Bezdrôtové technológie pre IoT

Ondrej Karpiš, 2023

Vytvorené v rámci projektu **KEGA 026TUKE-4/2021**

Oblasť použitia

IoT – Internet vecí

IoE – Internet všetkého (veci, procesy, ľudia, zvieratá ...)

WSN – Wireless Sensor Networks

Obmedzenia „vecí“

- veľkosť
- výkon
- spotreba
- dosah, rýchlosť

Bezdrôtové technológie pre IoT (IoE)

Bunkové siete (GSM, LTE) – licencované pásma

- EC-GSM-IoT, LTE-M, NB-IoT, 5G IoT

Low-power siete – ISM pásmo

- Bluetooth Low Energy, Bluetooth Mesh (WPAN)
- IEEE 802.15.4 (LR-WPAN), ZigBee
- LoRa, LoRaWAN
- iné

EC-GSM-IoT

- Low Power Wide Area Network (LPWAN)
- založené na 2G sieťach, 50 kb/s
- smart merače, zabudované senzory, asset trackers

+ dobrá životnosť batérií (roky)
+ takmer globálna použiteľnosť (zhoršuje sa)
+ kompatibilita s množstvom zariadení
+ nízka cena (zariadenia aj dáta)
- prestáva sa používať (Európa do 2025?)

LTE (Long Term Evolution)

- na rozhraní 3G a 4G (3.95G)
- teoreticky 50 Mbps upload, 150 Mbps download
- softvérovo definované rádio - flexibilita v podpore nových štandardov

Štandardy pre IoT:

- NB IoT - Narrow Band IoT (Cat-NB1, Cat-NB2)
- LTE-M (Cat-M1)
- Cat-1
- Cat-4

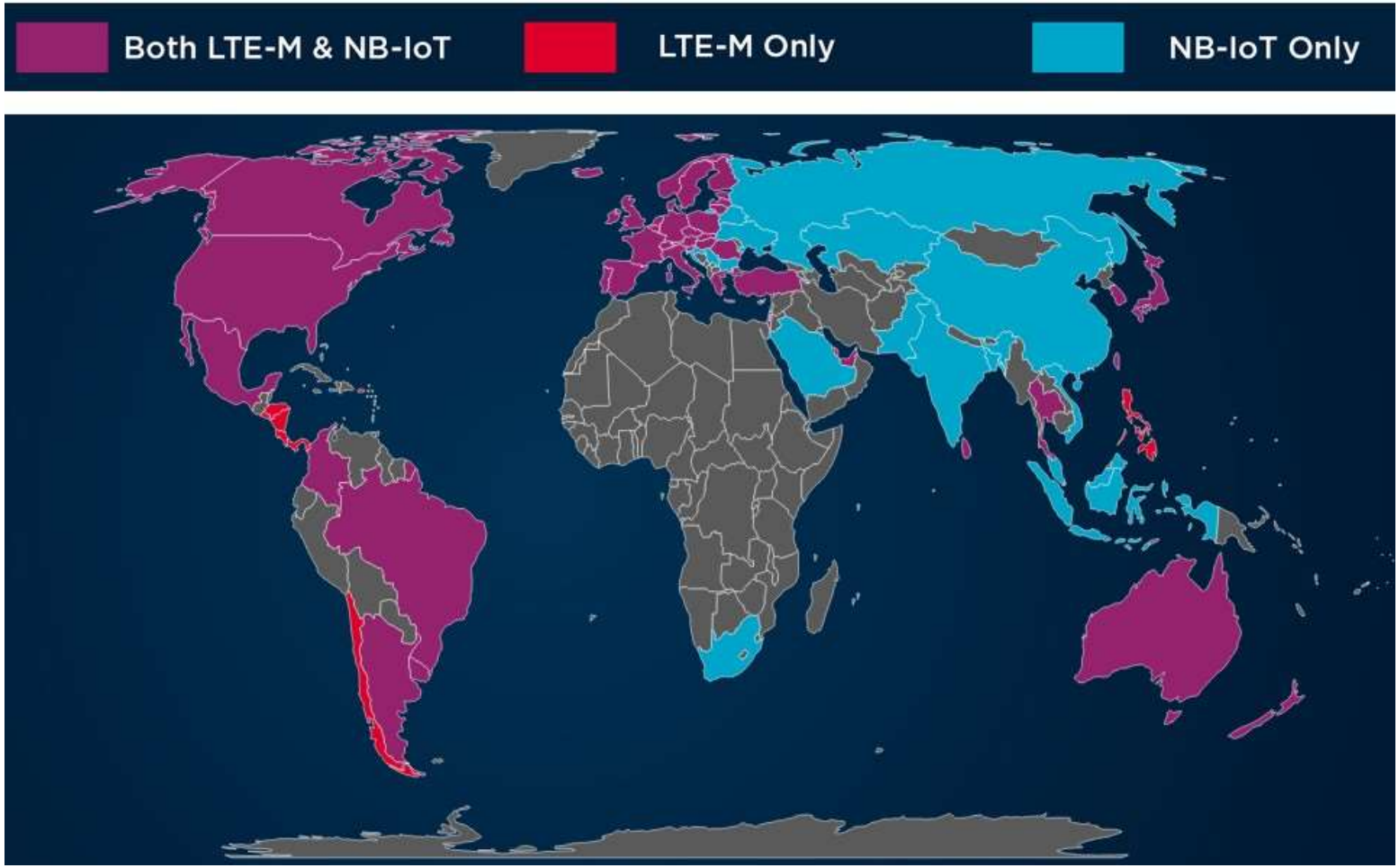
NB-IoT

- low-cost, low-power (10 rokov na 2 AA batérie)
- low-bandwidth (200 kHz) - môže využívať „guard band“
- zlepšené pokrytie v budovách, aj v podzemí
- dosah až do 10 km
- upload - 66 kb/s, download - 26 kb/s, half duplex
- latencia 1,6 až 10 s, max. dĺžka spania 3 hod
- len pre stacionárne zariadenia
- meranie spotreby (voda, el., plyn), smart city (osvetlenie, parkovanie), monitorovanie v priemysle, poľnohospodárstve ...

LTE-M

- low-cost, low power
- pásmo 1,4 MHz, half duplex aj full duplex
- 1 Mb/s (zvyčajne upload 380 kb/s, download 300 kb/s)
- latencia 10-15 ms, max. dĺžka spania 40 min
- podpora pre mobilné zariadenia (asset tracking, fleet management)
- podpora pre hlasové aplikácie (medical alert devices, home alarm systems)
- smart meters, industrial monitors, asset tracking, health monitor, alarms, wearables
- nie je dostupné globálne

Mapa pokrytia (2020)



Cat-1

- staršie než predošlé dva
- vyššia spotreba, menší dosah, drahšie
- lepšie globálne pokrytie
- 20 MHz pásmo, upload do 5 Mb/s, download do 10 Mb/s
- latencia 50-100 ms, full duplex
- podpora pre hlas, mobilné zar.
- nositeľnosti, kiosky, video dohľad, starostlivosť o zdravie, bankomaty, zdieľaná mobilita – prenájom bicyklov a kolobežiek, autonómne drony na doručovanie

Cat-4

- 20 MHz pásmo
- 50 Mbps upload, 150 Mbps download
- najdrahšie
- video dohľad, video aplikácie v reálnom čase, in-car hotspots, in-car infotainment, autonómne vozidlá

Porovnanie LTE IoT technológií

Koľko to stojí?

