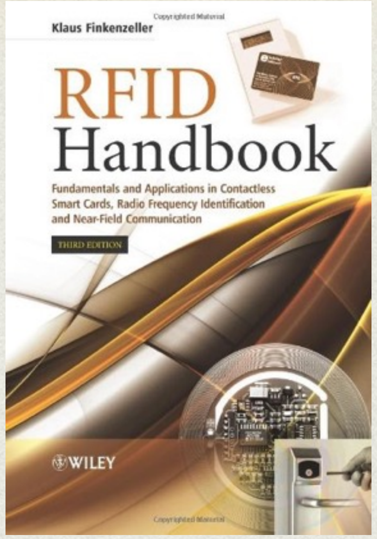
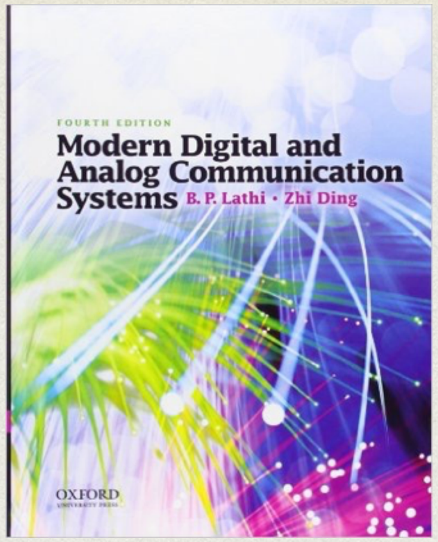
BLUETOOTH LOW ENERGY

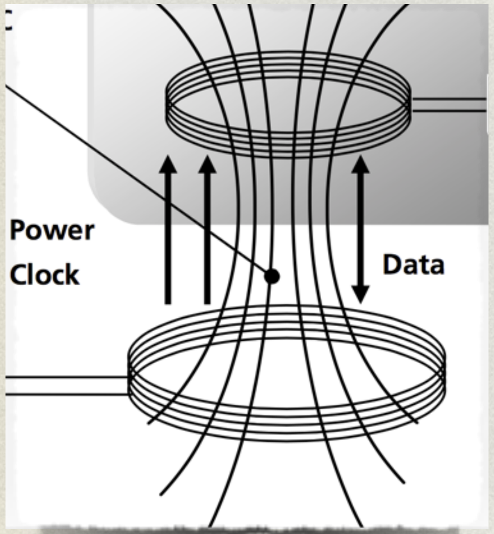
SMART CHOICE WITH JUST A FEW CAVEATS

Tomáš Rosa, Ph.D., OK1SFU

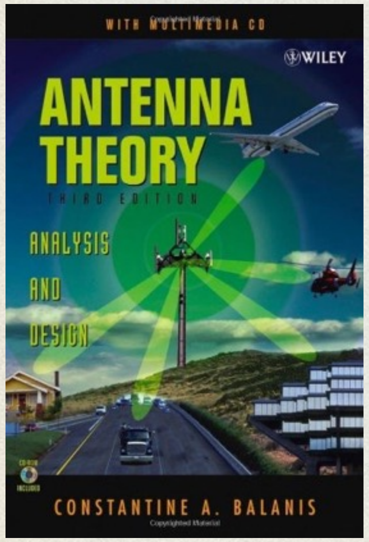
Raiffeisenbank a.s.

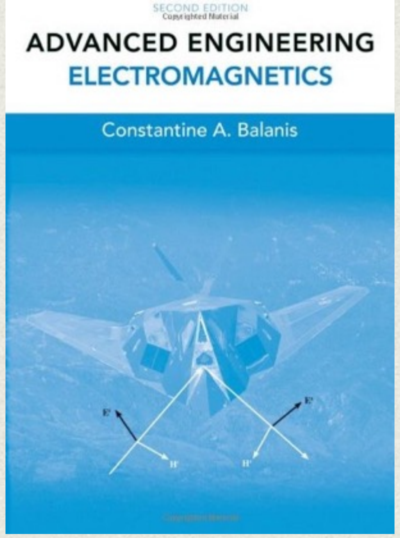


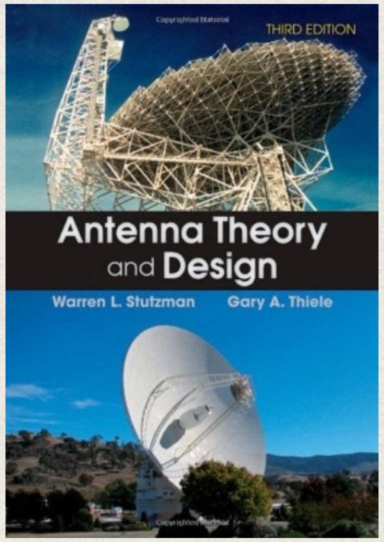


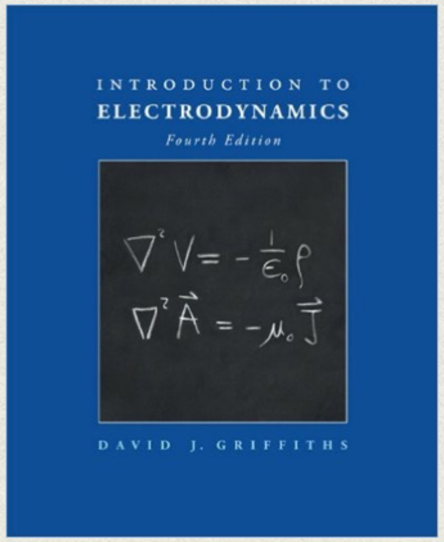


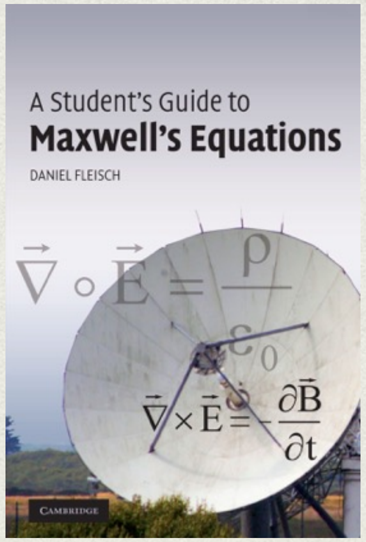
NFC CONTRA FFC

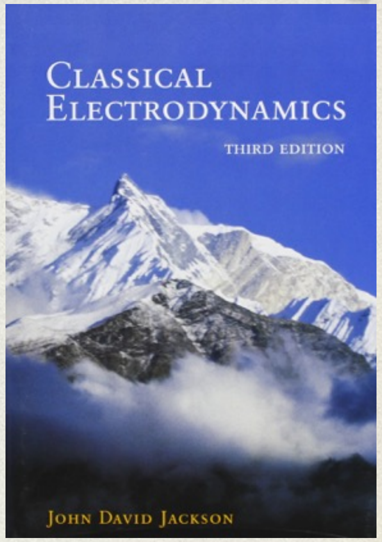












START WITH SOMETHING FAMILIAR

[Buddipole QRV by 5B8AP]

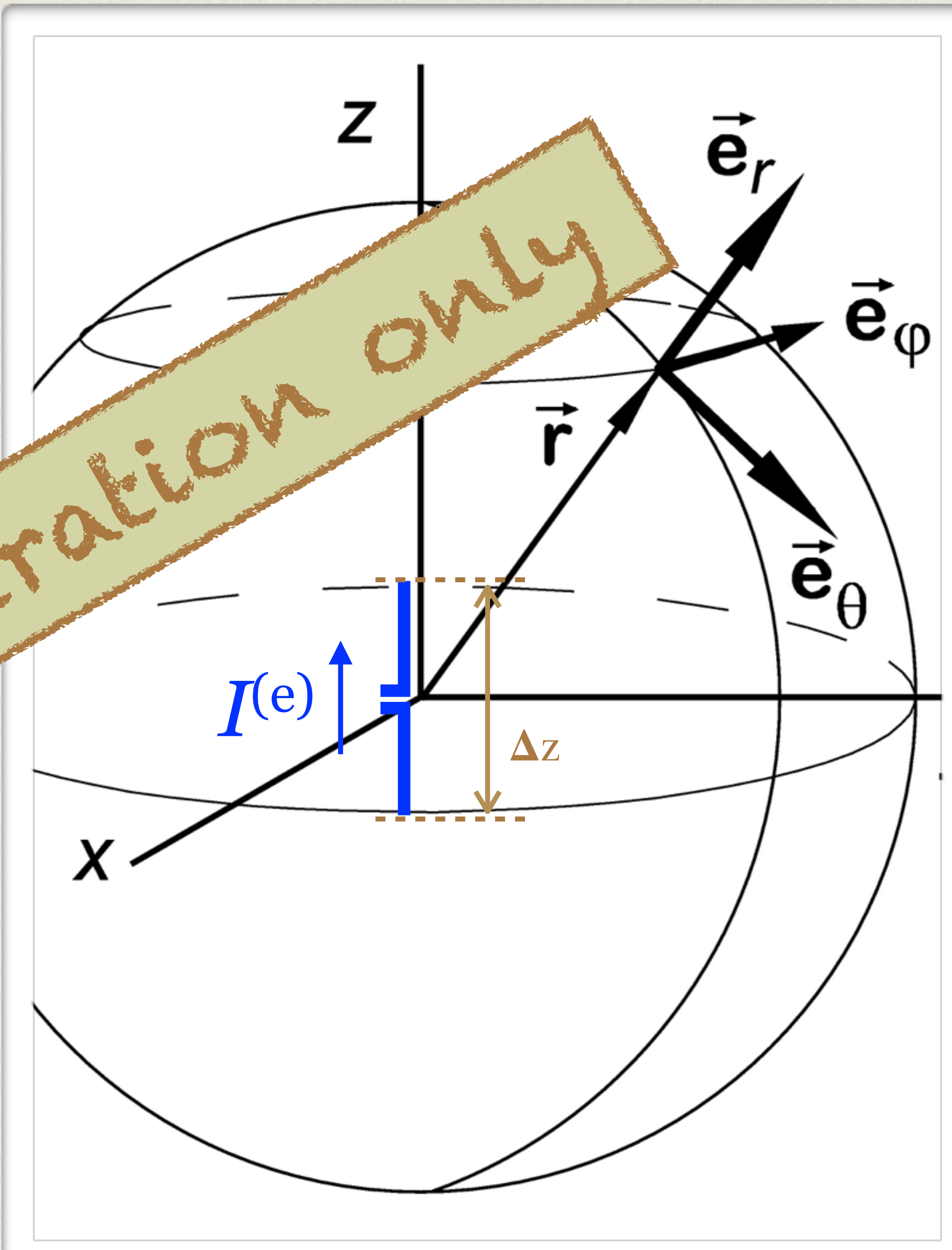
THE IDEAL ELECTRIC DIPOLE

- Electrically small, i.e. $\Delta z << \lambda$, uniform amplitude current element.
  - Ordinary dipole is covered by integration over these elements.
- In the far field, a donut-like pattern bearing t[illegible] vertical polarisation is produced.
- In general, its field has the fol[illegible] components.

$\vec{E}_{edp}(I^{(e)}) = E$ [illegible] $\hat{e}_\theta + E_{edp,r}(I^{(e)}) \cdot \hat{e}_r$

$\vec{H}_{edp}(I^{(e)}) =$ [illegible] $_{edp,\phi}(I^{(e)}) \cdot \hat{e}_\phi$

keep calm, illustration only



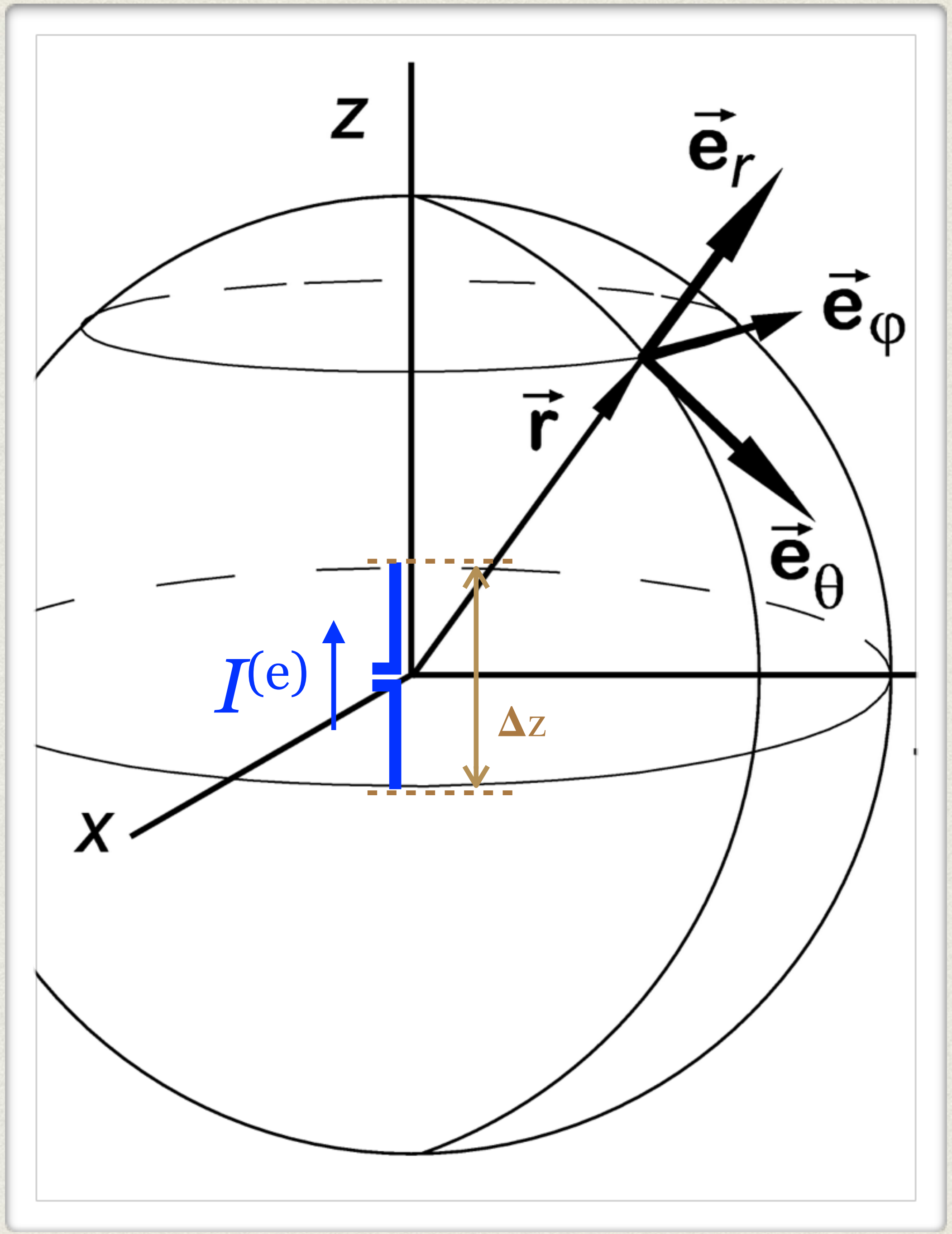
(illustration purpose only)

THE IDEAL ELECTRIC DIPOLE

- Electrically small, i.e. Δz << λ, uniform amplitude current element.
  - Ordinary dipole is covered by integration over these elements.
- In the far field, a donut-like pattern bearing the vertical polarisation is produced.
- In general, its field has the following components.

$$\overrightarrow{E}_{edp}(I^{(e)}) = E_{edp,\theta}(I^{(e)}) \cdot \widehat{e_\theta} + E_{edp,r}(I^{(e)}) \cdot \widehat{e_r}$$

$$\overrightarrow{H}_{edp}(I^{(e)}) = H_{edp,\phi}(I^{(e)}) \cdot \widehat{e_\phi}$$



(illustration purpose only)

