BLUETOOTH

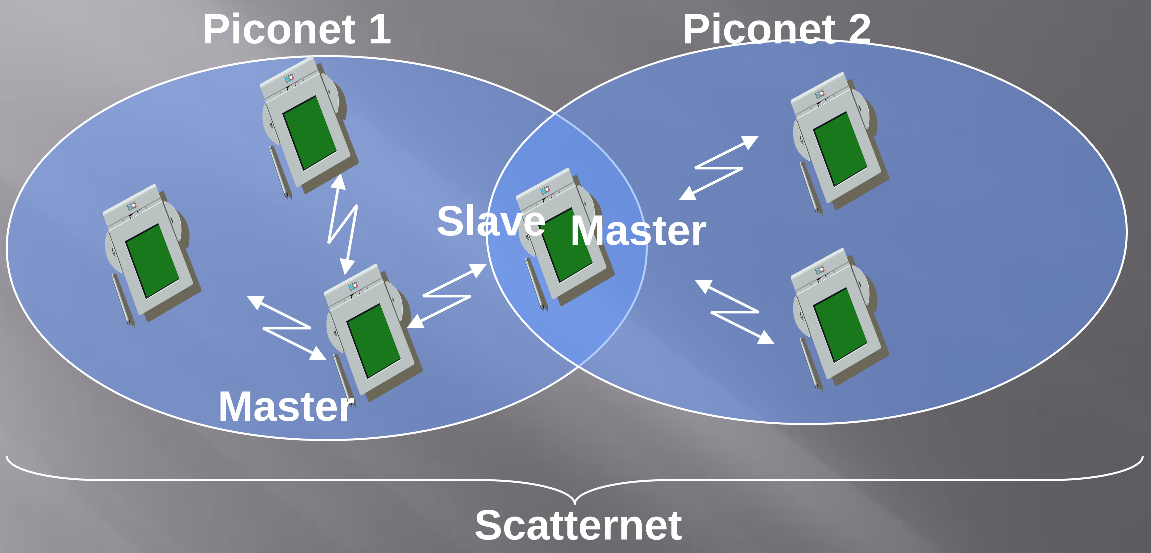
Image: plug-in.bestbuy.ca

Introduction

- Bluetooth is named after Harald Blaatand
- Originally started by Ericsson
- Designed as a cable replacement technology
- Used for short range communication (10 m)

Image :sites.psu.edu

System Architecture



- Piconet – set of bluetooth nodes synchronized to a master node.
- Scatternet – set of Piconets.
- One master can communicate with 7 slaves.

Standardization

- Originally started out as IEEE 802.15.1
- Now the Bluetooth SIG oversees the development of the specification, manages the qualification program, and protects the trademarks.
- To be marketed as a Bluetooth device, it must be qualified to the standards set by the SIG.
- The Bluetooth patents are licensed for the qualifying devices.

Market

- Canadian Users:
  - 35 million x 75% = 26 million users

- Equipment Sales:
  - 26 million users x $40 per year = $1 billion per year
  - 26 million users x $200 per year = $5 billion per year

- Licensing

How Bluetooth Operates

- Uses the ISM band (2.402 – 2.480 GHz).
- Uses FHSS over 79 channels (1MHz each) at 1600 hops/s.
- Jumps from channel to channel in a pseudo random sequence

