ETH zürich

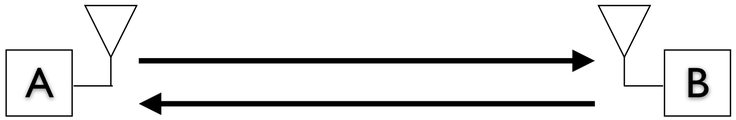
On the Physical Layer for Secure Distance Measurement

Srdjan Čapkun
Department of Computer Science
ETH Zurich

Secure Distance Measurement

Secure Distance Measurement:

- Measuring a correct distance (bound) between two devices in the presence of an attacker.
- Typically, secure proximity verification.



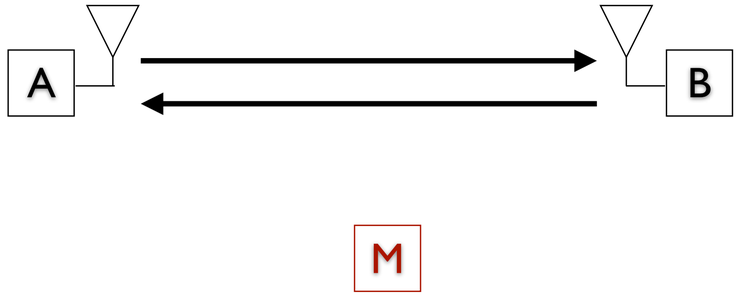
[DB] Stefan Brands, David Chaum: Distance-bounding protocols, Eurocrypt 1993

[Desmedt88] Desmedt, Y.: Major security problems with the 'unforgeable' (feige)-fiat-shamir proofs of identity and how to overcome them. In: SecuriCom 1988

Secure Distance Measurement

Secure Distance Measurement:

- Measuring a correct distance (bound) between two devices in the presence of an attacker.
- Typically, secure proximity verification.



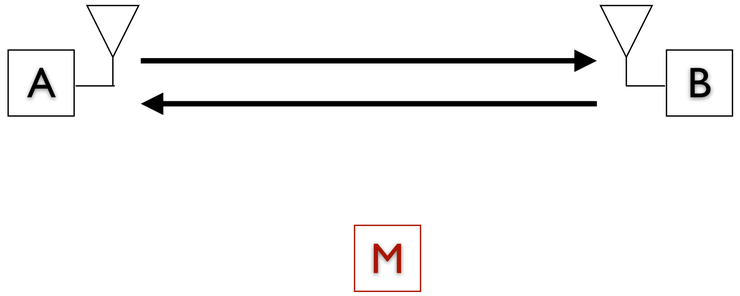
[DB] Stefan Brands, David Chaum: Distance-bounding protocols, Eurocrypt 1993

[Desmedt88] Desmedt, Y.: Major security problems with the 'unforgeable' (feige)-fiat-shamir proofs of identity and how to overcome them. In: SecuriCom 1988

Secure Distance Measurement

Secure Distance Measurement:

- Measuring a correct distance (bound) between two devices in the presence of an attacker.
- Typically, secure proximity verification.



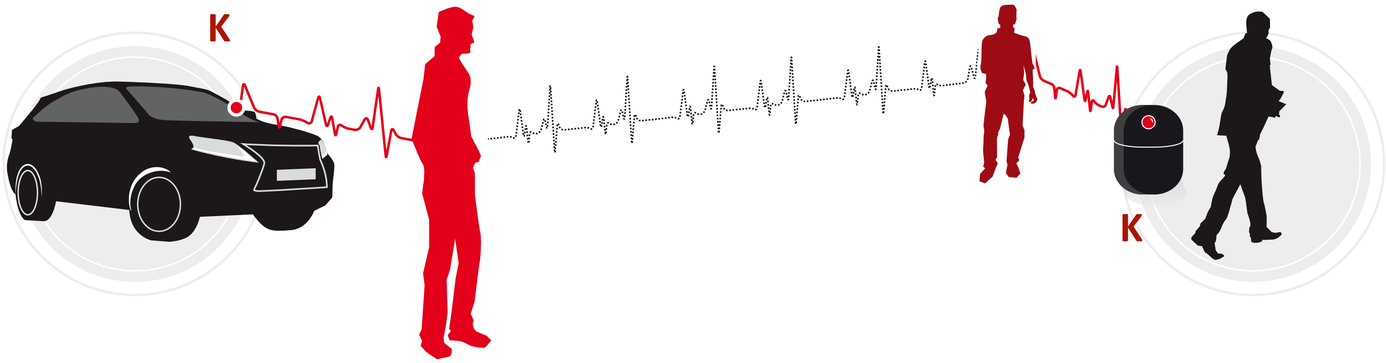
Secure *Proximity Detection:*

*Attacker cannot convince A and B that they are **closer** than they are. (i.e., distance **upper** bound)*

[DB] Stefan Brands, David Chaum: Distance-bounding protocols, Eurocrypt 1993

[Desmedt88] Desmedt, Y.: Major security problems with the 'unforgeable' (feige)-fiat-shamir proofs of identity and how to overcome them. In: SecuriCom 1988

Attack: Passive Keyless Entry and Start Systems

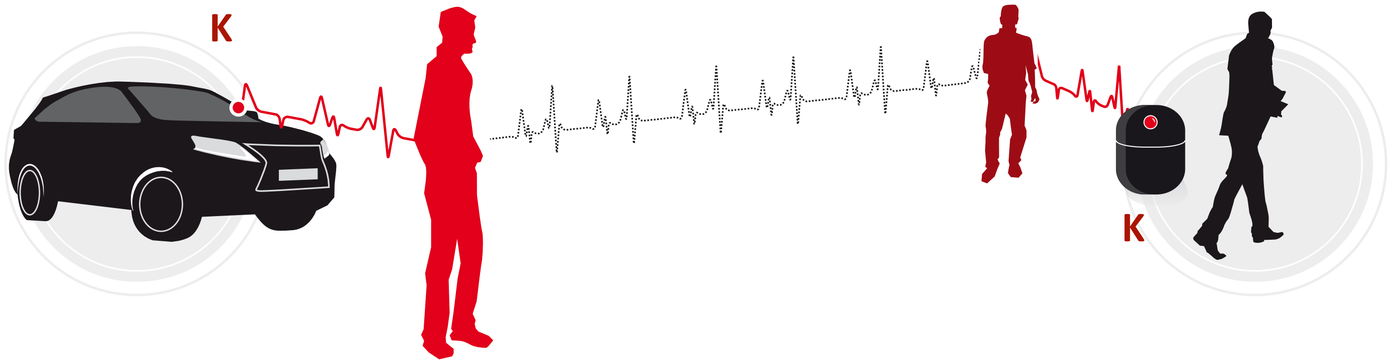


Tages-Anzeiger · Auto Bild · The Sunday Times · MIT Technology Review · Les Echos · The New York Times · VOX

[DA11] A. Francillon, B. Danev, S. Capkun

Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars, NDSS 2011

Attack: Passive Keyless Entry and Start Systems

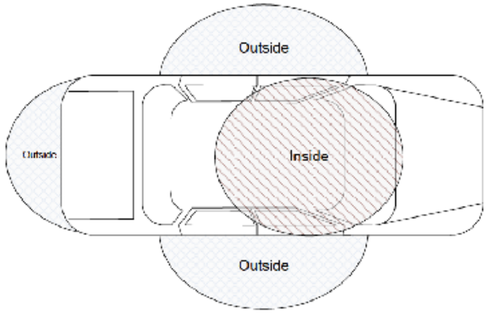


If:
- correct key K is used
- reply within *Max Delay*

then:
- open door / start car

short range (<2m)

Fresh Challenge
(LF, 120-135 KHz)



Authentic Reply
(UHF, 315-433 MHz)

