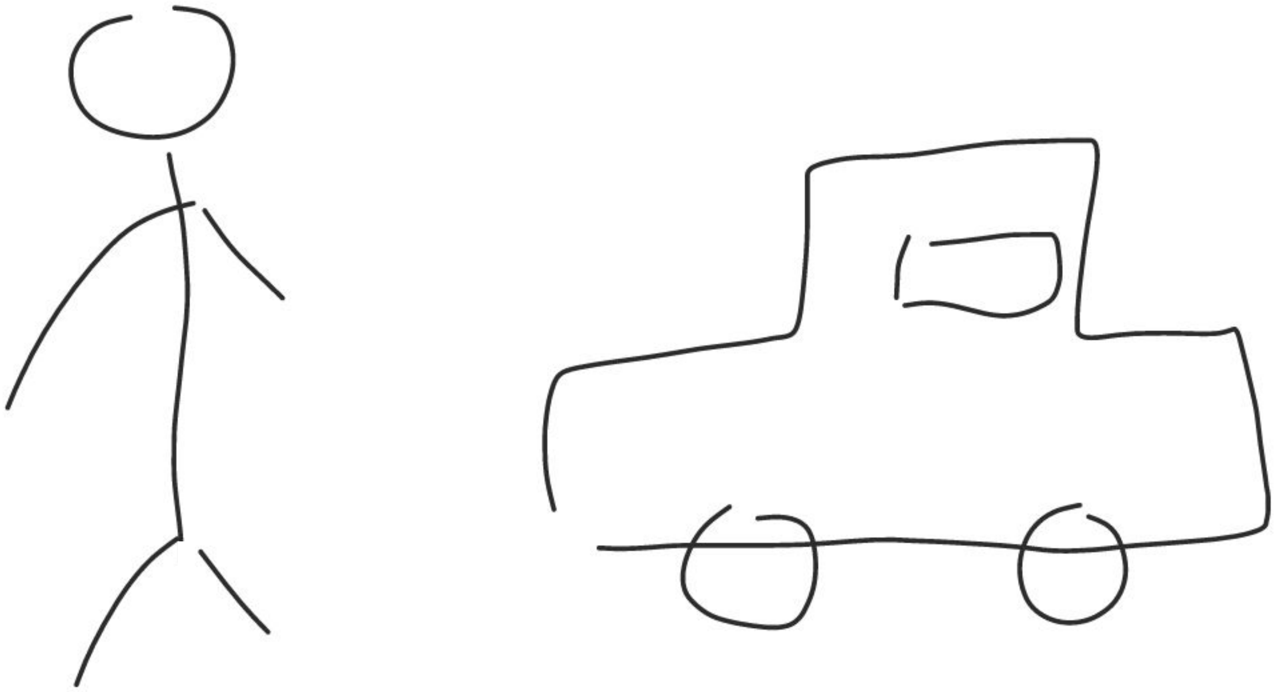
erc European Research Council

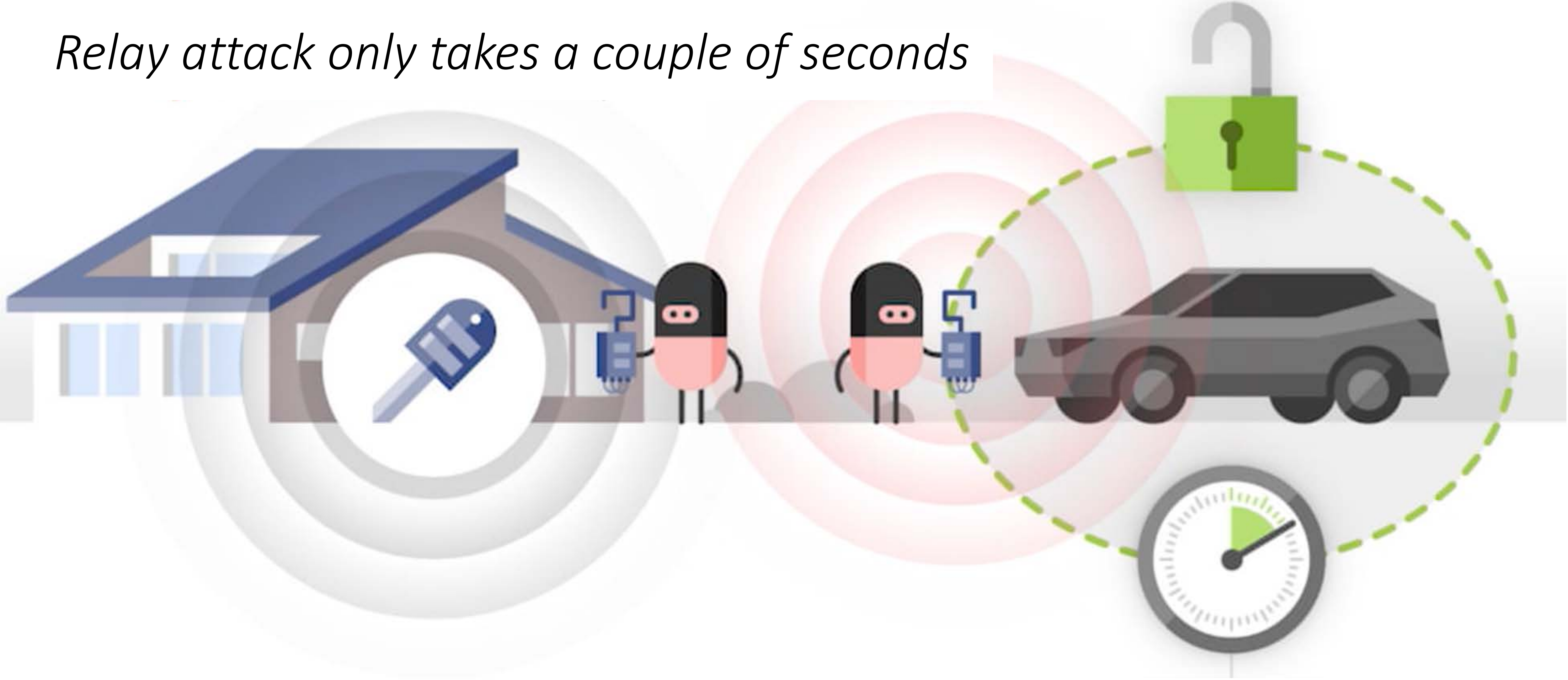
On Secure Positioning (Project CSP: Cross-Layer Design of Secure Positioning)