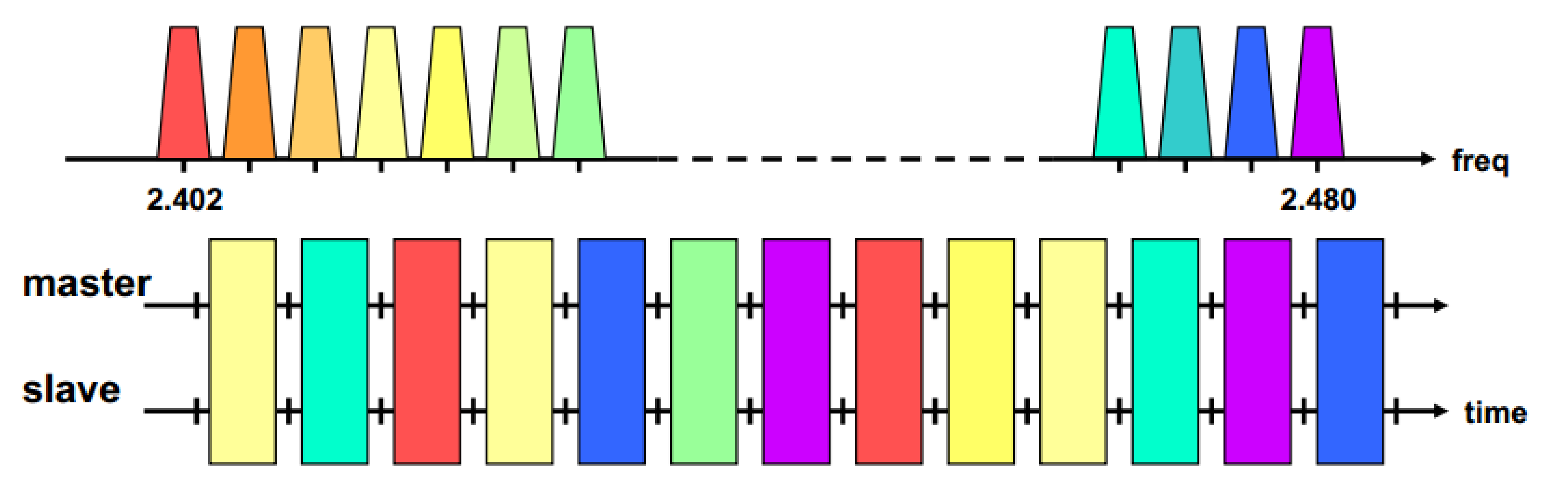


Image: http://mmlab.kaist.ac.kr/menu2/popup/ICE839/Bluetooth.pdf

How Bluetooth Operates

- 1Mbps data rate, or 2 – 3 Mbps with EDR.
- Bluetooth uses GFSK.
  - Bluetooth 2.0+EDR uses DQPSK and DPSK

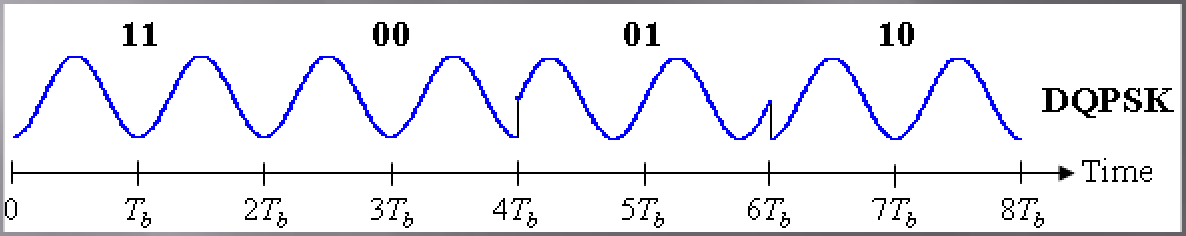


Image: http://en.wikipedia.org/wiki/DQPSK

Bluetooth Audio

- Voice encoding:
  - Pulse code modulation (PCM)
  - 64 kbit/s Continuously variable slope delta (CVSD) modulation
    - CVSD encodes at 1 bit per sample, so that audio sampled at 16kHz is encoded at 16kbit/s.

