Urządzenia Peryferyjne

Bluetooh

Wstęp

Technologia krótkodystansowego połączenia bezprzewodowego. Może służyć do budowania sieci PAN, w których wymieniane są dane między urządzeniami. Najczęściej stosuje się wersję Bluetooth o mocy 2,5 mV, która oferuje zasięg do 10 m. Transmisja w Bluetooth odbywa się za pośrednictwem fal elektromagnetycznych z pasma od 2,402 2,480 GHz (są to nielicencjonowane częstotliwości oddane do dowolnego użytki, ISM).

Działanie technologii Bluetooth zostało sprecyzowane w standardzie IEEE 802.15.1.

Działanie

Bluetooth używa technologii radiowej FHSS. Polega ona na okresowych, sekwencyjnych przeskokach między kanałami częstotliwościowymi. Wysyłane dane są dzielone na pakiety i wysyłane przez 79 kanałów Bluetooth. Każdy kanał ma szerokość 1 MHz. W ciągu sekundy wykonuje się 1600 przeskoków między kanałami. W technologii Bluetooth Low Energy (BLE, mniej energożernej alternatywy Bluetooth) kanałów jest 40 i mają one szerokość 2 MHz.

Bluetooth początkowo używał wyłącznie kluczowania częstotliwości (GFSK, o nośnych w kształcie krzywej Gaussa), ale wraz z nadejściem wersji 2.0+EDR użyta może być również kluczowanie fazy (DQPSK). Urządzenia korzystające z kluczowania częstotliwości GFSK operują na przepustowości podstawowej (BR, basic rate), która wynosi 1 Mb/s. Urządzenia korzystające z kluczowań fazy operują na przepustowości ulepszonej (EDR, Enchanced Data Rate), która wynosi 2 lub 3 Mb/s. Jeżeli urządzenie może działać z wykorzystaniem obydwu kluczowań działa ono w trybie BR/EDR.

Bluetooth działa w architekturze master-slave. Jedno urządzenie nadrzędne kontroluje w nim komunikację w pikosieci składającej się z do 7 urządzeń podrzędnych (nie każde urządzenie obsłuży to maksimum), pełniąc rolę dystrybutora wszystkich wysyłanych w sieci pakietów. Przesyłanie pakietów jest synchronizowane za pomocą zegara urządzenia master. Dwa tyknięcia tego zegara tworzą „slot" przesyłowy (trwający 625 us). Pakiety mogą być możliwe do wysłania w czasie 1, 3 lub 5 slotów. Transmisja pakietu po stronie urządzenia master zaczyna się przy tym zawsze w slotach parzystych (w momentach podzielnych przez 1250 us). Transmisja pakietu po stronie urządzenia slave zaczyna się zaś zawsze przy slotach nieparzystych (w momentach niepodzielnych przez 1250 us). Rola urządzenia nadrzędnego w pikosieci może być przekazywana między urządzeniami w niej uczestniczącymi.

Kilka pikosieci może być połączonych w większą sieć, czyli scatternet. Wówczas urządzenia mogą być jednocześnie nadrzędne w jednej z pikosieci składowych, pełniąc rolę podrzędną w innych pikosieciach składowych.

W dowolnym momencie połączenia urządzenie master adresuje jedno z urządzeń slave i rozpoczyna z nim komunikację. Najczęściej przełącza się ono nieustannie między wszystkimi urządzeniami slave w odpowiednich interwałach. Urządzenie slave zaś w każdym momencie musi nasłuchiwać każdy ze swoich slotów odbiorczych (przynajmniej teoretycznie).

Wersje technologii Bluetooth

Wszystkie wersje Bluetooth są kompatybilne wstecznie. Wersjami technologii rozważanymi na potrzeby laboratorium są:

- *Bluetooth 1.0/1.0B* – pierwsza wersja technologii Bluetooth. Nie pozwalała na anonimowość urządzeń.
- *Bluetooth 1.1* – ustandaryzowana za pomocą IEEE 802.15.1. Dodała możliwość użycia kanałów nieszyfrowanych. Wprowadziła RSSI (Received Signal Strength Indicator) mierzący moc zawartą w sygnale radiowym.
- *Bluetooth 1.2* – przyspieszyła proces łączenia i wykrywania urządzeń. Wprowadziła technologię AFH pozwalającą na unikanie przeciążonych kanałów w ramach przeskoków. Zwiększyła przepustowość do 721 kb/s. Wprowadziła technologie eSCO (Extended Synchronous Connections), która zwiększyła jakość połączeń audio poprzez zezwolenie na retransmisję uszkodzonych pakietów.
- *Bluetooth 2.0 + EDR* – wprowadziła kluczowanie fazy, a co za tym idzie EDR.
- *Bluetooth 2.1 + EDR* – wprowadziła SSP (secure simple pairing), które zwiększyło bezpieczeństwo i wygodę parowania urządzeń Bluetooth. Wprowadziła także EIR (extended inquiry response), które pozwoliło na pozyskiwanie większej ilości danych podczas wyszukiwania urządzeń do parowania.
- *Bluetooth 3.0 + HS* – zwiększono przepustowość do 24 Mb/s. Uzyskano ją poprzez użycie równoległego połączenia AMP (Alternative MAC, Physical Layer 1) zgodnego ze standardem IEEE 802.11 (MAC, warstwa fizyczna) zamiast łącza Bluetooth. Łącze Bluetooth służyć odtąd miało tylko do procesu negocjacji i ustanowienia połączenia. Urządzenia mogą odtąd działać w trybie z retransmisjami ERTM (Enchanced Retransmission Mode, na niezawodnym kanale L2CAP) bądź bez nich SM (Streaming Mode). Dane serwisowe mogły być od tej wersji wysyłane bezpołączeniowo, a co za tym idzie szybko.