- Orange: 0,48 Eur/mes - NB IoT Smart paušál
  0,25 Eur/mes (0,25 Eur/MB) - IoT connect
- O2 telemetria: 2 Eur/mes základ + 0,06 Eur za deň (do 100 kB)
- Česko (Vodafone): cca 20 Eur za 1 GB na 10 rokov

24 Eur

18 Eur

IEEE 802.x

- 802 – rodina štandardov pre LAN a MAN
  – len fyzická (PHY) a linková vrstva (LLC a MAC)

- 802.1 – LAN/MAN architektúra, prepájanie sietí, bezpečnosť ...
- 802.3 – Ethernet
- 802.11 (a/b/g/n) – WiFi
- 802.15 – Wireless PAN (Personal Area Network)

IEEE 802.15.x – wireless PAN

- **802.15.1** – Bluetooth
- 802.15.2 – koexistencia 802.11 a 802.15
- 802.15.3 – High-Rate wireless PAN
- **802.15.4** – Low-Rate wireless PAN (LR-WPAN) (ZigBee, WirelessHART, MiWi, ISA100.11a)
- 802.15.5 – Mesh siete pre WPAN
- 802.15.6 – Body area network (BAN)

Bluetooth

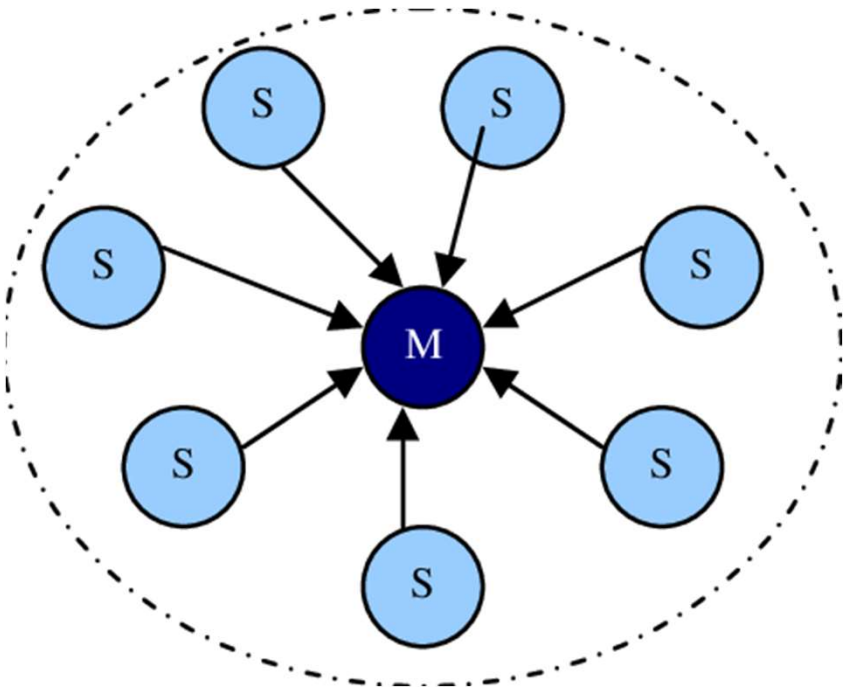
- pôvodný cieľ – náhrada drôtového spojenia na krátku vzdialenosť
- vyvinuté vo firme Ericsson (1994-1997)
- meno podľa dánskeho kráľa Haralda Bluetootha (Modrozuba)
  logo vytvorené z H a B: ᚼ ᛒ
- spravované združením Special Interest Group (SIG) Bluetooth (dnes viac ako 35000 členov)
- komerčne dostupné zariadenia od r.2001 – Ericsson T39 a IBM ThinkPad A30
- rozšírenie aj vďaka Motorole

Vlastnosti Bluetooth

- krátky dosah, nízka spotreba, low-cost
- ISM pásmo – 2.4 GHz (2,400 až 2,4835 GHz)
- 79 kanálov so šírkou 1 MHz
- FHSS (Frequency-hopping spread spectrum) – 1600 hopov za sekundu
- Modulácia:
  GFSK (Gaussian frequency-shift keying) – Basic Rate (BR), 1 Mb/s
  Enhanced Data Rate (EDR) – od verzie 2.0:
    PI/4-DQPSK (differential quadrature phase-shift keying) – 2 Mb/s
    8-DPSK – 3 Mb/s
  Apple (2019) – HDR4 a HDR8 – 4 MHz kanály s FEC

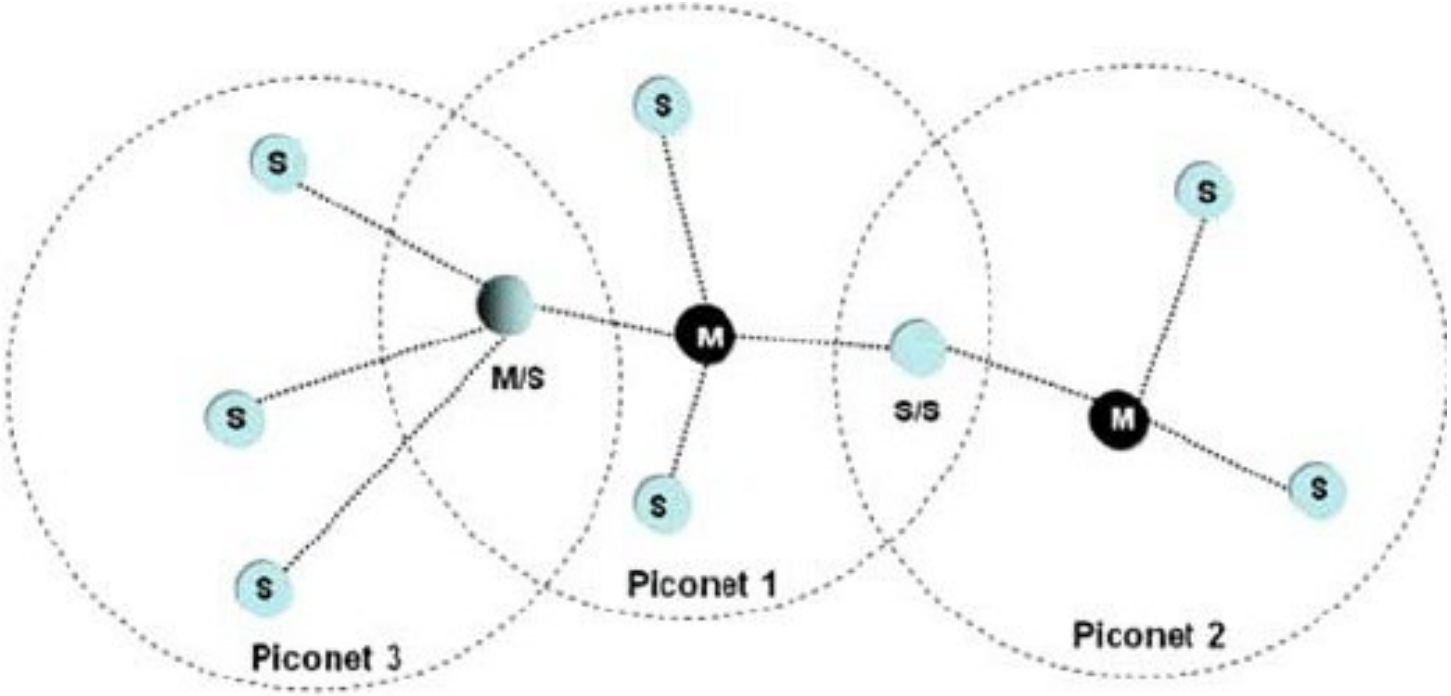
Komunikácia

- založená na paketoch
- Master/Slave architektúra
- jeden Master a max. 7 Slave – piconet
- najnovšie: 1 Master a 14 Slave (v dvoch kanáloch)



Komunikácia

- Scatternet – prepojenie viacerých piconetov (Master v jednej sieti, Slave v inej)