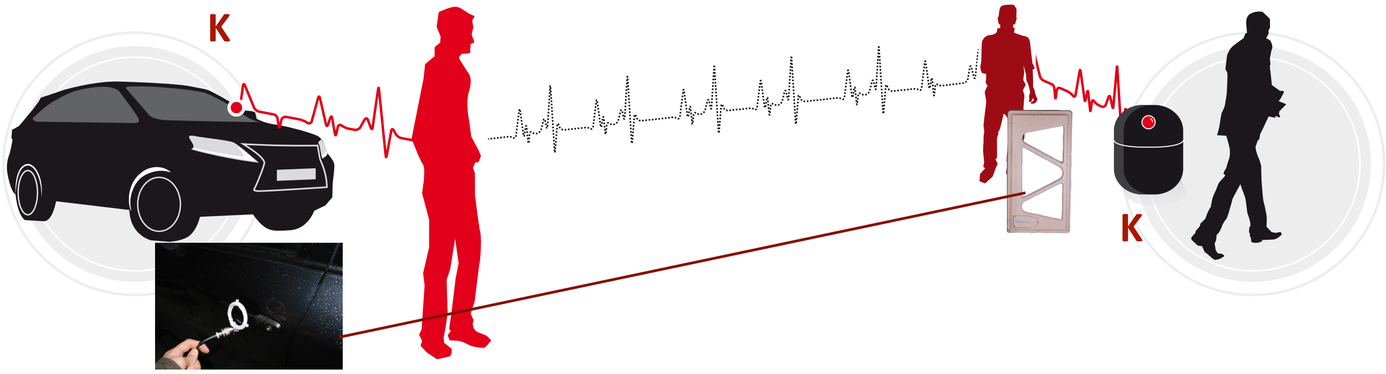
long range (<100m)

Tages-Anzeiger · Auto Bild · The Sunday Times · MIT Technology Review · Les Echos · The New York Times · Vox

[DA11] A. Francillon, B. Danev, S. Capkun
Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars, NDSS 2011

ETH zürich

Attack: Passive Keyless Entry and Start Systems

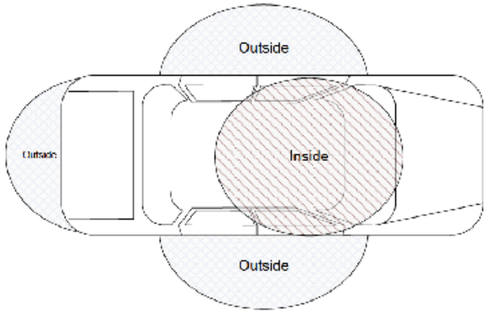


If:
- correct key K is used
- reply within *Max Delay*

then:
- open door / start car

short range (<2m)

Fresh Challenge
(LF, 120-135 KHz)



Authentic Reply
(UHF, 315-433 MHz)

long range (<100m)

Tages-Anzeiger · Auto Bild · The Sunday Times · MIT Technology Review · Les Echos · The New York Times · Vox

[DA11] A. Francillon, B. Danev, S. Capkun
Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars, NDSS 2011

ETH zürich

A

WIRED

Just a Pair of These $11 Radio Gadgets Can Steal a Car

BUSINESS | CULTURE | DESIGN | GEAR | SCIENCE

SHARE

SHARE 8264

TWEET

COMMENT 28

EMAIL

ANDY GREENBERG SECURITY 04.24.17 1:34 PM

JUST A PAIR OF THESE $11 RADIO GADGETS CAN STEAL A CAR

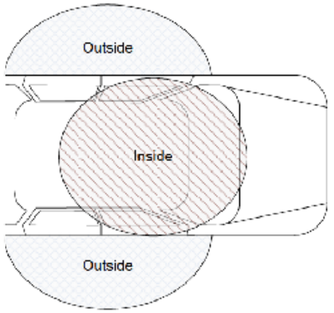
QIHOO 360 TEAM UNICORN

If:

- correct k
- reply wit

then:

- open doc



Tages-Anzeiger

mes

V•X

[DA11] A. Francillon, B. Danev, S. Capkun

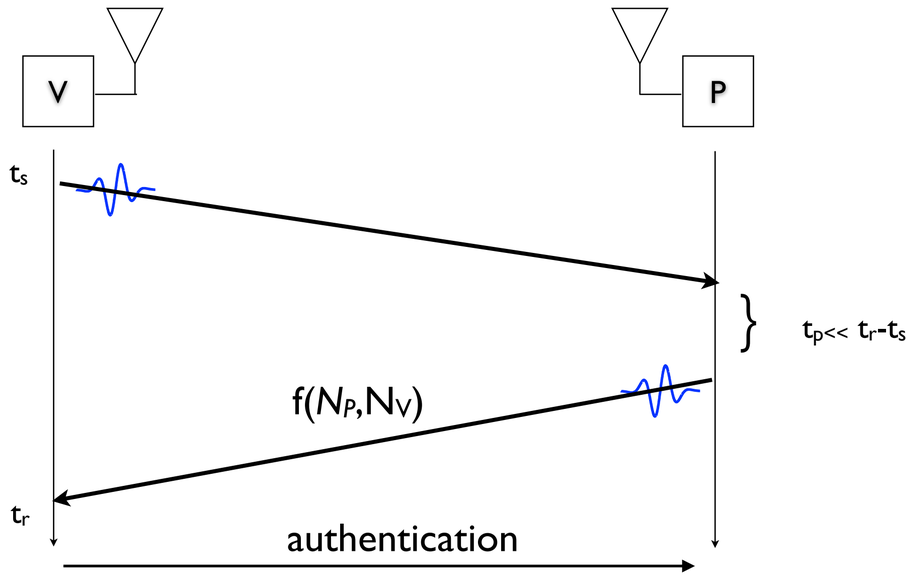
Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars, NDSS 2011

ETH zürich

How To Secure Distance Measurement?

We need

- an authenticated distance bounding protocol:
- a distance measurement technique (that provides good range and precision)
- **physical layer / distance measurement that is secure against all attacks**
- low power / complexity of implementation



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

How To Secure Distance Measurement?

Main idea: *Measure the distance between V and P + Authenticate Messages*

IDM = Indirect Distance Measurement (no 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)

Direct Distance Measurement (Time-of-Flight)

- Chirp Spread Spectrum (802.15.4a, ISO/IEC 24730-5, NanoLOC)
- Ultra Wide Band (UWB)
  - 802.15.4a UWB
  - **802.15.4f UWB (single pulse per bit) and multi-pulse per bit [Singh17]**

[Ran17] A. Ranganathan, S. Capkun, Are We Really Close? Verifying Proximity in Wireless Systems, IEEE Security & Privacy Magazine, May-June 2017 (overview)

How To Secure Distance Measurement?

Main idea: *Measure the distance between V and P + Authenticate Messages*

IDM = Indirect Distance Measurement (no 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)

Direct Distance Measurement (Time-of-Flight)

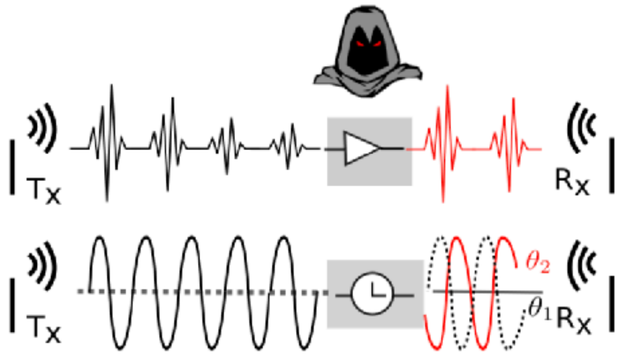
- Chirp Spread Spectrum (802.15.4a, ISO/IEC 24730-5, NanoLOC)
- Ultra Wide Band (UWB)
  - 802.15.4a UWB
  - **802.15.4f UWB (single pulse per bit) and multi-pulse per bit [Singh17]**

This talk

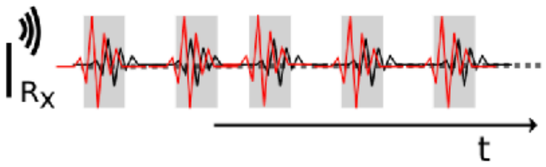
[Ran17] A. Ranganathan, S. Capkun, Are We Really Close? Verifying Proximity in Wireless Systems, IEEE Security & Privacy Magazine, May-June 2017 (overview)

