Secure Ranging (with focus on 802.15.4z)

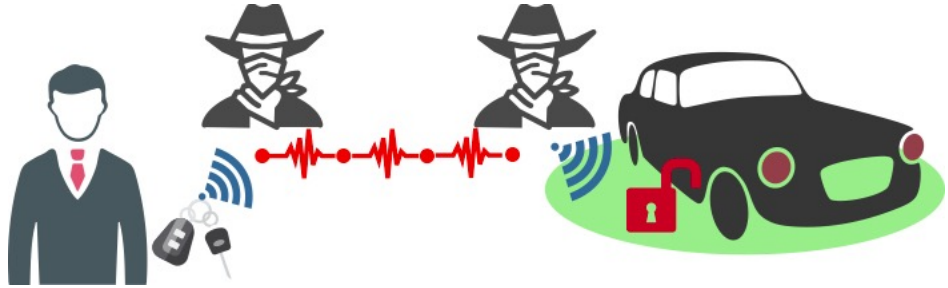
Srdjan Čapkun

ETH zürich


ring.com
21/08/2019 03:31:51 BST

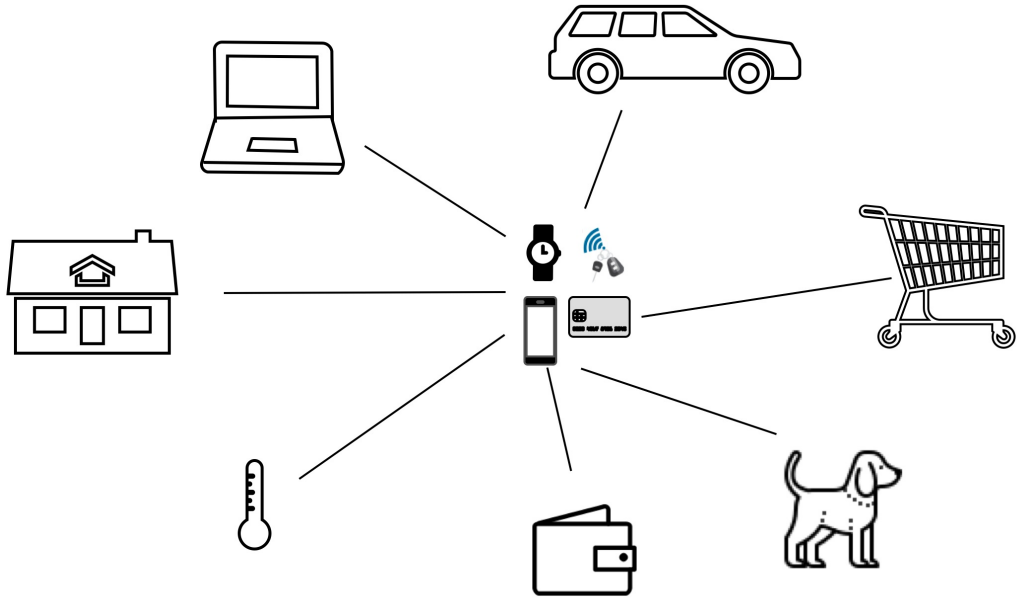
Secure Distance Measurement

Problem: prevent manipulation of measured distance.



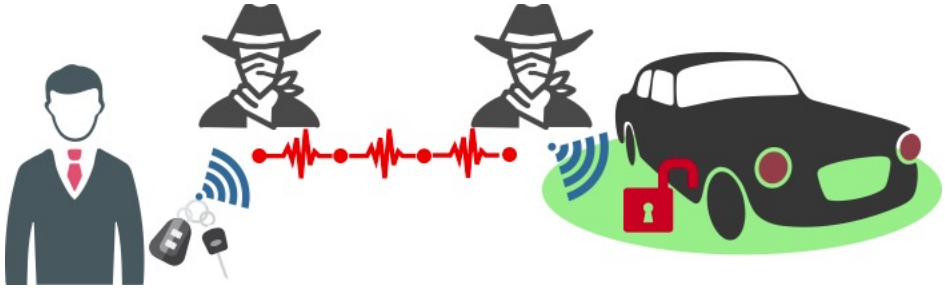
Broader Application Space:

- Access Control (e.g., PKES)
- Payments
- Tracking
- Automation



A. Francillon, B. Danev, S. Capkun
Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars, In NDSS 2011

Secure Ranging



- We need ranging that is

  (provably) secure from logical and physical layer attacks

- Security should not depend on the context or attacker abilities

- Should bind distance to identity

- Main focus: (also in 802.15.4z) prevention of distance reduction attacks

(Secure) Ranging Technologies

NON-Time-of-Flight:

- RSSI (e.g., WiFi, Bluetooth, 802.15.4, NFC / RFID) - Insecure
- Phase (multi-carrier) (e.g., Atmel AT86RF233) – Insecure
- FMCW (Frequency-Modulated Continuous-Wave) – Insecure

Time-of-Flight:

- Chirp Spread Spectrum (802.15.4 CSS, ISO/IEC 24730-5) – Insecure
- **Ultra Wide Band (UWB)** IEEE 802.15.4z – proposed for secure ranging
  https://standards.ieee.org/standard/802_15_4z-2020.html
- **WiFi** IEEE 802.11az, **5G** - first efforts to secure OFDM-based ranging

IEEE 802.15.4z: Two Modes

Low Rate Pulse (LRP) mode:

- PKES: Passive Keyless Entry and Start (VW, Daimler, …)
- Microchip (ATA8352/50), Renesas, 3dB
- Open, simple security design

High Rate Pulse (HRP) mode:

- PKES (BMW), iPhone/Airtags, Samsung/Smartags

- Apple (U1), NXP (SR040/150), Qorvo (DWM3000), 3dB (HRP+LRP, 2022)
- Closed/Proprietary security design

This Lecture

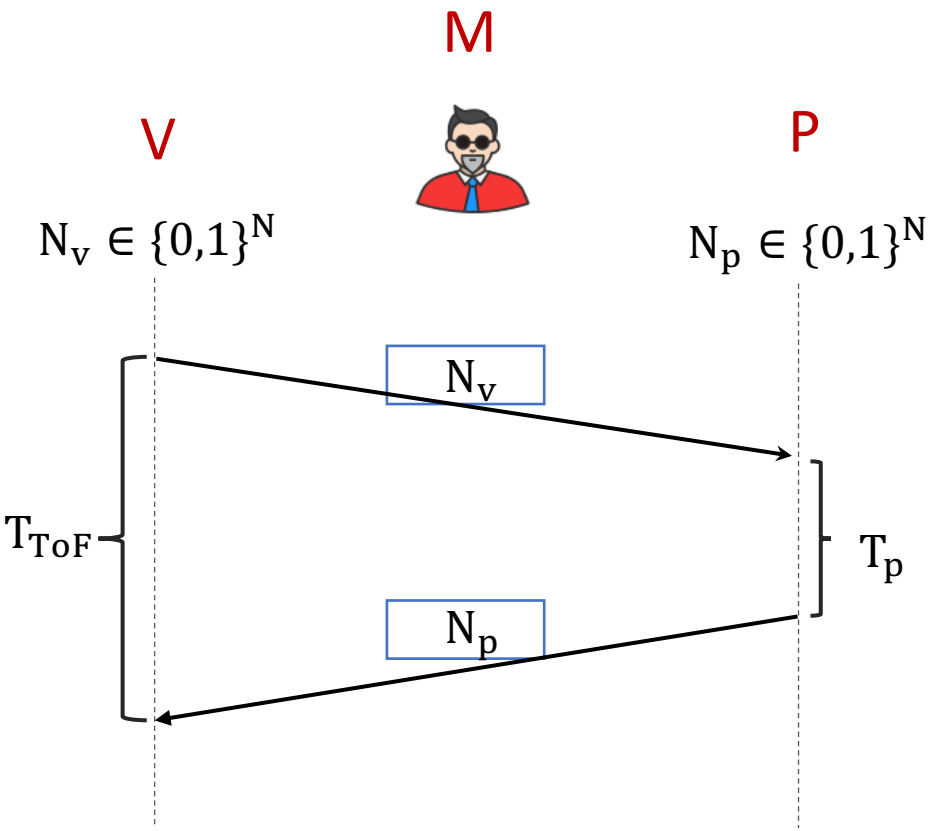
- Main Challenges in Securing (UWB) Ranging:
  - Logical and Physical Layer
  - HRP vs LRP Security Design

- Practical Distance Reduction Attacks on HRP ranging: iPhone/Airtags (U1), NXP (SR040/150), Qorvo (DWM3000)

Main Challenges in Securing (UWB) Ranging

Secure Ranging Background: Logical Layer

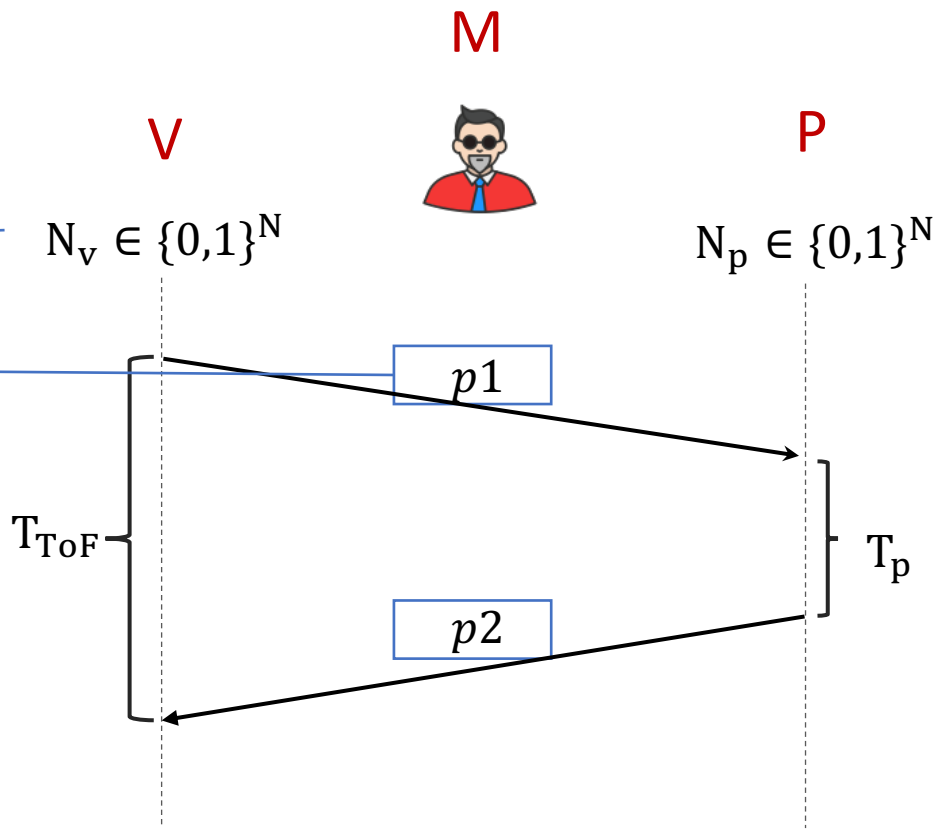
- Distance reduction prevented using challenge-response protocols with time measurements (i.e., distance-bounding)
- V and P share a secret key unknown to M
- V and P exchange messages that are (in part) unpredictable to M



Secure Ranging Background: Logical Layer

- STS cannot be predicted by M
  (before it is sent)

Figure 4: Example format of an HRP packet [4]. The lengths of the different parts and their order depend on the configuration.



Physical Layer header (PHR)
Start-of-frame delimiter (SFD)
Scrambled Timestamp Sequence (STS)

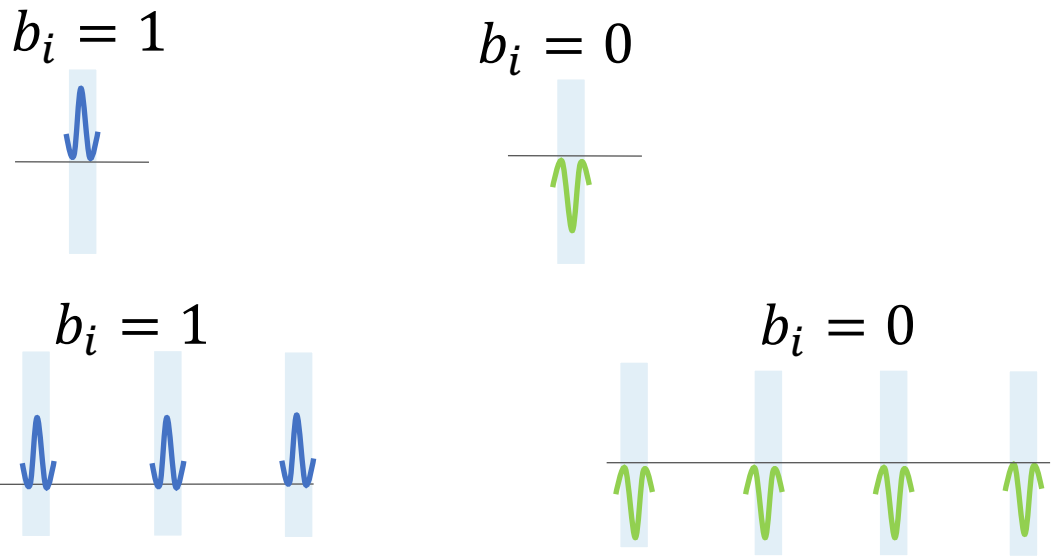
https://rfmw.em.keysight.com/wireless/helpfiles/89600b/webhelp/subsystems//hrpuwb/content/hrpuwb_fmt_tab.htm

This design prevents logical layer attacks.

But ranging also needs to be protected against physical layer attacks.

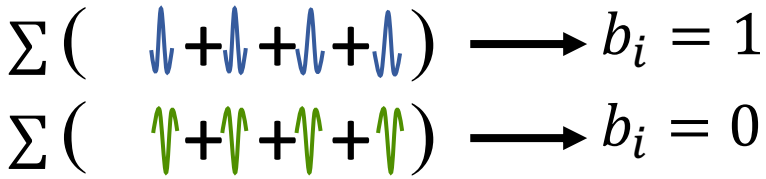
UWB Symbols (example)

Bit represented by one UWB pulse



Bit represented by multiple UWB pulses.

