Wireless Network Security

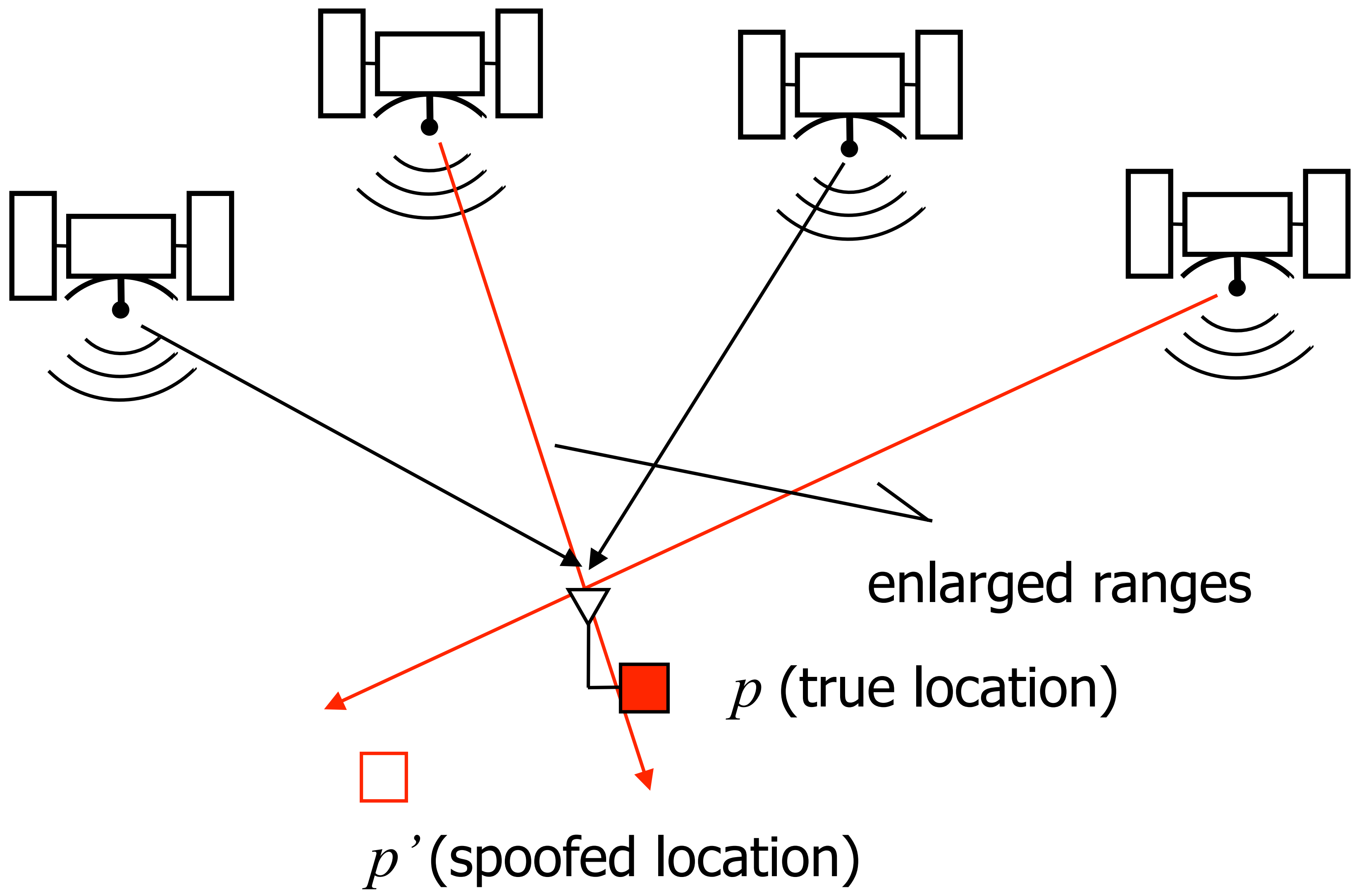
Lecture 5

Distance Bounding
Secure Ranging
Secure Proximity Verification

Srdjan Čapkun

GPS Spoofing can be Prevented in a number of Scenarios but …

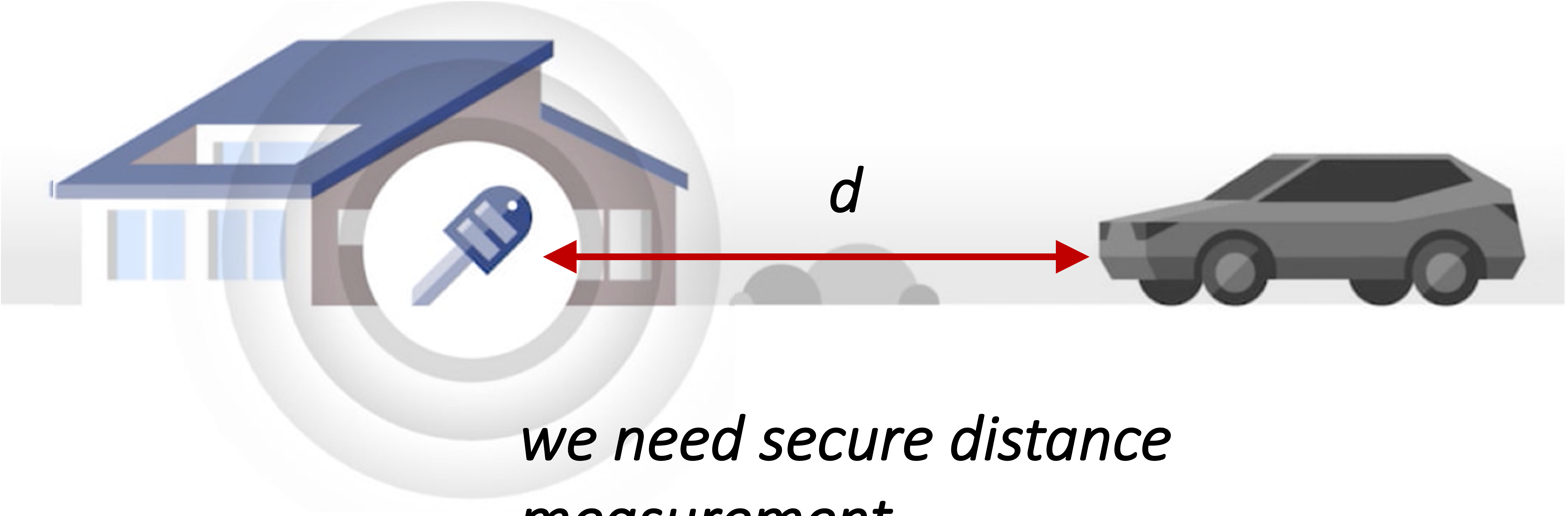
Broadcast systems like GPS cannot be ***fully*** *secured*
(ASSUMING DY ATTACKER) !!!



- Secure positioning requires either:
  - bidirectional communication ***or***
  - communication from the device to the infrastructure

Recommended Readings

- **Are We Really Close? Verifying Proximity in Wireless Systems.** *Aanjhan Ranganathan, Srdjan Capkun* (IEEE Security and Privacy Magazine)
- **Distance Bounding Protocols.** *Stefan Brands and David Chaum.* (extended abstract - Eurocrypt 1993)
- **Verifiable Multilateration.** *S. Capkun, J. P. Hubaux.* **(**Secure positioning in wireless networks, IEEE Journal on Selected Areas in Communications: Special Issue on Security in Wireless Ad Hoc Networks, February 2006.)



we need secure distance measurement

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


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

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

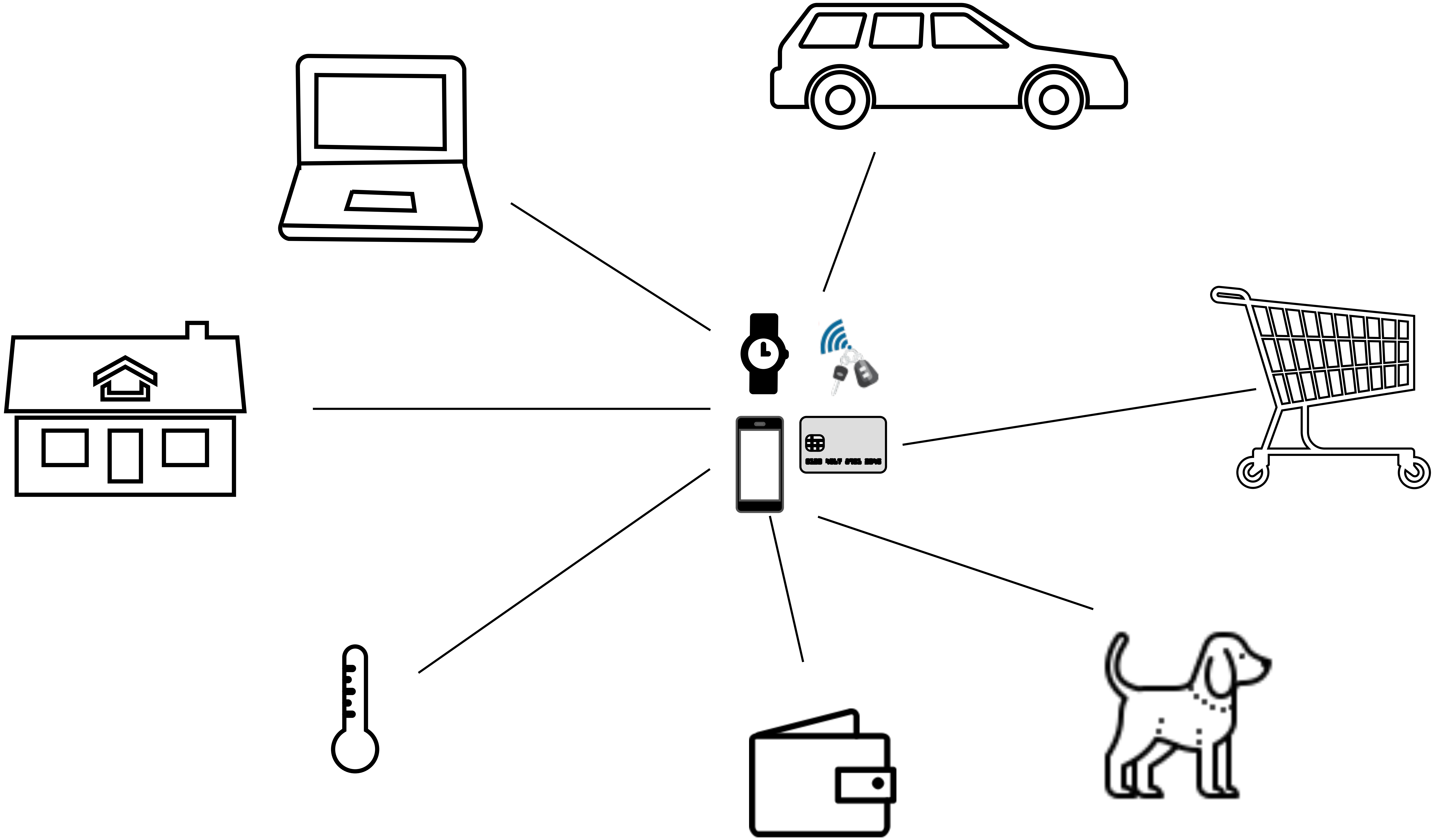
QIHOO 360 TEAM UNICORN

need to know where other objects/people are

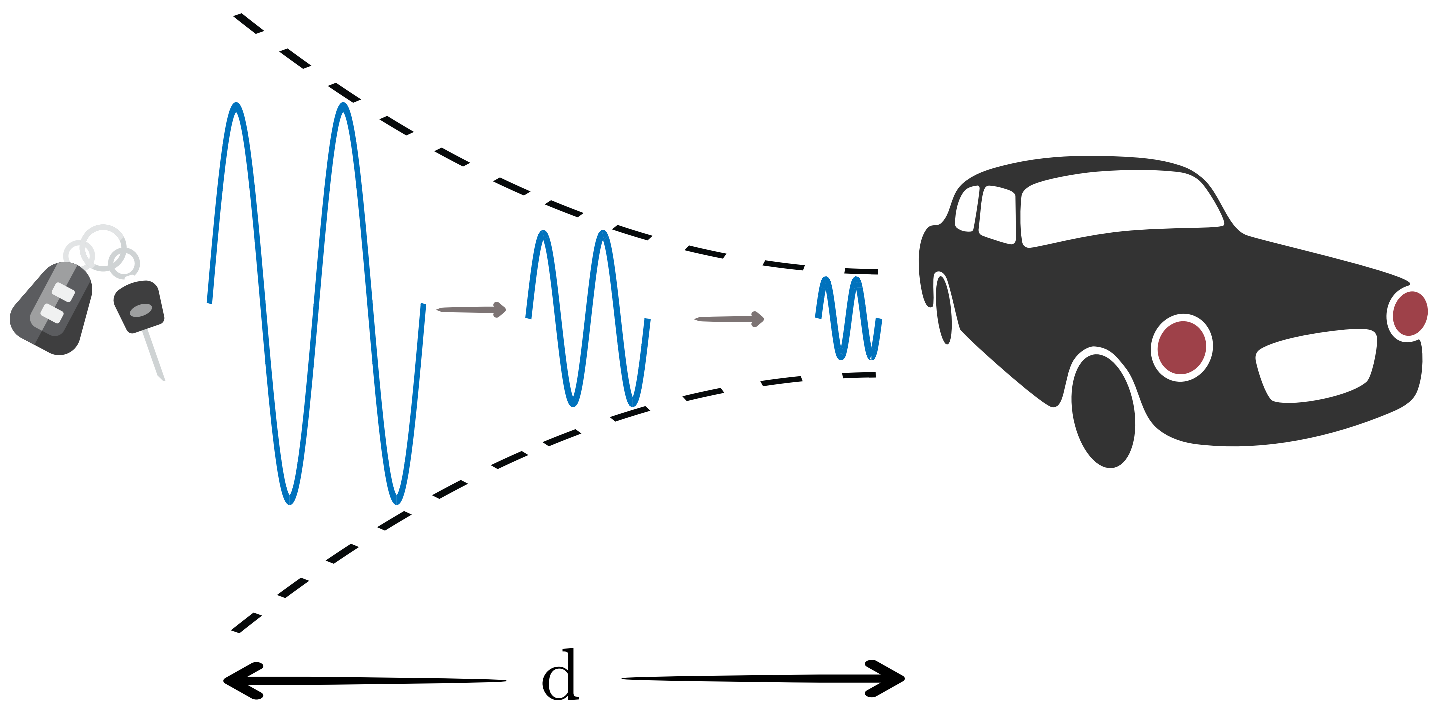
need to know where we are

securely

Applications

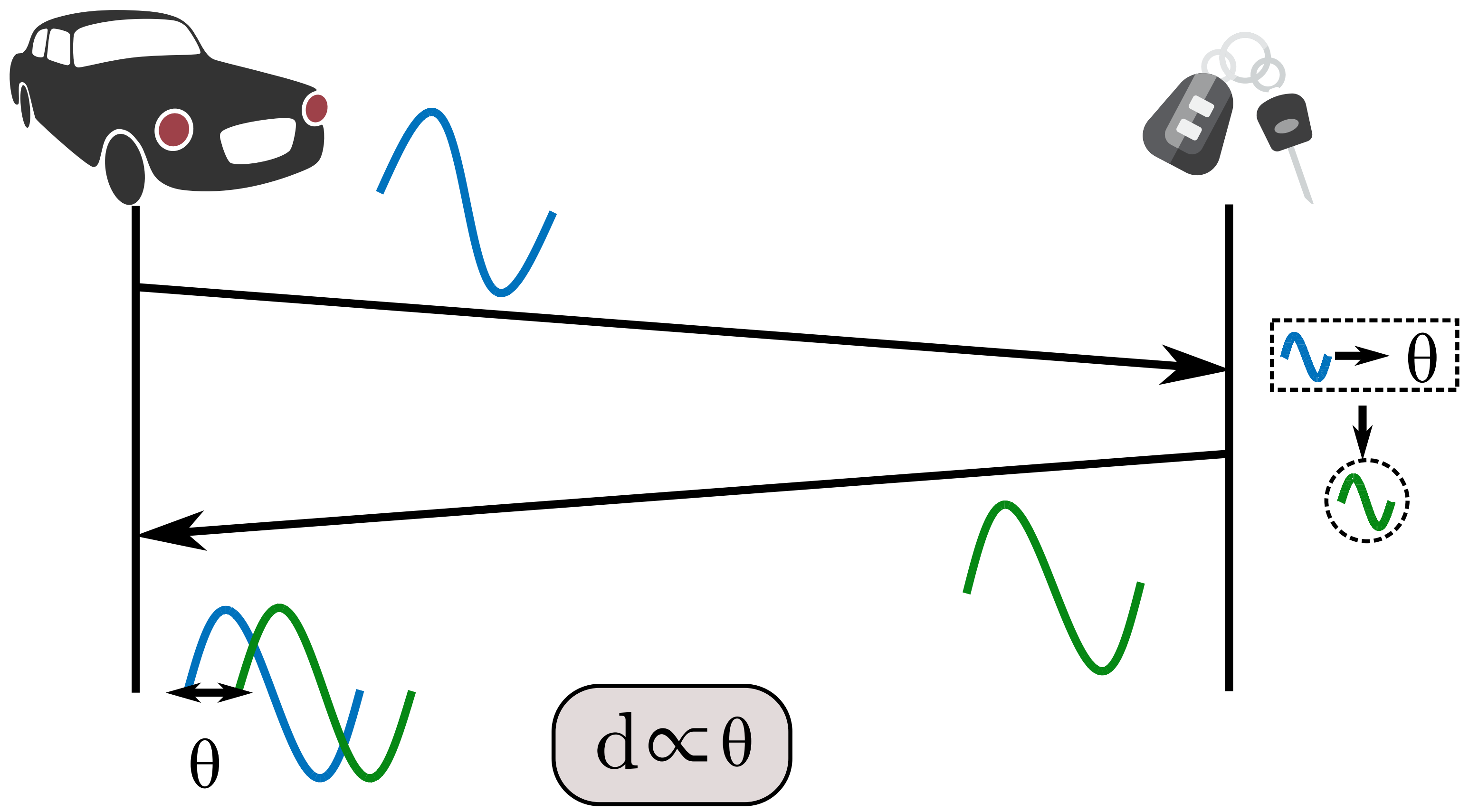


Estimating Proximity



Received Signal Strength

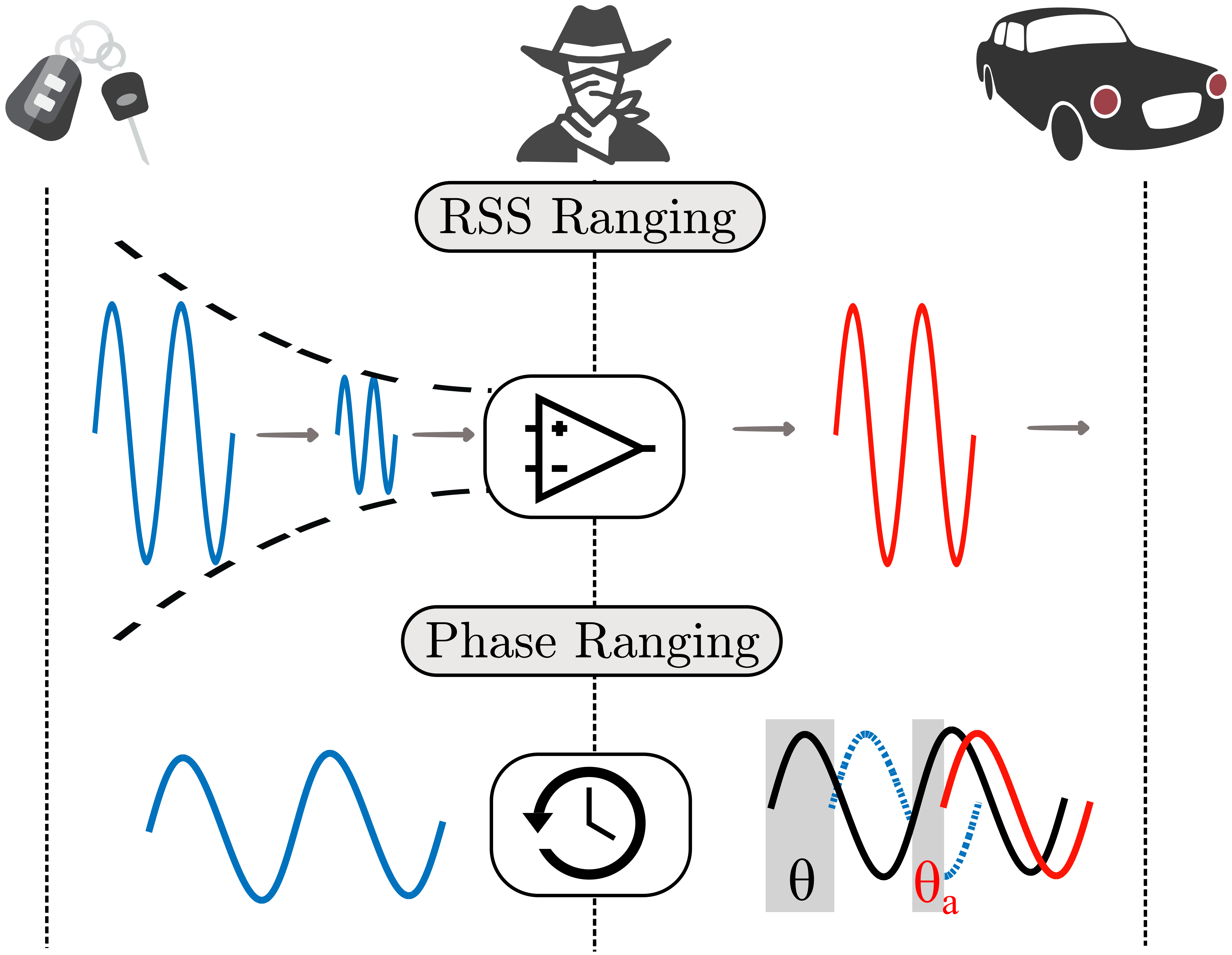
$$d = \frac{\lambda}{4\pi}\sqrt{\frac{P_t G_t G_r}{P_r}}$$



Carrier Phase Ranging

$$d = \frac{c}{2 \cdot f} \cdot \left(\frac{\theta}{2\pi} + n\right)$$

Attacking Proximity

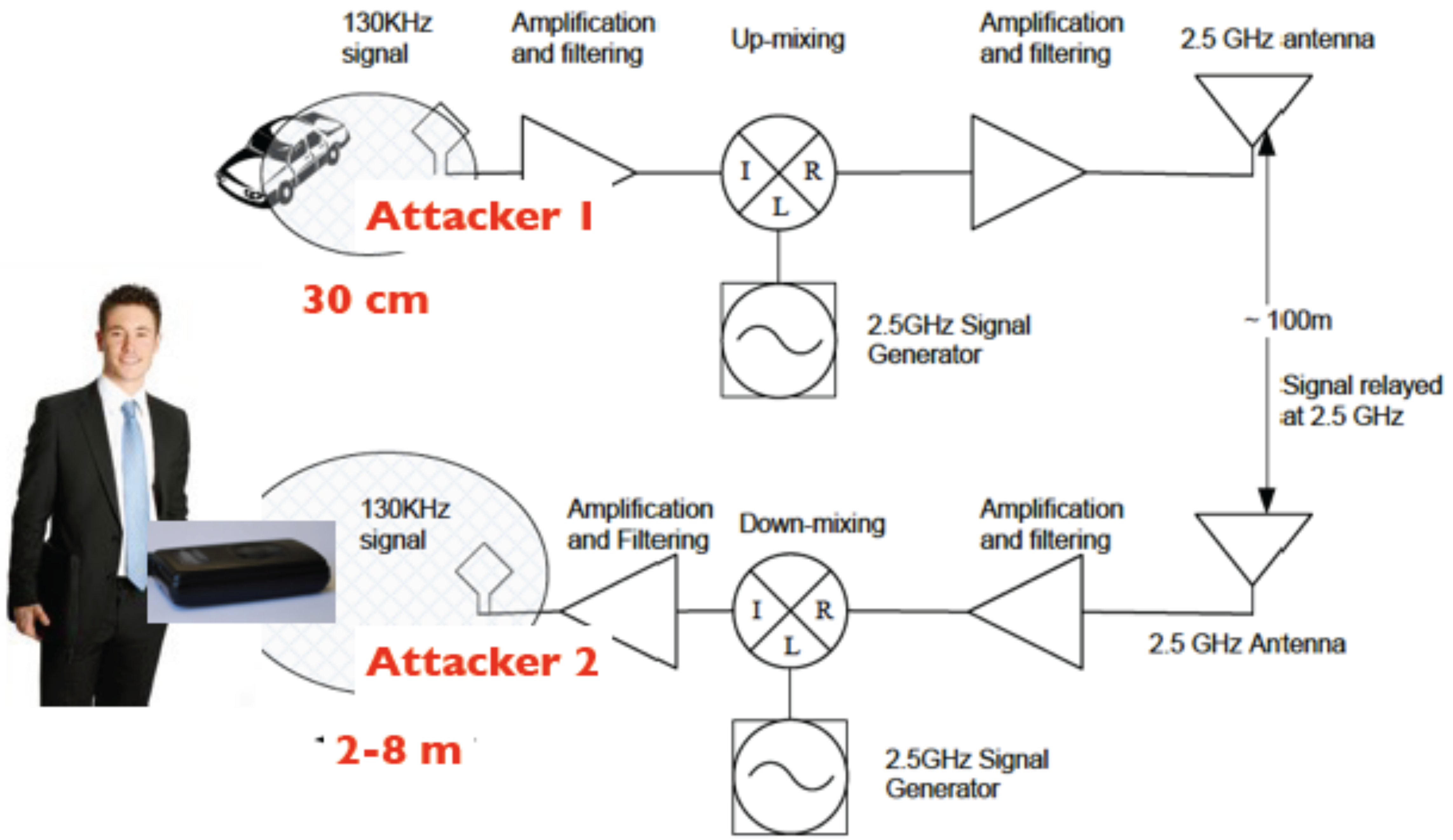


Example: PKES

(deployed by all major car manufacturers)

