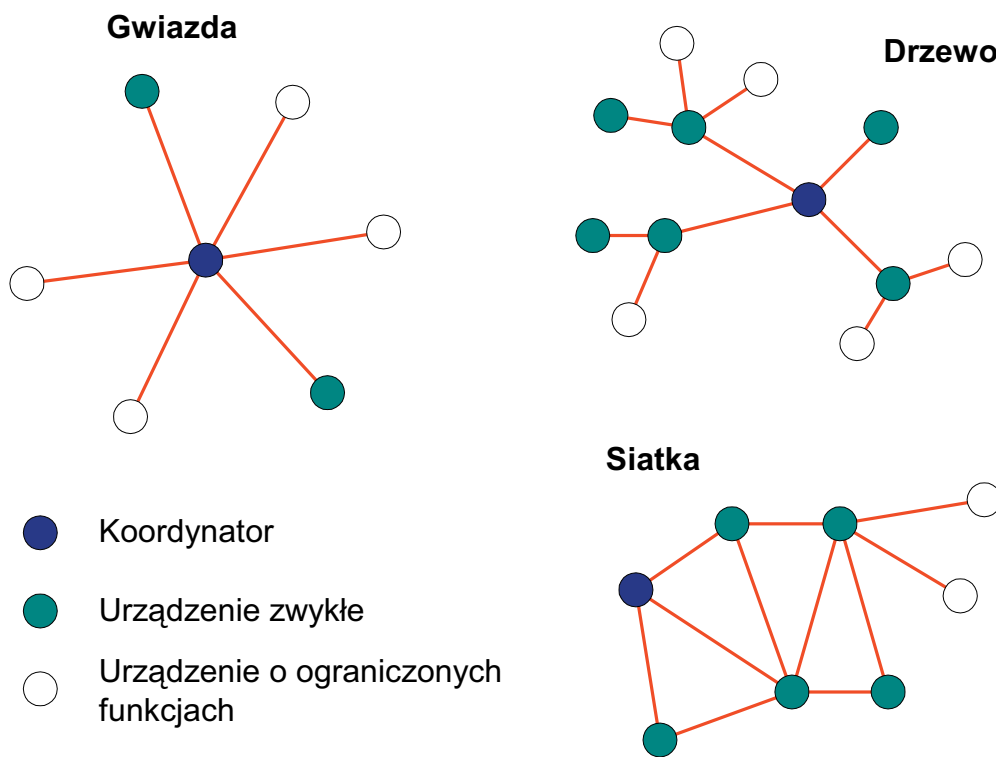
Urządzenia w sieci mogą być adresowane za pomocą pełnych adresów 64-bitowych wg standardu IEEE, albo za pomocą skróconych adresów 16-bitowych.

Mając na względzie, że niektóre aplikacje wymagają małych, stałych opóźnień, przewidziano specjalny tryb pracy. Ustalony "zarządca" koordynuje pracę podległych mu urządzeń, nadając w określonym czasie specjalne ramki kontrolne. Odstęp pomiędzy nimi może wynosić od 15 ms do aż 245 s i jest dzielony na 16 równych niezależnych szczelin czasowych. Dostęp do nich odbywa się na drodze rywalizacji, lecz koordynator może także przypisać szczelinę czasową (*Guaranteed Time Slots*) określonemu urządzeniu wymagającemu ustalonego pasma i opóźnienia.

Rozwiązanie ZigBee uwzględnia trzy stopnie zabezpieczeń na poziomie warstwy drugiej, z czego pierwszy z nich zakłada brak jakiegokolwiek ochrony. Kolejnym sposobem jest lista zaufanych urządzeń tworzona na podstawie adresu MAC bez zastosowania kryptografii. Największy poziom bezpieczeństwa zapewnia trzecia możliwość, tj. użycie 128-bitowego szyfrowania AES, jednakże IEEE nie precyzuje metody dystrybucji klucza.

4. TOPOLOGIA SIECI I URZĄDZENIA ZIGBEE

Urządzenia ZigBee mogą pracować w sieciach o topologii gwiazdy (*star*), siatkowej/kratowej (*mesh*) lub topologii drzewiastej (*cluster tree*) (rys. 5). Najczęściej stosuje się topologię gwiazdy, natomiast sieci siatkowe lub drzewiaste mogą zapewnić lepszą niezawodność komunikacji dzięki poprowadzeniu komunikacji pomiędzy węzłami wieloma drogami.



Rys. 5. Konfiguracja sieci z urządzeniami ZigBee

Standard IEEE definiuje dwa typy urządzeń:

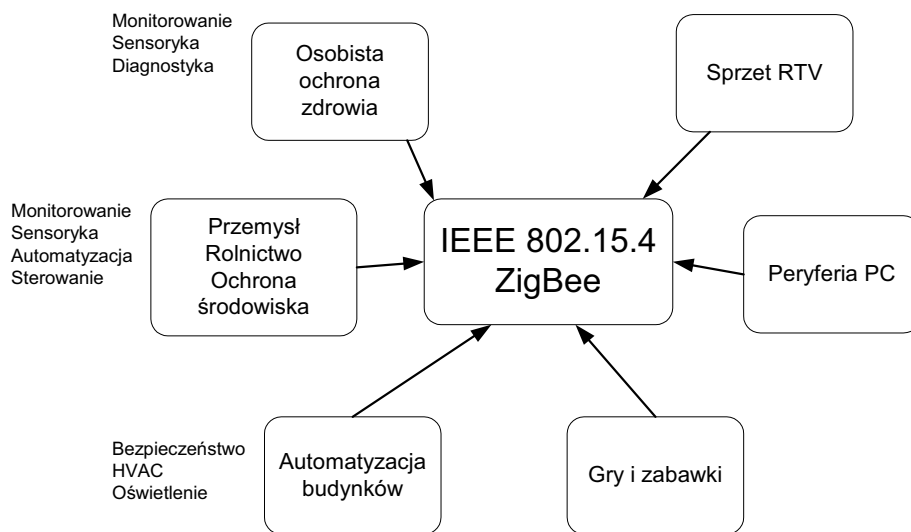
- FFD (*Full Function Device*) – implementujące wszystkie funkcje systemowe,
- RFD (*Reduced Function Device*) – podzespoły z ograniczonymi funkcjami systemowymi, nie wymagające dodatkowych pamięci RAM lub ROM oraz flash, zwykle tańsze niż urządzenia FFD.