Srdjan Čapkun

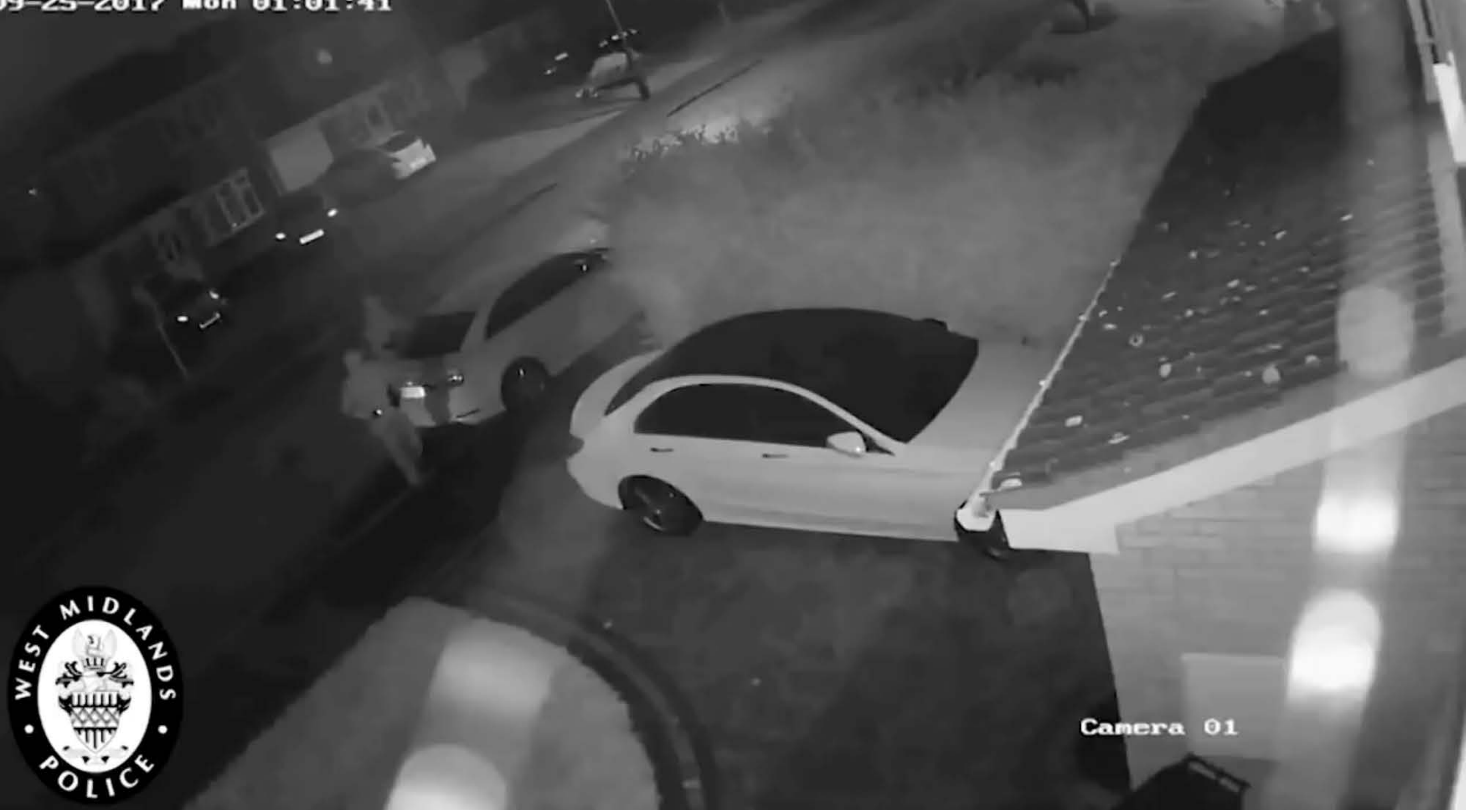
ETH zürich

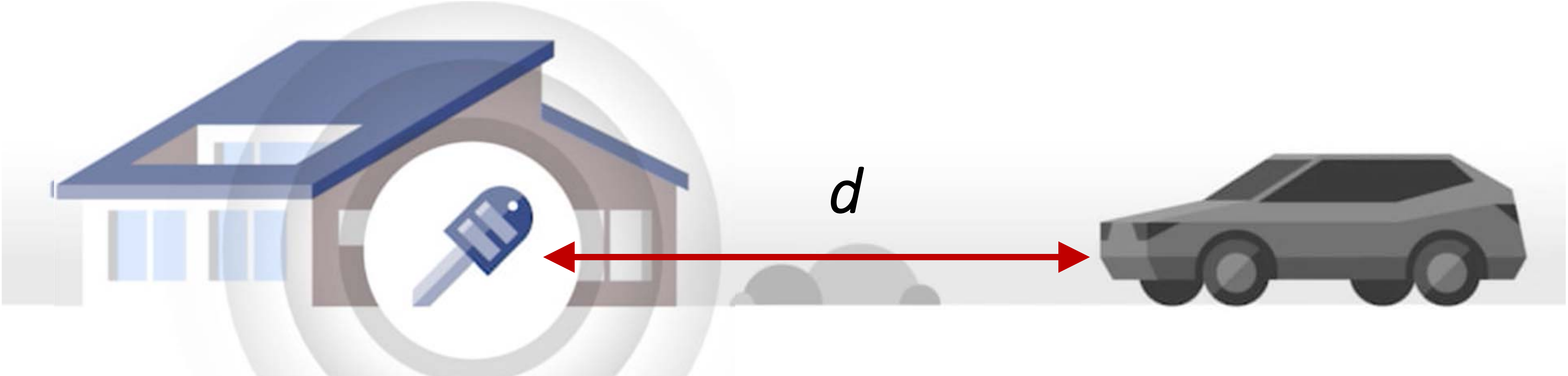


Relay attack only takes a couple of seconds

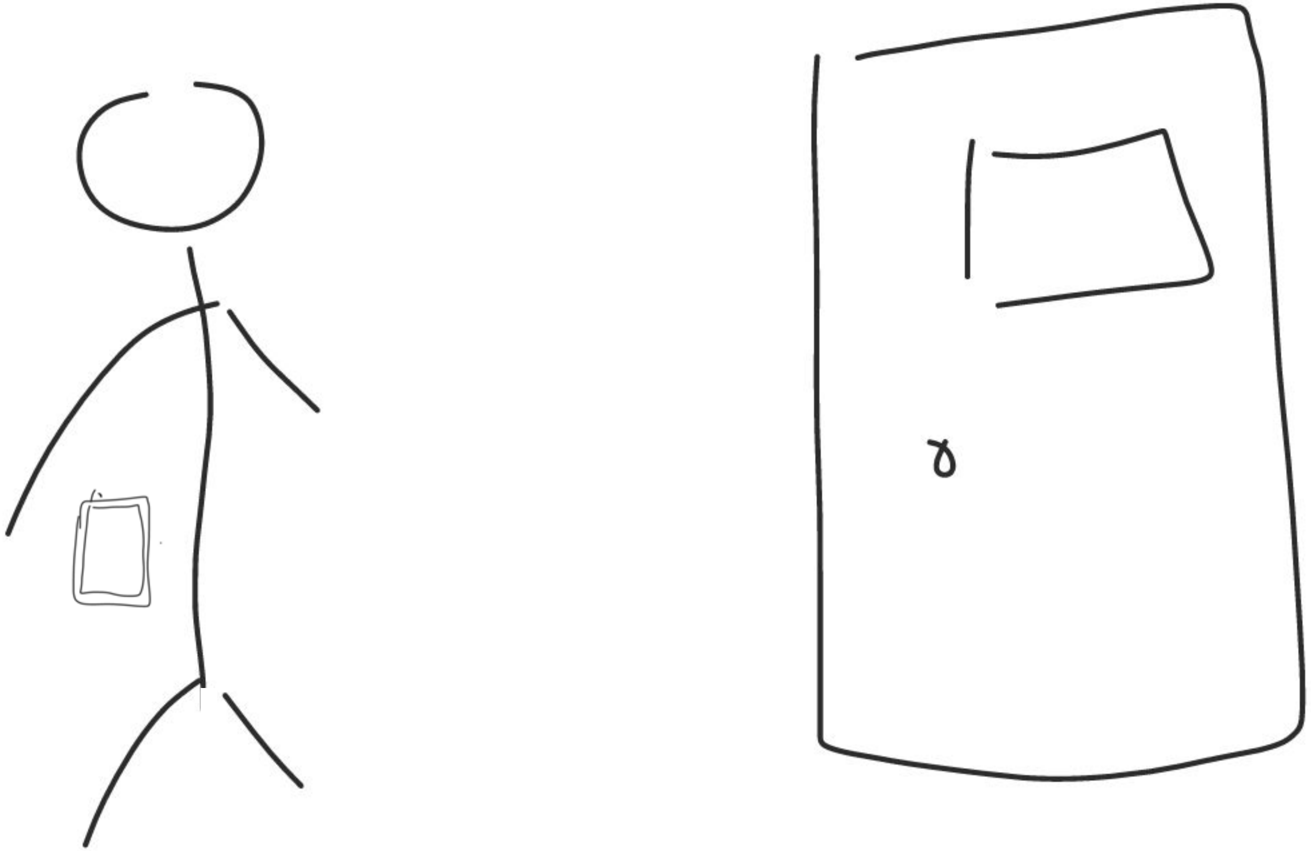


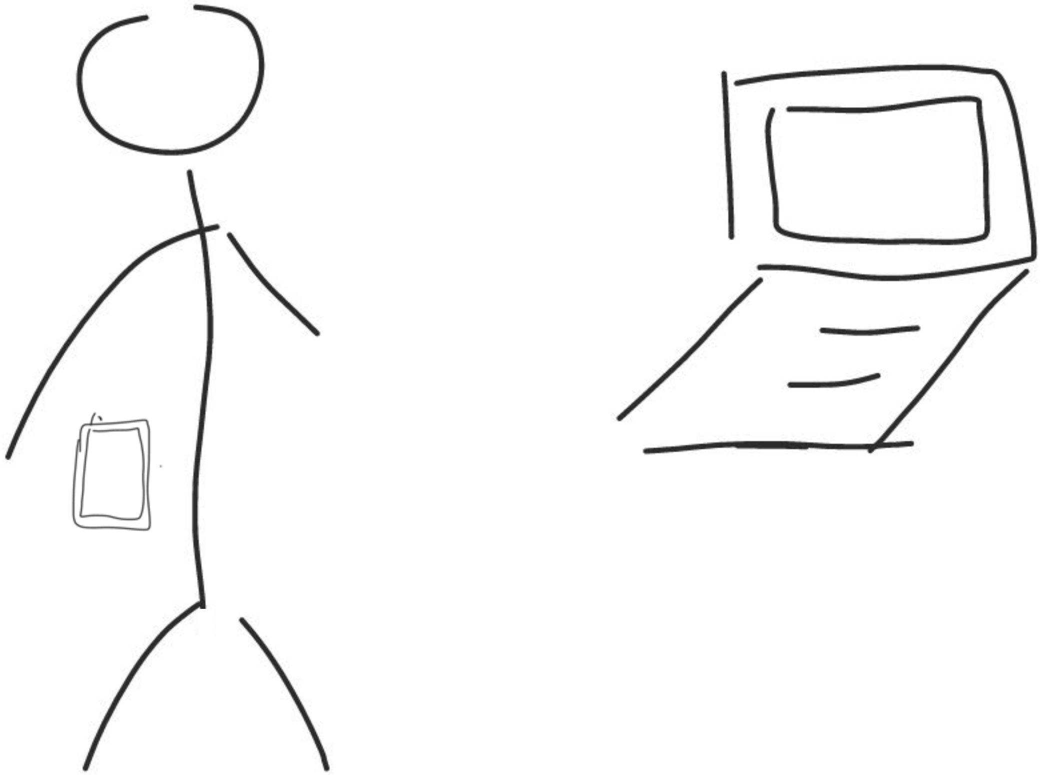
signal strength

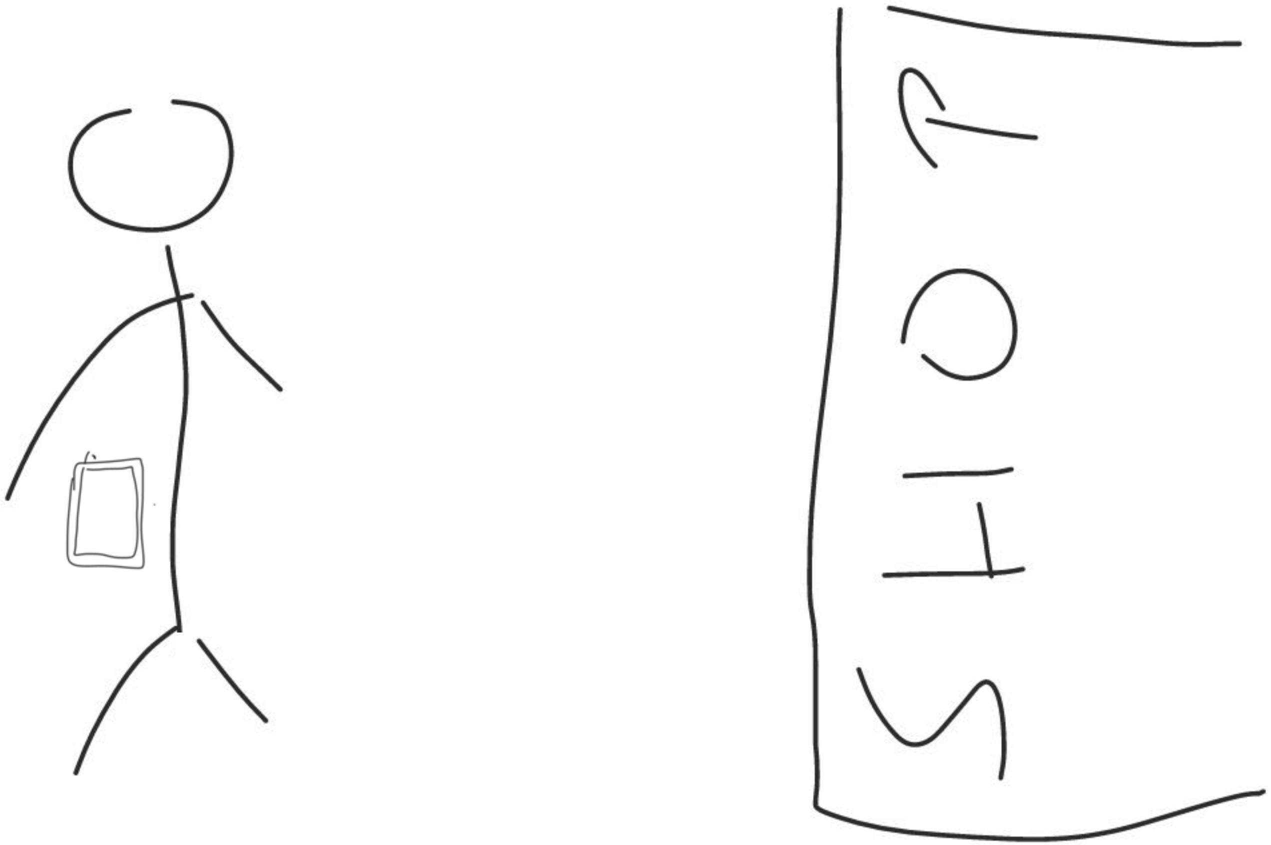

09-25-2017 Mon 01:01:41
Camera 01