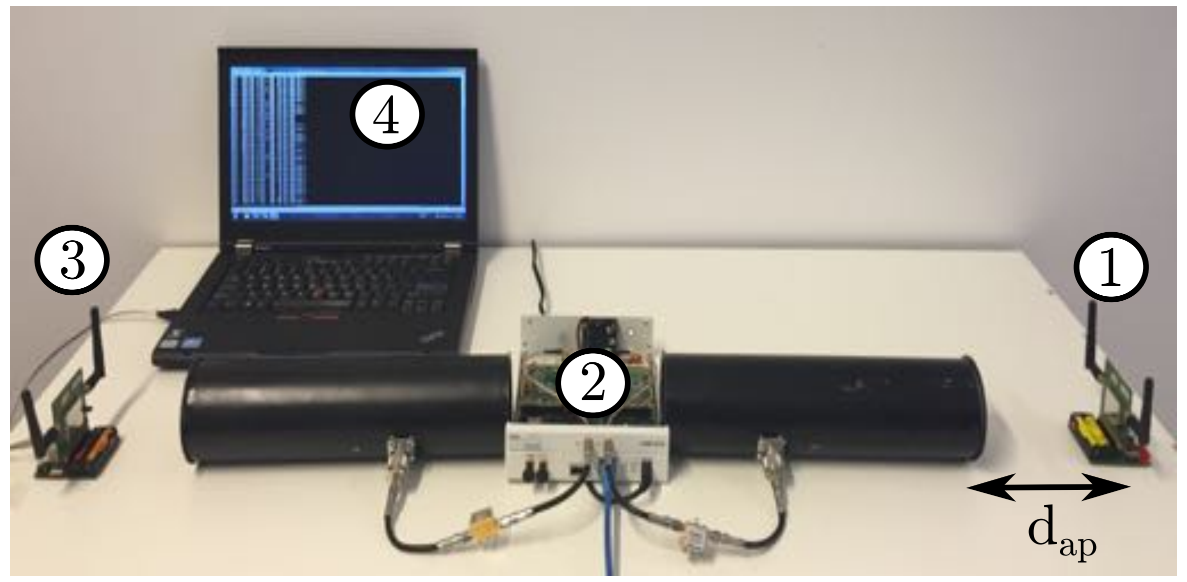
PKES: Key is “in pocket” - car opens when the key is *close to the car*

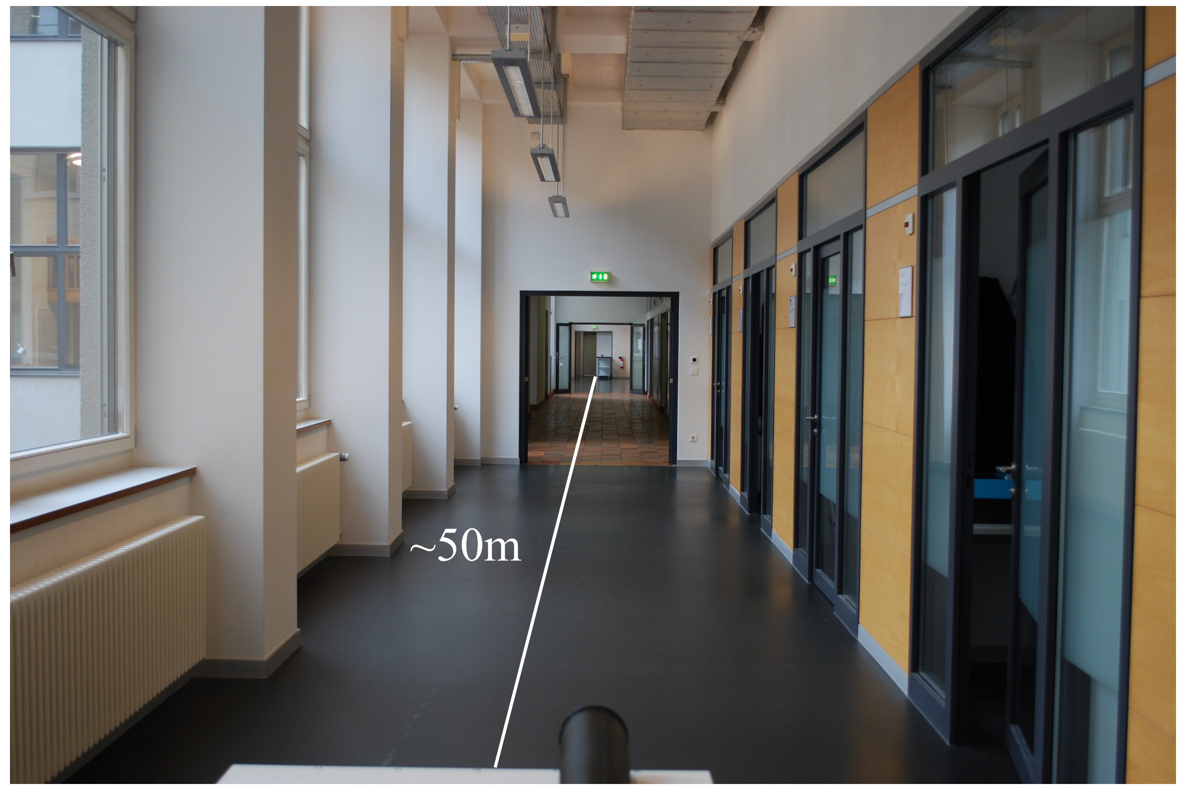
Relay attack [FrancillonNDSS11]

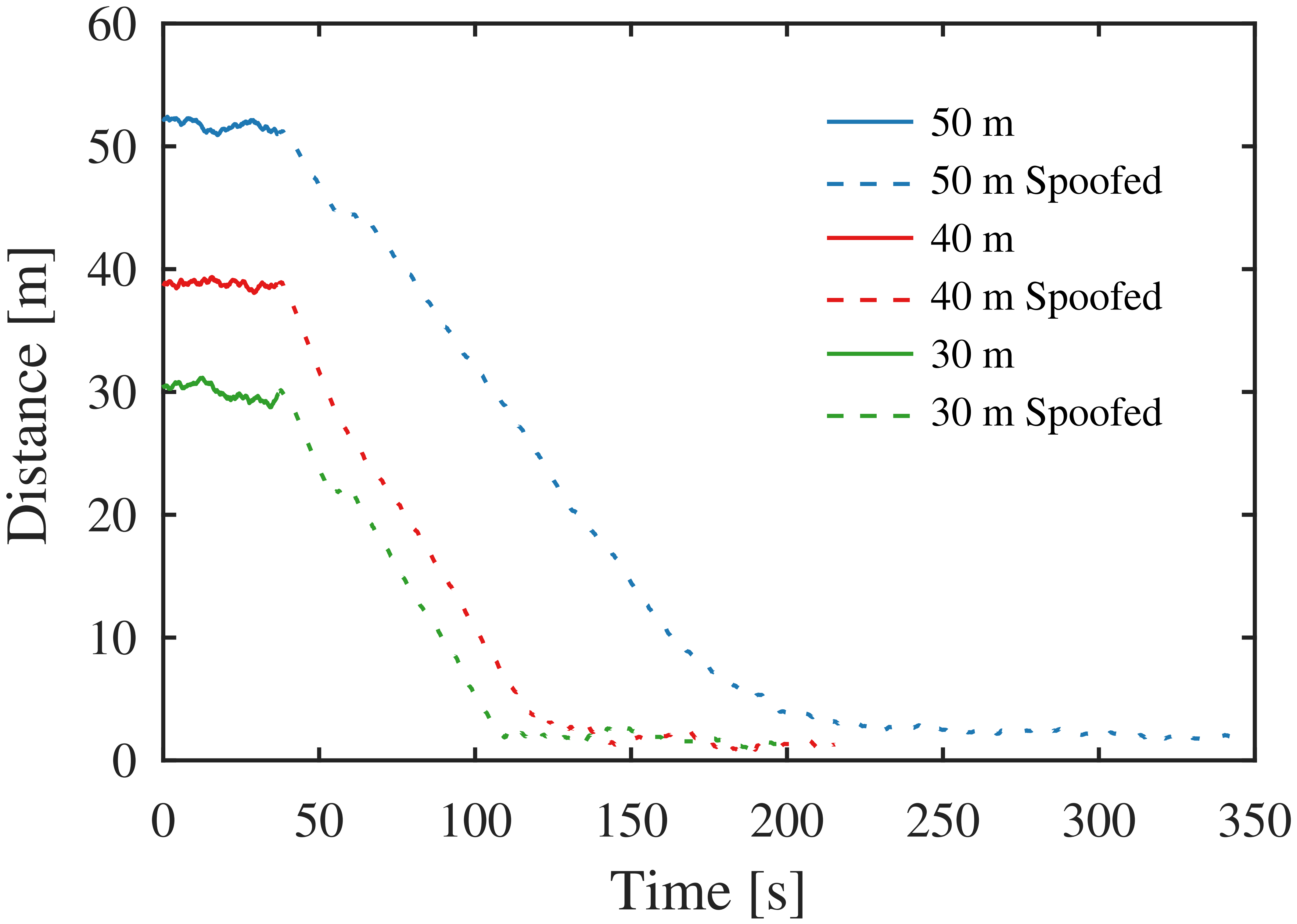


- Tested on 10 car models from 8 manufacturers
- Manufacturers are now redesigning Entry and Start Systems

Attacking Phase Ranging Systems





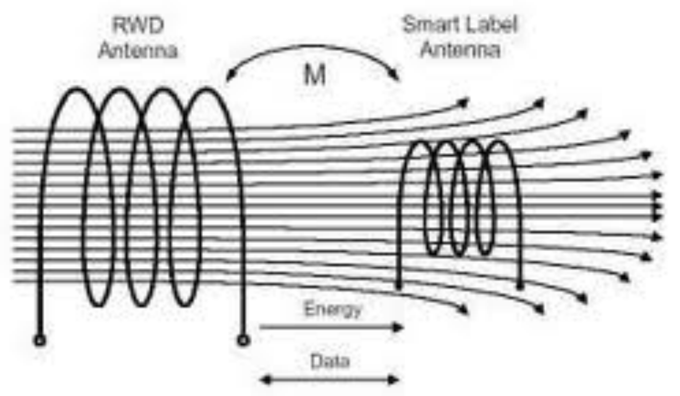


Hildur Ólafsdóttir, Aanjhan Ranganathan, and Srdjan Capkun. "On the Security of Carrier Phase-based Ranging." In *International Conference on Cryptographic Hardware and Embedded Systems*, 2017

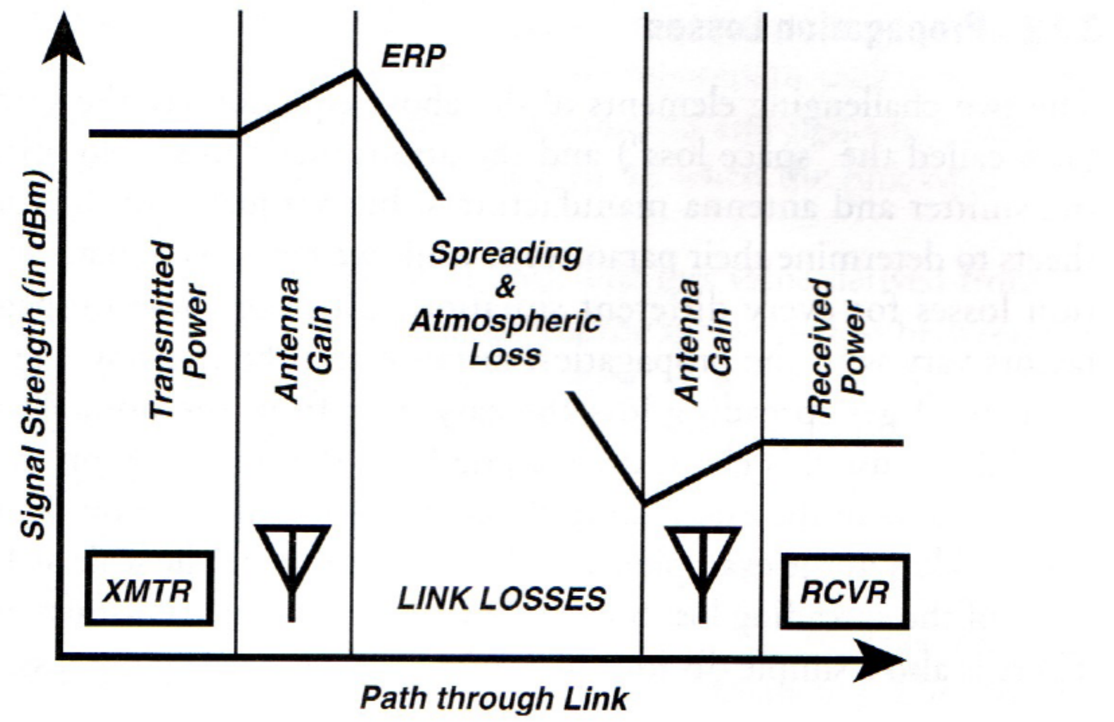
Secure Proximity Verification?

Secure Proximity Verification

- Inductive Coupling
- Radio Communication



Communication DOES NOT imply physical proximity.
(in adversarial environments)



To calculate the received signal level (in dBm), add the transmitting antenna gain (in dB), subtract the link losses (in dB), and add the receiving antenna gain (in dB) to the transmitter power (in dBm).

©D. Adamy, A First Course on Electronic Warfare

As shown in PKES systems, relying on the reduced communication range is either not convenient or not secure.

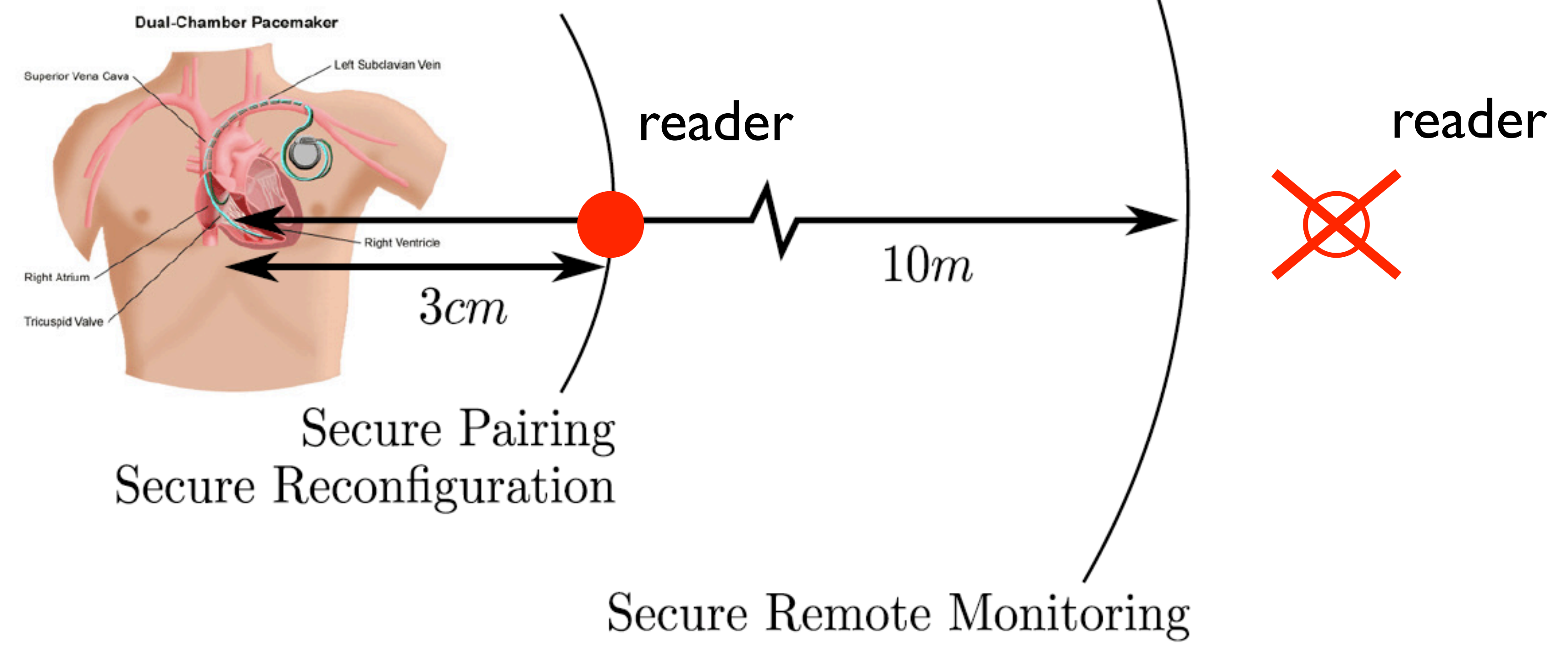
- *We need a difficult problem to hold on to.*

Solution: Secure Proximity Verification ***using secure ranging***.

Secure Proximity Verification

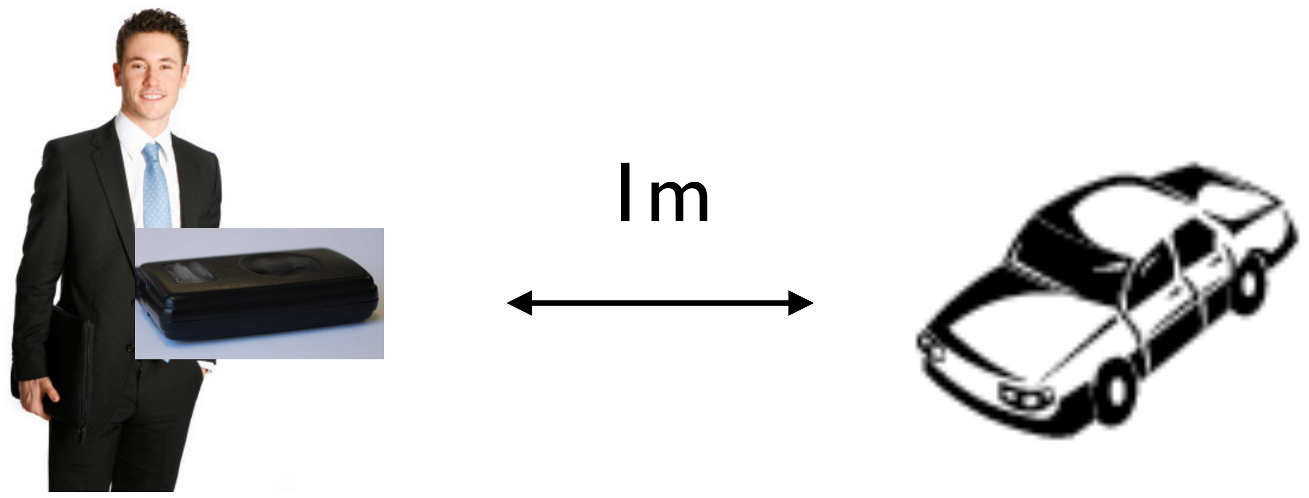
One (untrusted) device wants to *prove to be close* to another device.

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

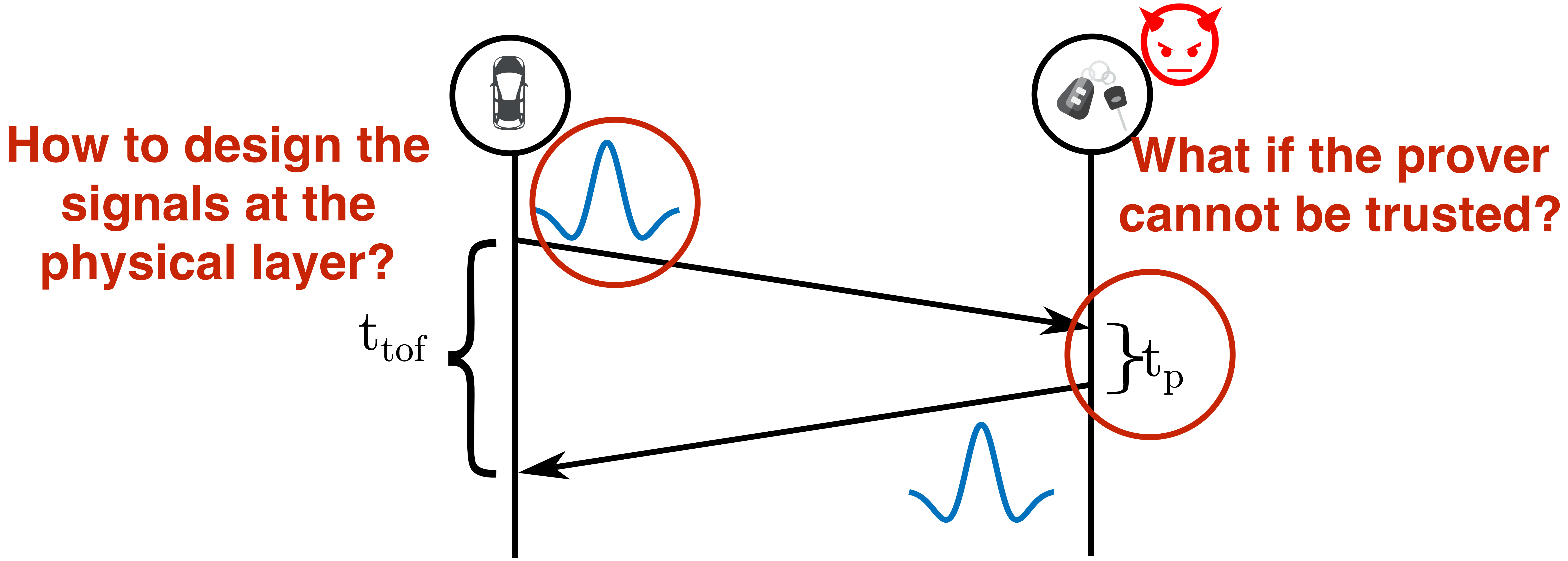


Two devices want to *verify if they are indeed close.*

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



Estimating Proximity using Time of Flight



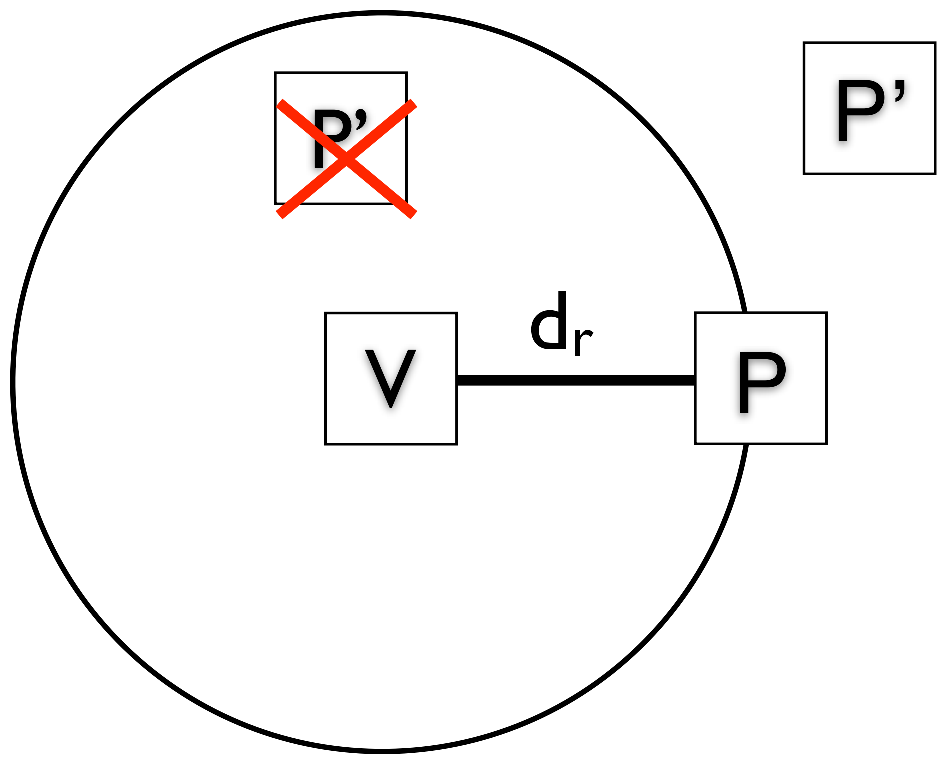
$$d = c * (t_{tof} - t_p) / 2$$

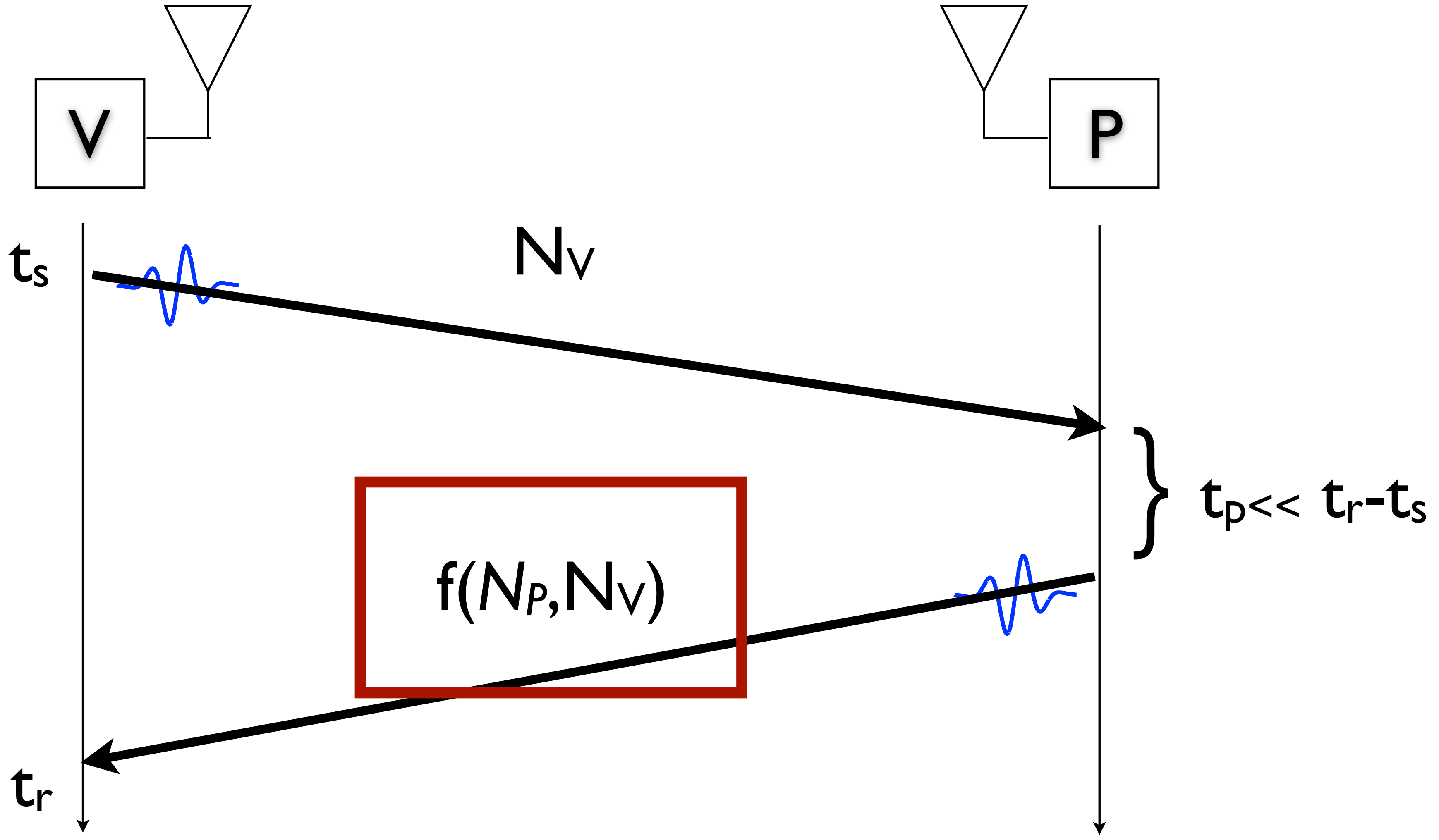
Can an attacker reduce time?