LONG STORY SHORT

$$\vec{H}_{edp}(I^{(e)}) = \frac{I^{(e)}\Delta z}{4\pi} j\beta\left(\frac{1}{r} + \frac{1}{j\beta r^2}\right)e^{-j\beta r}\sin\theta \cdot \hat{e}_\phi$$

$$\vec{E}_{epd}(I^{(e)}) = \frac{I^{(e)}\Delta z}{4\pi} j\omega\mu\left(\frac{1}{r} + \frac{1}{\cdots}\cdots\right)e^{\cdots}\sin\theta \cdot \hat{e}_\theta$$

$$+\frac{I^{(e)}\Delta z}{2\cdots}\cdots\frac{\cdots}{\cdots\beta r^2} - \frac{1}{\beta^2 r^3})e^{-j\beta r}\cos\theta \cdot \hat{e}_r$$

$$\cdots\frac{\cdots}{4\pi} j\omega\mu\left(\frac{1}{r} + \frac{1}{j\beta r^2} - \frac{1}{\beta^2 r^3}\right)e^{-j\beta r}\sin\theta \cdot \hat{e}_\theta$$

$$+\frac{I^{(e)}\Delta z}{2\pi}\eta\left(\frac{1}{r^2} - j\frac{1}{\beta r^3}\right)e^{-j\beta r}\cos\theta \cdot \hat{e}_r$$

keep calm, illustration only

LONG STORY SHORT

$$\vec{H}_{edp}(I^{(e)}) = \frac{I^{(e)}\Delta z}{4\pi} j\beta(\frac{1}{r} + \frac{1}{j\beta r^2})e^{-j\beta r}\sin\theta \cdot \hat{e}_\phi$$

$$\vec{E}_{epd}(I^{(e)}) = \frac{I^{(e)}\Delta z}{4\pi} j\omega\mu(\frac{1}{r} + \frac{1}{j\beta r^2} - \frac{1}{\beta^2 r^3})e^{-j\beta r}\sin\theta \cdot \hat{e}_\theta$$

$$+\frac{I^{(e)}\Delta z}{2\pi} j\omega\mu(\frac{1}{j\beta r^2} - \frac{1}{\beta^2 r^3})e^{-j\beta r}\cos\theta \cdot \hat{e}_r$$

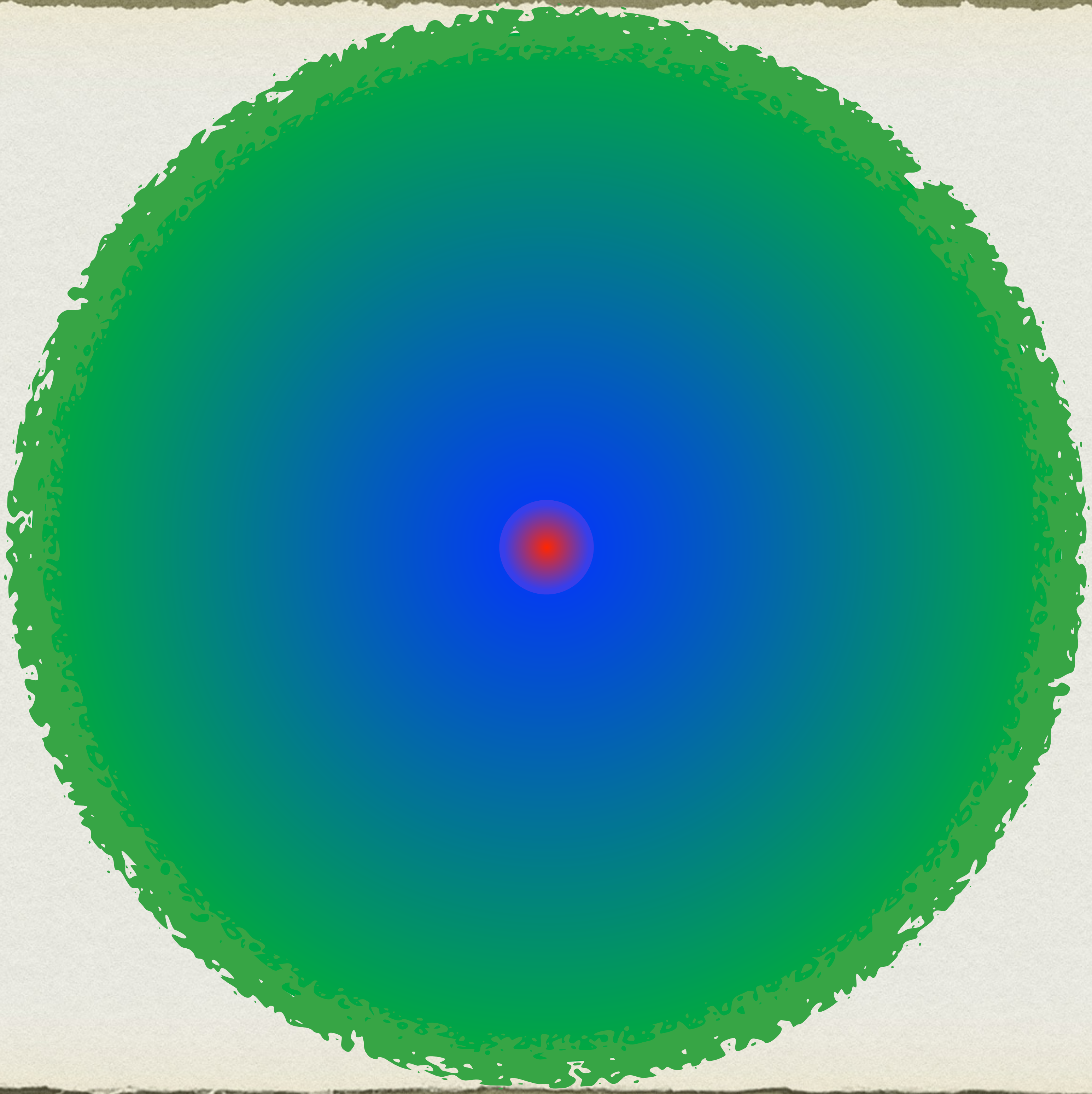
$$= \frac{I^{(e)}\Delta z}{4\pi} j\omega\mu(\frac{1}{r} + \frac{1}{j\beta r^2} - \frac{1}{\beta^2 r^3})e^{-j\beta r}\sin\theta \cdot \hat{e}_\theta$$

$$+\frac{I^{(e)}\Delta z}{2\pi} \eta(\frac{1}{r^2} - j\frac{1}{\beta r^3})e^{-j\beta r}\cos\theta \cdot \hat{e}_r$$

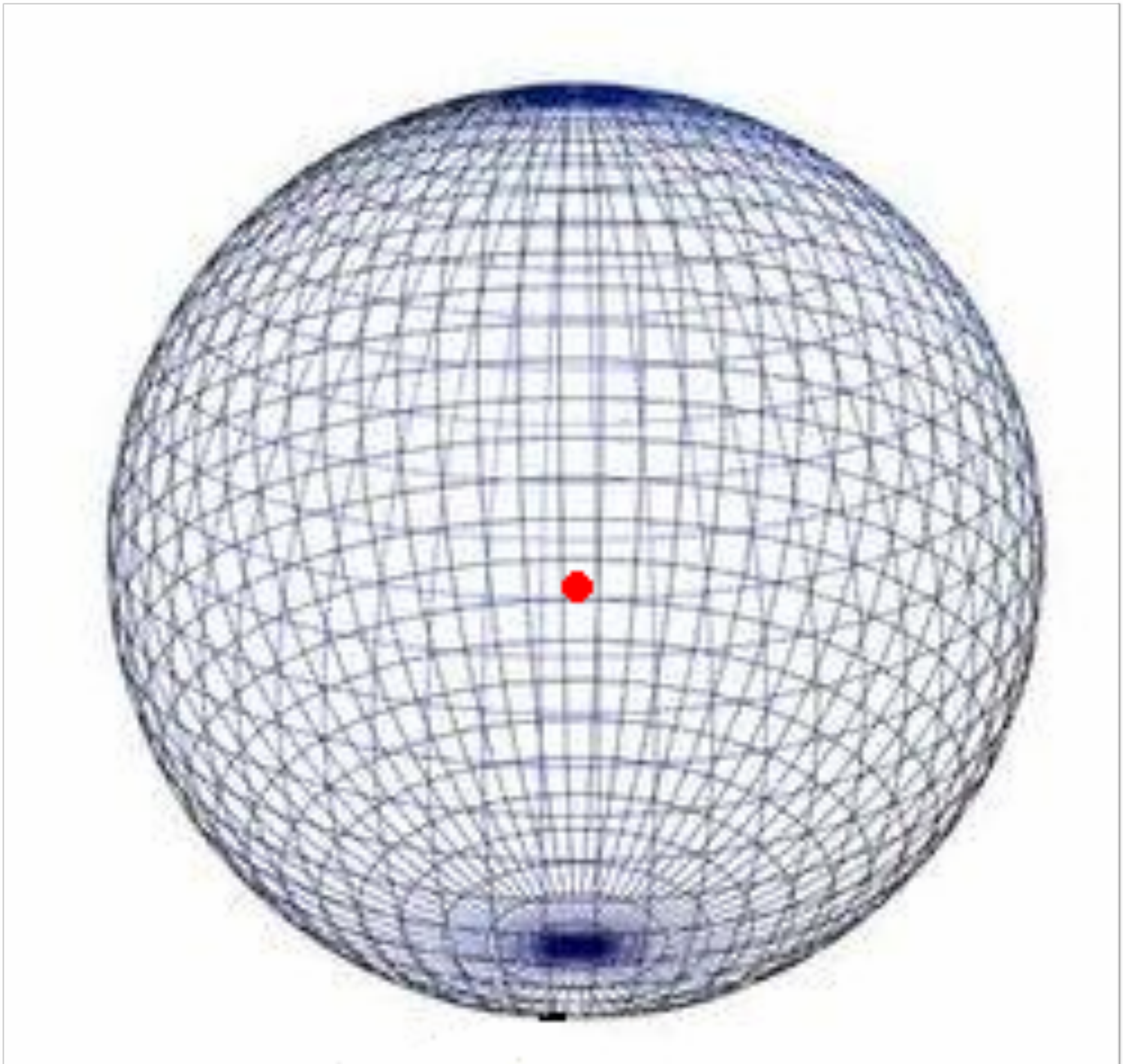
NEAR, FAR

- Basing on the dominating *E*, *H* field terms, it is useful to distinguish:
  - *Reactive near field* (XNF), where the terms with $1/r^2$ and $1/r^3$ dominate. Energy is mainly stored and exchanged between *E* and *H*.
  - *Radiating near field* (Fresnel region), where the $1/r^2$ terms start to dominate, i.e. $r > \lambda/2\pi$. Energy is mainly radiated with unstable patterns, however.
  - *Far field* (Fraunhofer region), where the $1/r$ terms remain to dominate and the plane wave model can be used. Several conditions shall be met: $r > 2D^2/\lambda$, $r > 5D$, $r > 1.6\lambda$, where D is the largest antenna dimension. Energy is radiated with a distance-independent field pattern.

WHEREVER YOU ARE

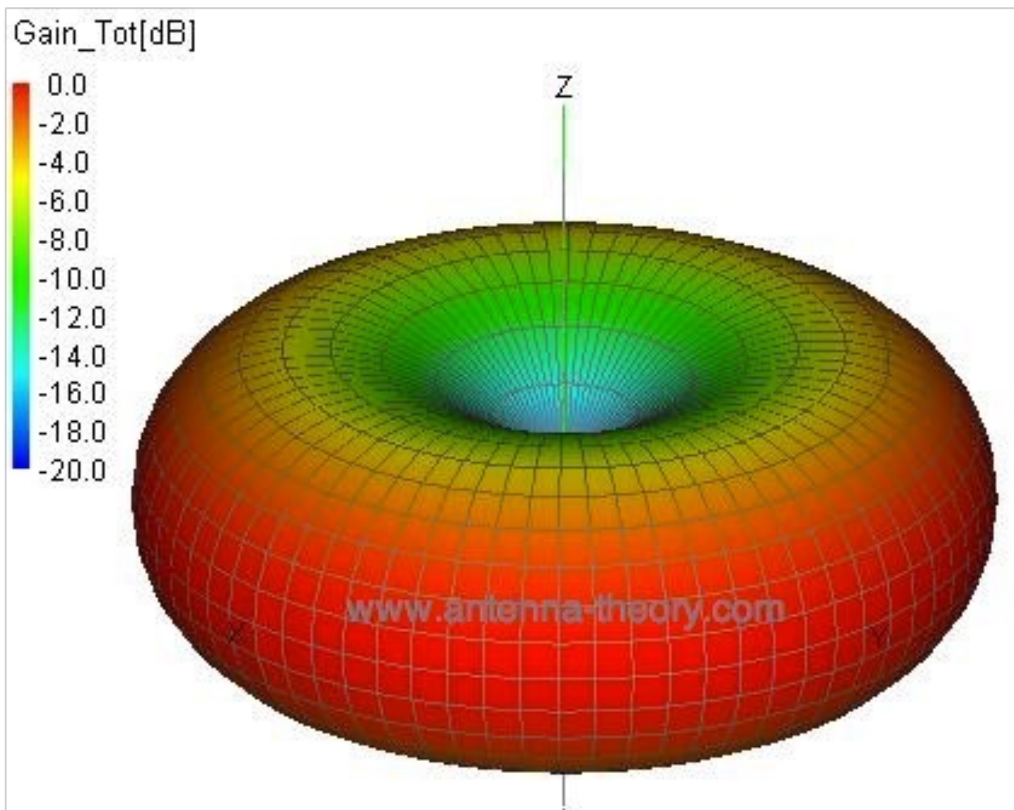


UNDERSTANDING DIRECTIVITY AND GAIN

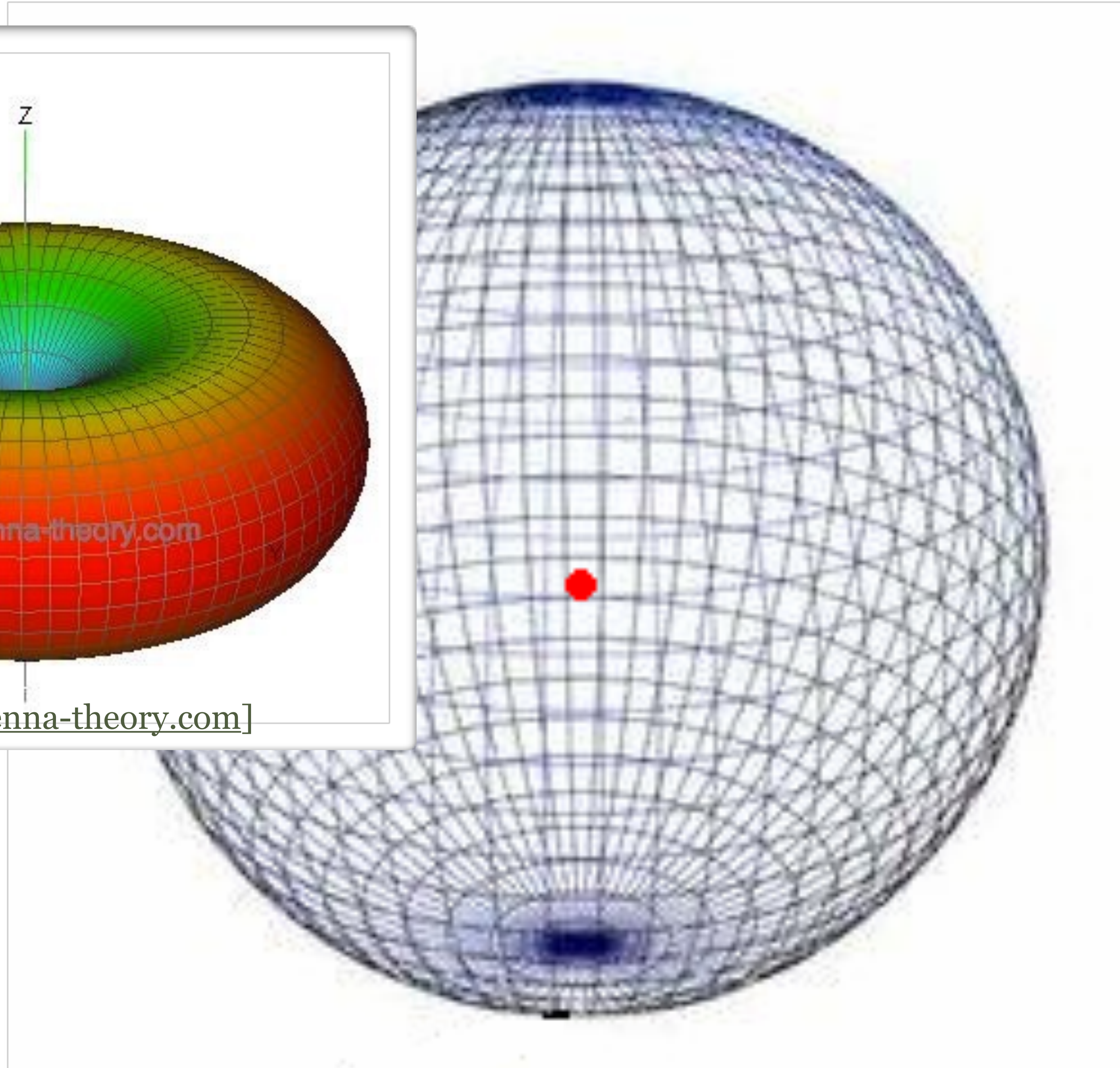


[Isotropic Radiator by www.dx-antenna.com]