WEST MIDLANDS
POLICE

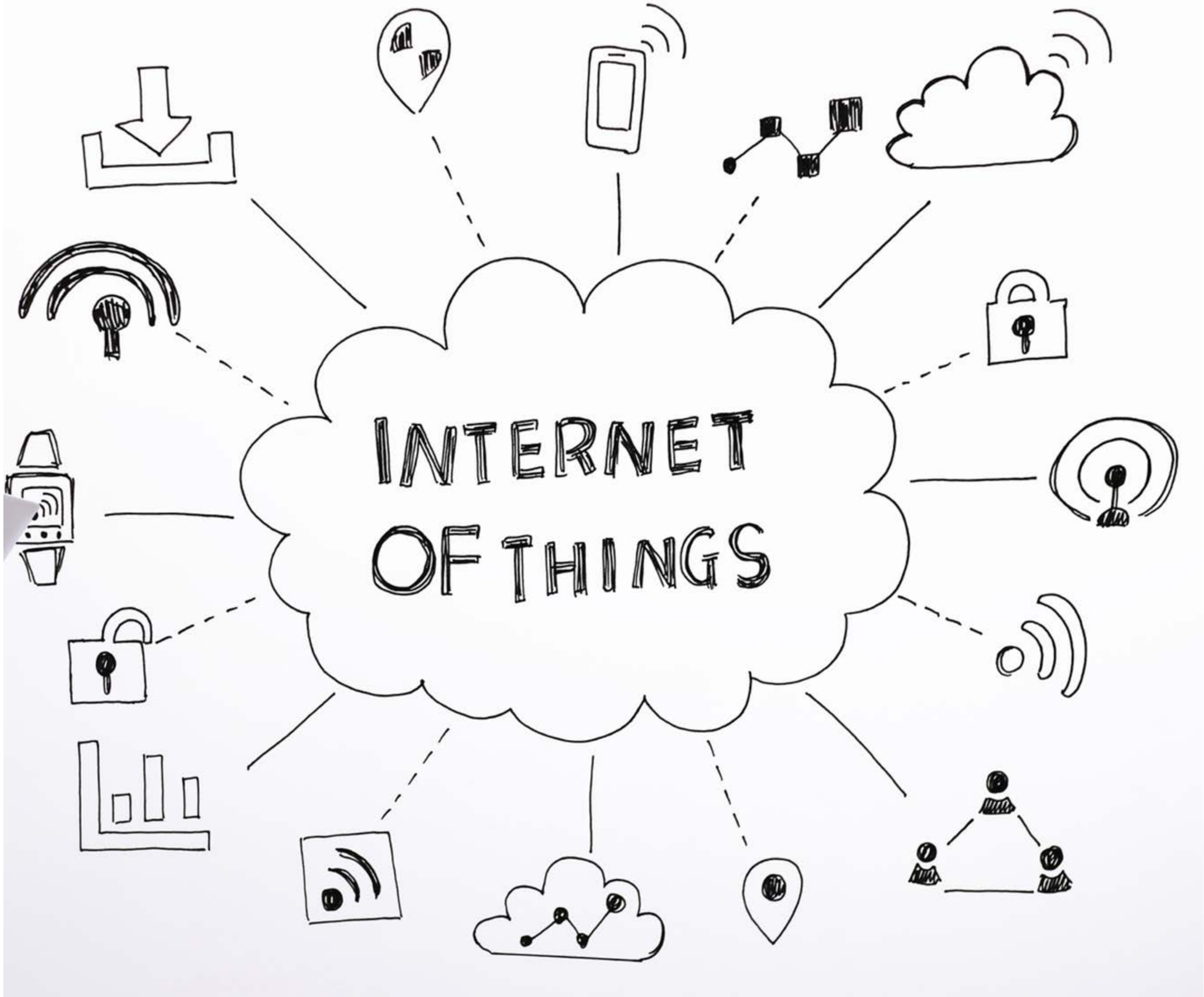


we need secure distance measurement






SHOP


INTERNET
OF THINGS

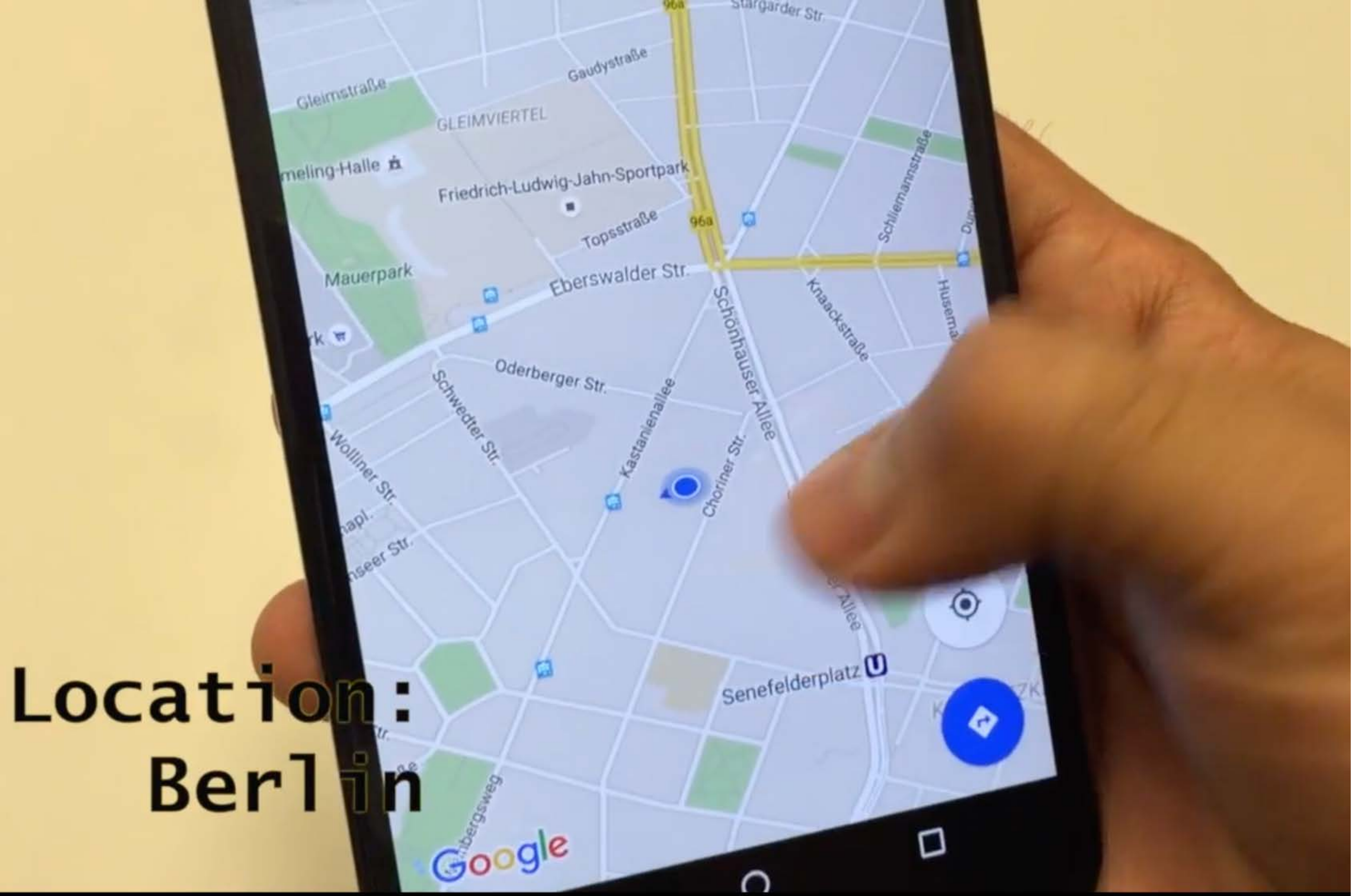
need to know where other objects/people are

need to know where we are

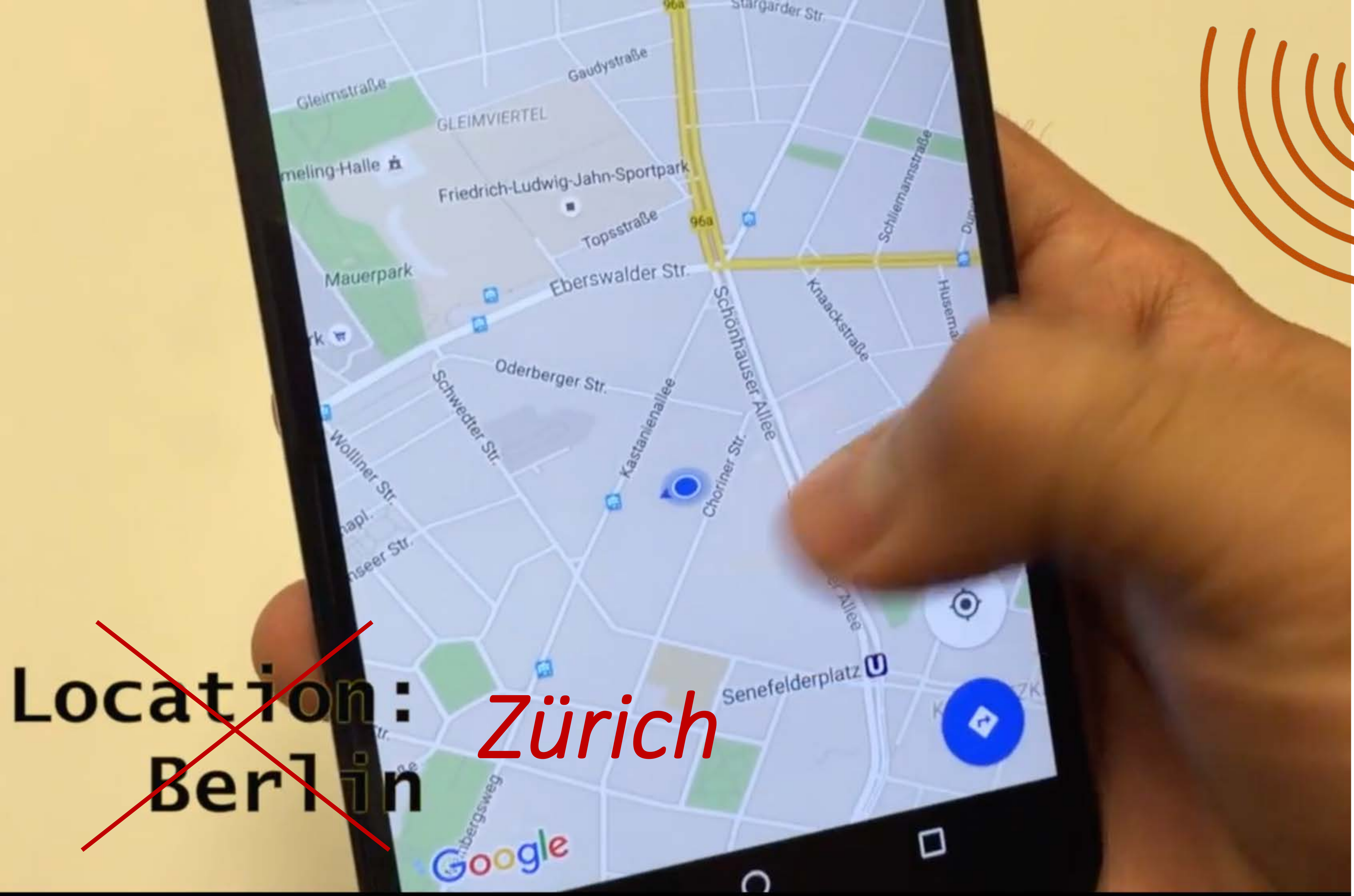
need to know where other objects/people are

