Welcome to Bluetooth Smart

TROOPERS12

Michael Ossmann
Great Scott Gadgets

2471-3855-7631-8386-3686

Bluetooth®

SMART

formerly

Bluetooth Low Energy

a
history
of
confusion

1999

Bluetooth 1.0

Basic Rate

Basic Rate (BR)

1 Mbit/s

GFSK

FHSS

2.4 GHz

2001

Bluetooth 1.1

interoperability

2003

Bluetooth 1.2

backward
compatible

2004

Bluetooth 2.0 + EDR

Enhanced
Data
Rate

Enhanced Data Rate (EDR)

2 Mbit/s 3 Mbit/s

packets start BR

connections start BR

BR

BR

\

EDR

pairing vulnerability

2004 Ollie Whitehouse

2005 Shaked & Wool

2007

Bluetooth 2.1 +EDR

Secure Simple Pairing

Secure Simple Pairing

attempts to correct Pairing weakness

Diffie-Hellman key exchange

Various MITM protection methods

SSP methods

Out of Band

Passkey Entry

Numeric Comparison

Just Works

2009

Bluetooth 3.0 + HS

High Speed

High Speed (HS)

Alternative MAC/PHY (AMP)

uses 802.11

connections start

BR

BR

\

EDR

BR

HS

EDR

802.11

BR

HS

EDR

2010

Bluetooth 4.0

Low Energy

BR vs. LE

BR

1 Mbit/s
GFSK

vs.

LE

1 Mbit/s
GFSK

BR

1 Mbit/s
GFSK

FHSS

vs.

LE

1 Mbit/s
GFSK

FHSS

BR

1 Mbit/s

GFSK

vs.

LE

1 Mbit/s

GFSK

FHSS

2.4 GHz

FHSS

2.4 GHz

why Low Energy?