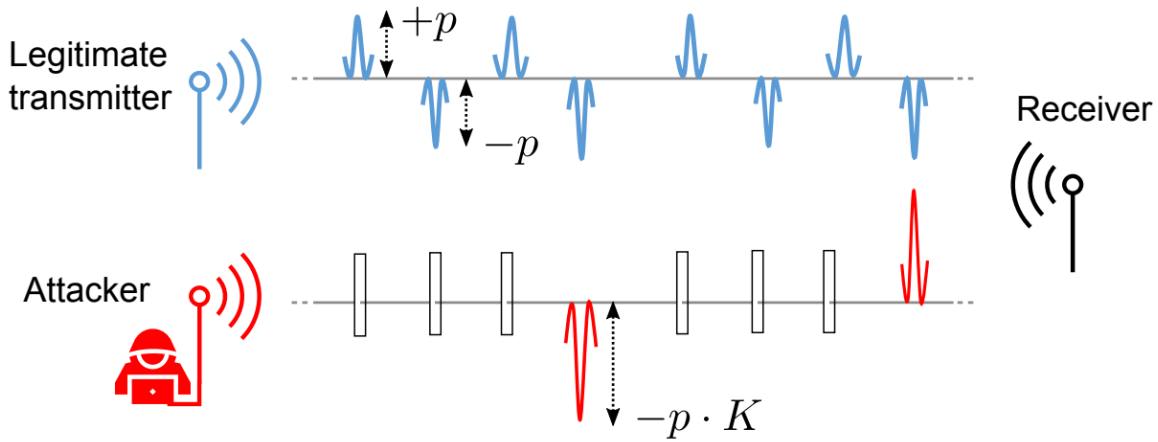
Example Demodulation



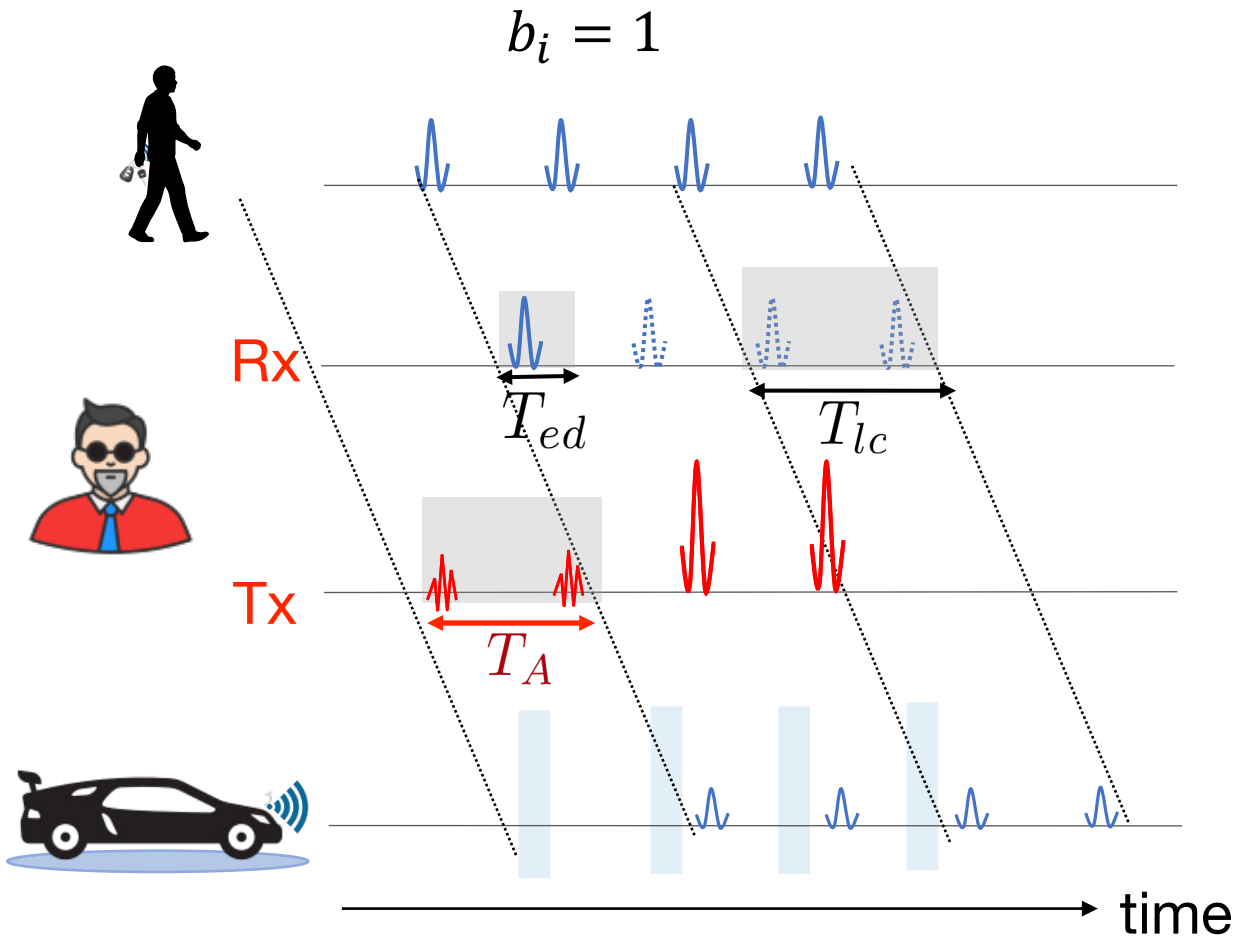
Longer symbols increase the range and robustness to noise and multipath.

UWB Security: Attacks on ToA Estimation

- Early Detect / Late Commit
- Cicada
- Cicada+
- Adaptive Injection
- Ghost Peak
- …?



Problem: Distance Shortening Attacks



Steps to insert an earlier path

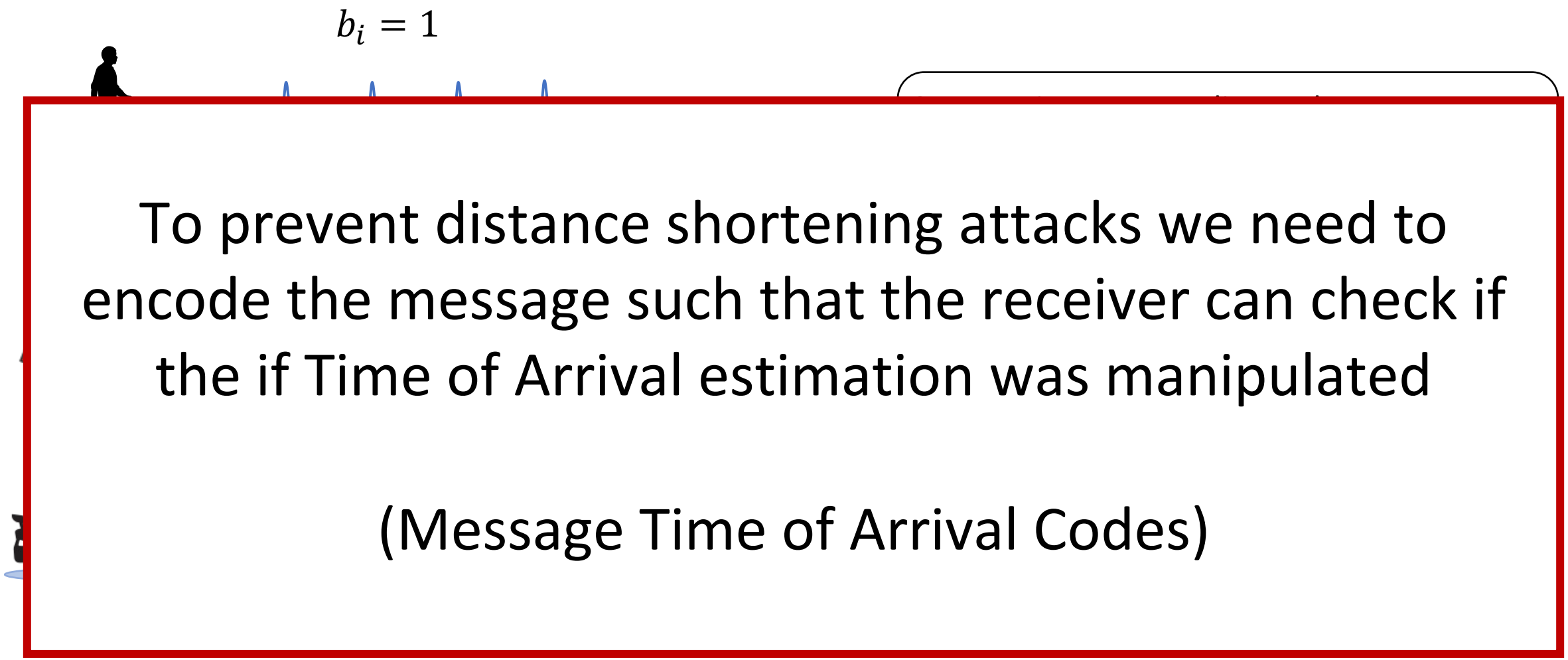
- Send noise in time $\mathbf{T_A}$
- Learn shape of the symbol in time $\mathbf{T_{ed}}$
- Commit correct symbol in time $\mathbf{T_{lc}}$

Σ(+ + +) → $b_i = 1$ Correct Bit

Early-detect/late-commit (ED/LC) Attack

"So near and yet so far: Distance-bounding attacks in wireless networks," in European Workshop on Security in Ad-hoc and Sensor Networks, 2006

Problem: Distance Shortening Attacks

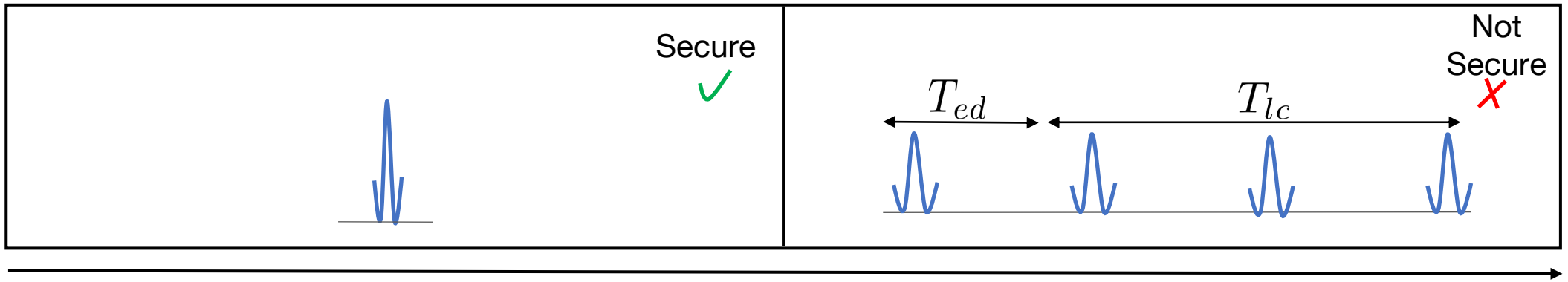


To prevent distance shortening attacks we need to encode the message such that the receiver can check if the if Time of Arrival estimation was manipulated

(Message Time of Arrival Codes)

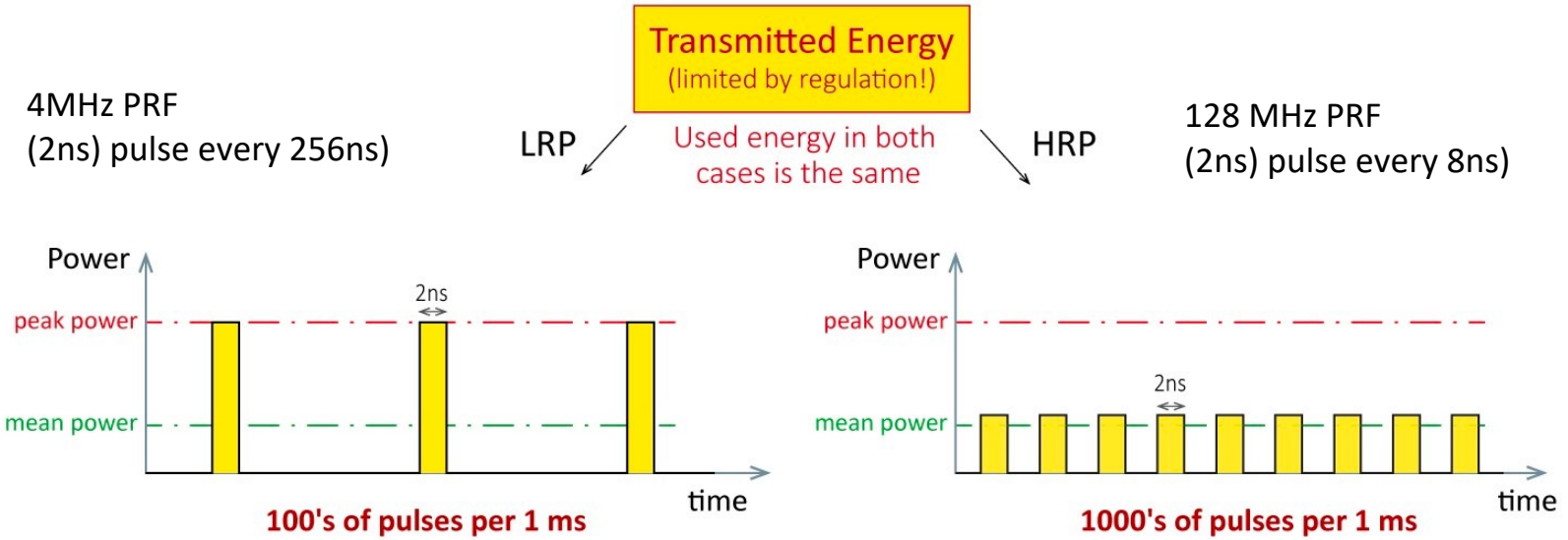
Early-detect/late-commit (ED/LC) Attack

Performance/Security Tradeoff?



802.15.4z was introduced in 2020 to enable secure ranging while providing both performance and robustness to attacks. **Does 4z protect Time of Arrival?**

IEEE 802.15.4z: LRP and HRP mode



- 1-2ns wide pulses
- > 500MHz bandwidth
- Frequencies 6-9GHz
- Power spectral density < −41.3 dBm/MHz avg. over $1ms$
- Power in 50 MHz bandwidth around peak frequency limited to 0 dBm

Low Rate Pulse (LRP)

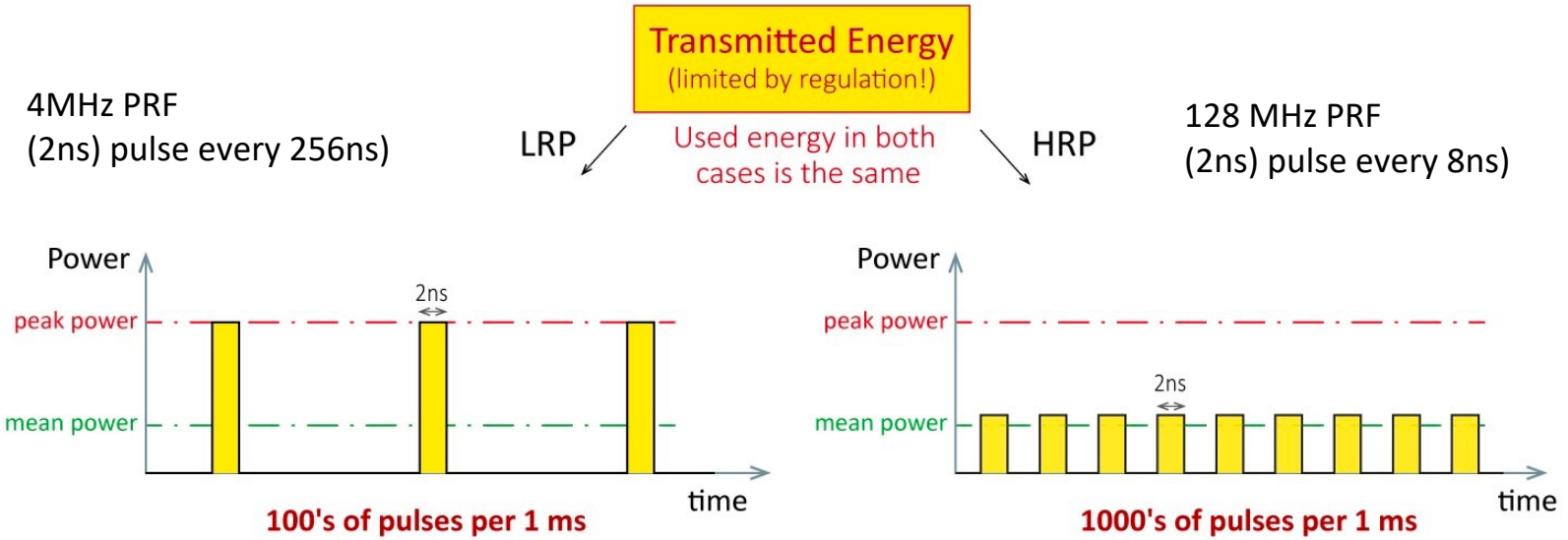
- Modulation: Binary Frequency Shift Keying (BFSK)
- Single ranging requires few (e.g. 100) pulses
- Bit represented by single or multiple pulses
- Non-coherent
- More power efficient than HRP

High Rate Pulse (HRP)

- Modulation: BPSK (secure ranging) and BPM+BPSK (data)
- Single ranging requires 1000s to 10000s pulses
- Each bit represented by multiple pulses
- Cannot use single pulse mode (energy too low)
- Coherent

Security of 802.15.4z LRP Mode

LRP vs HRP



- 1-2ns wide pulses
- > 500MHz bandwidth
- Frequencies 6-9GHz
- Power spectral density < −41.3 dBm/MHz avg. over $1ms$
- Power in 50 MHz bandwidth around peak frequency limited to 0 dBm

Low Rate Pulse (LRP)

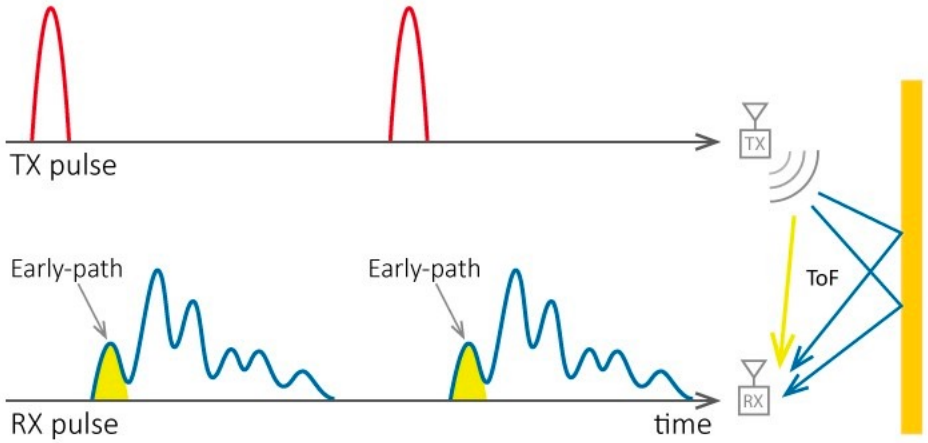
- Modulation: Binary Frequency Shift Keying (BFSK)
- Single ranging requires few (e.g. 100) pulses
- Bit represented by single or multiple pulses
- Non-coherent
- More power efficient than HRP

High Rate Pulse (HRP)

