



**Fundusze
Europejskie**
Wiedza Edukacja Rozwój

Unia Europejska
Europejski Fundusz Społeczny



**Akademia Techniczno-Informatyczna w
Naukach Stosowanych we Wrocławiu**

**Skrypt do zajęć Bezprzewodowe sieci
czujnikowe**

Paweł Dobrowolski

Wrocław 2024

Skrypt przygotowany w ramach projektu „Kształcenie przyszłości: internet rzeczy w zrównoważonej automatyce i robotyce” współfinansowanego ze środków Unii Europejskiej w ramach Programu Fundusze Europejskie dla Rozwoju Społecznego 2021-2027, Priorytet 1 Umiejętności, Działanie 01.05 Umiejętności w szkolnictwie wyższym, Typ projektu Dostosowanie oferty podmiotów systemu szkolnictwa wyższego do potrzeb rozwoju gospodarki oraz zielonej i cyfrowej transformacji.



Spis treści

1. Wstęp	3
2. Zigbee	4
2.1. Instalacja sieci wykorzystującej Zigbee	6
2.2. Bezpieczeństwo sieci Zigbee	8
3. Z-Wave	9
3.1. Transmisja danych w sieci	11
3.2. Bezpieczeństwo sieci	12
4. LoRa	13
4.1. Architektura sieci LoRaWAN	14
5. Bluetooth Low Energy (BLE).....	17
5.1. Architektura Bluetooth Low Energy	18
5.2. Pakiety Bluetooth Low Energy	24
6. RFID	26
7. NFC.....	30
8. Wykaz literatury.....	32



1. Wstęp

Idea Internetu rzeczy (IoT) wymaga, aby wszystkie urządzenia, które zaliczają się do tej grupy wymieniały ze sobą dane lub przekazywały je np. do chmury, skąd byłyby one dostępne dla innych urządzeń. Przesyłanie i transmisja danych może odbywać się na dwa sposoby – przewodowo wykorzystując sygnał elektryczny oraz bezprzewodowo wykorzystując fale elektromagnetyczne o określonej częstotliwości.

W niniejszym opracowaniu przedstawiono różne metody bezprzewodowego przesyłania danych. Każda z omówionych metod charakteryzuje się indywidualnym protokołem transmisyjnym, szybkością przesyłania danych oraz zasięgiem działania. Dzięki różnorodności technologii transmisji danych możemy przysyłać dane na odległość od kilku milimetrów (NFC) do kilku kilometrów (LoRa).

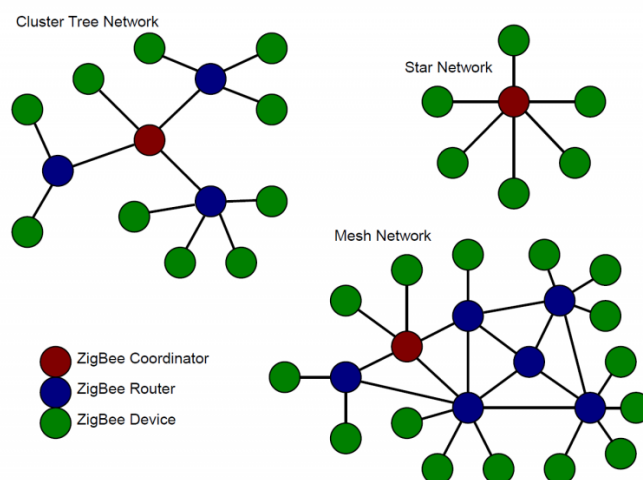


2. Zigbee

Zigbee jest standardem bezprzewodowej sieci typu mesh stosowanym w automatyce budynkowej, sterowaniu oświetleniem, urządzeniach w smart cities oraz w medycynie. Jest systemem typu low-power (podobnie jak Bluetooth Low Energy) implementowanym w małych, przenośnych urządzeniach o zasilaniu bateryjnym lub akumulatorowym, gdzie nie jest przesyłana duża ilość danych. Dzięki niewielkiemu zużyciu energii systemy te mogą pracować kilka lat zbierając, agregując i przysyłając dane. Standard Zigbee zapewnia niskie opóźnienia w komunikacji bezprzewodowej (do 100ms od rozpoczęcia nadawania). Moduły Zigbee najczęściej są zintegrowane z radiem oraz swobodnie programowalnym mikrokontrolerem, co umożliwia ich zastosowanie w wielu projektach elektronicznych.

Zigbee operuje na paśmie ISM. Wykorzystuje częstotliwość 2.4 GHz dla zastosowań w automatyce domowej (bezprzewodowe włączniki, monitory energii) oraz oświetleniu. W obiektach komercyjnych oraz dla zastosowań medycznych wykorzystuje się częstotliwości poniżej 1 GHz. Na terenie Europy jest to 868 – 870 MHz, na terenie Australii, Ameryki Północnej i Izraela 902 – 928 MHz, a na terenie Chin 779 – 787 MHz. Przepustowość danych dla częstotliwości poniżej 1 GHz to 20 kb/s i około 250 kb/s dla częstotliwości 2.4GHz.

Odległość na jaką możliwa jest transmisja danych pomiędzy dwoma urządzeniami określa się od 10 m do 100 m, przy czym 100 m jest możliwe do uzyskania, gdy pomiędzy dwoma urządzeniami nie znajdują się przeszkody zakłócające transmisję danych (*line – of – sight*). Z uwagi na fakt, iż technologia Zigbee tworzy sieć typu mesh rozpiętość sieci może być niemal nieograniczona. Każde urządzenie może przysyłać swoje dane do innego urządzenia, które znajduje się bliżej urządzenia centralnego, dzięki czemu dane zebrane z odległych urządzeń zostaną przesłane do urządzenia centralnego. Implementacja sieci mesh wymaga, aby w sieci zdefiniowano jedno urządzenie, które będzie zarządzało siecią. W sieciach typu gwiazda urządzenie zarządzające stanowi węzeł centralny sieci. W celu zwiększenia zasięgu sieci można wykorzystać routery przeznaczone do standardu Zigbee.



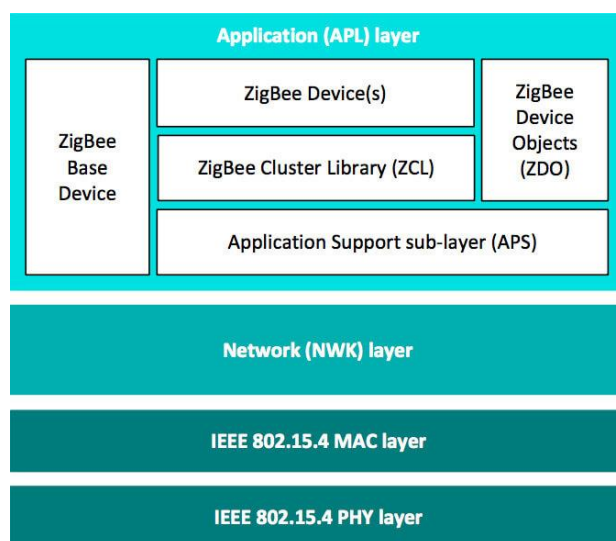
Rysunek 1 Topologie sieci Zigbee

ZigBee zbudowano na warstwie fizycznej i warstwie MAC (*medium access control*) zdefiniowanej zgodnie ze standardem IEEE 802.15.4 dla mało przepustowych bezprzewodowych sieci osobistych (WPANs). Pełna specyfikacja obejmuje cztery kluczowe komponenty: warstwę fizyczną, warstwę MAC, warstwę sieciową oraz warstwę aplikacji. Warstwa aplikacji zawiera:

- ZigBee Device Objects (ZDOs). ZDOs są odpowiedzialne za śledzenie ról urządzeń, zarządzanie prośbami o dołączenie do sieci, a także wykrywanie urządzeń i ich bezpieczeństwo,
- zdefiniowane przez producenta oprogramowania obiekty aplikacji,
- ZigBee Cluster Library (ZCL). Została zdefiniowana przez NXP jako kontener standardowych klastrów, zgodnie ze specyfikacją ZigBee Alliance na potrzeby aplikacji ZigBee 3.0, pracujących w różnorodnych sektorach rynku. Każdy klaster odpowiada specyficznym funkcjom poprzez zestaw atrybutów i/lub komend. Klastry mogą być wybierane przez ZCL, by nadać aplikacji oczekiwany zestaw możliwości. ZCL również dostarcza aplikacjom wspólnych sposobów do komunikacji. Definiuje nagłówek i właściwą zawartość, która znajduje się w PDU (Protocol Data Unit) wykorzystywanym do przesyłania wiadomości. Definiuje także typy atrybutów, takie jak liczby całkowite i łańcuchy znaków oraz określa wspólne komendy (np. do odczytu atrybutów) jak również domyślne odpowiedzi informujące o sukcesie lub niepowodzeniu. Instancje klastrów



klient/serwer mogą ze sobą współpracować z ustawieniami domyślnymi. Do przykładów zaliczyć należy funkcje włączania i wyłączania, kontrolowania poziomu, koloru, zasłaniania okien, wykrywania zajętości, obsługi termostatów i wiele innych. Podstawowe działanie w sieci ZigBee 3.0 opiera się na odczytywaniu i zapisywaniu wartości atrybutów urządzenia. W każdym urządzeniu wartości atrybutów są wymieniane pomiędzy aplikacjami i ZCL poprzez wspólną strukturę.



Rysunek 2 Architektura Zigbee

2.1.Instalacja sieci wykorzystującej Zigbee

Instalacja sieci obejmuje następujące elementy:

- tworzenie sieci,
- pozwalanie urządzeniom na dołączenie do sieci,
- dołączanie do sieci,
- powiązywanie lokalnego punktu końcowego z punktem końcowym na zdalnym węźle,
- dodawanie zdalnego węzła do grupy.