UNDERSTANDING DIRECTIVITY AND GAIN

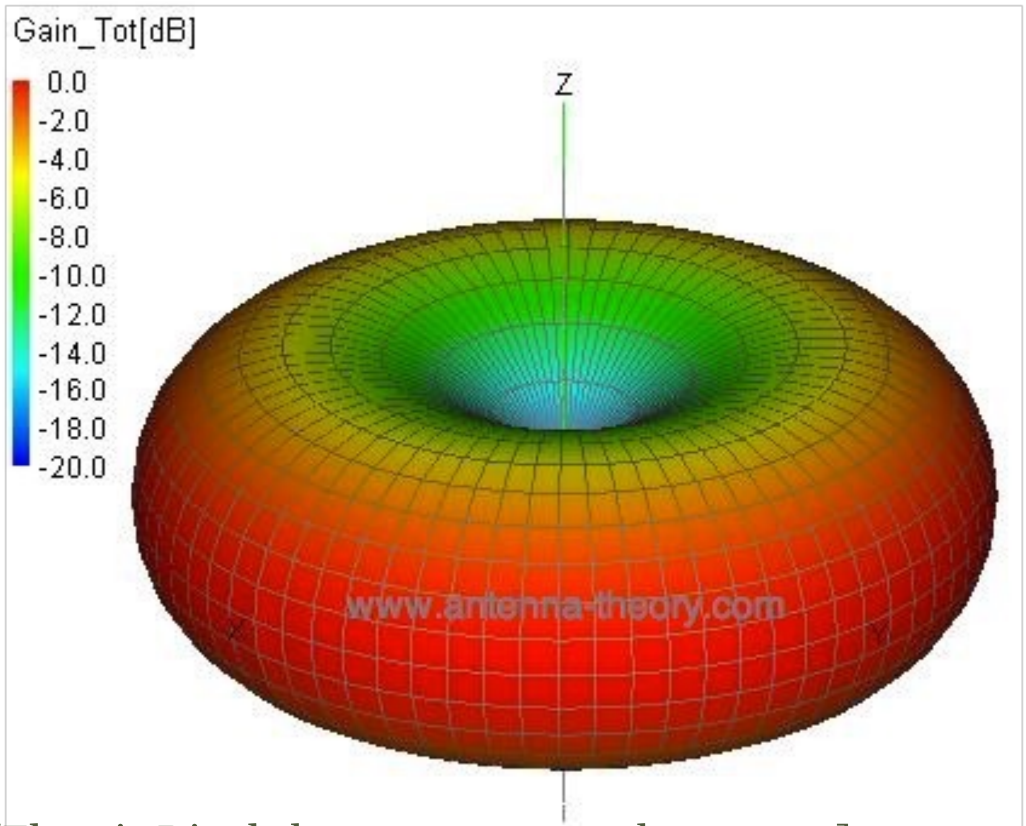


[Electric Dipole by www.antenna-theory.com]

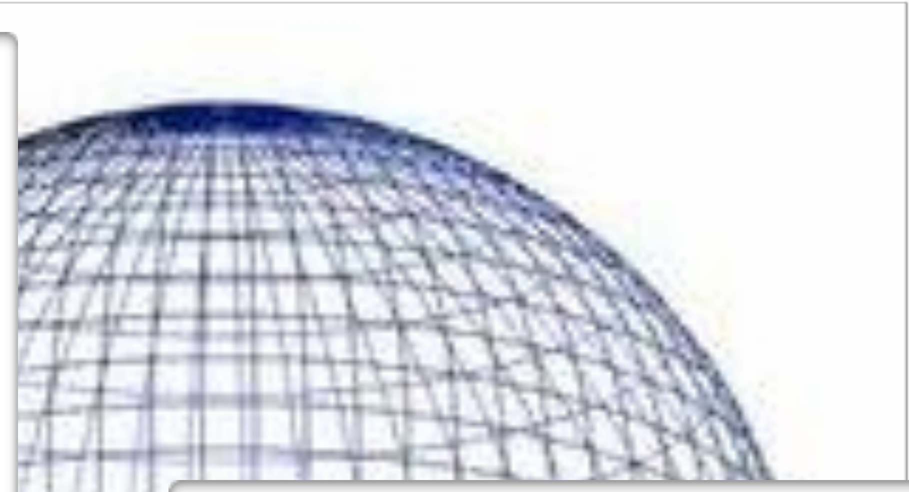


[Isotropic Radiator by www.dx-antenna.com]

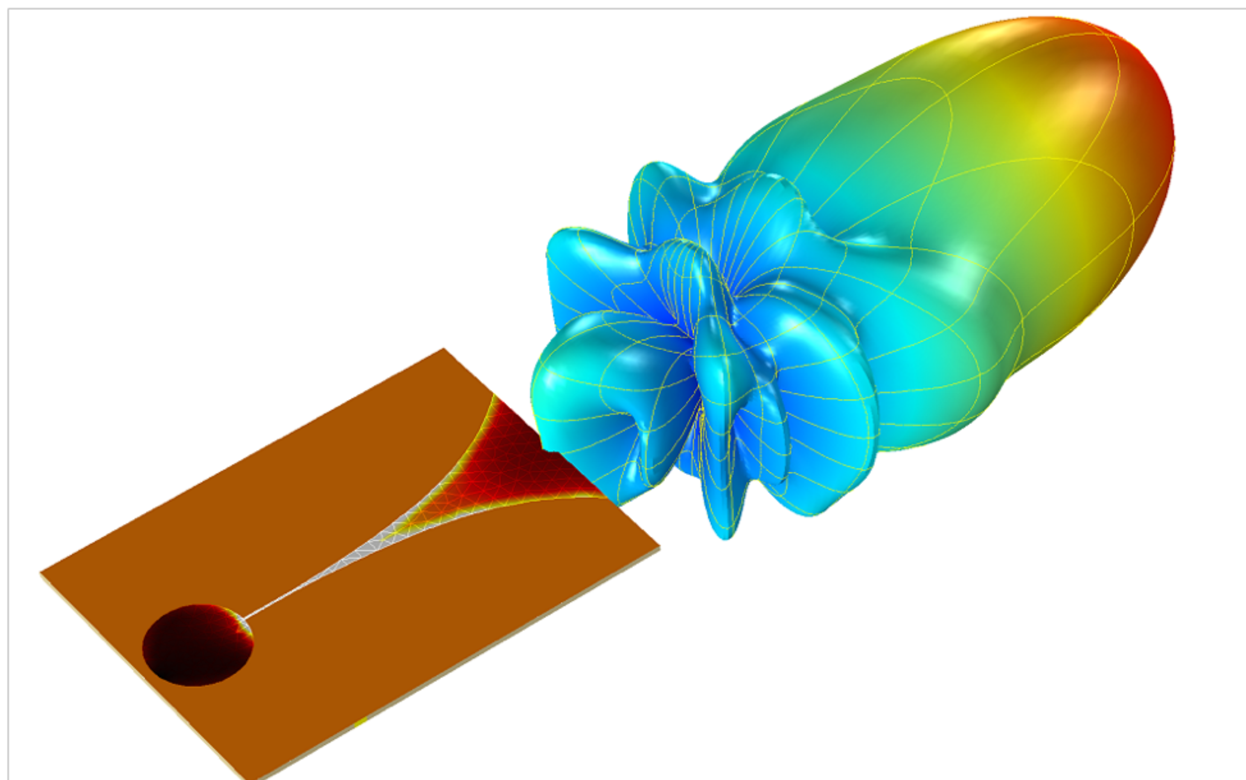
UNDERSTANDING DIRECTIVITY AND GAIN



[Electric Dipole by www.antenna-theory.com]



[Isotropic Radiator by www.dx-antenna.com]



[Vivaldi Antenna Design Analysis by Caty Fairclough]

BLUETOOTH VS. NFC

- radiating Far Field vs. inductive Near Field
- comfort vs. energy feed
- smart devices vs. smart cards

NFC IS NOT

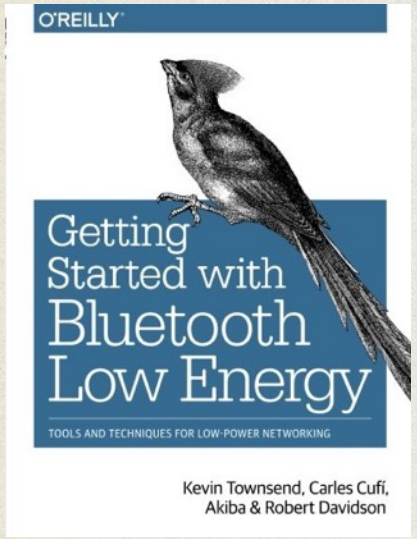
- …magically immune to radio attacks
- Passive sniffing confirmed to dekametres distance
- So, for NFC, a proper cryptographic protection of data being exchanged is also very important
  - in this viewpoint, Bluetooth LE has a better starting position, since the link encryption is a natural part of the standard

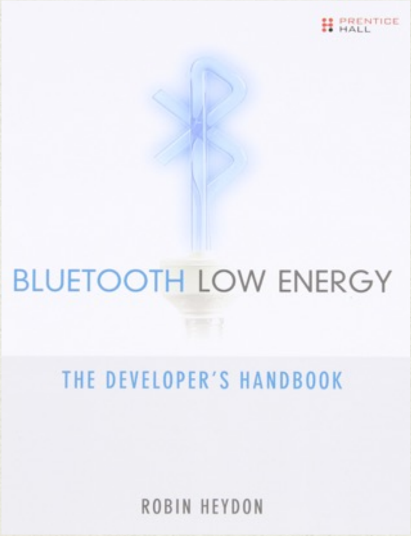
NFC TOGETHER WITH BLE

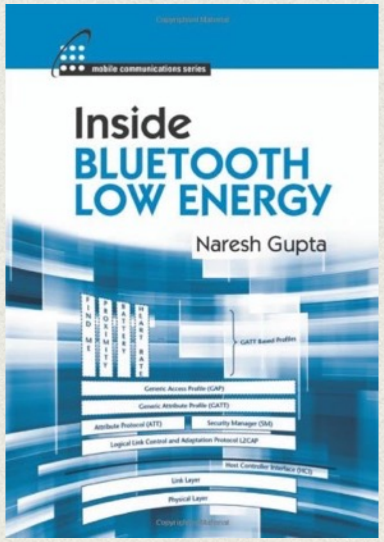
- Rather than competitors, we can assume these technologies will work hand-in-hand together in future applications

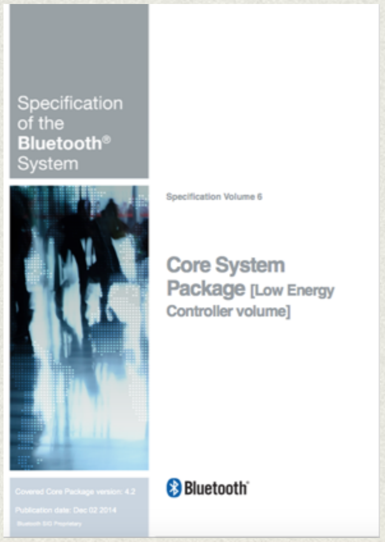
  - NFC-based “tap” can signalise user’s will to communicate while BLE would take care about the rest of data exchange enjoying the comfort of FFC

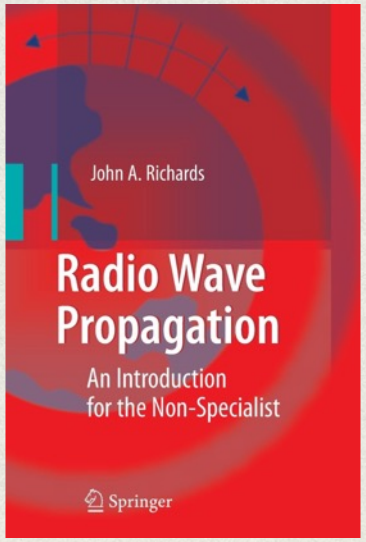
BLE ESSENTIALS

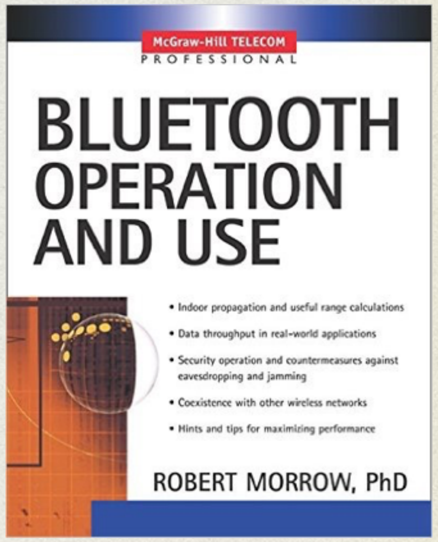












ALL THOSE BLUE TEETH

- Bluetooth **Basic Rate** (1 Mbps)
  - –core spec. 1.x, 1999-2003
- Bluetooth **Enhanced Data Rate** (2 or 3 Mbps)
  - –core spec. 2.x, 2004-2007
  - –taken together, BT BR/EDR is more or less a “serial link over the radio”

Bluetooth Classic

- Bluetooth **High Speed** (54 Mbps with 802.11)
  - –also called AMP ~ *Alternate MAC/PHY*
  - –core spec. 3.x, 2009
- Bluetooth **Low Energy**, a.k.a. Bluetooth Smart (1 Mbps, bulk-mode only)
  - –core spec. 4.x, 2010-2014

Bluetooth Smart

BLE SPECTRUM ALLOCATION

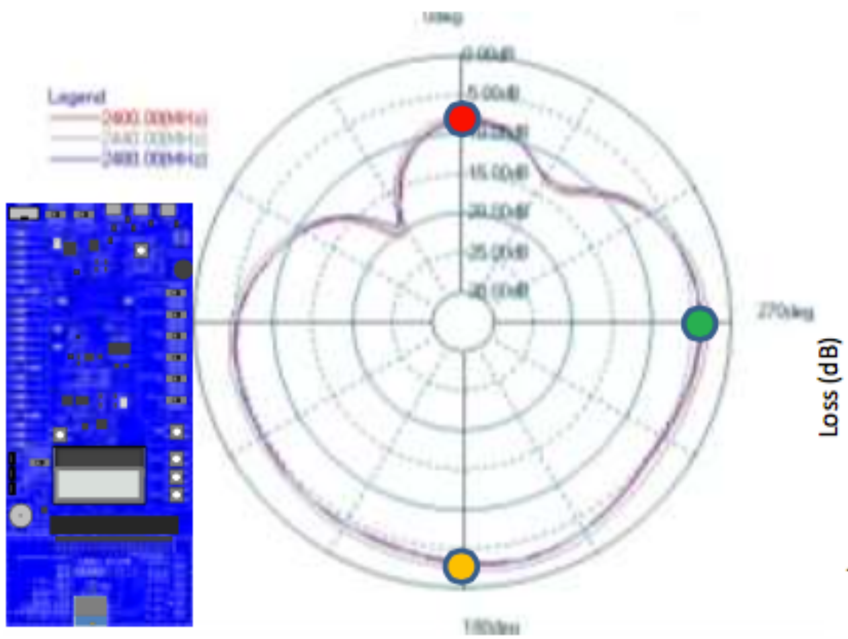
- BLE works in the 2.4 GHz ISM band
- Defines 40 RF channels of 2 MHz bandwidth as:

$$f_k = 2042 + 2k \text{ MHz, where } k = 0..39$$

- channels no. 0, 12, and 39 (RF numbering!) are reserved for the *advertisement* protocol
- GFSK modulation with TX power range -20 dBm to 10 dBm, RX sensitivity ≤ -70 dBm
- radio links defined by: frequency hopping sequence, access address, and connection intervals
- short range communication design with no special adaptive coding and modulation (it's understood…)

BLE RANGE LIMITS

Module	Typical TXP	Sensitivity	Direction	Antenna Attenuation	Link Budget	Calculated Range	Tested Range
BLE121LR	8 dBm	-98 dBm	Front	-3 dB	100 dB	470m	450m
BLE121LR	8 dBm	-98 dBm	Back	-7 dB	92 dB	300m	300m
BLE121LR	8 dBm	-98 dBm	Side	-5 dB	96 dB	370m	340m



