Bluetooth mesh

Ondrej Karpiš, 2023

Vytvorené v rámci projektu KEGA 026TUKE-4/2021

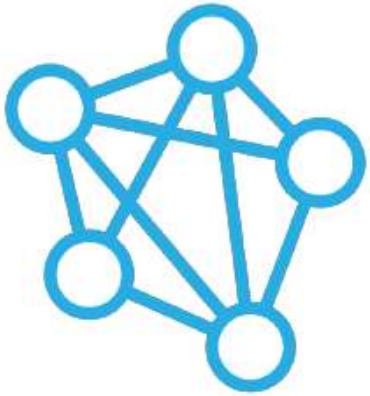
Bluetooth mesh

Mesh – topológia many-to-many (preposielanie správ)

- 2017 – Bluetooth mesh standard (samostatný)
- podpora BLE od 4.0, vyžaduje kompletný BLE stack
- SW update
- BT mesh 1.0 nepodporuje vlastnosti pridané BT 5

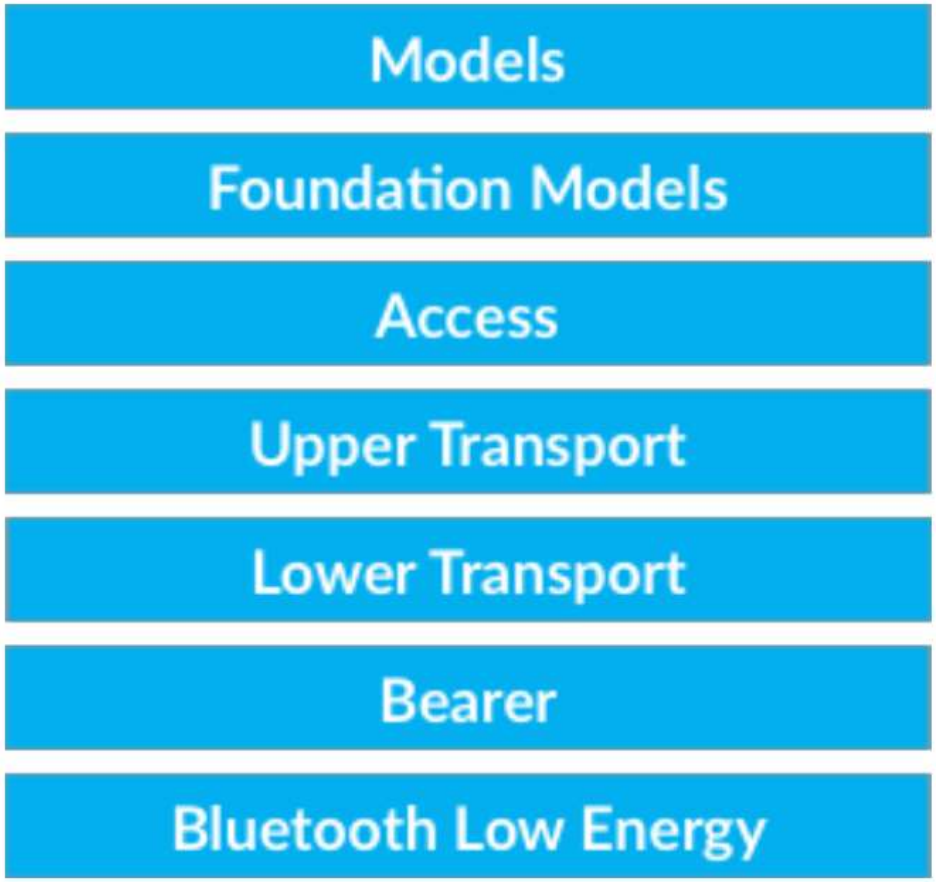
Vlastnosti BT mesh

- zväčšený dosah oproti BLE
- samoliečiaca schopnosť (self-healing)
- prenos správ pomocou inzerovania a skenovania
- rýchlosť prenosu cca 3,4 kb/s



Many-to-many

Architektúra BT mesh



Architektúra BT mesh

- Bearer layer – práca s rôznymi paketmi (Protocol Data Unit - PDU)
  - Advertising bearer – prenos dát v rámci mesh siete
  - GATT bearer – iné zariadenia (cez proxy node)
- Lower transport layer – spracovanie väčších paketov
- Upper transport layer – šifrovanie a dešifrovanie, autentifikácia, riadiace správy transportnej vrstvy
- Access layer – definuje, ako aplikácia využíva upper transport layer
- Foundation models layer – konfigurácia a manažment siete
- Models layer – implementácia modelov (správanie, správy, stavy, prepojenia stavov)