Czynności związane z instalacją, które można wykonać w ramach pojedynczego węzła, zależą od jego typu – a więc tego czy jest koordynatorem, routerem czy urządzeniem końcowym. Znaczenie mają także tryby instalacji, dopuszczone dla danego węzła. Dostępny jest szereg



trybów instalacji, oferowanych przez ZigBee Base Device. Zostały one podsumowane na poniższej grafice.

Commissioning Mode	Functionality
Touchlink	Creating a new network Allowing other devices to join an existing network Joining local device to an existing network
Network Steering	Allowing other devices to join an existing network Joining local device to an existing network
Network Formation	Creating a new network
Finding and Binding	Binding a local endpoint to an endpoint on a remote node Adding a remote node to a group

Rysunek 3 Tryby instalacji Zigbee

Instalacja *Touchlink* może zostać użyta do stworzenia nowej sieci lub do dołączenia węzła do sieci istniejącej. Operacja *Touchlink* jest inicjalizowana na węźle określonym mianem inicjatora, który może być albo członkiem istniejącej sieci, albo w przeciwnym wypadku sam stworzy nową sieć. W obu przypadkach inicjator dołączy drugi węzeł – nazywany węzłem docelowym do sieci. Metoda *Touchlink* jest dostarczana jako klaster w ramach ZCL.

Sterowanie siecią (*Network Steering*) może zostać użyte do dołączenia lokalnego węzła do istniejącej sieci lub by pozwolić innym węzłom na dołączenie do sieci poprzez lokalny węzeł. Obrana ścieżka zależy od tego, czy lokalny węzeł jest już członkiem sieci. Jeżeli tak, to węzeł będący członkiem sieci otwiera sieć dla innych węzłów na określony czas poprzez rozgłaszanie żądania *Management Permit Joining Request*, trwającego domyślnie 180 sekund. Jeśli węzeł nie jest członkiem sieci, ale jest routerem albo urządzeniem końcowym to szuka odpowiedniej sieci do dołączenia i próbuje do niej dołączyć.

Tworzenie sieci (*Network Formation*) pozwala na zbudowanie sieci przez koordynatora lub router. Koordynator stworzy sieć ze scentralizowanym systemem bezpieczeństwa i aktywuje swoje funkcje *Trust Center*, podczas gdy router tworzy sieć z rozproszonymi mechanizmami bezpieczeństwa.

Tryb znajdowania i łączenia (*Finding and Binding*) pozwala węzłowi w sieci na zostanie sparowanym z innym węzłem – przykładowo nowa lampa może wymagać sparowania z



kontrolerem, by umożliwić sterowanie nią. Ten tryb instalacji został pomyślany z myślą o łączeniu punktów końcowych na nowym węźle z kompatybilnym punktem końcowym na zdalnym węźle w sieci zależnie od tego, jakie klastry obsługują. Alternatywnie, nowy węzeł może zostać dodany do grupy węzłów, które są sterowane wspólnie. W trybie *Finding and Binding*, węzeł może mieć jedną z dwóch ról:

- inicjatora: w tym trybie może zarówno stworzyć (lokalne) powiązanie ze zdalnym punktem końcowym jak i zażądać by zdalny punkt został dodany do grupy,
- celu: taki węzeł identyfikuje się oraz otrzymuje i odpowiada na żądania inicjatora.

Oczekiwany rezultat to parowanie inicjatora i celu. Zazwyczaj inicjatorem jest urządzenie kontrolujące. Ścieżka jaką przebiega proces w trybie *Finding and Binding* zależy od tego, czy lokalny punkt końcowy jest inicjatorem czy celem.

2.2. Bezpieczeństwo sieci Zigbee

ZigBee 3.0 wprowadziło zaawansowany zestaw narzędzi, który umożliwia projektantom na wprowadzenie niezawodnych sieci ze zbalansowaną polityką bezpieczeństwa oraz łatwością instalacji. Dostępne funkcje są stale aktualizowane, by odpowiadać na nowo pojawiające się zagrożenia. Zastosowane rozwiązanie bezpieczeństwa bazuje na sieci mesh ze standardu ZigBee PRO, który oryginalnie powstał na potrzeby profilu ZigBee Smart Energy. Jest on obecnie używany przez setki milionów mierników zużycia mediów na całym świecie bez wykrycia jakichkolwiek luk bezpieczeństwa.

Do nowych funkcji bezpieczeństwa należą:

- unikalna dla urządzenia autentykacja podczas podłączania do sieci,
- aktualizacja wykorzystywanych kluczy podczas pracy,
- bezpieczna aktualizacja oprogramowania przez sieć bezprzewodową,
- szyfrowanie w warstwie logicznej łącza.

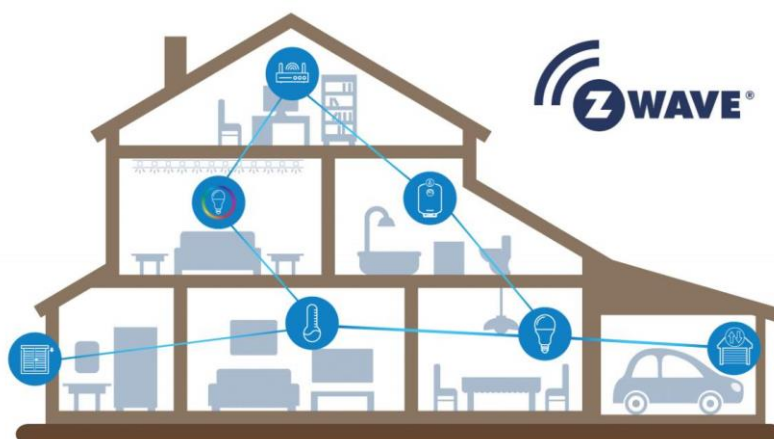
Zigbee zapewnia bezpieczną komunikację, ochronę ustanawiania i transportu kluczy kryptograficznych, ramek szyfrujących i kontrolowania urządzeń. Opiera się na podstawowej strukturze bezpieczeństwa zdefiniowanej w IEEE 802.15.4 Sieć Zigbee zabezpieczona jest 128-bitowym kluczem AES-CCM.



3. Z-Wave

Z-Wave to bezprzewodowy protokół komunikacyjny stosowany do automatyzacji budynków mieszkalnych i komercyjnych. Oparty jest o sieć mesh wykorzystującą fale elektromagnetyczne do komunikacji pomiędzy urządzeniami. Umożliwia bezprzewodowe sterowanie inteligentnymi urządzeniami domowymi takimi jak inteligentne oświetlenie, systemy bezpieczeństwa, termostaty, czujniki, inteligentne zamki do drzwi czy napędy bram garażowych. Marka i technologia Z-Wave są własnością Silicon Labs. Obecnie ponad 300 firm zaangażowanych jest w rozwój technologii i są uczestnikami w Z-Wave Alliance.

Do sterowania systemem Z-Wave można wykorzystać smartfon, tablet lub komputer. Systemem można sterować również lokalnie za pomocą dedykowanego bezprzewodowego pilota, panelu ściennego z bramką Z-Wave lub centralnym urządzeniem sterującym służącym zarówno jako hub oraz kontroler. Z-Wave zapewnia spójność warstwy aplikacji pomiędzy systemami sterowania domem różnych producentów, którzy są uczestnikami w Z-Wave Alliance.



Rysunek 4 Zastosowanie sieci Z-Wave

Z-Wave został zaprojektowany tak, aby zapewnić niezawodną transmisję małych pakietów danych o niskim opóźnieniu przy szybkości transmisji danych do 100 kb/s. Maksymalna odległość na jaką można przesyłać dane pomiędzy dwoma węzłami wynosi 200 metrów na zewnątrz, gdy pomiędzy dwoma urządzeniami nie znajdują się przeszkody zakłócające transmisję danych (*line – of – sight*) i 50 metrów wewnątrz budynków. Dzięki możliwości przesyłania wiadomości pomiędzy urządzeniami (sieć mesh) standard zapewnia zasięg odpowiedni dla większości domów mieszkalnych. Technologia Z-Wave występuje



również w wersji LR (*Long – Range*). Wówczas maksymalny zasięg może wynosić nawet 1600 metrów, przy założeniu, że pomiędzy dwoma urządzeniami nie znajdują się przeszkody zakłócające transmisję danych (*line – of – sight*).

Technologia Z-Wave opiera się na falach elektromagnetycznych o częstotliwościach od 865 MHz do 926 MHz zależnie od regionu występowania (tabela 1). Wykorzystuje się w niej modulację FSK z kodowaniem Manchester. Z-Wave obsługuje również modulację GFSK i DSSS-OQPSK. Technologia Z-Wave wykorzystuje nielicencjonowane pasmo ISM.

