Bluetooth

Bezprzewodowa transmisja danych na niewielkie odległości, część 2

Drugą część artykułu poświęcamy prezentacji praktycznych zagadnień związanych z protokołem transmisji danych wykorzystywanym w systemie Bluetooth. Przedstawione w artykule informacje stanowią podstawę do dobrego zrozumienia sposobu działania interfejsu, co z pewnością zaowocuje podczas budowania urządzeń wyposazonych w Bluetootha.

Ramki protokołu HCI

Rozróżniamy pięć typów ramek HCI. Typ ramki określa pierwszy bajt ramki:

Kod	Typ ramki	Komentarz
0x01	Ramka - rozkaz HCI	Ramka sterująca, ustawiająca parametry modułu BT itp.
0x02	Ramka danych ACL	Dane przesyłane w sposób asynchroniczny i *connectionless*. Są to dane sterujące (np. wyższych warstw - L2CAP), lub dane użytkownika.
0x03	Ramka danych SCO	Połączenie synchroniczne, punkt - punkt. Główne przeznaczenie - transmisja danych głosowych - PCM. Pakiety SCO nie są nigdy retransmitowane.
0x04	Ramka zdarzenia	Informuje o zdarzeniach w systemie. Jest również odpowiedzią na Ramkę - Rozkaz.
0x05	Ramka błędów	Informuje o błędach w systemie. Jest również odpowiedzią na źle sformułowaną Ramkę - Rozkaz.

Typ ramki-rozkazu HCI jest zdefiniowany w szesnastobitowym polu **OpCode**. Pole *OpCode* składa się z dwóch pól **OGF** (**O***pCode* **G***roup* **F***ield*) i **OCF** (**O***pCode* **C***ommand* **F***ield*). OGF określa grupę rozkazów:

OGF = 1 Link Control Commands

OCF	Nazwa komendy
0001h	HCI Inquiry
0002h	HCI Inquiry Cancel
0003h	HCI Periodic Inquiry Mode
0004h	HCI Exit Periodic Inquiry Mode
0005h	HCI Create Connection
0006h	HCI Disconnect
0007h	HCI Add SCO Connection
0009h	HCI Accept Connection Request
000Ah	HCI Reject Connection Request
000Bh	HCI Link Key Request Reply
000Ch	HCI Link Key Request Negative Reply
000Dh	HCI PIN Code Request Reply
000Eh	HCI PIN Code Request Negative Reply
000Fh	HCI Change Connection Packet Type
0011h	HCI Authentication Requested
0013h	HCI Set Connection Encryption
0015h	HCI Change Connection Link Key
0017h	HCI Master Link Key
0019h	HCI Remote Name Request
001Bh	HCI Read Remote Supported Features
001Dh	HCI Read Remote Version Information
001Fh	HCI Read Clock Offset

OGF = 2 Link Policy Commands

OCF	Nazwa komendy
0001h	HCI Hold Mode
0003h	HCI Sniff Mode
0004h	HCI Exit Sniff Mode
0005h	HCI Park Mode
0006h	HCI Exit Park Mode
0007h	HCI QoS Setup
0009h	HCI Role Discovery
000Bh	HCI Switch Role
000Ch	HCI Read Link Policy Settings
000Dh	HCI Write Link Policy Settings