802.11

BR

HS

EDR

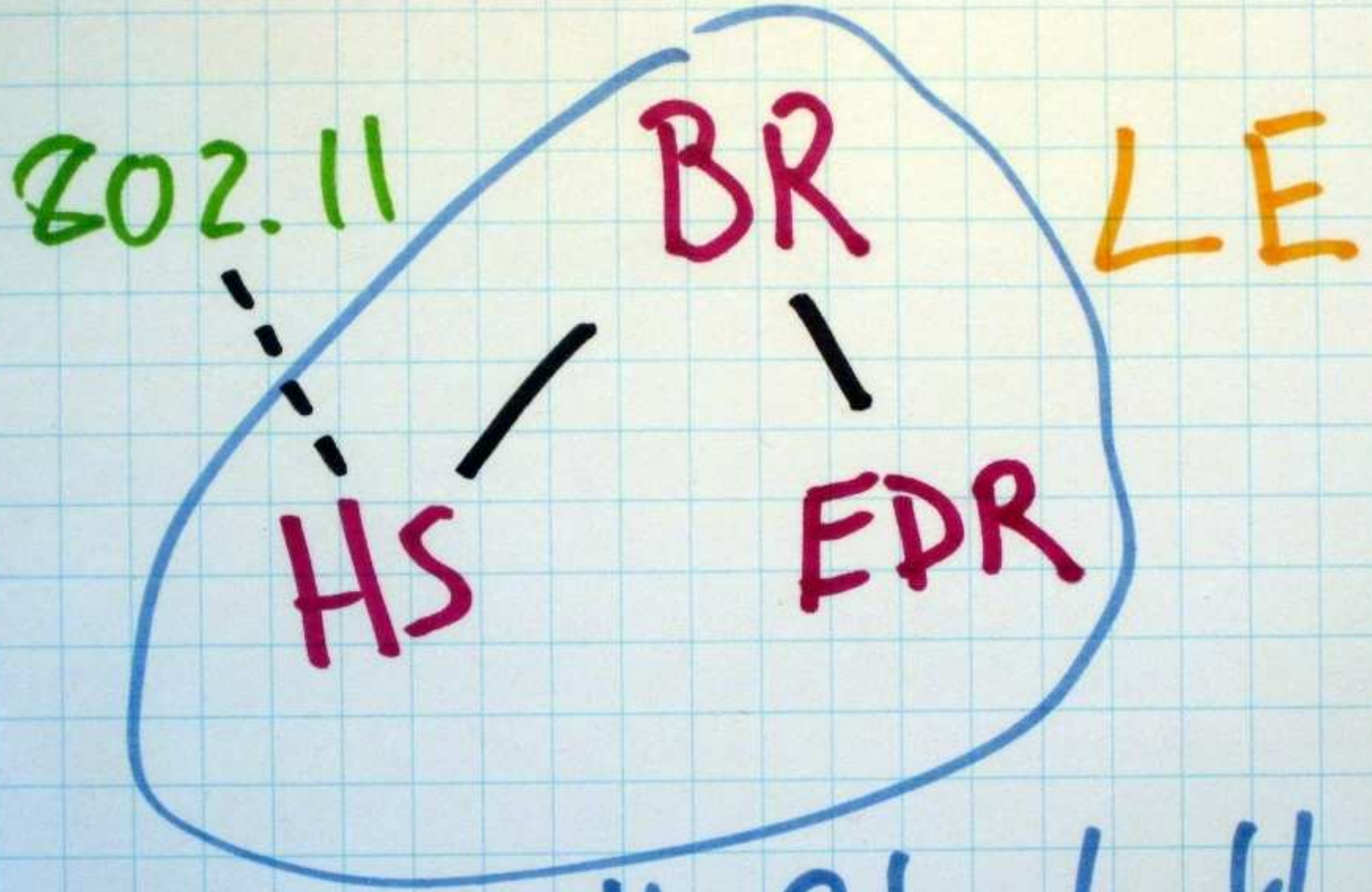
802.11

BR

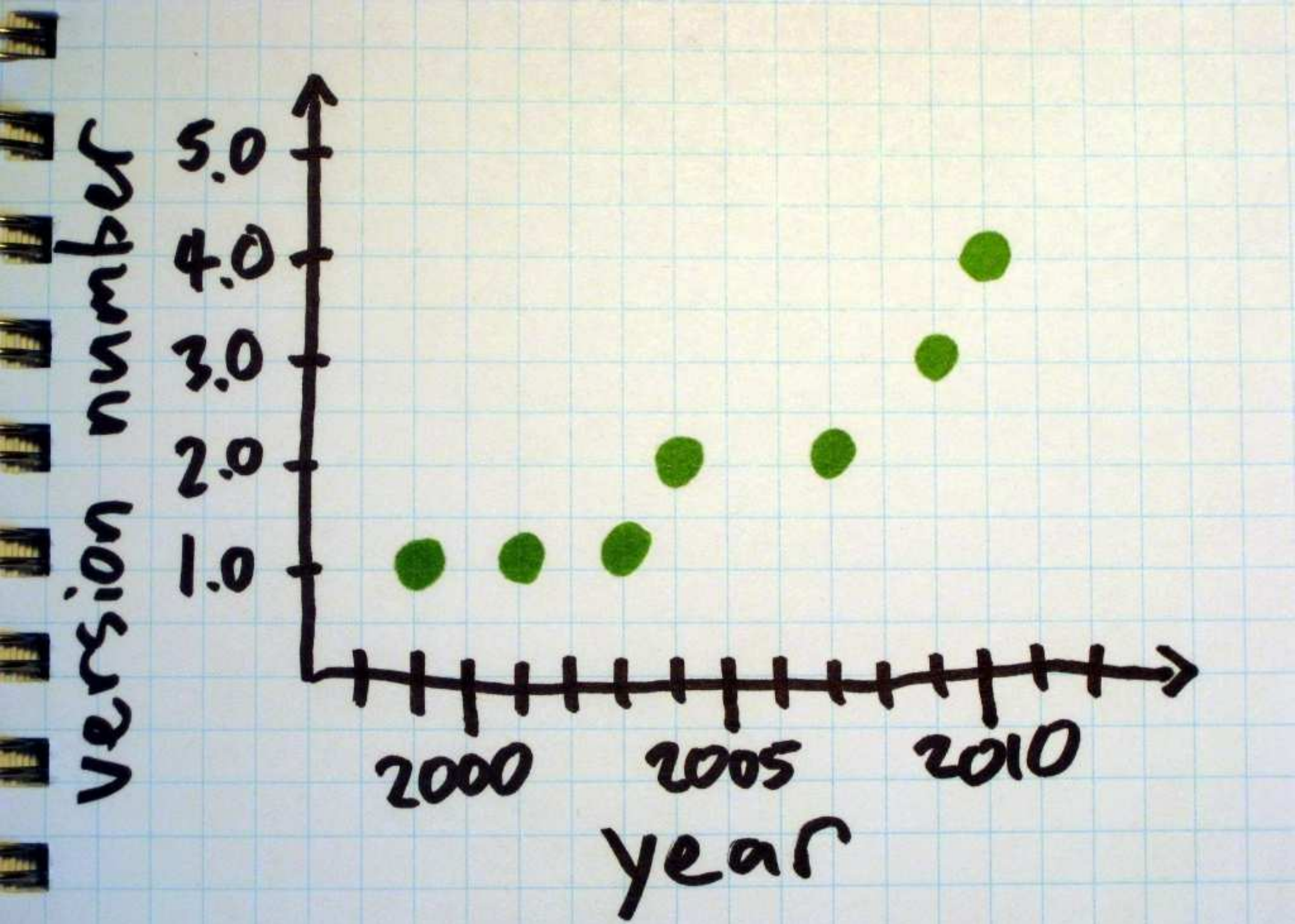
LE

HS

EDR



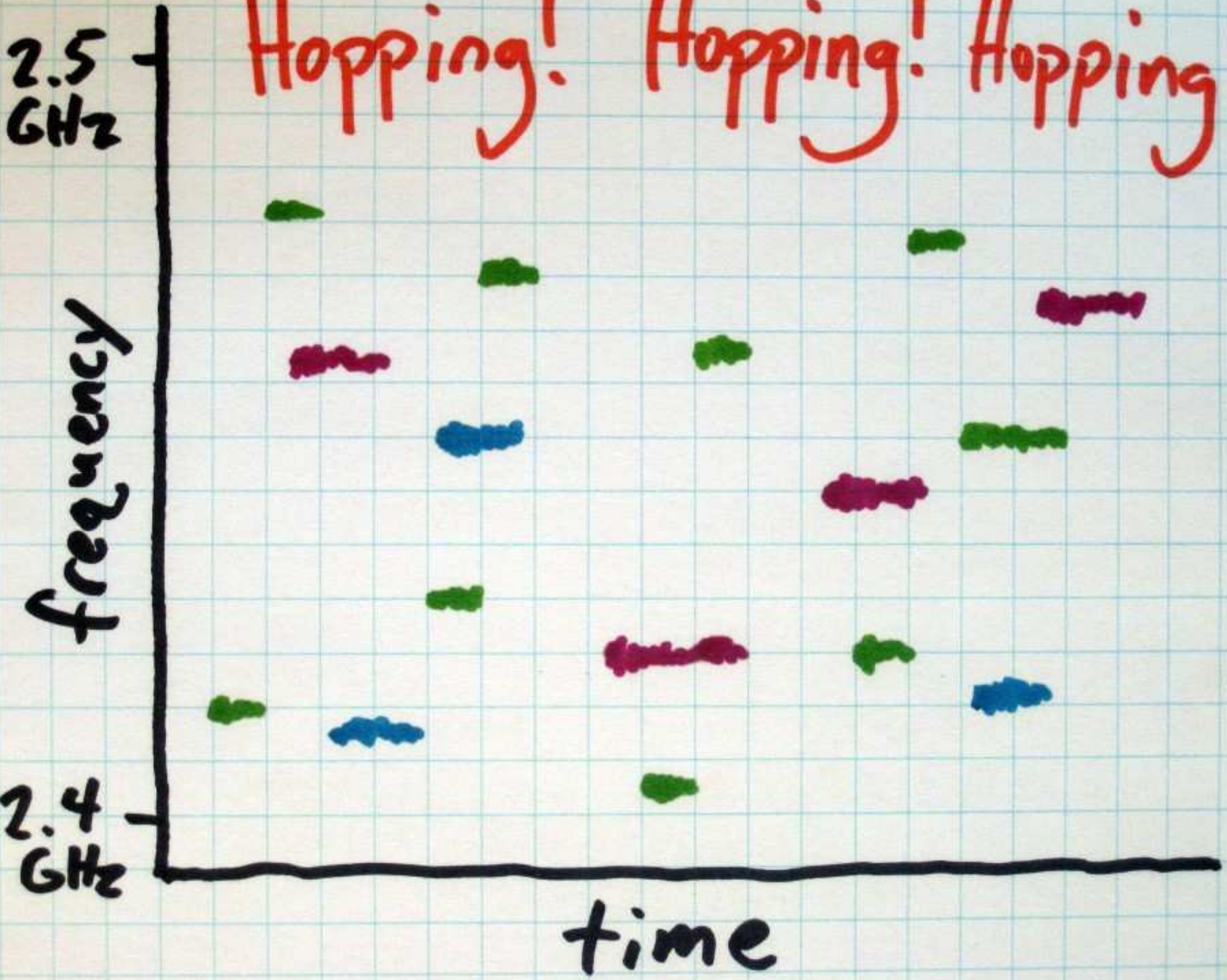
"classic" Bluetooth


version number
5.0
4.0
3.0
2.0
1.0
2000
2005
2010
year

2019

Bluetooth 3.0?

Hopping! Hopping! Hopping!