Tabela 1 Częstotliwość pracy Z-Wave

Częstotliwość	Obszar zastosowania
865.2 MHz	Indie
868.4 MHz	Chiny, Południowa Afryka
868.4 MHz, 869.85 MHz	Armenia, Bahrajn, Europa, Egipt, Guana, Georgia, Irak, Jordan, Kazachstan, Kuwejt, Lizbona, Libia, Nigeria, Oman, Filipiny, Katar, Arabia Saudyjska, Południowa Afryka, Turkmenistan, Zjednoczone Emiraty Arabskie, Wielka Brytania, Uzbekistan, Jemen
869 MHz	Rosja
908.4 MHz 916 MHz	Argentyna, Bahamy, Barbados, Bermudy, Boliwia, Kanada, Wyspy Kanaryjskie, Kolumbia, Gwatemala, Haiti, Honduras, Jamajka, Malediwy, Mauritius, Meksyk, Mołdawia, Maroko, Nikaragua, Panama, Turcja, Urugwaj, USA
916 MHz	Izrael
919.8 MHz 921.4 MHz	Australia, Brazylia, Chile, Dominikana, Ekwador, Salwador, Indonezja, Malezja, Nowa Zelandia, Paragwaj, Peru, Urugwaj, Wenezuela, Wietnam
920.9 MHz 921.7 MHz 923.1 MHz	Makau, Singapur, Korea Południowa, Tajwan, Tajlandia
922.5 MHz 923.9 MHz 926.3 MHz	Kostaryka, Japonia

W sieci Z-Wave wyróżniamy trzy typy urządzeń:

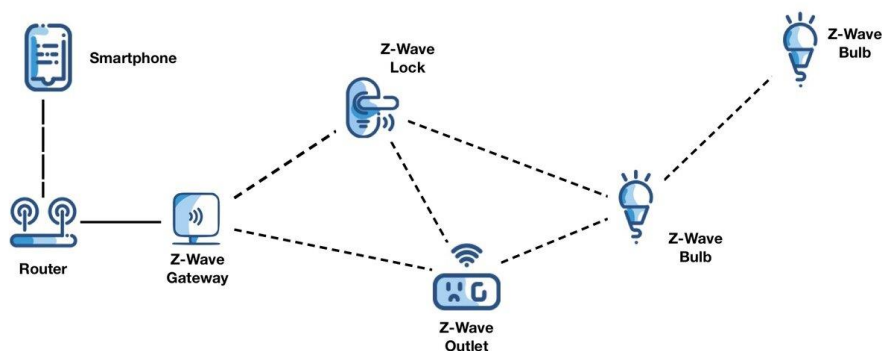
- *kontroler* – podstawowe urządzenie sieci. Zarządza bezpieczeństwem sieci oraz odpowiada za kontrolę podłączonych urządzeń.



- *routery* – urządzenia stale podłączone do zasilania jak żarówki, przełączniki czy termostaty. Mogą one działać jako urządzenia przekazujące sygnał od urządzeń zamontowanych poza zasięgiem kontrolera.
- *slave'y* – zasilane bateryjnie, nisko energetyczne (low-power) urządzenia takie jak bezprzewodowe czujniki np. temperatury czy wilgotności. Ich głównym zadaniem jest zbieranie i transmisja danych. Nie zawierają elementów wykonawczych np. przekaźników.

3.1. Transmisja danych w sieci

Technologia Z-Wave oparta jest o sieć mesh, która do swojego działania wymaga jednego centralnego punktu (główny kontroler), do którego podłączane są pozostałe urządzenia. Najprostsza sieć to pojedyncze sterowalne urządzenie i główny kontroler. Urządzenia te mogą się komunikować ze sobą za pomocą węzłów pośrednich (innych urządzeń), aby omijać przeszkody lub martwe punkty radiowe. Wiadomość z węzła A (urządzenia A) do węzła C (urządzenia C) może zostać pomyślnie dostarczona, nawet jeśli oba węzły nie znajdują się w zasięgu, pod warunkiem, że trzeci węzeł B (urządzenie B) może komunikować się z węzłami A i C. Jeśli połączenie jest niedostępne nadawca wiadomości spróbuje przesłać dane za pomocą innych urządzeń, aż zostanie znaleziona ścieżka do węzła C. Z uwagi na charakterystykę sieci mesh, sieć Z-Wave może rozciągać się znacznie dalej niż zasięg radiowy pojedynczej jednostki. Należy pamiętać, że im więcej urządzeń pośredniczy przy procesie transmisji danych pomiędzy dwoma urządzeniami, tym powstałe opóźnienia w transmisji są większe.



Rysunek 5 Sieć mesh Z-Wave



Rozbudowa sieci Z-Wave jest możliwa w dowolnym momencie. Po uruchomieniu urządzenia należy wykonać procedurę parowania nowego urządzenia z kontrolerem. Po wykonaniu procedury parowania urządzenie jest dostępne w systemie i może dokonywać transmisji danych do innych urządzeń. Pojedyncza sieć Z-Wave może składać się maksymalnie z 232 urządzeń lub 4000 węzłów.

Sieć Z-Wave jest identyfikowana przez Network ID, a każde urządzenie jest dodatkowo identyfikowane przez własny Node ID. Network ID (nazywany również Home ID) jest wspólnym identyfikatorem wszystkich węzłów należących do jednej sieci Z-Wave. Network ID ma długość 32 bitów i jest przypisywany do każdego urządzenia przez kontroler główny, podczas procesu parowania. Urządzenia (węzły) z różnymi Network ID nie mogą się ze sobą komunikować. Node ID to adres pojedynczego węzła w sieci. Ma długość 8 bitów i musi być unikalny w swojej sieci.

3.2. Bezpieczeństwo sieci

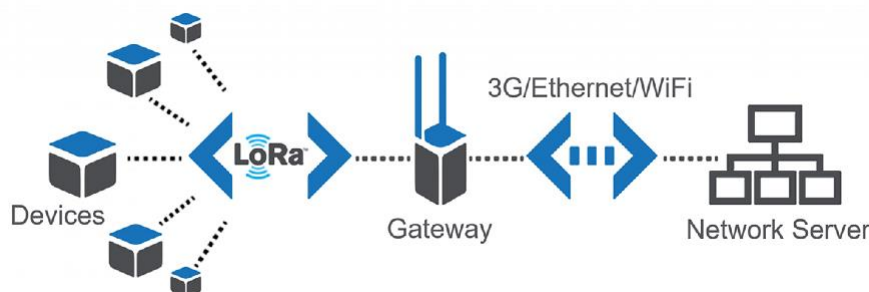
Sieć Z-Wave otrzymała certyfikat Security 2 (S2). Zapewnia on zaawansowane zabezpieczenia dla inteligentnych urządzeń domowych, bram i koncentratorów. Poprawiono standardy szyfrowania (AES 128-bit) dla transmisji pomiędzy węzłami i wdrożono nowe metody parowania nowych urządzeń. Parowanie urządzeń odbywa się za pomocą unikalnego kodu PIN lub QR. Nowa warstwa uwierzytelniania ma na celu uniemożliwienie przejęcia kontroli nad niezabezpieczonymi lub słabo zabezpieczonymi urządzeniami. Według Z-Wave Alliance nowy standard bezpieczeństwa jest najbardziej zaawansowanym zabezpieczeniem dostępnym na rynku dla inteligentnych urządzeń domowych i kontrolerów, bram i koncentratorów. Chipy serii 800 wydane pod koniec 2021 r. nadal obsługują standardowe funkcje bezpieczeństwa S2, a także technologię Silicon Labs Secure Vault, umożliwiając urządzeniom bezprzewodowym uzyskanie bezpieczeństwa PSA Certification Level 3.



4. LoRa

LoRa to skrót od Long Range – jest to technika komunikacji radiowej oparta na technice modulacji rozproszonego widma wzorującej się na technologii chirp spread spectrum (CSS). Została opracowana przez firmę Cycleo. Obecnie właścicielem technologii jest firma Semtech. Technikę LoRa wykorzystano do budowy sieci rozległej, tj. LoRaWAN. Ciągły rozwój protokołu sieciowego LoRaWAN jest zarządzany przez otwarte, non-profitowe stowarzyszenie LoRa Alliance, którego Semtech jest założycielem.

LoRaWAN definiuje protokół sieciowy o niskim poborze mocy i szerokim obszarze działania (LPWA) zaprojektowany do bezprzewodowego łączenia urządzeń zasilanych bateryjnie z internetem w sieciach regionalnych, krajowych lub globalnych. Protokół jest dedykowany dla wymagań idei Internetu rzeczy (IoT) takich jak dwukierunkowa komunikacja, kompleksowe zabezpieczenia czy usługi mobilne i lokalizacyjne. Niski pobór mocy i niska prędkość transmisji danych skutkuje wykorzystaniem technologii w aplikacjach IoT. Prędkość transmisji danych z wykorzystaniem LoRa waha się od 0,3 kb/s do 50 kb/s na kanał.



Rysunek 6 Idea technologii

Technologia LoRa obejmuje warstwę fizyczną, podczas gdy inne technologie i protokoły, takie jak LoRaWAN (sieć rozległa dalekiego zasięgu), obejmują warstwy wyższe. LoRa wykorzystuje wolne od licencji pasma częstotliwości radiowych:

- EU868: 863 – 870 MHz / 873 MHz w Europie,
- AU915/AS923-1: 915 MHz – 928 MHz w Ameryce Południowej,
- US915: 902 MHz – 928 MHz w Ameryce Północnej,
- IN865: 865 MHz – 867 MHz w Indiach,
- AS923: 915 MHz – 928 MHz w Azji.



LoRa wykorzystuje technikę modulacji rozproszonego widma, która wzoruje się na technologii chirp spread spectrum (CSS) i jest jej pochodną. Każdy transmitowany symbol jest reprezentowany przez cyklicznie przesunięty chirp w przedziale częstotliwości:

$$\left(f_0 - \frac{B}{2}, f_0 + \frac{B}{2}\right) [Hz]$$

gdzie: f_0 to częstotliwość środkowa sygnału, a B to szerokość pasma.

Współczynnik rozprzestrzeniania (SF) to parametr, który ma znaczący wpływ na prędkość transmisji danych. Jest to wybieralny parametr radiowy z zakresu od 5 do 12, który reprezentuje liczbę bitów wysyłanych na symbol. Dodatkowo określa on, w jakim stopniu informacja jest rozprzestrzeniana w czasie. Dzieli on liniowo całą szerokość pasma na $M = 2^{SF}$ przedziałów. Nadawanie rozpoczyna się od najniższej częstotliwości $f_0 - \frac{B}{2} [Hz]$ i wzrasta o krok M , aż do momentu osiągnięcia częstotliwości maksymalnej $f_0 + \frac{B}{2} [Hz]$. Po jej osiągnięciu częstotliwość ponownie ustawiana jest na najniższą dopuszczalną wartość. W związku z powyższym szybkość przesyłania symboli R_s określa zależność $R_s = B / M$.