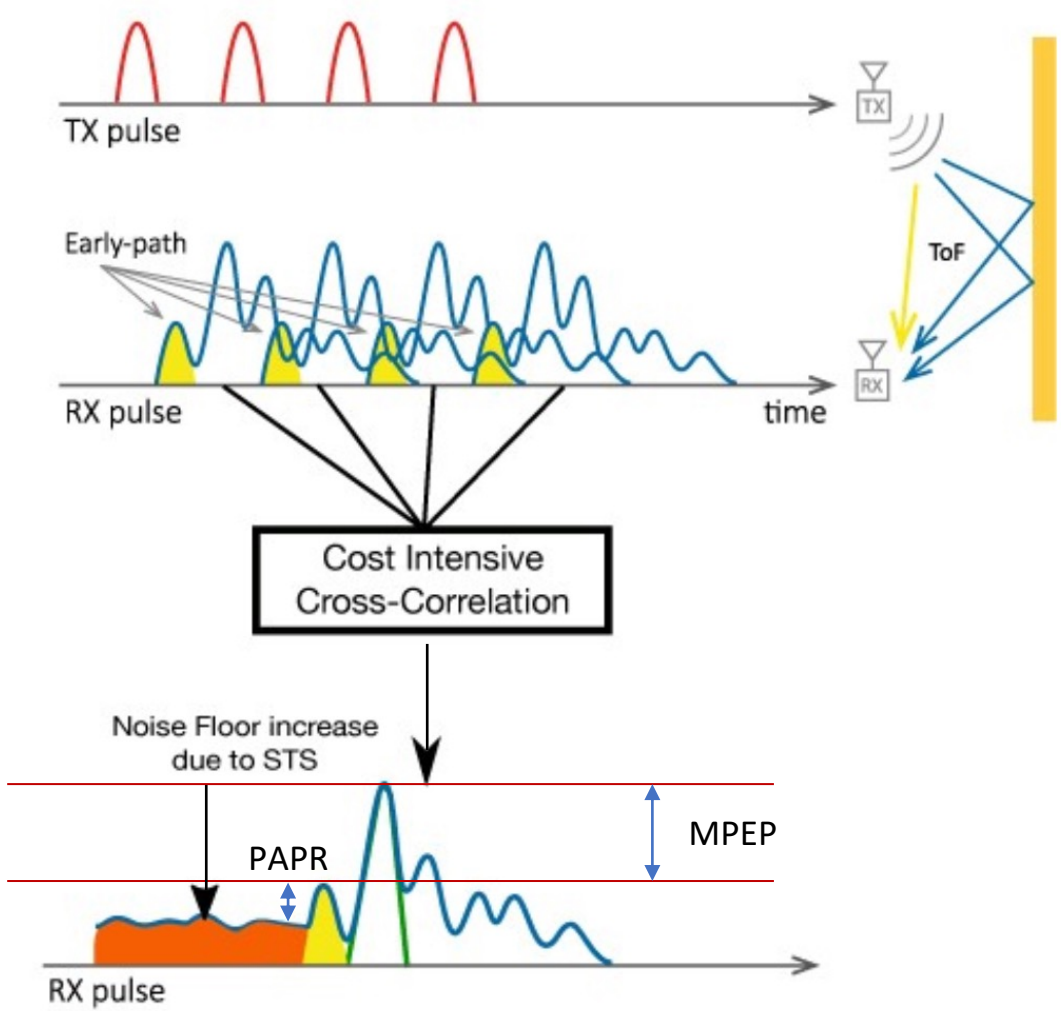
- Modulation: BPSK (secure ranging) and BPM+BPSK (data)
- Single ranging requires 1000s to 10000s pulses
- Each bit represented by multiple pulses
- Cannot use single pulse mode (energy too low)
- Coherent

LRP vs HRP

LRP 4MHz PRF (1 (2ns) pulse every 256ns)



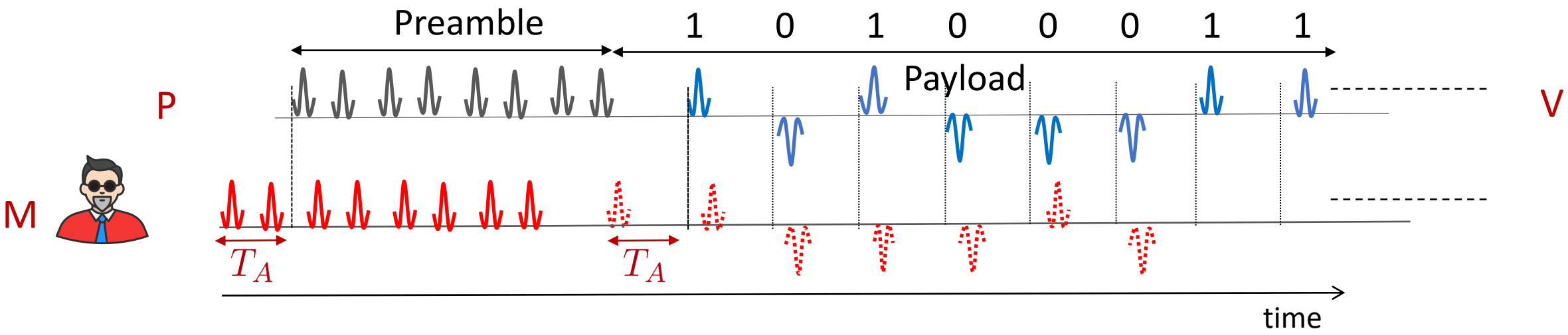
HRP STS 128 MHz PRF (1 (2ns) pulse every 8ns)



In LRP pulses are stronger than in HRP

In LRP pulses are spaced more apart and less susceptible to inter-pulse-interference
=> Less noise => better reliability and security

LRP Security: Single-Pulse Per Bit Secure Ranging

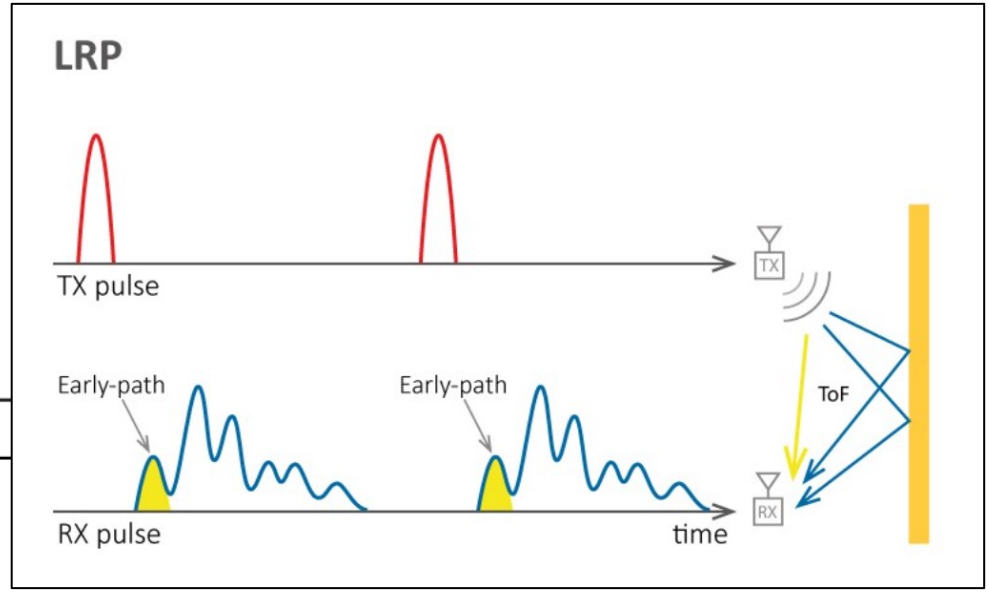


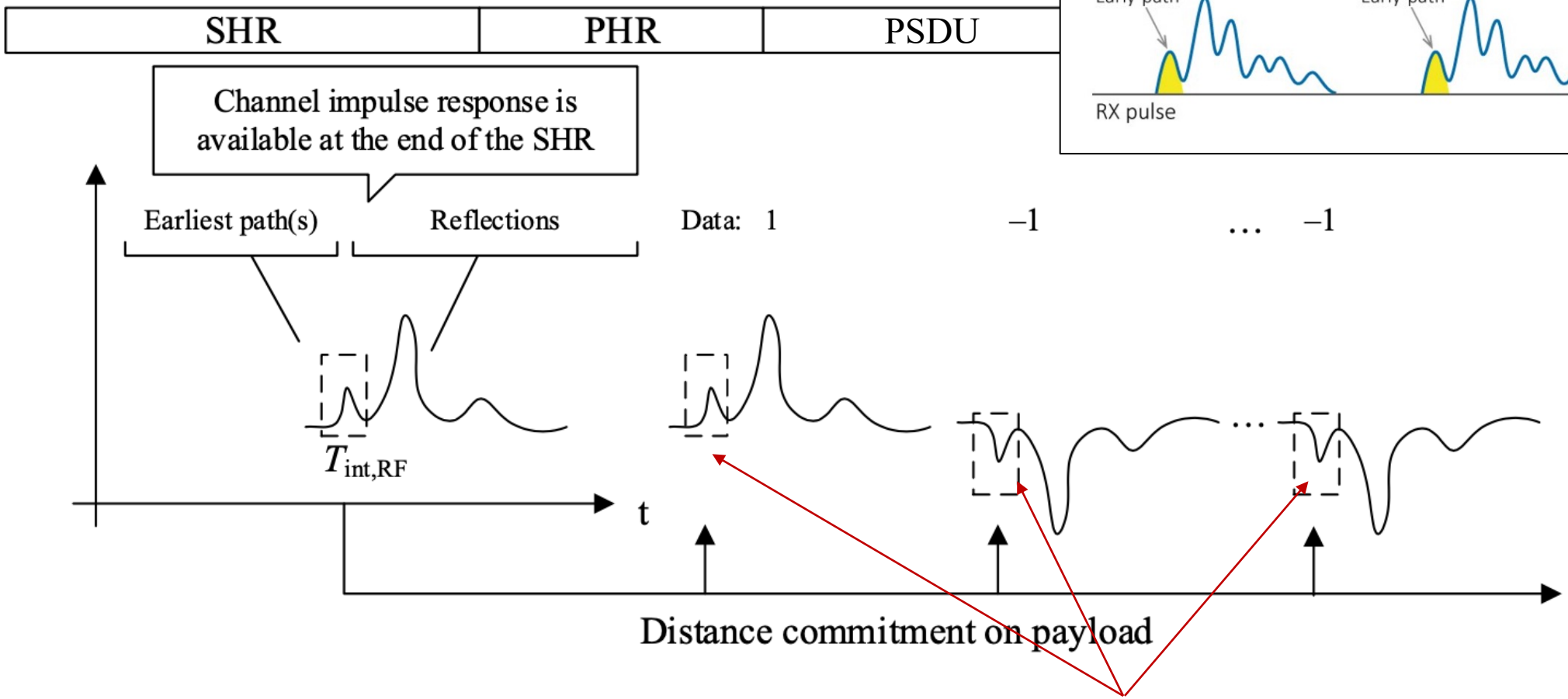
Step 1. ToA measured over a public preamble (distance commitment)

Step 2. ToA verified over random payload bits (receiver decodes each pulse into one bit), attacker needs to guess every pulse/bit.

N. Tippenhauer, H. Luecken, M. Kuhn, S. Capkun, ***UWB Rapid-Bit-Exchange System for Distance Bounding,***
ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), 2015

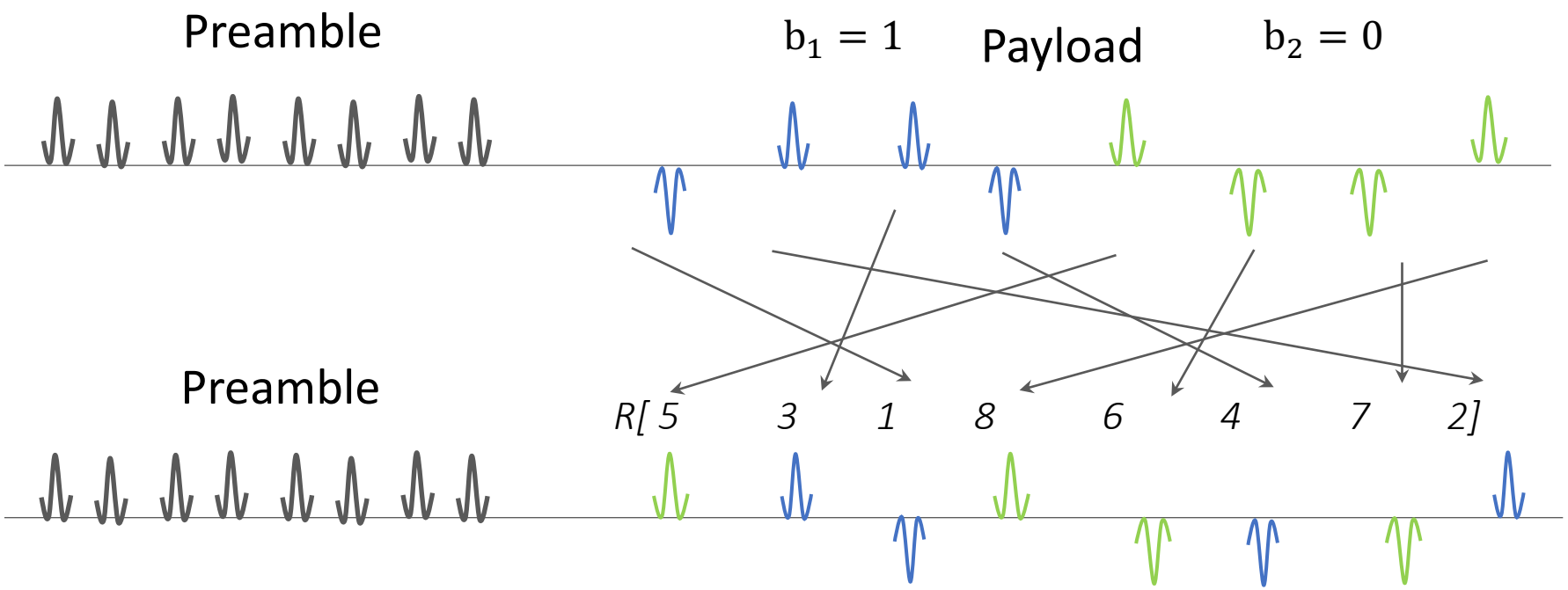
LRP Security





Attacker needs to create a correct pulse polarity at each of these point in time. i.e., attacker needs to guess.

LRP Security: Multi-Pulse Per Bit Secure Ranging



- For cases where individual pulses not visible to receiver
- UWB with Pulse Reordering (UWB-PR):
  shape, start/end time of symbols is unpredictable => robusness to attacks

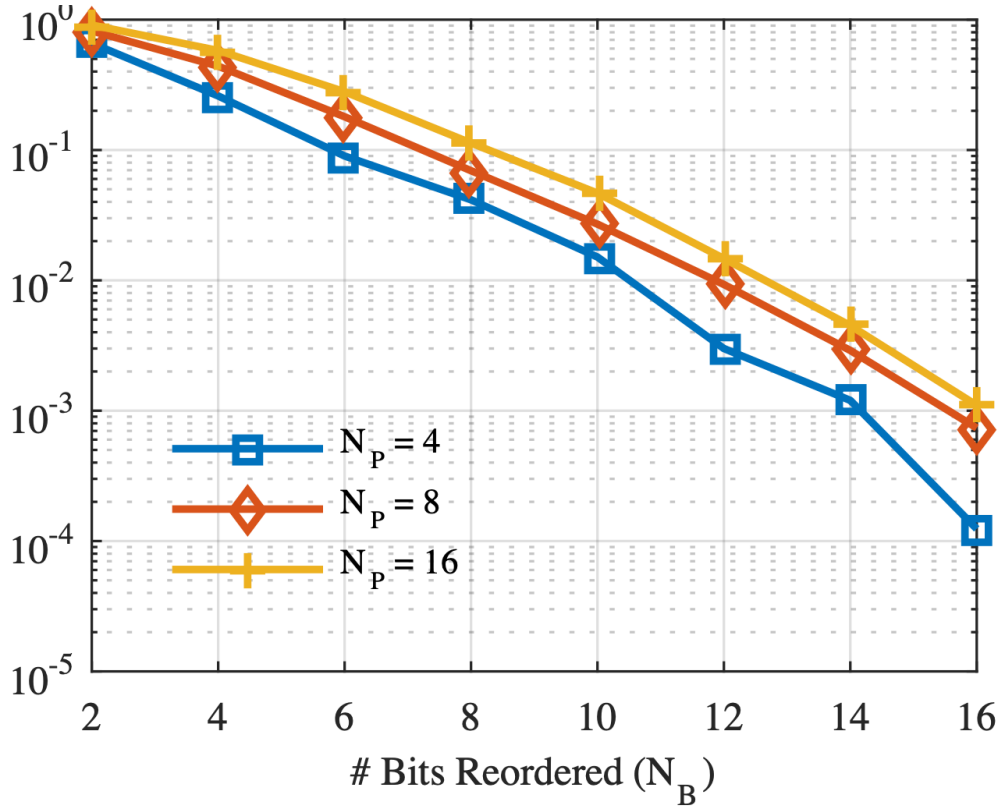
M. Singh, P. Leu, S. Capkun, ***UWB with Pulse Reordering: Securing Ranging against Relay and Physical Layer Attacks,***
in Proceedings of the Network and Distributed System Security Symposium (NDSS), 2019

LRP Security: Probability of Attacker Success

- Single-Pulse per bit
  Probability of attacker's success: $2^{-|payload|}$ (2^{-32}, 2^{-64}, 2^{-128}, …)

- Multi-Pulse per bit
  (LRP with Pulse Reordering) →

- *LRP is open, simple and comes with explicit security guarantees.*



=>

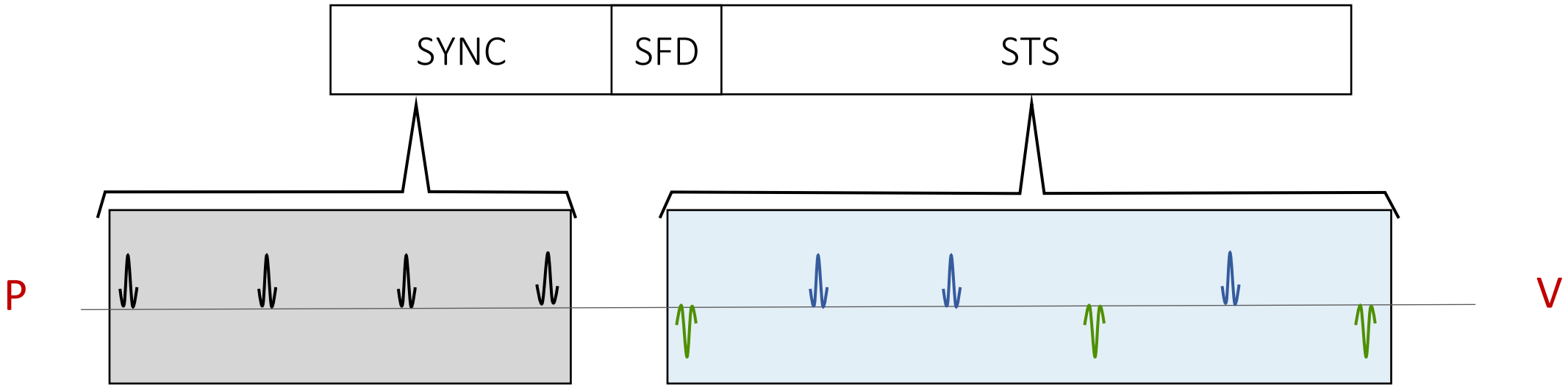
In LRP receivers can decode individual pulses

(|secure payload| = 32,64,128,… pulses; 1 pulse per bit)

In HRP receivers **cannot** decode individual pulses

(STS is 4092 pulses long, bits(?))