Secure Distance Measurement: **Physical Layer** Attacks

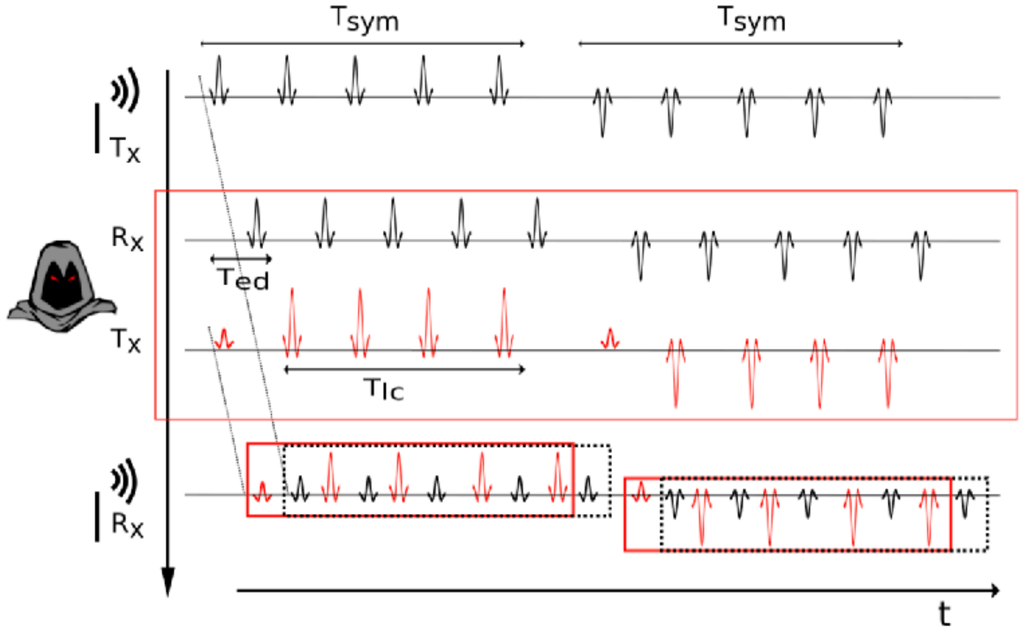
Simple Relay, Phase Relay, Signal Amplification, Early Detect / Late Commit, Cicada, Preamble Advance, …



a) Relay Attack



b) Cicada Attack



c) ED/LC Attack

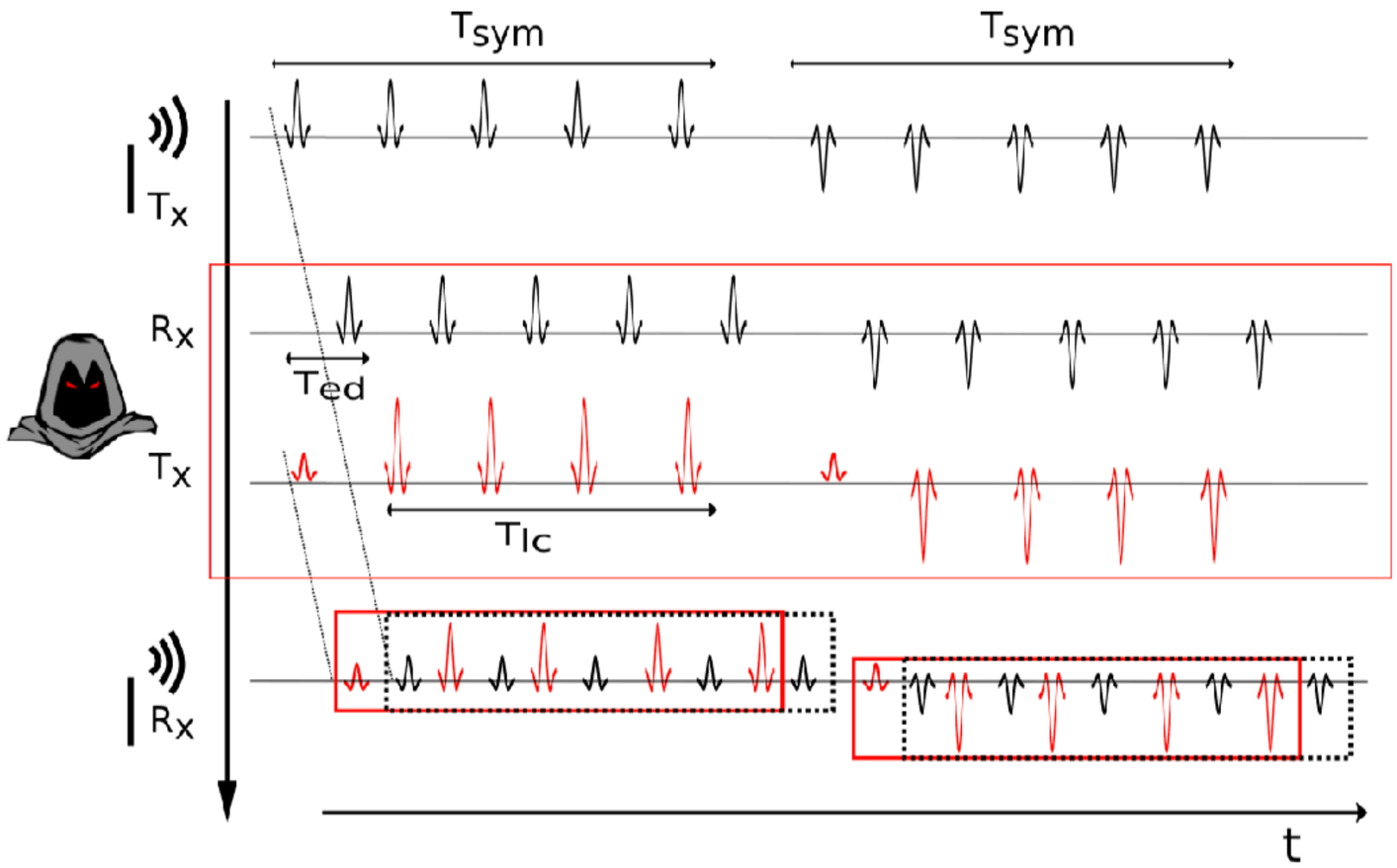
Attacker reduces the measured distance! By

- advancing the arrival of the signal (or directly changing its features) (a)

- injecting signals to change the ToA estimate (b, c)

ETH zürich

Secure Distance Measurement: Attacks

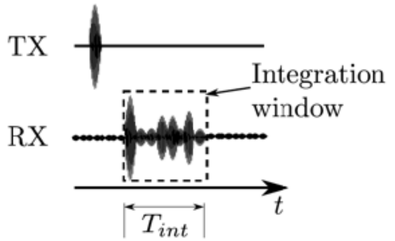


Early Detect / Late Commit Attack

[CL06] J. Clulow, G. P. Hancke, M. G. Kuhn, T. Moore,
So Near and Yet So Far: Distance-Bounding Attacks in Wireless Networks, ESAS 2006

Physical Layer

We know: long symbols (from a small symbol space) => ED/LC and Cicada attacks



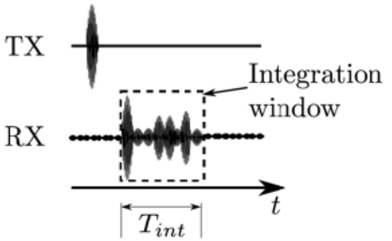
Two options to counter attacks:

- short symbols (ToA over 1 pulse => short range)
  - 1 UWB pulse per bit **=> fully secure (attacker can cheat within the width of the pulse)**

- long symbols (ToA over sequence => long range)
  - randomized symbols
    - **UWB with pulse reordering: interleaving of multi-pulse symbols [Singh17]**