Manipulating time is harder than changing signal strength or phase

Distance Bounding [BrandsChaum93]

Basic Idea



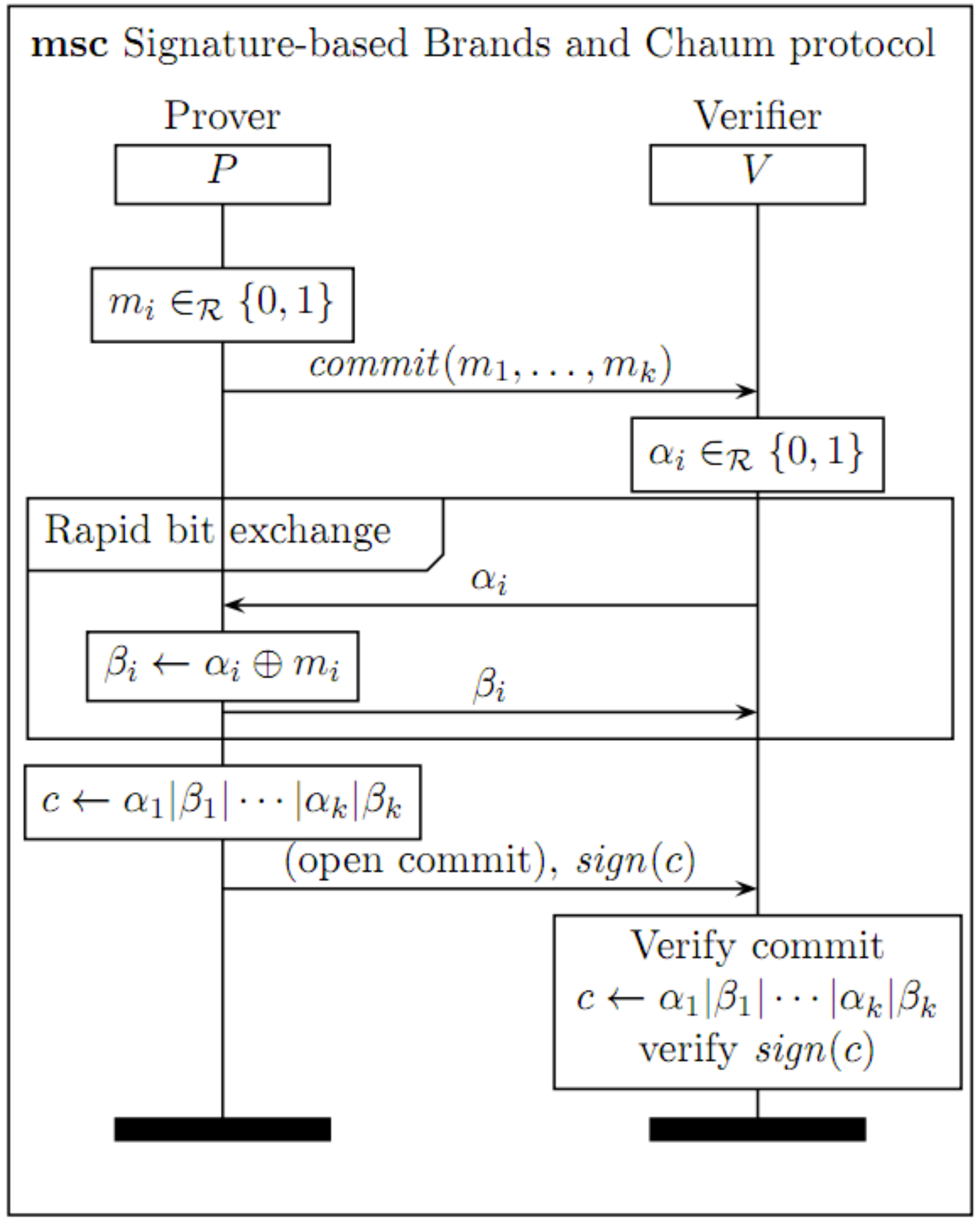


$d = (t_r - t_s - t_P)c/2$

Property:

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

Distance Bounding [BrandsChaum93]



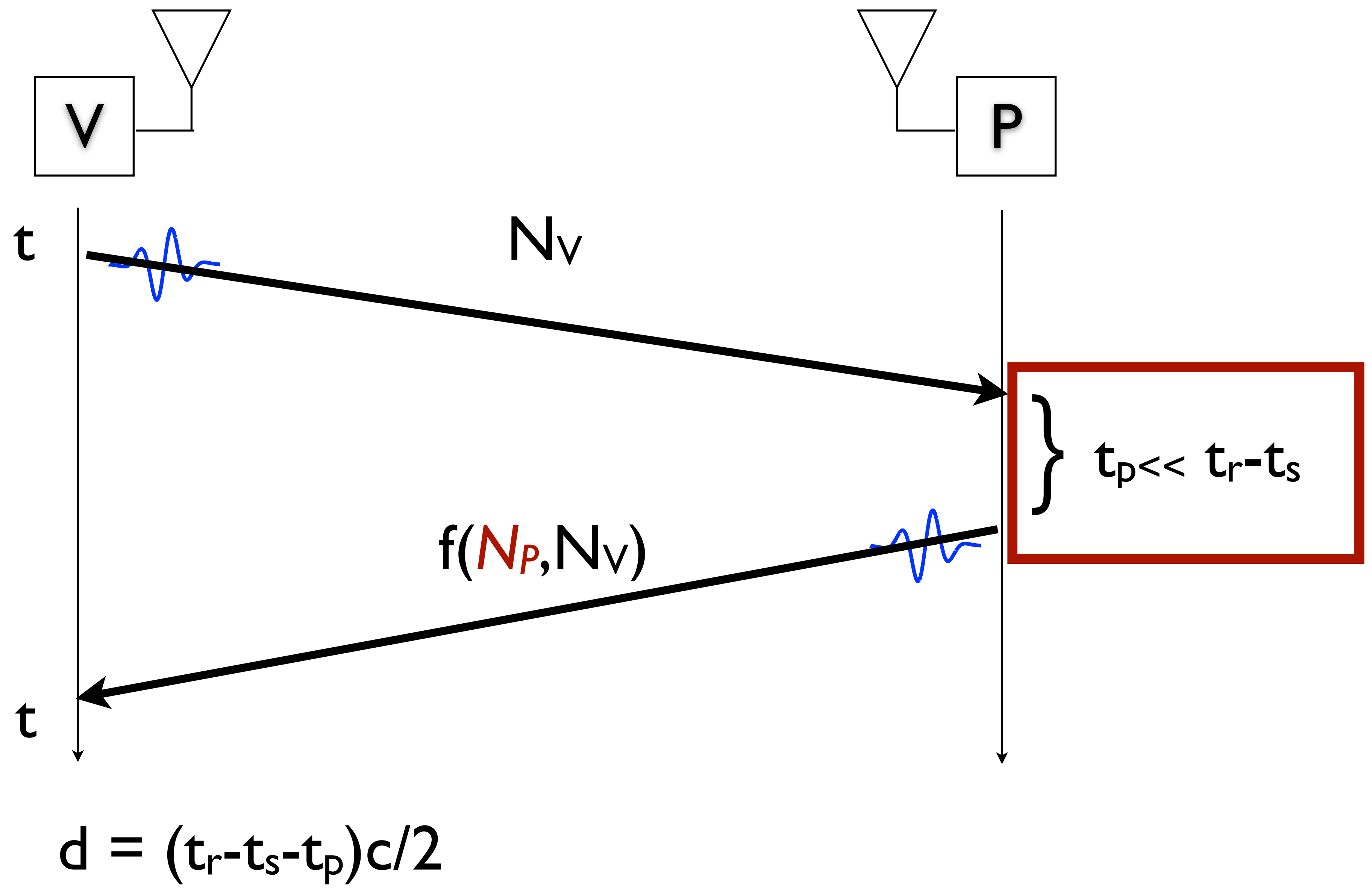
Distance Bounding: *f() and t_p*

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:

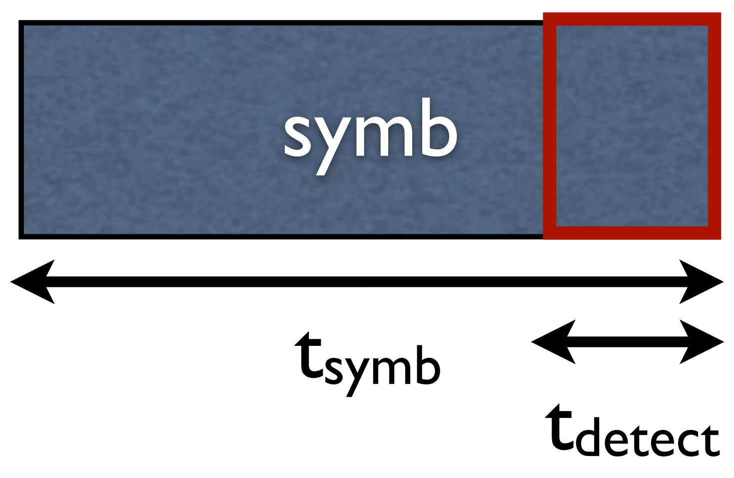
we do not control the prover



Distance Bounding: *symbols*

Assuming $|N_V|$=1bit, the symbols should be short as well

- short compared to the required accuracy / security
- Early Detection
- Late Commit
- Note: *channel spread does not help*



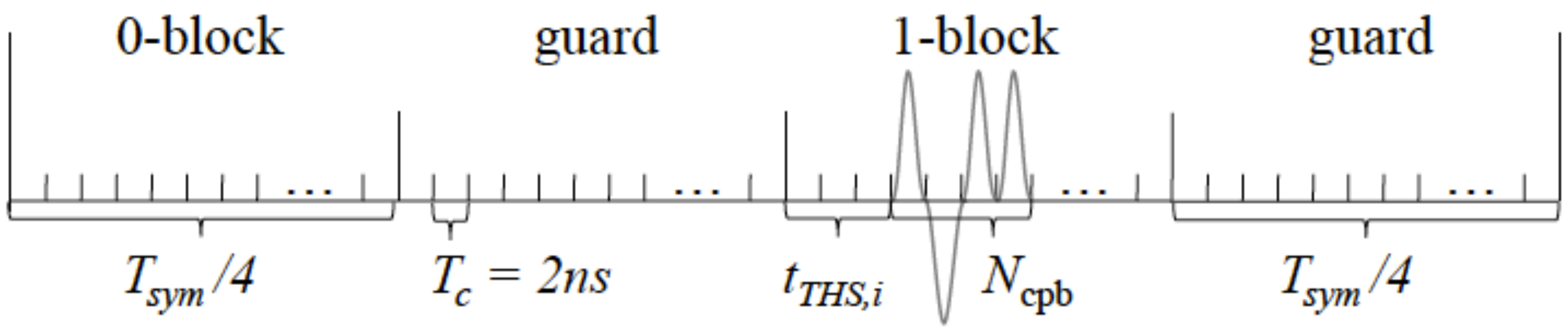
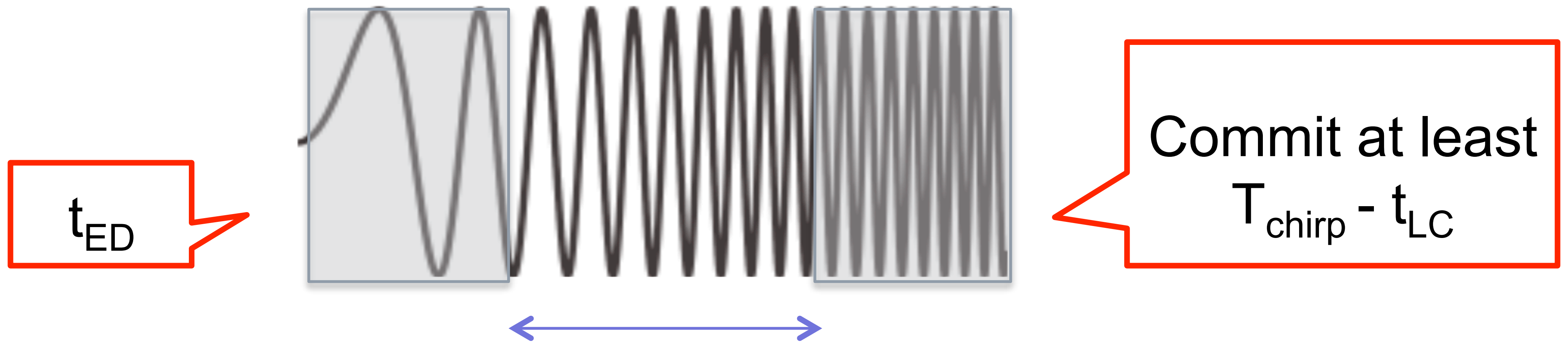


Figure 4.2: IEEE 802.15.4a data symbol structure [Poturalski2011]

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." (WiSe

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(N_V); h(N_V); mac(N_V); E(N_V); ... => 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)

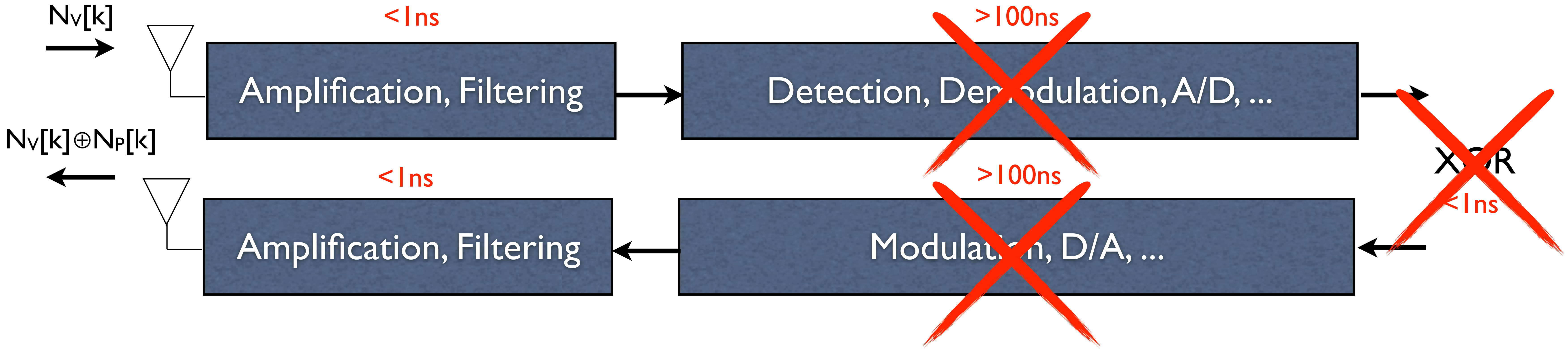
[BethDesmedt] sign(); h(); mac(); E(); ... => t_p >> ns

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

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

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

... > 20 proposed protocols



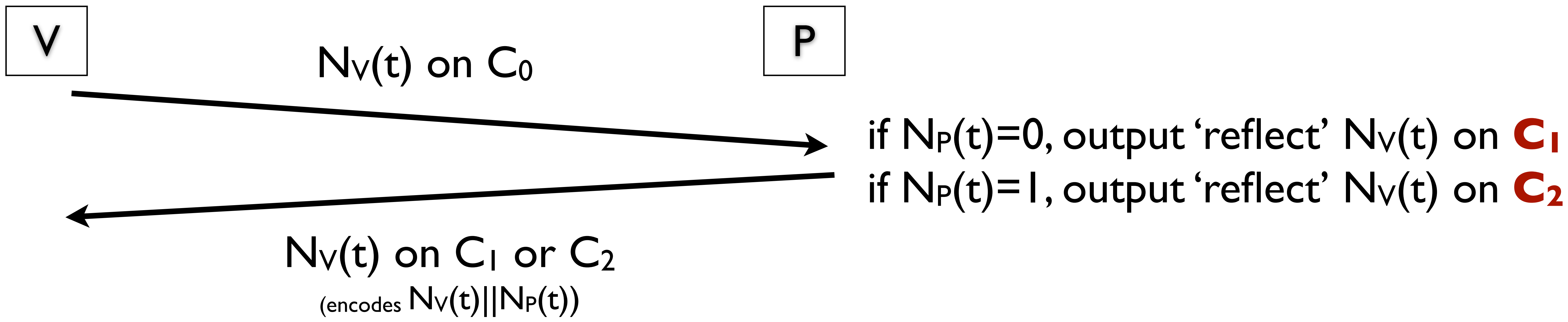
Can we use functions that don't require interpretation (demodulation) Nv ?

A new Function: CRCS

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)

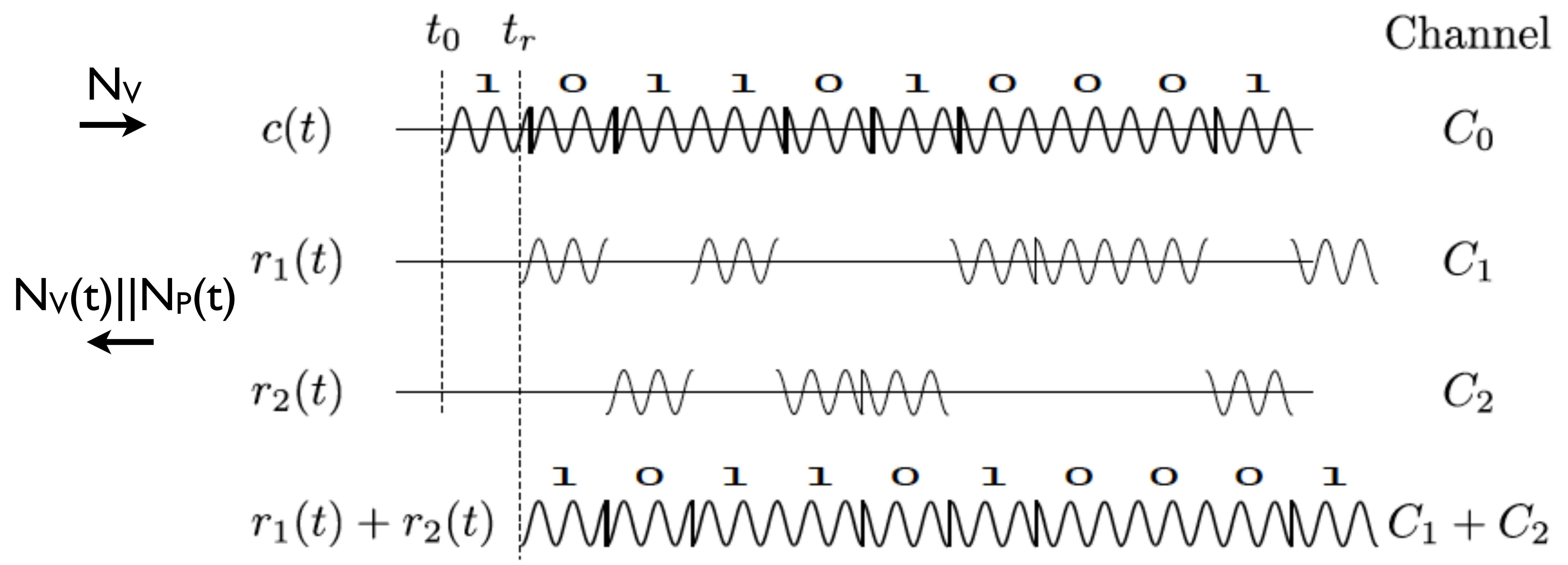


A new Function: CRCS

Challenge Reflection with Channel Selection

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

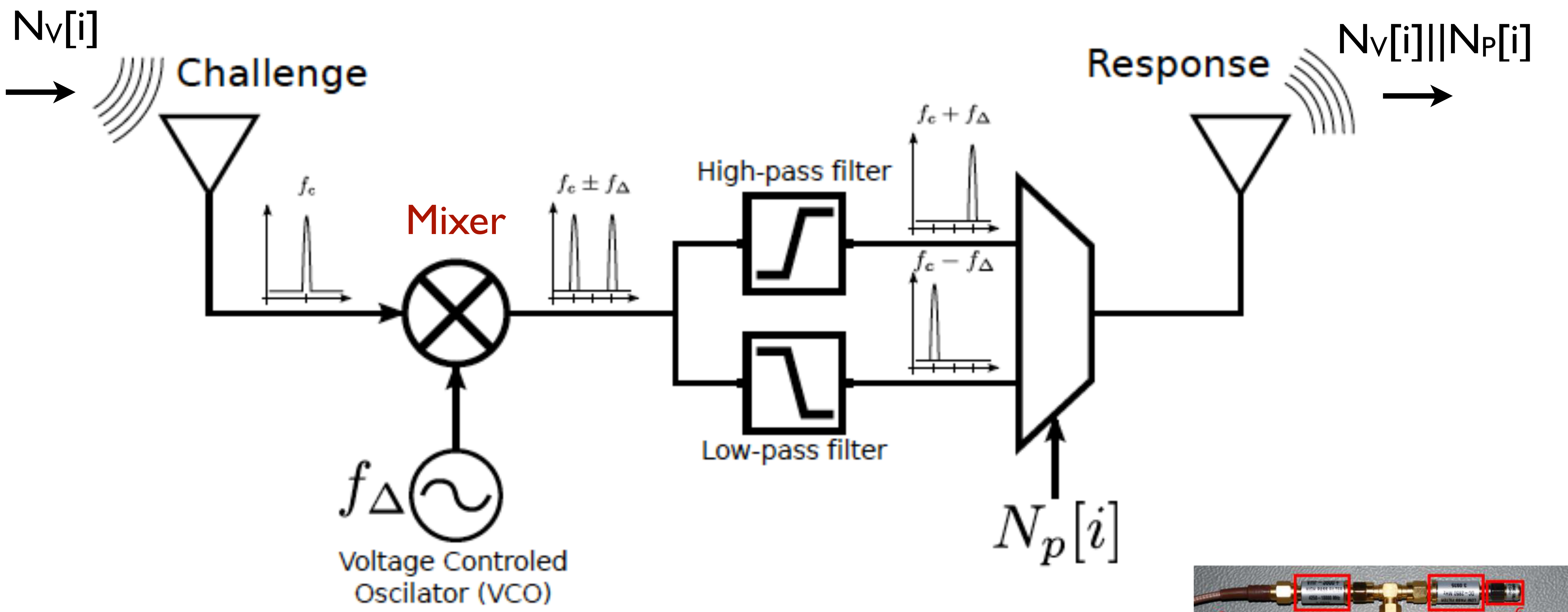
Main idea (C_0,C_1,C_2 are channels)