HRP Security: Scrambled Timestamp Sequence



public preamble

Scrambled Timestamp Sequence: random pulses
(known to P and V, hard to predict for M)

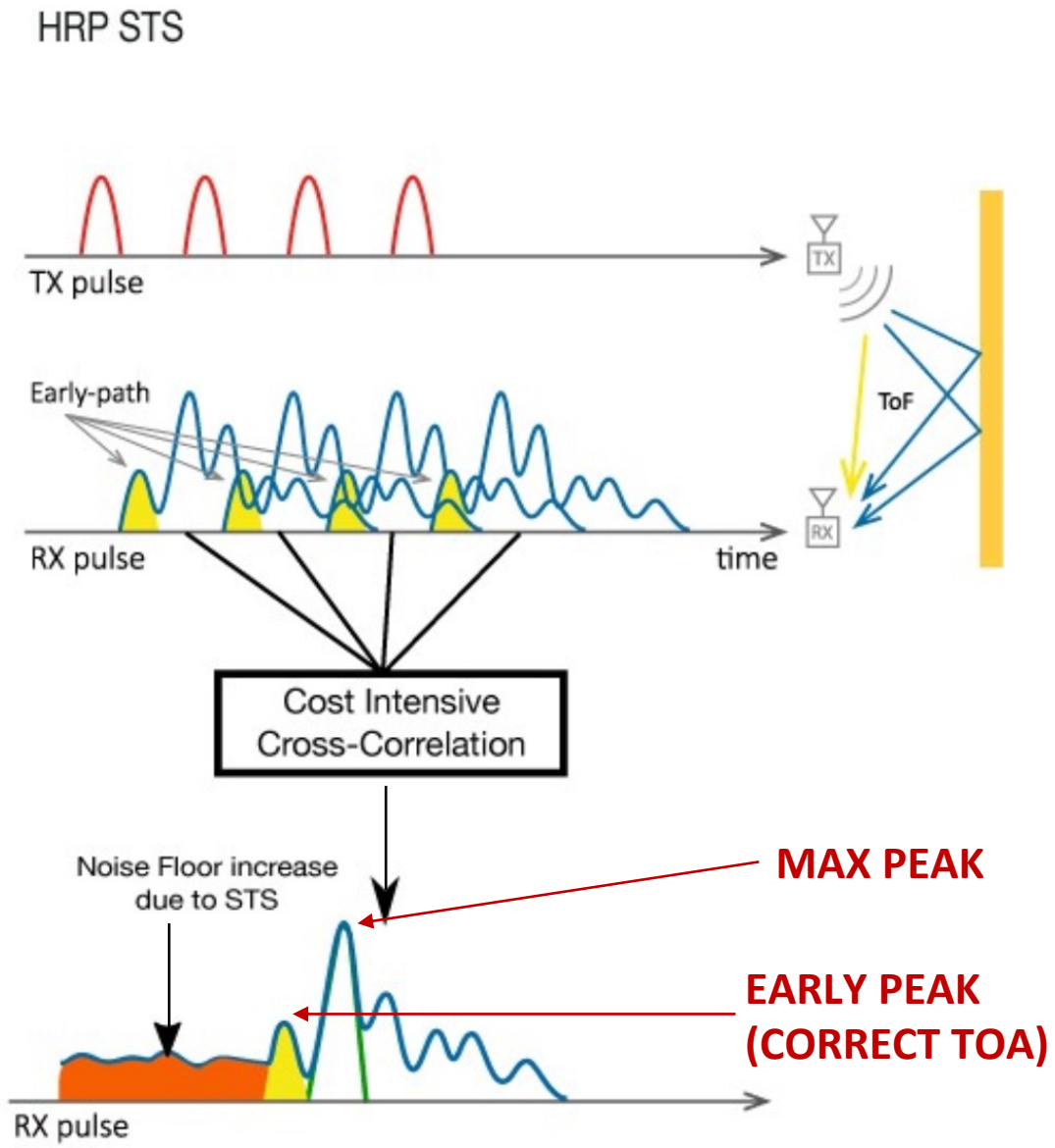
Receiver correlates the received STS with the local STS copy.
Autocorrelation peak determines the Time of Arrival.

https://www.ieee802.org/15/pub/TG4z.html

HRP Security: Time of Arrival Estimation

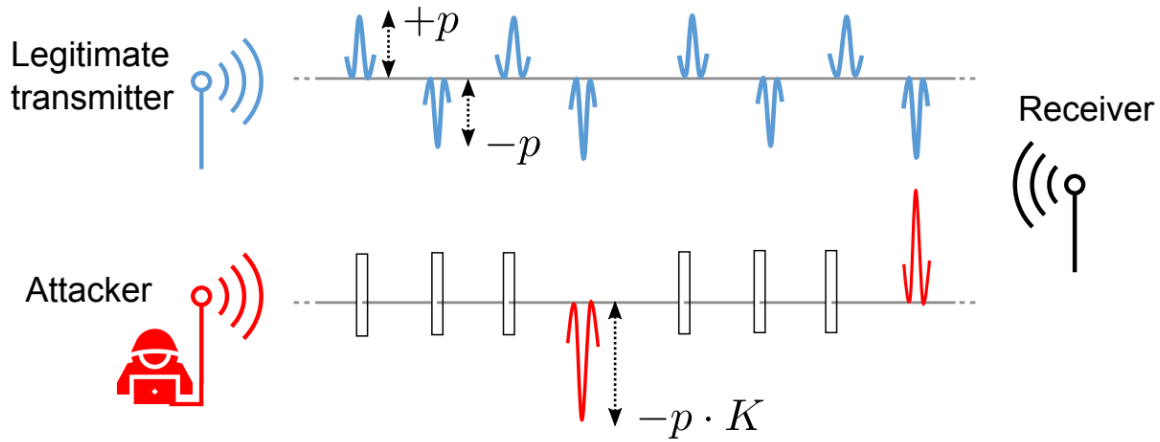
- Max autocorrelation peak is not the correct ToA
- Receivers look for Early Path (leading edge / correct ToA)
- How to identify Early Path? How weaker than Max Peak and stronger than Avg Noise should it be?

Reliability / Security Tradeoff?



HRP Security: Attacks on ToA Estimation

- Early Detect / Late Commit
- Cicada
- Cicada+
- Adaptive Injection
- Ghost Peak
- …?



Goal of the attacker:
create a FAKE EARLY PEAK despite not knowing STS
(remember: receiver doesn't 'see' individual pulses)

HRP Security: Attacks on ToA Estimation

- Ghost-Peak Attack shows that physical-layer attacks on HRP are a real threat.
- Apple/NXP/Qorvo use hidden ToA estimation algorithms making it hard to evaluate if their HRP ranging systems are truly secure. These algorithms should be public and comprehensively evaluated.
- Like with ciphers/signatures/MACs security should rely only on the unpredictability of the STS, not on the secrecy of the algorithms.

HRP Security: How To Move Forward?

- Using autocorrelation for secure ToA estimation is not well understood.

- Currently, we cannot fully answer the following questions:
  "If STS is 4092 pulses long, what is the probability that the attacker creates a fake early path (i.e., reduces the distance)?"
  How many bits of security does a 4092 pulse long STS provide?

- Initial analysis can be found in:

P. Leu, M. Singh, M. Roeschlin, K. Paterson, S. Čapkun
***Message Time of Arrival Codes: A Fundamental Primitive for Secure Distance Measurement**, in IEEE Symposium on Security and Privacy (S&P), 2020*

M. Singh, M. Röschlin, E. Zalzala, P. Leu, S. Čapkun
Security Analysis of IEEE 802.15.4z/HRP UWB Time-of-Flight
In ACM WiSec 2021

Ghost-Peak: Practical Distance Reduction Attacks on HRP UWB Ranging

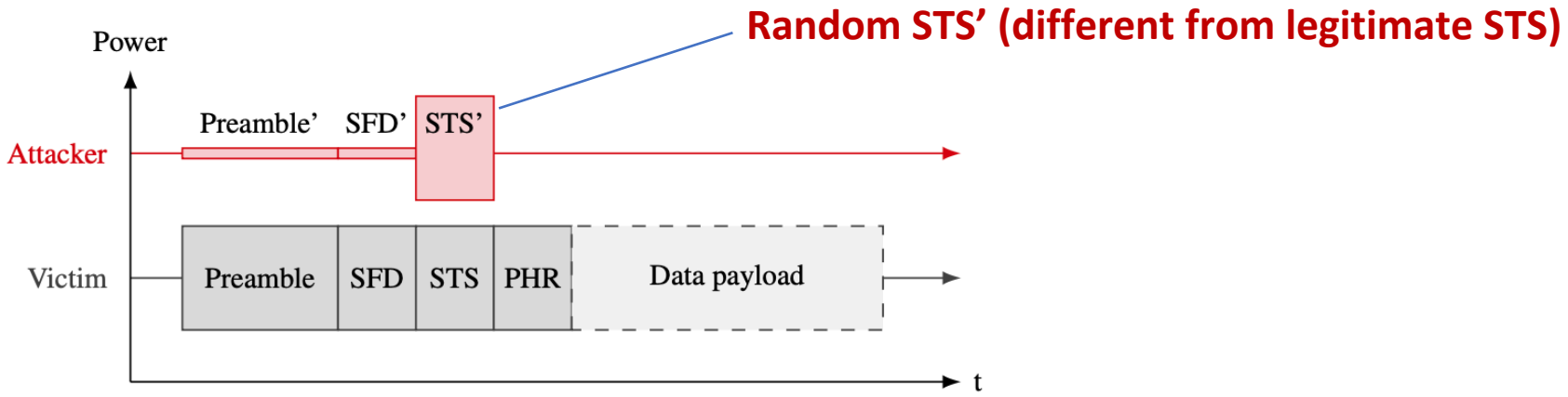
Patrick Leu[1],*, Giovanni Camurati[1],*, Alexander Heinrich[2], Marc Roeschlin[1], Claudio Anliker[1], Mathias Hollick[2], Srdjan Čapkun[1], and Jiska Classen[2]

[2] SEEMOO SECURE MOBILE NETWORKING
TECHNISCHE UNIVERSITÄT DARMSTADT

[1] ETH zürich

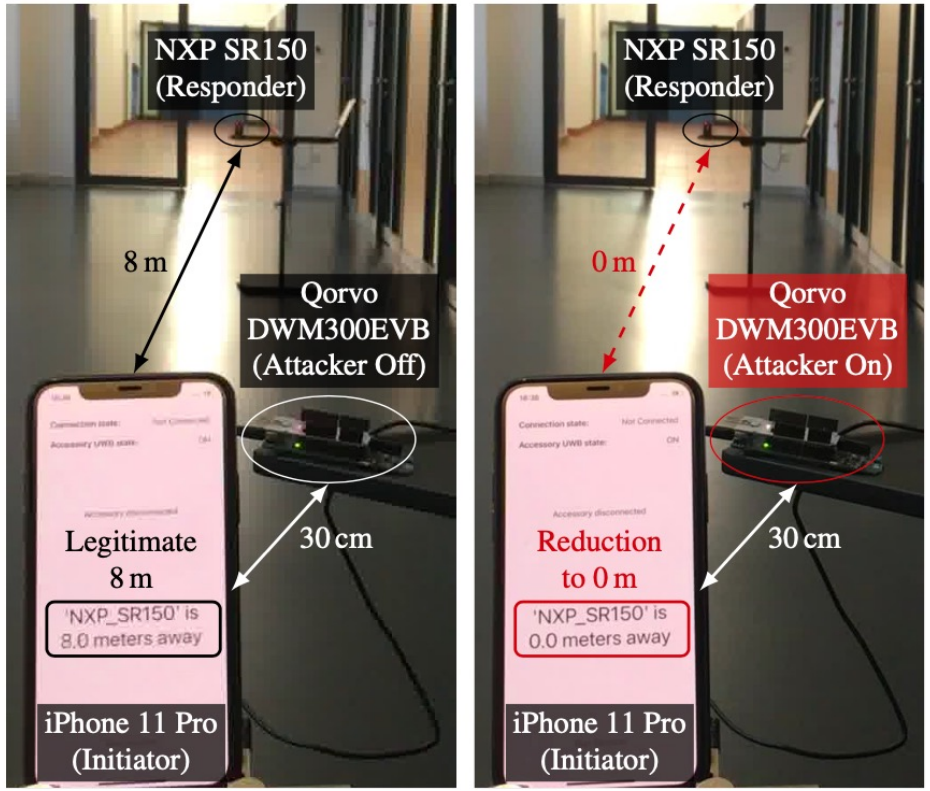
www.securepositioning.com/ghost-peak

HRP Security: Ghost Peak Attacks

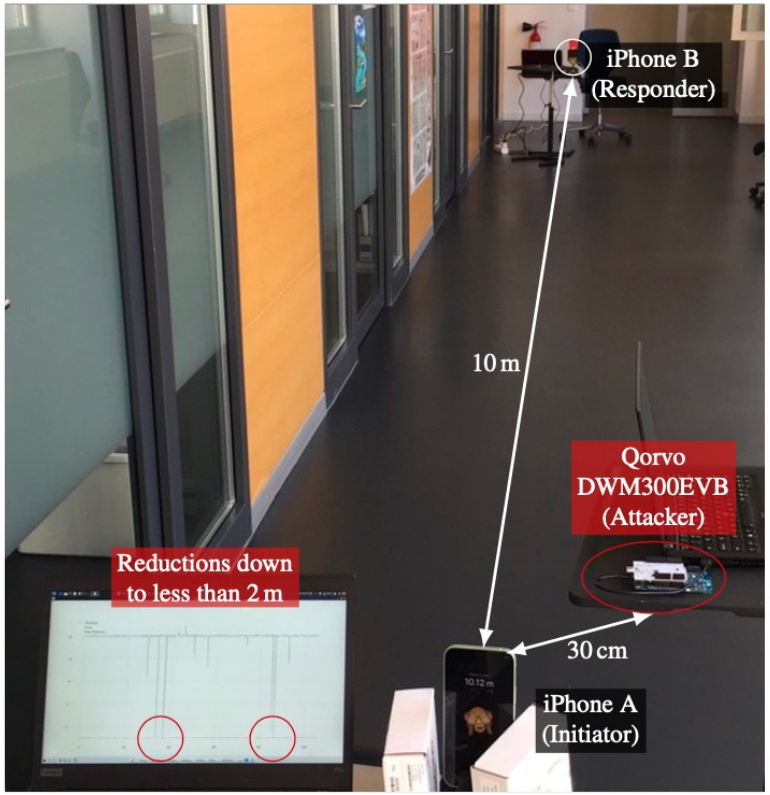


- **Main idea:** inject a packet in-synch (µs) with legitimate transmission, but with varying power of Preamble', SFD', STS' (randomly generated)
- **Attack assumptions:**
  - No knowledge of keys shared between victim devices
  - No ability to predict scrambled timing sequence (STS)
- **Attack setup:** inexpensive (USD 65) commercial off-the-shelf device