Niższa wartość SF odpowiada wyższej prędkości transmisji danych, co wpływa na krótszy czas transmisji danych. Wyższa wartość współczynnika rozproszenia oznacza lepszą dokładność, ale niższą prędkość transmisji danych. Dłuższy czas transmisji danych powoduje, że nadajnik nadaje przez dłuższy czas i zużywa więcej energii. Ogólnodostępne modemy LoRa obsługują moce do +22 dBm. Moc ta może jednak być ograniczona zależnie od uwarunkowań prawnych miejsca, w którym stosowana jest technologia.

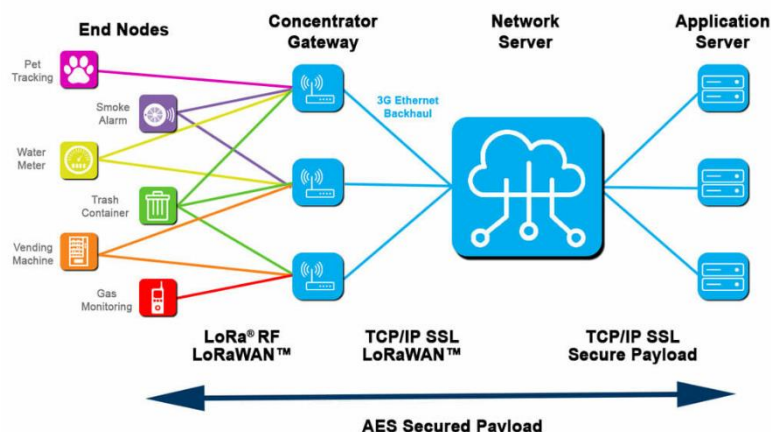
Według LoRa Development Portal maksymalny zasięg zapewniany przez technologię LoRa może wynosić aż do 4.8 km na obszarach miejskich i do 16 km lub więcej na obszarach wiejskich, gdy pomiędzy nadajnikiem a odbiornikiem nie występują przeszkody terenowe.

4.1. Architektura sieci LoRaWAN

Architektura sieci LoRaWAN to topologia połączonych gwiazd. Umożliwia to stacjom bazowym przekazywanie danych między czujnikami a serwerem sieciowym. Komunikacja z nimi odbywa się za pośrednictwem kanału bezprzewodowego wykorzystującego warstwę



fizyczną LoRa, podczas gdy połączenie pomiędzy bramami a serwerem centralnym odbywa się za pośrednictwem połączenia Ethernet.



Rysunek 7 Architektura sieci

Węzłami końcowymi są urządzenia, które zbierają i przesyłają dane do bram z wykorzystaniem protokołu LoRa. Zbudowane są one z czujników do pomiaru określonych wielkości fizycznych lub innych sygnałów elektrycznych oraz z transpondera LoRa, który przesyła zgromadzone informacje. Węzły końcowe to zazwyczaj czujniki zasilane bateryjnie (klasa A i klasa B). Żywotność baterii węzła może zwykle trwać od dwóch do pięciu lat (zależnie od częstotliwości pomiarów i środowiska pracy).

Tabela 2 Typy węzłów w LoRaWAN

Klasa A	Klasa B	Klasa C
Zasilany bateryjnie	Zasilany bateryjnie	Brak opóźnienia
Dwukierunkowy	Dwukierunkowy	Dwukierunkowy z trybem słuchania przez większość czasu
Wiadomości emisji pojedynczej	Wiadomości emisji pojedynczej i multiemisji	Wiadomości emisji pojedynczej i multiemisji
Mała ilość danych Długie okresy czasu pomiędzy transmisją danych	Mała ilość danych Długie okresy czasu pomiędzy transmisją danych Okresowy sygnał nawigacyjny z bramy	Mała ilość danych



Typ klasy A	Klasa typu B	Typ klasy C
Urządzenie końcowe inicjuje komunikację (Uplink) Serwer komunikuje się z urządzeniem końcowym	Serwer może inicjować transmisję w ustalonych odstępach czasu	Serwer może w każdej chwili zainicjować transmisję

Dane z węzłów przesyłane są do bram LoRa. Bramy LoRa łączą się z internetem za pomocą Ethernet i przesyłają dane do serwera lub chmury konwertując pakiety RF na pakiety IP i odwrotnie. Urządzenia bramy są zawsze podłączone do źródła zasilania.



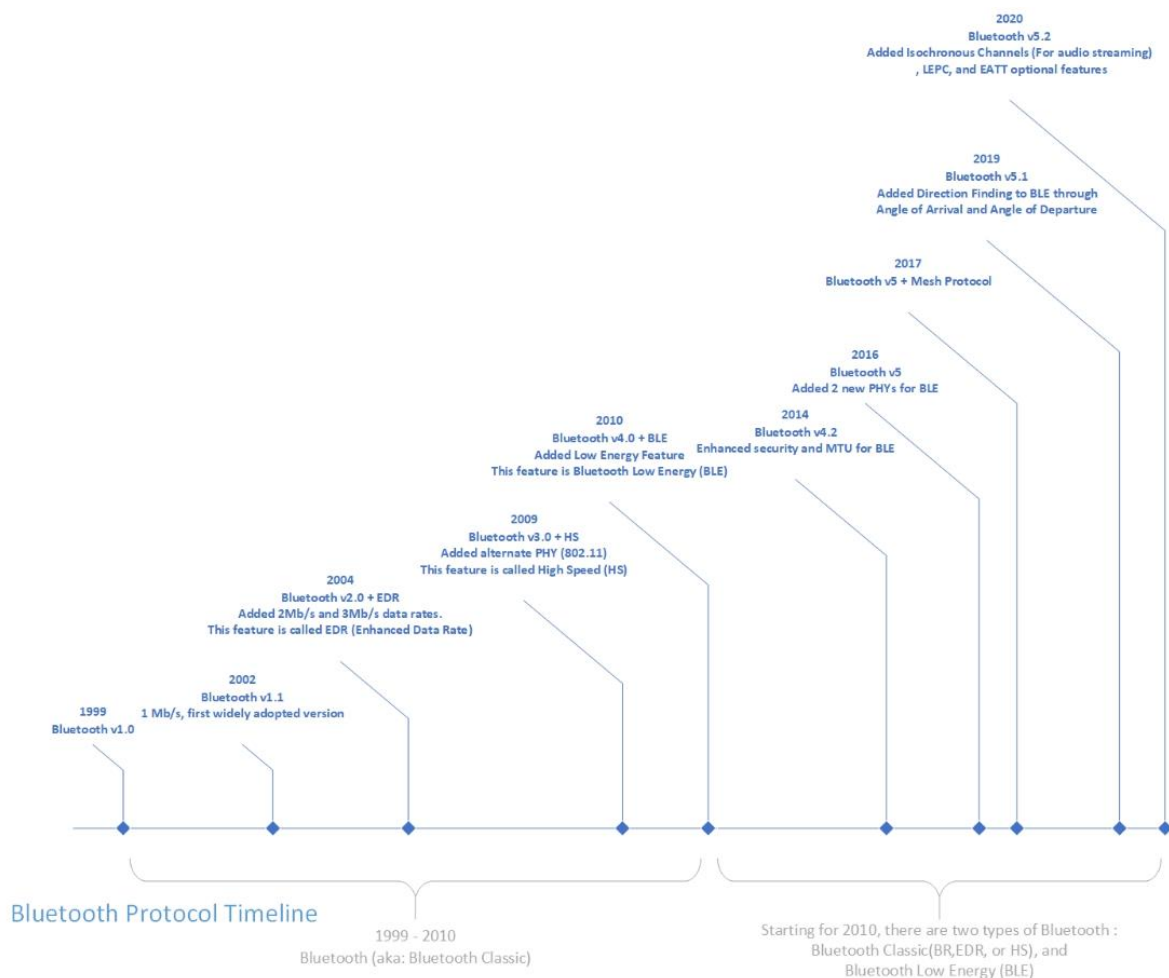
5. Bluetooth Low Energy (BLE)

Technologia Bluetooth Low Energy (BLE) opiera się na popularnej technologii transmisji danych jakim jest klasyczny Bluetooth i rozwijana jest równolegle z nim od 2010 roku. Pierwsza wersja BLE miała na celu zminimalizowanie zapotrzebowania energetycznego na transmisję i odbieranie danych tak, aby można było ją zastosować w aplikacjach typu low-energy.

W 2014 roku opracowano wersję BLE 4.2, w której zwiększono poziom bezpieczeństwa protokołu oraz ilość przesyłanych danych (*MTU – maximum transmission unit*). W kolejnych wersjach protokołu BLE (wersja 5.0 i nowsze) dodano nowe funkcjonalności tj.:

- obsługa sieci Mesh, w której urządzenia automatycznie budują własną sieć połączeń tak, aby przekazać dane na jak największym obszarze,
- AoA (Angle of Arrival), dzięki któremu możliwe jest określenie kąta nadejścia fali elektromagnetycznej wysłanej z anteny nadawczej,
- AoD (Angle of Departure), dzięki któremu możliwe jest określenie kąta pod jakim sygnał rozprzestrzenia się od anteny nadawczej,
- Direction Finding oparty na AOA oraz AoD, którego celem jest określenie pozycji obiektu w zamkniętym systemie lokalizacji RTLS (Real Time Location System).

W najnowszej wersji Bluetooth Low Energy 5.3 poprawiono jej wydajność oraz niezawodność. W celu uniknięcia potencjalnych interferencji z innym nadawanym sygnałem ulepszono sposób wyboru kanału do transmisji danych. Dla zapewnienia stabilnej komunikacji zmodyfikowano sposób nawiązywania i utrzymywania połączenia. Obniżono zapotrzebowanie energetyczne w stosunku do poprzednich wersji protokołu w sytuacji, gdy urządzenia są ze sobą połączone, ale nie przesyłają pomiędzy sobą danych. Pomimo, że specyfikacja wersji BLE 5.3 została ogłoszona w sierpniu 2023 roku do dziś (sierpień 2024) w sprzedaży są głównie moduły z wersją BLE 5.2 i starszymi. Najprawdopodobniej wersja BLE 5.3 zagości niebawem na rynku komponentów i modułów elektronicznych wypierając starsze generacje.