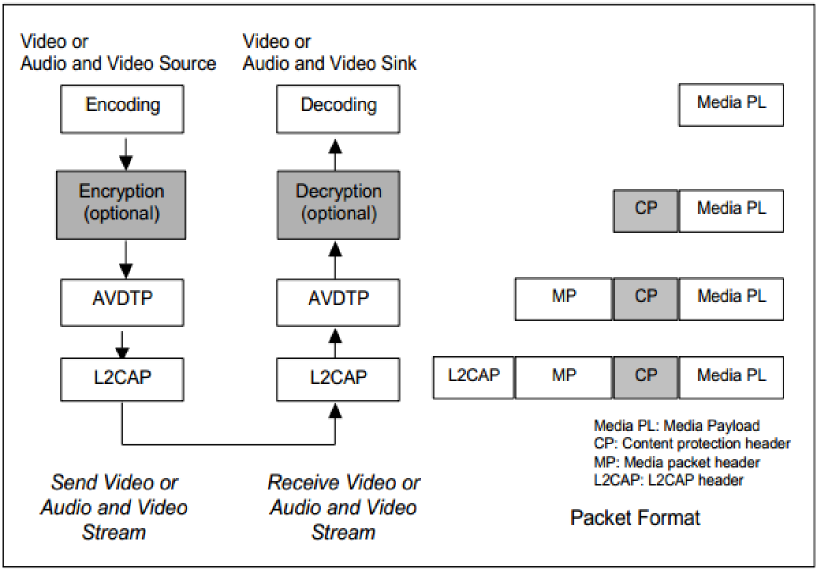


Image: http://developer.bluetooth.org/TechnologyOverview/Documents/VDP_SPEC.pdf

Bluetooth Security

- Based on SAFER+ encryption algorithm
- Elements:
  - Authentication – verify claimed identity
  - Encryption – privacy
  - Key management and usage
- Security algorithm parameters:
  - Unit address
  - Secret authentication key (128 bits key)
  - Secret privacy key (4-128 bits secret key)
  - Random number

Bluetooth Security

- Bluejacking
- 2005
  - Lasco – used Bluetooth enabled devices to replicate and spread.
  - Thieves able to track down cars/homes of people from Bluetooth enabled devices.
- 2007
  - Demonstrated first Bluetooth PIN and Linkkeys cracker.

Link Budget

- The nominal transmit power is 0 dBm.
- The thermal noise power at room temperature is -174 dBm/Hz or -114 dBm for the bandwidth of 1 MHz.
- Noise floor is allowed to be hight for a low cost reciever 23 dB.
- Receiver sensitivity is -70 dBm.
- The C/I level is 21 dB.

$$\frac{C}{I} = \frac{P_{b(p_v)} G_{b\_em(p_v)}(\theta_v, \phi_v)}{\sum_{i \in A_v} P_{b(p_i)} G_{b\_em(p_i)}(\theta_v, \phi_v) + \sum_{j \in B_v} P_{b(p_j)} G_{b\_em\_cp(p_j)}(\theta_v, \phi_v)}$$

- Total link budget is 70 dB.
- Mean free space propagation loss is ~ -55 dB
- Leaves 15 dB link margin for:
  - Shadow fading
  - Multipath fading
  - Floor attenuation

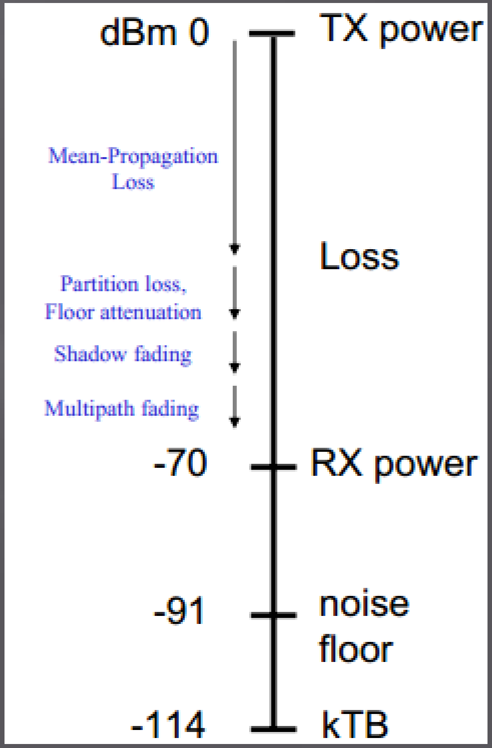


Image: http://mmlab.kaist.ac.kr/menu2/popup/ICE839/Bluetooth.pdf

References

- http://developer.bluetooth.org/Pages/default.aspx
- http://en.wikipedia.org/wiki/Bluetoothhttp://mmlab.kaist.ac.kr/menu2/popup/ICE839/Bluetooth.pdf
- http://www.mobileinfo.com/Bluetooth/FAQ.htm#r5
- http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA445220
- http://www.hp.com/rnd/library/pdf/understandingBluetooth.pdf