Komunikácia

- synchronizácia Mastrom – každých 312,5 μs (tik hodín)
- slot – 625 μs
- pár – 1250 μs
- paket – 1, 3 alebo 5 slotov
- Master začína v párnom, Slave v nepárnom slote
- možnosť výmeny úloh (Master <-> Slave)
- v jednom čase komunikácia len s jedným
  - zvyčajne round-robin

Výkon a dosah

Trieda	Max. výkon [mW]	Max. výkon [dBm]	Typický dosah [m]
1	100	20	100
1.5	10	10	20
2	**2,5**	**4**	**10**
3	1	0	1
4	0,5	-3	0,5

$$Výkon\ [dBm] = 10.log\ \frac{Výkon\ [mW]}{1\ [mW]}$$

Bluetooth profil

- definícia možných aplikácií, popis správania sa zariadenia
- nastavenia (parametrizácia) a riadenie komunikácie
- jednoduché vytvorenie spojenia

Profil obsahuje:

- závislosť na iných formátoch (profiloch)
- doporučený formát užívateľského rozhrania
- časti BT stacku používané profilom a nastavenia parametrov

Bluetooth profily

- Advanced Audio Distribution Profile (A2DP)
- Human Interface Device Profile (HID)
- Hands-Free Profile (HFP)
- Headset Profile (HSP)
- Serial Port Profile (SPP)
- Attribute Profile (ATT)
- Generic Attribute Profile (GATT)
- prenos súborov, remote control, tlač, video, LAN, Mesh, proximity ...

Verzie Bluetooth

- 1.0 (2000) - bez anonymity
- 1.1 (2002) - IEEE 802.15.1 - možnosť nešifrovaných kanálov, RSSI
- 1.2 (2005) - rýchlejšie spojenie, väčšia rýchlosť (do 721 kb/s), adaptívne FHSS (AFH)
- 2.0 + EDR (2005) - 3 Mb/s (data 2,1 Mb/s)
- 2.1 + EDR (2007) - Secure simle pairing ...
- 3.0 + HS (2009) - prenos až 24 Mb/s, ale cez WIFI

Verzie Bluetooth

- 4.0 (2010) - okrem BT Classic a BT HS obsahuje BLE, GATT
- 4.1 (2013) - software update, podpora zastávania rôznych rolí
- 4.2 (2014) - rozšírenia pre Internet vecí - bezpečnosť, konektivita
- 5 (2016) - rozšírenia najmä pre BLE, Internet vecí, dvojnásobná rýchlosť (2 Mb/s), štvornásobný dosah, 8-násobná kapacita inzerovania (advertising)
- 5.1 (2019) - zlepšenie lokalizácie a sledovania (tracking)
- 5.2 (2019) - LE Audio (one-to-many, many-to-one)
- 5.3 (2021) - interval inzerovania, riadenie šírky šifrovacieho kľúča ...

Bluetooth Low Energy

- od verzie 4.0
- systémy napájané batériami (low power), málo prenášaných dát
  - minimalizácia používania rádiového prenosu
- nie je kompatibilné s BT Classic
  - 40 kanálov so šírkou 2 MHz
  - discovery na 3 kanáloch (32 na BT Classic)
- šifrovanie je voliteľné
  - AES CCM s 128-bit kľúčom
- spätná kompatibilita BLE

Bluetooth Low Energy

- 4.0: 1 Mb/s (300 kb/s)
  5, high-speed: 2 Mb/s (1,34 Mb/s)
  5, long-range: 500 alebo 125 kb/s
- dosah závisí na móde (long-range vs. high-speed)
  - do 100 m, BLE 5 do 1000 m (ideálne podmienky)
- spotreba tiež závisí od nastavení, implementácie ...
  - max. prúd počas vysielania < 15 mA
  - priemerný prúd môže byť < 1 μA
- BLE je asymetrické – väčšina práce je na Mastrovi (riadenie spojenia, časovanie, spracovanie dát)

Bluetooth Low Energy – výhody

V porovnaní s konkurenciou (ZigBee, Z-Wave, Thread ...)

- nižšia spotreba
- špecifikácia zadarmo
- lacnejšie moduly a čipsety
- prítomnosť vo väčšine smartfónov

Bluetooth Low Energy - vlastnosti

- veľmi nízka spotreba (gombíková batéria 1 rok+)
- malé pakety (do 244 B – BLE 5)
- krátke vysielacie a prijímacie okná
  - zapínanie rádia čo najmenej
  - vypínanie rádia čo najskôr
- rýchle pripojenie (cca 6 ms)
- malá spotreba pamäte (cca od 100 kB)
- dáta vo formáte key-value

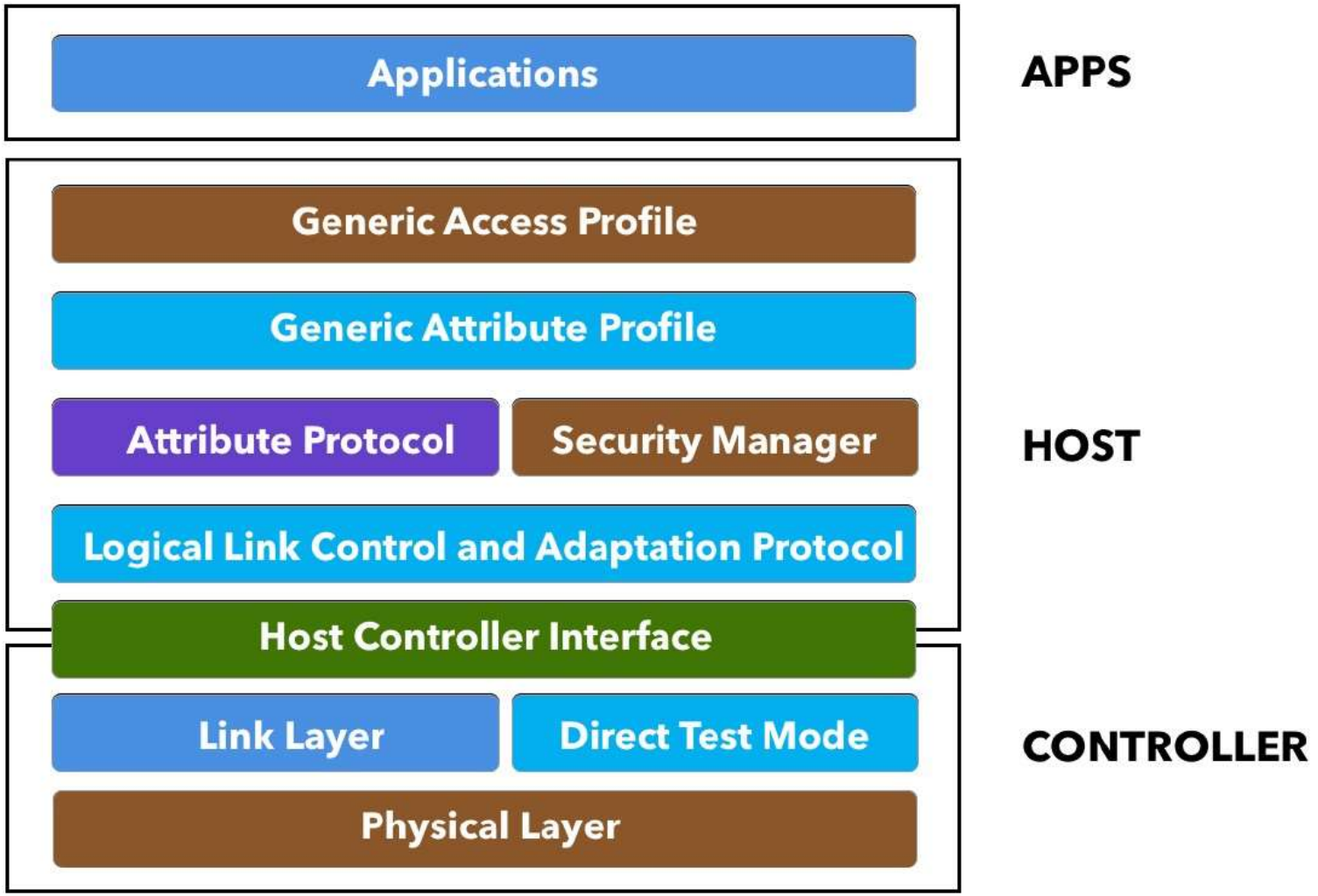
Bluetooth Low Energy - aplikácie

- šport, fitnes
- asistenčná technika, monitorovanie zdravotných funkcií
- smart tagy (kľúče, peňaženka, kufor ...)
- konfigurácia zariadení, smartfón ako používateľského rozhranie
- ovládanie zariadení, zber dát (domáca automatizácia)
- obchod - reklama, kupóny, info o tovare
- navigácia – letiská, múzeá, športové arény
- manažment ľudí (koncert, show)
- monitorovanie zvierat ...