Physical Layer

We know: long symbols (from a small symbol space) => ED/LC and Cicada attacks



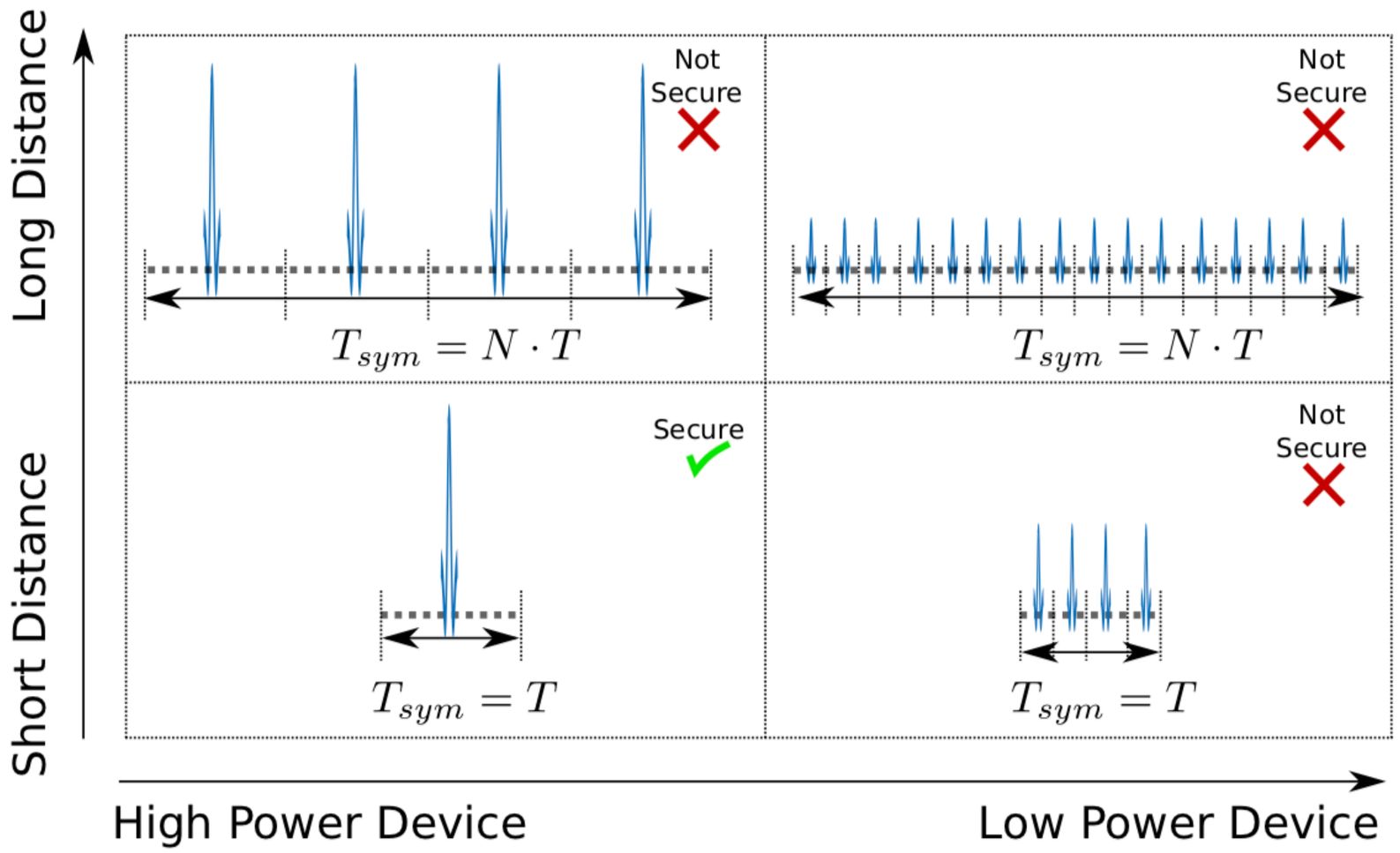
Two options to counter attacks:

- short symbols (ToA over 1 pulse => short range)
  - 1 UWB pulse per bit **=> fully secure (attacker can cheat within the width of the pulse)**

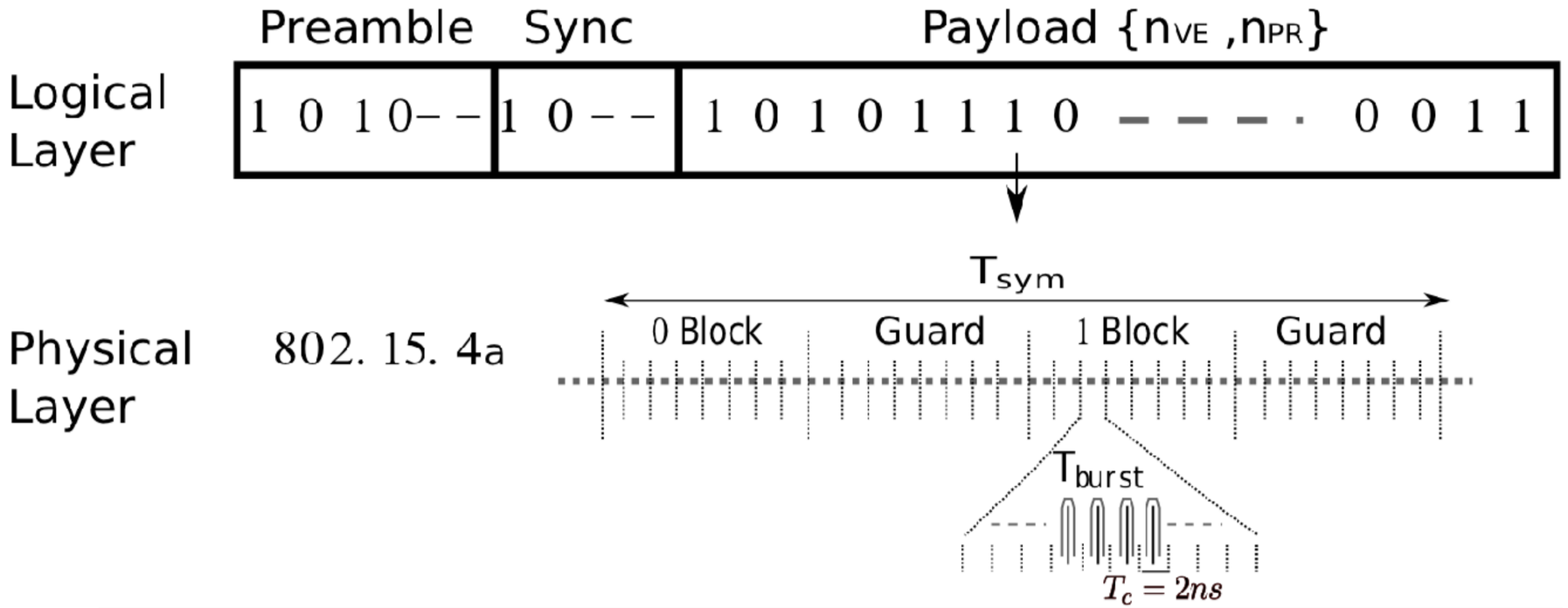
- long symbols (ToA over sequence => long range)
  - randomized symbols
    - **UWB with pulse reordering: interleaving of multi-pulse symbols [Singh17]**

This talk

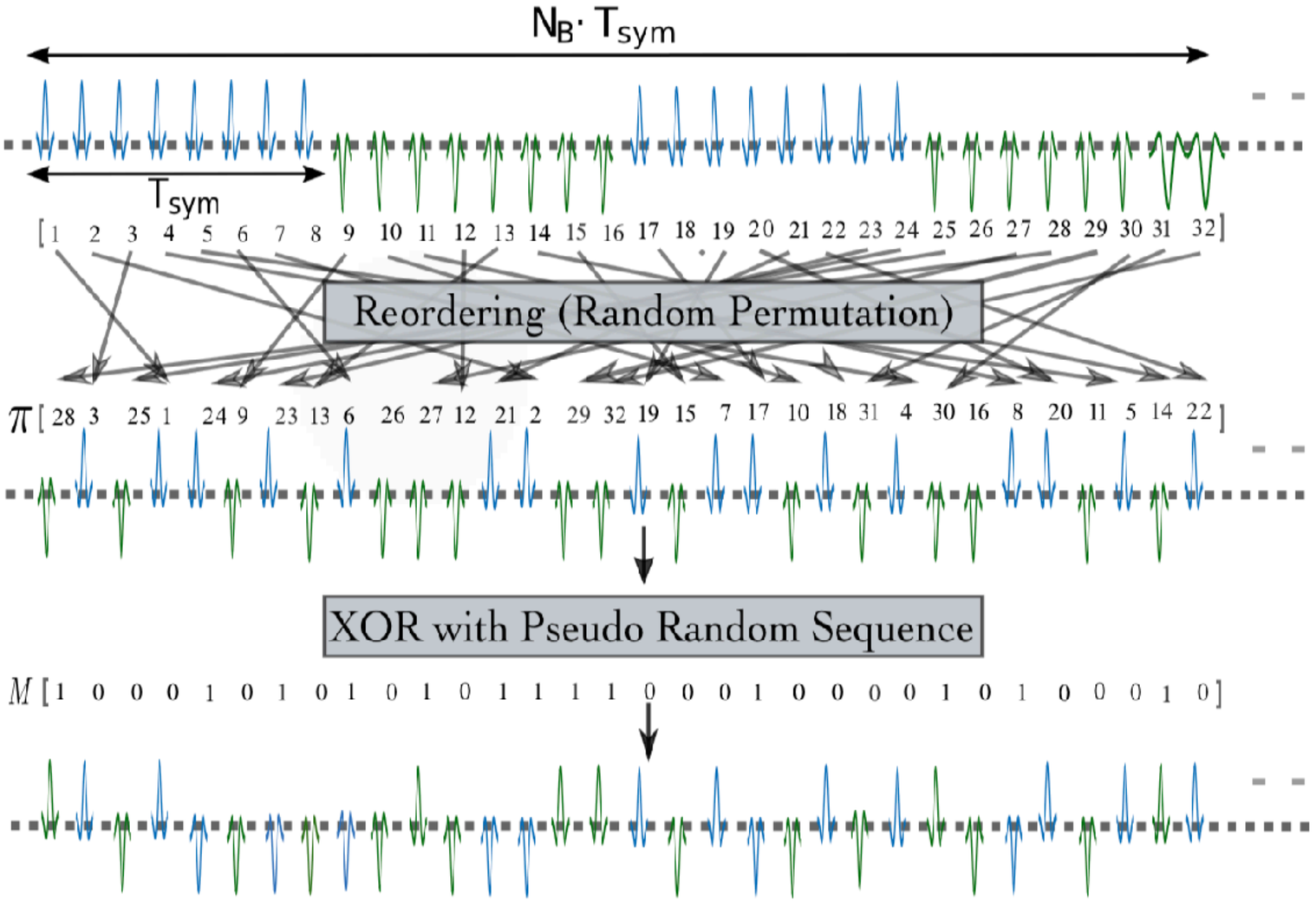
How To Secure Distance Measurement? [Singh17]