Rysunek 8 Wersje Bluetooth Low Energy z datami ich wprowadzenia

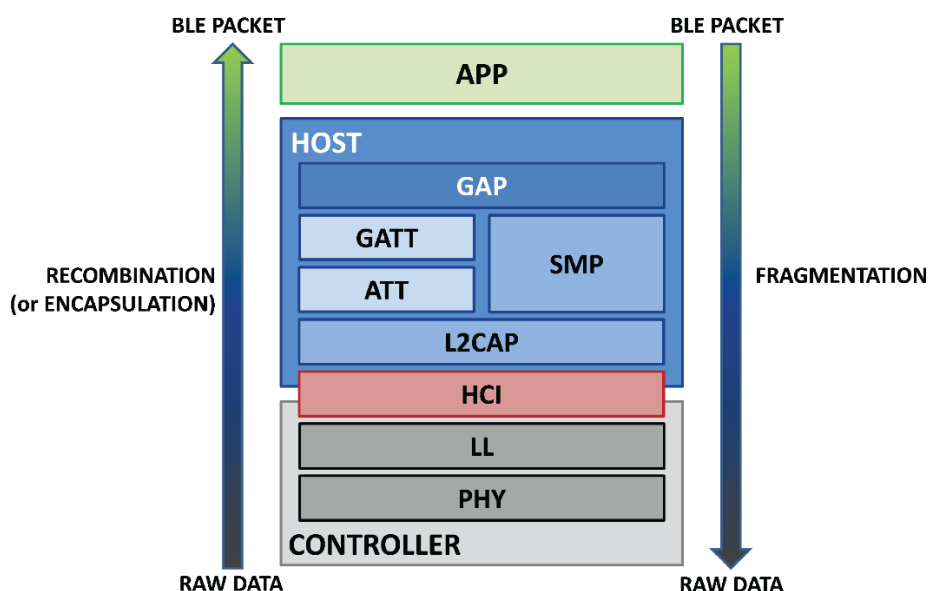
5.1. Architektura Bluetooth Low Energy

Na podstawie informacji udostępnionych przez Nordic Semiconductor, producenta chipów serii nRF5x, które są dedykowane do urządzeń IoT, poniżej omówiono architekturę protokołu BLE. Składa się ona z trzech głównych poziomów:

- poziom aplikacji – jest to oprogramowanie, które tworzą programiści dla danego urządzenia dostosowując je do potrzeb i ograniczeń projektowanego produktu. Część oprogramowania do obsługi protokołów komunikacyjnych czy stosu BLE jest importowana z pakietu SDK (Software Development Kit) dedykowanego dla nRF5x.
- poziom hosta – wyższe warstwy stosu protokołu BLE. Do ich obsługi wykorzystuje się biblioteki producenta. W przypadku nRF5x jest to stos protokołów SoftDevice.



- poziom kontrolera – niższe warstwy stosu protokołu BLE w skład której wchodzi również nadajnik/odbiornik. Warstwa ta jest częściowo zrealizowana sprzętowo (hardware), a pozostałą część implementuje oprogramowanie SoftDevice.



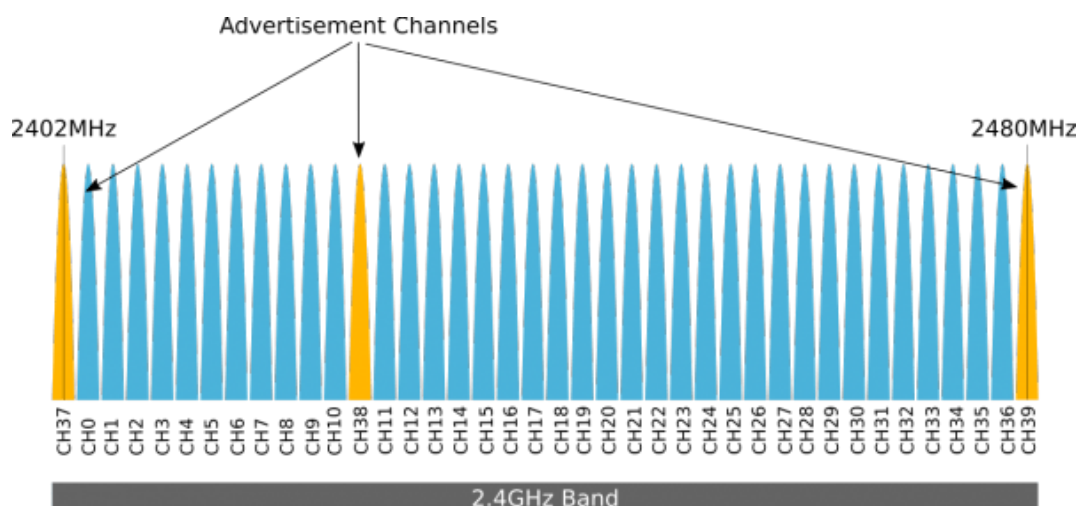
Rysunek 9 Architektura Bluetooth Low Energy

Poziom kontrolera – warstwa fizyczna

Warstwa fizyczna (PHY) jest odpowiedzialna za modulację i demodulację sygnału radiowego. Jest najniższą warstwą w protokole i komunikuje się bezpośrednio z warstwą łącza danych (Link Layer). Do transmisji danych wykorzystuje się nielicencjonowane pasmo ISM 2.4GHz, z którego korzystają również inne bezprzewodowe protokoły komunikacyjne np. Wi-Fi. Jest ono podzielone na 40 kanałów – pierwszy kanał zajmuje częstotliwość 2.402 GHz, a pasmo przepustowe wynosi 2 MHz. Ostatni kanał zajmuje częstotliwość 2.480 GHz. Kanały 37, 38 oraz 39 zdefiniowano jako kanały rozgłoszeniowe. Stosuje się je w celu wykrywania urządzenia (rozgłaszanie ramki danych z identyfikatorem urządzenia), nawiązywania połączenia czy nadawania w trybie broadcast (tryb rozgłoszeniowy jeden-do-wielu). Pozostałe kanały to kanały dwukierunkowej transmisji danych. W celu uniknięcia interferencji z innymi urządzeniami pracującymi w paśmie 2.4 GHz BLE



wykorzystuje metodę skokowej zmiany częstotliwości (*Frequency hopping scheme*), która określa jaki kanał powinien zostać wykorzystany dla nawiązania następnego połączenia.



Rysunek 10 Kanały Bluetooth Low Energy

Zależnie od wybranego układu i jego wersji możliwe jest wybranie jednego z trzech typów warstwy fizycznej:

- standard BLE 4.x z prędkością transmisji danych do 1 Mbps (dostępne we wszystkich rodzinach układów nRF5x),
- standard BLE 5.x z prędkością transmisji danych do 2 Mbps (dostępne tylko w układach nRF52),
- standard Long Range oparty o BLE 5.x z prędkością transmisji danych do 125 Kbps i zasięgiem do 1000 metrów, gdy pomiędzy nadajnikiem a odbiornikiem nie znajdują się przeszkody zakłócające transmisję (dostępne tylko w wybranych układach tj. nRF52840, nRF52833, nRF52820, nRF52811).

Poziom kontrolera – warstwa łączy danych

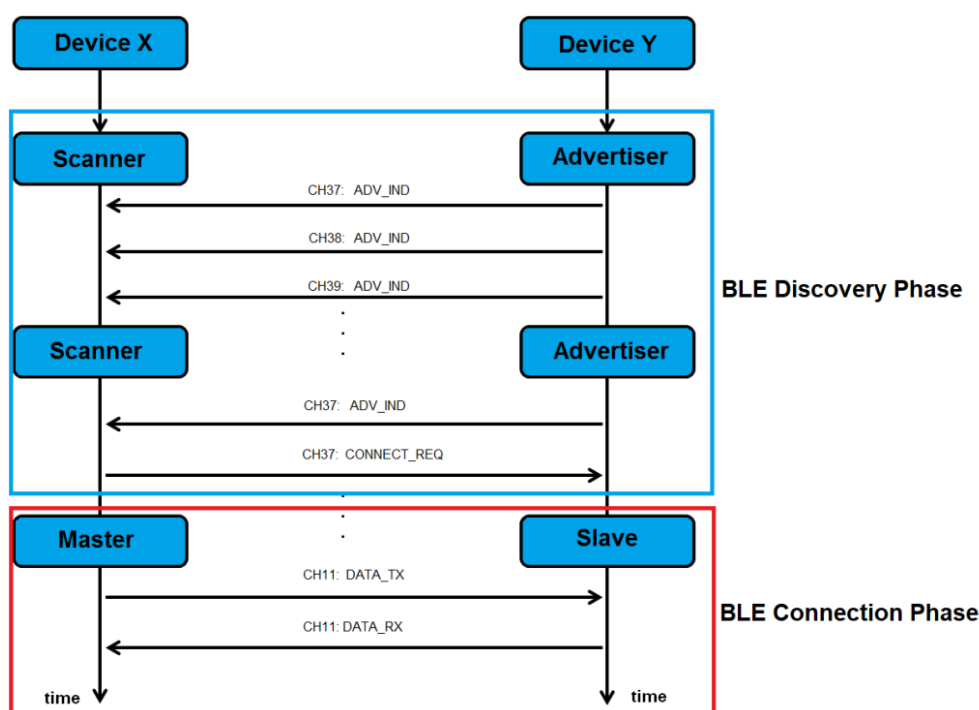
Warstwa łączy danych bezpośrednio współpracuje z warstwą fizyczną (PHY). Większość funkcjonalności warstwy zrealizowana została hardware'owo dzięki czemu BLE może funkcjonować w czasie rzeczywistym. Pozostała część warstwy łączy danych została zaimplementowana przez SoftDevice producenta układu. Warstwa łączy danych odpowiada za:

- rozgłaszanie, skanowanie, tworzenie i utrzymywanie połączeń,



- enkapsulację danych otrzymanych z wyższych warstw i generowanie pakietów BLE, które są przesyłane bit po bicie do warstwy fizycznej (PHY),
- wykrywanie błędnych pakietów BLE za pomocą weryfikacji CRC,
- szyfrowanie / deszyfrowanie pakietów za pomocą algorytmu AES-CCM 128-bits,
- zarządzanie adresami urządzeń BLE,
- definiowanie trybu pracy urządzenia:
 - rozgłoszeniowy – urządzenie wysyła pakiety rozgłoszeniowe,
 - skanowanie – urządzenie odbiera pakiety rozgłoszeniowe,
 - master – urządzenie inicjalizuje i utrzymuje połączenie,
 - slave – urządzenie akceptuje połączenie i komunikuje się z masterem.