Bluetooth Classic vs. BLE

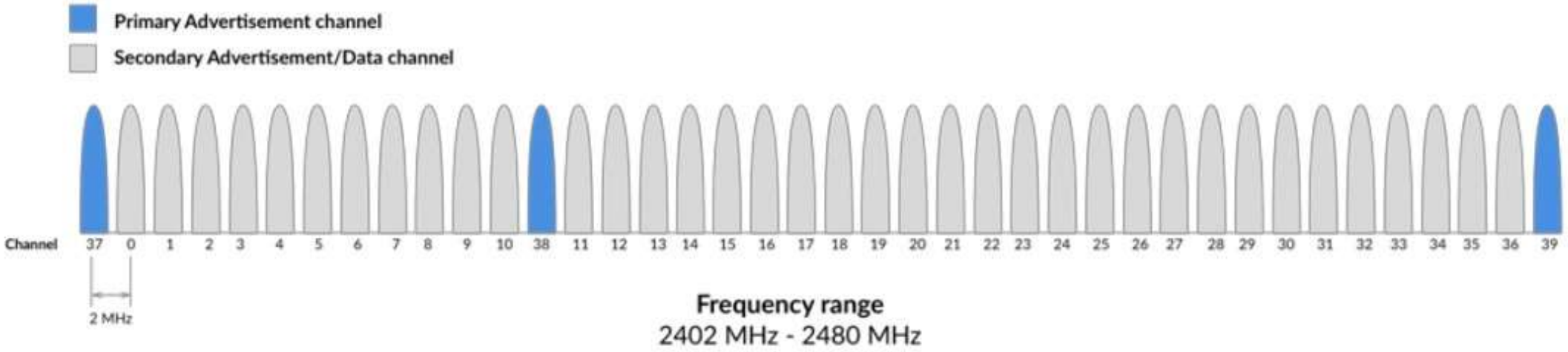
Bluetooth Classic	Bluetooth Low Energy
Streamovacie aplikácie – audio, prenos súborov	Low-bandwidth aplikácie – snímanie dát, ovládanie zariadení
Vyššia rýchlosť, nie pre low-power	Optimalizácia pre low-power
79 kanálov (1 MHz)	40 kanálov (2 MHz)
Discovery na 32 kanáloch	Discovery na 3 kanáloch

Architektúra BLE



Fyzická vrstva

- FHSS, 40 kanálov (2 MHz), 3 kanály primárne inzerovanie
- Do 4.2 – 1 Mb/s, max 10 mW (10 dBm), 5 – 2 Mb/s, 100 mW (20 dBm)
- modulácia, demodulácia



Linková vrstva

- abstrakcia od fyzickej vrstvy pre vyššie vrstvy (cez HCI)
- inzerovanie, skenovanie, vytváranie a udržovanie spojení
- tvorba paketov, riadenie stavu rádia, časovania, hardvérovo akcelerovaných operácií
  - CRC, generovanie náhodných čísiel, šifrovanie
- definuje rolu a stav zariadenia (inzerent, skener, master, slave)

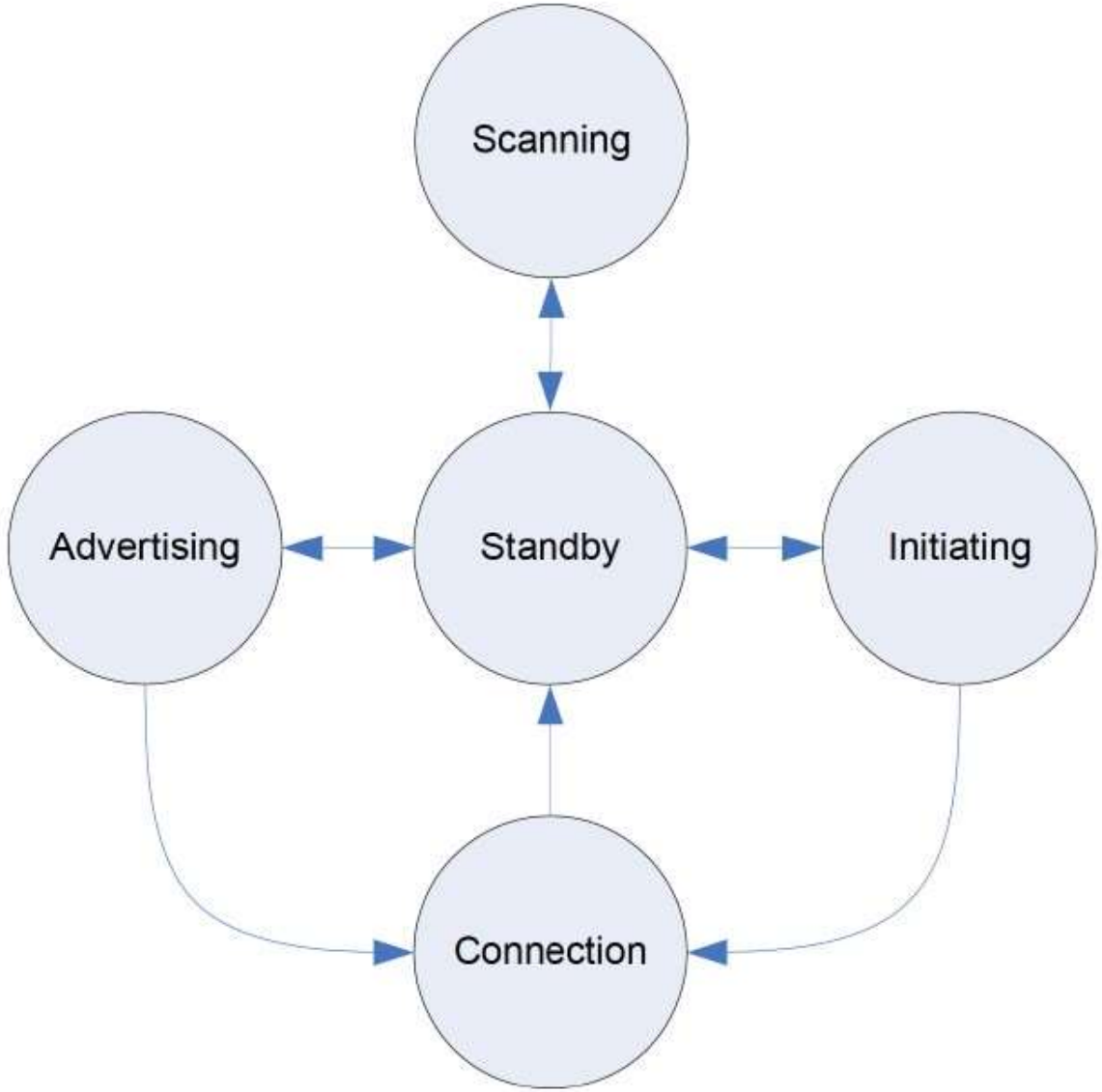
HCI vrstva (Host Controller interface)