UWB (802.15.4a/f)

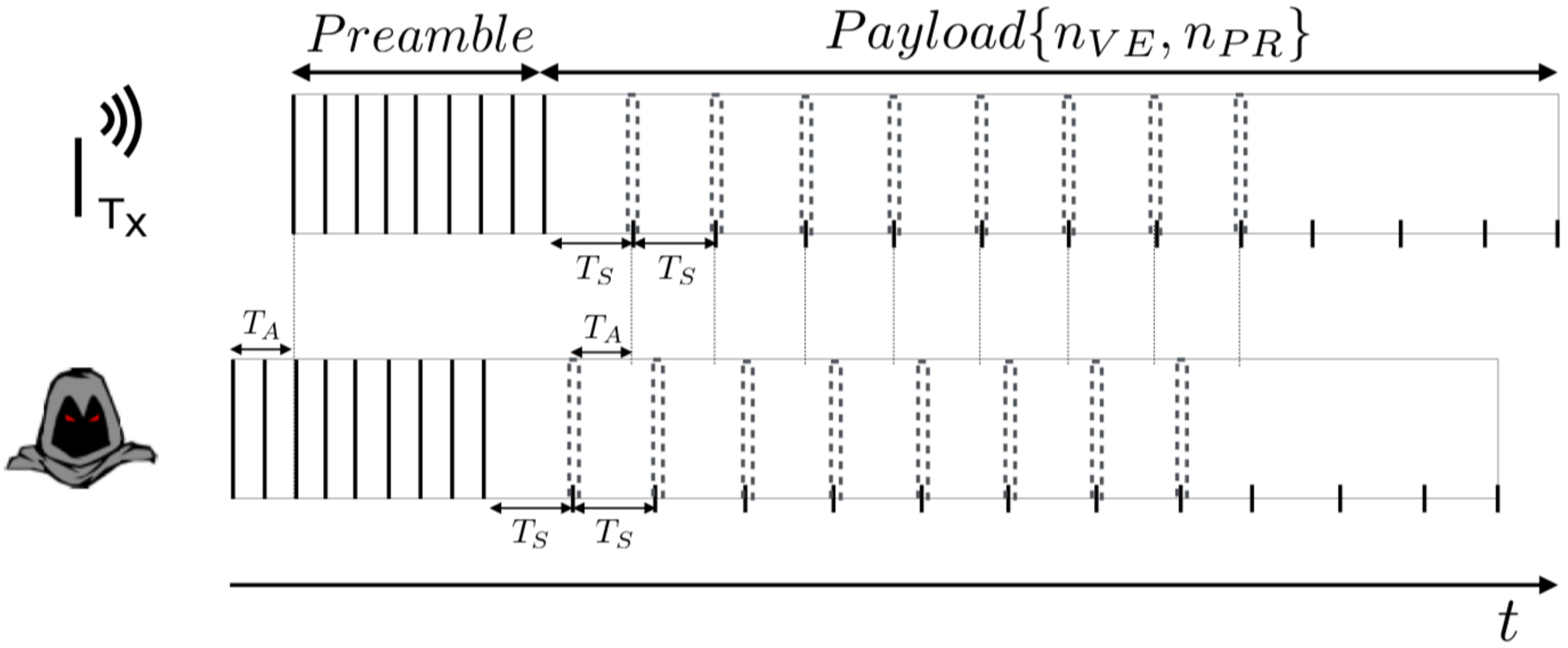


How To Secure Distance Measurement? [Singh17]



UWB with pulse reordering: interleaving of multi-pulse symbols

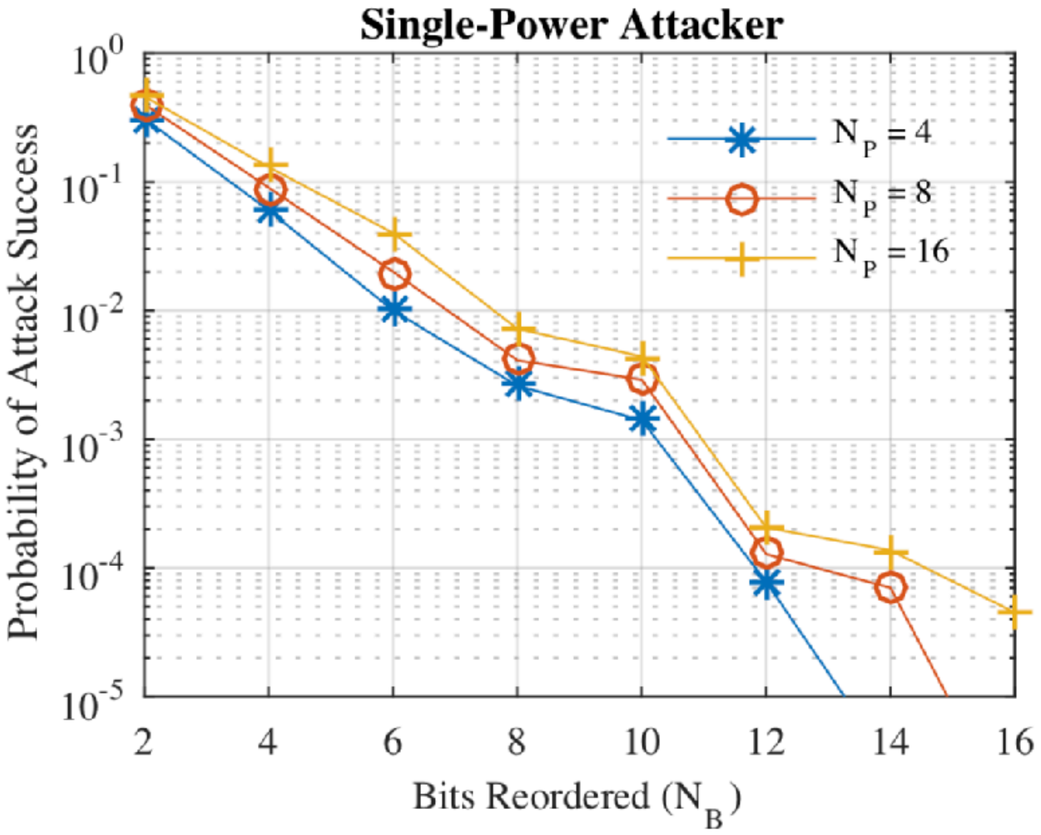
How To Secure Distance Measurement? [Singh17]