LE frequency hopping

3 advertising channels

2402 MHz

2426

2480

37 data channels

2404 MHz

2406

⋮

BR hop selection complicated

based on normally clock (not

UAP (not transmitted) and normally transmitted)

LE hop selection

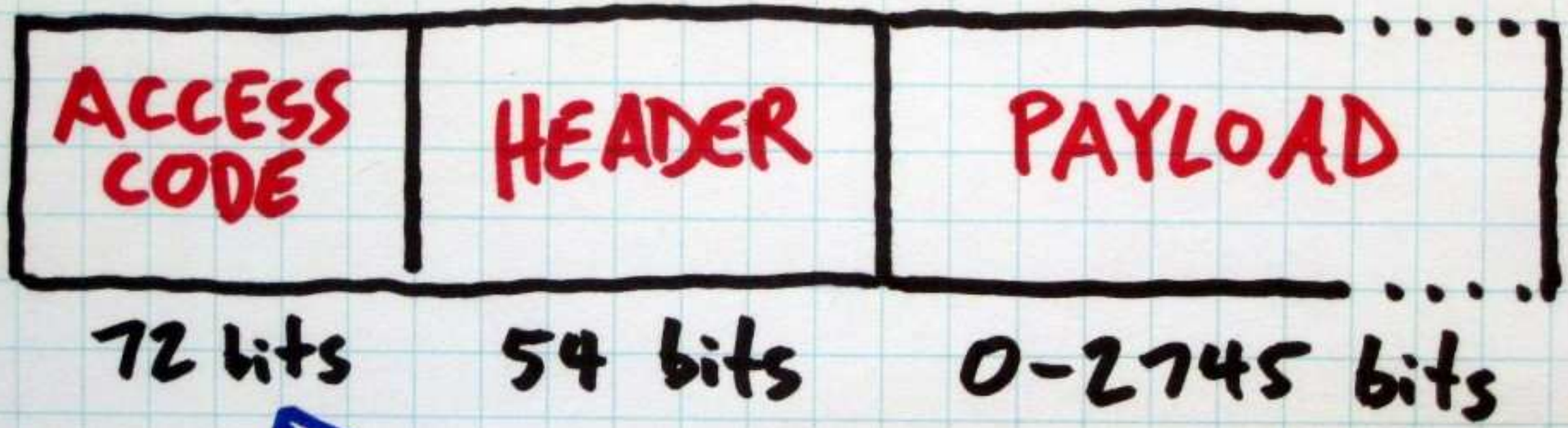
simple

based on previous

hop and channel

map (usually all 37)

device-specific access code



derived from LAP

LE access address

random!

advertising: 0x8E89BED6

whitening

data to transmit

1 1 0 1 0 1 0 1 ...

⊕ top

pseudo random sequence

1 0 0 0 1 1 0 1 ...

↓

transmitted bits

0 1 0 1 1 0 0 0 ...