- protokol pre komunikáciu medzi Hostom a Controllerom
- možnosť kombináciu čipsetov od rôznych výrobcov

Linková vrstva

Hlavné stavy

- inzerovanie (advertising)
- skenovanie
- pripojenie



Logical Link Control and Adaptation Protocol (L2CAP)

- prepínanie protokolov - z vyššej vrstvy berie rôzne protokoly (ATT a SMP) a tvorí z nich štandardné BLE pakety, ktoré posiela nižšie
- fragmentácia a defragmentácia správ (do 64 kB)

BLE adresa

- 48 bitov, výrobcovia si volia typ adresy
- verejná (public) - pevná adresa registrovaná IEEE, obdoba MAC
- náhodná (random) - nemusí byť registrovaná, generuje sa za behu
  - statická - generovaná pri boote alebo nastavená natvrdo
  - súkromná (private)
    - non-resolvable private address - náhodná, dočasná, nezvykne sa používať
    - resolvable public address - používaná pre zabezpečenie súkromia, pravidelne sa mení

Typy zariadení

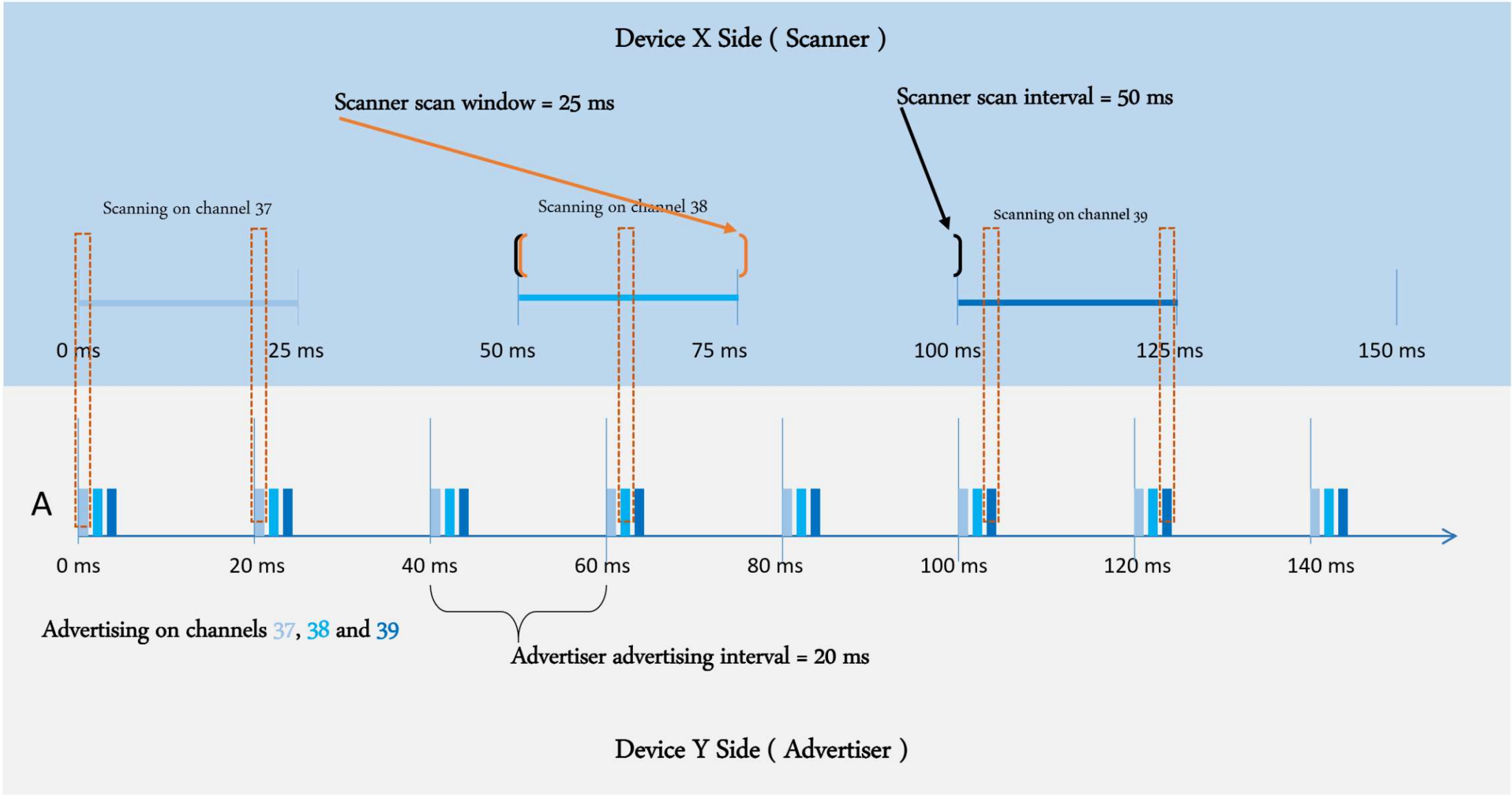
- periféria (peripheral) – inzeruje a umožňuje pripojenie
- centrum (central) – skenuje, počúva a môže sa pripojiť
- observer – skenuje, počúva, ale nepripája sa
- broadcaster – inzeruje, ale neumožňuje pripojenie
  - majáky (možnosť lokalizácie)
  - každý môže počúvať
  - nespoľahlivý prenos

Inzerovanie (Advertising)

- pravidelne s pevným intervalom (20 ms – 10,24s s krokom 625 μs)
  (kratšia perióda = vyššia spotreba ale príjemnejšie pre používateľa)
- 3 kanály na primárne inzerovanie, max 31 B dát
  v každej perióde inzeruje vo všetkých kanáloch
- prídavné informácie – odpoveď na scan request = scan response
  (max 31/254 B) „aktívne skenovanie“

Skenovanie

- periodicky, v oknách (perióda a okno môžu byť rovnaké)
- Scan Window - ako dlho skenovať
- Scan Interval - ako často skenovať
- Typ: pasívne - len počúvanie inzercie
  aktívne - scan request - scan response


Device X Side (Scanner)
Scanner scan window = 25 ms
Scanner scan interval = 50 ms
Scanning on channel 37
Scanning on channel 38
Scanning on channel 39
0 ms
25 ms
50 ms
75 ms
100 ms
125 ms
150 ms
A
0 ms
20 ms
40 ms
60 ms
80 ms
100 ms
120 ms
140 ms
Advertising on channels 37, 38 and 39
Advertiser advertising interval = 20 ms
Device Y Side (Advertiser)

Módy periférie z hľadiska viditeľnosti

- Non-Discoverable Peripheral - default, nie je možné odhalenie ani spojenie
- Limited-Discoverable Peripheral - obmedzené z hľadiska času, odhalenie možné len určitý čas
- General-Discoverable Peripheral - inzeruje na neurčitú dobu, kým nedôjde k spojeniu

Módy periférie z hľadiska spojenia

- Non-connectable Peripheral - nie je možné vytvoriť spojenie (Broadcaster alebo Idle)
- Directed-connectable Peripheral - periféria inzeruje, kto sa môže pripojiť
- Undirected-connectable Peripheral – ktokoľvek, ak je na whiteliste

8 typov inzerujúcich paketov:

Connectable and Scannable Undirected, Connectable Undirected, Connectable Directed, Non-Connectable and Non-Scannable Undirected,Non-Connectable and Non-Scannable Directed, Scannable Undirected, Scannable Directed

directed – len pre určité zariadenia, undirected – pre všetkých

Inzerujúci paket a Scan Response paket

Pozostávajú z niekoľko AD štruktúr:

- dĺžka (1B): spolu typ + dáta
- typ (min 1B)
  - meno
  - TX power level (dBm)
  - príznaky o schopnostiach BT
  - **UUID podporovaných služieb**
  - typ/vzhľad zariadenia (Appearance) ...
- dáta (max. 31 resp. 254 B)

Môže obsahovať aj dáta napr. zo snímača

Vytvorenie spojenia

1. Periféria musí inzerovať (typ connectable)
2. Centrálne zariadenie skenuje, prečíta si inzerujúci paket
3. Central vyšle Connection request paket (CONNECT_IND)
4. Spojenie je vytvorené (created) ale nie platné (established).
   Platné je až po prijatí paketu od periférie.
   Central = Master
   Periféria = Slave

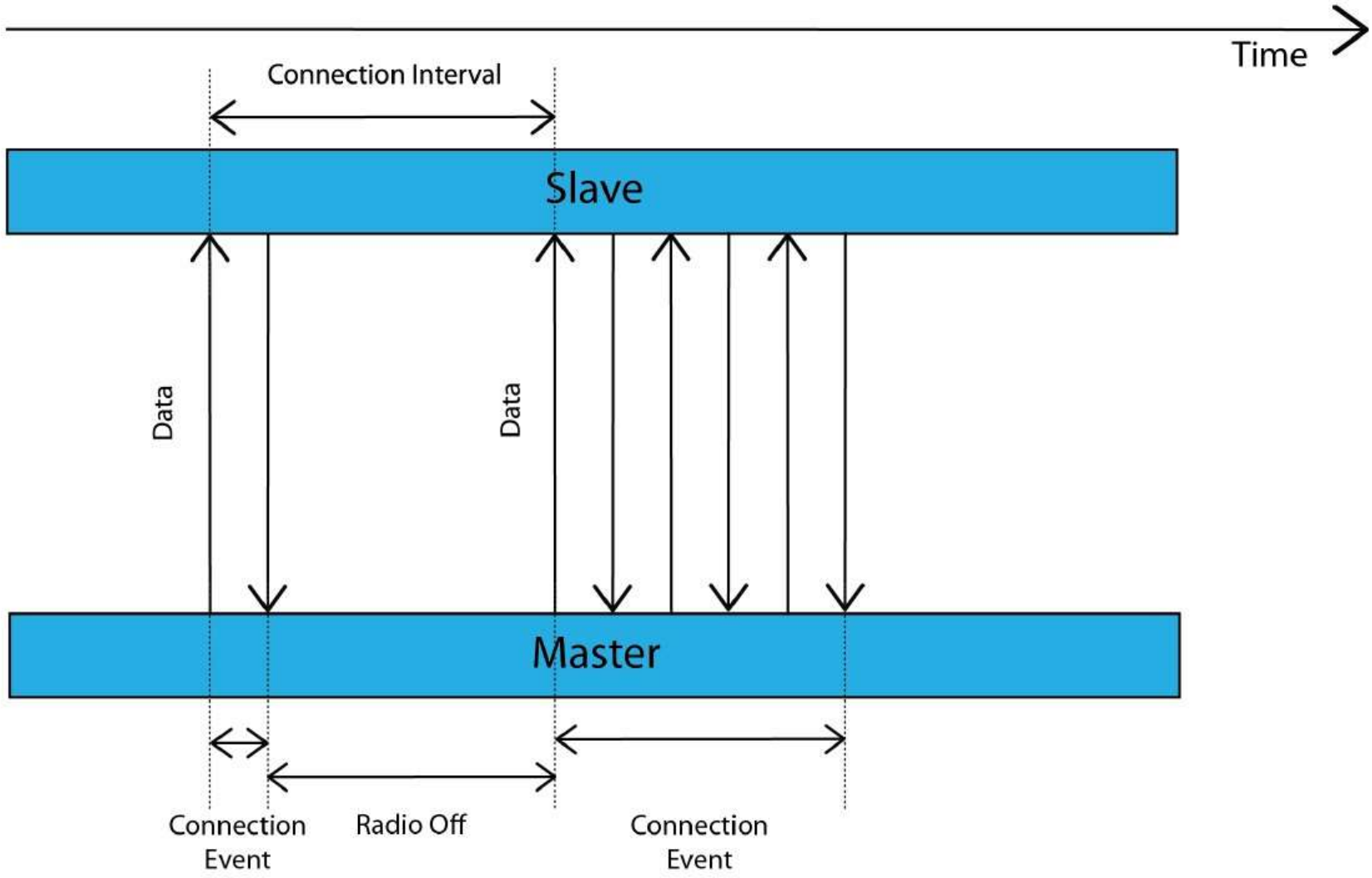
Udalosť spojenia (Connection Event)

- Master a Slave si vymieňajú pakety, kým majú čo posielať

Vlastnosti:

- opakované periodicky až do ukončenia alebo straty spojenia (začiatky udalostí sú oddelené intervalom spojenia)
- udalosť obsahuje aspoň jeden paket od Mastra
- Slave vždy odpovedá na paket od Mastra
- ak Master nedostane odpoveď, ukončí udalosť a pokračuje pri ďalšej udalosti (t.j. spojenie sa nezruší)
- udalosť môže ukončiť každá strana

Connection Event



Parametre spojenia

- Interval spojenia – 7,5 ms - 4s s krokom 1,25 ms – nastavuje Master
- Slave latency – počet udalostí spojenia, ktoré Slave môže vynechať
- Supervision timeout – max. čas medzi dvomi prijatými paketmi aby nebolo stratené spojenie: 100 ms - 32s s krokom 10 ms
  *Timeout > (1 + Slave latency) * Interval spojenia * 2*
  (výnimka: po vytvorení spojenia sa čaká *6 * Interval spojenia*)
- Data Length Extension (DLE) – možnosť posielať až do 251 B dát, namiesto 27 B (od ver. 4.2)
- Maximum Transmission Unit (MTU) – max. veľkosť paketu