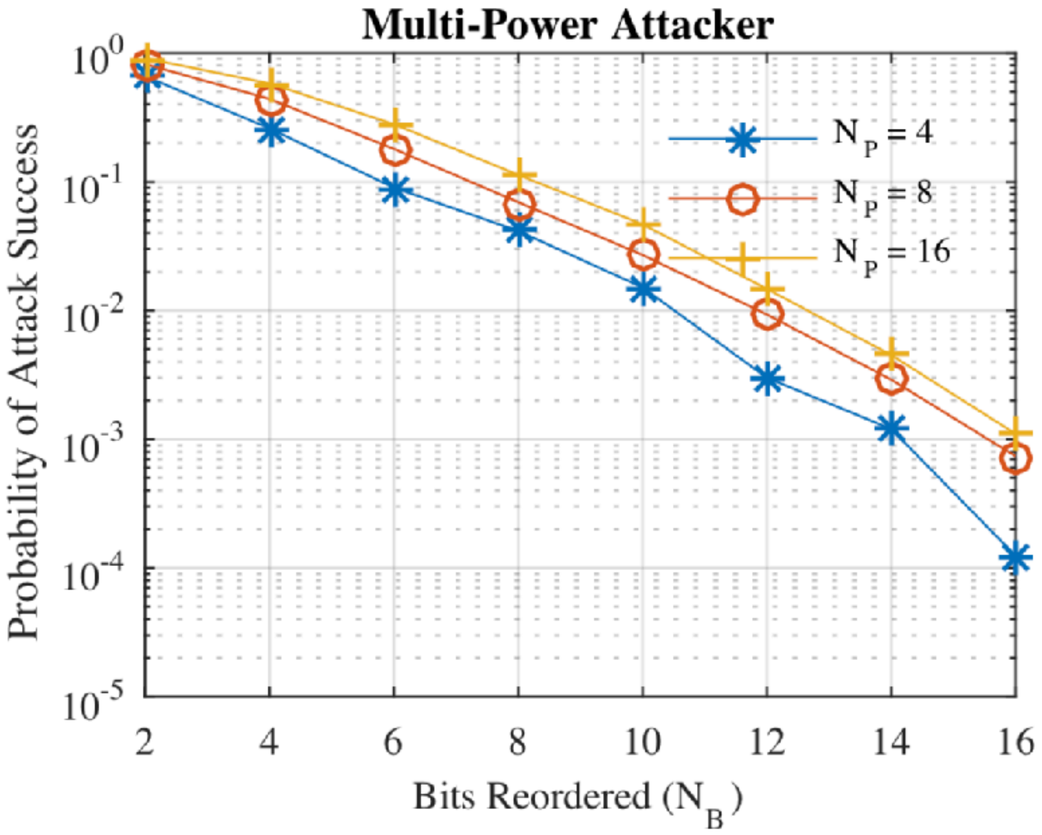


Distance Commitment = distance computed on a fixed preamble (known to the attacker) & then 'verified' on the random payload [Tipp15].

[Tipp15] N. Tippenhauer, H. Luecken, M. Kuhn and S. Capkun,
UWB Rapid-Bit-Exchange System for Distance Bounding, ACM WiSec 2015

Security [Singh17]





How To Secure Distance Measurement? [Singh17]

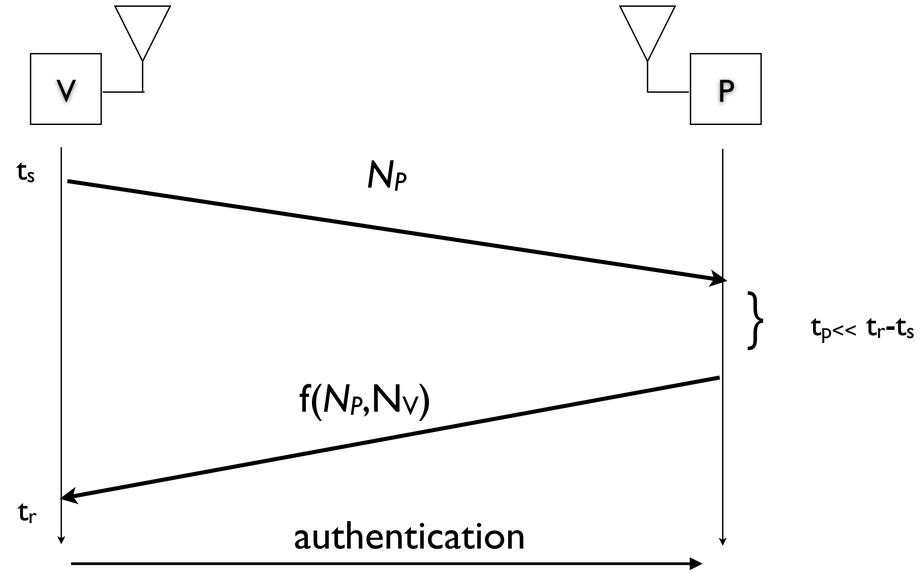
Support for Both Trusted and Untrusted Prover

Trusted Prover is trivially supported:

- Prover decodes UWB PR sequences
- Computes a reply (fixed time computation)
- Replies

Untrusted Prover:

- Prover replies “blindly” to pulses (similar to CRCS [Rasmussen10])
- No “real time” decoding at the prover
- Verifier decodes the UWB PR sequences



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

(illustration - different protocols can be supported)

How To Secure Distance Measurement? [Singh17]

Physical layer that supports distance measurement and is secure against all attacks

- Based on UWB 802.15.4f, 500MHz - 1GHz bandwidth
- Round trip time of flight

Current implementation:

- 150-200m (LoS) range, 15cm precision
- 1ms per measurement
- Low power
- Only support for ***Trusted Prover*** (only Mafia Fraud Resilience)

Using long symbols with Reordering, range can be extended "arbitrarily" (trading off time of measurement)

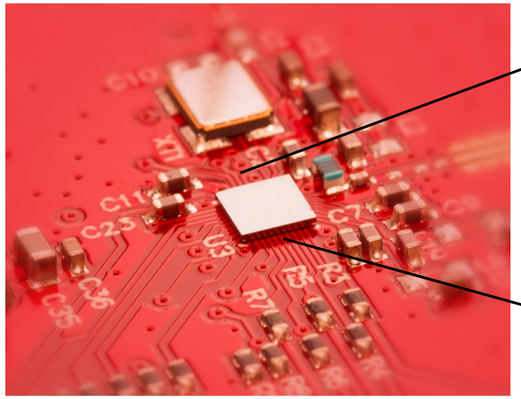
(in contrast to e.g., [Rasmussen10] or [Tipp15] that have limited range)

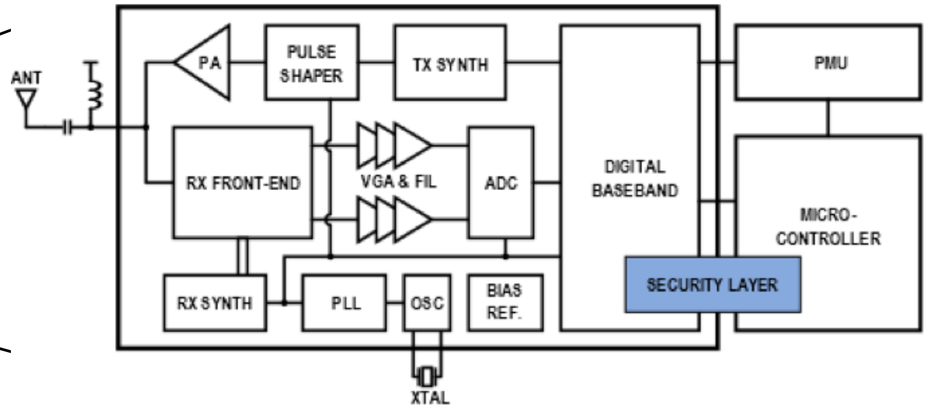
[Singh17] M. Singh, P. Leu, S. Capkun, UWB with Pulse Reordering: Securing Ranging against Relay and Physical Layer Attacks, EPrint Archive, 2017

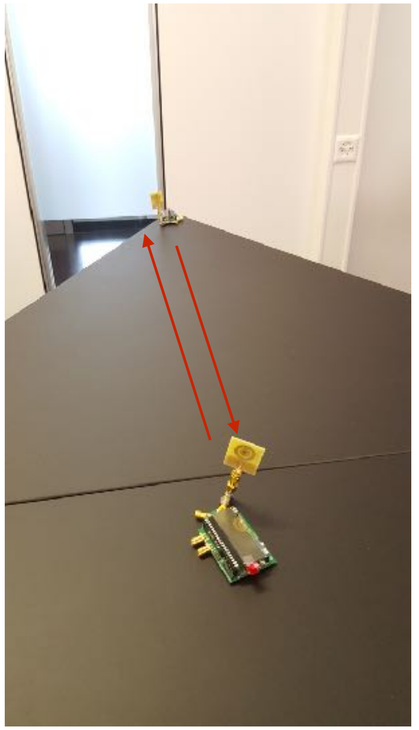
[Rasmussen10] K. Rasmussen, S. Capkun. Realization of rf distance bounding. In Proceedings of the USENIX Security Symposium , 2010

Technology and Implementation

With 3DB technologies (https://www.3db-access.com)







Implications for Past Research / Assumptions Made in the Community

Some Comments on the Assumptions Made in the Community

- Is rapid bit exchange needed for distance bounding?

No. We show that multi-bit nonces can also be used.

It will also require more time since roundtrip time measurement is executed several times.

- Are protocols based on multi-bit nonces insecure?

No, unless one uses “insecure” physical layer.

- Is the distance measured on ‘individual bits’?

No. For robustness / performance, distance is typically measured over a series of symbols and buts Actually, typically it is measured over a preamble and then verified over the data (Distance Commitment).

- Does Rapid Bit Exchange improve the Robustness? Do we need “robust” rapid bit exchange?