need to know where we are

securely



Location:
Berlin



~~Location: Berlin~~

Zürich

ETH zürich

WIRED Spoof, Jam, Destroy: Why We Need a Backup for GPS

SHARE

755

SARAH SCOLES SCIENCE 03.02.18 08:00 AM

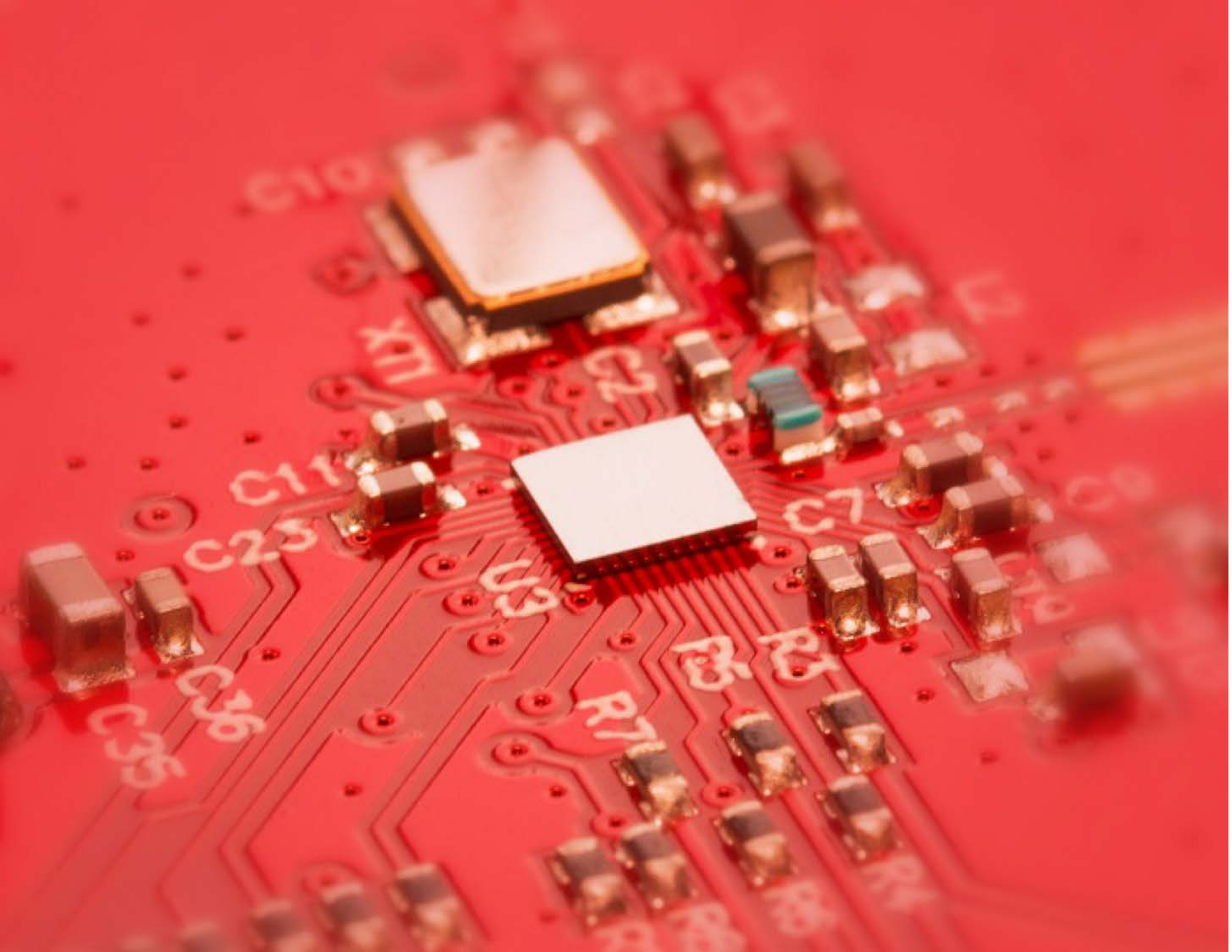
SPOOF, JAM, DESTROY: WHY WE NEED A BACKUP FOR GPS

The 24 satellites that keep GPS running in the US aren't especially secure.

LOCKHEED MARTIN

until now no fully secure distance measurement or positioning systems *until now no <u>fully</u> secure distance measurement or positioning system*

[so we decided to build one at ETH]