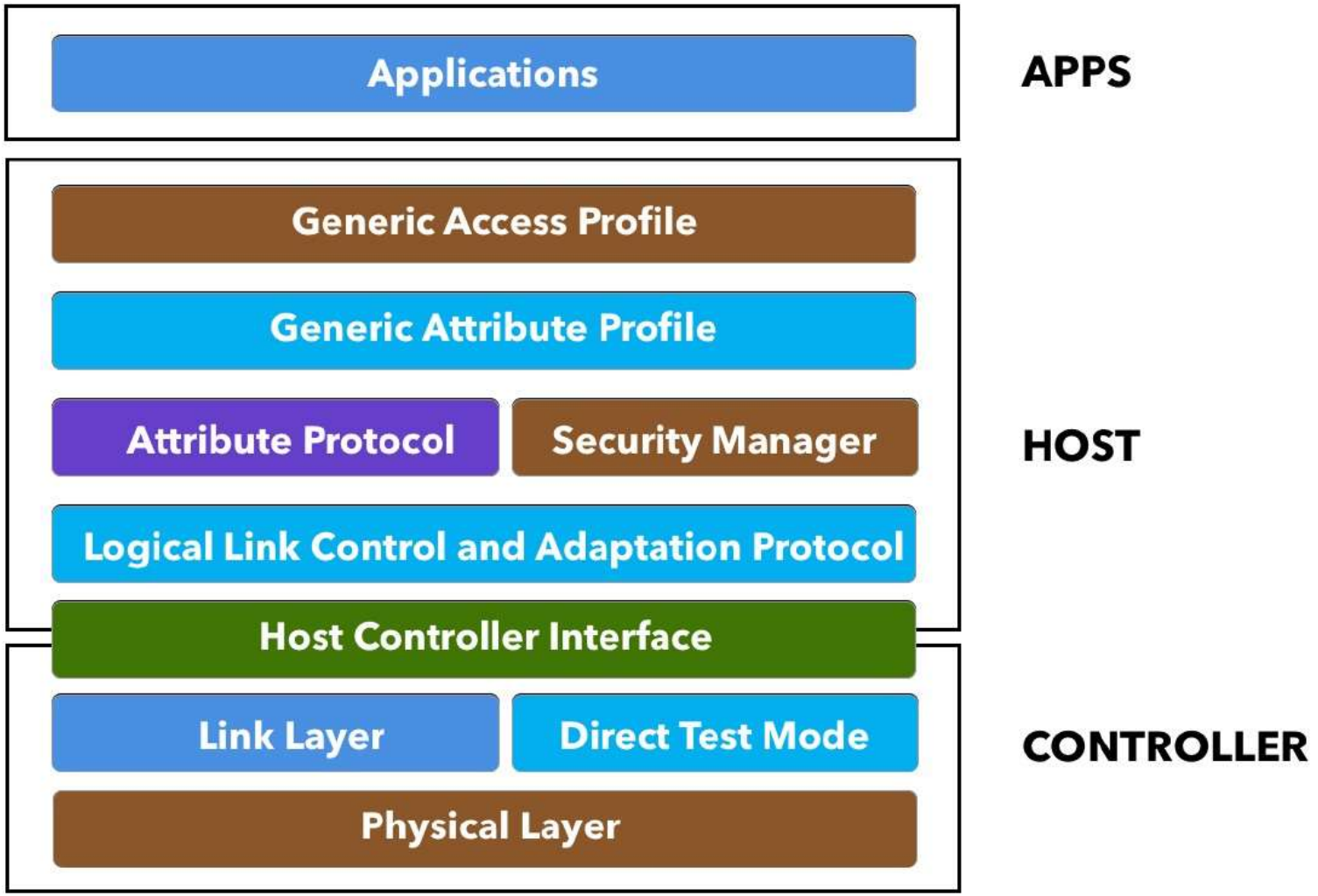
White list

- zoznam adries a typov adries zariadení
  - umožňuje určiť aké zariadenia nás zaujímajú
  - "anonymous" zodpovedá všetkým
- filtrovanie na linkovej vrstve (controller)
  - šetrí prácu vyšším vrstvám (host)

Typy White listov

- Inzerovanie (periféria)
  - prijíma všetky požiadavky od každého (žiadny white list)
  - prijíma všetky požiadavky len z white listu
  - skenovanie z white listu, pripojenie od každého
  - skenovanie od každého, pripojenie z white listu
- Skenovanie (central)
  - spracuje inzerciu od všetkých alebo len z white listu
- Iniciovanie spojenia (central)
  - iniciovanie spojenia všetkým z white listu
  - len zariadeniu zvolenému hostiteľom (nie je možné spojenie so zariadením, ktoré nie je z white listu)

Architektúra BLE



Attribute protocol (ATT)

- definuje spôsob sprístupnenia dát a štruktúru dát

Dva typy zariadení (role):

- server
  - poskytuje dáta
  - prijíma príkazy a posiela odpovede, notifikácie a indikácie
- klient
  - číta/zapisuje dáta na serveri, nastavuje notifikácie a indikácie

Dáta sú štruktúrované v podobe atribútov (key-value)

Štruktúra atribútu

- handle (key)
  - 16 bit číslo, ktoré server priraďuje atribútu (adresa, referencia)
- UUID – typ atribútu
  - 16 bit. (definované atribúty – Bluetooth SIG-Adopted Attributes)
  - ľubovoľné 128 bit. číslo (okrem Base UUID)
- povolenia (permissions)
  - čítanie, zápis s/bez potvrdenia, notifikácia, indikácia, úroveň bezpečnosti
- hodnota (value), dáta

Služba

- zoskupenie jedného alebo viac atribútov, ktoré navzájom súvisia (napr. služba Battery service - charakteristika Battery level)
- niektoré atribúty sú charakteristikami
- obsahuje aj atribúty, ktoré slúžia na štruktúrovanie dát (deklarácie)
- môže obsahovať aj odkazy na iné služby (include)

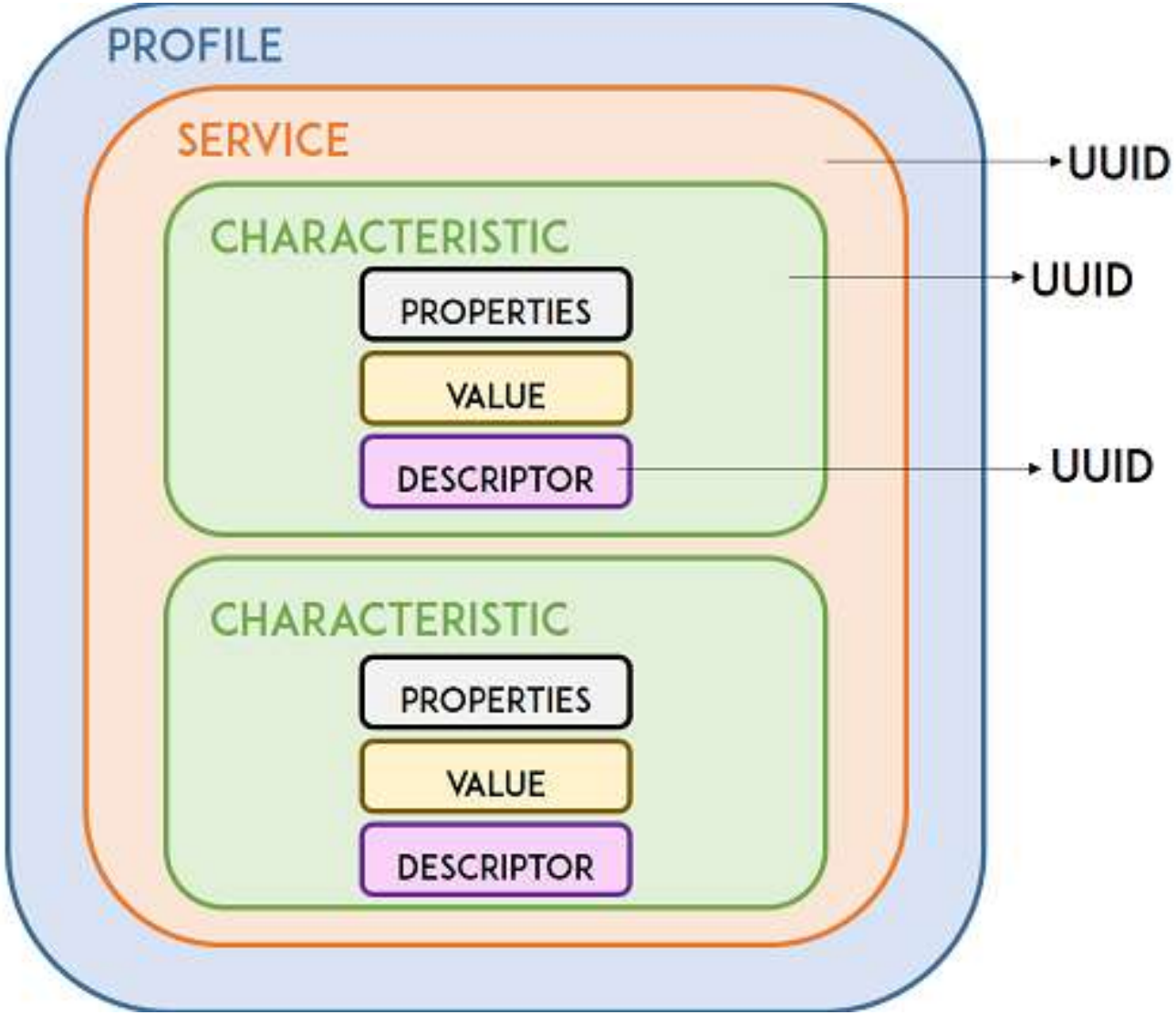
Charakteristika

- je vždy súčasť služby
  - dáta, ktoré server poskytuje klientovi
- najnižšia úroveň v hierarchii atribútov

Obsahuje:

- hodnotu (dáta)
- deklaráciu (metadáta) – typ, spôsob použitia (read, write, write without response, notify, indicate)
- deskriptor/y – rozšírené vlastnosti, užívateľský popis, formát hodnoty, jednotka ...