Not really, if bits are encoded as long sequences of pulses, there is enough robustness to compensate for failures on the channel.

Were Brands and Chaum [BC] and [CL06] Right?

[BC]:

- use rapid bit exchange

[CL06]:

- use rapid bit exchange (multi-bit challenge-response is insecure)
- use 1 (UWB) symbol per bit
- specific protocols that use multi-bit challenge-responses are insecure

Our work [Singh17] shows that

- Multi-pulse per bit symbols can be secure
- Multi-bit challenge response can be secure
- Protocols that were claimed to be vulnerable in [CL06] are secure

[CL06] J. Clulow, G. P. Hancke, M. G. Kuhn, T. Moore,
So Near and Yet So Far: Distance-Bounding Attacks in Wireless Networks, ESAS 2006

[Singh17] M. Singh, P. Leu, S. Capkun, UWB with Pulse Reordering: Securing Ranging against Relay and Physical Layer Attacks, EPrint Archive, 2017

Clulow et al. [CL06] - ED/LC attacks

"We show that proposed distance-bounding protocols of Hu, Perrig and Johnson (2003), Sastry, Shankar and Wagner (2003), and Čapkun and Hubaux (2005, 2006) ***are vulnerable to a guessing attack where the malicious prover preemptively transmits guessed values for a number of response bits.*****"**

and

"We propose a number of principles to adhere to when implementing distance-bounding systems. These restrict the choice of communication medium to speed- of-light channels, ***the communication format to single bit exchanges for timing****, symbol length to narrow (ultra wideband) pulses, and protocols to error-tolerant versions. These restrictions increase the technical challenge of implementing secure distance bounding. "*

Based on our results, these conclusions do not hold.

[CL06] J. Clulow, G. P. Hancke, M. G. Kuhn, T. Moore,
So Near and Yet So Far: Distance-Bounding Attacks in Wireless Networks, ESAS 2006

Were Brands and Chaum [BC] and [CL06] Right?

[CL06]:

- multi-bit challenge-response distance bounding and protocols of Hu/Perrig/Johnson, Sastry/ Shankar and Capkun/Hubaux that use them are vulnerable to ED/LC attacks

Our work [Singh17] shows that this is not correct:

- multi-bit constructions and therefore the above protocols are secure if an appropriate physical layer is chosen.
- None of these protocols assumed a particular physical layer and therefore the attacks claimed in [CL06] do not hold except under the physical layer assumed in [CL06].

[CL06]:

- Symbol length is restricted to single UWB pulses and protocols to error tolerant versions

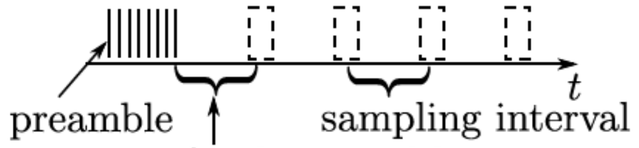
Our work [Singh17] shows that this is not correct:

- Multi-pulse and multi-bit constructions are possible **(and preferable)**
- Error tolerance is not necessary at the protocol level, as it follows from the robust physical layer

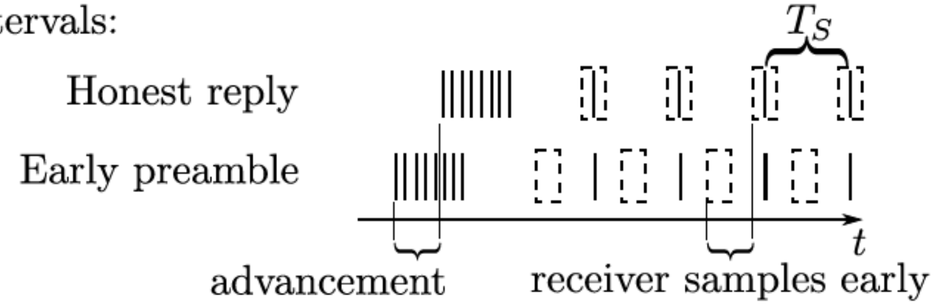
[Singh17] M. Singh, P. Leu, S. Capkun, UWB with Pulse Reordering: Securing Ranging against Relay and Physical Layer Attacks, EPrint Archive, 2017

Direct Time Measurement vs “Distance Commitment”

The timing of the preamble determines the sampling points for the symbols:



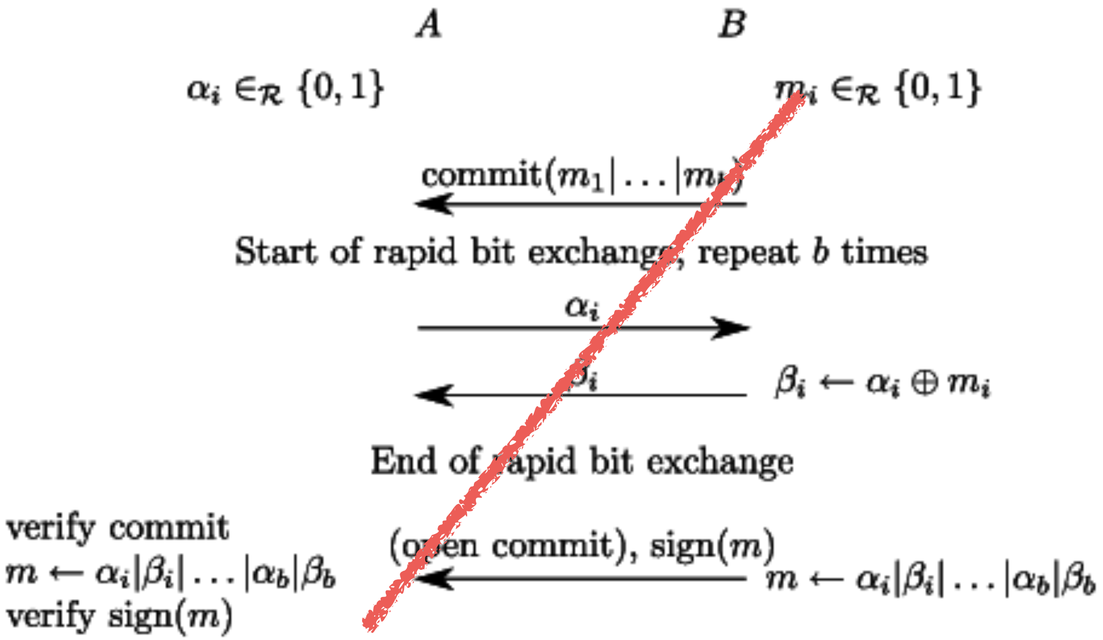
Advancing the preamble also advances the receiver’s sampling intervals:

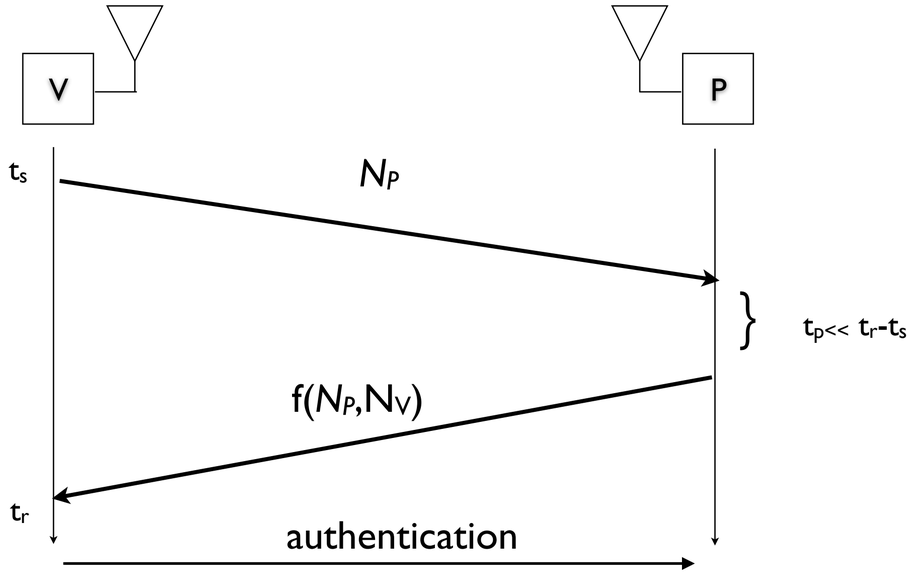


Allows for the prover to respond before it even decodes the received symbol / bit. [Tipp15, Singh17]

=> distance fraud can be implemented with multi-pulse symbols and multi-bit nonces

Do we Need Rapid Bit Exchange?