Podczas pracy warstwa łącza danych może zmieniać swoją konfigurację oraz tryb pracy. Przykładowo: urządzenie X chce nawiązać komunikację z urządzeniem Y. Urządzenie Y pracuje w trybie rozgłoszeniowym (*advertiser*). Urządzenie X uruchamia się w trybie skanowania (*scanner*). Po odebraniu pakietów od urządzenia Y dochodzi do inicjalizacji połączenia pomiędzy urządzeniami (*connect_request*). Po inicjalizacji urządzenie X rozpoczyna pracę w trybie master, a urządzenie Y pracuje jako slave.



Rysunek 11 Zmiana trybu pracy w warstwie łącza danych



Poziom kontrolera – warstwa interfejsu kontrolera hosta (HCI)

Warstwa interfejsu kontrolera hosta (HCI) odpowiada za transport poleceń i zdarzeń pomiędzy poziomami hosta i kontrolera dla stosu protokołu BLE. Zapewnia on komunikację dwukierunkową pomiędzy hostem a kontrolerem, umożliwiając przesyłanie poleceń oraz danych. HCI jest implementowany z wykorzystaniem SPI lub UART. Może on być wykorzystywany również w implementacjach dwurdzeniowych (dual-chip), w których jeden z rdzeni odpowiada za poziom aplikacyjny, a drugi za obsługę BLE.

Poziom hosta – Logical Link Control and Adaptation Layer Protocol (L2CAP)

L2CAP zapewnia zarządzanie zasobami i adaptację dla warstw niższych. Umożliwia innym protokołom tj. Attribute Protocol (ATT) oraz Security Manager Protocol (SMP) współdzielenie tego samego kontrolera BLE stosując mechanizm multipleksowania. Odpowiada również za segmentację oraz składanie pakietów wymienianych pomiędzy wyższymi warstwami a kontrolerem BLE. Dzięki funkcji segmentacji oraz ponownego składania, L2CAP umożliwia protokołom i aplikacjom wyższego poziomu przesyłanie i odbieranie pakietów danych wyższej warstwy o długości do 64 KB. L2CAP posiada również rozbudowane mechanizmy wykrywania błędów, które umożliwiają identyfikację i korektę przekłamań podczas transmisji.

Poziom hosta – Security Manager Protocol (SMP)

Protokół SMP odpowiada za inicjowanie, zarządzanie i koordynację procesów zabezpieczania połączeń w BLE. Jego głównym zadaniem jest zapewnienie, że komunikacja między urządzeniami odbywa się w sposób bezpieczny i prywatny. SMP świadczy usługi:

- uwierzytelniania urządzenia,
- autoryzacji urządzenia,
- spójności danych,
- poufności danych.

Poziom hosta – Attribute Protocol (ATT)

ATT to protokół klient / serwer oparty na atrybutach przechowywanych przez serwer. Definiuje on sposób przesyłania jednostki danych (atrybutu). Protokół ATT umożliwia klientowi dostęp



do atrybutów serwera poprzez operacje odczytu, zapisu czy aktualizacji danych. Każdy atrybut definiuje 4 pola:

- **handle** – jest to klucz atrybutu, za pomocą którego można zaadresować atrybut. Jest to 16-bitowa wartość (0x0001 – 0xFFFF) przypisana przez SoftDevice do atrybutu w celu jego jednoznacznej identyfikacji wśród innych atrybutów w tabeli,
- **UUID** (*Universally Unique Identifier*) – uniwersalny unikalny identyfikator wykorzystywany jest do określenia typu atrybutu. UUID może występować jako standardowy Bluetooth UUID (16 bitów, znanym również jako BLE_UUID_TYPE_BLE), albo specyficznym dla dostawcy UUID (128 bitów, znanym również jako BLE_UUID_TYPE_VENDOR_BEGIN),
- **uprawnienia** – określa uprawnienia dostępu i poziom zabezpieczeń danego atrybutu,
- **wartość** – aktualna wartość danego atrybutu.



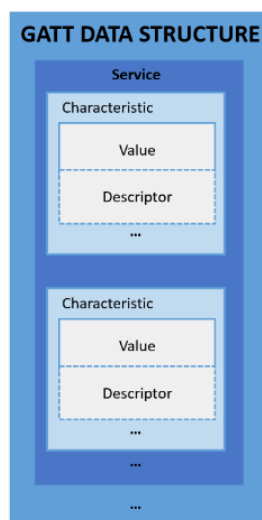
Rysunek 12 Struktura atrybutów ATT

Poziom hosta – Generic Attribute Profile (GATT)

Jest to jedna z najczęściej używanych warstw stosu BLE upraszczająca proces wymiany danych. Jest implementowana z wykorzystaniem ATT i wykorzystuje się ją jako warstwę transportową. Atrybuty w GATT są zorganizowane hierarchicznie jak poniżej:

- **usługa** – grupa cech,
- **cechy** – kontenery danych,
- **deskryptor** – dodatkowe opcjonalne metadane.

Innymi słowy, każda usługa zawiera jedną lub więcej cech, a każda cecha jest połączeniem danych użytkownika i informacji opisowych (metadanych).



Rysunek 13 Struktura danych GATT

Poziom hosta – Generic Access Profile (GAP)

Ta warstwa definiuje procedury dotyczące sposobu wykrywania i łączenia się urządzeń. Zapewnia również uproszczoną warstwę dla SMP do parowania, tworzenia wiązań i zapewniania prywatności. Dzięki tej warstwie możemy skonfigurować warstwę łącza danych, gdzie możemy zdefiniować różne tryby pracy urządzenia tj.:

- tryb rozgłoszeniowy – urządzenie wysyła pakiety rozgłoszeniowe,
- tryb skanowania – urządzenie odbiera pakiety rozgłoszeniowe,
- tryb master – urządzenie inicjalizuje i utrzymuje połączenie,
- tryb slave – urządzenie akceptuje połączenie i komunikuje się z masterem.

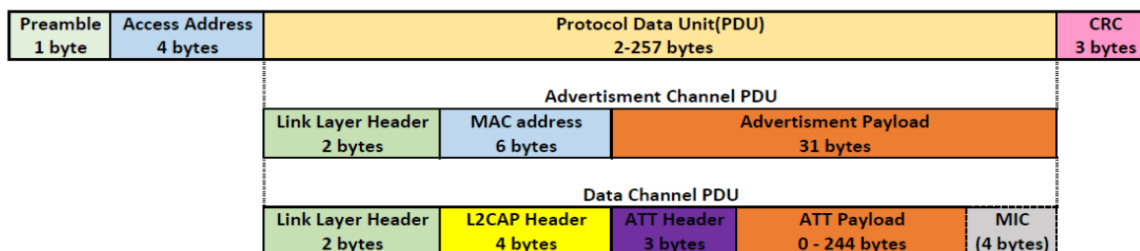
5.2. Pakiety Bluetooth Low Energy

Pakiety BLE tworzone są przez warstwę łącza danych i wyróżnia się ich dwa typy:

- rozgłoszeniowy:
 - BLE 4.0: 31 bajtów przeznaczonych do transmisji oraz możliwość odebrania 31 bajtów w wyniku skanowania,
 - BLE 5.x: 255 bajtów przeznaczonych do transmisji.
- transmisji danych:



- BLE 4.0: 27 bajtów przeznaczonych do transmisji. 20 z 27 bajtów są dostępne dla danych użytkownika,
- BLE 4.2 i nowsze: 251 bajtów przeznaczonych do transmisji. 244 z 251 bajtów są dostępne dla danych użytkownika.