Protokoły Bluetooth

Komunikacja w ramach Bluetooth jest wspomagana przez stos protokołów komunikacyjnych. Dzielą się one na protokoły obowiązkowe oraz nieobowiązkowe. Na protokoły obowiązkowe składają się:

1. Link Manager Protocol (LMP)
2. L2CAP (Logical Link Control and Adaptation Protocol)
3. Service Discovery Protocol (SDP)

Link Manager to system odpowiadający za ustanawianie połączeń między urządzeniami i zarządzanie tymi połączeniami. Za pomocą protokołu Link Managera komunikuje się z Link Managerami innych urządzeń. Protokół Link Managera definiuje kilka PDU, które zawierają odpowiadają za:

- Wysyłanie i odbieranie danych
- Żądanie danych na temat nazwy
- Żądanie danych na temat adresacji
- Ustanawianie połączeń
- Autentyfikacje
- Negocjacje parametrów połączenia

Logical Link Control and Adaptation Protocol (L2CAP) odpowiada za multipleksację połączeń logicznych między dwoma urządzeniami oraz segmentacje pakietów. Oferuje dwa podstawowe tryby pracy. W trybie *Basic Mode* nieobecne są mechanizmy niezawodnościowe, a protokół pozwala na wysyłanie

maksymalnie 672-bajtowych pakietów (minimalny rozmiar pakietu 48B). W trybie pracy *Retransmission and Flow Control* dodaje do pakietów mechanizmy niezwodnościowe w postaci sumy kontrolnej CRC.

Service Discovery Protocol (SDP) pozwala urządzeniu na zdefiniowanie usług oferowanych przez inne urządzenia oraz zdefiniowanie parametrów tychże usług.

Protokół RFCOMM (Radio Frequency Communications) pozwala na emulowanie komunikacji szeregowej. Pozwala on między innymi na przesyłanie komend Hayes'a (AT) oraz jest warstwą transportową dla OBEX. Jest powszechnie używany przez wiele aplikacji Bluetooth ze względu na szerokie wsparcie.

Protokół BNEP (Bluetooth Network Encapsulation Protocol) pozwala na transfer danych innych protokołów przez kanał L2CAP. Głównie używa się go na przesyłanie pakietów IP w sieciach PAN (Bluetooth).

Protokół AVCTP (Audio/Video Control Transport Protocol) używany jest do zapewnienia zdalnego zadawania komend AV/C przez kanał L2CAP. Używane często przez urządzenia sterujące systemami Audio/Video.

Protokół AVDTP (Audio/Video Distribution Transport Protocol) używany jest do strumieniowego przesyłania muzyki przez kanał L2CAP, który przeznaczony jest do przesyłania wideo za pomocą Bluetooth.

Protokół TCS BIN (Telephony Control Protocol – Binary) używany jest do przesyłania sygnałów kontrolujących rozmowy głosowe i danowe między urządzeniami Bluetooth.

Protokół OBEX (Object Exchange Protocol) to protokół warstwy sesji odpowiadający za wymianę obiektów w formie binarnej między urządzeniami.

Ustanawianie połączenia

Każde urządzenie Bluetooth będące w stanie *discoverable mode* musi na żądanie innych urządzeń przesyłać dane o:

- Swojej nazwie
- Swojej klasie
- Liście oferowanych usług
- Informacjach technicznych (producent, specyfikacja Bluetooth itd.)

Każde urządzenie Bluetooth może wykonywać skanowanie w celu znalezienia urządzeń do połączenia oraz może odpowiadać na skany innych urządzeń. Jeżeli udostępniony innemu urządzeniu zostanie adres urządzenia to musi ono na żądanie innego urządzenia przesyłać dane z powyższej listy. Użycie usług może jednak wymagać zgody usługodawcy lub sparowania.

Każde urządzenie posiada unikalny 6-bajtowy adres MAC. Jednakże dla wygody użytkowników używane zamiast nich są specjalne nazwy w Bluetooth w języku naturalnym.

Parowanie urządzeń

Ustanowienie połączenia między urządzeniami w Bluetooth jest nieskomplikowane. Jednakże wiele usług dających dostęp do danych urządzenia lub pozwalających na sterowanie nim wymaga lepszych zabezpieczeń. Stąd powstał wymóg parowania urządzeń. Parowanie rozpoczyna się po wysłaniu specjalnego żądania (przez użytkownika lub automatycznie w ramach usług). Wymaga ono często

interakcji z użytkownikiem, który potwierdza identyfikację urządzeń. Urządzenia pozostają sparowane do momentu zerwania więzi. Zwykłe zerwania połączenia nie zrywa więzi.

Urządzenia są sparowane jeżeli przechowują ten sam, wspólny, sekretny klucz. Klucz jest generowany w procesie parowania i wysyłany specjalnym, zakodowanym kanałem. Zapominany jest przy zrywaniu więzi.