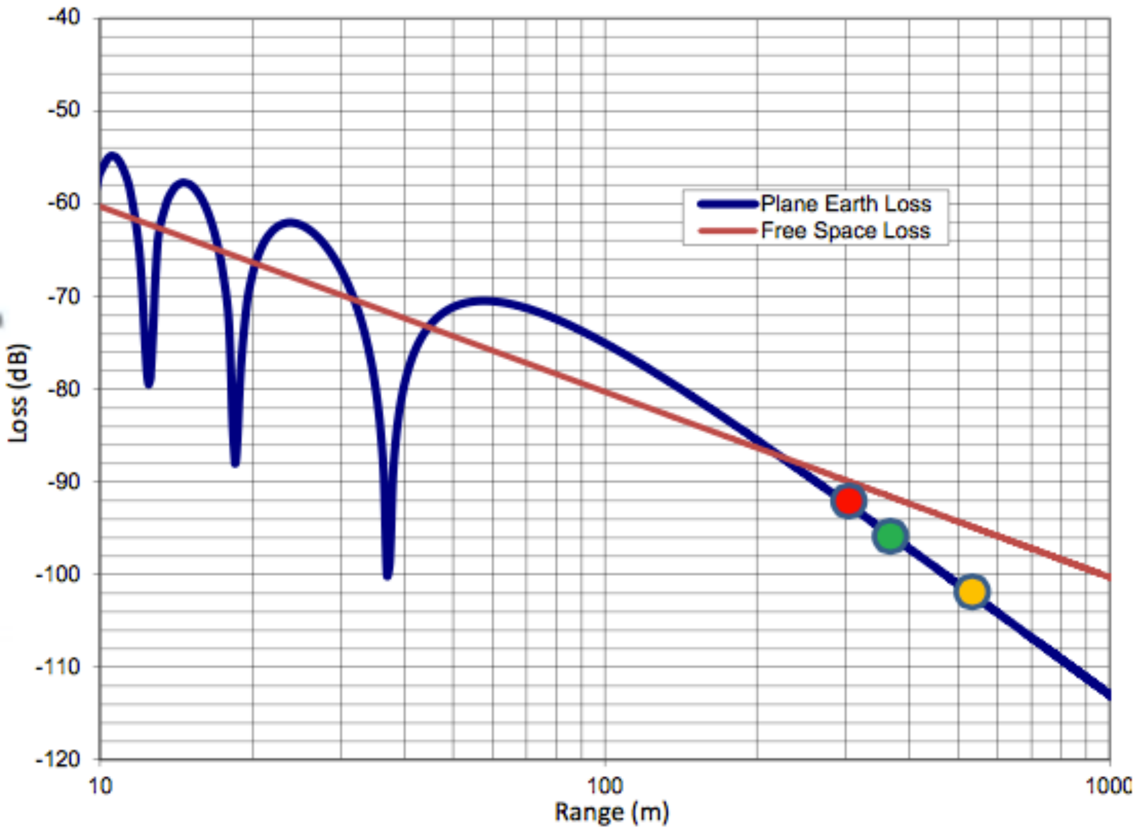


Figure 12: Range of BLE121LR vs BLE121LR when antennas are 1.5m above GND

[BLE112, BLE113, and BLE121LR Range Analysis by Bluegiga Tech.]

GROUND PLANE EFFECTS

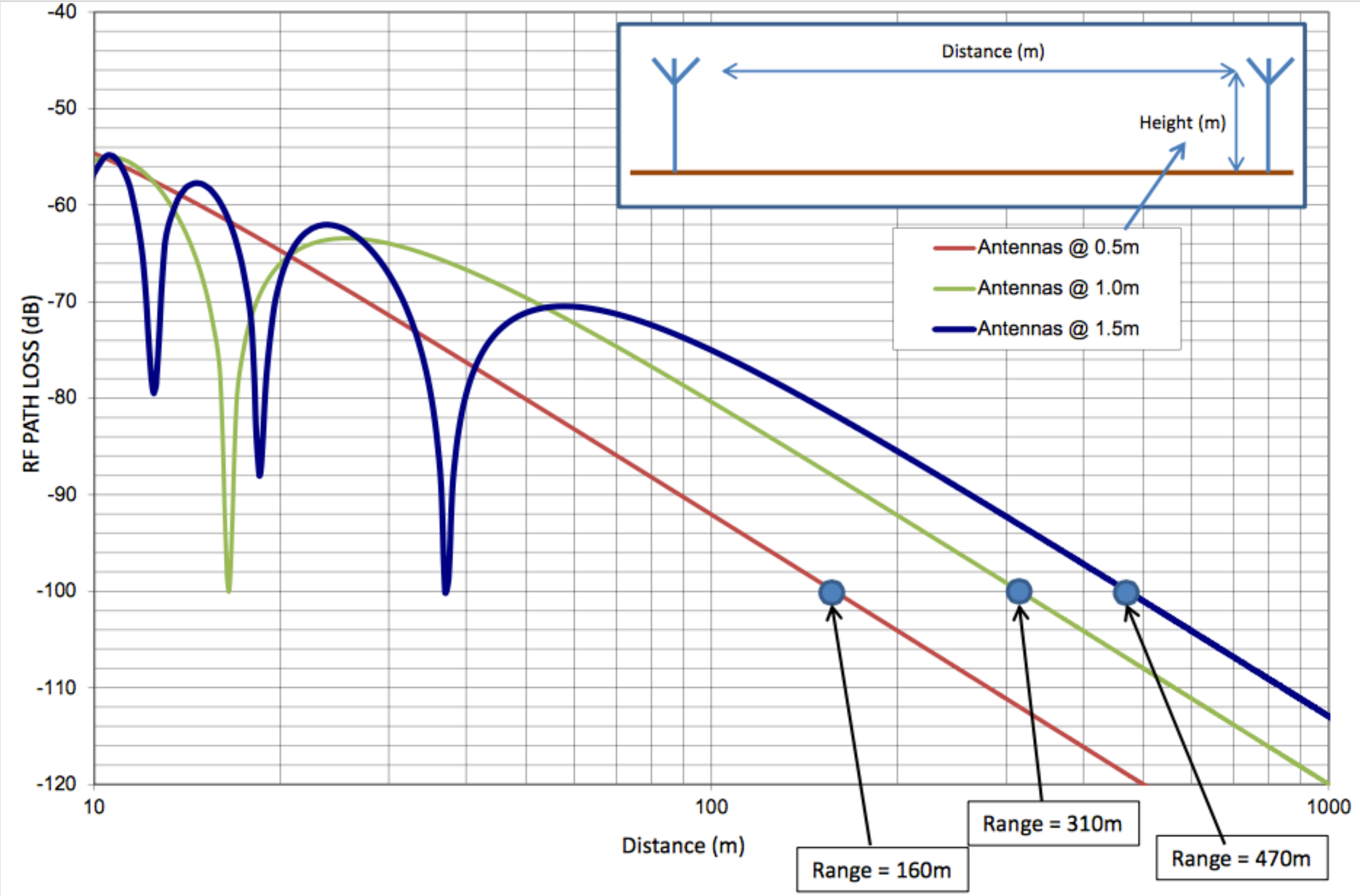


Figure 14: Impact of module height above GND to RF path loss

[BLE112, BLE113, and BLE121LR Range Analysis by Bluegiga Tech.]

FRIIS TRANSMISSION EQ.

- Let dBm denote decibels over 1 mW power and let dBi denote decibels of the antenna power gain over the isotropic source.
  - $[P]_{\text{dBm}} = 10\log(P/10^{-3}) = 10\log P + 30$
  - $[G]_{\text{dBi}} = 10\log(G/1) = 10\log G$
- The available receiver antenna terminal power is then:

$$[P_r]_{dBm} = [P_t]_{dBm} + [G_t]_{dBi} + [G_r]_{dBi} - 20\log\frac{4\pi}{\lambda} - \boxed{10n\log d}$$

n = 2 for the free space loss

RSSI MODEL

- Let RSSI denote the value provided by the Read RSSI Command via BLE HCI.
- Inspired by the Friis transmission eq., we can write:

$$RSSI(d) = RSSI(d_0) - 10n\log\frac{d}{d_0} + X$$

  - d_0 denotes the calibration distance
  - n is a model parametrisation constant (n = 2 in the free space), referred to as the *attenuation factor*
  - X is a random variable covering fluctuations

RSSI MODEL

- Let RSSI denote the value provided by the R… ad RSSI Command via BLE HCI.
- Inspired by the Friis transmissi… write:

$$RSSI(d) = P \ \ldots \ \log\frac{d}{d_0} + X$$

  - d_0 denotes… nce
  - n is … tion constant (n = 2 in the free space), referred to as the … *factor*
  - X is a ra… m variable covering fluctuations

please see Richards, 2008, and Morrow, 2002, for more

BLE LL STATE MACHINE

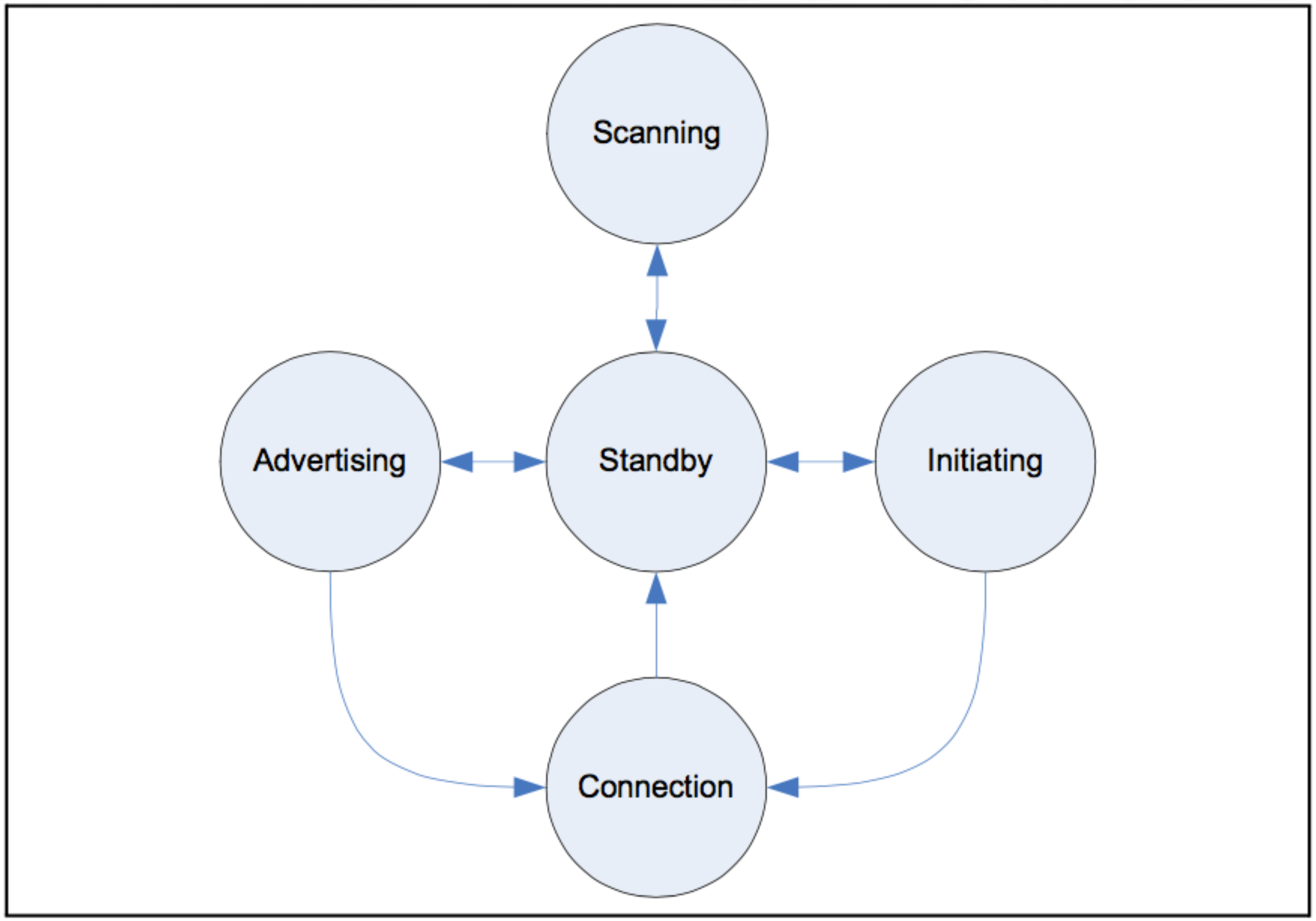


Figure 1.1: State diagram of the Link Layer state machine

[Bluetooth Core Spec. v 4.2, Vol 6, Part B]

RADIO PACKET

LSB MSB

Preamble	Access Address	PDU	CRC
(1 octet)	(4 octets)	(2 to 257 octets)	(3 octets)

Figure 2.1: Link Layer packet format

Maximum Supported Payload Length (bytes)	BER (%)
≤ 37	0.1
≥ 38 and ≤ 63	0.064
≥ 64 and ≤ 127	0.034
≥ 128	0.017

Table 4.1: Actual sensitivity BER by maximum payload length

[Bluetooth Core Spec. v 4.2, Vol 6, Part B]

ADVERTISEMENT

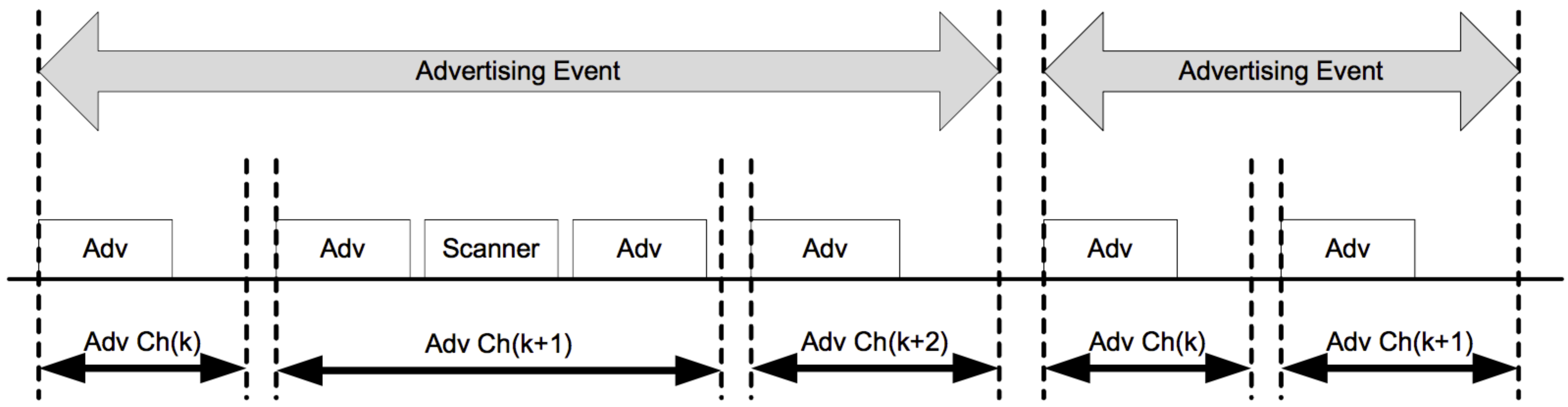
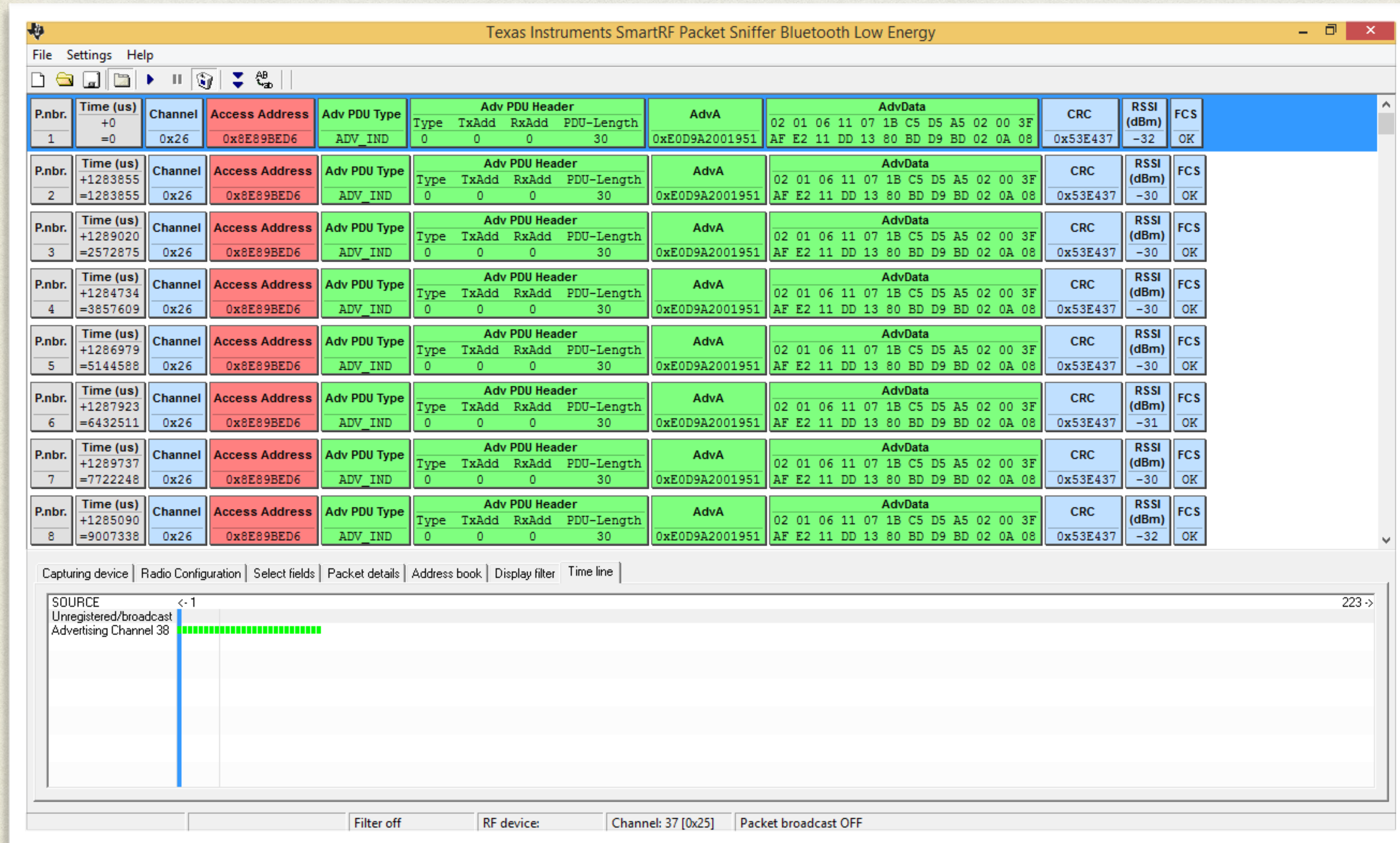