Rysunek 14 Ramka danych Bluetooth Low Energy

Preamble – służy do synchronizacji częstotliwości oraz uruchamiania automatycznej kontroli wzmocnienia w odbiorniku

Access Address – to 32-bitowy identyfikator używany do jednoznacznego określenia danego połączenia między urządzeniem nadawczym a odbiorczym. Jest to wartość, która musi być znana obu stronom w trakcie nawiązywania połączenia. Access Address umożliwia odbiornikowi jednoznaczne zidentyfikowanie pakietów związanych z konkretnym połączeniem, co jest istotne w środowisku, gdzie występuje wiele urządzeń BLE

CRC – to 24-bitowa wartość kontrolna używana do wykrywania błędów w przesyłanych danych

Link Layer Header – nagłówek konfiguracyjny warstwy łącza danych zawierający m.in. długość ramki danych

MAC address – adres MAC

Advertisement Payload – dane wysyłane w trybie rozgłoszeniowym

L2CAP Header – nagłówek konfiguracyjny protokołu L2CAP

ATT Header – nagłówek konfiguracyjny protokołu ATT

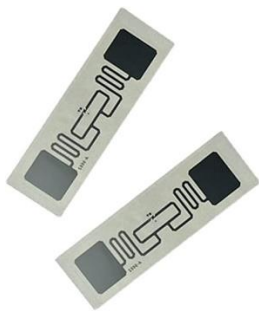
ATT Payload – dane wysyłane przez użytkownika w trybie przesyłania danych



6. RFID

RFID (*radio-frequency identification*) to technologia, która wykorzystuje fale radiowe do zdalnej identyfikacji obiektów. Podstawowym elementem systemu jest etykieta RFID lub tag RFID, które przechowują we wbudowanej pamięci nieulotnej własne dane identyfikacyjne. Etykieta RFID składa się z dwóch części:

- układu elektronicznego (pamięci), która przechowuje dane identyfikacyjne. Taki układ elektroniczny może występować bez obudowy i być napylony bezpośrednio na etykietę. Jego wymiary mogą wynosić już od 50 x 50 um (najmniejszy chip Hitachi).
- anteny, która jest największym elementem elektronicznym etykiety RFID. Za jej pomocą możliwe jest przesyłanie oraz odbieranie danych z etykiety, a także jej zasilanie. Wykorzystując zjawisko indukcji magnetycznej antena etykiety RFID stanowi cewkę odbiorczą, w której indukuje się napięcie służące do zasilania układu pamięci. Dzięki takiemu rozwiązaniu etykiety RFID oraz tagi RFID nie wymagają własnego zasilania (np. baterijnego czy akumulatorowego) i mogą być bardzo cienkie.



Rysunek 15 Etykieta RFID



Rysunek 16 Tag RFID

Do zapisu i odczytu danych zapisanych w pamięci taga lub etykiety wykorzystuje się dedykowane czytniki. Czytnik zbudowany jest z:

- elektronicznego układu nadawczego, odbiorczego oraz dekodera, które umożliwiają dwukierunkową transmisję danych. Dekoder dokonuje translacji sygnału napięciowego na cyfrowy w sytuacji odbierania danych oraz translacji sygnału cyfrowego na napięciowy w przypadku nadawania sygnału.



- anteny nadawczo-odbiorczej lub (w niektórych modelach czytników) dwóch anten: nadawczej i odbiorczej. Za jej pomocą zasilana jest etykieta lub tag RFID.

Uruchomienie oraz odczyt i zapis danych do etykiety / taga RFID polega na zbliżeniu etykiety / taga do czytnika. Czytnik za pomocą anteny nadawczo-odbiorczej wytwarza falę elektromagnetyczną, która jest odbierana przez antenę umieszczoną na etykiecie / tagu. Dzięki temu, że antena odbiorcza etykiety / taga RFID znajduje się w polu elektromagnetycznym o własnej częstotliwości rezonansowej na antenie (cewce) indukuje się napięcie, a ładunek elektryczny jest gromadzony w kondensatorze, który jest nasycony w strukturze etykiety. Po odebraniu wystarczającej ilości energii i naładowaniu kondensatora etykieta / tag RFID wysyła odpowiedź zawierającą swój kod identyfikacyjny. W czasie transmisji danych przez etykietę czytnik przełącza się na tryb odbioru danych wyłączając przy tym antenę nadawczą. Wówczas etykieta zasilana jest ze zgromadzonego ładunku elektrycznego w kondensatorze. Czytnik odbiera nadawaną przez etykietę falę elektromagnetyczną oraz dekoduje przesłane dane.

Do transmisji danych i zasilania etykiet / tagów system RFID wykorzystuje częstotliwość 125 kHz. Pozwala ona na odczyt i zapis danych z odległości nie większej niż 10 cm. Wykorzystywane są również inne częstotliwości zależnie od zastosowania, co przedstawia poniższa tabela.

Tabela 3 Częstotliwości pracy systemów RFID

Pasmo	Zasięg	Szybkość transmisji
LF: 120 – 150 kHz	10 cm	niska
HF: 13.56 MHz	10 cm – 1 m	niska → umiarkowana
UHF: 433 MHz	1 – 100 m	umiarkowana
UHF: 865–868 MHz (Europa) 902–928 MHz (Ameryka Północna)	1 – 12 m	umiarkowana → wysoka
mikrofale: 2450 – 5800 MHz	1 – 2 m	wysoka
mikrofale: 3.1 – 10 GHz	do 200 m	wysoka
fale milimetrowe: 24.125 GHz	10–200 m	wysoka



Etykiety RFID wykorzystywane są do identyfikacji produktów i stanowią elektroniczny kod produktu (*Electronic Product Code – EPC*). Każda etykieta zawiera dane identyfikacyjne produktu, który reprezentuje. W jej pamięci ROM zapisany jest 96 bitowy string (ciąg znaków), w skład którego wchodzi:

- 8 bitów identyfikujących wersję protokołu komunikacyjnego,
- 28 bitów określających organizację zarządzającą danymi zawartymi w tagu. Numer nadawany jest przez konsorcjum EPCGlobal,
- 24 bity identyfikujące rodzaj produktu,
- 36 bitów zawierających unikalny numer seryjny dla danego znacznika.

Prawo do edycji danych umożliwiające jest tylko w sekcji 24-bitowej oraz 36-bitowej. Pozostałe pola posiadają status *tylko do odczytu*.



Rysunek 17 Struktura pamięci etykiety RFID dla EPC

W związku z wieloma technicznymi możliwościami realizacji RFID – rodzaj kodowania, szybkość transmisji, wielkość pamięci znacznika – występuje wiele standardów RFID.

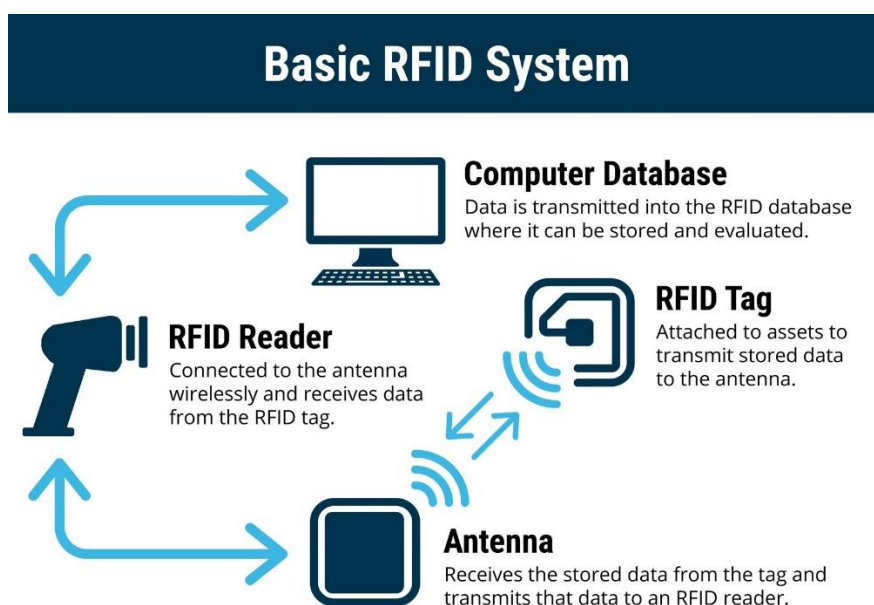
- *Tiris* – jest to jeden z pierwszych systemów RFID oparty na transmisji FM.
- *Unique* – najprostszy i powszechnie stosowany system RFID wykorzystujący częstotliwość 125 kHz, a prędkość transmisji danych to 2 kb/s. Znaczniki zapisywane są unikalnym kodem podczas produkcji, występują również w postaci kart. Stosuje się je m.in. w celu kontroli dostępu oraz rejestracji czasu pracy.
- *Hitag* – jest to standard do zastosowań przemysłowych. Umożliwia zapis odraz odczyt danych w etykietach / tagach. Wykorzystuje częstotliwość 125 kHz, a prędkość transmisji danych to 4 kb/s. Zastosowano w nim algorytm antykolizyjny, a także istnieje możliwość



kodowania przesyłanych danych. Stosuje się je np. w prostych systemach pobierania opłat, systemach znakowania produktów czy tagowaniu zwierząt.

- *ISO/IEC 14443 (MIFARE)* – standard umożliwiający stosowanie prostych znaczników pamięciowych jak i szyfrowanych. Częstotliwość pracy to 13.56 MHz, a prędkość transmisji danych wynosi do 106 kb/s. Standard został opracowany przez firmę Philips. Wykorzystuje się go m. in. w kartach bankowych (smart-cards) czy kartach identyfikacyjnych.
- *Icode* – standard charakteryzujący się bardzo płaskimi znacznikami. Umożliwiają one zapis oraz odczyt danych z 512 bitowej pamięci. Częstotliwość pracy to 13.56 MHz. Standard umożliwia obsługę do 30 znaczników na sekundę. Wykorzystywany jest w sklepach do znakowania produktów, bibliotekach, itp.
- *EPC C1G2* – to globalny standard RFID wykorzystujący częstotliwości UHF o dalekim zasięgu. Stosowany m.in. w logistyce, magazynowaniu czy systemach parkingowych.

Dla pełnej funkcjonalności systemu RFID wymagane jest stałe połączenie z bazą danych, w której zapisane są informacje na temat zidentyfikowanego produktu. Dzięki tym informacjom można określić typ, cenę czy ilość danego artykułu. W przypadku zastosowań logistycznych czy magazynowych numer identyfikacyjny czytnika określa ostatnie położenie transportowanego produktu.