HRP Security: Ghost Peak Attacks



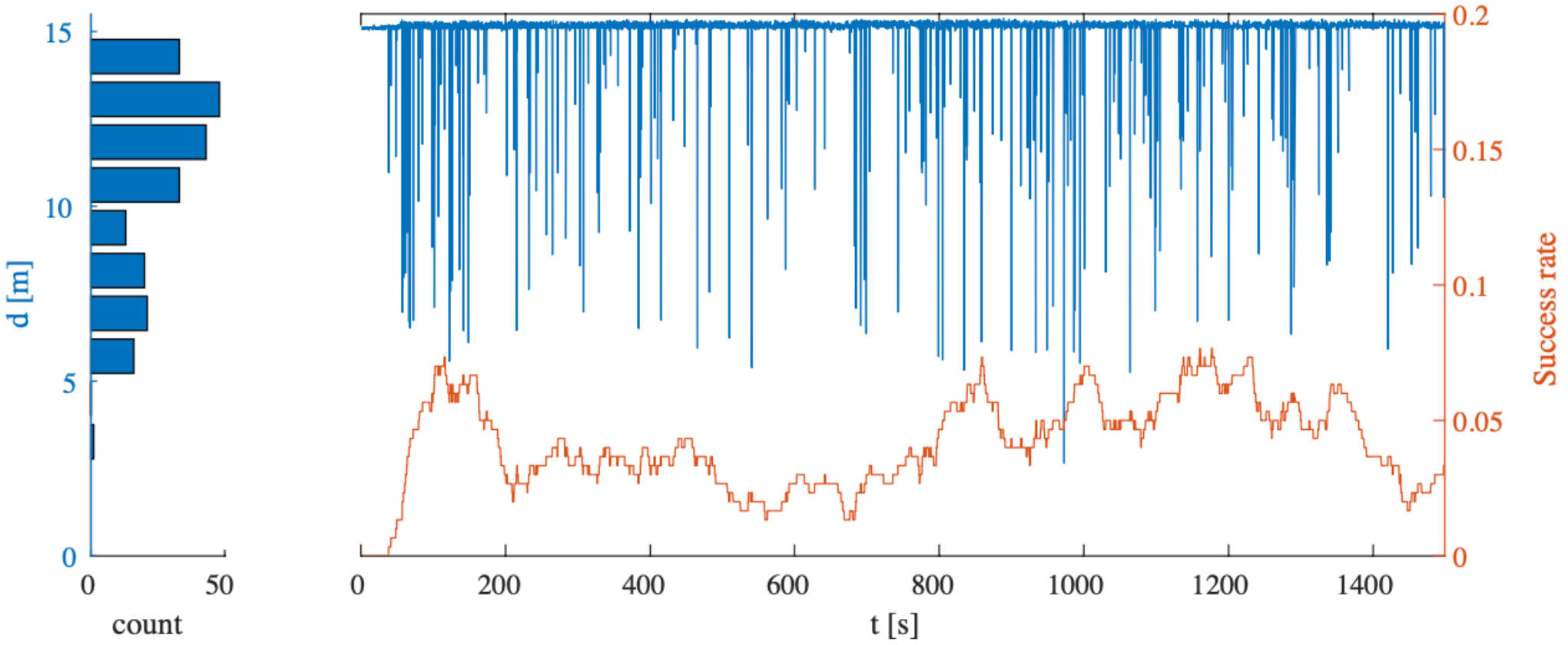
(a) iPhone (initiator, victim) + NXP SR150 (responder): reduction from 8 m to 0 m visible on the screen of the iPhone.



(b) iPhone + iPhone: reduction from 10 m to less than 2 m visible in the raw measurements logs.

Figure 9: Two concrete examples of distance reduction attacks.

HRP Security: Ghost Peak Attacks

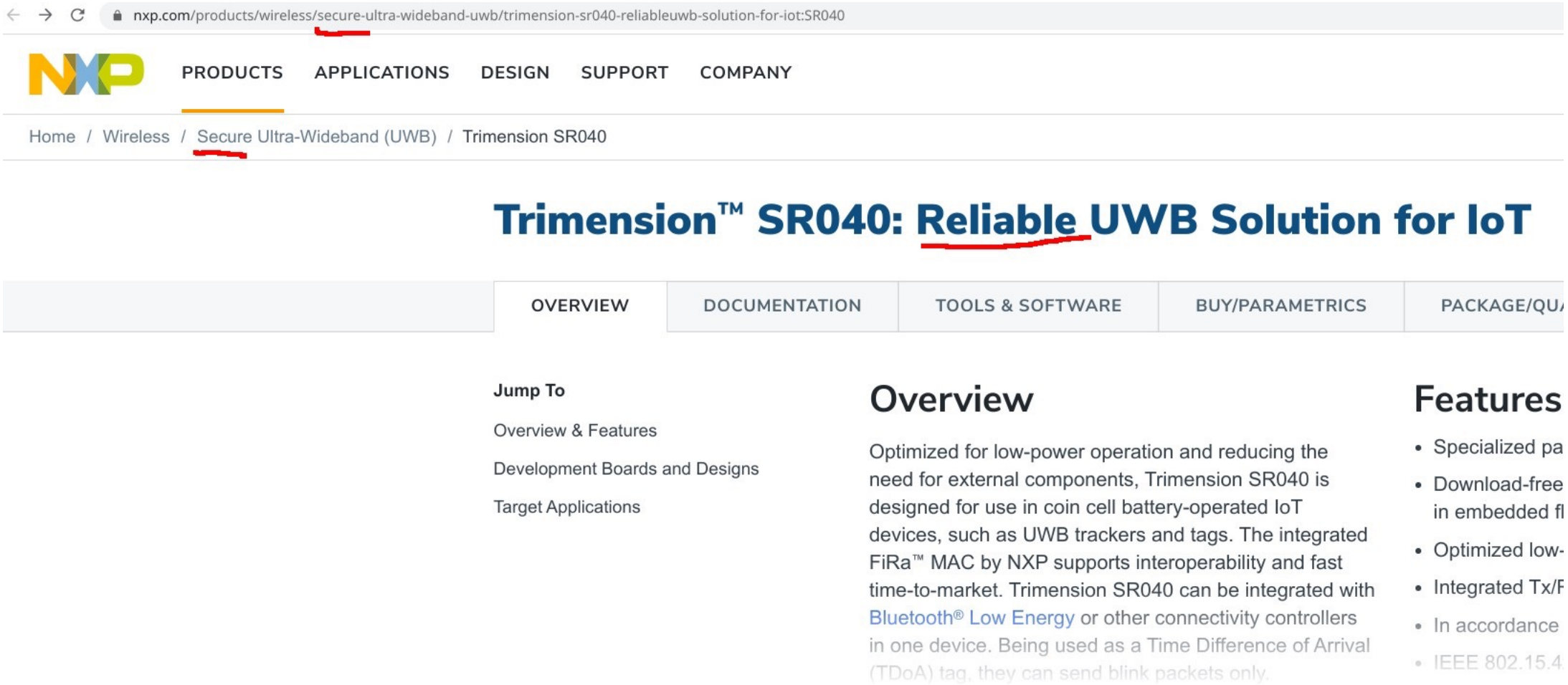


HRP Security: Ghost Peak Attacks

Table 2: Overview of attack scenarios and results.

Scenario	Primary Victim (V1)	Secondary Victim (V2)	Maximum Reduction	Success Rate
Handoff Music	iPhone (Apple U1)	HomePod mini (Apple U1)	9.01 m	2.10 %
Nearby Interaction	iPhone (Apple U1)	iPhone (Apple U1)	12.45 m	4.08 %
AirTag	AirTag (Apple U1)	iPhone (Apple U1)	9.09 m	4.25 %
NXP Initiator	iPhone (Apple U1)	Tag (NXP SR040)	4.80 m	1.87 %
NXP Responder	iPhone (Apple U1)	Tag (NXP SR150)	9.68 m	2.15 %
Qorvo	iPhone (Apple U1)	Tag (Qorvo DWM3000)	8.13 m	3.09 %

HRP Security: Ghost Peak Attacks



Conclusion

Conclusion

- UWB provides a strong basis for secure ranging. No other radio technology is likely to provide stronger guarantees.

- 802.15.4z HRP:
  - HRP security algorithms used by Apple/NXP/Qorvo are not public
  - Autocorrelation seems used for (secure) ToA estimation: this is not well understood
  - More transparency needed: Ghost Peak attack show that physical layer attacks on HRP are possible and need to be addressed.

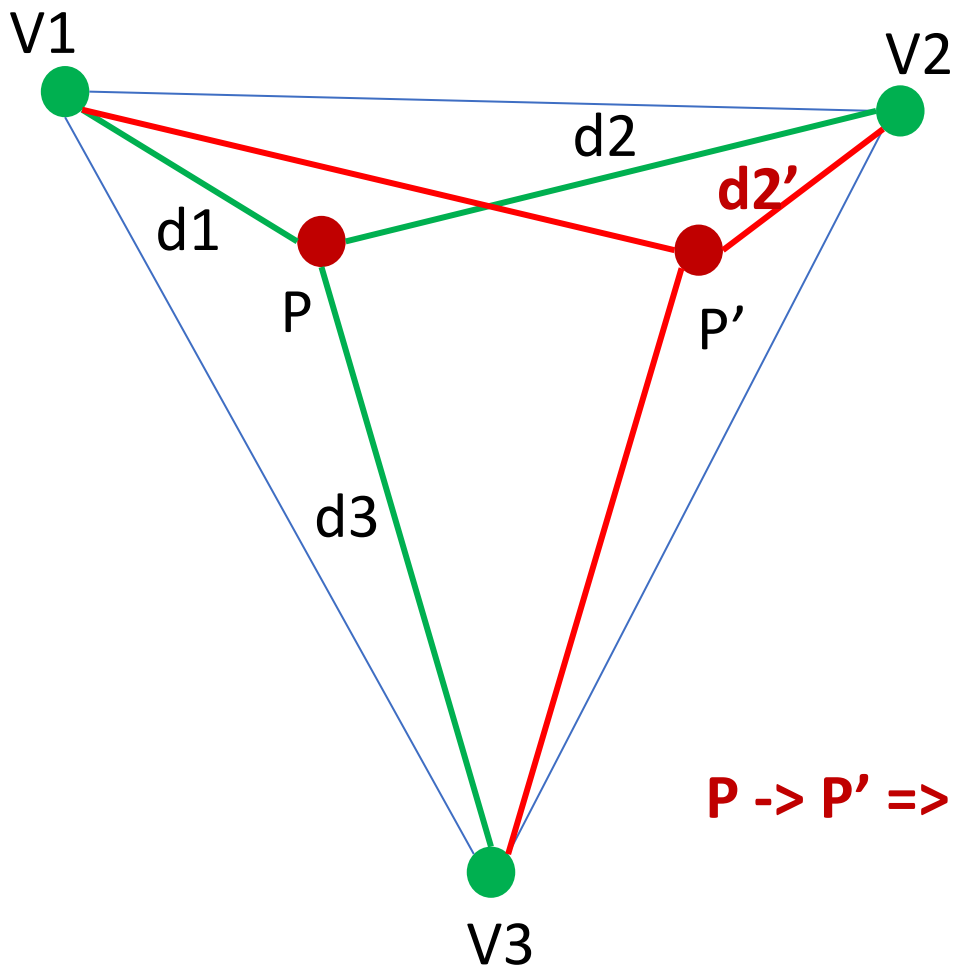
- 802.15.4z LRP:
  - Security design is open and simple.
  - Does not seem to suffer from the same issues like HRP.

Secure Positioning

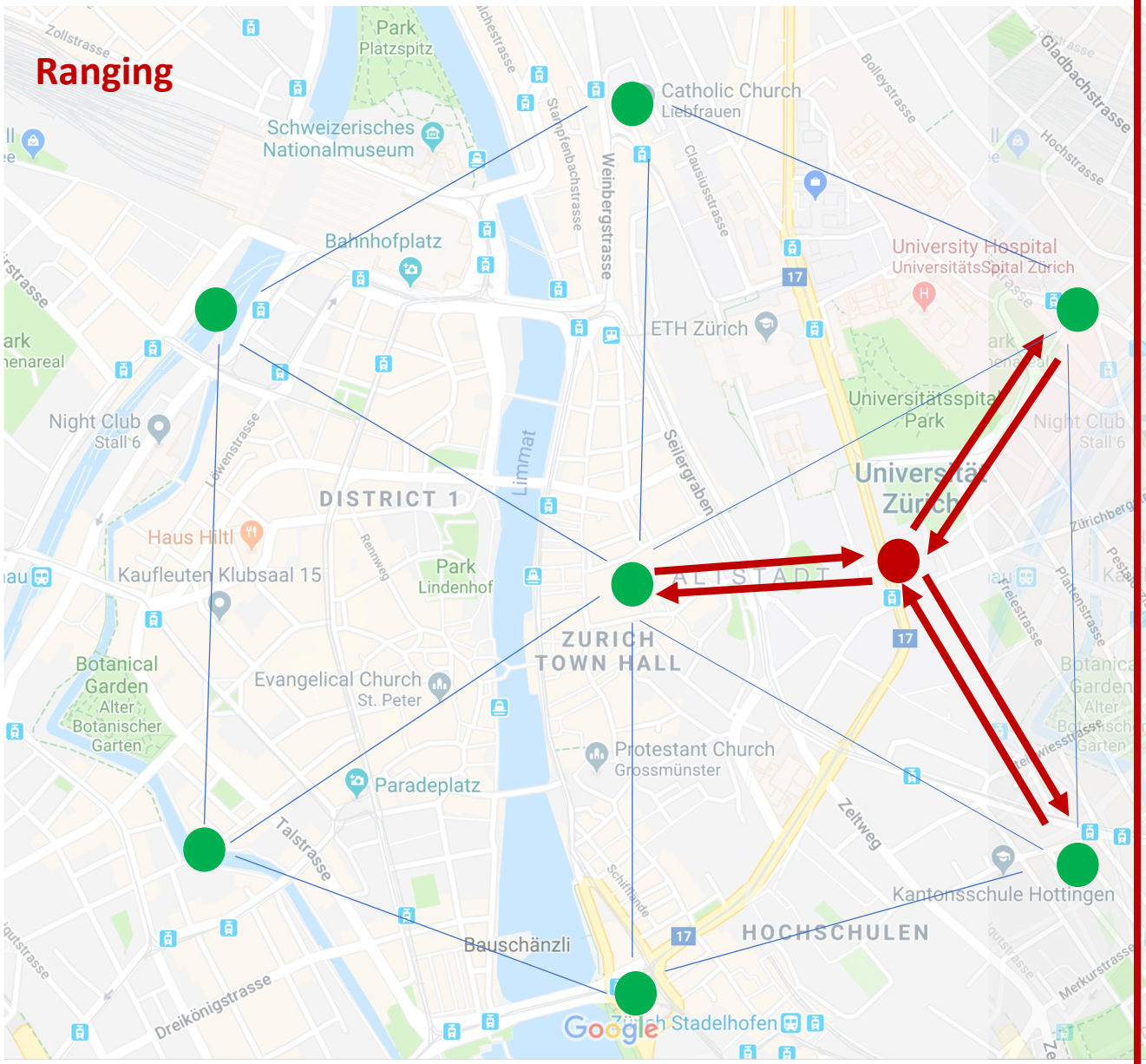
Bi-Directional Ranging and Verifiable Multilateration