new radio IC

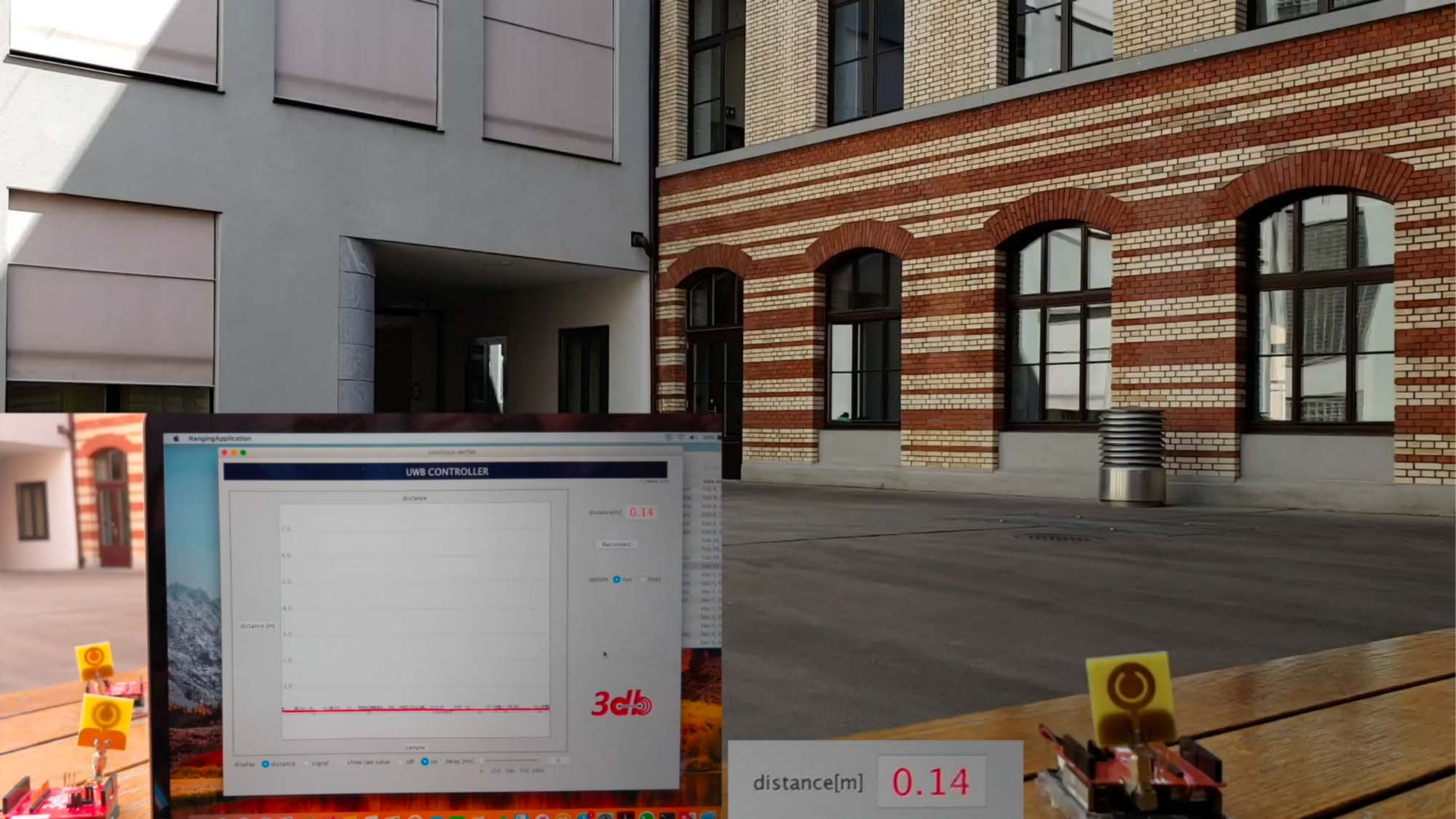
low power

provably secure

precise

fast

3db ETH zürich



distance[m] 0.14

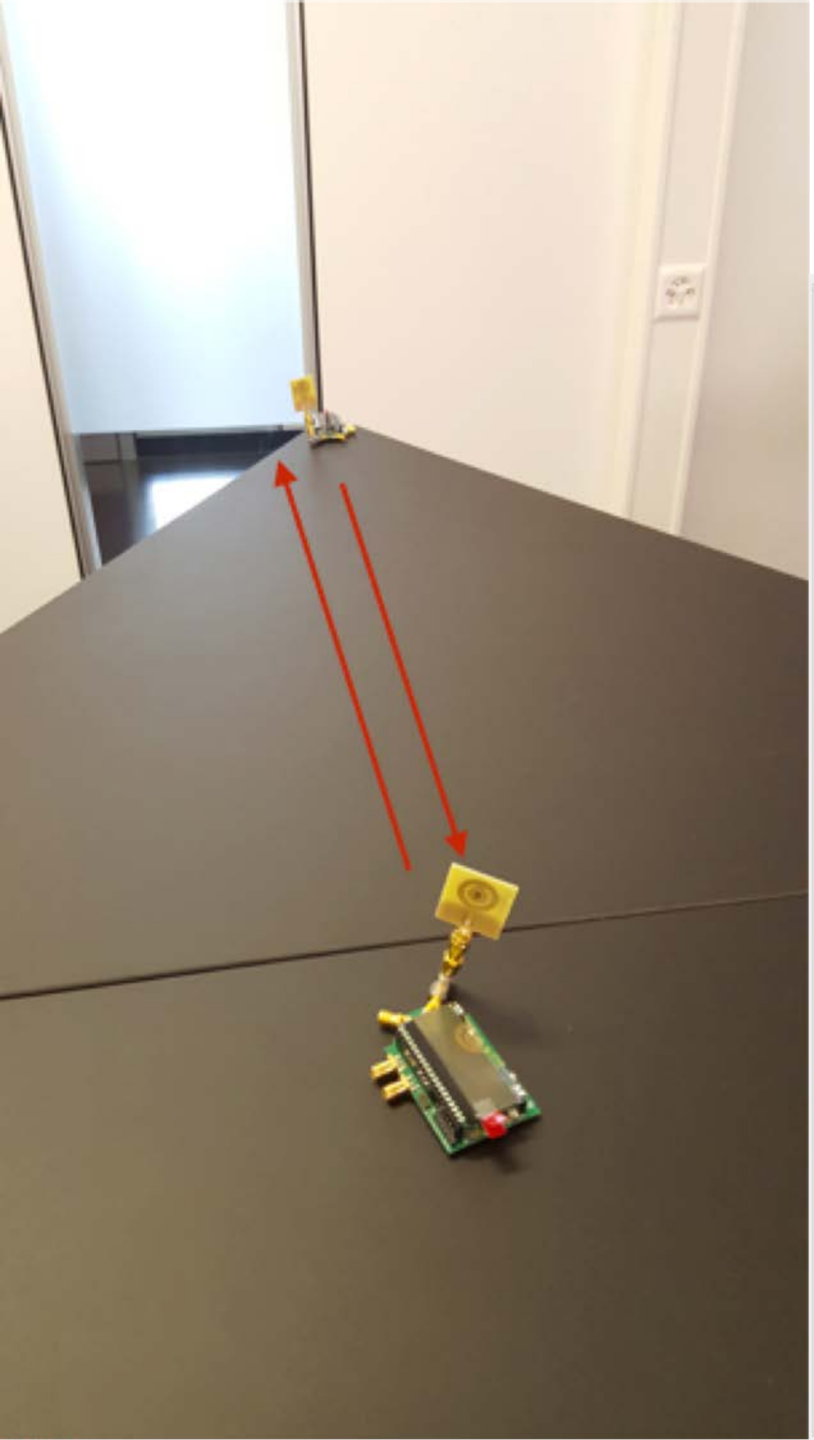
update ● run ○ hold

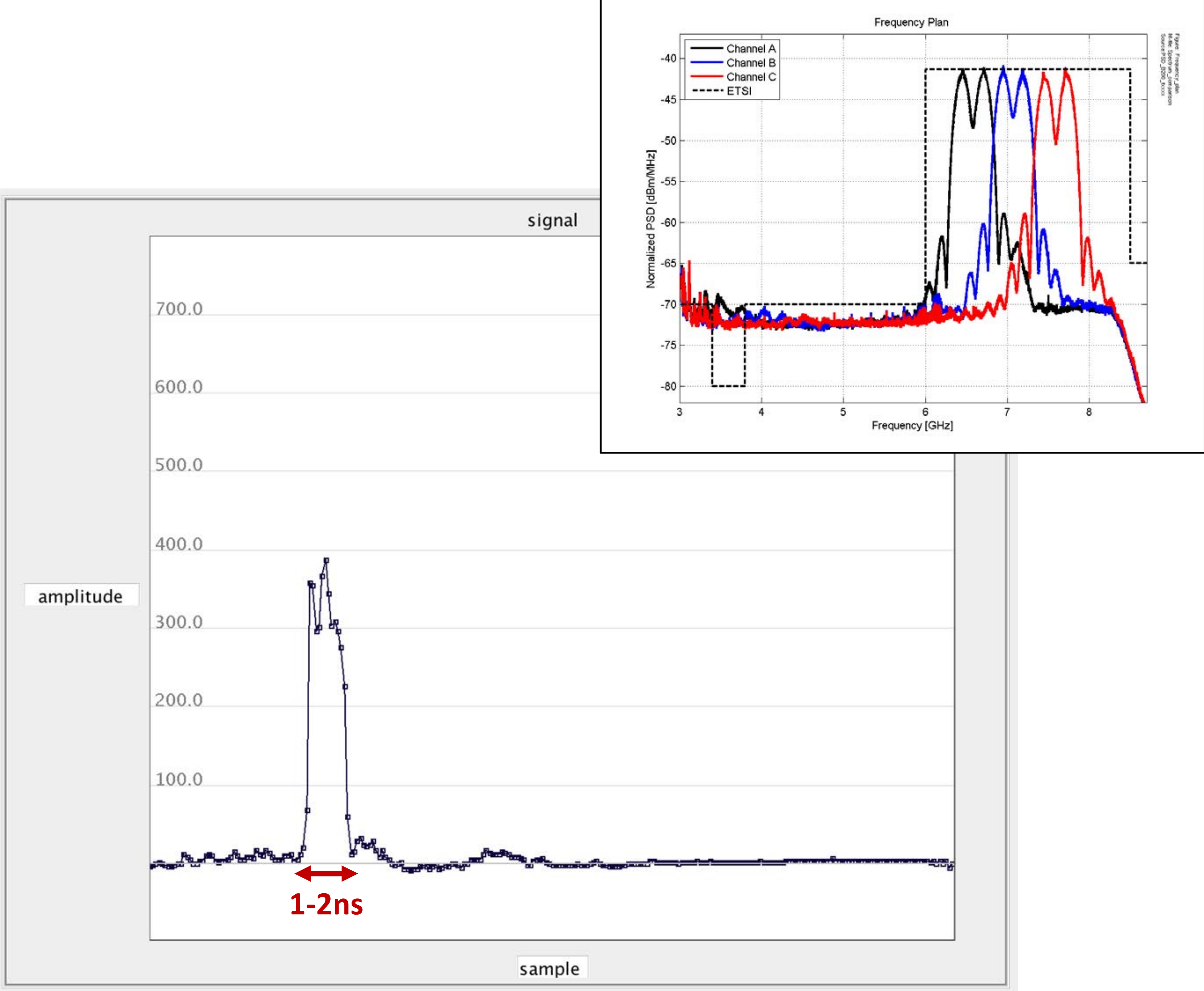
display ● distance ○ signal

show raw value ○ off ● on

delay [ms] 0

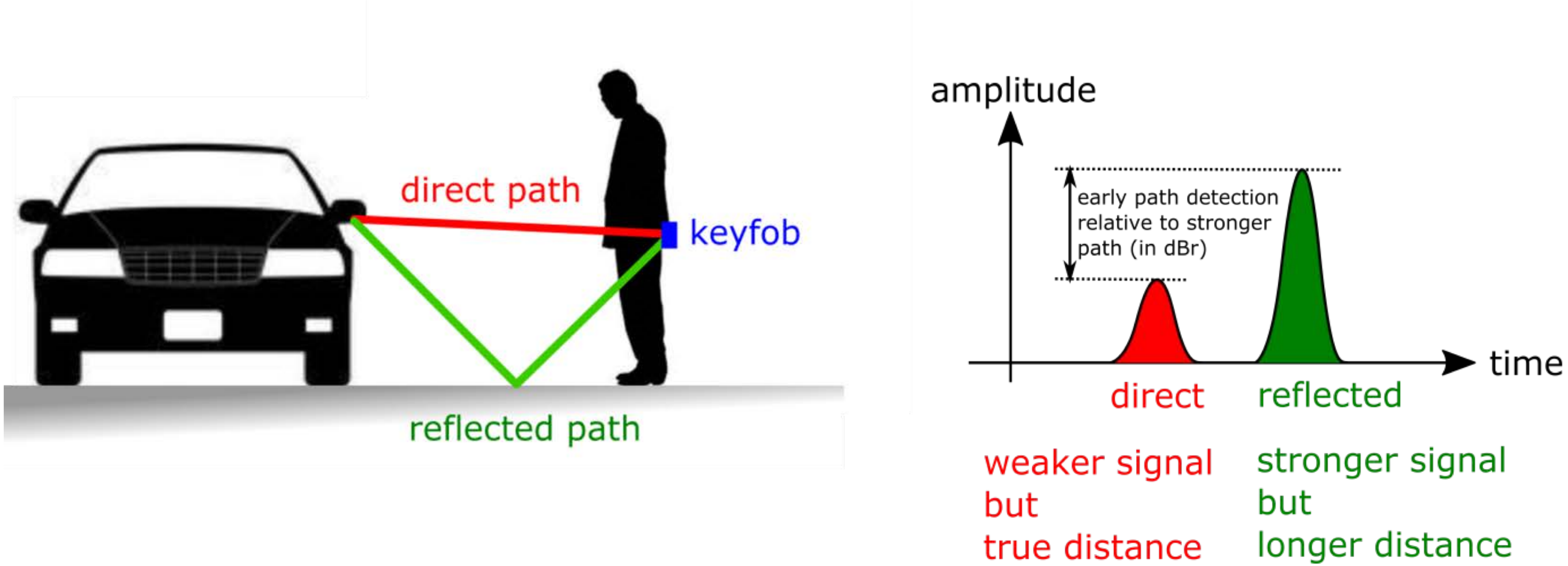
distance[m] 0.14





signal
amplitude
sample
700.0
600.0
500.0
400.0
300.0
200.0
100.0
Frequency Plan
Channel A
Channel B
Channel C
ETSI
Normalized PSD [dBm/MHz]
Frequency [GHz]
-40
-45
-50
-55
-60
-65
-70
-75
-80
3
4
5
6
7
8

1-2ns



early_path_scenario.svg

Securing distance measurement:
Measure the distance between V and P + Authenticate Messages?

Insecure schemes:

NON-Time-of-Flight

NFC / RFID (e.g., ISO)

RSSI measurement (e.g., WiFi, Bluetooth, 802.15.4)

Phase (multi-carrier) measurement (e.g., Atmel AT86RF233)

FMCW (Frequency-Modulated Continuous-Wave)

AoA (Angle of Arrival) measurement (e.g., Bluetooth 5.0)

Time-of-Flight

Chirp Spread Spectrum (802.15.4a, ISO/IEC 24730-5, NanoLOC)

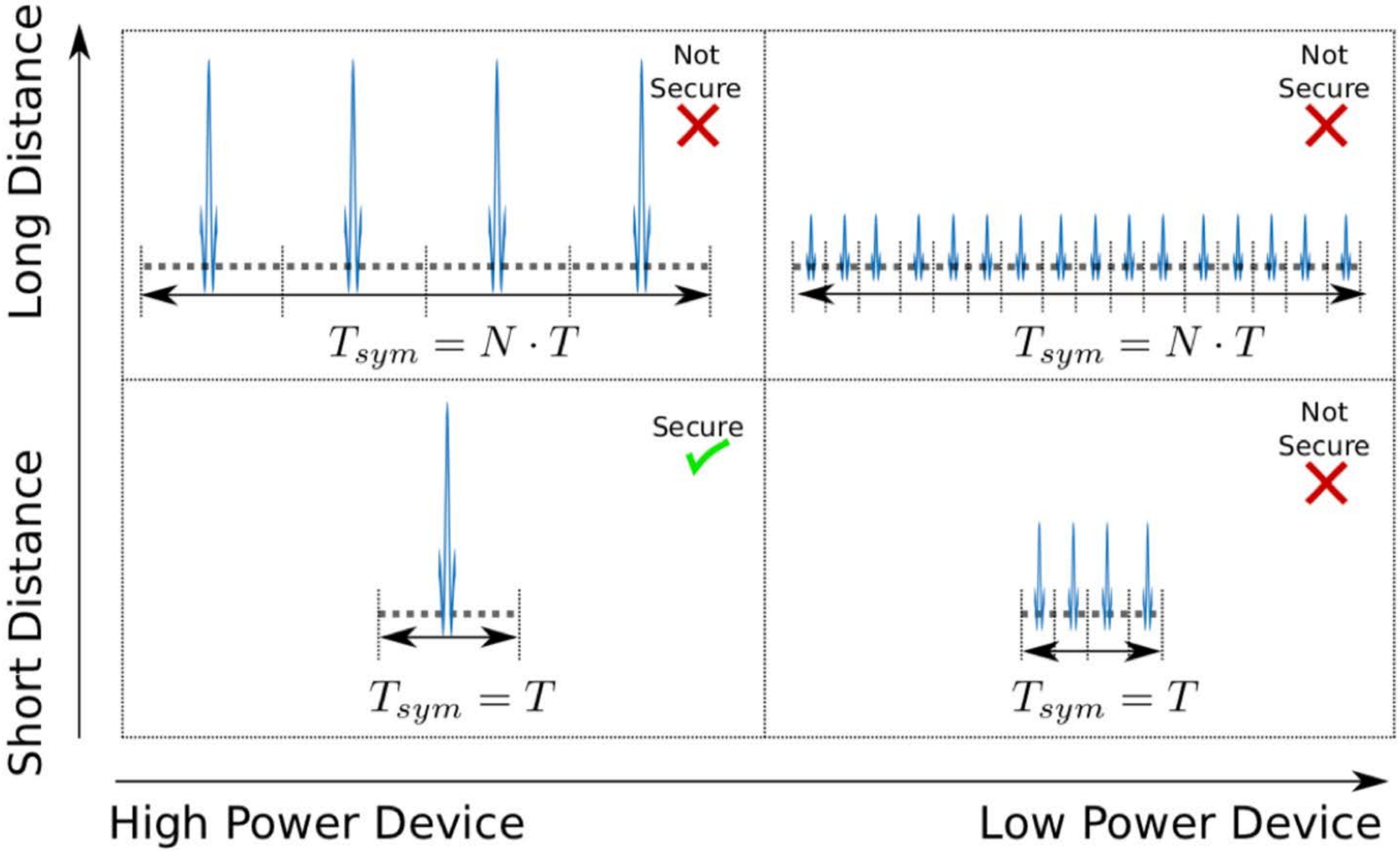
Ultra Wide Band (UWB)