Figure 1.3: Advertising Events

[Bluetooth Core Spec. v 4.2, Vol 1, Part A]



CC-2540-based BLE sniffer

CONNECTION

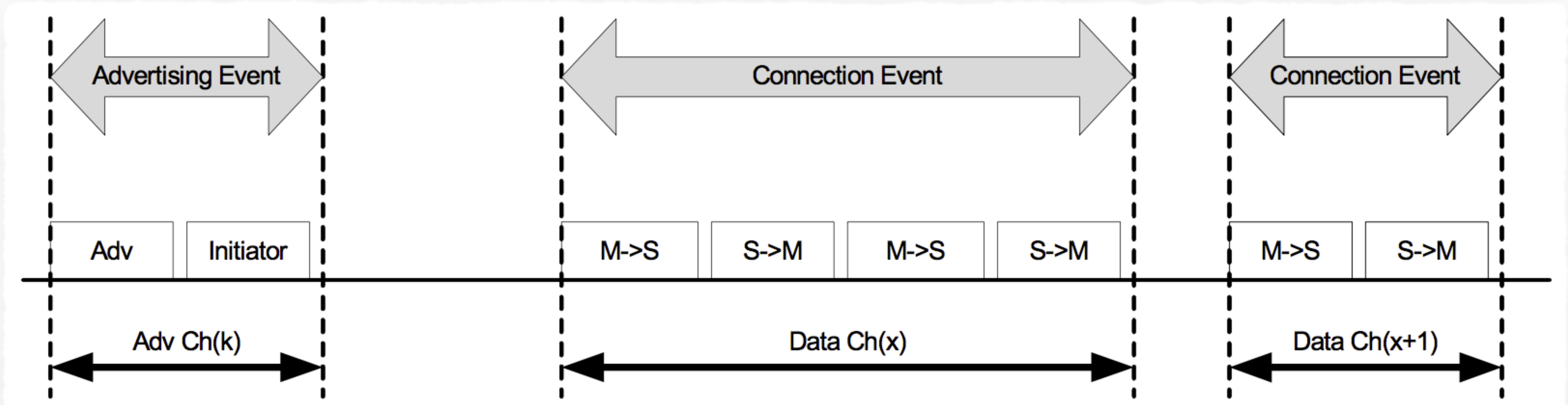
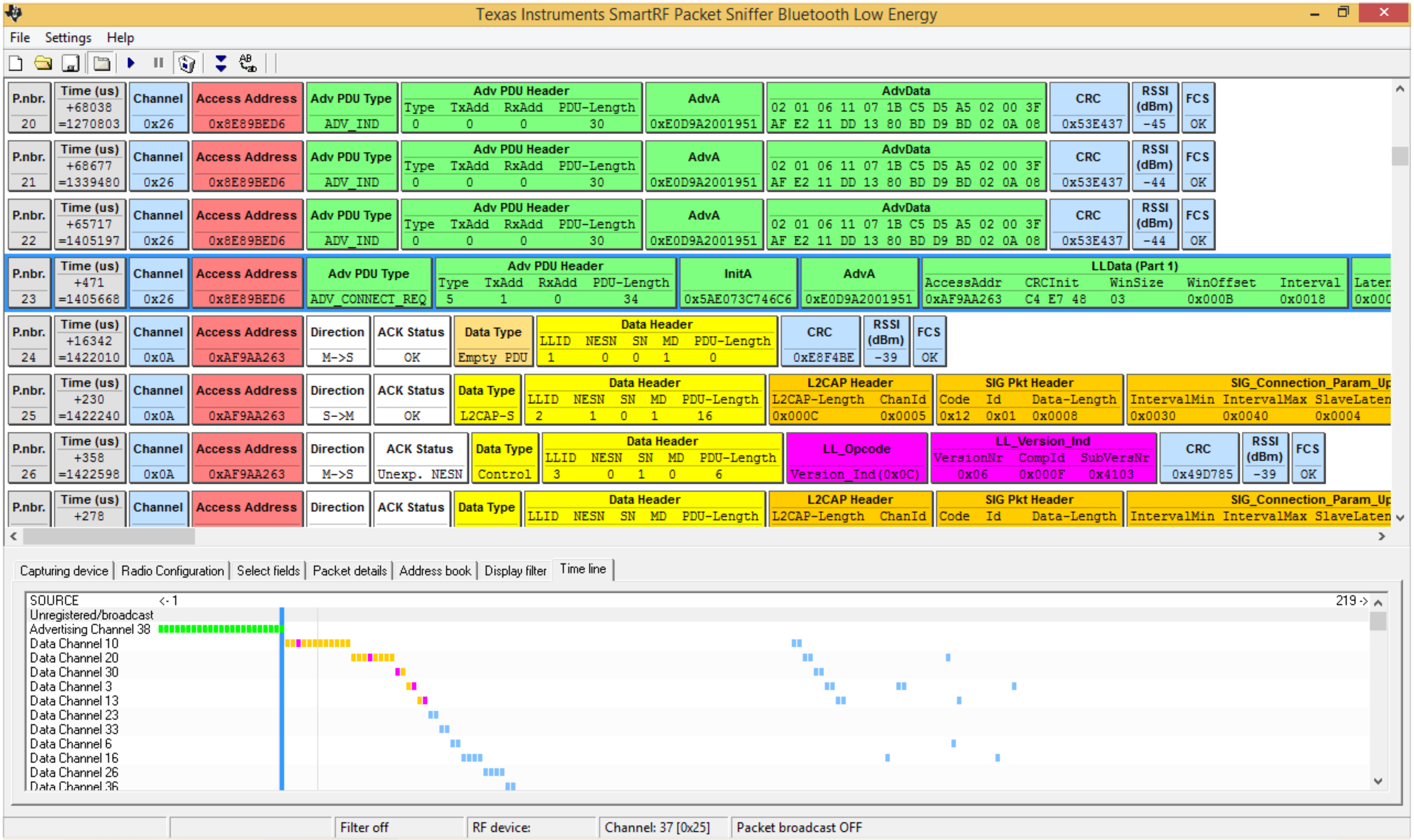


Figure 1.4: Connection Events

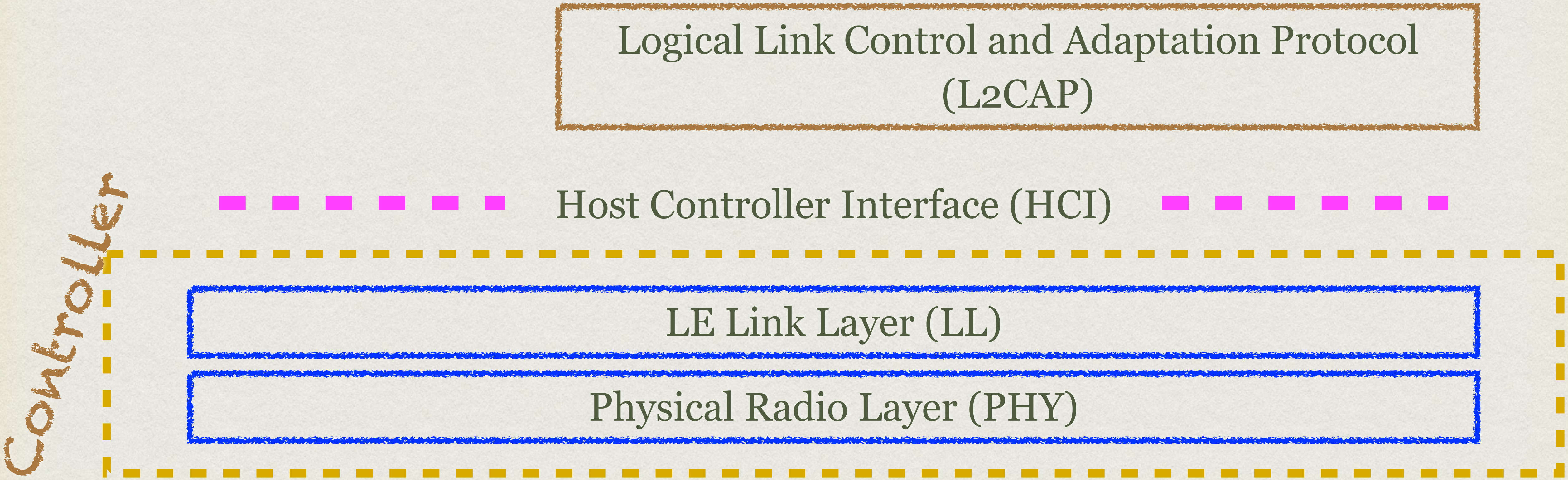
[Bluetooth Core Spec. v 4.2, Vol 1, Part A]