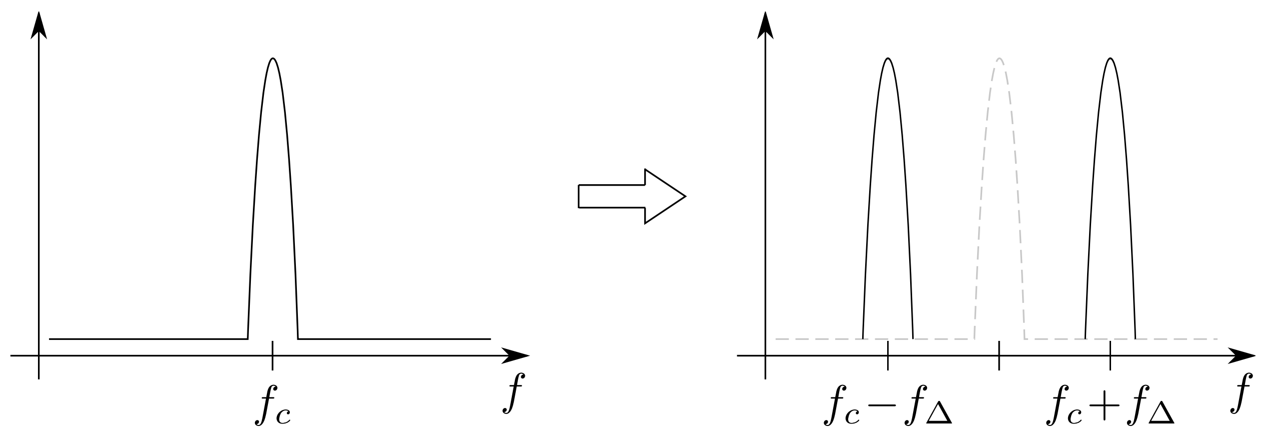


A new Function: CRCS

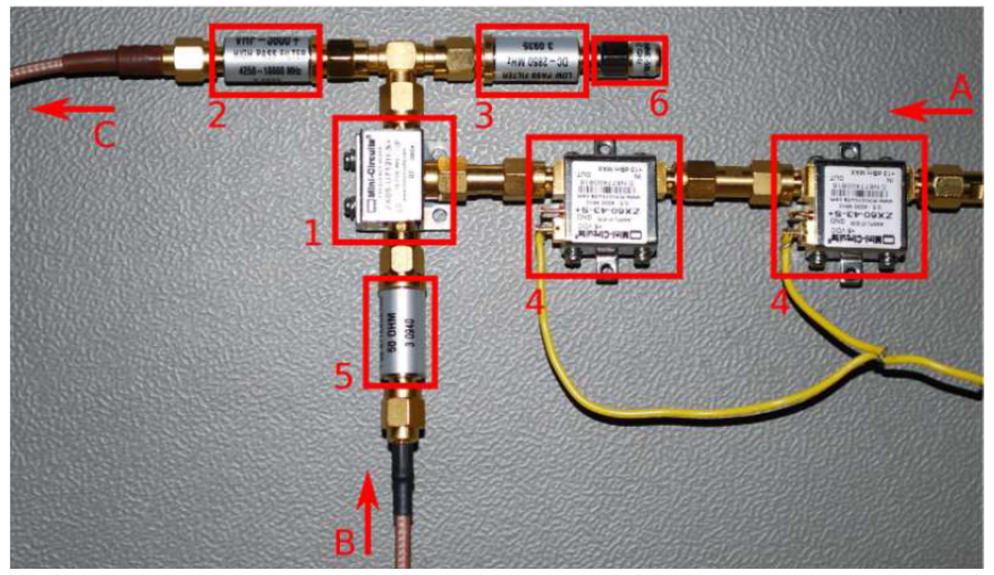
Implementation of CRCS

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





Mixer up+down converts the input signal

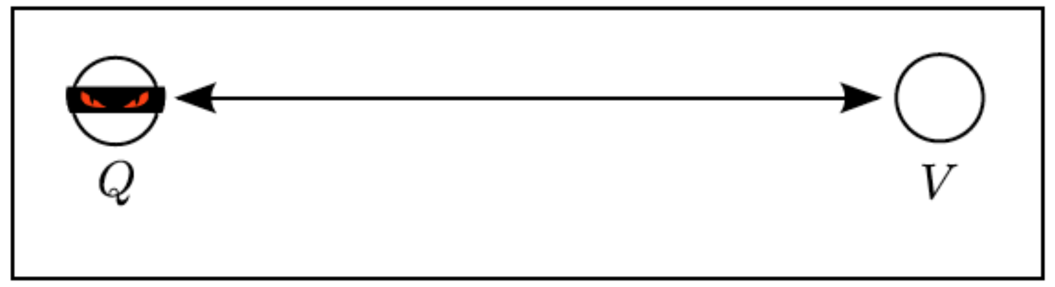


Two basic Attacks on DB protocols

Distance Fraud

- dishonest prover pretends to be closer to the verifier
- “pacemaker scenario”

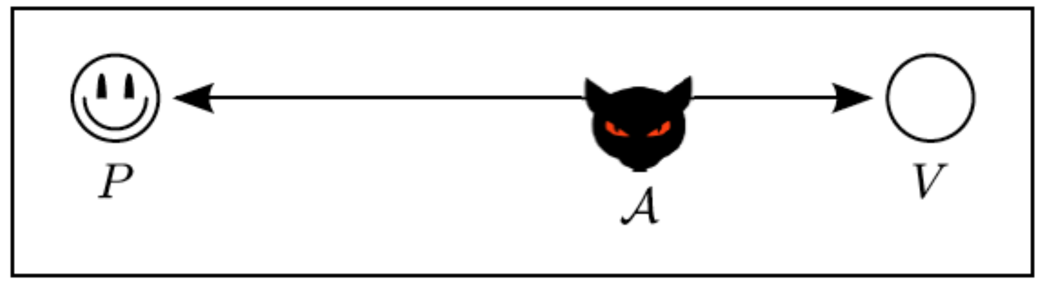
Distance Fraud



Mafia Fraud

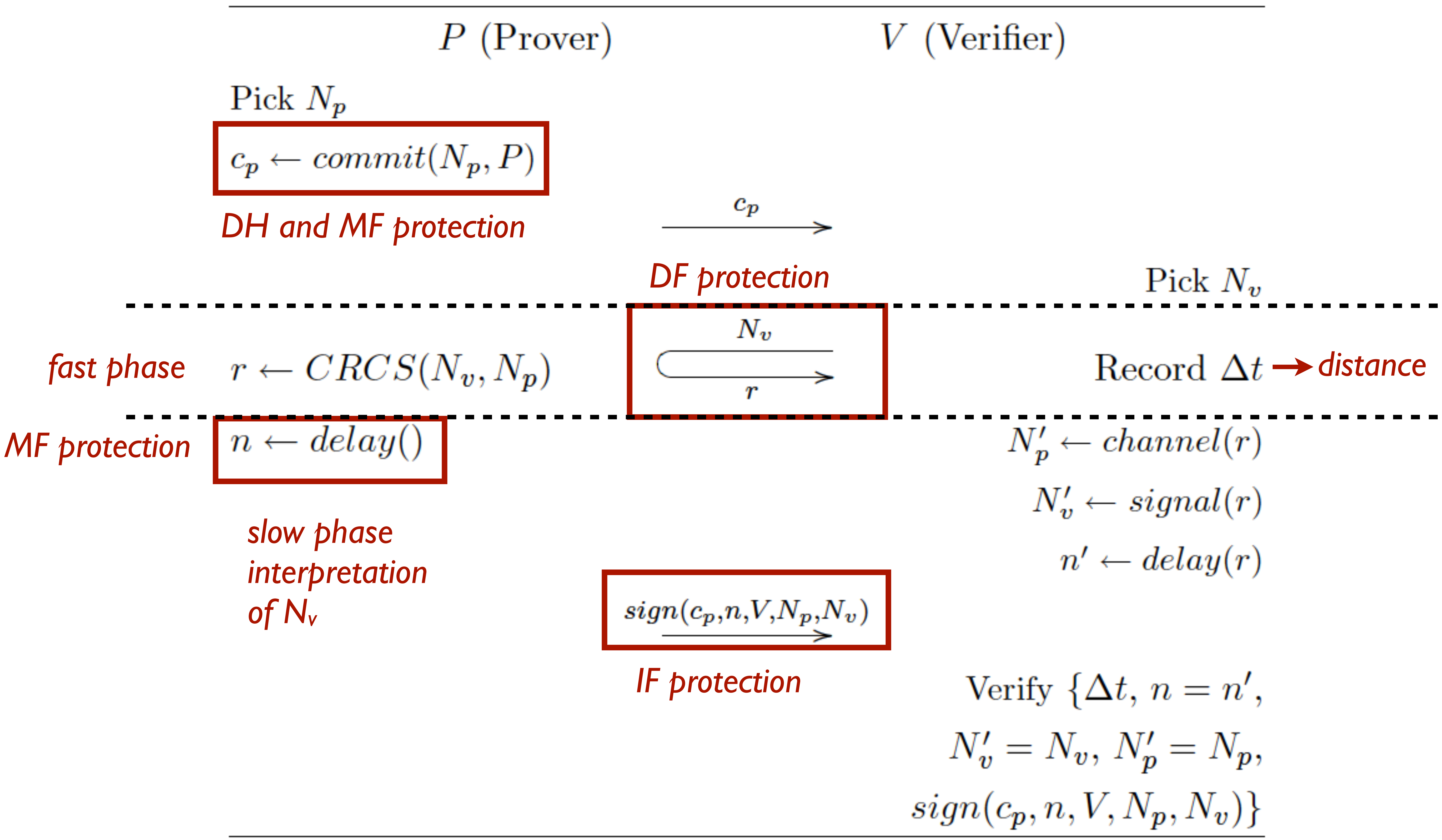
- honest prover
- attacker convinces verifier and prover that they are closer
- relay attack (“car and key scenario)

Mafia Fraud



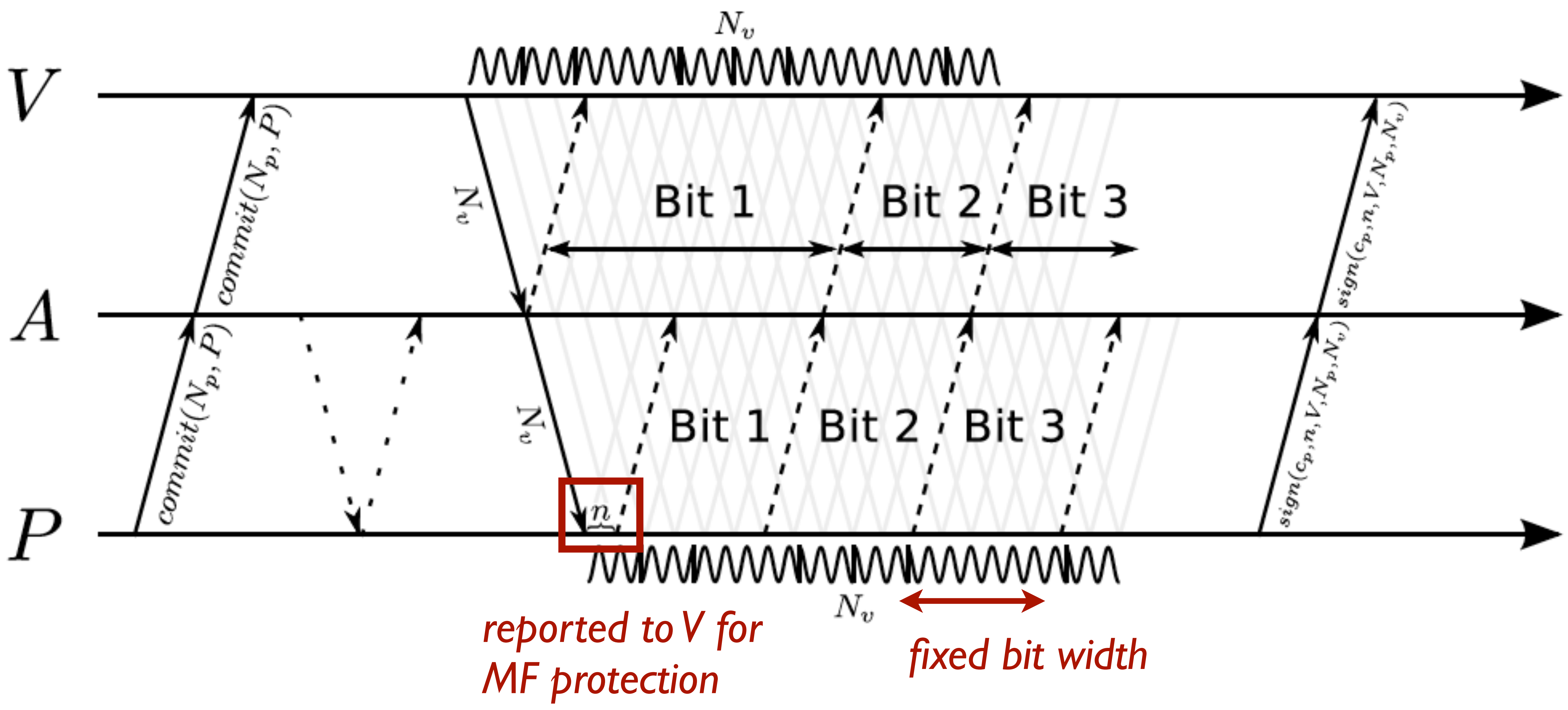
CRCS

CRCS-based DB protocol *(vs Distance and Mafia Fraud)*



A new Function: CRCS

Mafia Fraud Detection *(physical layer)*



MF attack: $\frac{1}{2^{|N_p|}}$; DF atta $\frac{1}{2^{|N_v|}}$

CRCS eliminates early detection, late commit attacks

Ongoing work on CRCS

Using CRCS the prover also reflects noise
=> CRCS increases complexity of the Verifier

In essence, CRCS trades

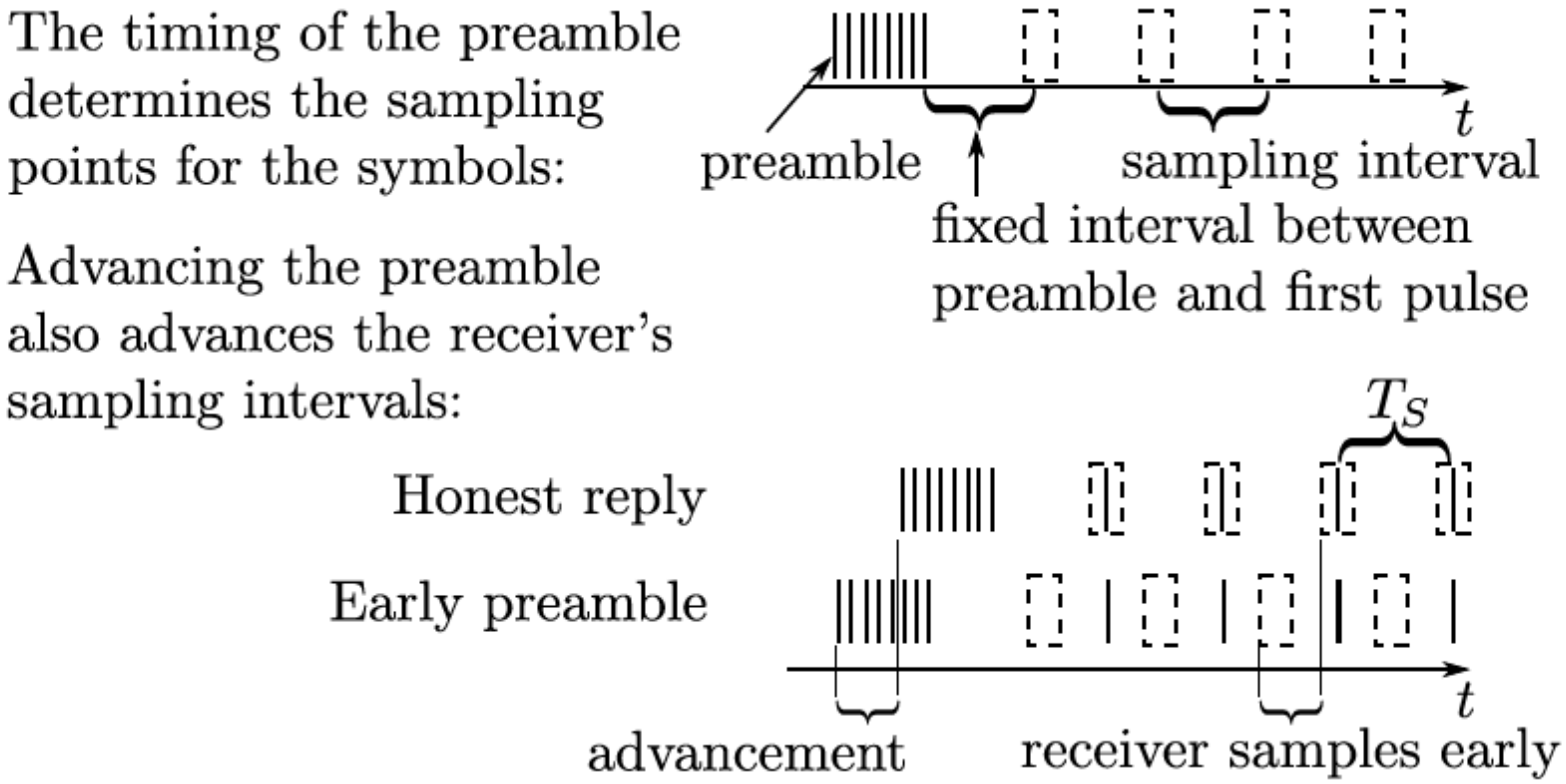
- robustness for increased security
- reduces complexity of the prover but increases the complexity of the verifier
- range might be affected by the use of CRCS (?)

What I didn’t talk about (synchronization, preambles, ...).

Ongoing implementations ...

...

Direct Time Measurement vs "Distance Commitment"



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

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

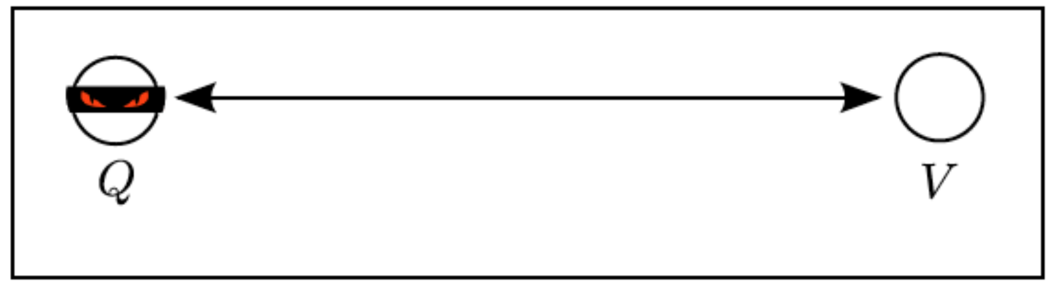
Protocol Analysis

Two main protocol constructs:

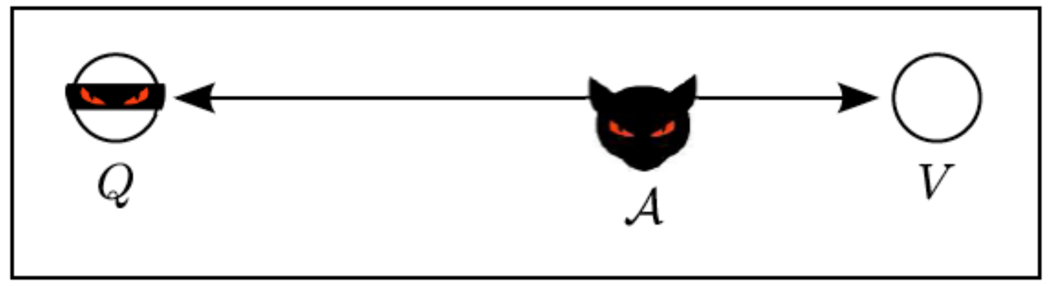
- Hancke-Kuhn
- Brands-Chaum

Three main attacks considered:

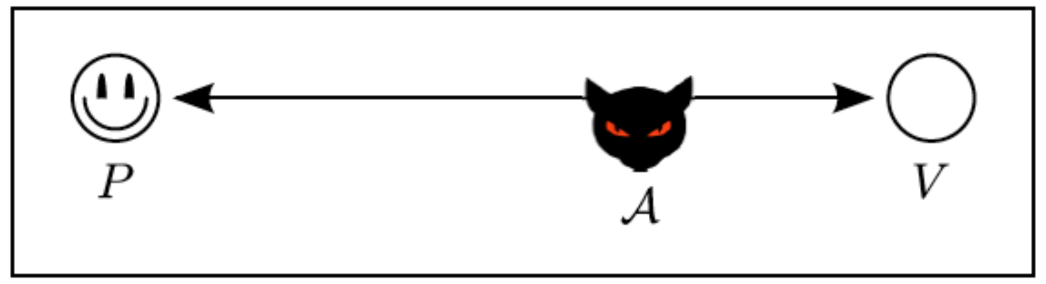
Distance Fraud



Terrorist Fraud



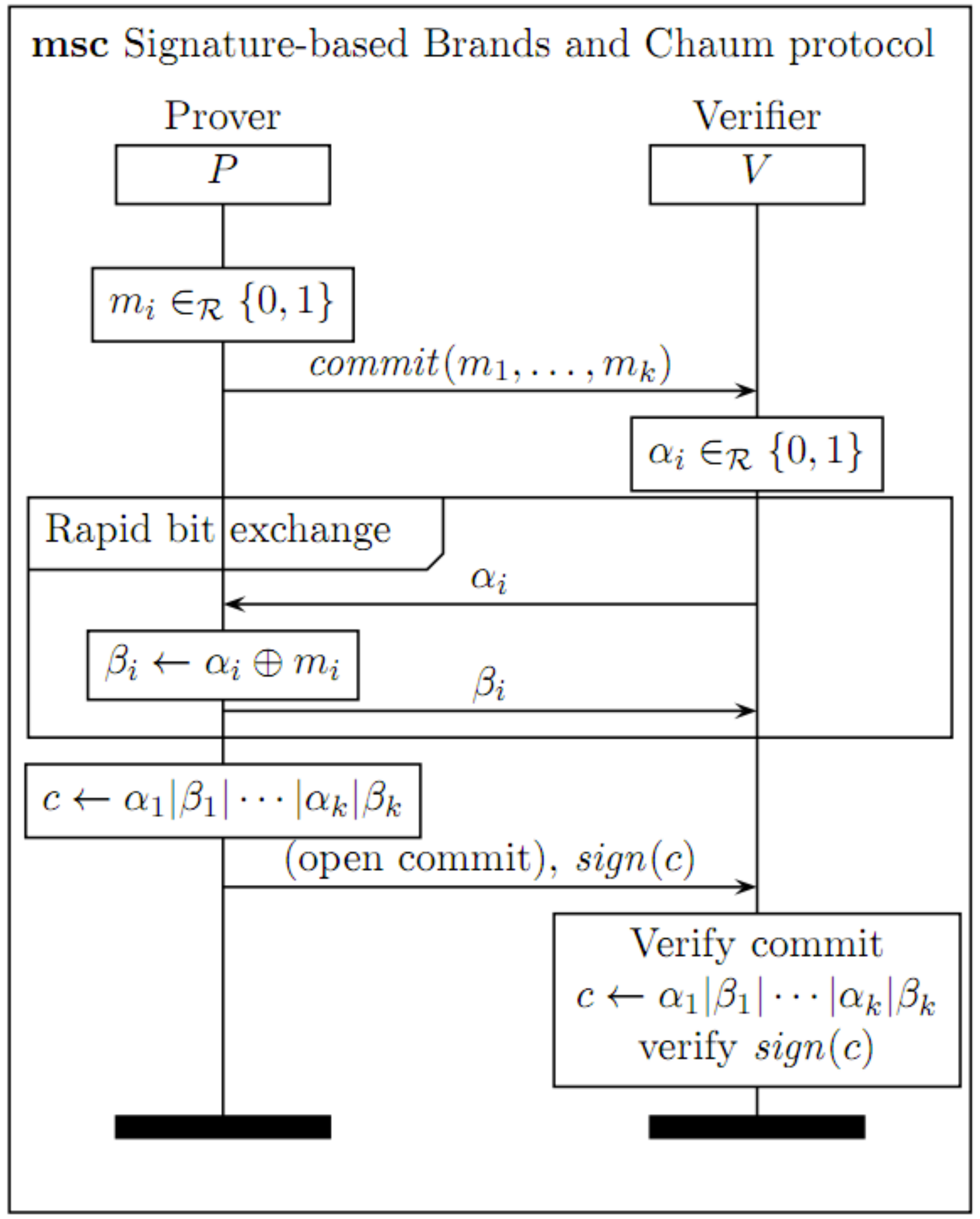
Mafia Fraud



Protocol Analysis

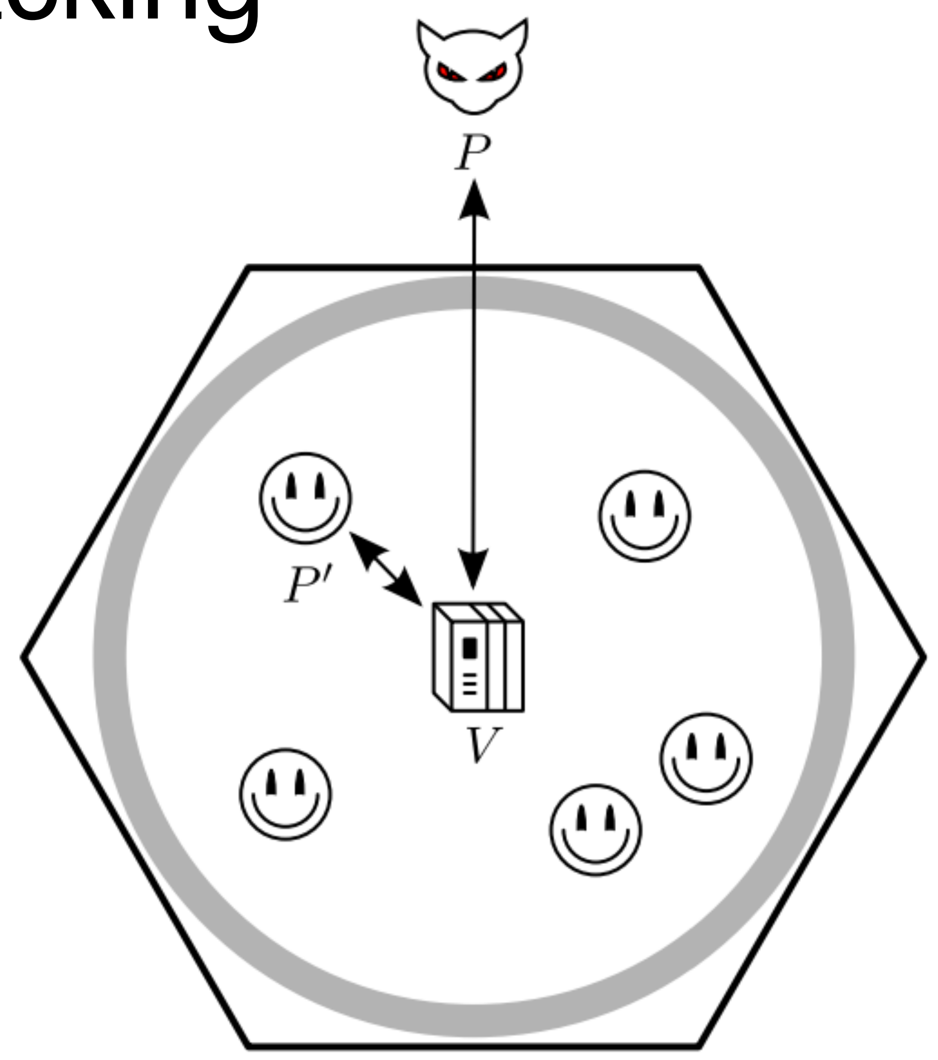
Two main protocol constructs:

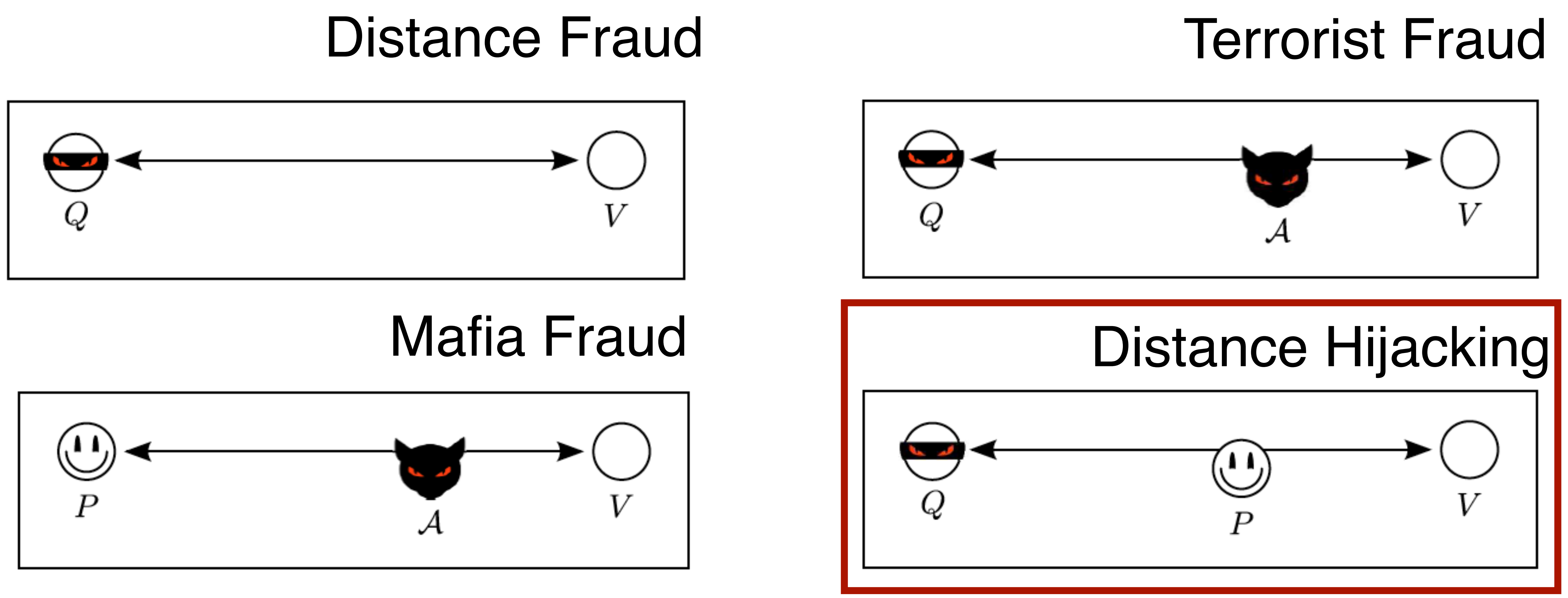
- Hancke-Kuhn
- Brands-Chaum



Protocol Analysis

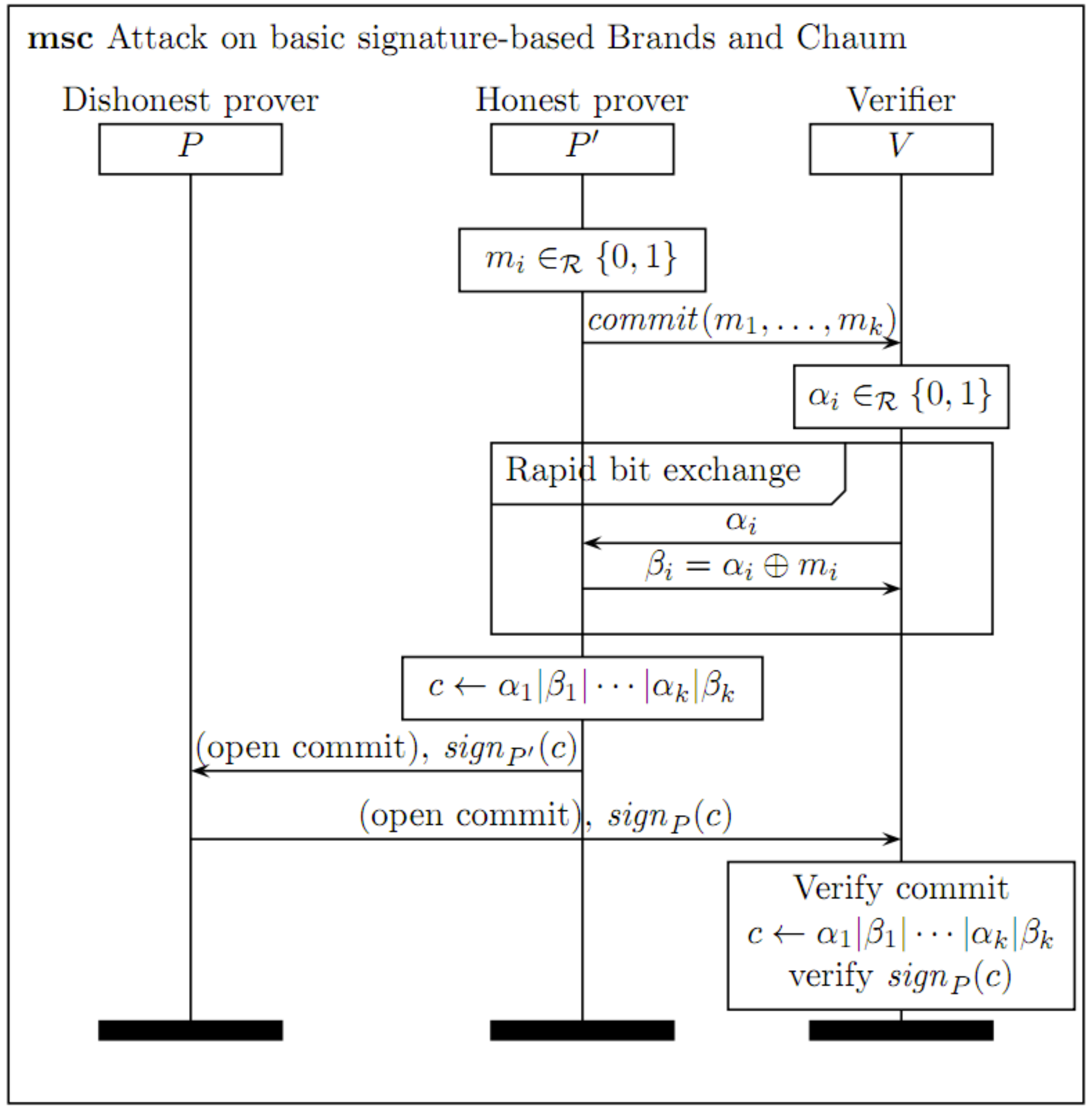
Novel attack: Distance Hijacking





Protocol Analysis

Distance Hijacking on Brands and Chaum



What if we want to verify if two trusted devices are close?
(focus on Mafia attacks)

Can we do better?
Most promising solutions of today use Ultra wide band radio (UWB)

Ranging Techniques

NON-Time-of-Flight:

RSSI measurement (e.g., WiFi, Bluetooth, 802.15.4, NFC / RFID) – Insecure

Phase (multi-carrier) measurement (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

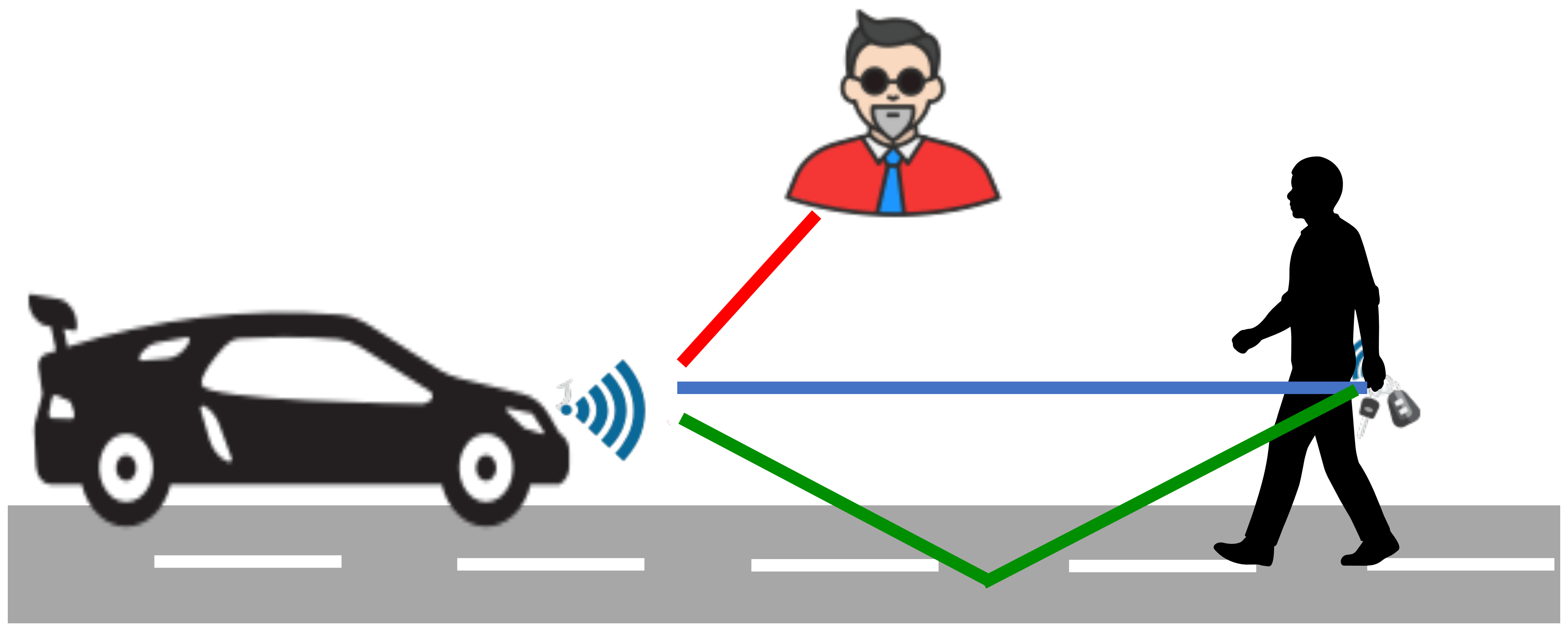
Ultra Wide Band (UWB) 802.15.4/4z – **Security depends on the logical and physical layer design**

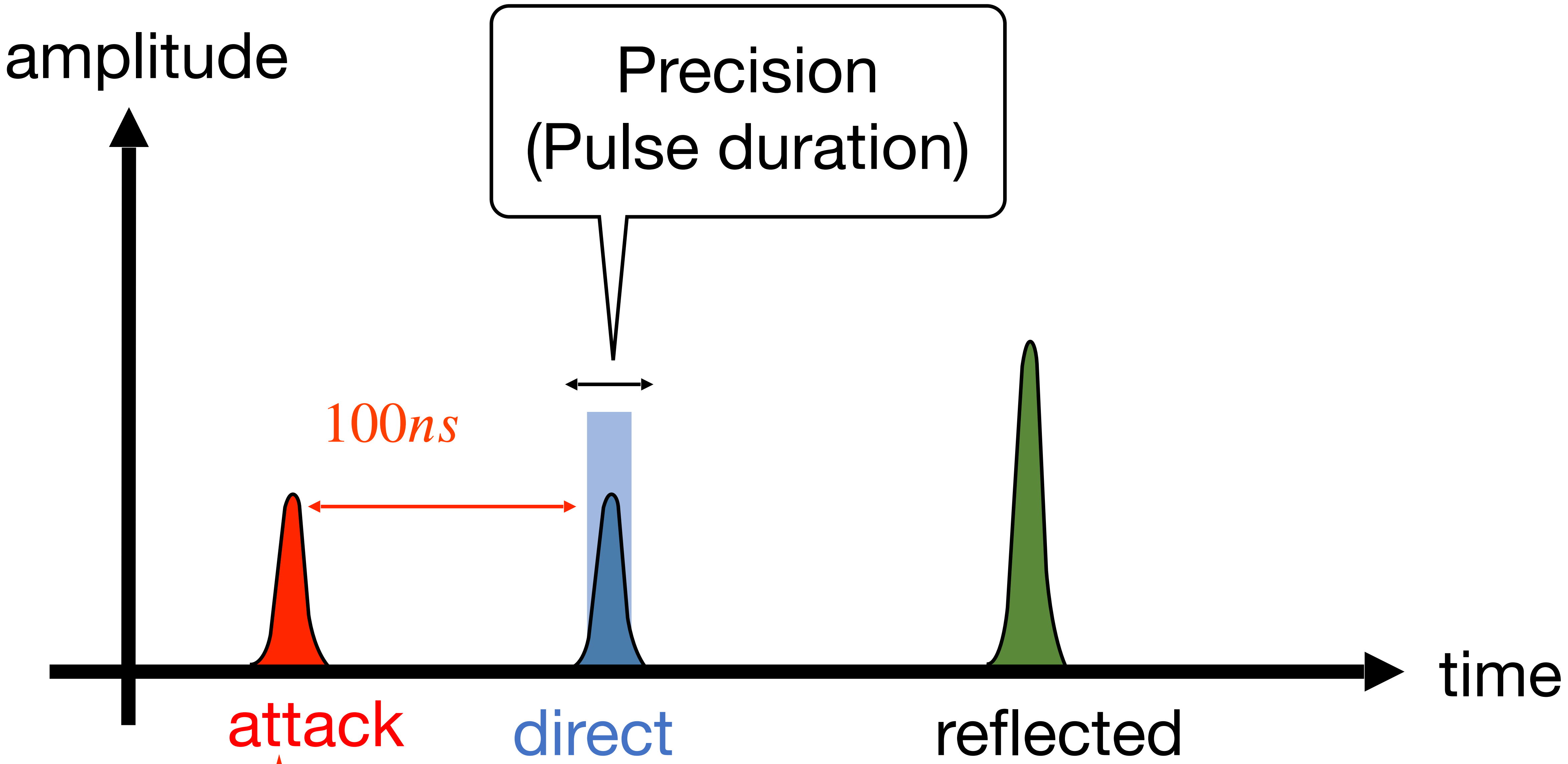
IEEE 802.15 WPAN™
Task Group 4z
Enhanced Impulse Radio

fira | The Power to Be Precise

CARCONNECTIVITY consortium®

Time-of-flight Measurement





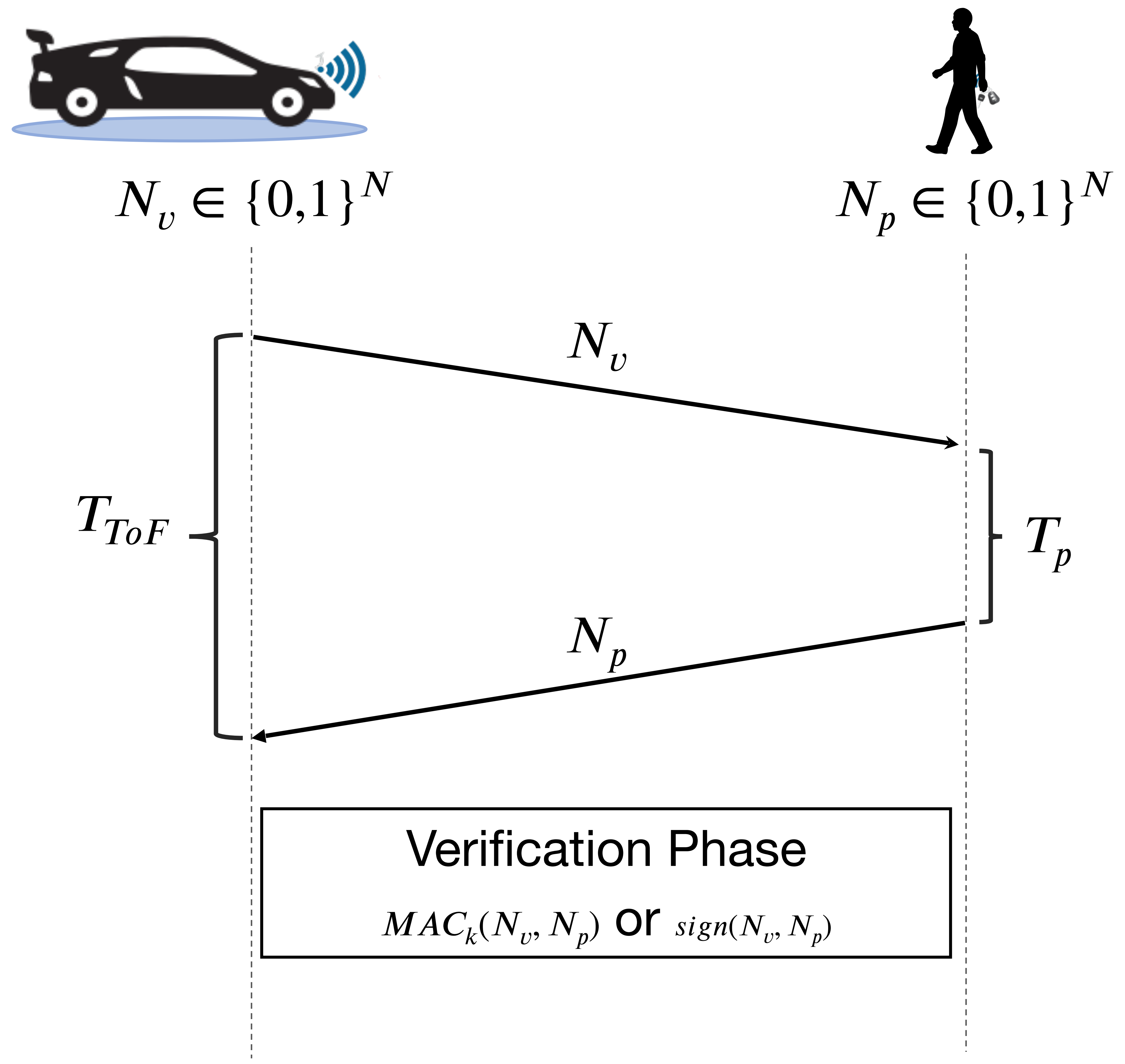
Weaker signal but true distance

Stronger signal but longer distance

Attacker needs to generate an earlier path to reduce the measured distance

The time-of-flight measurement shall be trusted only if it is verified by a provably secure technique

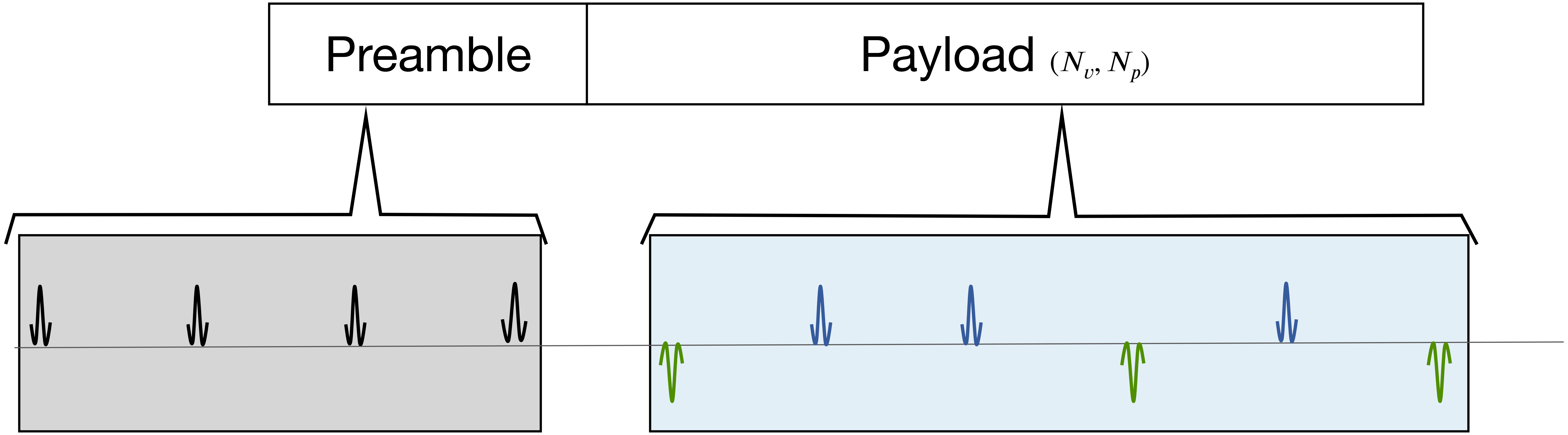
Recap: Distance Bounding



- Challenge-Response protocols

- Probability of distance reduction depends on the attacker's ability to predict (N_v, N_p) or break the cryptographic primitives

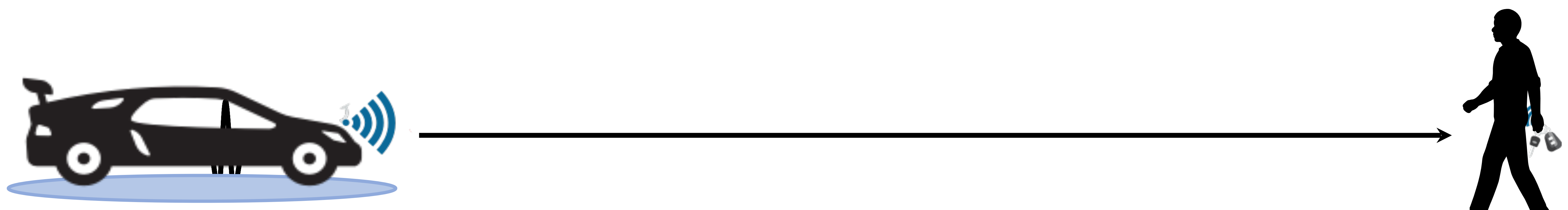
UWB: Logical to Physical Layer



- Fixed Sequence - known to all entities
- Time-of-flight estimation

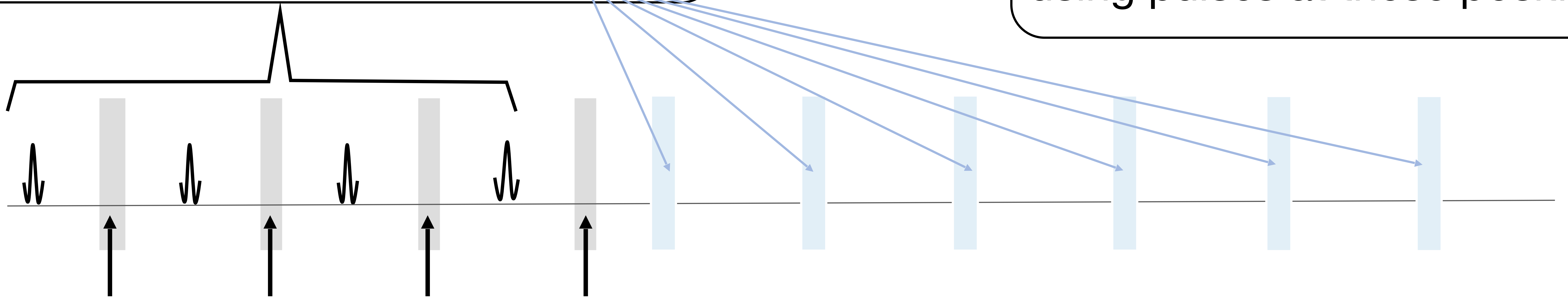
- Generated Cryptographically
- Time-of-flight verification

Physical Layer: Distance Commitment



Preamble indicates the time to search for data pulses
— To check integrity of arrival time