802.15.4 UWB

Only provably secure:

802.15.4z LPR single pulse per bit

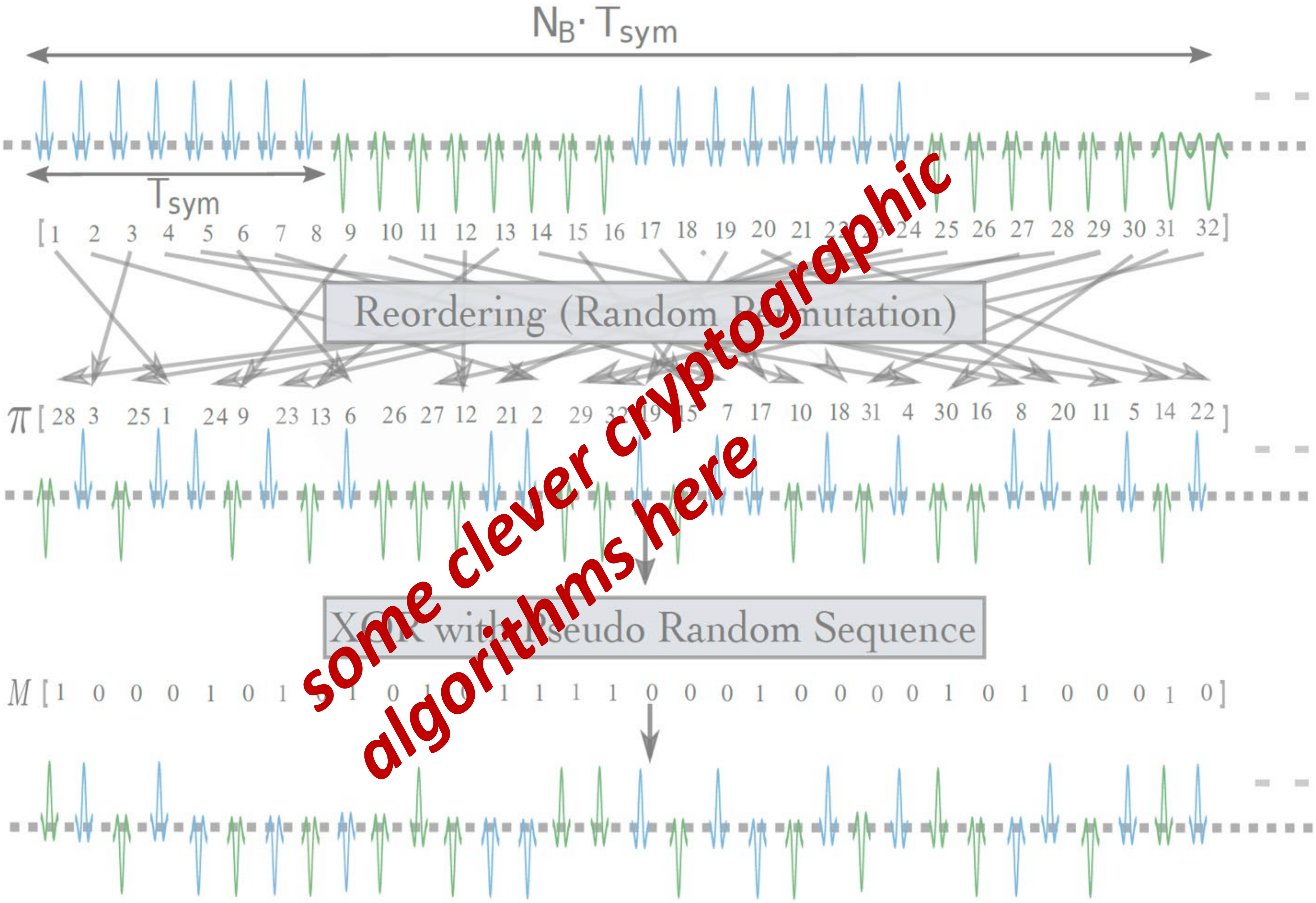
UWB-PR multi-pulse per bit [Singh17]


Long Distance
Short Distance
Not Secure
✗
$T_{sym} = N \cdot T$
Not Secure
✗
$T_{sym} = N \cdot T$
Secure
✓
$T_{sym} = T$
Not Secure
✗
$T_{sym} = T$
High Power Device
Low Power Device

common assumption in distance bounding research:

only short (UWB) pulses and rapid bit exchange are secure *we showed [2017] that this is wrong*

distance bounding can be done using longer symbols (we fully implemented it)



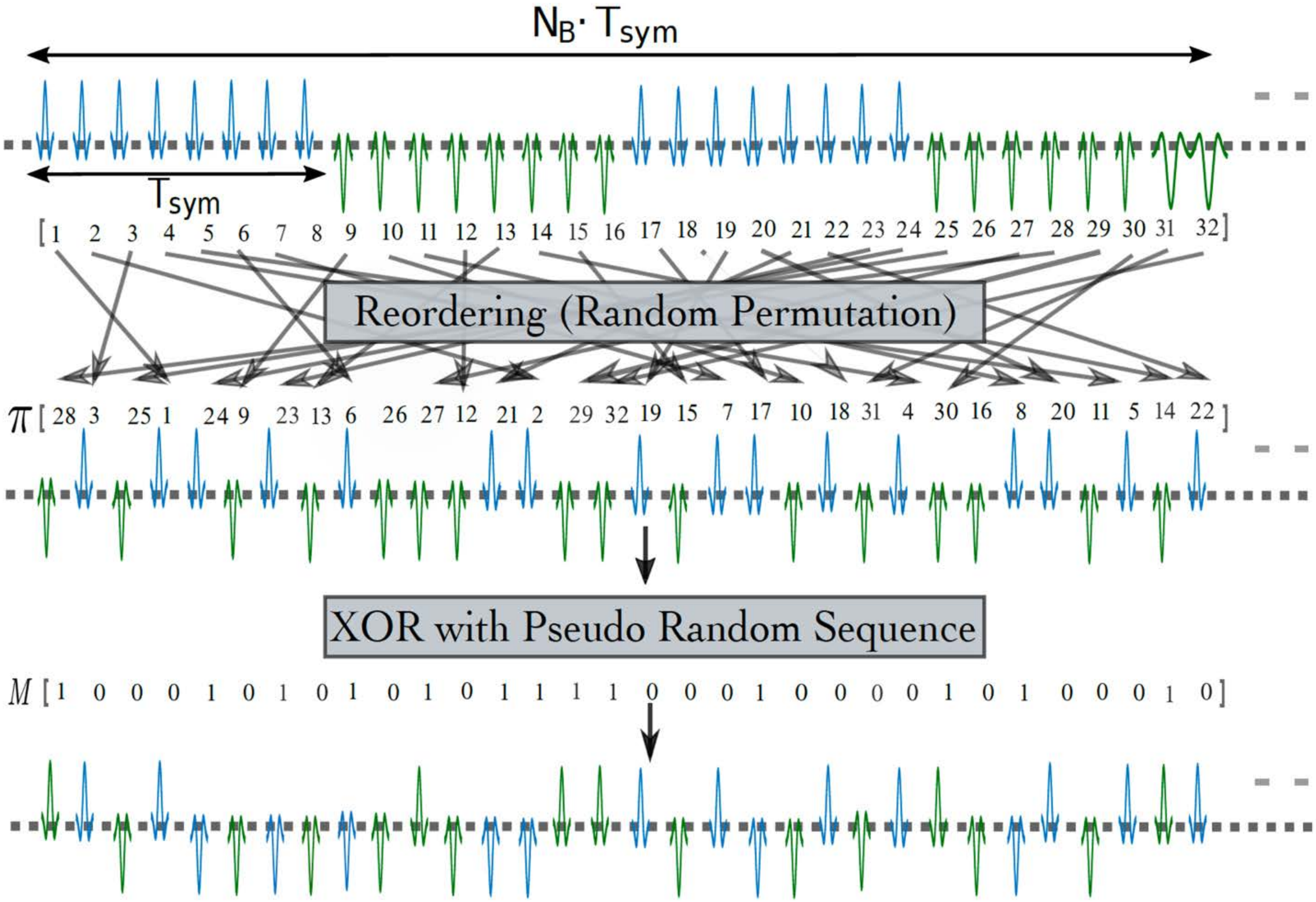
$N_B \cdot T_{sym}$
T_{sym}
[1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32]
Reordering (Random Permutation)
π [28 3 25 1 24 9 23 13 6 26 27 12 21 2 29 32 19 15 7 17 10 18 31 4 30 16 8 20 11 5 14 22]
XOR with Pseudo Random Sequence
M [1 0 0 0 1 0 1 1 0 1 0 1 1 1 1 0 0 0 1 0 0 0 0 1 0 1 0 0 0 1 0]

some clever cryptographic algorithms here

special secure modulation

long range

UWB with pulse reordering (UWB-PR)



$N_B \cdot T_{sym}$

T_{sym}

[1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32]

Reordering (Random Permutation)

π [28 3 25 1 24 9 23 13 6 26 27 12 21 2 29 32 19 15 7 17 10 18 31 4 30 16 8 20 11 5 14 22]