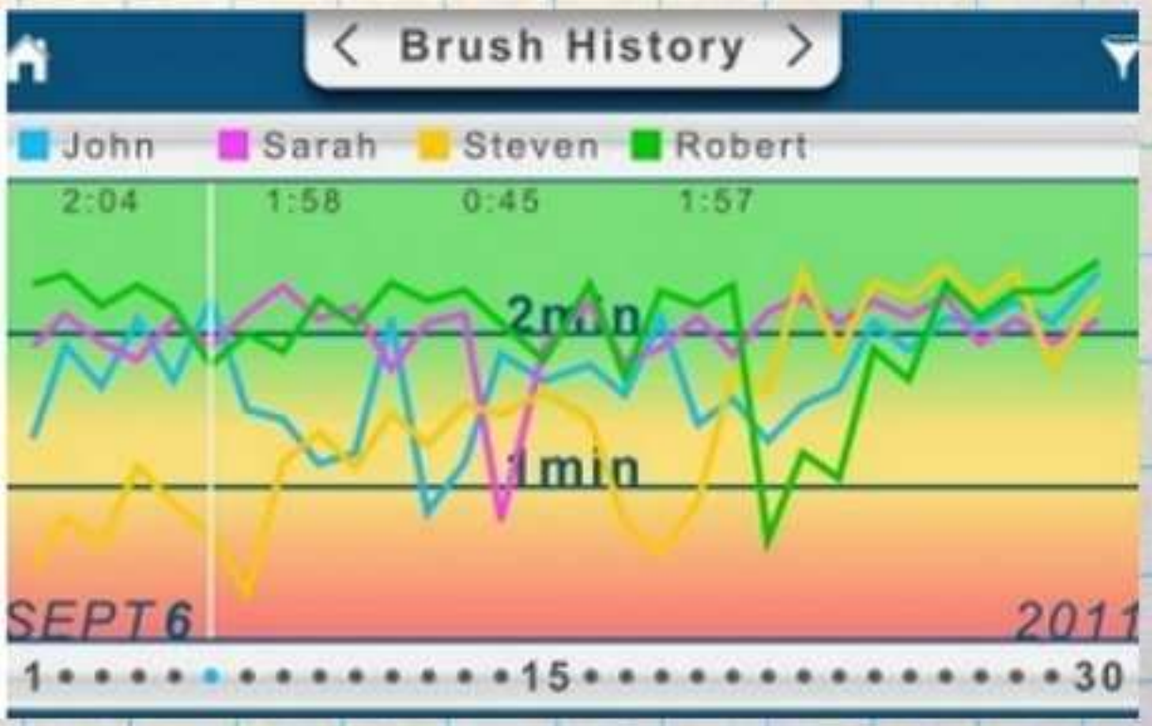
whitening

BR based on UAP, clock

LE based on channel

monitoring hardware


G-SHOCK
WATER 20BAR RESIST
CASIO
ADJUST
SET
MUTE VIB
PS SIG ALM
SHOCK RESIST
POWER
SPLIT·RESET
6·30
P 10:58 50
SELECT
MODE
FIND
START·STOP
Bluetooth


Brush History
John
Sarah
Steven
Robert
2:04
1:58
0:45
1:57
2min
1min
SEPT 6
2011
1
15
30


44:10


AV

MOTOACTV

+

Droid RAZR

?


DEBUG
TEST
TEXAS INSTRUMENTS
CC2540

demonstration

Bluetooth®
SMART

Bluetooth®
SMART READY

If your product bears this logo…	It's compatible with products bearing any of these logos…
Bluetooth® SMART READY	Bluetooth® SMART READY Bluetooth® Bluetooth® SMART
Bluetooth®	Bluetooth® SMART READY Bluetooth®
Bluetooth® SMART	Bluetooth® SMART READY

call it

"Bluetooth Low Energy"

call it
"Bluetooth Low Energy"

BTLE?

BLE?

call it
"Bluetooth Smart"

Call it
"Bluetooth Smart"

BS?

"4.0"

is just

wrong

encryption

BR

LE

E0

AES-CCM

LE pairing methods

Out of Band

Passkey Entry

Just Works

LE pairing methods

Out of Band

Passkey Entry

Just Works

not SSP!

LE pairing methods

Out of Band

Passkey Entry

Just works

not SSP!

not Diffie-Hellman!

Thank you!

http://ubertooth.sf.net/

http://greatscottgadgets.com/

@michaelossmann