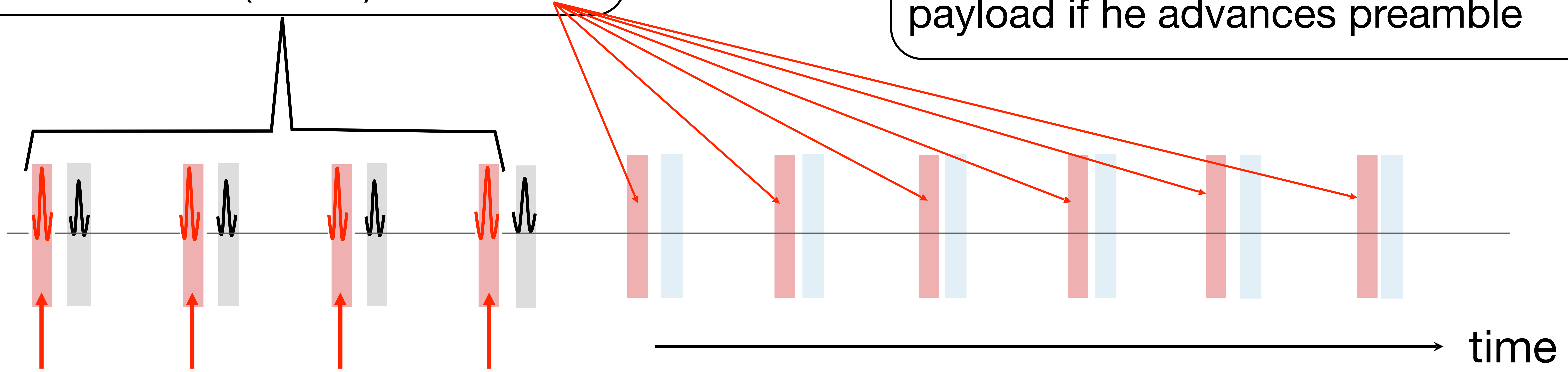
Receiver “verify” payload (N_v, N_p) using pulses at these positions



Attack: Distance Commitment

Receiver estimate time-of-flight on attacker preamble and search data at these (earlier) times

The timing of the preamble is binding.
— An attacker needs to advance payload if he advances preamble



time-of-flight estimation

Physical Layer Design (IEEE 802.15.4)

Single-pulse/bit

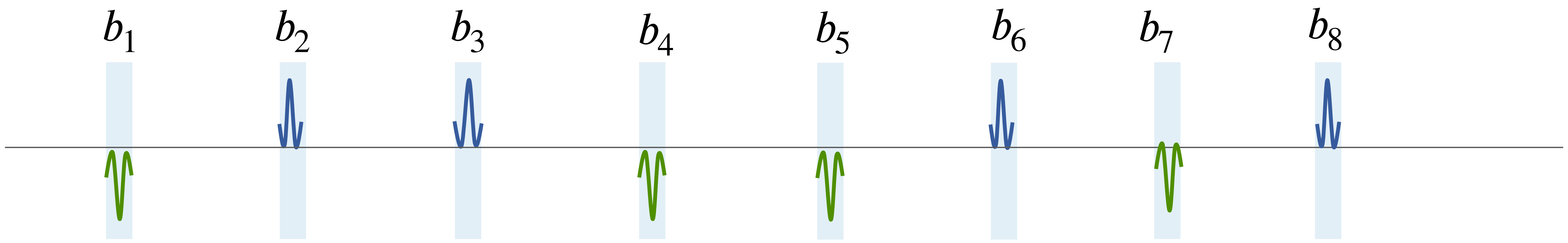
Multi-pulse/bit

- Transmission energy per pulse is limited by FCC and ETSI regulations

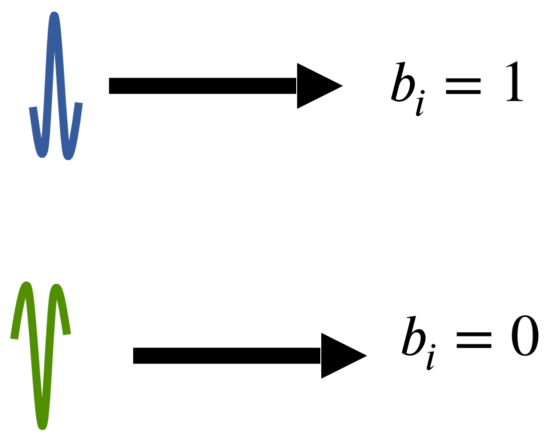
- Receiver doesn't "see" individual pulses (TOO WEAK) at longer distances
- Energy of multiple pulses is AGGREGATED

Single-pulse/bit (IEEE 802.15.4)

Payload (N_v, N_p)

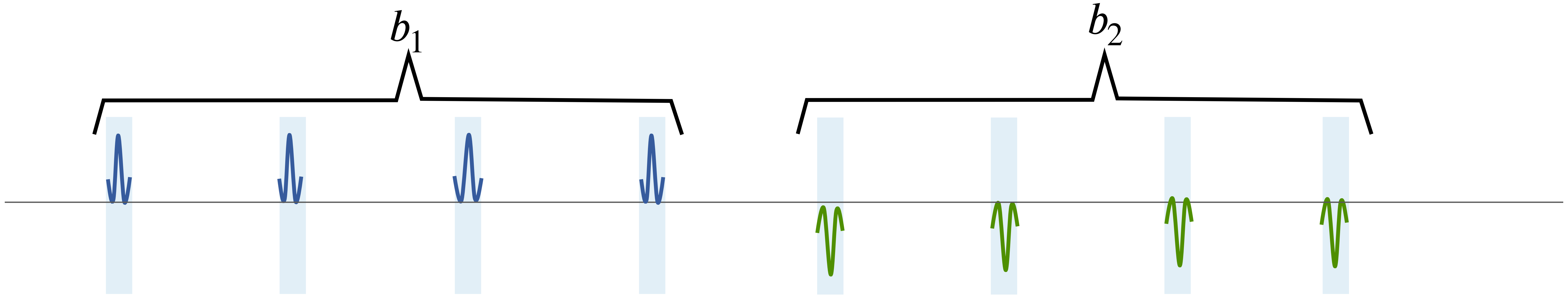


Detection

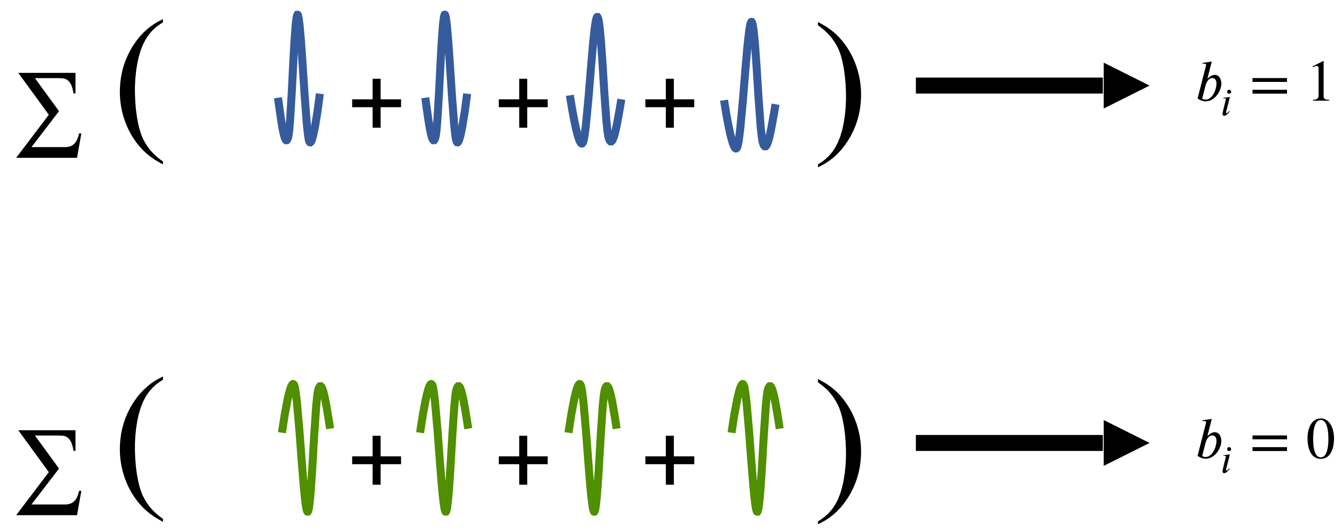


Multi-pulse/bit (IEEE 802.15.4)

Payload (N_v, N_p)



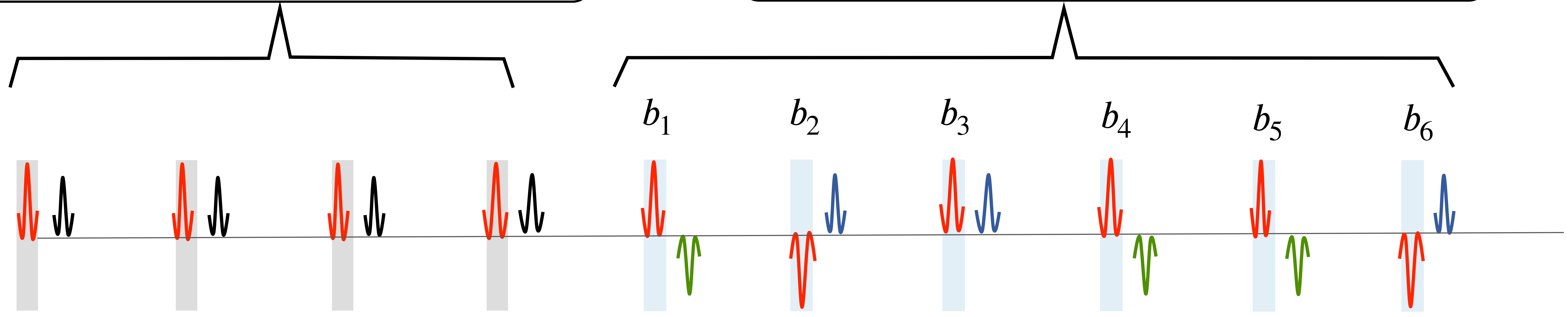
Detection



Attack Case: Single-pulse/bit

Receiver estimate time-of-flight at on attacker preamble

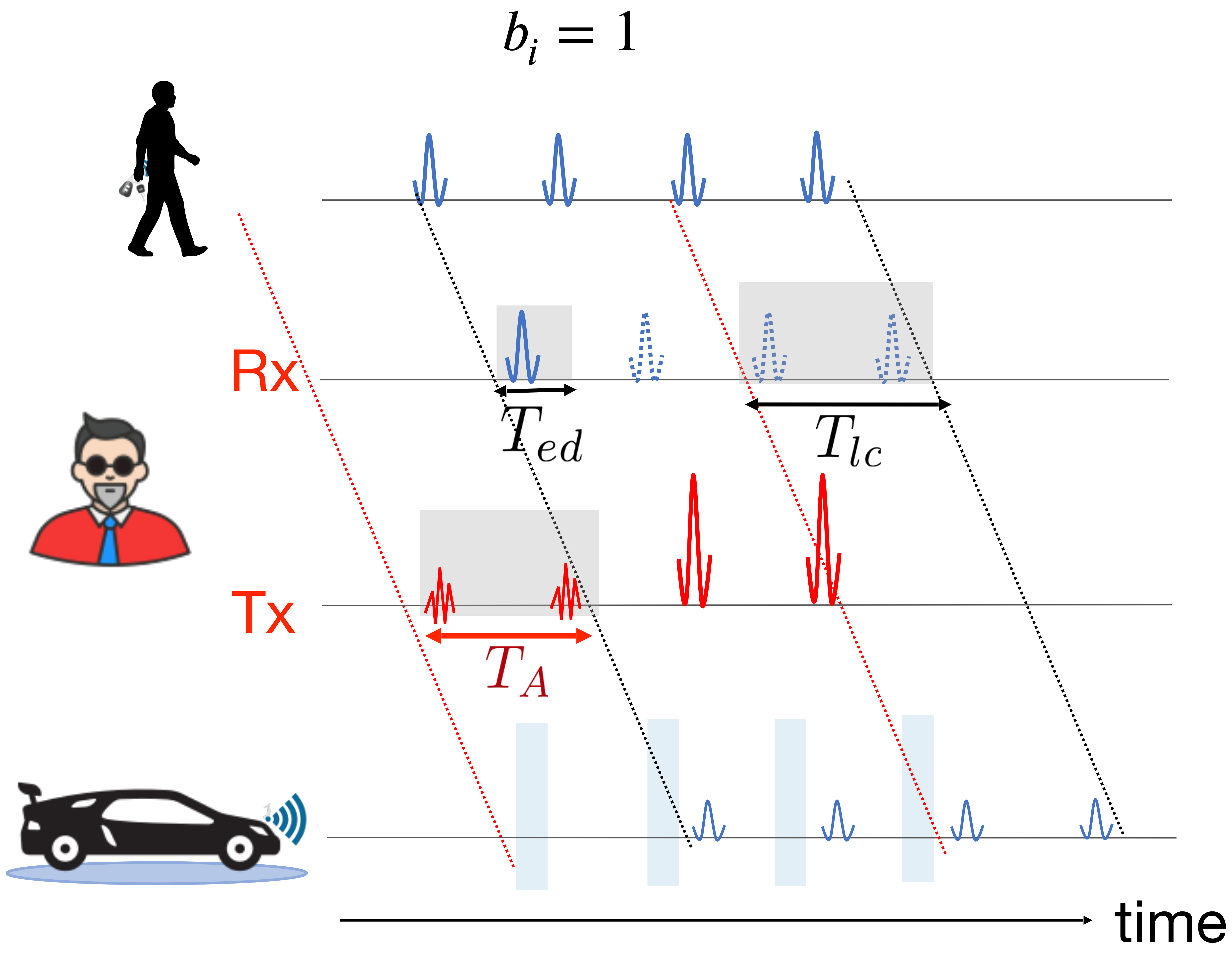
Receiver “verify” payload for estimated time-of-flight



- Attacker can only place random response

- Short Distance : Probability of distance reductions = probability to predict payload $(N_v, N_p) = 2^{-N}$ (N = number of data bits)
- Long Distance: Probability of distance reduction depend on the allowed bit error rate

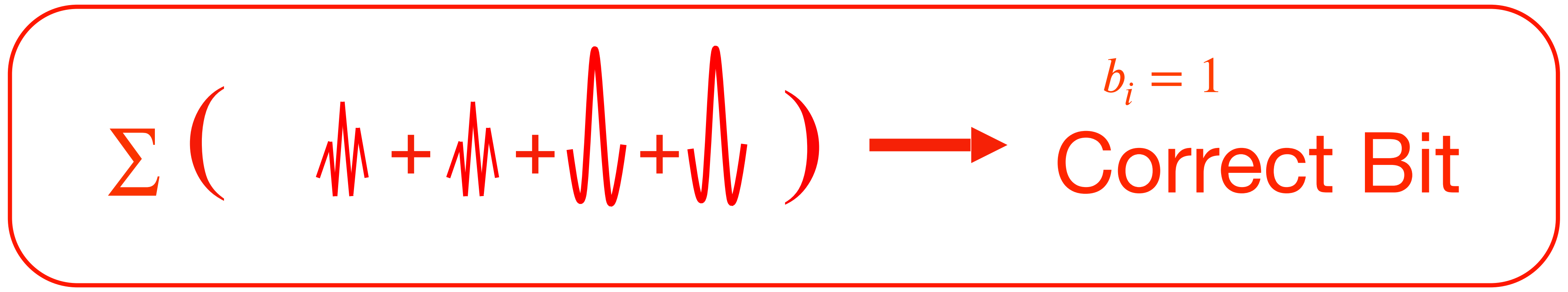
Attack Case: Multi-pulse/bit



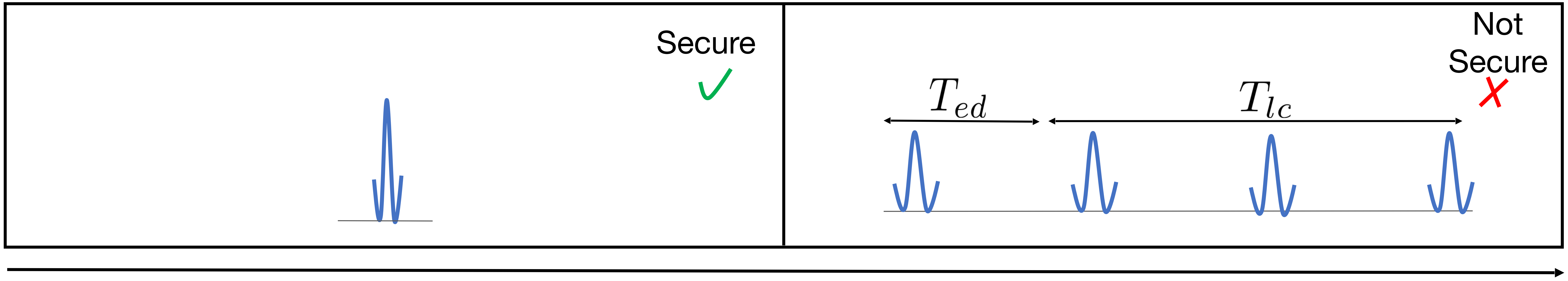
Early-detect/late-commit (ED/LC) Attack

Steps to insert an earlier path

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



Performance and Security Tradeoff: Multi-pulse/bit



High Peak Power Device

Low Peak Power Device/
Longer distance with pulses aggregated over multiple milliseconds

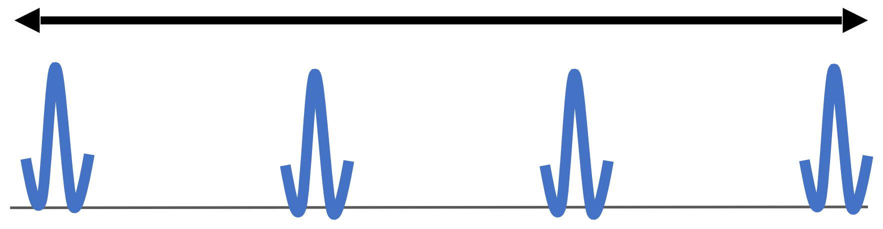
- We need longer symbols (multi-pulse) for performance (range and robustness)

- Longer symbols are vulnerable to ED/LC attack

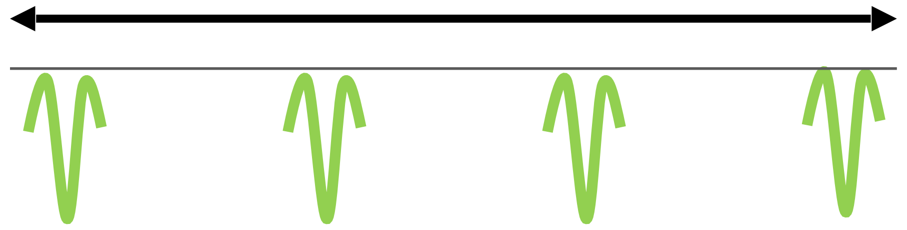
Why ED/LC attack succeed?

- Symbol structure is predictable

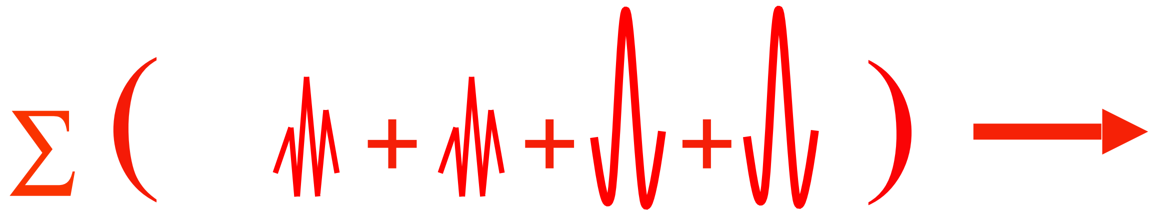
$T_{sym}(b_i = 1)$



$T_{sym}(b_i = 0)$



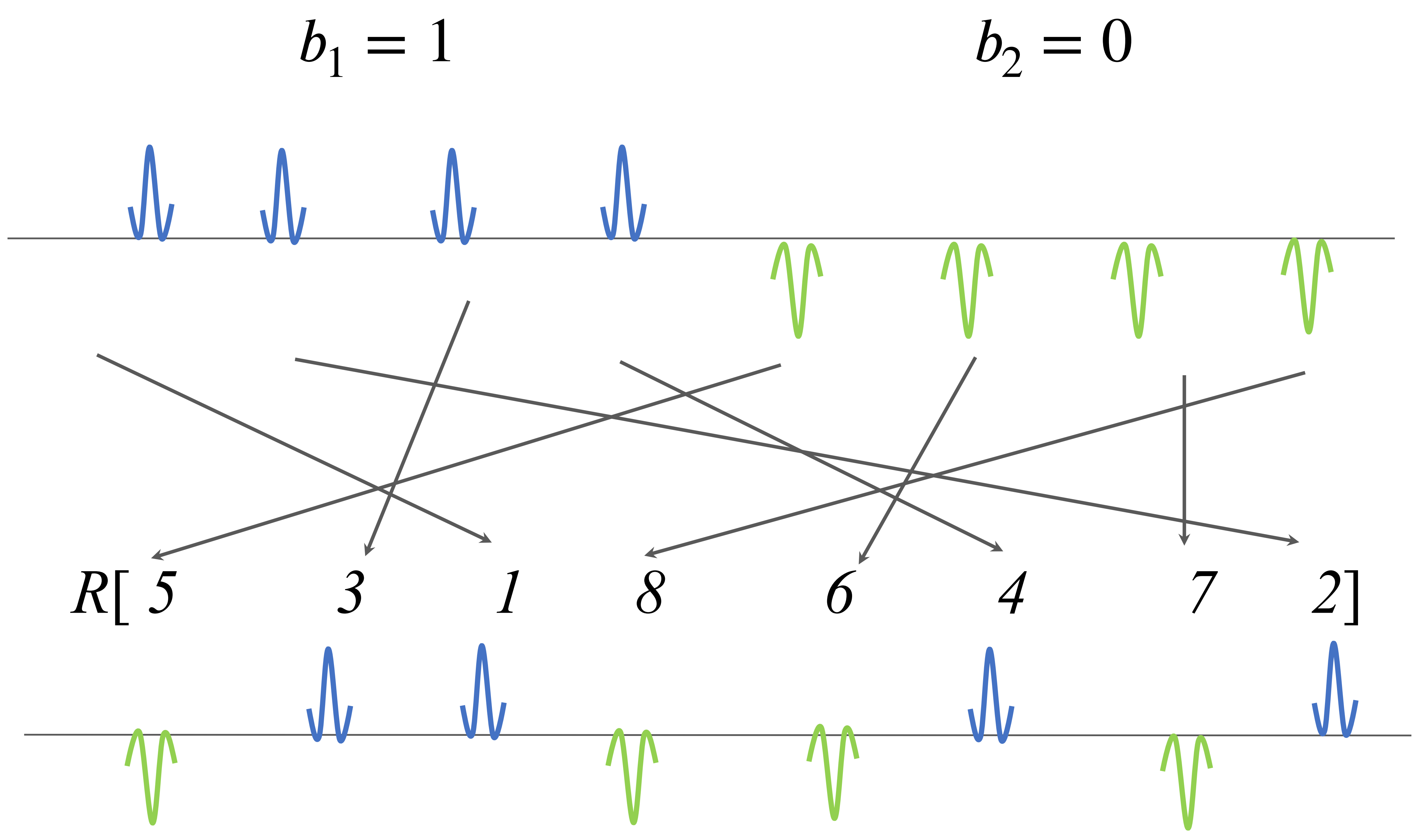
- Receiver does not check physical layer integrity of the signal



$b_i = 1$

Correct Bit

Example 1: Multi-pulse/bit with pulse reordering



Cryptographic operations on pulses

- Symbol interleaving through pulse reordering

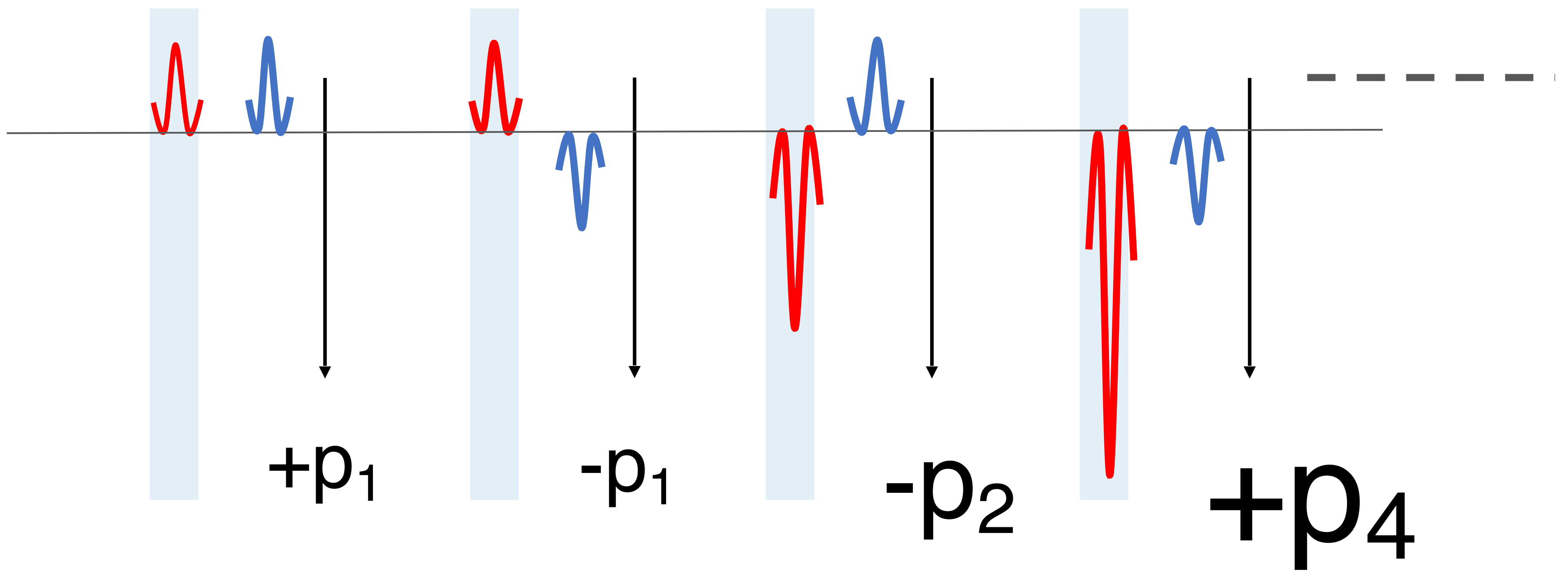
Verification: Aggregate the energy

Information needed for the ED/LC attack is lost

- Shape of the symbols is hidden
- Start and end time of symbols is unpredictable

Attacker can only guess!