Terminológia

Nody – uzly mesh siete

Elementy – časti nodu, ktoré je možné samostatne ovládať

Stavy – stavy elementu. Zmena (state transition) zvyčajne spôsobí zmenu správania elementu. Môžu byť prepojené (bound)

Vlastnosti (properties) – vysvetlenie kontextu pre stavy

- Manufacturer property – len na čítanie
- Admin property – čítanie a zápis

Typy nodov

Nod – základný typ, žiadne špeciálne vlastnosti

Relay nod – dokáže preposielať správy

Proxy nod – komunikácia so zariadeniami bez BLE

Low power nod – nod s obmedzeným napájaním, musí mať priateľa

Friend nod – priateľ LPN, uchováva pre neho správy

Friendship

- vzťah LPN a friend nodu
- kľúčový koncept pre podporu low-power

Správy

BT mesh – message-oriented

Správa vyvolá operáciu na jednom alebo viacerých stavoch

- GET správa – žiadosť na čítanie stavu
- SET správa – príkaz na zmenu hodnoty stavu
- STATUS správa
  - odpoveď na GET správu – obsahuje hodnotu stavu
  - odpoveď na potvrdzovanú SET správu
  - nezávislé na iných správach – oznam o stave elementu

Správy môžu vyžadovať potvrdenie (acknowledgment)

Doručovanie správ – Managed flooding

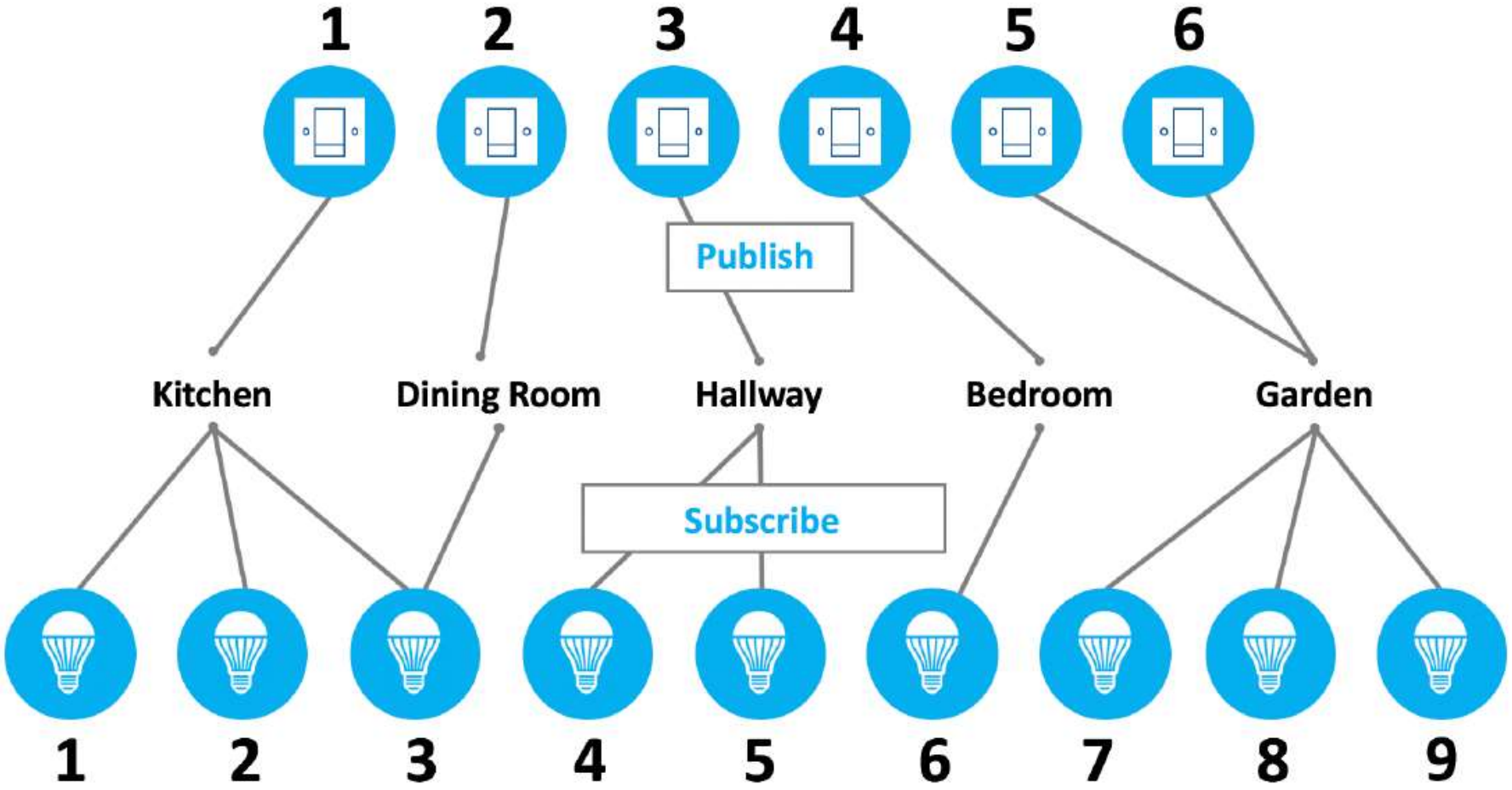
Prenos správ broadcastom s vylepšeniami:

- TTL (time-to-live) – obmedzenie počtu hopov správ
  - 0 - správa nebola preposielaná (relayed) a ani sa nemá preposielať
  - 1 - správa bola preposlaná a nemá sa preposlať
  - 2 a viac - má s preposlať (so zníženým TTL)
- správy sú buffrované
- pravidelné vysielanie Hartbeat správ
- Friendship

Adresy

- unicast adresa – identifikuje nod v rámci siete, pridelená počas provisioningu
- skupinová adresa (group) – spoločná pre skupinu nodov
  - SIG-Fixed group address - definovane BT SIG: All-proxies, All-friends, All-relays, All-nodes
  - dynamické adresy - definované používateľom
- virtuálne adresy – jeden/viac elementov na jednom/viac nodoch (128 bit UUID)

Publish - subscribe



Model

- definuje časť alebo všetku funkcionalitu elementu

- Server model – súbor stavov, zmien stavov, prepojení stavov a správ, ktoré môže element prijímať alebo vysielať
- Client model – nedefinuje stavy ale len správy GET, SET a STATUS posielané server modelu
- Control model – obsahuje server aj client model. Umožňuje komunikáciu s ďalšími server a client modelmi.

Scéna

- uložený súbor stavov
- identifikovaná jedinečným 16-bitovým číslom
- umožňuje jednou akciou nastaviť viaceré stavy na rôznych nodoch

Provisioning - pridanie zariadenia do siete

1. Beaconing – zariadenia začne vysielať beacon
2. Invitation (pozvánka) – špeciálny typ paketu. Zariadenie odpovie paketom o svojich schopnostiach.
3. Výmena verejného kľúča – priamo pomocou BLE alebo pomocou OOB (Out-of-band)
4. Autentifikácia (overenie) – zvyčajne vyžaduje zásah používateľa na obidvoch zariadeniach
5. Distribúcia provision dát – network key, bezpečnostný parameter IV index a unicastová adresa

Zariadenie sa stáva nodom.

Bezpečnosť

- je povinná
- všetky správy sú šifrované a autentifikované
- nezávislé oblasti bezpečnosti – device security, application security, network security
- bezpečnostné kľúče sa môžu meniť

Kľúče

- sieťový kľúč – jeho vlastnenie robí zariadenie nodom, dešifrovanie a autentifikovanie správy po sieťovú vrstvu (preposielanie správ)
- aplikačný kľúč – zdieľaný zariadeniami zapojenými do rovnakej aplikácie (osvetlenie, zabezpečenie budovy, kúrenie ...)
- device key – pre konkrétne zariadenie, používa sa len počas provisioningu na zabezpečenie komunikácie
- privacy key – pre zabezpečenie súkromnosti, zahmlievanie adresy odosielateľa

Ochrana pred útokmi

- Trash can attack - prístup do siete prostredníctvom vyradených zariadení
  - zariadenie sa dá na black list
  - vymenia sa všetky kľúče (sieťové a aplikačné)

- Replay attack - opakovanie správ zariadením útočníka
  - používanie sequnce number (SEQ) - elementy zvyšujú SEQ v každej správe
  - inkrementovanie IV indexu - tiež sa validuje po prijatí správy

Otázky z oblasti Bluetooth

- Princípy šetrenia energie v bezdrôtových sieťach
- Hlavné stavy BLE zariadenia
- Komunikácia medzi BLE zariadeniami (operácie)
- Terminológia v BT mesh (nod, element, stav, správa ...)
- Friendship
- Publish-subscribe

Vytvorené v rámci projektu KEGA 026TUKE-4/2021