Hierarchická štruktúra dát



Generic Attribute protocol (GATT)

- framework na manažovanie dát

Definuje

- formát služieb (services)
- formát charakteristík (characteristics)
- spôsob interakcie s atribútmi (service discovery, čítanie a zápis charakteristík, notifikácie, indikácie)

Tie isté role ako ATT, ale na úrovní transakcií – počas jedného spojenia môže byť to isté zariadenie chvíľu serverom a chvíľu klientom

Typy základných operácií

- Príkaz (command) – posiela klient, nevyžaduje odpoveď
- Žiadosť (request) – posiela klient, vyžaduje odpoveď
  - Find Information Request
  - Read Request
- Odpoveď (response) – odpoveď servera na žiadosť
- Notifikácia (notification) – informácia klientovi o zmene dát, nevyžaduje odpoveď
- Indikácia (indication) – to isté ako notifikácia, ale vyžaduje odpoveď
- Potvrdenie (confirmation) – posiela klient serveru, potvrdenie prijatia indikácie

Operácie s atribútmi

Čítanie atribútov

- Read request
- Read blob request

Zápis atribútov

- Write request – vyžaduje odpoveď, že dáta boli zapísané
- Write command – nevyžaduje odpoveď
- Queued writes – žiadosť (vyžaduje odpoveď), umožňuje atomický zápis väčších dát
  (Prepare write request, Execute write request)

Generic Access Profile (GAP)

- framework na manažovanie BLE zariadenia
- módy a roly zariadení (periféria, centrum, observer, broadcaster)
- procedúry na nájdenie zariadenia a vytvorenie spojenia
- inzerovanie a skenovanie (parametre, dáta)
- zjednodušuje párovanie, "bonding", šifrovanie, podpisovanie dát, zabezpečenie súkromia

GAP je povinná časť – umožňuje interoperabilitu

Profil

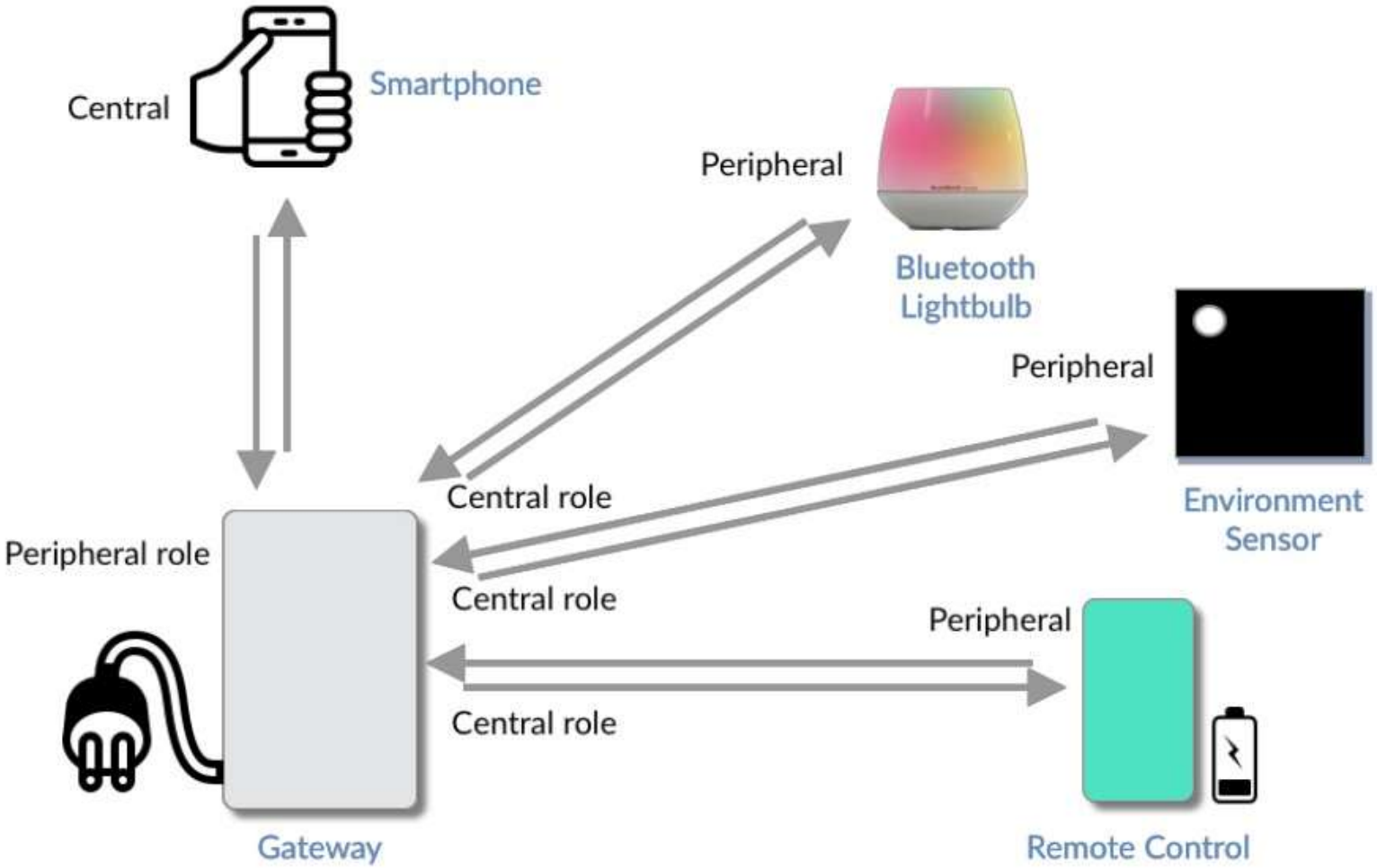
- aplikačná vrstva pre konkrétny prípad použitia

Zvyčajne obsahuje

- definíciu rolí a vzťahy medzi GATT serverom a klientom
- požadované (povinné) služby
- použitie služieb a charakteristík
- detaily o vytvorení spojenia vrátane parametrov inzerovania a pripájania
- požiadavky na zabezpečenie

Príklady profilov

- Heart Rate Profile (HRP) - tep srdca
- Health Thermometer Profile (HTP) – teplota
- Proximity Profile (PXP) - (hľadanie kľúčov), alarm po link loss
- Cycling Speed and Cadence Profile (CSCP) – rýchlosť, vzdialenosť, kadencia, prevod
- Running Speed and Cadence Profile (RSCP) - rýchlosť, kadencia, vzdialenosť, počet krokov
- Apple Notification Center Service (ANCS) - notifikácie z iOS: zmeškané hovory, hlasové maily, emaily ...


Central
Smartphone
Peripheral
Bluetooth
Lightbulb
Peripheral
Environment
Sensor
Central role
Peripheral role
Central role
Peripheral
Central role
Gateway
Remote Control

Ukážky

Bluetooth Classic

- Bluetooth RC Controller – SPP profil

Bluetooth Low Energy

- BLE Scanner

SPP aj BLE UART

- Serial Bluetooth Terminal

Vytvorené v rámci projektu KEGA 026TUKE-4/2021