OGF = 3 Host Controller & BaseBand Commands

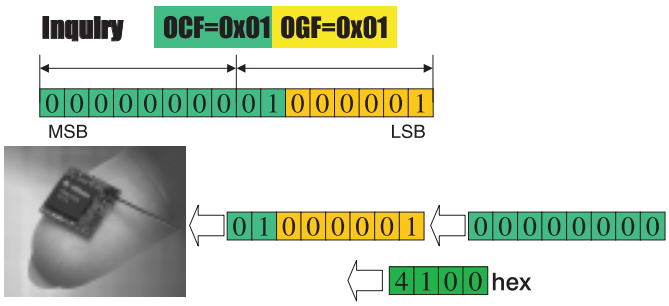
OCF	Nazwa komendy
0028h	HCI Write Automatic Flush Timeout
0029h	HCI Read Num Broadcast Retransmissions
002Ah	HCI Write Num Broadcast Retransmissions
002Bh	HCI Read Hold Mode Activity
002Ch	HCI Write Hold Mode Activity
002Dh	HCI Read Transmit Power Level
002Eh	HCI Read SCO Flow Control Enable
002Fh	HCI Write SCO Flow Control Enable
0031h	HCI Set Host Controller To Host Flow Control
0033h	HCI Host Buffer Size
0035h	HCI Host Number Of Completed Packets
0036h	HCI Read Link Supervision Timeout
0037h	HCI Write Link Supervision Timeout
0038h	HCI Read Number Of Supported IAC
0039h	HCI Read Current IAC LAP
003Ah	HCI Write Current IAC LAP
003Bh	HCI Read Page Scan Period Mode
003Ch	HCI Write Page Scan Period Mode
003Dh	HCI Read Page Scan Mode
003Eh	HCI Write Page Scan Mode

OGF = 4 Informational Parameters

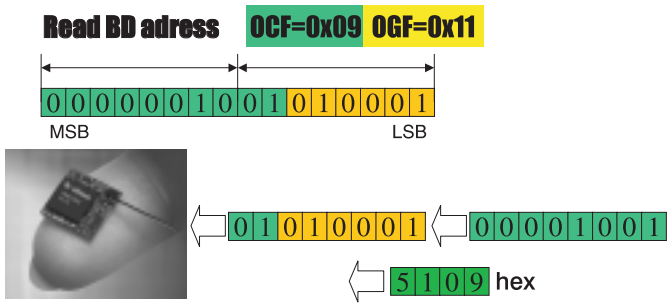
OCF	Nazwa komendy
0001h	HCI Read Local Version Information
0003h	HCI Read Local Supported Features
0005h	HCI Read Buffer Size
0007h	HCI Read Country Code
0009h	HCI Read BD ADDR

Wartości OCF mogą się różnić w następnych wersjach specyfikacji CORE. Obecnie obowiązująca wersja to 1.1 - należy się spodziewać się pojawienia już wkrótce wersji 2.0

Pole OGF jest przechowywane na sześciu bitach, a pole OCF na dziesięciu bitach. Na **rys. 6** i **7** pokazano sposób tworzenia *OpCode* dla różnych ramek HCI. Przy przesyłaniu danych do BT należy się przyzwyczaić, że najpierw transmitujemy mniej znaczący bajt następnie bardziej znaczący bajt.



Rys. 6. Sposób tworzenia pola OpCode przy danym OCF i OGF



Rys. 7. OpCode dla odczytywania modułu BT

Funkcje wybranych ramek HCI

Inquiry (zapytanie) - przesłanie tej ramki *OpCode* do BT powoduje, że moduł wykrywa czy w jego najbliższym otoczeniu są inne BT. Przykład ramki:

0x01	0x0001 0x01	0x05	0x33	0x8B	0x9E	0x0A	0x64

Objaśnienia:
- Typ ramki - tutaj ramka typu *rozkaz*
- Pole **OpCode**. OCF=0x001 OGF=0x01. Tworzenie pola *OpCode* zostało wyjaśnione powyżej
- Liczba parametrów w bajtach
- LAP Address. LAP Adress - Każde urządzenie BT posiada swój własny 48-bitowy unikalny adres. Format tego adresu jest zgodny ze standardem IEEE802. Adres można podzielić na trzy części:

- Pole **LAP** (*Lower Adress Part*) składające się z 24 bitów.
- Pole **UAP** (*Upper Adress Part*) składające się z 8 bitów.
- Pole **NAP** (*Non-significant Adress Part*) składające się z 16 bitów.