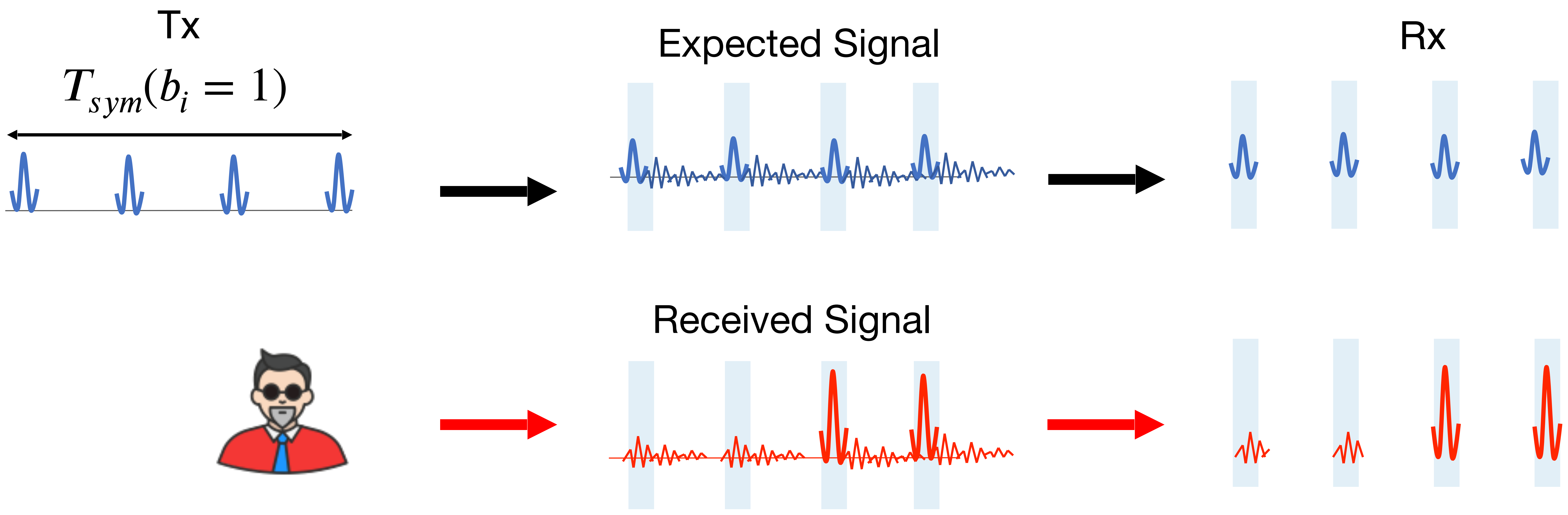
Attacker can only guess!



- Predict the polarity of pulses correctly
- Compensate for wrong guesses with a higher transmission power

- Attacker succeed if data (N_v, N_p) is correct
- Probability of distance reduction depends on the number of bits interleaved

Example 2: Secure Verification Function



- Pulses are sent with a long repetition period
  - No inter-pulse interference
- Perform statistical analysis (eg., Variance of the expected and received signal)

Message Time of Arrival Codes (MTAC)

- A new class of cryptographic primitives to verify integrity of message arrival time
- Single-pulse/bit, UWB with pulse reordering and Secure verification function can be considered as different classes of MTACs

Gen K

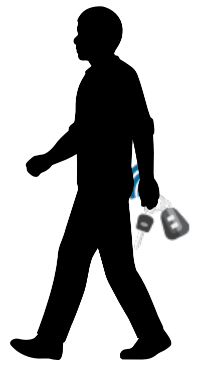
Mtac

$N_v \in \{0,1\}^N$

$c \leftarrow MTAC_K(N_v)$

$c = [c_1, c_2, \ldots, c_n]$

c => c'



Vrfy

$b := Vrfy_K(N_v, c')$

Use c' for ToF estimation when $b = 1$

MTAC’s are secure against all known ranging attacks

- Relay attack
- Replay attack
- Cicada attack
- Preamble injection attack
- Early detect late commit (ED/LC) attack
- Clock-offset manipulation attack
- Guessing attacks with different power level

IEEE 802.15.4z

Low Rate Pulse (LRP)

- Longer pulse repetition period
- Ranging require few 100 pulses
- Low-cost and low-energy
- Open security design and analysis
- Provably secure distance measurement

High Rate Pulse (HRP)

- Small pulses repetition period — pulses are affected by inter-pulse interference
- Ranging require few 1000 pulses
- High-cost and high-energy
- Security is not fully disclosed/core parts are proprietary

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

Selected Publication

1. Patrick Leu, Mridula Singh, Marc Roeschlin, Kenneth G. Paterson, Srdjan Capkun
   Message Time of Arrival Codes: A Fundamental Primitive for Secure Distance Measurement
   in IEEE Symposium on Security and Privacy (**S&P**), 2020
2. Mridula Singh, Patrick Leu, AbdelRahman Abdou,Srdjan Capkun
   UWB-ED: Distance Enlargement Attack Detection in Ultra-Wideband
   Usenix Security Symposium, 2019
3. Mridula Singh, Patrick Leu, Srdjan 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
4. Nils Ole Tippenhauer, Heinrich Luecken, Marc Kuhn and Srdjan Capkun
   UWB Rapid-Bit-Exchange System for Distance Bounding
   ACM Conference on Security and Privacy in Wireless and Mobile Networks (**WiSec**), 2015
5. Aanjhan Ranganathan, Boris Danev, Aurélien Francillon, Srdjan Capkun
   Physical-Layer Attacks on Chirp-based Ranging Systems
   ACM Conference on Security and Privacy in Wireless and Mobile Networks (**WiSec**), 2012
6. S.Capkun, J.P. Hubaux,
   Secure positioning of wireless devices with application to sensor networks,
   in Proceedings of IEEE **INFOCOM** 2005

Secure Localization

From Proximity Verification
to Location Verification and Secure Localization

Secure Localization

User’s perspective:
to obtain a correct information about its own location

Infrastructure perspective:
to obtain a correct information about the location of a device

Secure localization goals

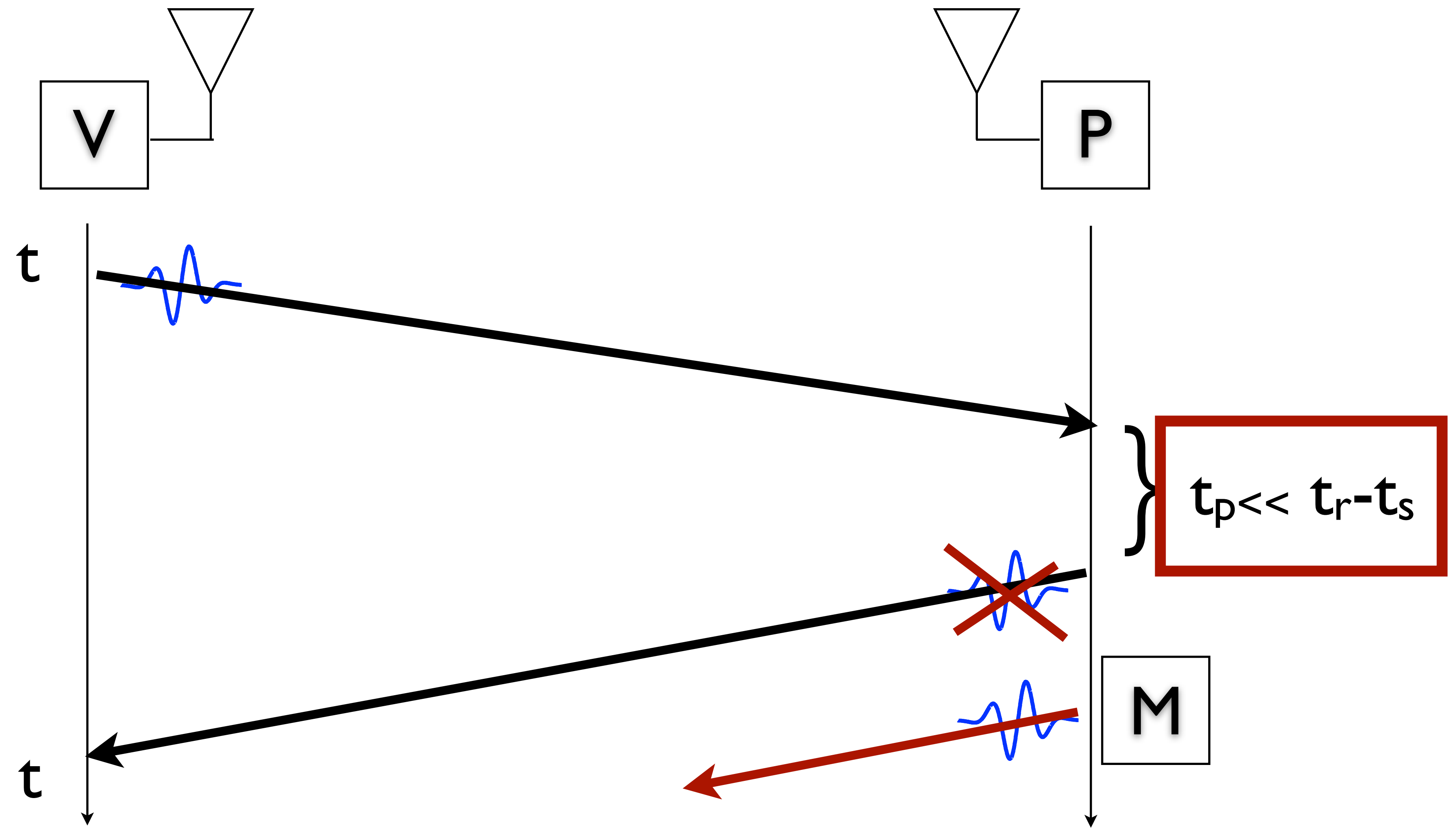
- Compute a ‘correct’ location of a (trusted) device in the presence of an attacker. *(Secure Localization)*
- Verify the correctness of a location of an untrusted device.
  (that e.g., claims a certain location) *(Location Verification)*

Distance Bounding

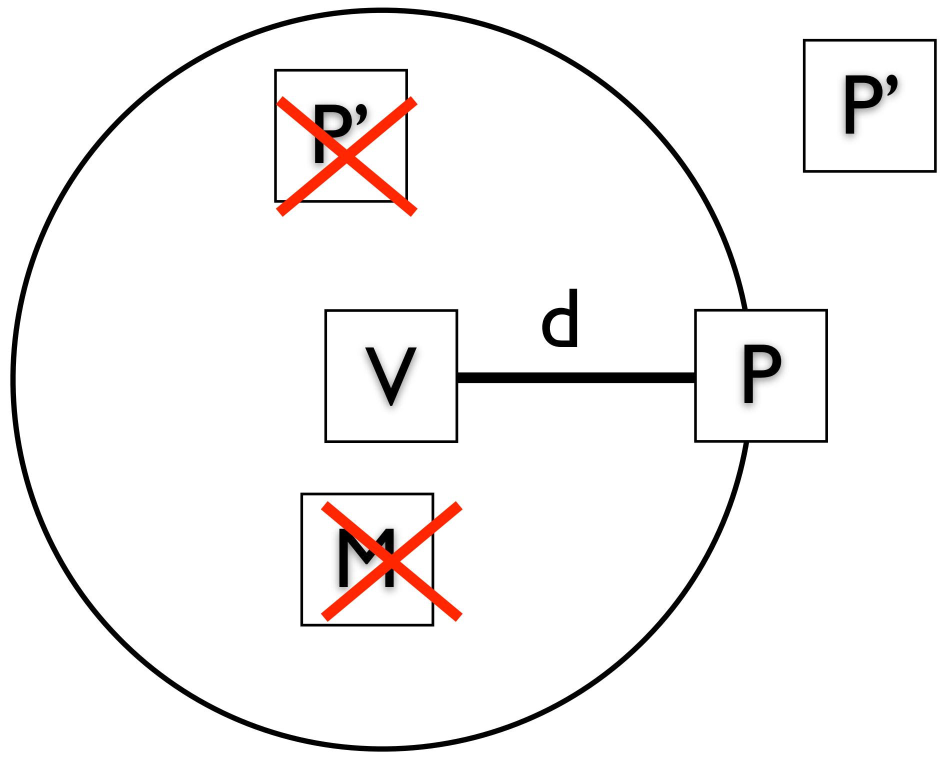
- P can always pretend to be further from V
- M can always convince P and V that they are further away

*=> Distance **enlargement is easy**, **distance reduction can be prevented***

Ranging



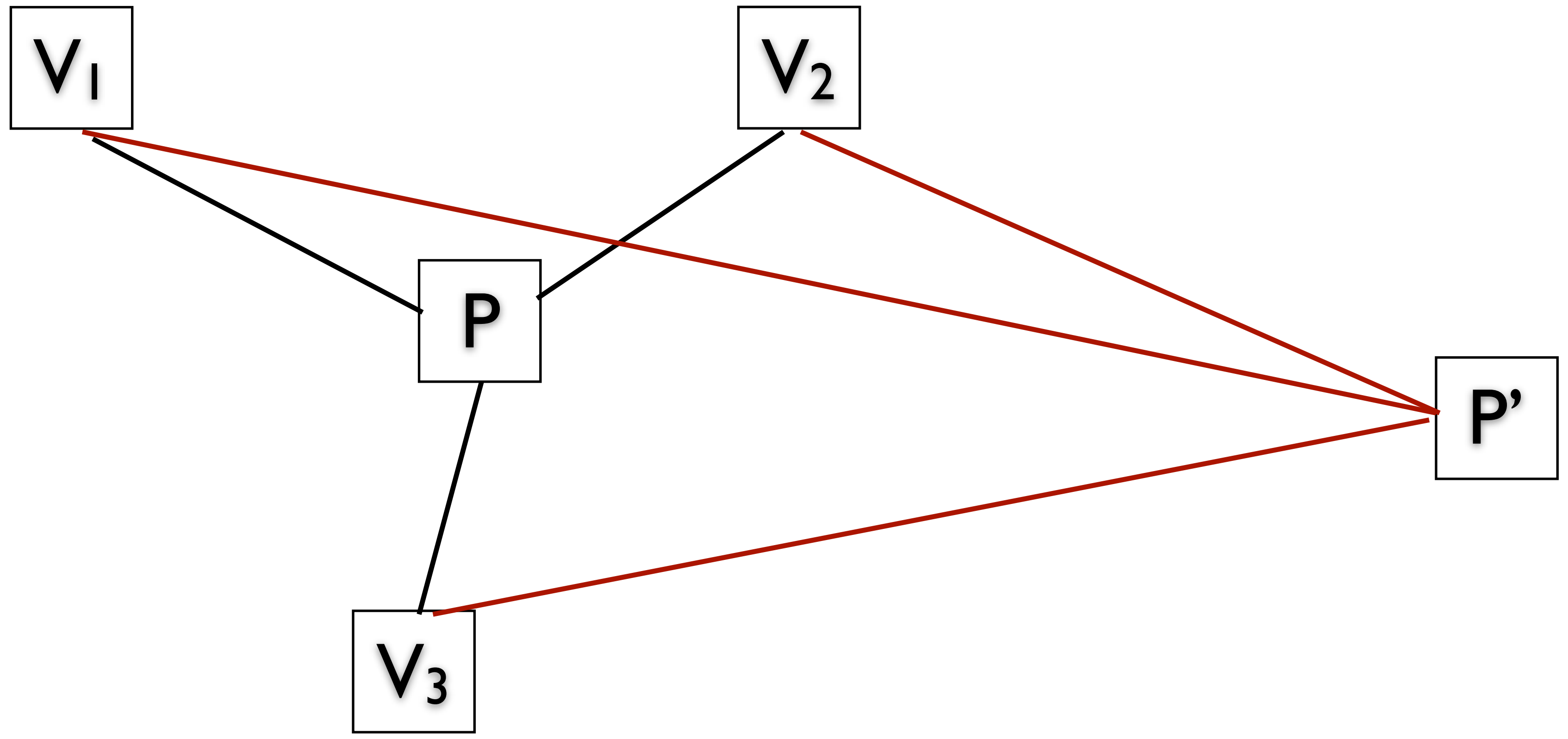
$d = (t_r - t_s - t_p)c/2$



Verifiable Multilateration

Distance enlargement is easy, distance reduction is prevented using distance bounding protocols

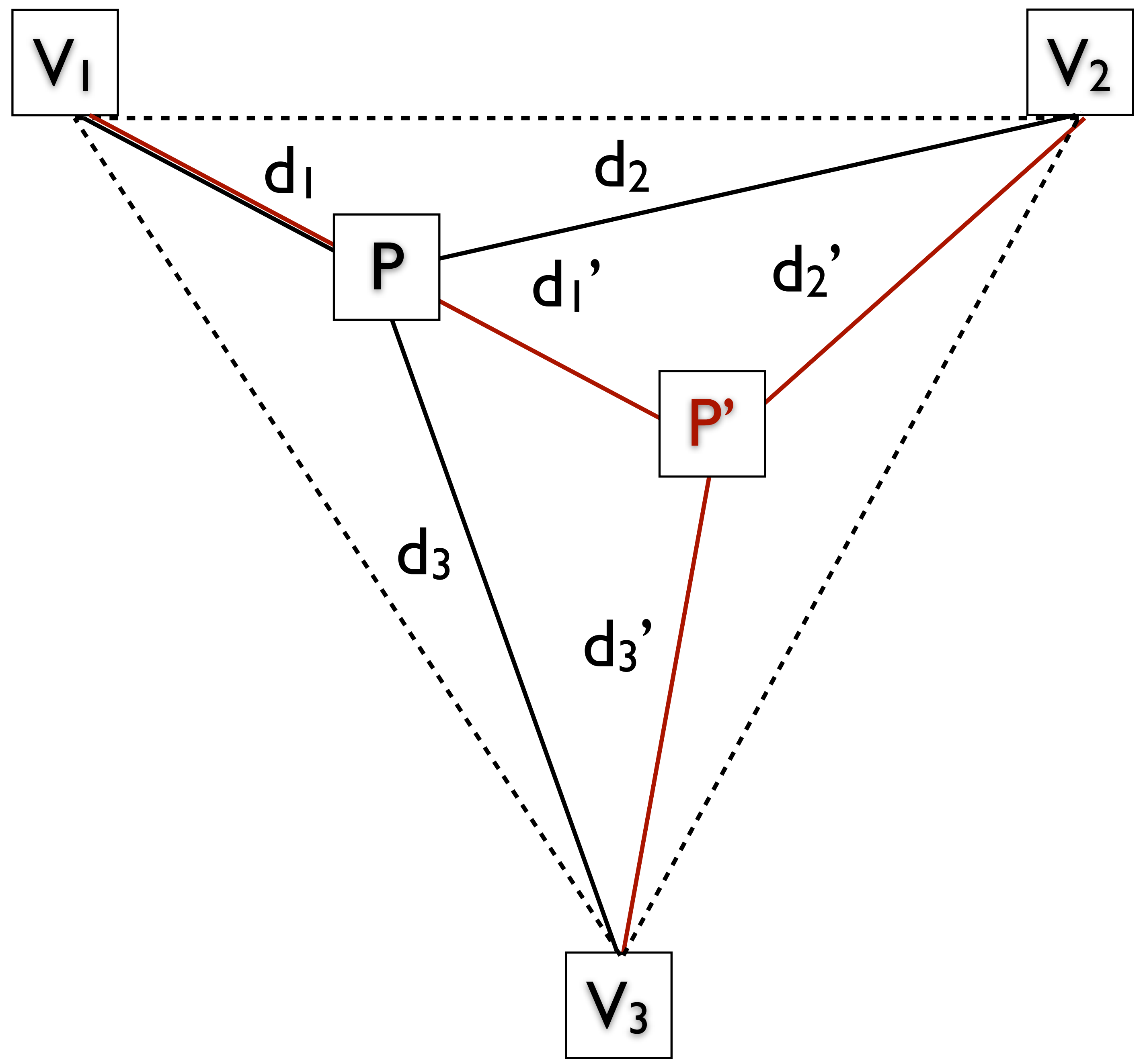
- *So can we realize Location Verification or Secure Localization using Distance Bounding protocols?*



Verifiable Multilateration

Verifiable Multilateration in 3 steps:

1. Verifiers (known locations) form a *verification triangle*.
2. Based on the measured distance bounds, compute the location of the Prover.
3. *If the computed location is in the verification triangle, the verifiers conclude that this is a correct location.*

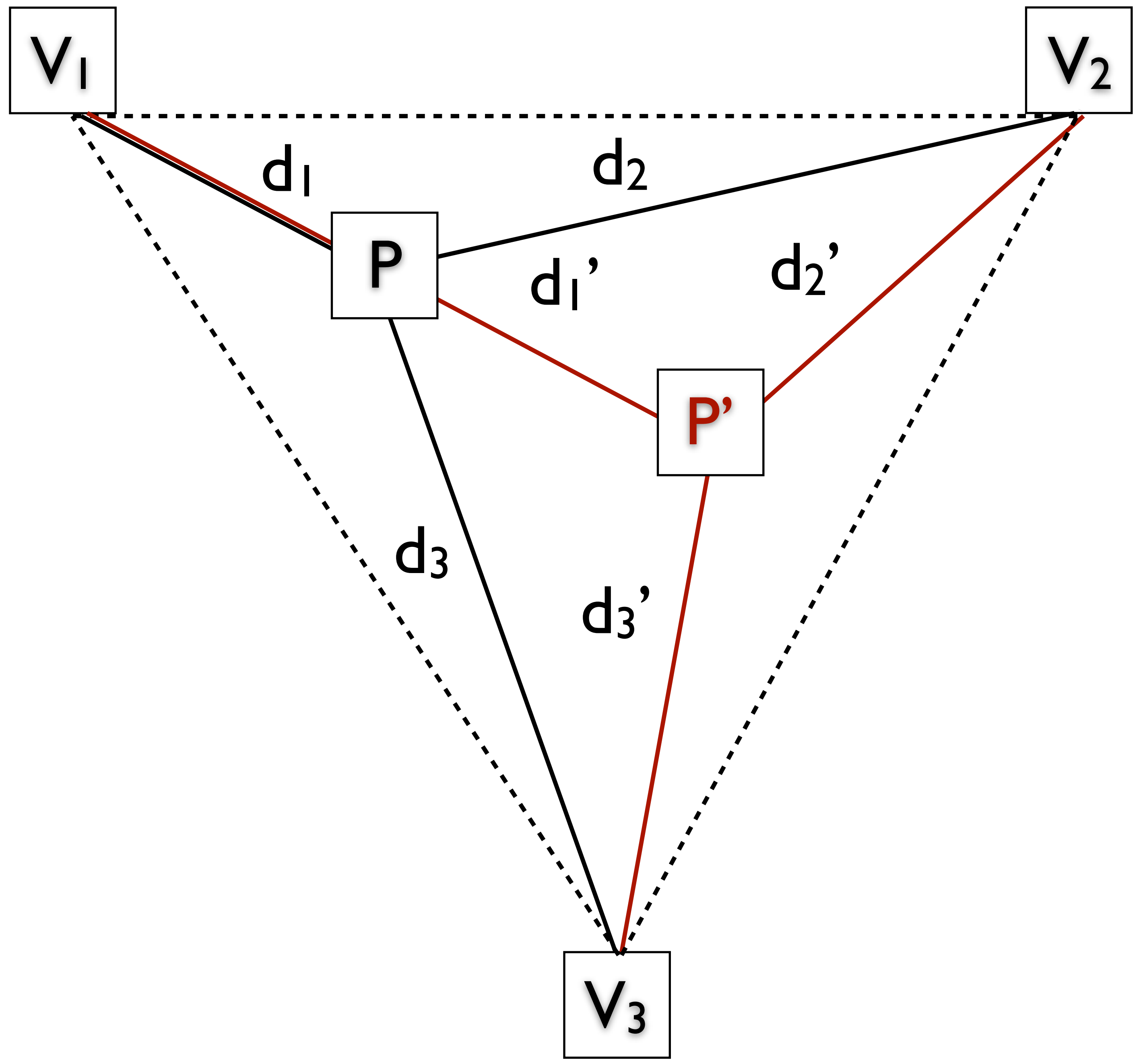


P→P' => d2'<d2

Verifiable Multilateration

Properties:

1. *P cannot successfully claim to be at P'≠P, where* ***P' is within the triangle***
2. *M cannot convince Vs and P that P is at P'≠P where* ***P' is within the triangle***
3. *P or M can spoof a location from P to P' where P' is* ***outside the triangle***