Wymagane jest, aby w sieci znajdowało się przynajmniej jedno urządzenie FFD pracujące jako koordynator. W zależności od funkcji spełnianych w sieci urządzenia dzielą się na:

- koordynatory sieci, rozpoczynające jej pracę, zarządzający jej węzłami i przechowujący dane,
- routery, kierujące przepływem danych pomiędzy węzłami
- terminale, zwykle wysyłające informacje, np. czujniki, radiomodemy, itp.

5. OBSZARY I MOŻLIWOŚCI ZASTOSOWAŃ

Ogólnie obszar zastosowań ZigBee to bezprzewodowe monitorowanie i zdalne sterowanie we wszystkich możliwych dziedzinach (przemysłe, medycynie, biurze, domu). Możliwość tworzenia rozproszonych sieci bezprzewodowych ad-hoc o dynamicznie zmieniającej się topologii okazała się doskonałym rozwiązaniem dla firm transportowych, systemach monitoringu, kontroli dostępu, a także sterowania dla wielu systemów produkcyjnych. Niestety rozwiązania te dość powoli wkraczają na niektóre obszary, dla których ta technologia była projektowana. Na przykład stosunkowo dość wysokie koszty modułów ZigBee (ok. 3 dolarów za transceiver) w porównaniu do czujników automatyki domowej – np. kontraktonowego czujnika otwarcia okna (kilkanaście centów) powoduje że te rozwiązania jak dotychczas nie przyjęły się dość szeroko w systemach automatyki domowej czy też „inteligentnego” domu.



Rys. 6. Obszary zastosowań rozwiązań IEEE 802.15.4/ZigBee

ZigBee aspiruje do pozycji globalnego standardu obsługującego sieci sensorowe współpracujące z systemami ogólnie rozumianej automatyki. Możliwe jest zastosowanie tej technologii np. w motoryzacji (np. w połączeniu z czujnikami ciśnienia umieszczonymi w kołach raportujące centralnemu komputerowi o aktualnym ciśnieniu w poszczególnych

kołach). Możliwe jest wykorzystanie układów z wbudowanym tzw. *location engine* (rozwiązanie zawarte np. w układach Texas Instruments CC2431) do monitorowania np. rozkładu temperatury czy też innych parametrów fizykochemicznych w zbiornikach, użycie w systemach lokalizacji i monitorowania systemów mobilnych, itp. Jako że technologia ta jest energooszczędna, można zastosować takie układy w rozwiązaniach dla rolnictwa, ochrony środowiska czy też zoologii – systemy śledzące i monitorujące zachowanie zwierząt (obraczkowanie) przez długi okres czasu bez konieczności wymiany akumulatorów – pozyskane dane mogą być odczytywane z większej odległości bez niepotrzebnego niepokojenia zwierząt. Istnieje tutaj szerokie pole możliwych zastosowań w poszczególnych obszarach przemysłu, medycyny, rolnictwa czy też ochrony środowiska, jako że technologia ta mimo kilkuletniej już obecności na rynku dopiero od niedawna znajduje szersze zastosowanie. Na rynku dostępnych jest szereg nowoczesnych rozwiązań dla technologii ZigBee różnych firm – od układów scalonych transceiver'ów IEEE 802.15.4 poprzez moduły OEM a skończywszy na radiomodemach ZigBee. Obecnie do ZigBee Alliance zajmującej się standaryzacją i popularyzacją tej technologii należy ponad 250 firm światowych (np. Philips, Motorola, TI, ST, Siemens itd.).

PODSUMOWANIE

Urządzenia zaprojektowane do pracy zgodnie ze standardem ZigBee znajdują coraz częściej zastosowanie w automatyce przemysłowej, systemach kontroli i pomiaru, automatyce budynków oraz wszędzie tam gdzie potrzebna jest energooszczędna transmisja radiowa. Rozwiązania takie mogą sprawdzić się doskonale w wielu różnorodnych aplikacjach, szczególnie tam, gdzie wymagana jest niezbyt duża prędkość transmisji danych, a jednymi z istotnych kryteriów są niski pobór energii, bezpieczeństwo transmisji danych, możliwość tworzenia wielu ścieżek komunikacyjnych oraz duża liczba urządzeń w sieci.

Przedstawiona w artykule charakterystyka ZigBee, wskazująca na bardziej specjalistyczno-aplikacyjny niż masowy charakter zastosowań tego standardu, stanowi argument do zastanowienia się nad zastosowaniem tego standardu jako rozwiązań gotowych, jak również jako standard komunikacji w projektowanych urządzeniach.

LITERATURA

1. „ZigBee Specification”, ZigBee Standard organization, December 2006.
2. Nawarocki W., Rozproszone systemy pomiarowe. WKŁ, Warszawa 2006.
3. ZigBee Alliance, <http://www.zigbee.org>