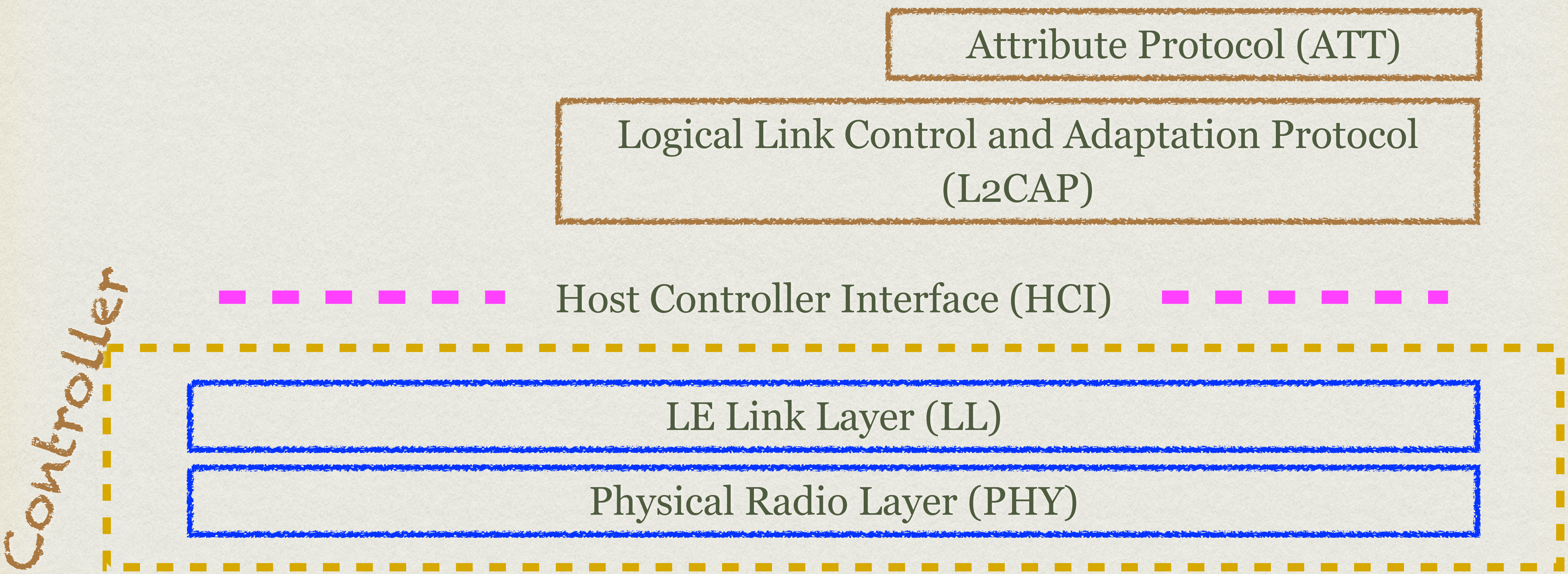


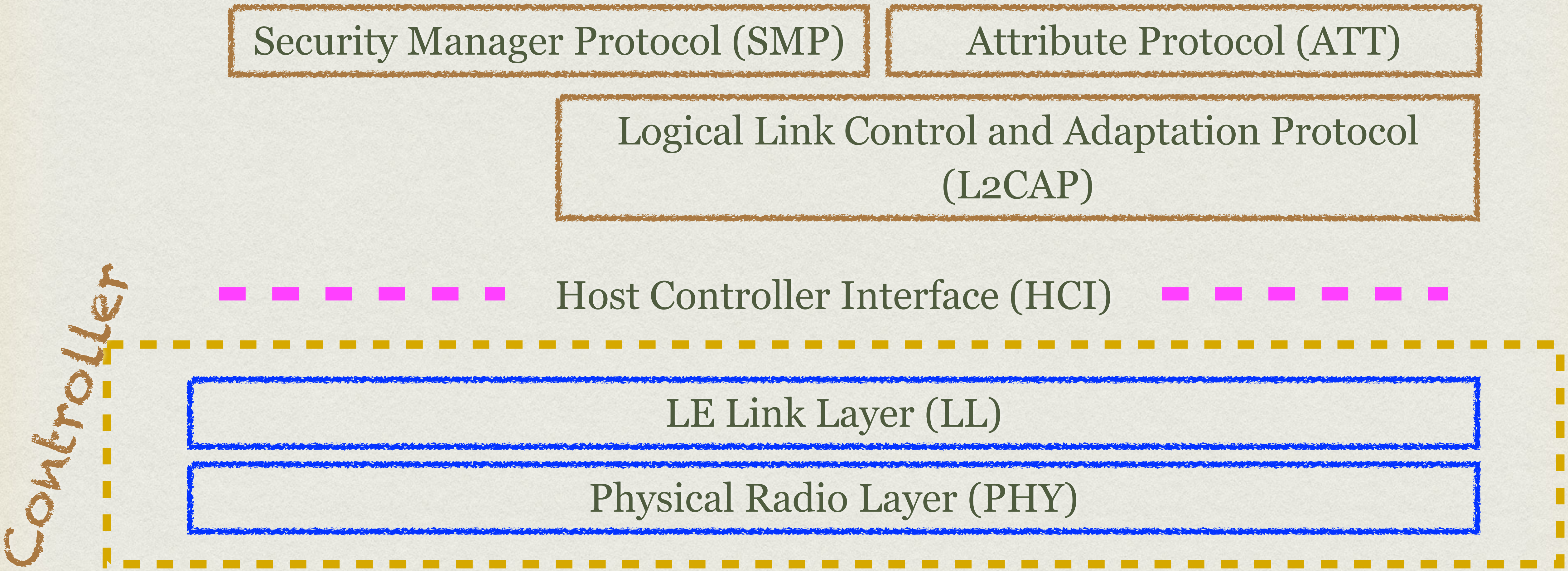
CC-2540-based BLE sniffer

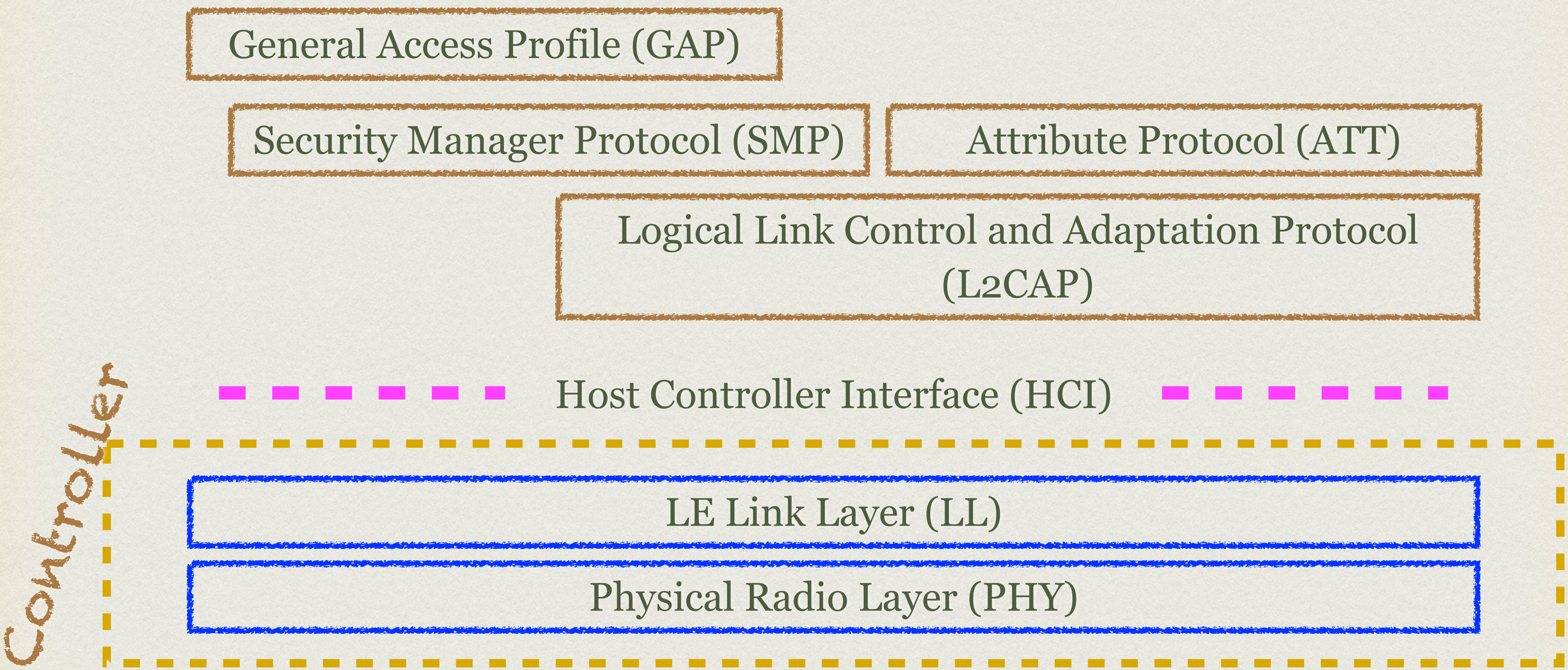
Physical Radio Layer (PHY)

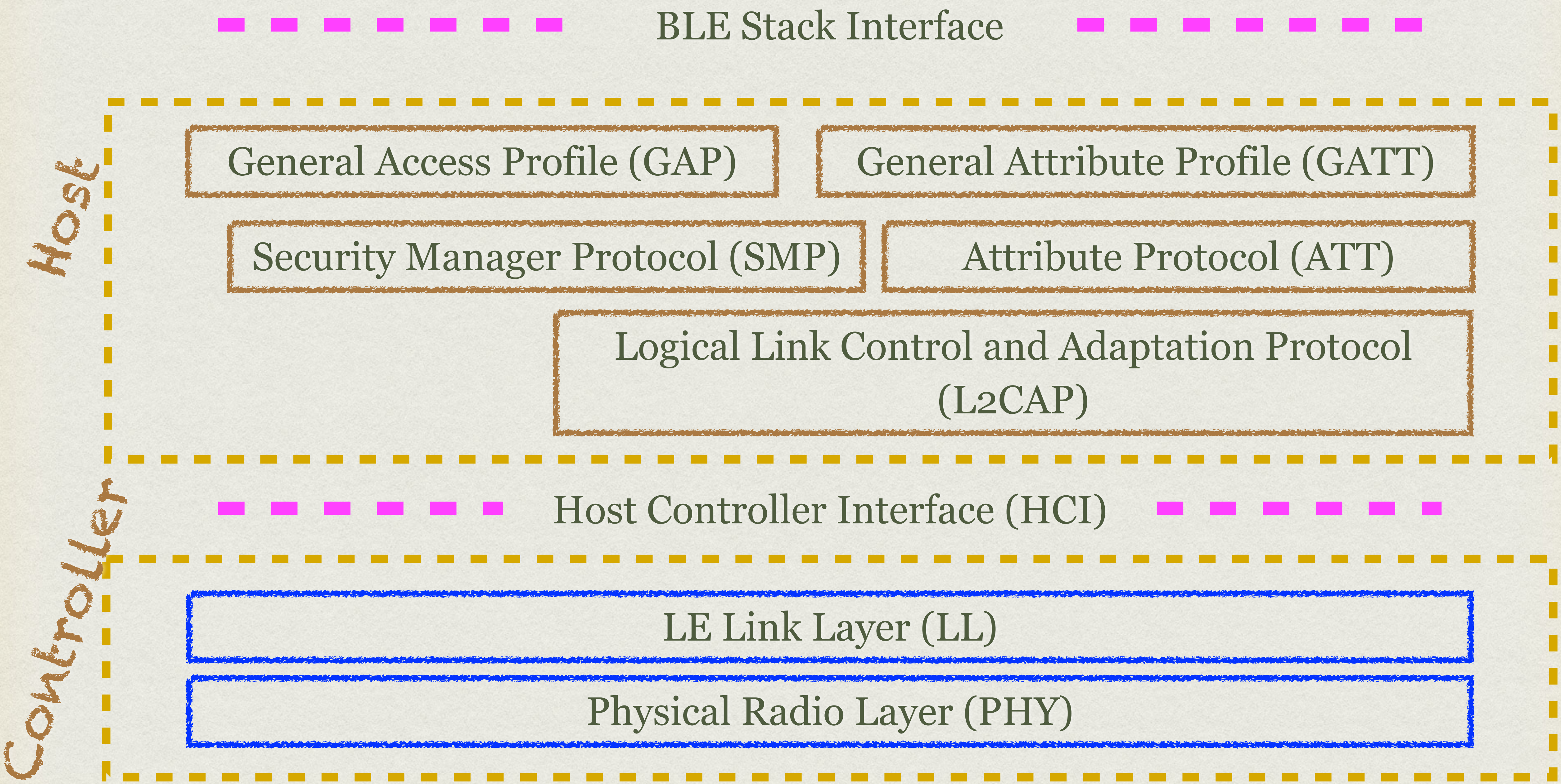

Host Controller Interface (HCI)
Controller
LE Link Layer (LL)
Physical Radio Layer (PHY)

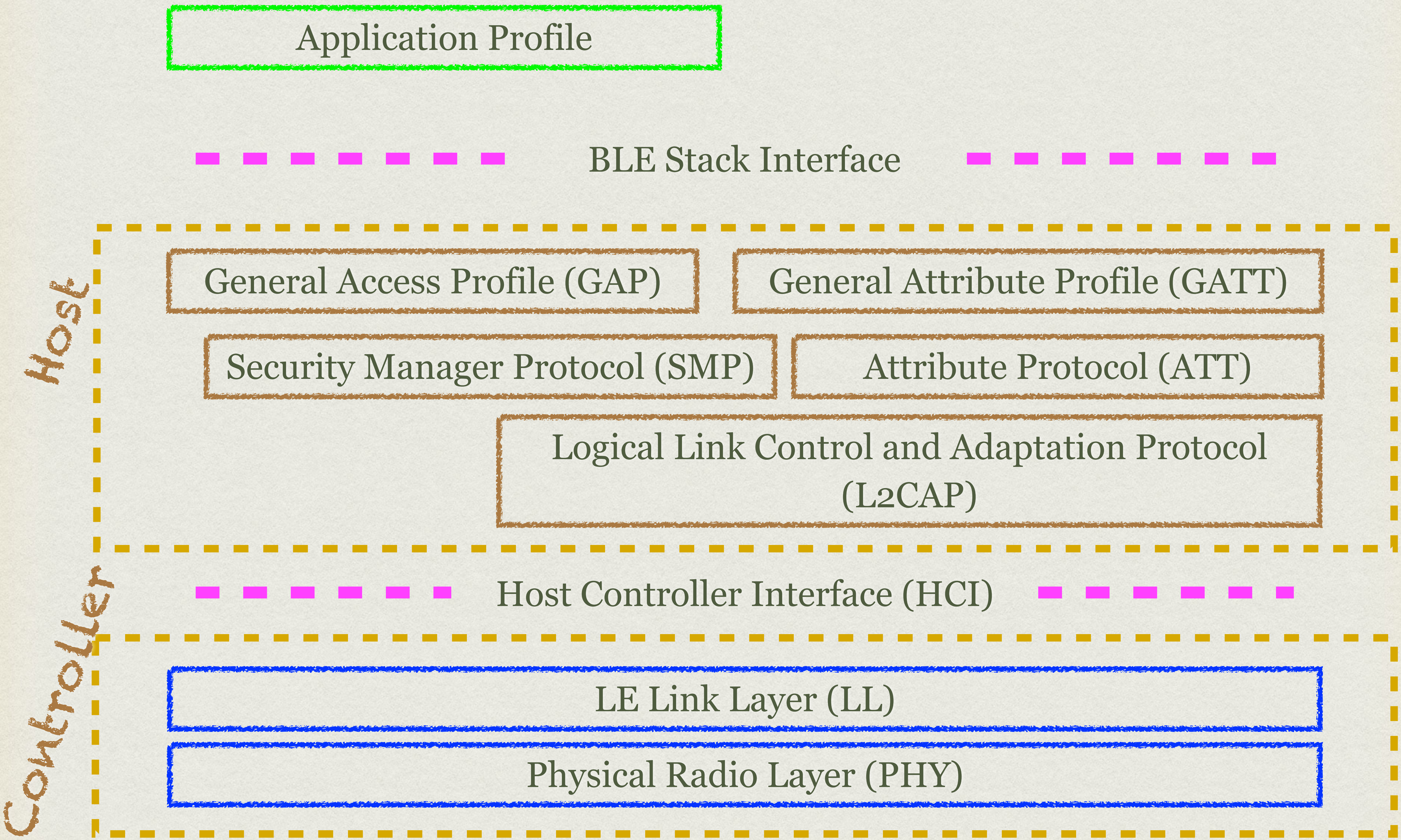

Logical Link Control and Adaptation Protocol (L2CAP)
Host Controller Interface (HCI)
Controller
LE Link Layer (LL)
Physical Radio Layer (PHY)


Attribute Protocol (ATT)
Logical Link Control and Adaptation Protocol (L2CAP)
Host Controller Interface (HCI)
Controller
LE Link Layer (LL)
Physical Radio Layer (PHY)

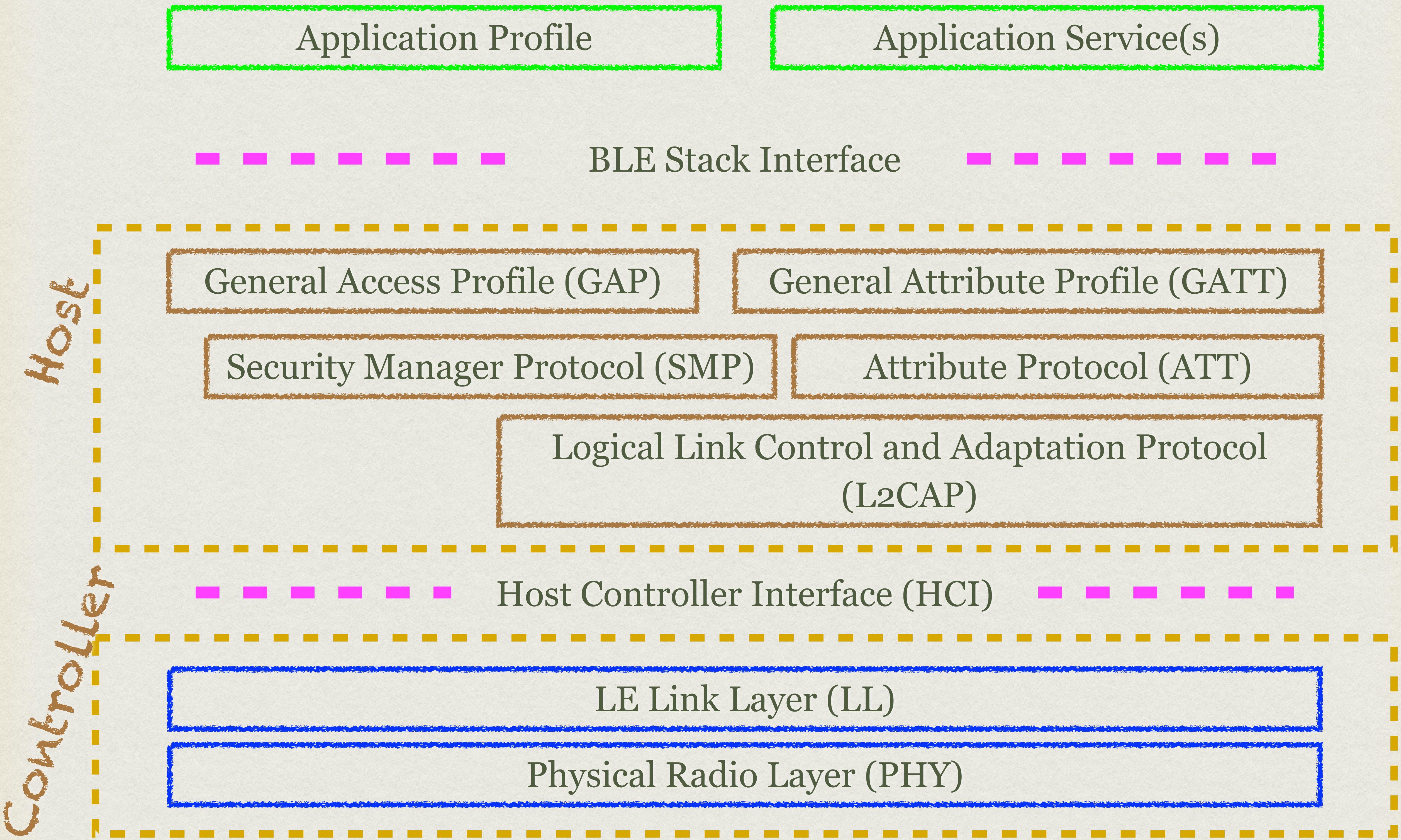

Security Manager Protocol (SMP)
Attribute Protocol (ATT)
Logical Link Control and Adaptation Protocol (L2CAP)
Host Controller Interface (HCI)
Controller
LE Link Layer (LL)
Physical Radio Layer (PHY)