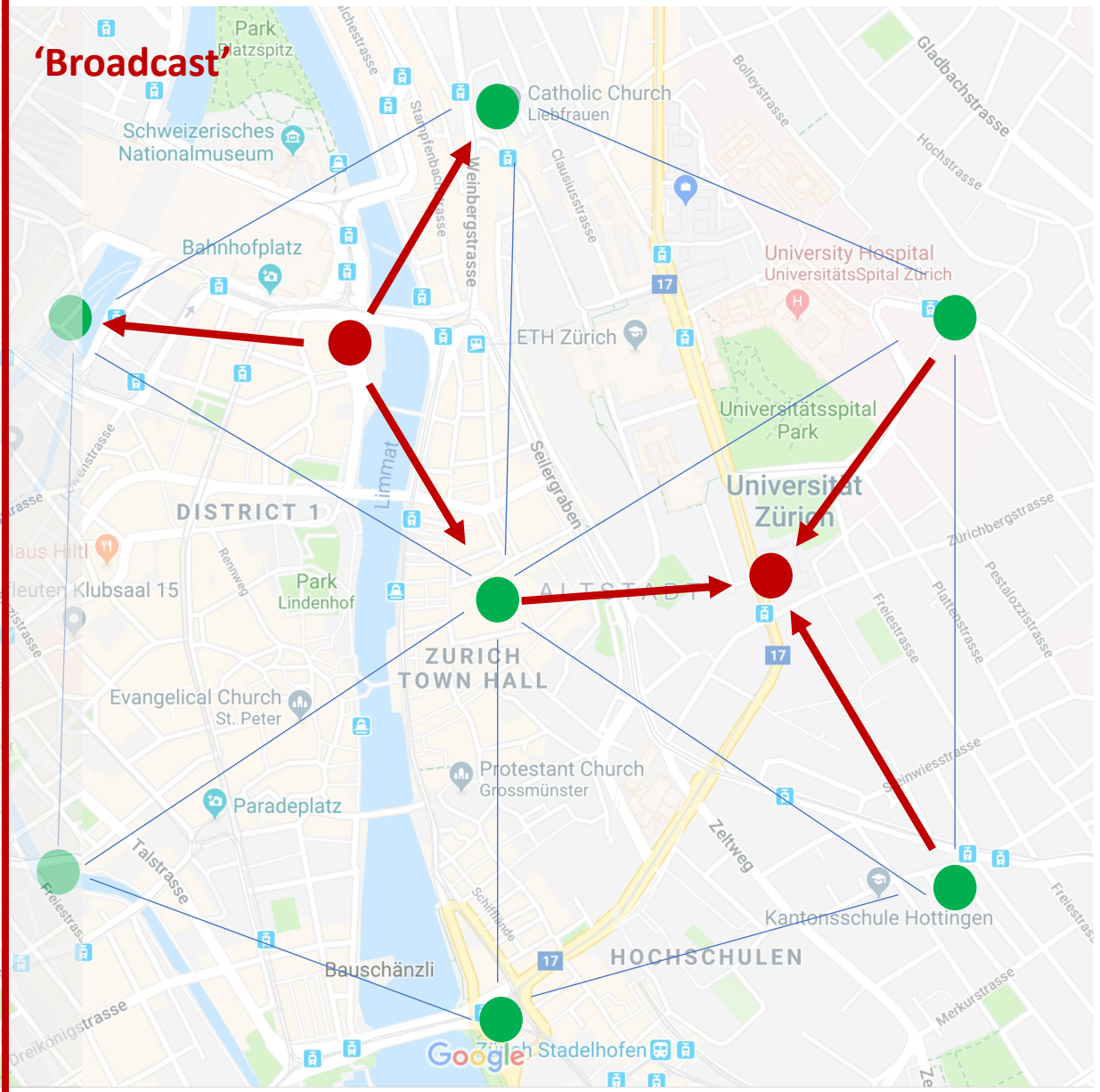
- Bi-Directional ranging offers hope.
- Round-trip Time-of-Flight Protocols can *prevent distance shortening attacks.*

- If distance shortening is prevented, we can build a secure positioning system based on *Verifiable Multilateration within verification triangles.*



Securing Positioning with Secure Ranging





Replay / Relays on Broadcast Techniques

Broadcast techniques are subject relay/replay/delay-based spoofing attacks.

Hard to fully prevent.

Relay/replay attacks on GNSS signals

Authors: Malte Lenhart, Marco Spanghero, Panagiotis Papadimitratos Au

…on Security and Privacy in Wireless
…48300.3468256

Investigation of Multi-device Location Spoofing Attacks on Air Traffic Control and Possible Countermeasures

Daniel Moser
Dept. of Computer Science
ETH Zürich, Switzerland

Patrick Leu
Dept. of Computer Science
ETH Zürich, Switzerland

Vincent Lenders
armasuisse
Thun, Switzerland

Aanjhan Ranganathan
Dept. of Computer Science
ETH Zürich, Switzerland

Fabio Ricciato
Faculty of Computer and Information Science
University Ljubljana, Slovenia

Srdjan Capkun
Dept. of Computer Science
ETH Zürich, Switzerland

BBC News Sport More Search

NEWS

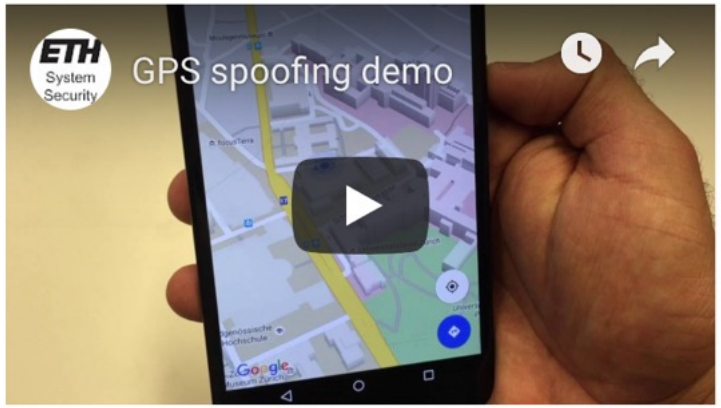
Home Video World UK Business Tech Science More

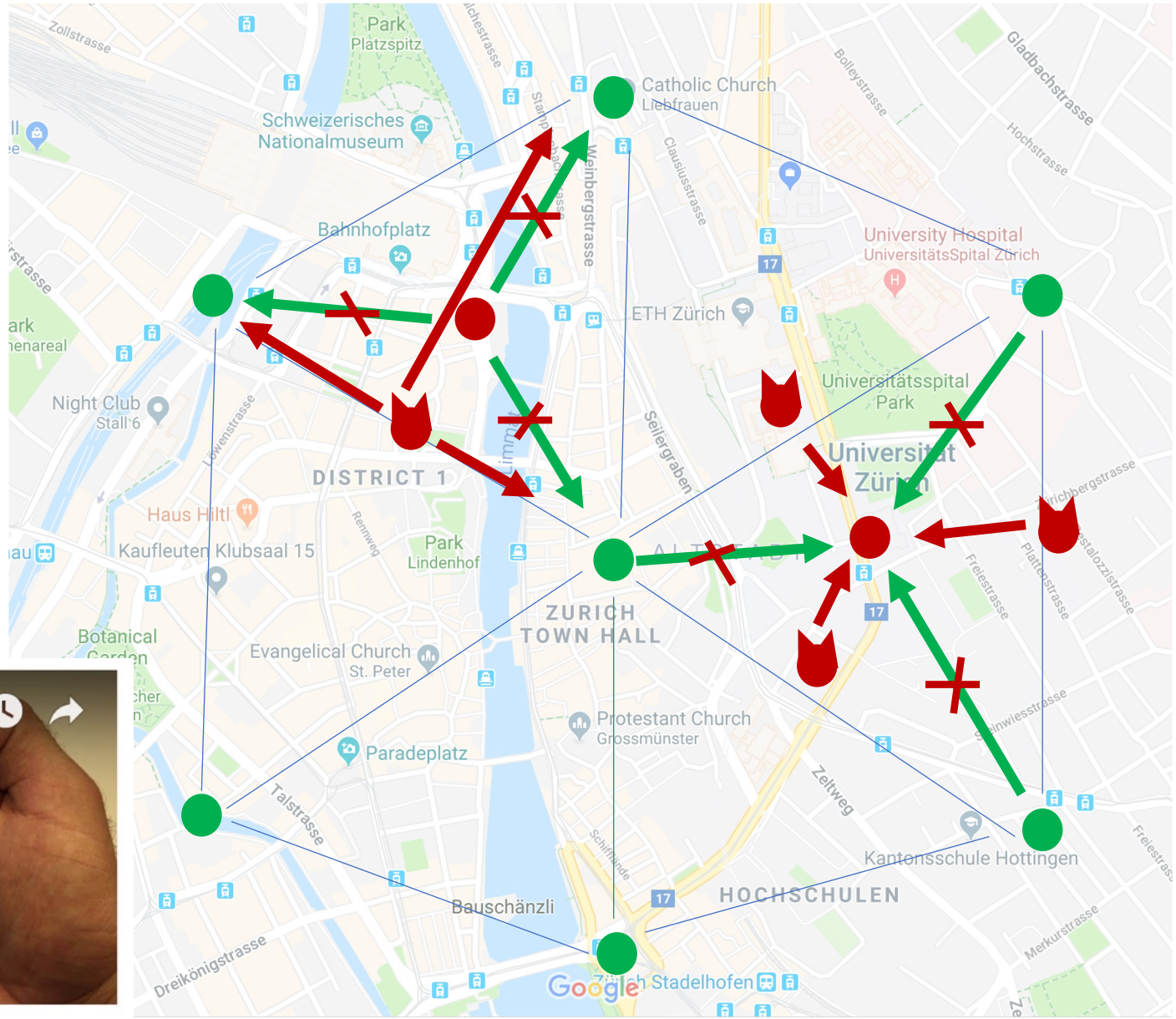
Technology

Researchers use spoofing to 'hack' into a flying drone

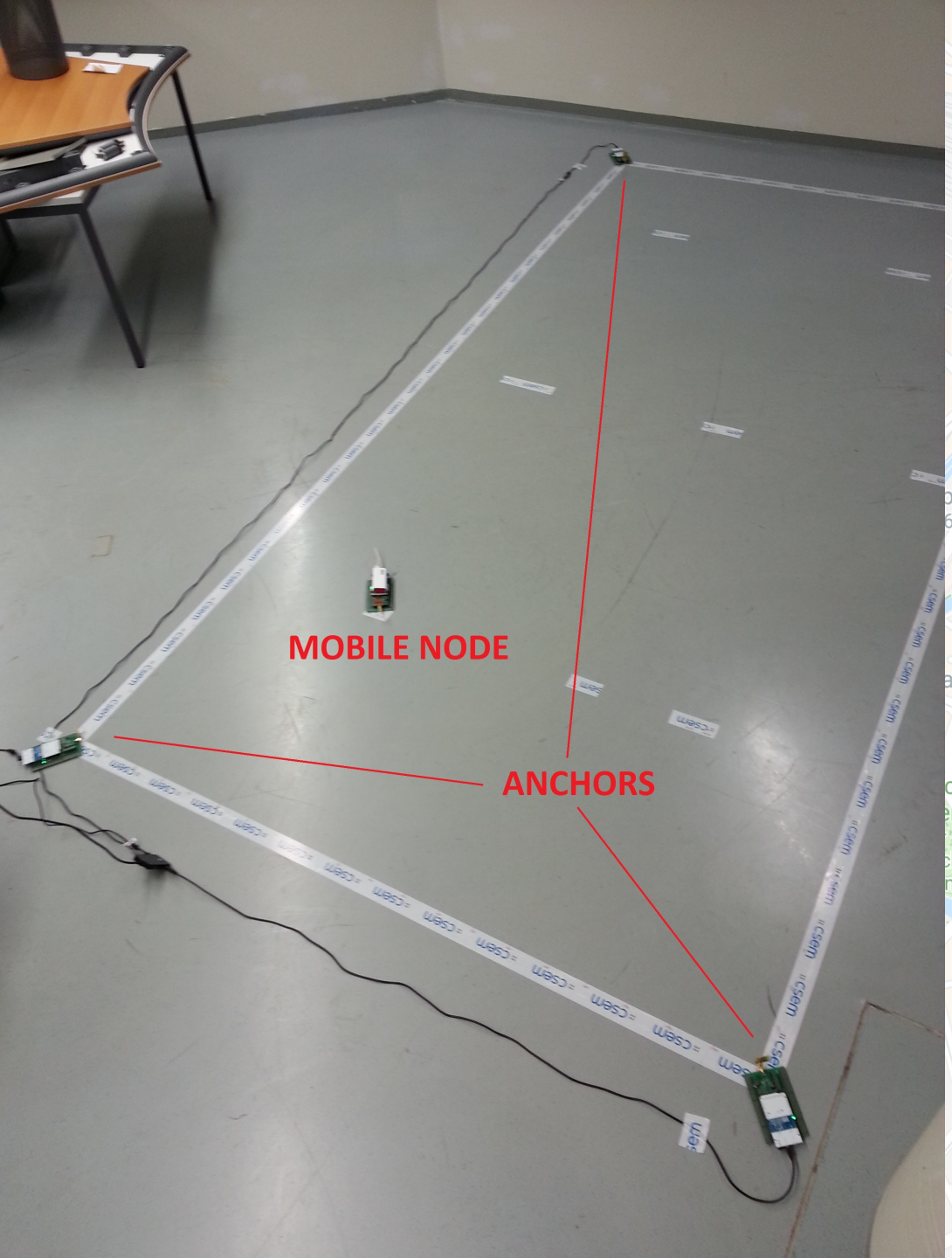
29 June 2012 Share

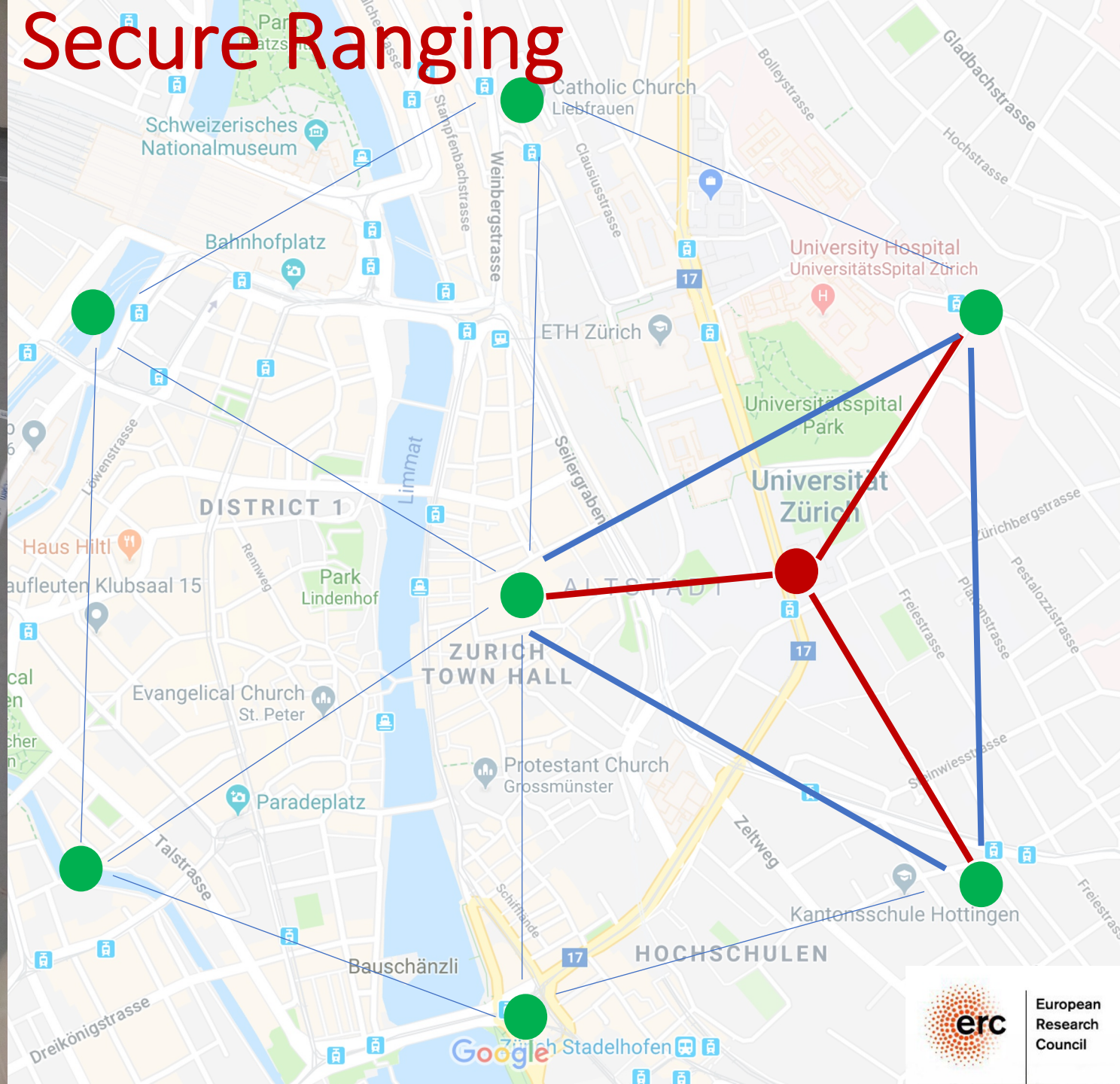
American researchers took control of a flying drone by "hacking" into its GPS system - acting on a $1,000 (£640) dare from the US Department of Homeland Security (DHS).