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

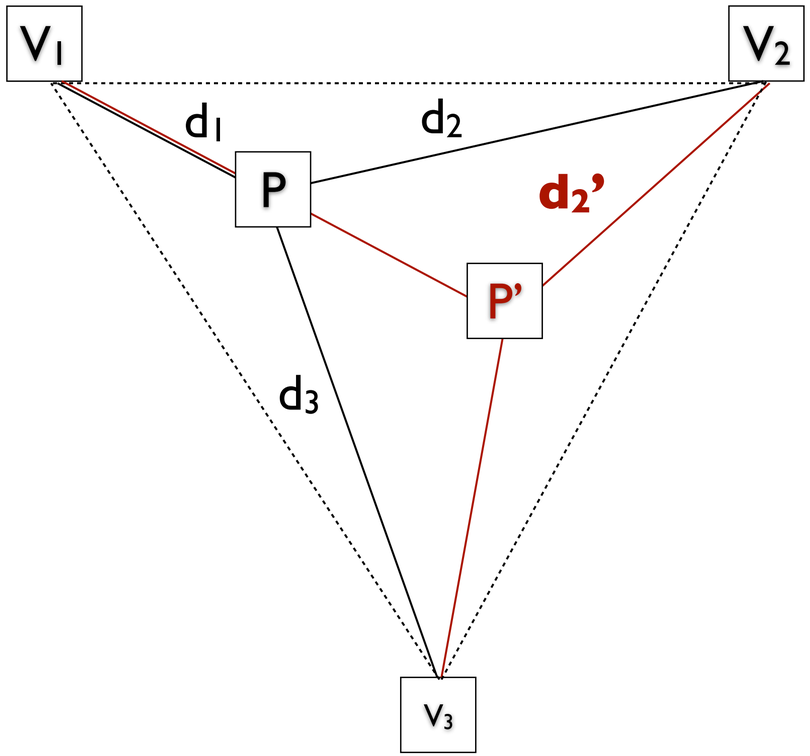
(illustration - different protocols can be supported)

No - single round distance measurement over a single message is both secure and preferable.

Secure Positioning

Now that we can do secure distance measurement with **“unlimited range”** (i.e., attacker cannot reduce the measured distance)

=> Secure Positioning through **Verifiable Multilateration** [Cap05]



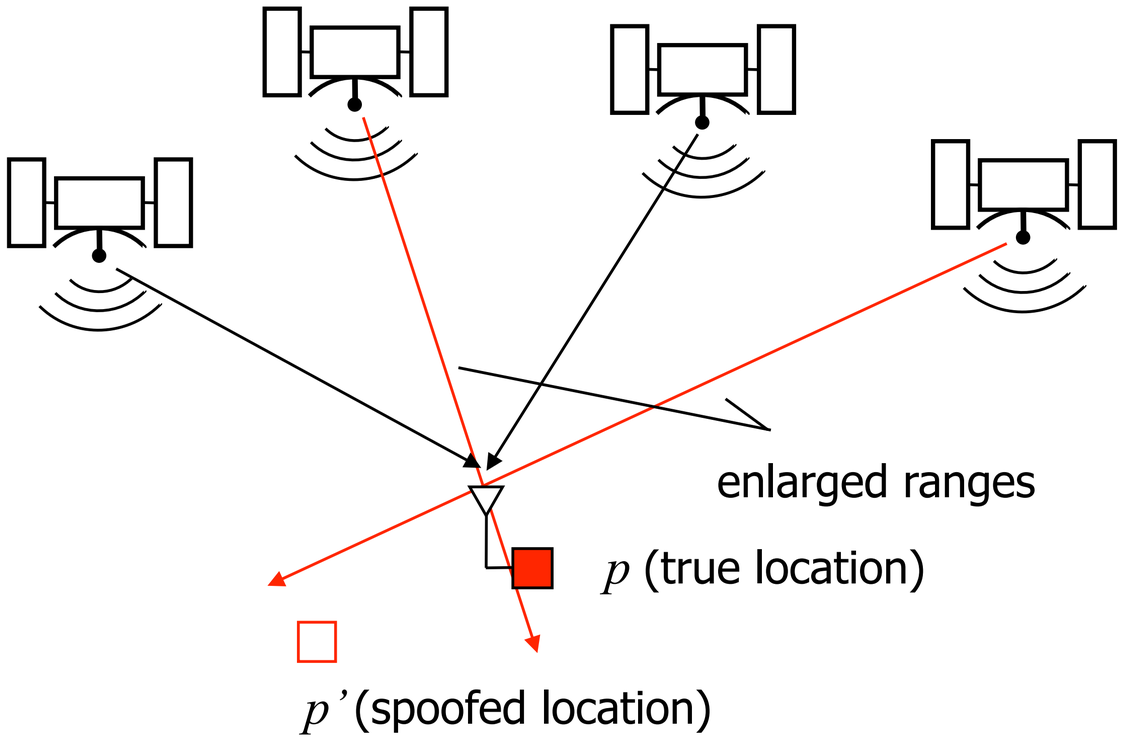
P→P’ => d2’<d2

[Cap05] S.Capkun, J.P. Hubaux,
Secure positioning in wireless networks, JSAC 2006/ INFOCOM 2005

Do we Need Distance Bounding for Secure Positioning?

Can one have secure positioning with unidirectional (broadcast) systems like GPS?

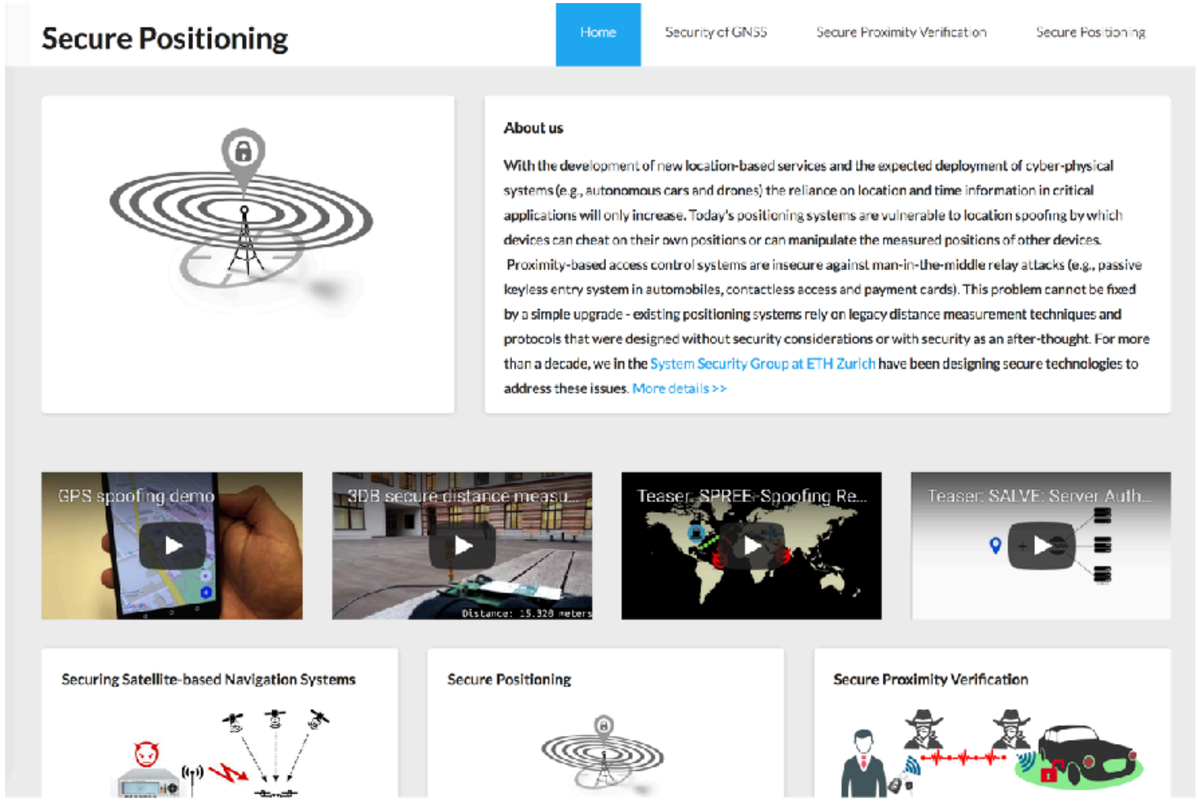
- In principle not
- The attacker can in principle always delay / generate signals



More Information

- www.zisc.ethz.ch
- https://securepositioning.com/

- capkuns@inf.ethz.ch



ETH ZISC Zurich Information Security & Privacy Center

erc European Research Council

3db

ETH zürich