Rysunek 18 Schemat systemu RFID



7. NFC

NFC (*near-field communication*) jest to skrót nazwy technologii do komunikacji bliskiego zasięgu. Zastosowanie sygnału o wysokiej częstotliwości pozwala na wymianę danych na odległość do 4 centymetrów. Technologia ta bazuje na standardzie ISO/IEC 14443, który definiuje standard dla kart zbliżeniowych używanych w celu identyfikacji użytkownika oraz protokoły transmisji używane podczas komunikowania się z kartami. NFC to połączenie interfejsu komunikacyjnego kart zbliżeniowych (emulator) oraz czytnika kart zbliżeniowych. Urządzenia NFC mogą również komunikować się między sobą. NFC głównie wykorzystywane jest w telefonach komórkowych do emulacji kart płatniczych dla płatności zbliżeniowych.

NFC wykorzystuje częstotliwość $13.56 \text{ MHz} \pm 7 \text{ kHz}$ w paśmie ISM, a maksymalna szerokość pasma to 2 MHz. Prędkość transmisji danych wynosi 106 kb/s, 212 kb/s, 424 kb/s lub 848 kb/s. Urządzenia wykorzystujące NFC do komunikacji mogą pracować w dwóch trybach:

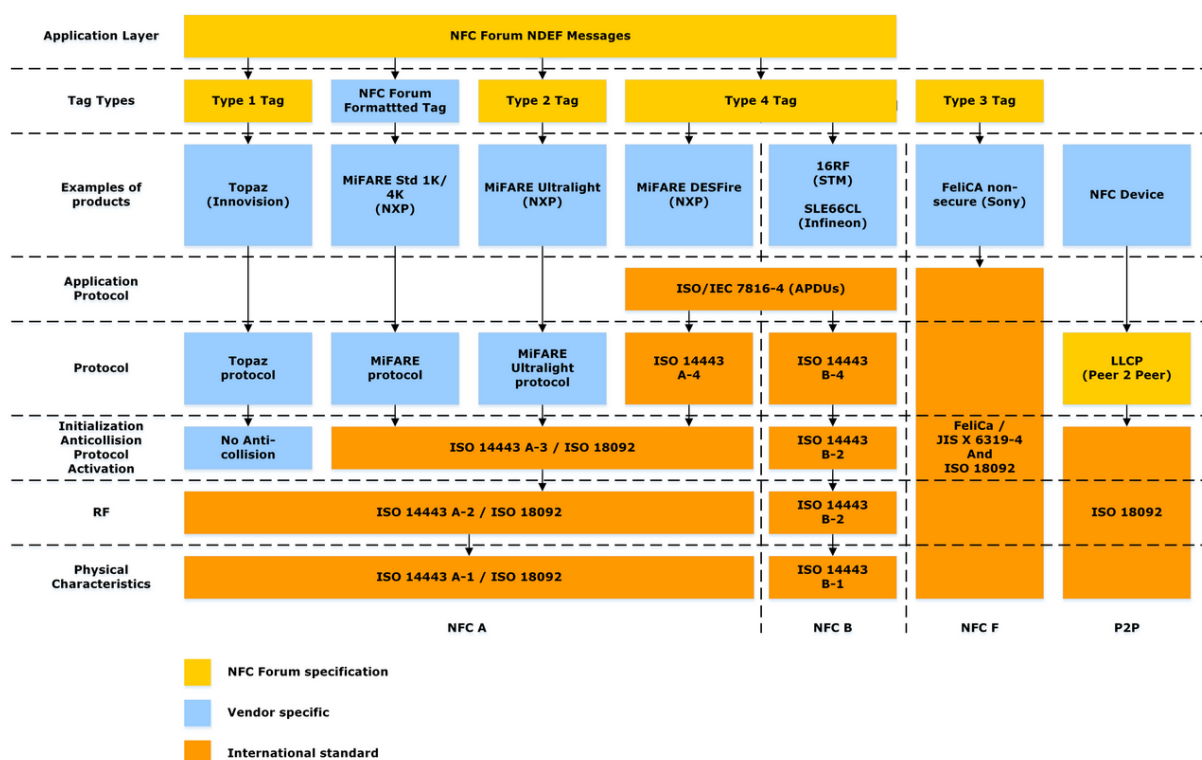
- tryb pasywny, w którym urządzenie inicjujące komunikację wytwarza pole elektromagnetyczne, a docelowe urządzenie odpowiada poprzez modulację tego pola. W tym trybie urządzenie docelowe jest zasilane mocą pola elektromagnetycznego urządzenia inicjującego i nie wymaga własnego źródła zasilania.
- tryb aktywny, w którym obydwa urządzenia komunikują się naprzemiennie. Każde z nich generuje własne pole elektromagnetyczne podczas nadawania. Gdy jedno urządzenie nadaje wówczas drugie pracuje w trybie odbioru i nie generuje swojego pola elektromagnetycznego. W trybie aktywnym obydwa urządzenia wymagają zasilania.

NFC może działać w jednym z trzech trybów:

- emulacji karty, w którym możliwa jest płatność zbliżeniowa z wykorzystaniem smartphona tak, jak kartą zbliżeniową,
- odczytu / zapisu, w którym możliwe jest odczytanie lub zapisanie danych do tagów NFC (podobnie jak w RFID),
- P2P (urządzenie – urządzenie), gdzie dwa urządzenia komunikują się i przesyłają dane.



Poza przesyłaniem danych, NFC można również wykorzystać do bezprzewodowego ładowania małych, przenośnych urządzeń. Standard NFC Wireless Charging (WLC) oferuje bezprzewodowe ładowanie urządzeń z mocą do 1W. Podczas ładowania dystans pomiędzy cewką nadawczą a odbiorczą nie może przekraczać 2 cm. Drugim standardem umożliwiającym ładowanie bezprzewodowe za pośrednictwem NFC jest Qi Wireless Power Consortium. Oferuje on moc ładowania do 15 W. Podczas ładowania dystans pomiędzy cewką nadawczą a odbiorczą nie może przekraczać 4 cm. Obydwa standardy zapewniają funkcję ładowania bezprzewodowego jednak standard NFC WLC korzysta ze znacznie mniejszego rozmiaru anteny. Dzięki temu NFC WLC jest idealnym rozwiązaniem do ładowania małych urządzeń np. słuchawek bezprzewodowych czy smartwatch'y.



Rysunek 19 Standardy NFC

8. Wykaz literatury

- [1]. Drew Gislason, „Zigbee wireless networking”, Newnes & Elsevier, 2008
- [2]. Pan MS., Tseng YC., „ZigBee and Their Applications”, Sensor Networks and Configuration, Springer, 2007
- [3]. Behrang Fouladi, Sahand Ghanoun, „Security Evaluation of the Z-Wave Wireless Protocol”, 2013
- [4]. Muneer Bani Yassein, Wail Mardini, Ashwaq Khalil, „Smart Homes Automation using Z-wave Protocol”, 2016 International Conference on Engineering & MIS (ICEMIS)
- [5]. Shilpa Devalal, A. Karthikeyan, „LoRa technology-an overview”, 2nd International conference on Electronics, Communication and Aerospace Technology (ICECA 2018)
- [6]. Martin Bor, John Vidler, Utz Roedig, „LoRa for the Internet of Things”, International Conference on Embedded Wireless Systems and Networks (EWSN), 2016
Jacopo Tosi, Fabrizio Taffoni, Marco Santacatterina, Roberto Sannino, Domenico Formica, „Performance Evaluation of Bluetooth Low Energy: A Systematic Review”, Sensors 2017
- [7]. Weis, Stephen A., *RFID (Radio Frequency Identification): Principles and Applications*, MIT CSAIL, CiteSeerX, 2007
- [8]. Elke Mackensen, Matthias Lai, Thomas M. Wendt, „Bluetooth Low Energy (BLE) based wireless sensors”, SENSORS, 2012 IEEE
- [9]. Kang Eun Jeon, James She, Perm Soonsawad, Pai Chet Ng, „BLE Beacons for Internet of Things Applications: Survey, Challenges, and Opportunities”, IEEE Internet of Things Journal Volume: 5, Issue: 2, April 2018
- [10]. R. Weinstein, „RFID: a technical overview and its application to the enterprise”, IT Professional Volume: 7, Issue: 3, May-June 2005
- [11]. Paul G. Ranky, „An introduction to radio frequency identification (RFID) methods and solutions”, Assembly Automation, 2006
- [12]. Gerald Madlmayr, Josef Langer, Christian Kantner, Josef Scharinger, „NFC Devices: Security and Privacy”, Third International Conference on Availability, Reliability and Security, 2008
- [13]. Vedat Coskun, Kerem Ok, Busra Ozdenizci, „Near Field Communication from theory to practice”, Wiley, 2012



Spis rysunków

Rysunek 1 Topologie sieci Zigbee.....	5
Rysunek 2 Architektura Zigbee	6
Rysunek 3 Tryby instalacji Zigbee	7
Rysunek 4 Zastosowanie sieci Z-Wave	9
Rysunek 5 Sieć mesh Z-Wave	11
Rysunek 6 Idea technologii	13
Rysunek 7 Architektura sieci.....	15
Rysunek 8 Wersje Bluetooth Low Energy z datami ich wprowadzenia.....	18
Rysunek 9 Architektura Bluetooth Low Energy	19
Rysunek 10 Kanały Bluetooth Low Energy	20
Rysunek 11 Zmiana trybu pracy w warstwie łącza danych.....	21
Rysunek 12 Struktura atrybutów ATT	23
Rysunek 13 Struktura danych GATT	24
Rysunek 14 Ramka danych Bluetooth Low Energy.....	25
Rysunek 15 Etykieta RFID.....	26
Rysunek 16 Tag RFID	26
Rysunek 17 Struktura pamięci etykiety RFID dla EPC	28
Rysunek 18 Schemat systemu RFID	29
Rysunek 19 Standardy NFC	31

Spis tabel

Tabela 1 Częstotliwość pracy Z-Wave	10
Tabela 2 Typy węzłów w LoRaWAN	15
Tabela 3 Częstotliwości pracy systemów RFID.....	27