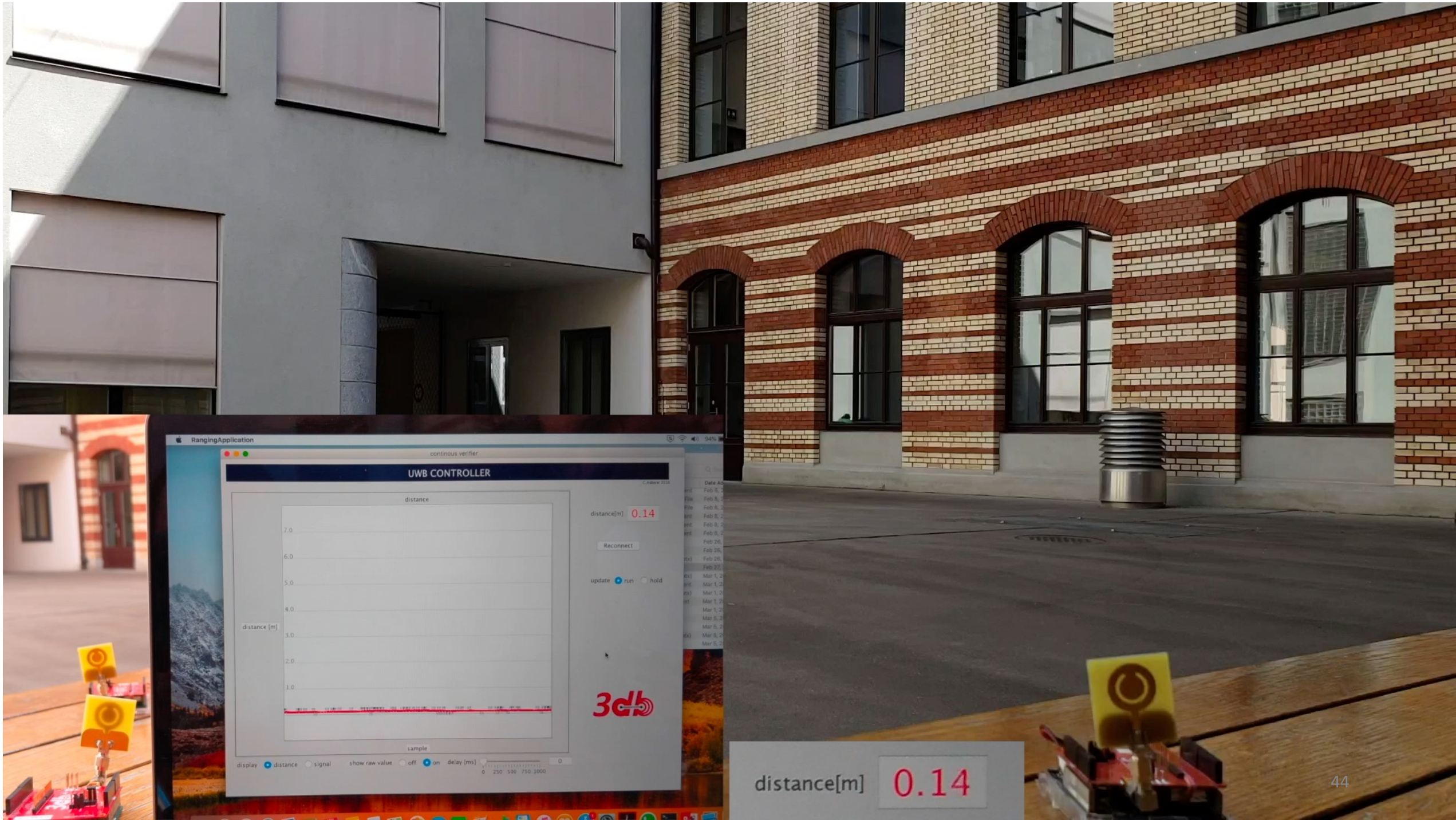


Secure Ranging





erc European Research Council

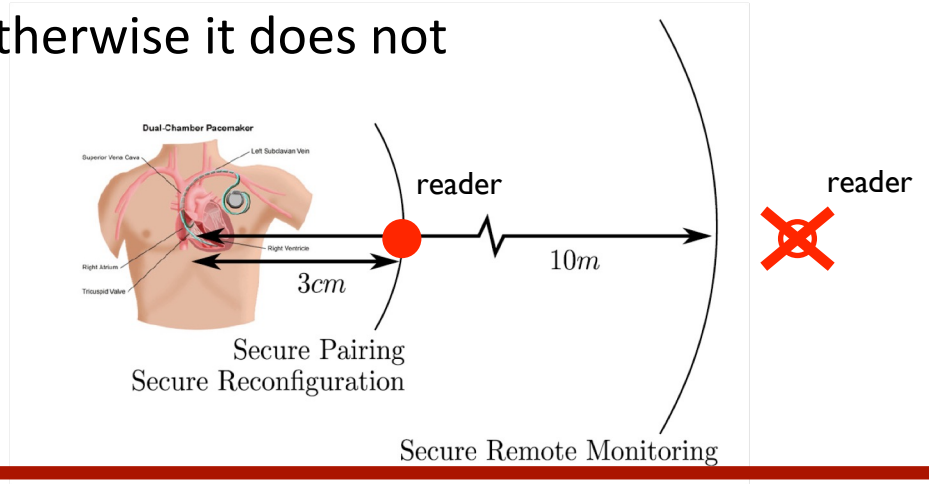

RangingApplication
continous verifier
UWB CONTROLLER
distance
distance[m]
0.14
Reconnect
update
run
hold
distance [m]
7.0
6.0
5.0
4.0
3.0
2.0
1.0
sample
display
distance
signal
show raw value
off
on
delay [ms]
0
250
500
750
1000
3db
distance[m]
0.14

Untrusted Prover (Distance Bounding)

Secure Proximity Verification

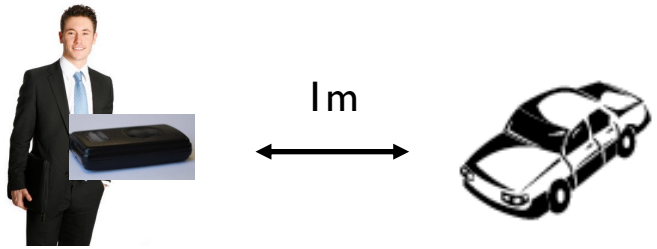
One (untrusted) device wants to *prove to be close* to another device.

- e.g., if a reader is close to the pacemaker, it gets access, otherwise it does not

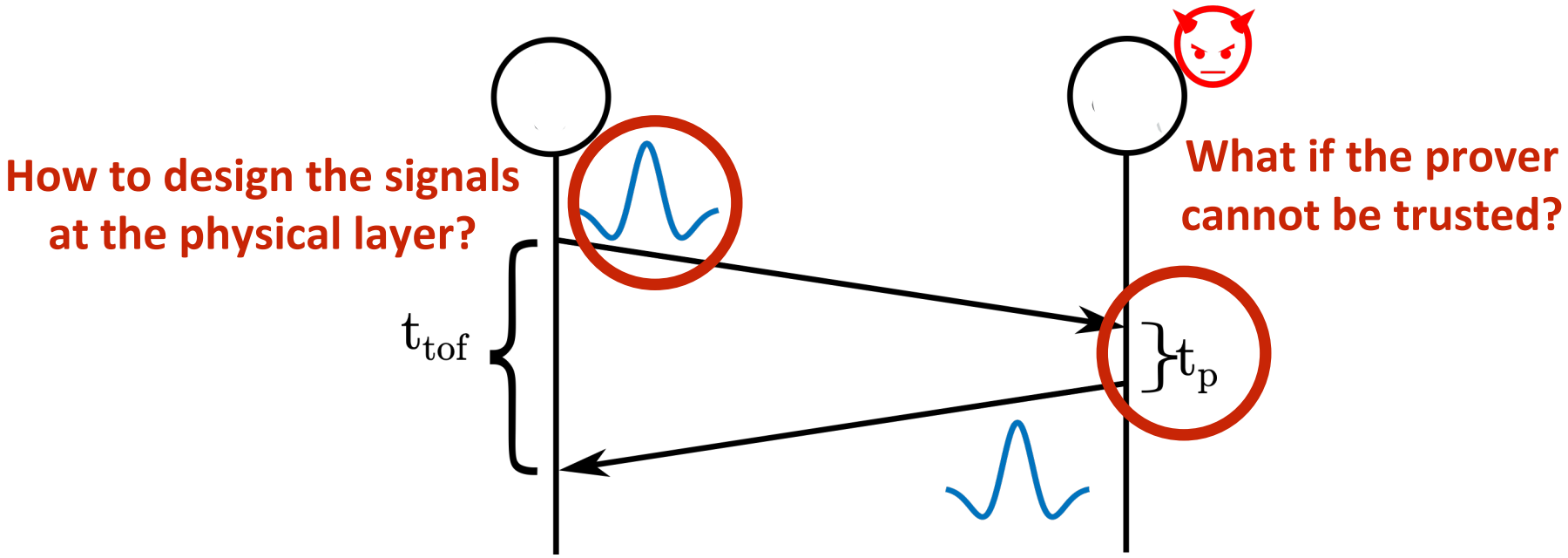


Two devices want to *verify if they are indeed close.*

- e.g., a car and a key want to verify if they are physically close



Estimating Proximity using Time of Flight



$$d = c * (t_{tof} - t_p) / 2$$

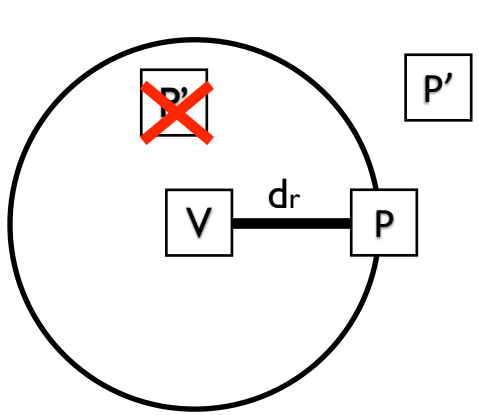
Can an attacker reduce time?

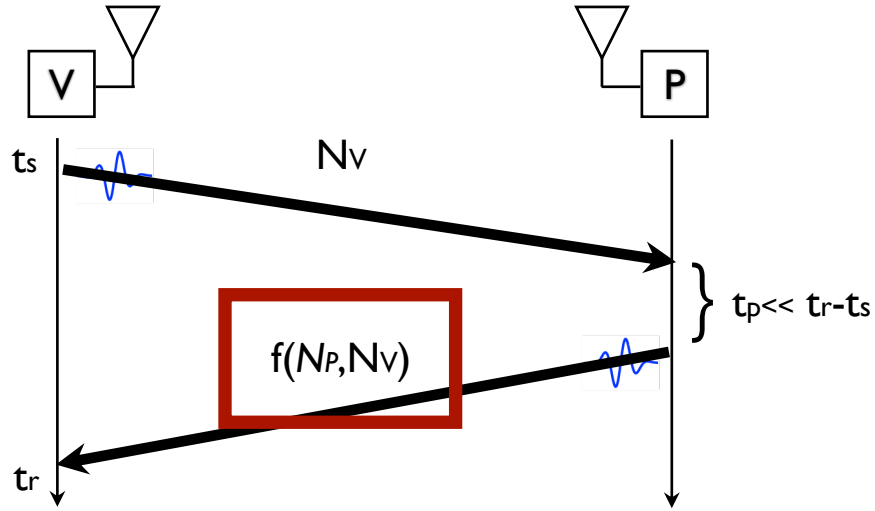
Manipulating time is harder than changing signal strength or phase

BUT…

Distance Bounding [BrandsChaum93]

Basic Idea



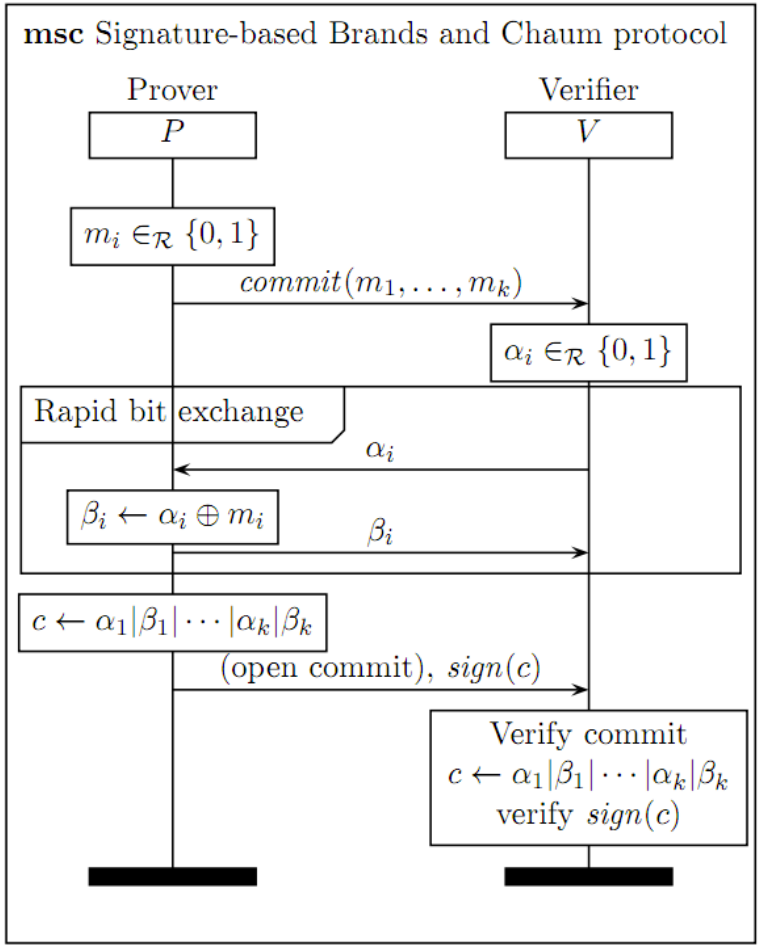


$d = (t_r - t_s - t_p)c/2$

Property:

Measured distance *d* should be an *upper bound* on the true distance d_r between V and P.

Distance Bounding [BrandsChaum93]

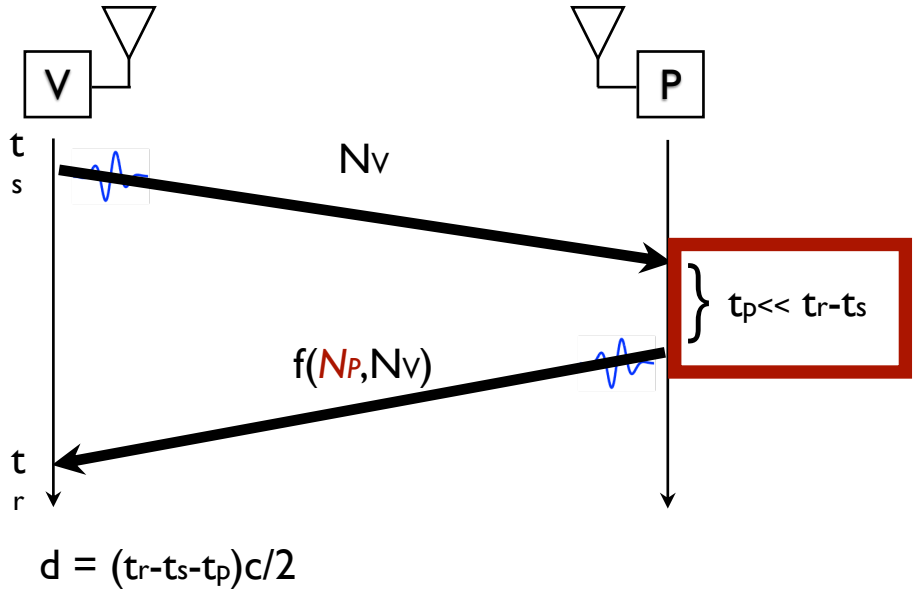


Distance Bounding: *f() and t_p*

Provers should ***quickly*** *receive N_V, compute $f(N_V,N_P)$ and send $f(N_V,N_P)$*

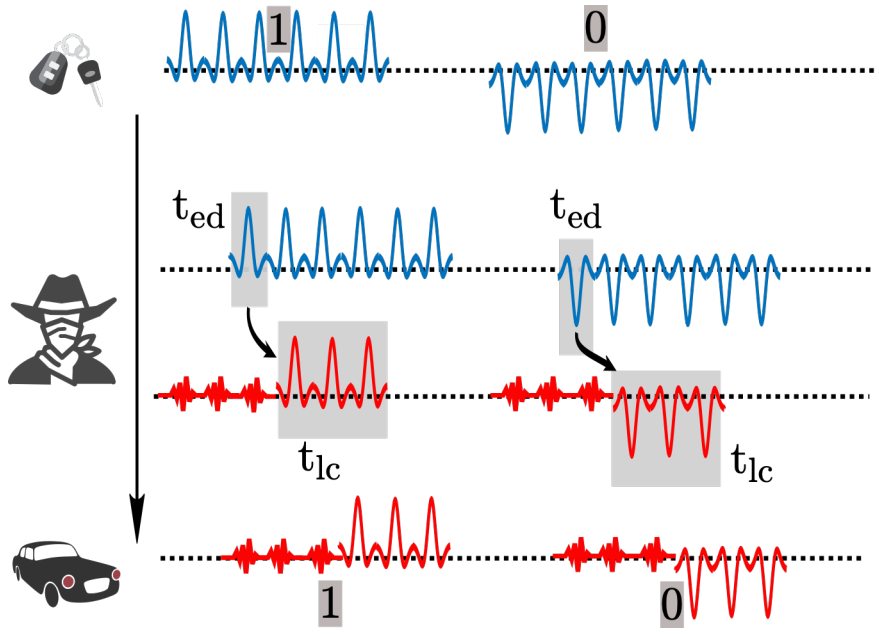
- The verifier estimates prover's processing = t_p
- If attacker's processing = 0 then he *can cheat by $t_p/2$*
- Thus ideally t_p=0s, in most applications t_p=1-2ns (15-30cm)
- t_p needs to be *stable and* ***short***

Main assumption: we do not control the prover



Distance Bounding: *symbols*

Early detect and late commit attacks

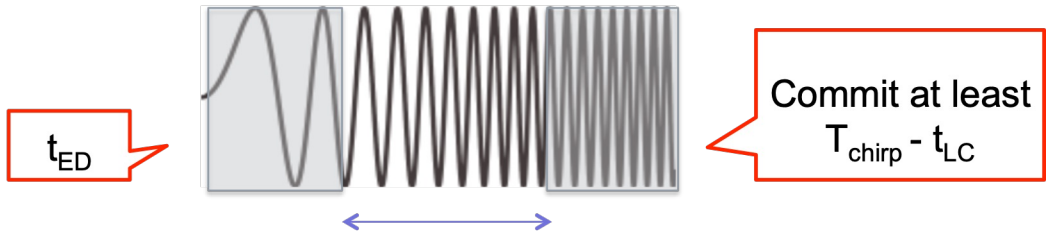


- Predicting the bit even before **completely** receiving it.
- Detecting a bit ‘1’ and ‘0’ from partially received symbols
- Transmit arbitrary signal until the symbol is **early detected**. Leverage receiver robustness.
- Short symbol length?