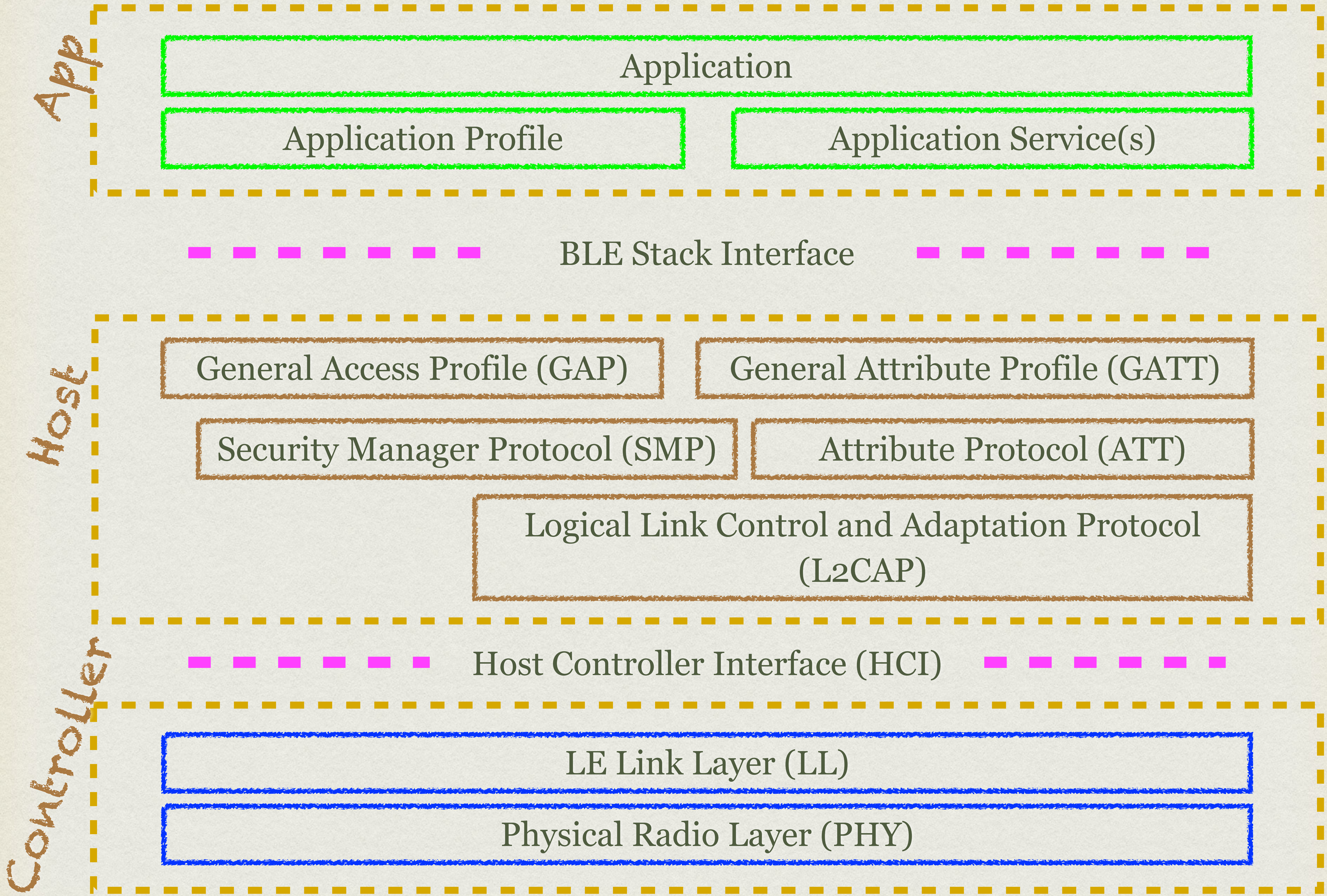

General Access Profile (GAP)
Security Manager Protocol (SMP)
Attribute Protocol (ATT)
Logical Link Control and Adaptation Protocol (L2CAP)
Host Controller Interface (HCI)
Controller
LE Link Layer (LL)
Physical Radio Layer (PHY)


BLE Stack Interface
Host
General Access Profile (GAP)
General Attribute Profile (GATT)
Security Manager Protocol (SMP)
Attribute Protocol (ATT)
Logical Link Control and Adaptation Protocol (L2CAP)
Host Controller Interface (HCI)
Controller
LE Link Layer (LL)
Physical Radio Layer (PHY)

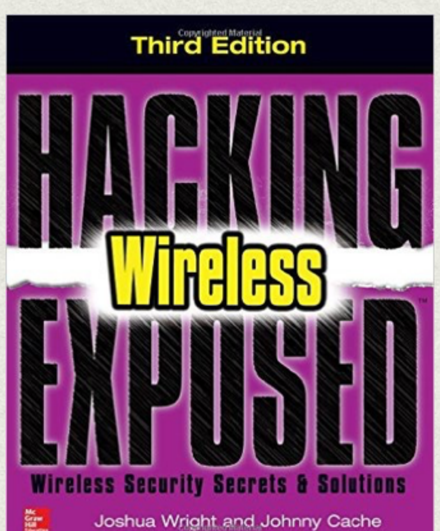


Application Profile
BLE Stack Interface
Host
General Access Profile (GAP)
General Attribute Profile (GATT)
Security Manager Protocol (SMP)
Attribute Protocol (ATT)
Logical Link Control and Adaptation Protocol (L2CAP)
Host Controller Interface (HCI)
Controller
LE Link Layer (LL)
Physical Radio Layer (PHY)

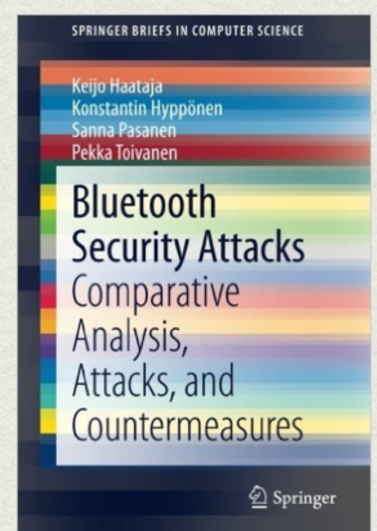

Application Profile
Application Service(s)
BLE Stack Interface
Host
General Access Profile (GAP)
General Attribute Profile (GATT)
Security Manager Protocol (SMP)
Attribute Protocol (ATT)
Logical Link Control and Adaptation Protocol (L2CAP)
Host Controller Interface (HCI)
Controller
LE Link Layer (LL)
Physical Radio Layer (PHY)

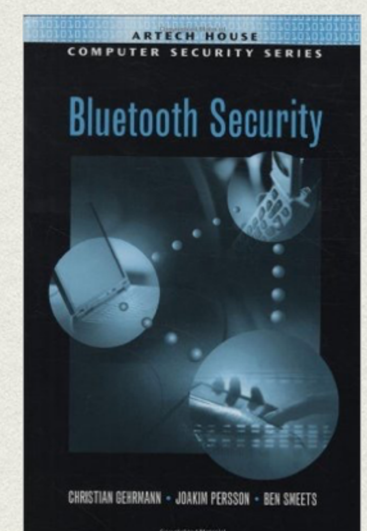

App
Application
Application Profile
Application Service(s)
BLE Stack Interface
Host
General Access Profile (GAP)
General Attribute Profile (GATT)
Security Manager Protocol (SMP)
Attribute Protocol (ATT)
Logical Link Control and Adaptation Protocol (L2CAP)
Host Controller Interface (HCI)
Controller
LE Link Layer (LL)
Physical Radio Layer (PHY)

BLE SECURITY



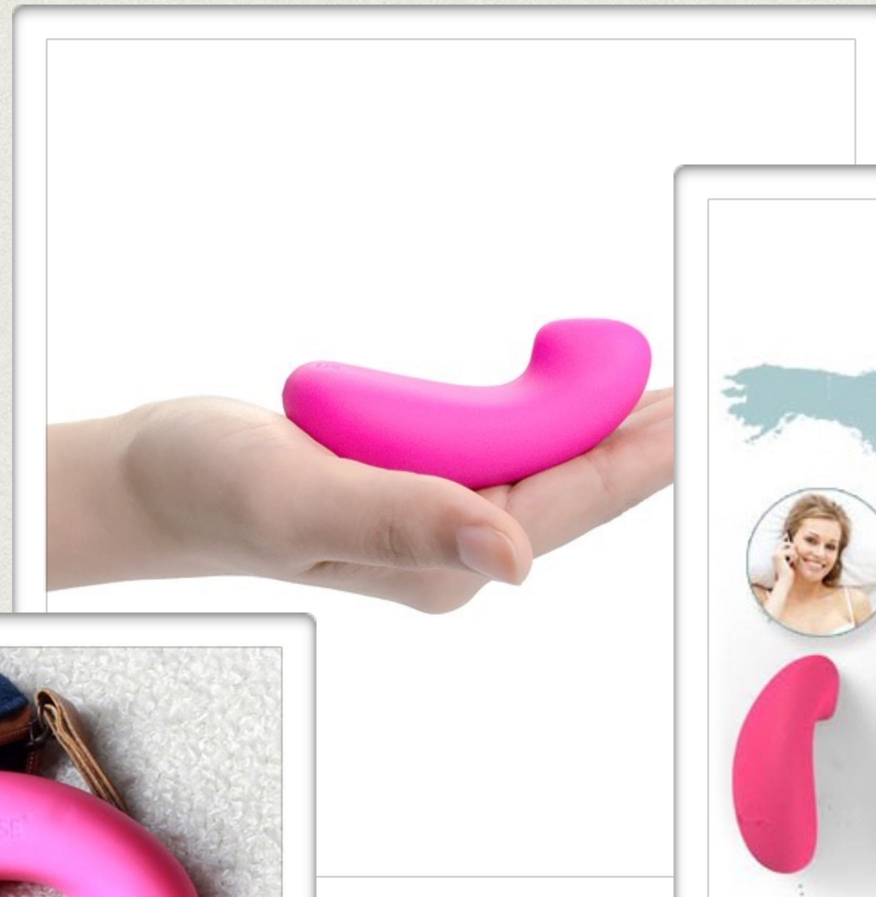
(

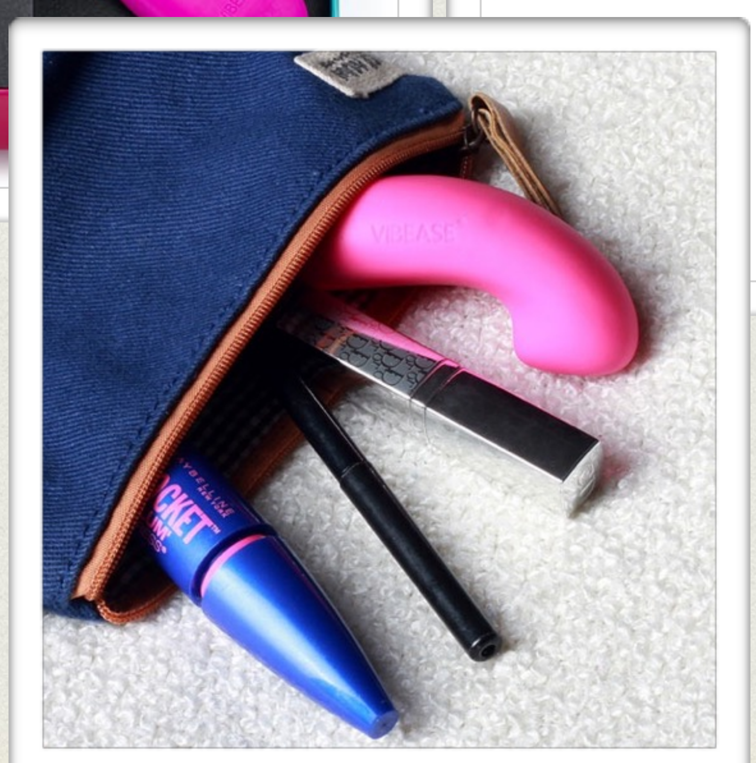


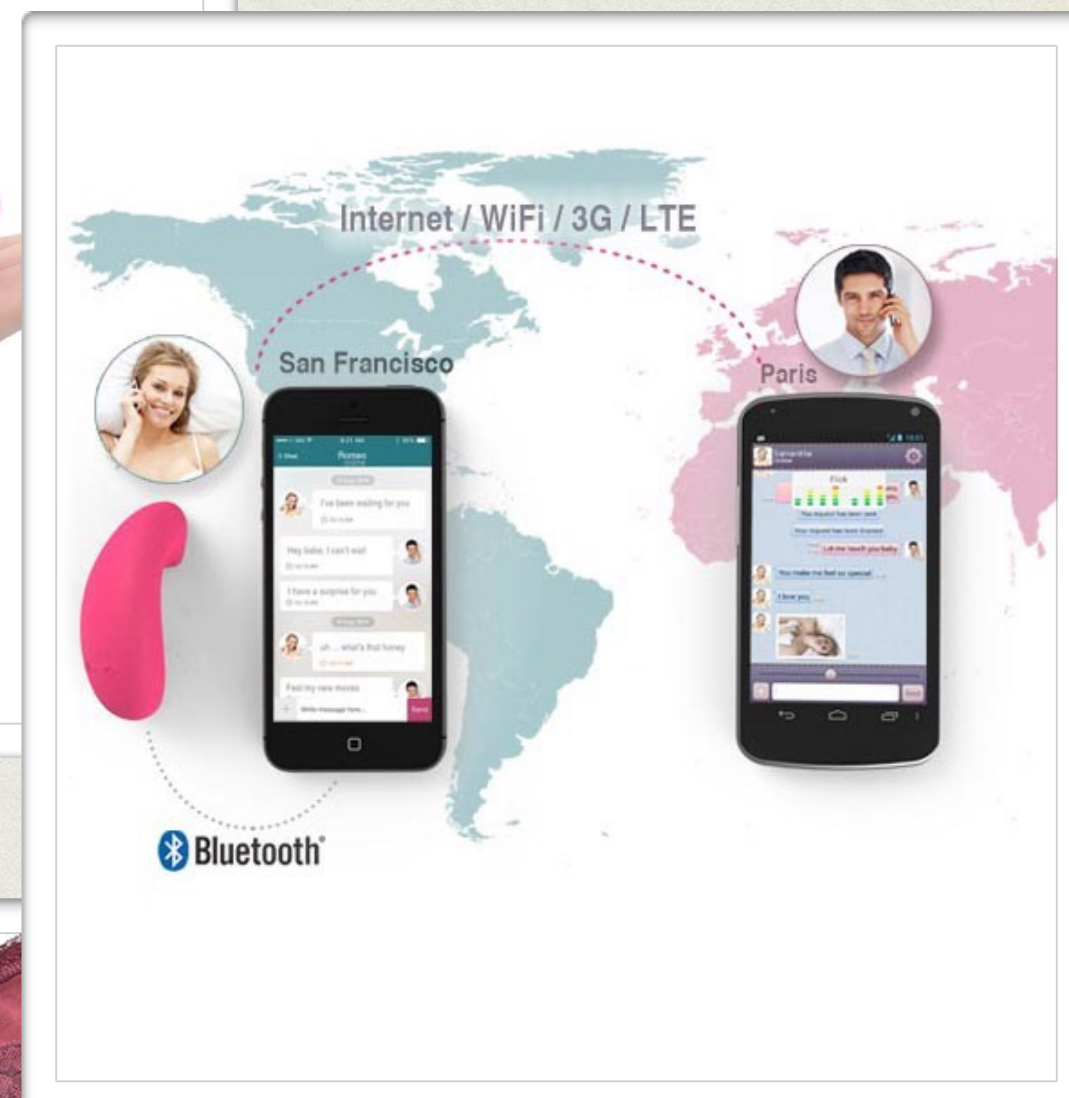


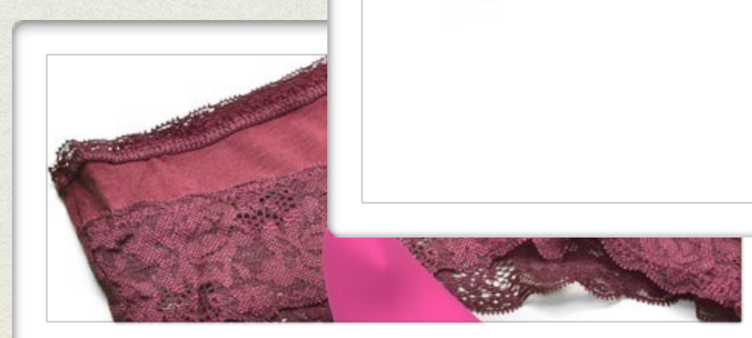
)

BLE GETTING PERSONAL









BLE GETTING PERSONAL

BLE SECURITY GOALS - WHAT WAS PLANNED

- *Privacy* - attacker cannot track user IDs
- *Confidentiality* - attacker cannot understand the data being exchanged
- *Authentication* - attacker cannot impersonate a peer device or spoof its data response

BLE SECURITY GOALS - WHAT WAS PLANNED

AES-based address resolver

- *Privacy* - attacker cannot track user IDs
- *Confidentiality* - attacker cannot understand the data being exchanged
- *Authentication* - attacker cannot impersonate a peer device or spoof its data response