Pewne adresy LAP (*0x9E8B00-0x9E8B3*) są zarezerwowane dla różnych potrzeb. Adres *0x9E8B33* został zarezerwowany dla potrzeb funkcji **Inquiry**

- Czas trwania procedury inquiry (jak długo BT czeka na odpowiedzi od innych modułów). Każda jednostka tego pola to 1,28 sekundy. Pole to może przyjmować wartości z zakresu 0x01 do 0x30. Czyli procedura inquiry może trwać min. 1,28 sekundy a maksymalnie 61,44 sekundy.
- Ile maksymalnie chcemy wykryć innych modułów BT. 0x00 - wszystkie.

Scan Enable - aby moduł BT mógł być wykrywany w procesie *Inquiry* musi zostać wywołana funkcja *Scan Enable*. W przeciwnym razie moduł BT pozostanie niewidoczny dla innych.

0x01	0x001A 0x01	0x01	0x03

Objaśnienia:
- Typ ramki - tutaj ramka typu *rozkaz*
- Pole **OpCode**. OCF=0x001 OGF=0x01. Tworzenie pola OpCode zostało wyjaśnione powyżej.
- Liczba parametrów w bajtach
- Dwa najmłodsze bity w bajcie - 00 wyłączenie, 11 włączenie

Inquiry Complete (wyszukiwanie zakończone) - po zakończeniu procedury Inquiry otrzymujemy od BT ramkę, która jest zdarzeniem (*event*). Zawiera ona informację ile urządzeń udało się wykryć oraz status procedury Inquiry.

0x04	0x01	0x00	0x01

Objaśnienia:
- Typ ramki - tutaj ramka typu *zdarzenie*
- Pole **EventCode**. 0x01 = Inquiry Complete
- Status, gdy 0x00 - Sukces.
- Dwa najmłodsze bity w bajcie - 00 wyłączenie 11 włączenie

Inquiry Result (rezultat wyszukiwania) - po otrzymaniu ramki sygnalizującej zdarzenie Inquiry Complete (gdy status = 0x00) otrzymujemy właśnie tą ramkę. Zawiera ona 48-bitowe adresy modułów BT oraz dodatkowe parametry.

0x04	0x02	0x01	XX	XX	XX	XX	XX	XX
AA	BB	CC	DD	DD	DD	EE	EE	

Objaśnienia:
- Typ ramki - tutaj ramka typu *zdarzenie*
- Pole **EventCode**. 0x02 = Inquiry Result
- Ilość znalezionych modułów BT
- 6 bajtów (48 bitów) - adres znalezionego urządzenia BT (tzw. BD Address)
- Page Scan Repetition Mode
- Page Scan Period Mode
- Page Scan Mode
- Klasa urządzenia
- Clock offset (przesunięcie zegara między masterem a slavem w sieci PicoNet)

Create Connection - gdy znamy adres drugiego urządzenia możemy spróbować utworzyć połączenie HCI. Odbywa się to poprzez wysłanie ramki:

0x01	0x0005 0x01	0x0D	XX	XX	XX	XX	XX	XX
0x18	0xCC	AA	BB	CC	CC	EE		

Objaśnienia:
- Typ ramki - tutaj ramka zdarzenie
- Pole **EventCode**. 0x02 = Inquiry Result
- Ilość parametrów w bajtach
- 6 bajtów (48 bitów) - adres znalezionego urządzenia BT (tzw. BD Adress)
- Typ pakietów. W obecnej chwili dostępne rodzaje pakietów (dla specyfikacji Core ver. 1.1) to: DM1 (0x0008), DM3(0x0400), DH1 (0x0010), DH3 (0x0800). Są to pakiety jakie są przesyłane drogą radiową. Wartość 0xCC18 oznacza wszystkie te pakiety. Pole to określa, jakie rodzaje pakietów mogą być używane - przynajmniej jeden z nich musi być zadeklarowany. Wymienione pakiety różnią się między sobą liczbą bitów kontrolnych, kodami zabezpieczeń oraz algorytmami retransmisji.
- Page Scan Repetition Mode
- Page Scan Mode
- Clock offset

Allow role switch. Pole to określa czy dane urządzenie dopuszcza zamianę ról - np. z Mastera na Slaveía lub odwrotnie.