Distance Bounding: *symbols*

Chirp SS ranging (802.15.4) systems strongly affected

- long symbol lengths allow for simple ED and LC attacks
- Early Detection
- Late Commit



$$t_{GAIN} = t_{LC} - t_{ED} - t_{HW}$$

$$D = c \times t_{GAIN}$$

Aanjhan Ranganathan, Boris Danev, Aurélien Francillon, and Srdjan Capkun. "Physical-layer attacks on chirp-based ranging systems." (WiSec 2012)

Realization of RF Distance Bounding: *Processing Function $f(N_v,N_p)$*

f(Nv,Np) is computed by the prover:

- takes as input Nv (received from the verifier)
- takes as input Np (locally generated by the prover)
- Should allow that the prover: *receives Nv, computes and outputs f(Nv,Np)* **in a short time (few ns)**

DB protocols in the literature:

[BethDesmedt] sign(Nv); h(Nv); mac(Nv); E(Nv); ... => t_p >> ns

[BrandsChaum, *CapkunInfocom05*, ...] *XOR* => t_p = ?

[HanckeKuhn, *TippenhauerESORICS09*, ...] *bit comparison* => t_p = ?

> 20 proposed protocols, not one was ***fully*** implemented

Can the proposed DB protocols be realized?

Realization of RF Distance Bounding:
Processing Function $f(N_v, N_p)$

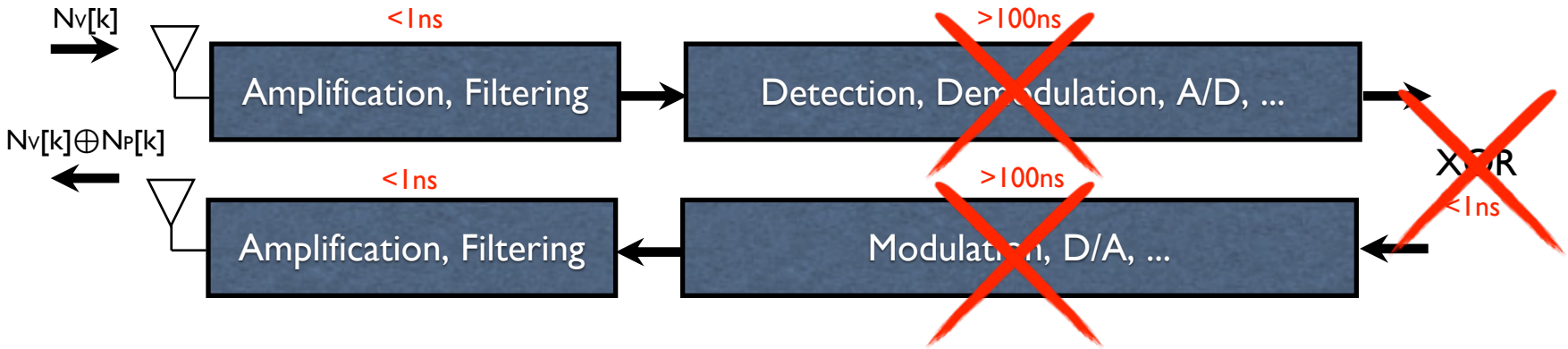
[BethDesmedt] sign(); h(); mac(); E(); ... => t_p >> ns

[**BrandsChaum**, ...] *XOR* => t_p = ? (nx100ns ?)

[**HanckeKuhn**, ...] *bit comparison* => t_p = ? (nx100ns ?)

[RasmussenSec09, ...] *CRCS (analog modulation)* => t_p < 1ns

... > 20 proposed protocols



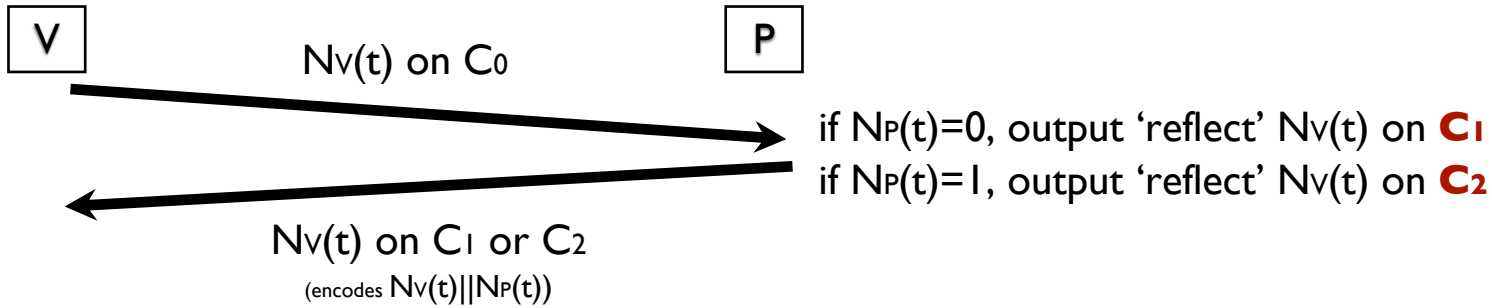
Can we use functions that don't require interpretation (demodulation) Nv ?

A new Function: CRCS

This approach: *Challenge Reflection with Channel Selection*

- Prover does not interpret Nv
- All *time-critical* processing is done in *analog*
- Verifier does “all the work”

Main idea (C_0,C_1,C_2 are channels)

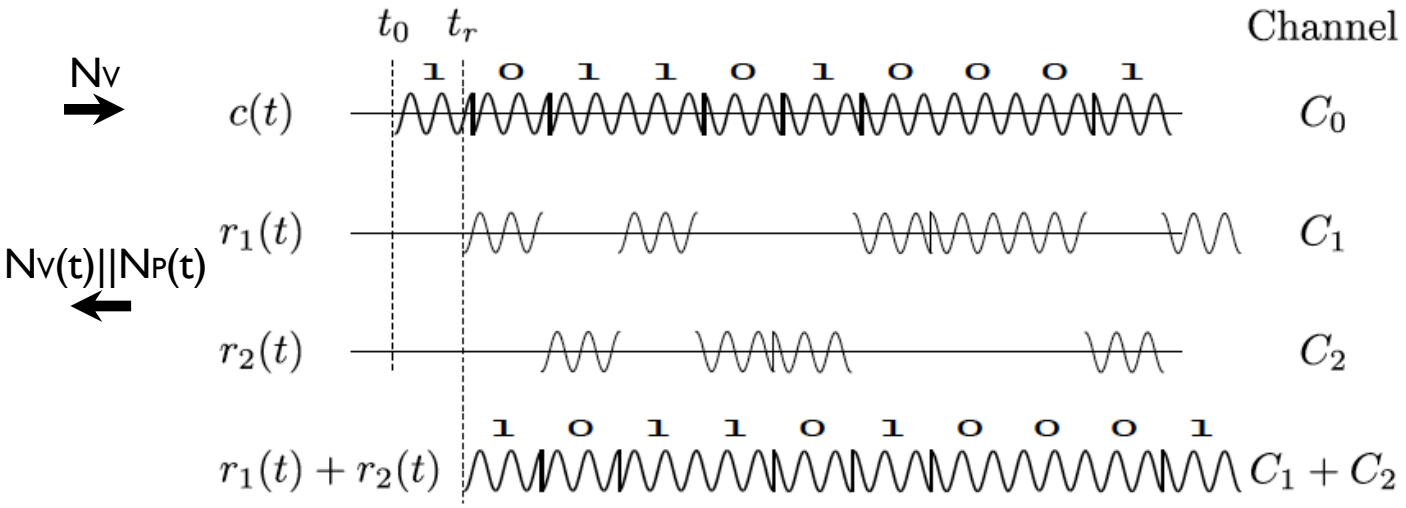


A new Function: CRCS

This approach: *Challenge Reflection with Channel Selection*

- Prover does not interpret Nv
- All *time-critical* processing is done in *analog*
- Verifier does “all the work”

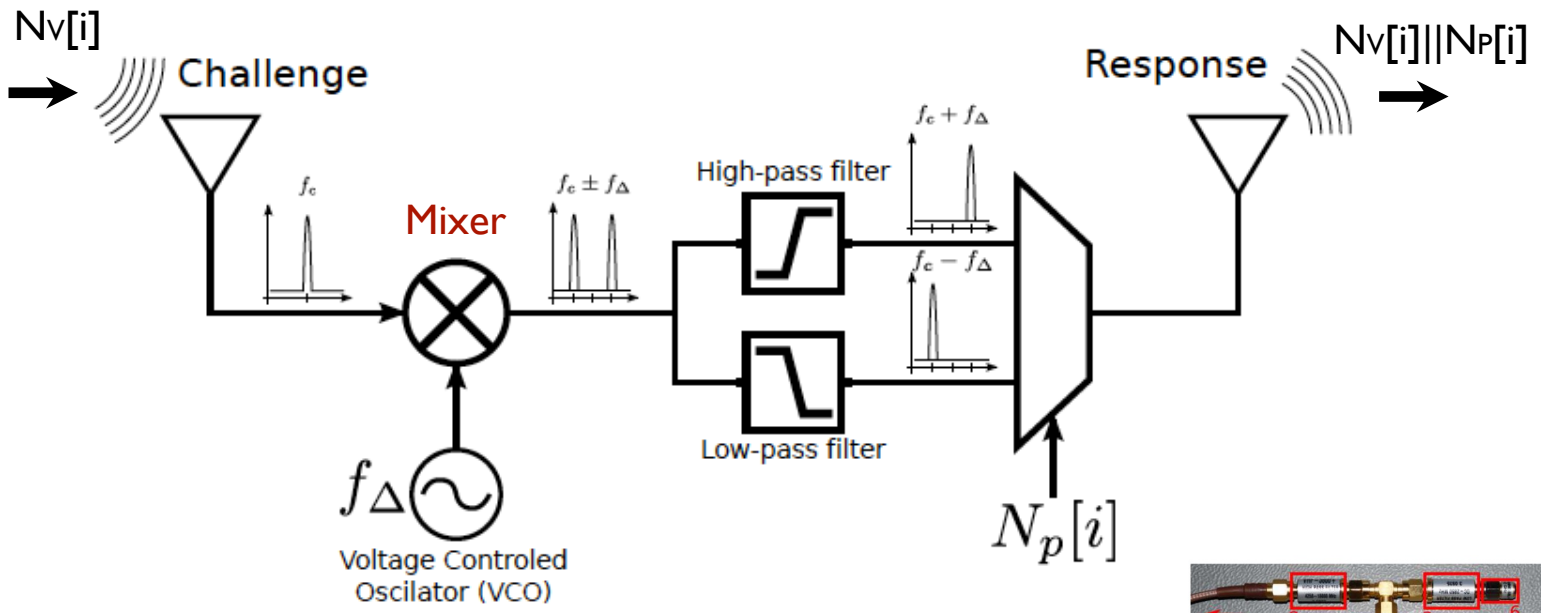
Main idea (C_0,C_1,C_2 are channels)

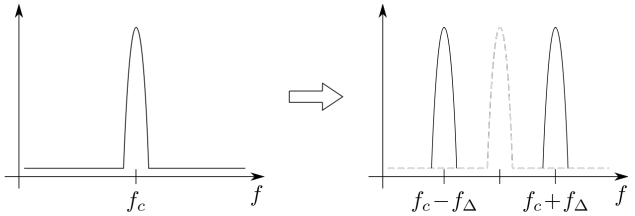


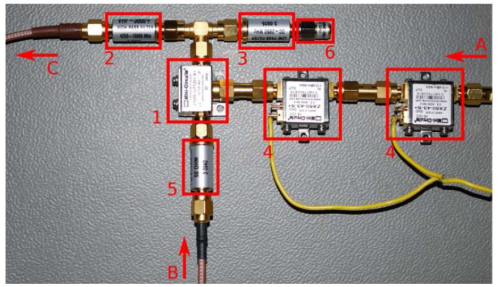
A new Function: CRCS

Implementation of CRCS

t_p < 1ns, st. dev. 61ps, full duplex







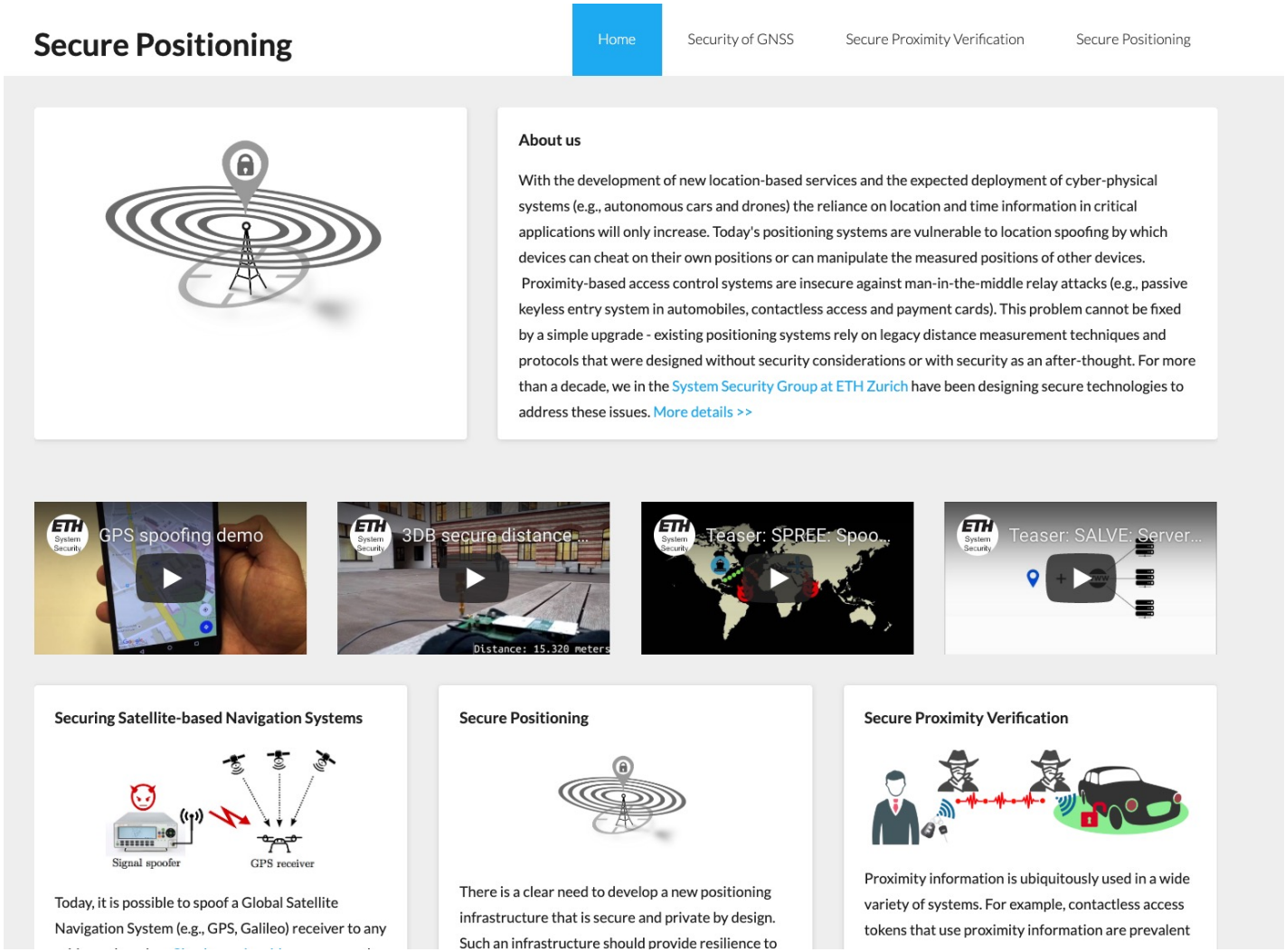
Mixer up+down converts the input signal

ETH zürich

ETH zürich

European Research Council

www.zisc.ethz.ch



www.securepositioning.com