BLE SECURITY GOALS - WHAT WAS PLANNED

- *Privacy* - attacker cannot track user IDs
- *Confidentiality* - attacker cannot understand the data being exchanged
- *Authentication* - attacker cannot impersonate a peer device or spoof its data response

AES-based address resolver

AES-CCM

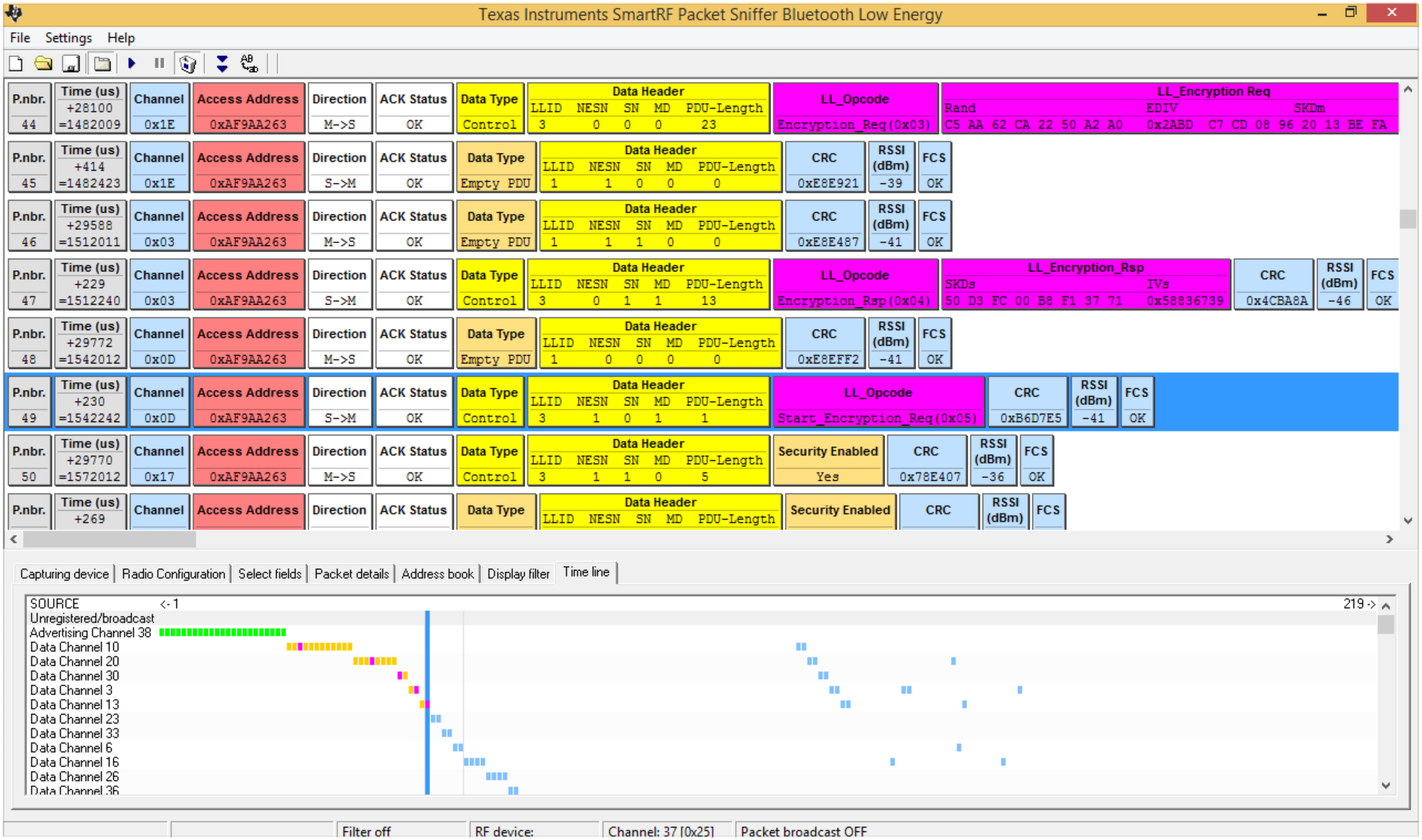
BLE SECURITY GOALS - WHAT WAS PLANNED

- *Privacy* - attacker cannot track user IDs
- *Confidentiality* - attacker cannot understand the data being exchanged
- *Authentication* - attacker cannot impersonate a peer device or spoof its data response

AES-based address resolver

AES-CCM

AES-based bit commitment together with ECDHE



CC-2540-based BLE sniffer

BLE SECURITY GOALS - WHAT IS ACHIEVED

- Private address generation and data link encryption cryptographic schemes are quite robust and sufficient
- They do, however, both rely on the authentication and key agreement step - i.e. so called *pairing*

–unfortunately, this procedure is still flawed, even after the introduction of the *Secure Connections* protocol in BT Core Spec. v 4.2

BLE LEGACY PAIRING

- Vulnerable to passive eavesdropping
  - basically the same problem as with BT BR/EDR PIN-based link key generation
- Vulnerable to active impersonation
  - works even for a one-time PIN
- Vulnerable to MITM
  - different cryptographic flaw, but at the end, it is again a similar situation to that of the PIN-based link key generation in BT BR/EDR

BLE LEGACY PAIRING

- Vulnerable to passive eavesdropping
  - –basically the same problem as with BT BR/ED ... k key generation
- Vulnerable to active impersona...
  - –works even for a o...
- Vulnerabl...
  - –differe... graphic flaw, but at the end, it is again a similar situation ... that of the PIN-based link key generation in BT BR/EDR

excellent for pairing in a well shielded secret chamber

BLE SECURE CONNECTIONS

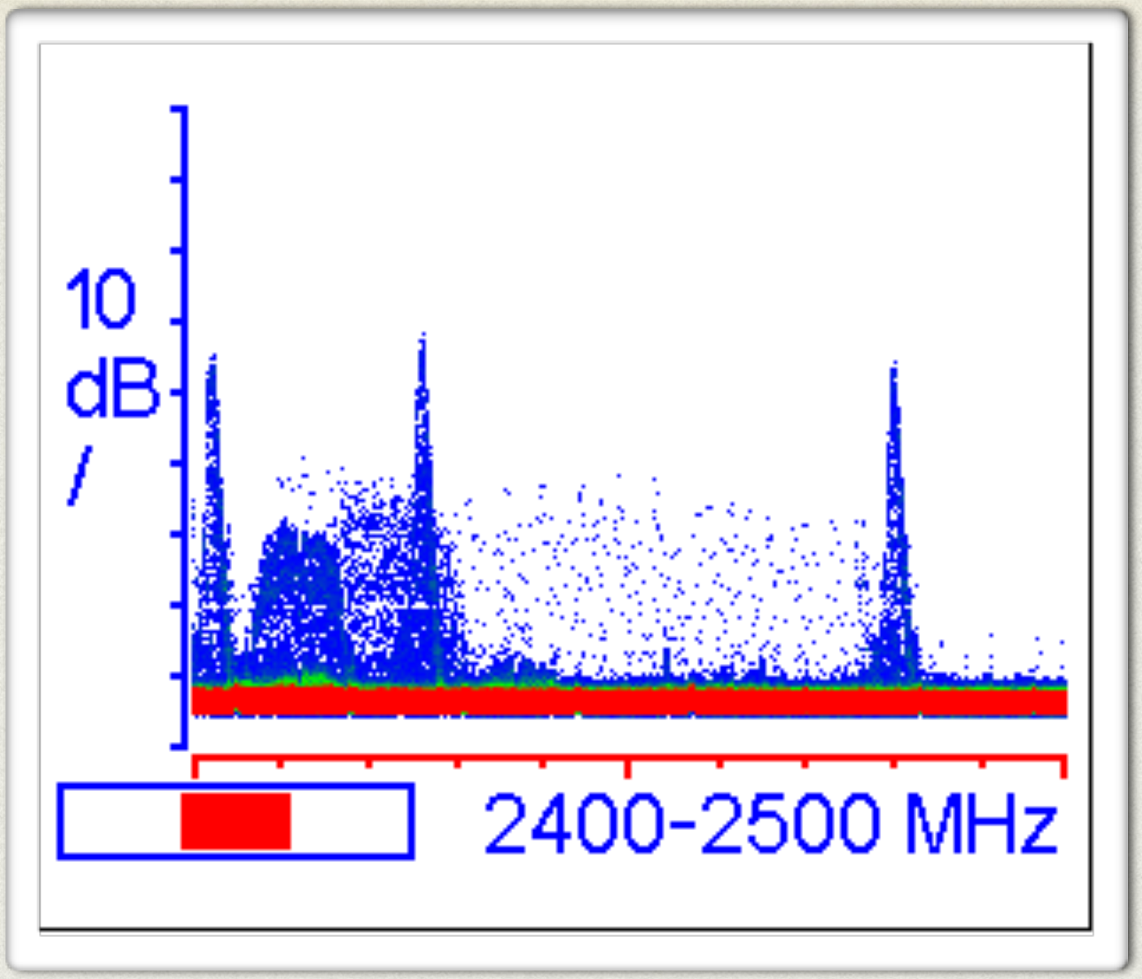
- Designed as an enhancement of the *Legacy Pairing*
  - in the very same way as *Secure Simple Pairing* for BT BR/EDR replaced the insufficient PIN-based link key generation and authentication
- Cryptographically speaking, it fails to protect namely:
  - against the passive eavesdropping of the authentication PIN
  - against the active MITM based on device capabilities spoofing

  (in the very same way as *Secure Simple Pairing* does NOT do for BT BR/EDR…)
- Anyway, we can still revert to the *Out Of Band* mode of *Legacy Pairing* to provide our own authenticated key agreement protocol
  - similarly, we can (shall) explicitly insist on the device capabilities that were reported/used

BLE SECURE PING PROCEDURE

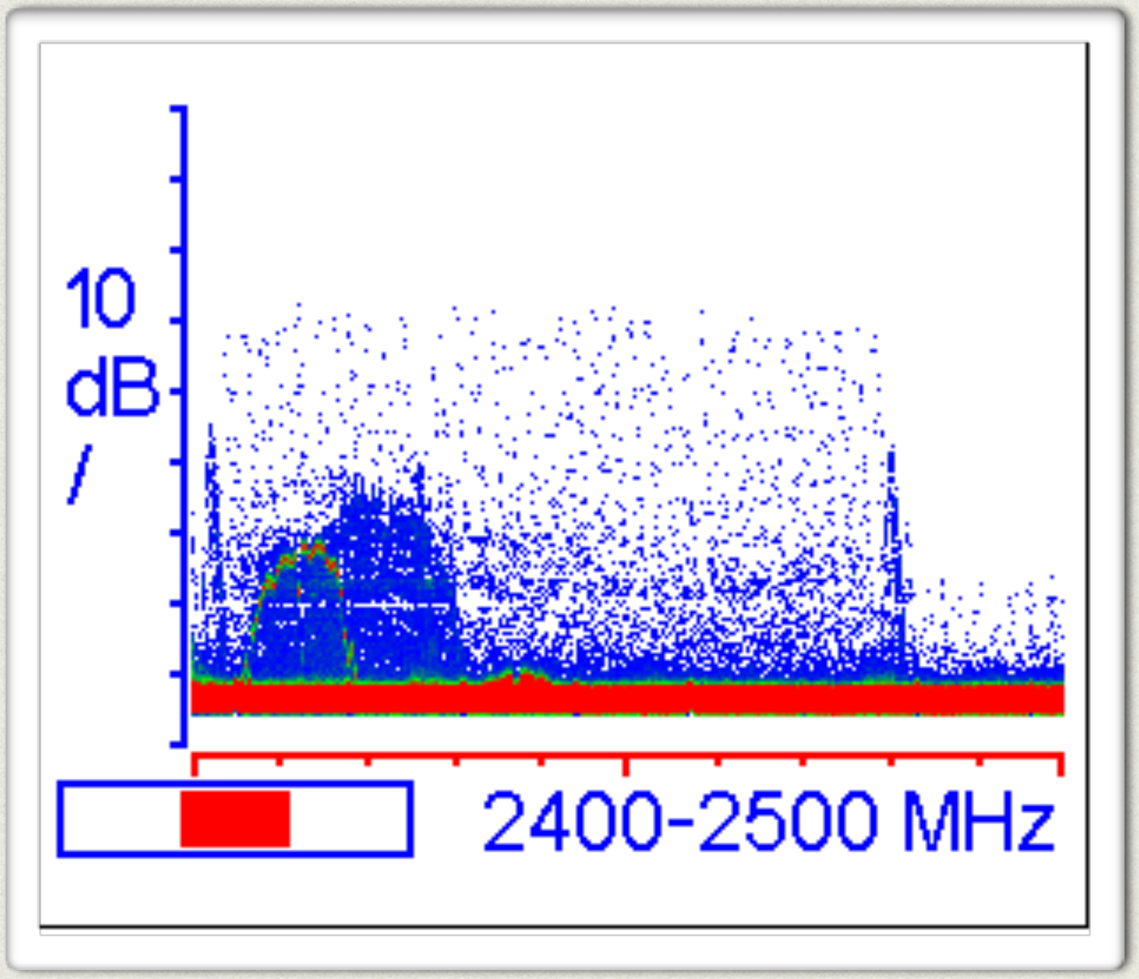
- Offers a standard, reliable check of whether a particular device is still in the radio range of the peer device (e.g. of a mobile phone or a computer)
- Based on ACL packet with cryptographically protected integrity
  - works together with LE Authenticated Payload Timeout
- Assumes proper checking of *packetCounter* in CCM *nonce*

RF SPECTRUM WRAP-UP



advertising

connection



[Indicative wide-band RF scans by RigExpert IT-24 analyser for 2.4 GHz]

CONCLUSIONS

- Bluetooth Low Energy is a new, completely redesigned radio interface in the Bluetooth family
  - for instance, the connection establishment can be a breeze, now, thanks to the *advertisement* procedure
- Excellent choice for a telemetry, in particular with mobile applications
  - assumes ad hoc “tweets” rather than intensive persistent communication
  - audio-video applications shall rather stay with BT BR/EDR
- Ideal interface for small size, personal security modules
- Can work for years with a standard button-cell battery

CAVEATS

- We shall be aware of known weaknesses, especially in the pairing procedure
  - we shall possibly devise an extra protection based on our risk analysis outputs
- Furthermore, the BLE services deserve a penetration test that would also focus on the host OS and application integrity
  - fuzz-testing would be highly welcome here to prevent a malware take-over


REALLY, DO THE PENTEST!

REFERENCES
(BESIDES THE BOOKS NOTED ABOVE)

1. Bluegiga Technologies: BLE112, BLE113 and BLE121LR Range Analysis, Application Note, version 1.1, May 15th, 2014
2. Bluetooth SIG: Bluetooth Core Specification, version 4.2, 2014
3. Bluetooth SIG: Bluetooth Core Specification Supplement (CSS), version 6, 2015
4. Brown, T.-C.-W., Diakos, T., and Briffa, J.-A.: *Evaluating the Eavesdropping Range of Varying Magnetic Field Strengths in NFC Standards*, 2013
5. CC2540: 2.4-GHz Bluetooth low energy System-on-Chip, Product Datasheet, SWRS084F, Texas Instruments, 2010-2013
6. Diakos, T.-P., Briffa, J.-A., Brown, T.-W.-C., and Wesemeyer, S.: *Eavesdropping near-field contactless payments: a quantitative analysis*, 2013
7. Engelhardt, M., Pfeiffer, F., Finkenzeller, K., and Biebl, E.: *Extending ISO/IEC 14443 Type A Eavesdropping Range using Higher Harmonics*, 2013
8. Hata, M.: *Empirical Formulae for Propagation Loss in Land Mobile Radio Service*, IEEE Trans. on Vehicular Technology, Vol. 29, No. 3, pp. 317-325, August 1980
9. Lindell, A.-Y.: *Attacks on the Pairing Protocol of Bluetooth v2.1*, Black Hat USA 2008, June 2008
10. Rosa, T.: *Bypassing Passkey Authentication in Bluetooth Low Energy*, Cryptology ePrint Archive: Report 2013/309, http://eprint.iacr.com, 2013 [link checked Oct-5-2015]
11. Ryan, M.: *Bluetooth: With Low Energy comes Low Security*, 7th USENIX Workshop on Offensive Technologies (WOOT '13), 2013
12. Smart RF Packet Sniffer, User Manual, SWRU187F, Texas Instruments, 2008-2011
13. Zhu, J.-Y., Chen, Z., Luo, H.-Y., and Li, Z.: *RSSI Based Bluetooth Low Energy Indoor Positioning*, In Proc. of International Conference on Indoor Positioning and Indoor Navigation, October 2014