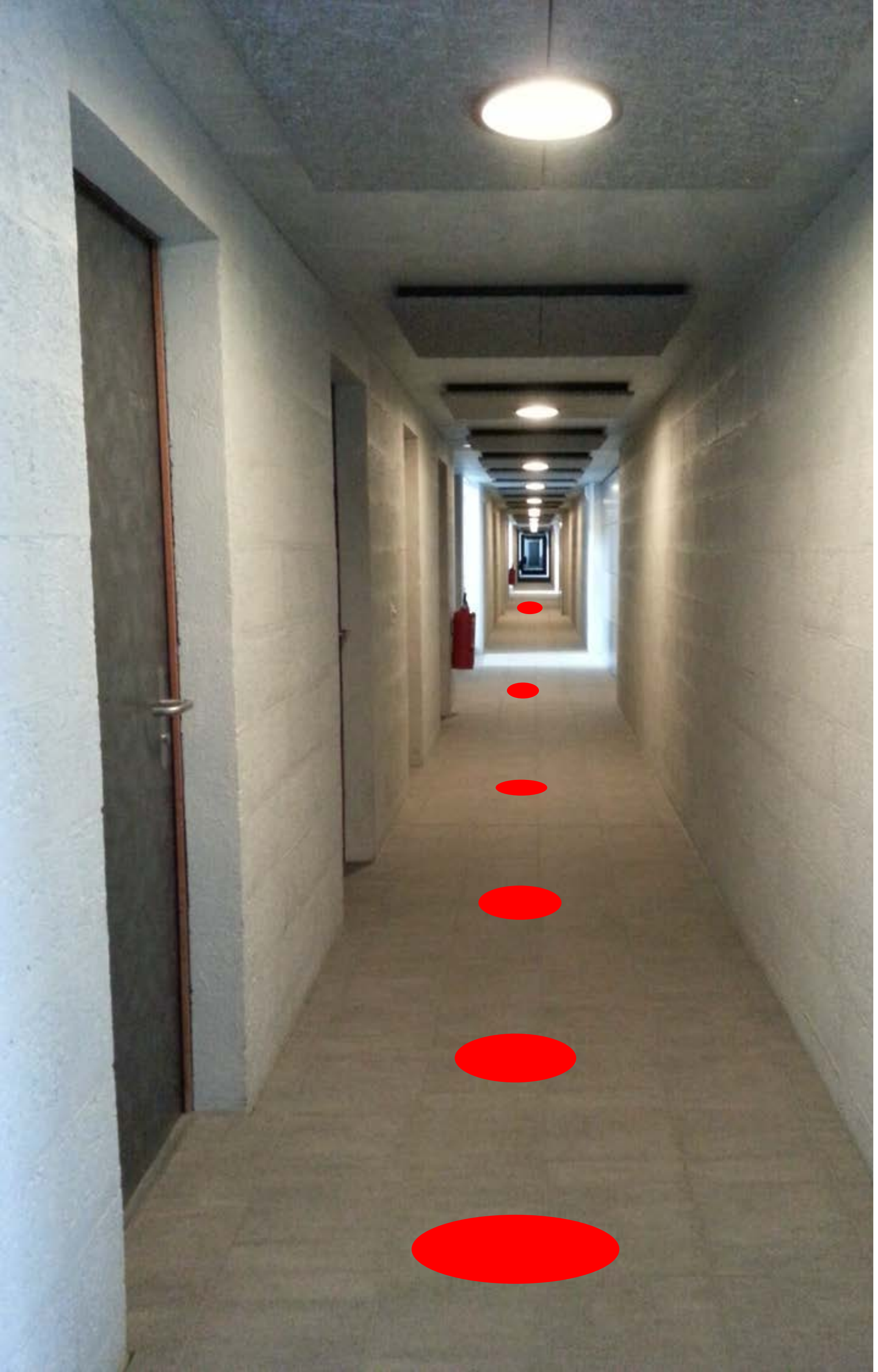
XOR with Pseudo Random Sequence

M [1 0 0 0 1 0 1 0 1 0 1 0 1 1 1 1 0 0 0 1 0 0 0 0 1 0 1 0 0 0 1 0]

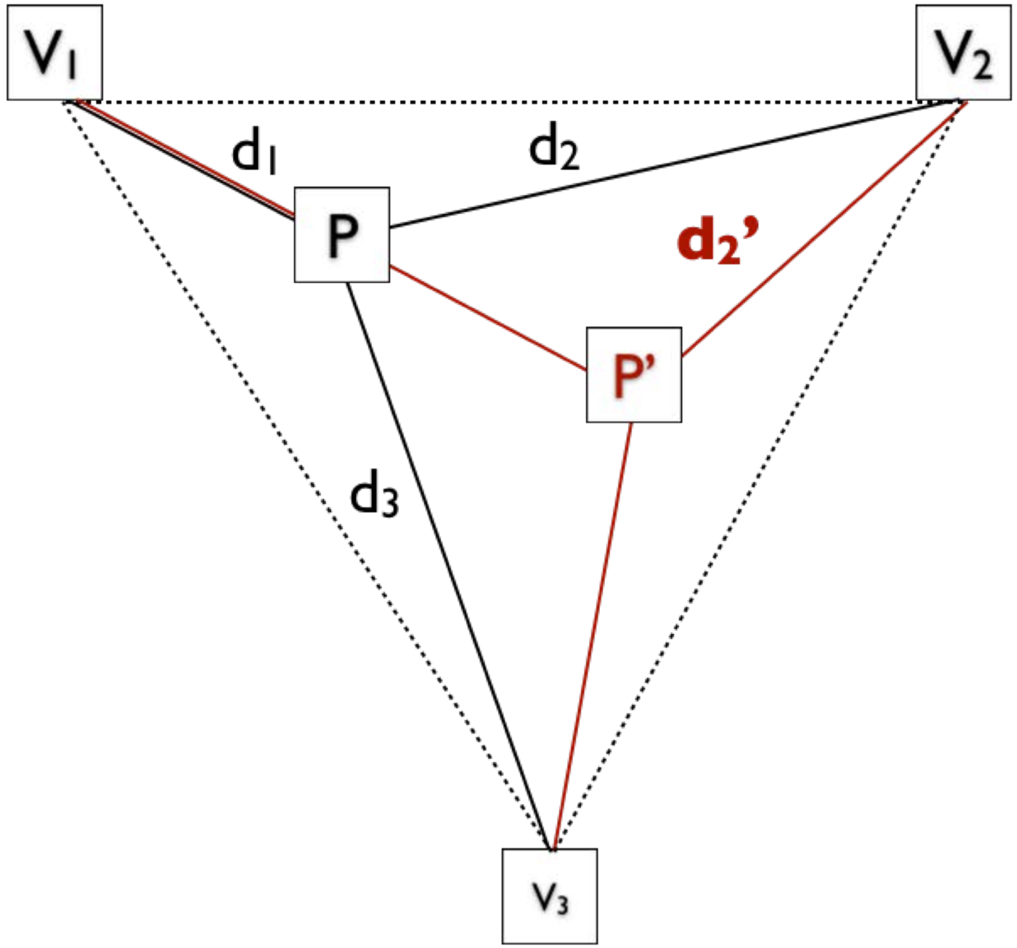
special secure modulation

long range

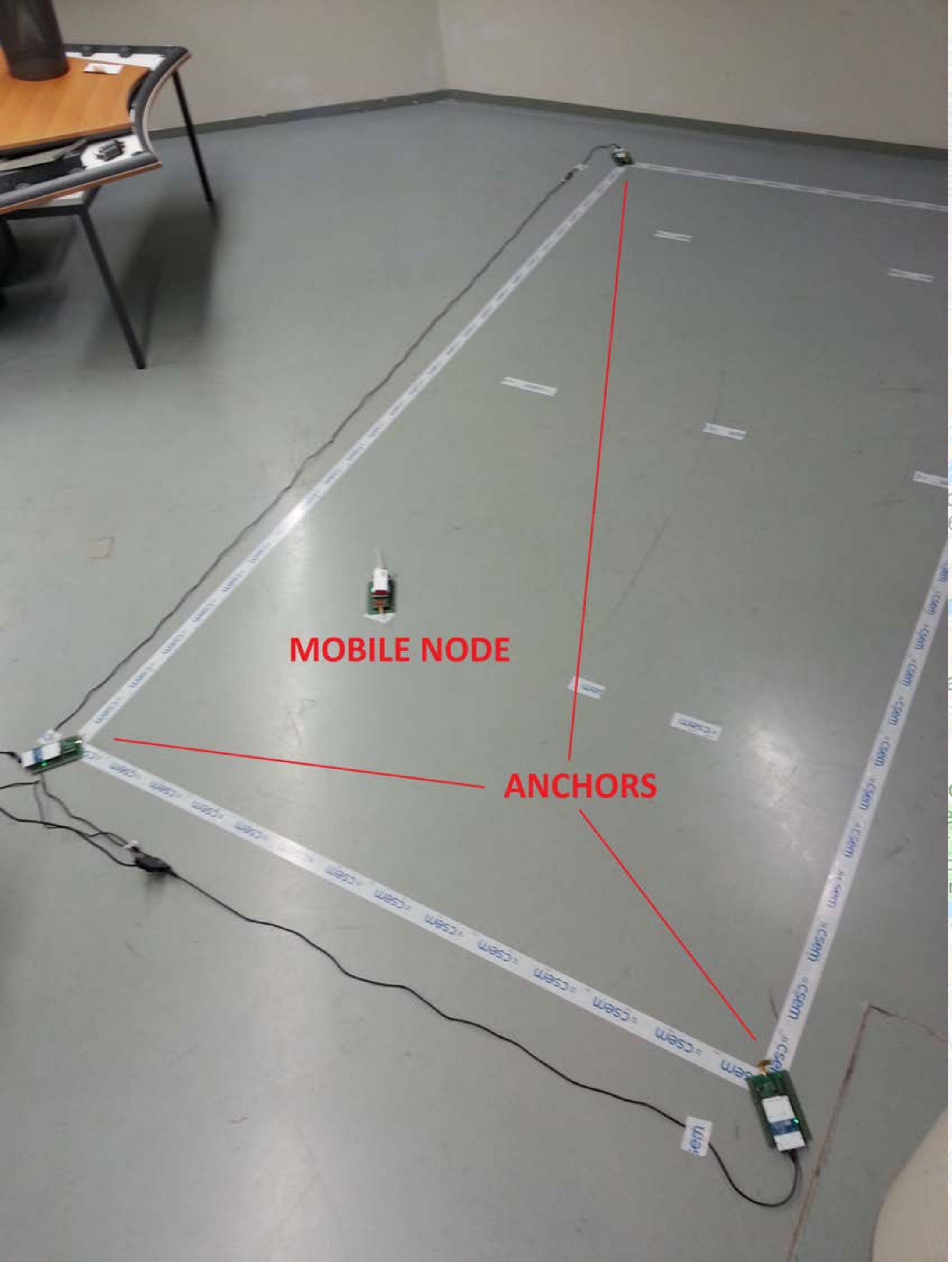
UWB with pulse reordering (UWB-PR)