P→P' => d2'<d2

Verifiable Multilateration

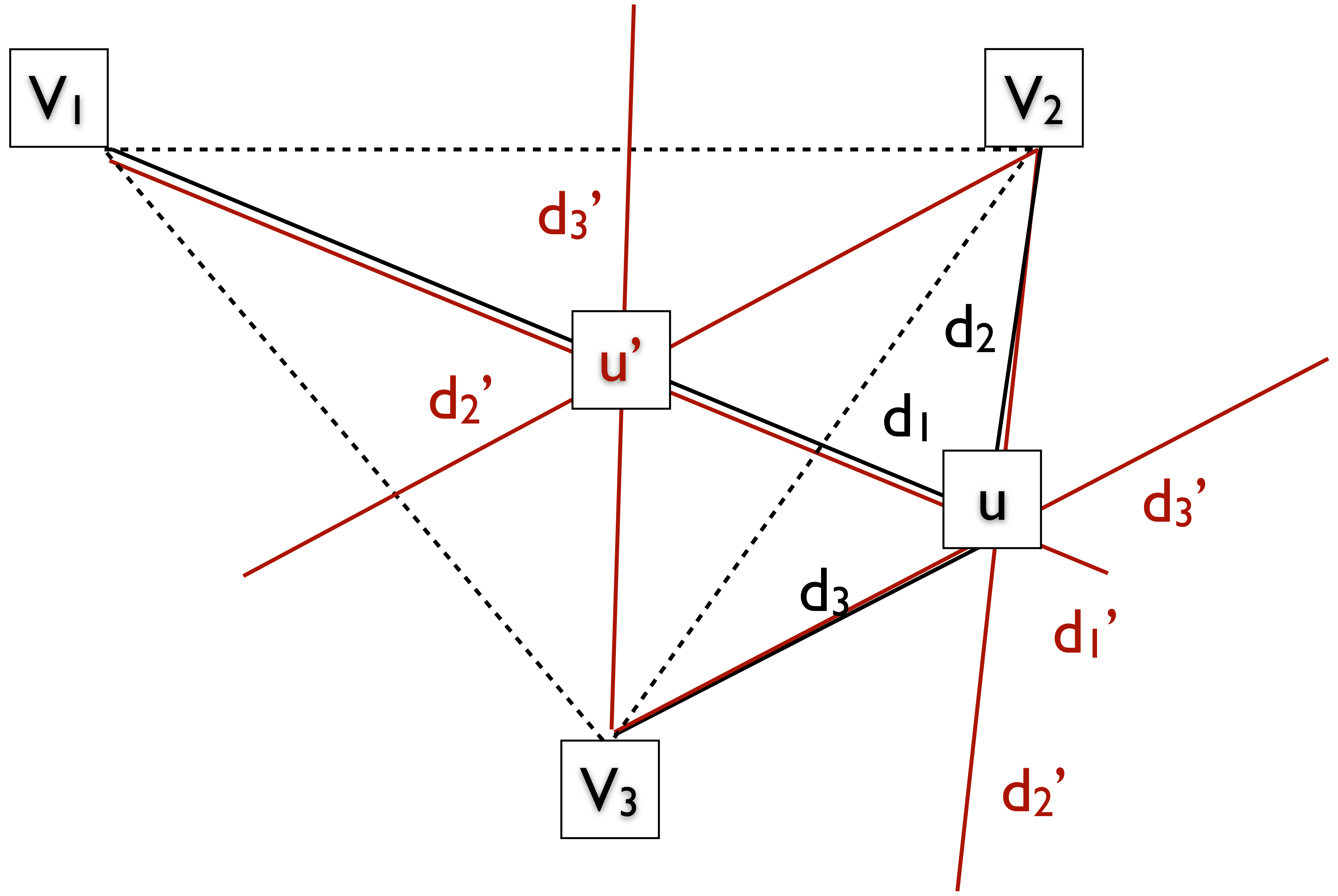
The algorithm and the errors:

- Need to be careful how the position is computed!
- Example: *Minimum Mean Square Estimate (MMSE)*

Let $f_i(x'_u, y'_u) = db_i - \sqrt{(x_i - x'_u)^2 + (y_i - y'_u)^2}$

The position of u is obtained by minimizing $F(x'_u, y'_u) = \sum_{v_i \in \mathcal{T}} f_i^2(x'_u, y'_u)$ over all estimates of u

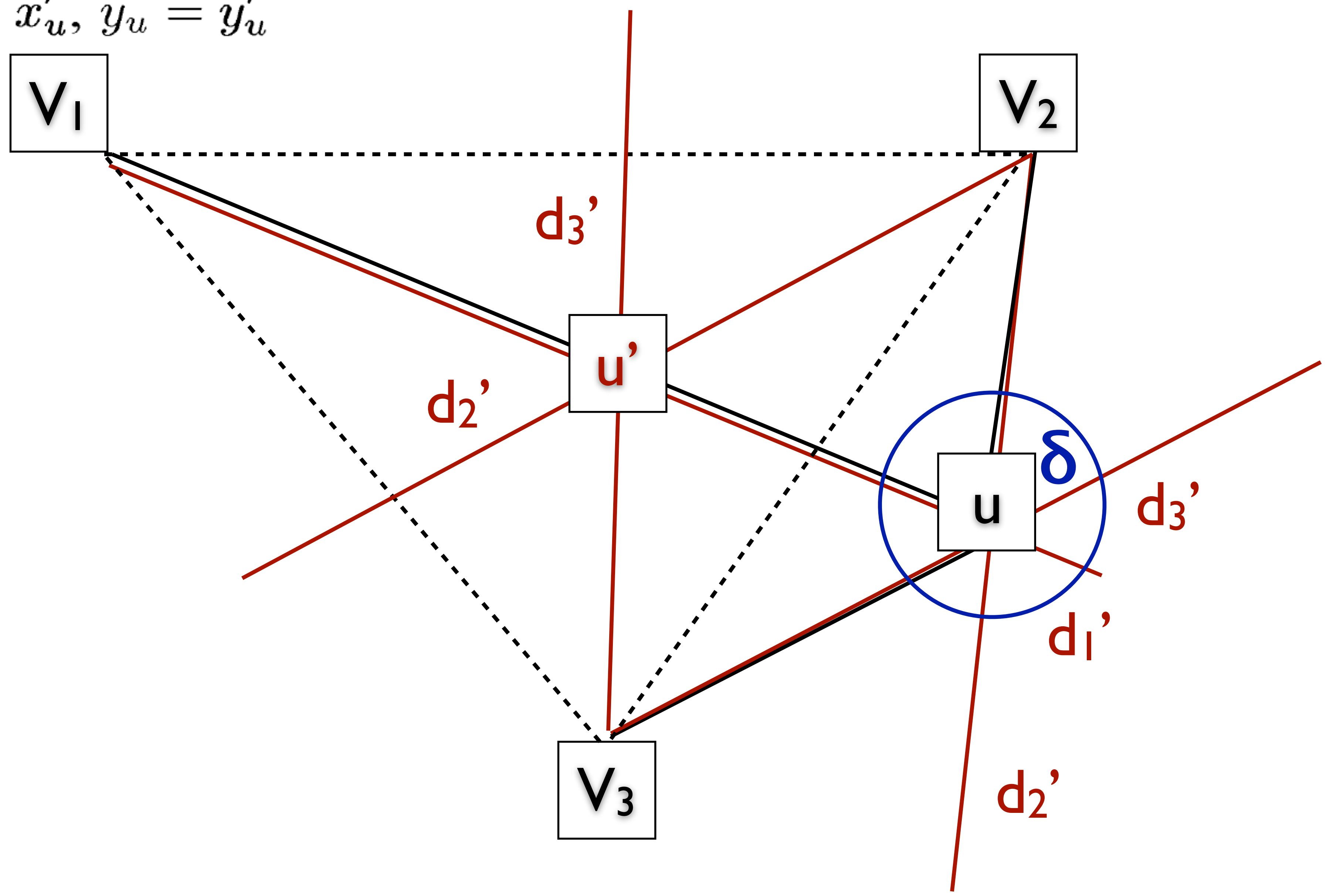
- *Attack:*



Verifiable Multilateration

Verifiable Multilateration Algorithm

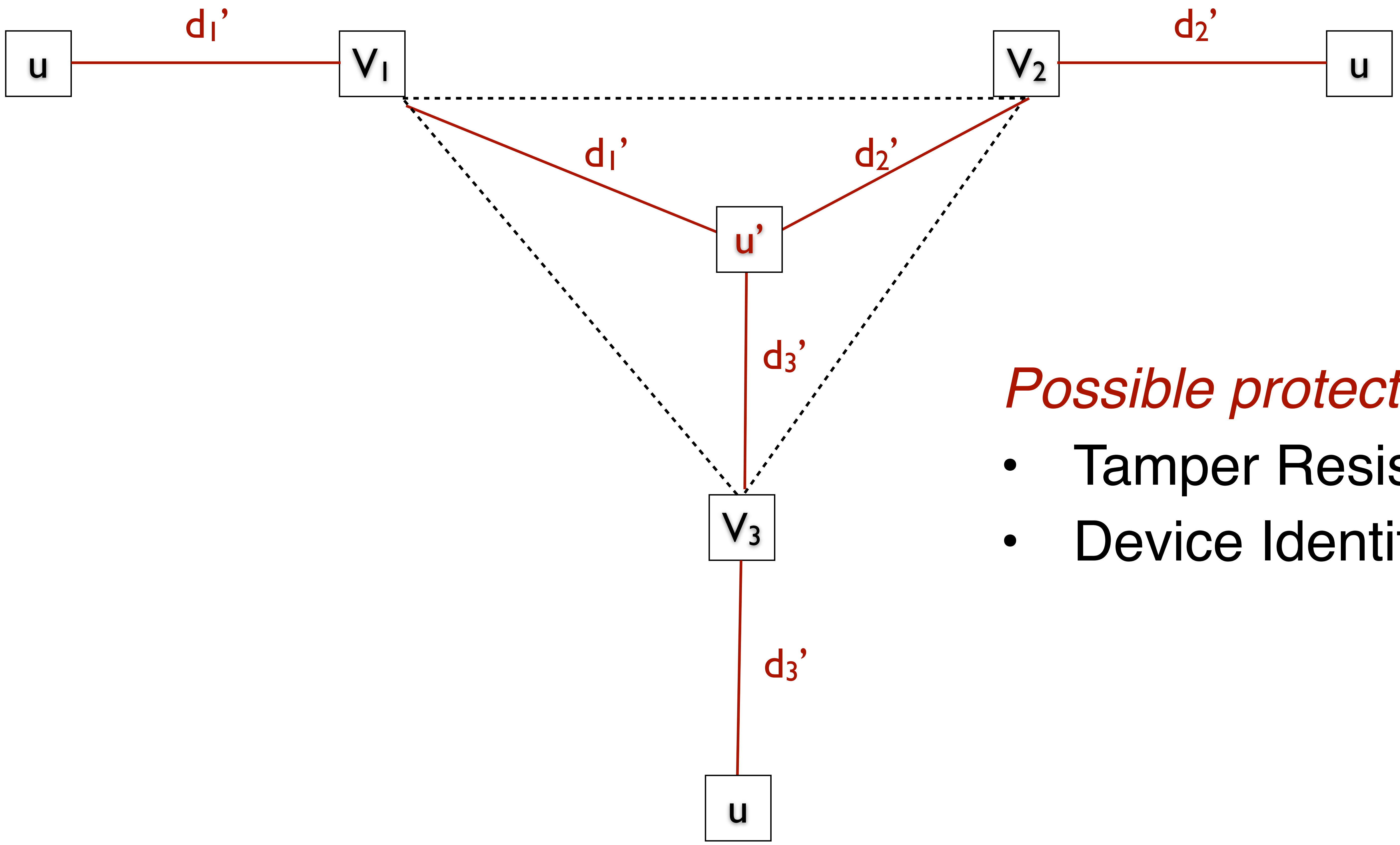
$\mathcal{T} = \emptyset$; set of verification triangles enclosing u
$\mathcal{V} = \{v_1, ..., v_n\}$; set of verifiers in the power range of u
1 *For all* $v_i \in \mathcal{V}$, perform distance bounding
from v_i to u and obtain db_i
2 With all $v_i \in \mathcal{V}$, compute the estimate (x'_u, y'_u) of the position
by MMSE
3 *If for all* $v_i \in \mathcal{V}$, $\left| db_i - \sqrt{(x_i - x'_u)^2 + (y_i - y'_u)^2} \right| \leq \delta$ *then*
for all $(v_i, v_j, v_k) \in \mathcal{V}^3$, *if* $(x'_u, y'_u) \in \triangle(v_i, v_j, v_k)$
then $\mathcal{T} = \mathcal{T} \cup (v_i, v_j, v_k)$
if $|\mathcal{T}| > 0$ *then* position is accepted and $x_u = x'_u$, $y_u = y'_u$
else the position is rejected
else the position is rejected



Verifiable Multilateration

Collusion attacks (only with untrusted prover under location verification)

- *Attack:*



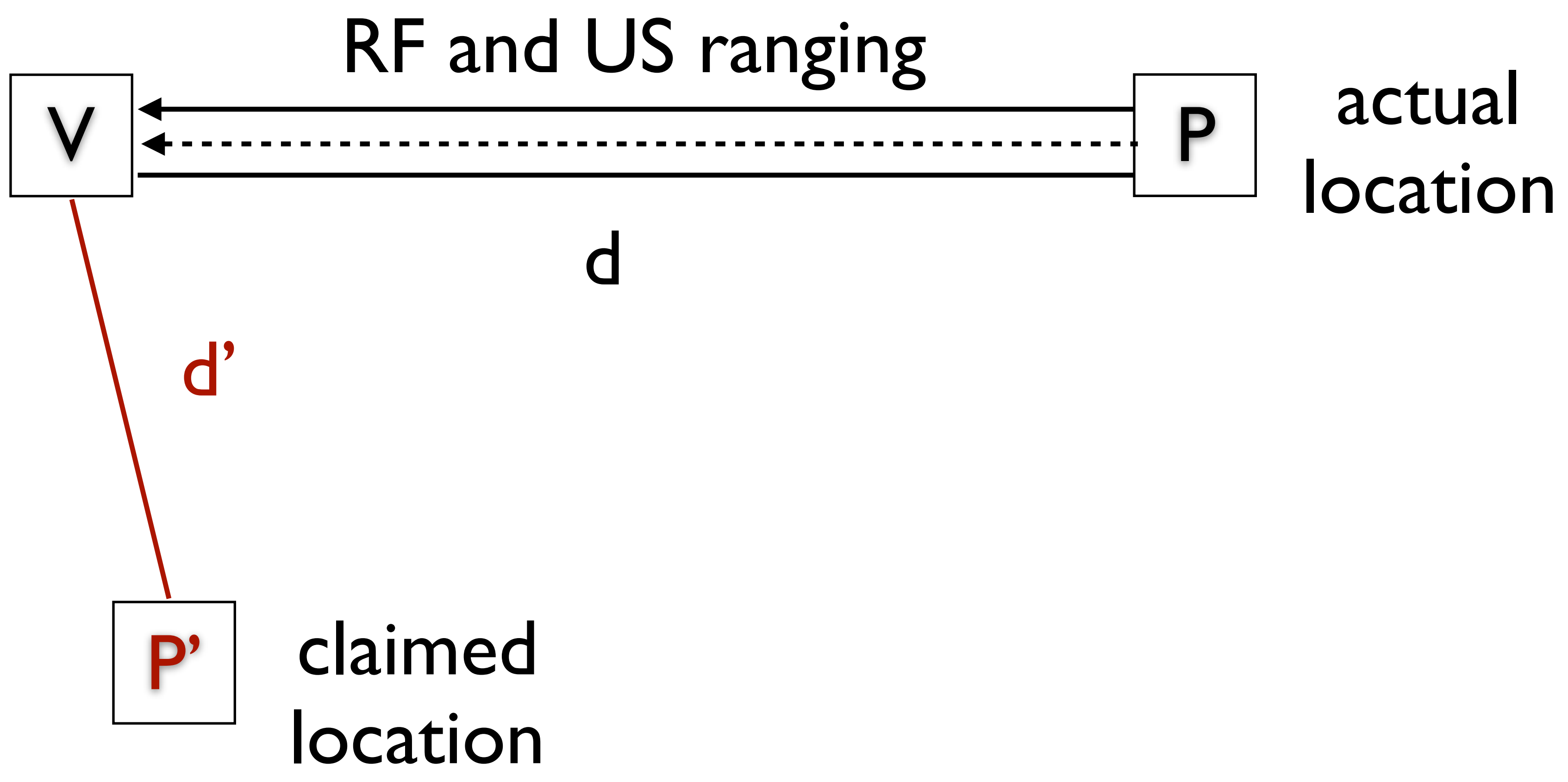
Possible protections:

- Tamper Resistance
- Device Identification

Location Verification using Hidden and Mobile Stations *(Verifiers)*

The basic idea:

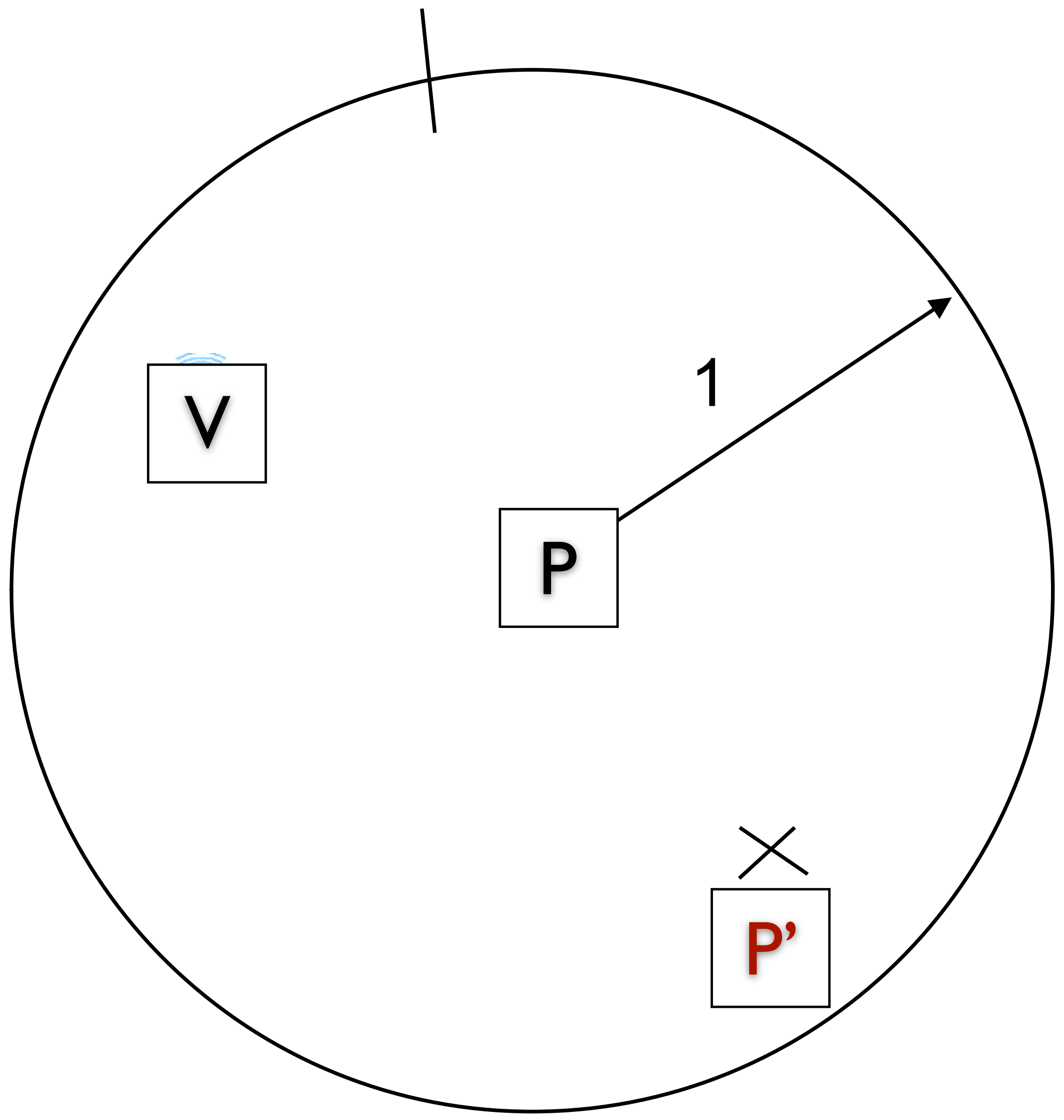
- *If the prover does not know where the verifiers are, it doesn't know how to cheat.*



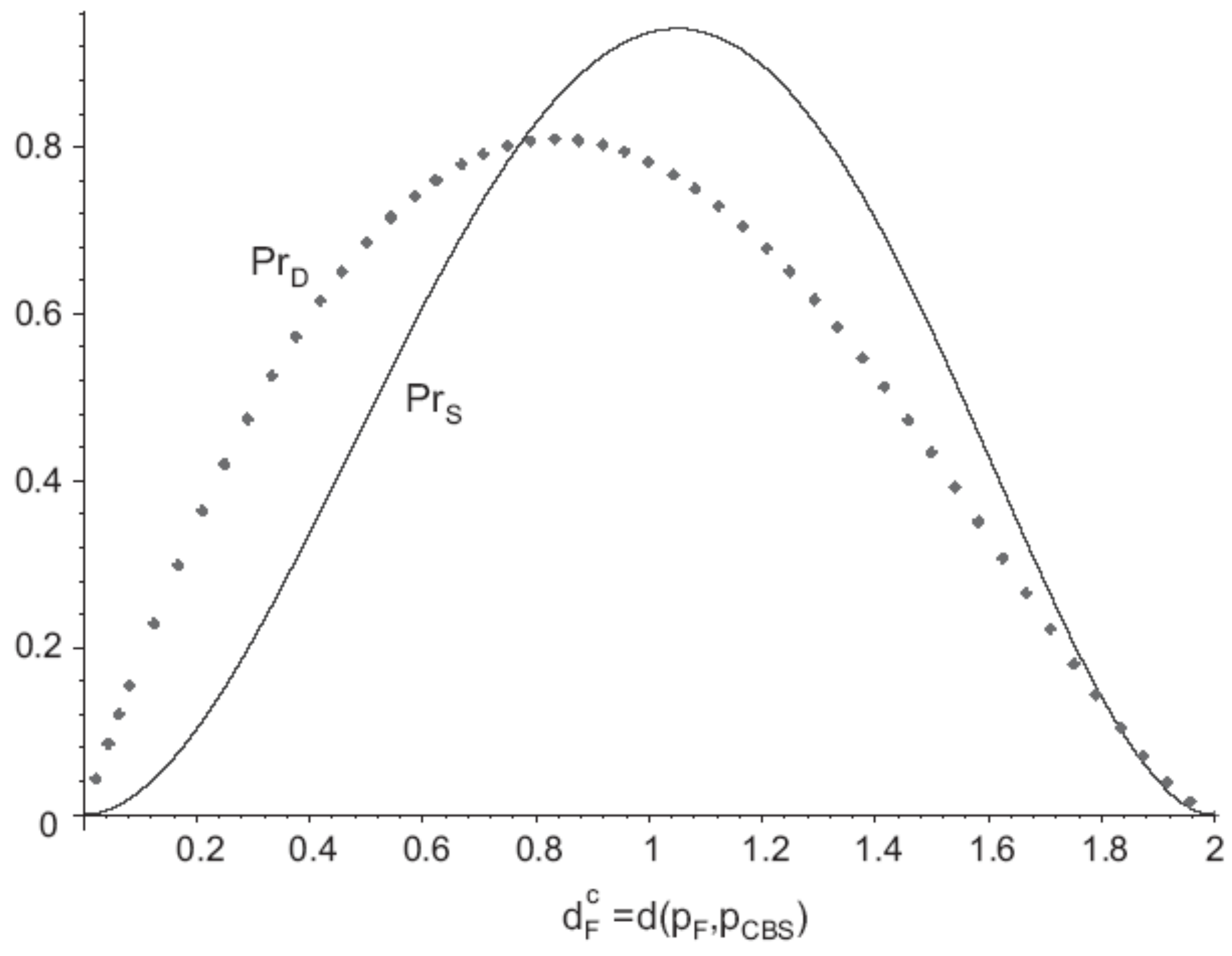
p(successful cheating) = *p(d-d'≤ Δ)*

where Δ is the ranging/localization accuracy

Location Verification using Hidden and Mobile Stations *(Verifiers)*



Observation 1:



not all distances are equally likely

- Not all locations are equally easy to fake (center is the 'easiest').
- *Problems if the attacker knows where verifiers cannot be.*

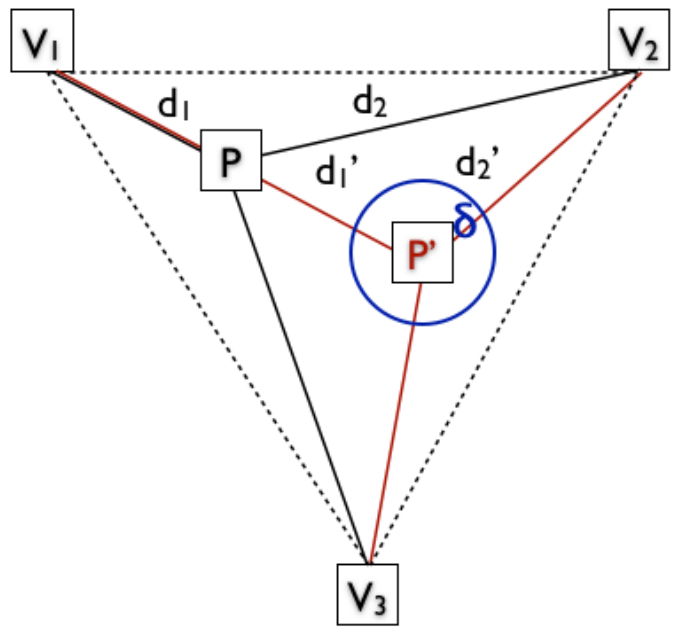
Summary (on secure localization)

Main ideas

- Use time as a side-channel (e.g., distance bounding)
- Use hidden verifier locations
- Use spread spectrum communication (hide the signals such that they cannot be manipulated - in time)

Summary

- Secure Localization / Location Verification is a fascinating area
- Brings up interesting interactions between logical and physical layer
- New challenges in formal protocol analysis



- Can be used for Secure Localization and Location Verification
- Numerous Applications
  - Physical and Logical Access Control, Anti-Spoofing, Protection of Networking Functions, ...