Connection request - gdy wyślemy powyższą ramkę do BT to z drugiego modułu BT o adresie XXXXXX powinniśmy otrzymać ramkę:

0x04	0x04	0x0A	0xYY	0xYY	0xYY	0xYY	0xYY	0xYY
0x00	0x43	0x00	0x01					

Objaśnienia:
- Typ ramki - tutaj ramka typu *zdarzenie*
- Pole **EventCode**. 0x04 = Connection Request
- Ilość Bajtów danych
- Adres urządzenia chcącego się połączyć
- Klasa urządzenia
- Typ połączenia. Wartość 0x00 - żądane połączenie SCO (transmisja głosowa), 0x01 - żądane połączenie ACL (dane)

Accept Connection Request - (akceptuj połączenie). Ramka typu *rozkaz* może być przesłana tylko w odpowiedzi na ramkę typu *zdarzenie* Connection Request:

0x01	0x0009	0x07	0xYY	0xYY	0xYY	0xYY	0xYY	0xYY	0x01
	0x01								

Objaśnienia:
- Typ ramki - tutaj ramka typu *rozkaz*
- 0x009 = Accept Connection Request
- Ilość Bajtów danych
- Adres urządzenia chcącego się połączyć
- Accept role switch - 0x01 Nie akceptujemy zmian Master <-> Slave

Reject Connection Request - (odrzuć połączenie). Ramka typu rozkaz wysyłana, gdy nie chcemy aby moduł BT o adresie YYYYYY łączył się z nami. Za pomocą poniższej ramki możemy odrzucić połączenie:

0x01	0x0009	0x07	0xYY	0xYY	0xYY	0xYY	0xYY	0xYY	0x01
	0x01								

Objaśnienia:
- Typ ramki - tutaj ramka typu *rozkaz*
- 0x009 = Accept Connection Request
- Ilość Bajtów danych
- Adres urządzenia chcącego się połączyć.
- Reason. Przyczyna odrzucenia połączenia. Pole może przyjmować wartości z przedziału 0x0D - 0x0F:
  0x0D - adresat odrzucił połączenie ze względu na brak zasobów - np. Niewystarczająca ilość pamięci.
  0x0E - adresat odrzucił połączenie z powodów bezpieczeństwa.
  0x0F - adresat odrzucił połączenie, ponieważ jest tzw. osobistym urządzeniem.

Connection Complete Event - W przypadku, gdy zdecydowaliśmy się zaakceptować połączenie otrzymamy ramkę - zdarzenie mówiące nam, że połączenie zostało utworzone:

0x04	0x03	0x0b	0x10	0x00	0x0f	0xYY	0xYY	0xYY
0xYY	0xYY	0xYY	0x01	0x00				

Objaśnienia:
- Typ ramki - tutaj ramka zdarzenie
- Pole **EventCode**. 0x03 = Connection Complete
- Ilość Bajtów danych
- Adres urządzenia chcącego się połączyć
- Status połączenia
- Uchwyt połączenia (*Connection Handle*)
- BD adres modułu BT z którym się połączyliśmy
- Typ połączenia - 0x01 ACL 0x00 SCO
- Encryption Mode - 0x00 daje połączenie bez szyfrowania

Henryk Nowak

Dodatkowe informacje

Dodatkowe informacje są dostępne na płycie CD-EP12/2002B oraz w Internecie pod adresami:
- http://www.bluetooth.com/pdf/Bluetooth_11_Specifications_Book.pdf,
- http://www.bluetooth.com/pdf/Bluetooth_11_Profiles_Book.pdf,
- http://www.bluetooth.prv.pl.