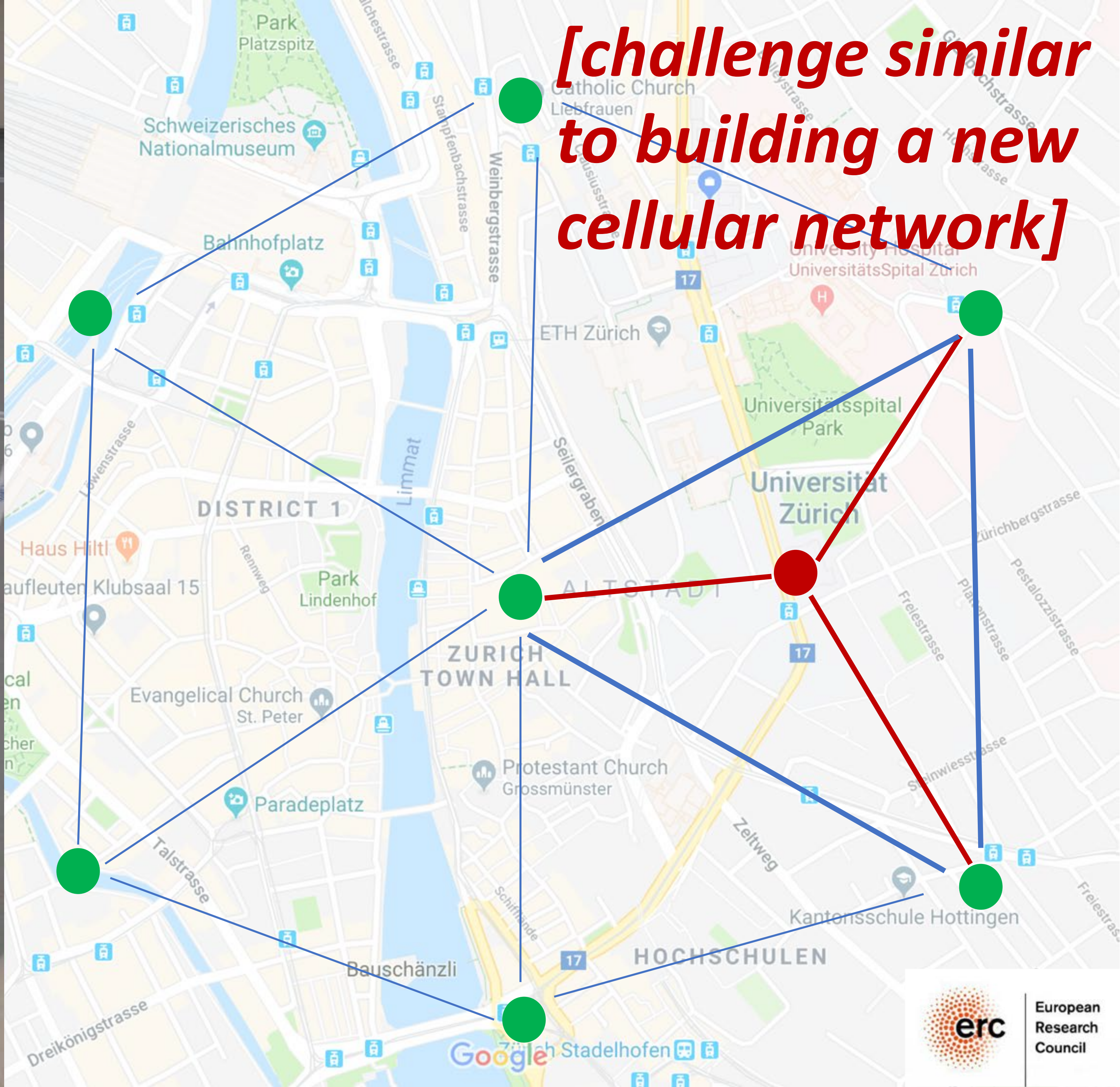


Most secure distance measurement schemes =>
distance cannot be shortened by the attacker
This is sufficient to build SECURE POSITIONING



P→P' => d2'<d2





[challenge similar to building a new cellular network]

erc European Research Council

Long Term Goal:
widely deployed secure positioning infrastructure

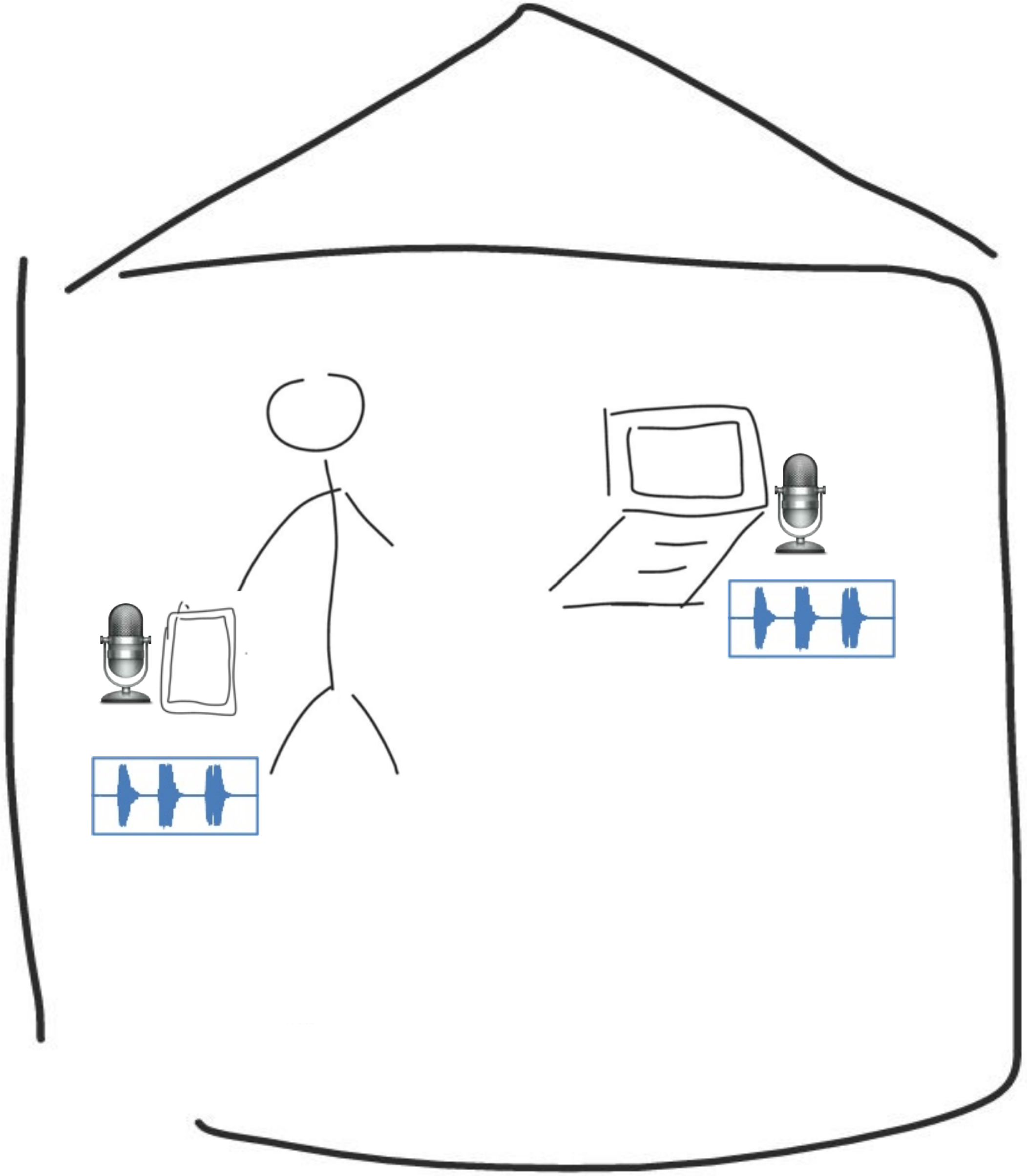
Standardization:

802.15.4z (UWB)

- *Interact with relevant partners*
- *Increase adoption*

But RF is not the only sensing modality

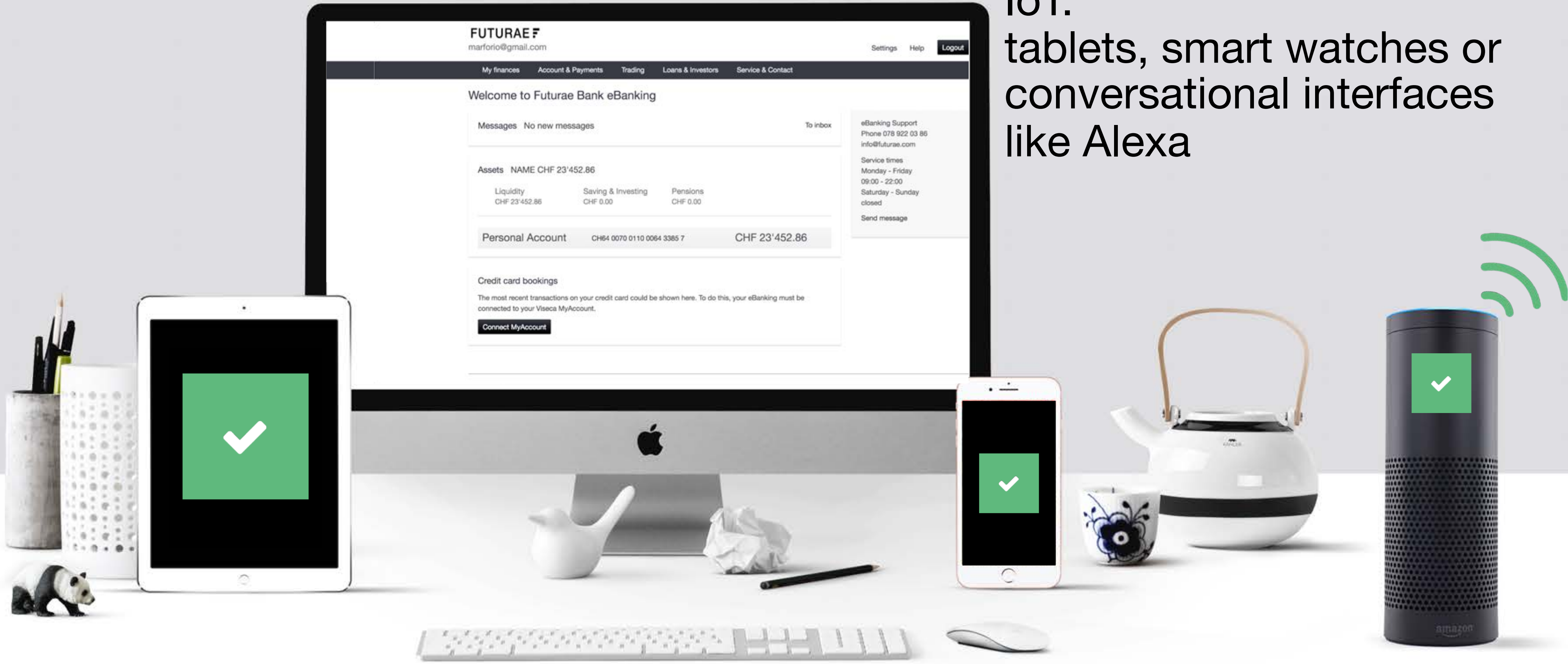
SoundProof: Non-Interactive Online Authentication



ETH zürich FUTURAE

SoundProof: Non-Interactive Online Authentication

IoT:
tablets, smart watches or conversational interfaces like Alexa



marforio@gmail.com

Welcome to Futurae Bank eBanking

Messages No new messages

Assets NAME CHF 23'452.86

Liquidity	Saving & Investing	Pensions
CHF 23'452.86	CHF 0.00	CHF 0.00

Personal Account CH64 0070 0110 0064 3385 7 CHF 23'452.86

Credit card bookings

The most recent transactions on your credit card could be shown here. To do this, your eBanking must be connected to your Viseca MyAccount.

eBanking Support
Phone 078 922 03 86
info@futurae.com

Service times
Monday - Friday
09:00 - 22:00
Saturday - Sunday
closed

ETH zürich FUTURAE

it is time to “de-virtualize”

we need to “get physical” again to …

it is time to “de-virtualize”

we need to “get physical” again to …

… secure existing systems

… enable deployment of new systems

ETH zürich

ZISC
Zurich
Information
Security & Privacy
Center

www.securepositioning.com

capkuns@inf.ethz.ch

erc
European
Research
Council

Acknowledgements (in random order):

- Mridula Singh (ETH Zurich)
- Patrick Leu (ETH Zurich)
- Aanjhan Ranganathan (NorthEastern)
- Boris Danev (3DB)
- David Barras (3DB)
- Nils Tippenhauer (CISPA/Helmholtz)
- Kasper Rasmussen (Oxford)
- Christina Popper (NYU AD)
- Nikos Karapanos (Futurae)
- Claudio Soriente (NEC)
- Claudio Marforio (Futurae)
- Hildur Olafsdottir