Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Selected Topics in Physical Layer Security:

On Secure Ranging and Localization

Srdjan Čapkun
Department of Computer Science
ETH Zurich

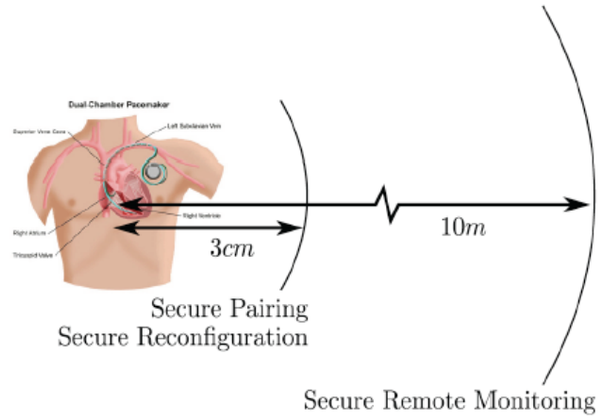
This slide:

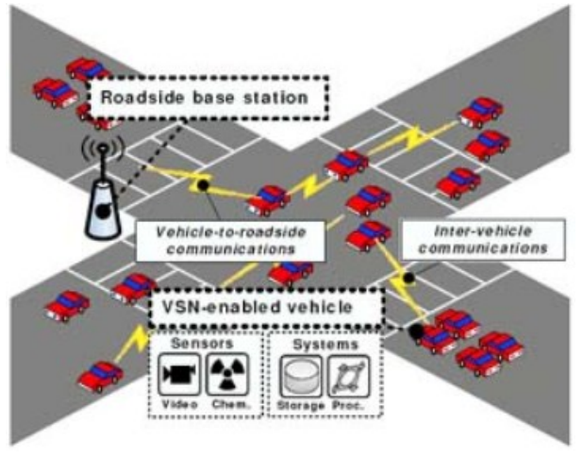
“Wireless is everywhere and important”

Location Information: Large and Small Scale

Interaction between the cyber and physical systems:

- increased security, privacy and safety risks
- Navigation, Location-based Access Control, Tracking of people and valuables, Protection of critical infrastructures, Emergency and rescue
- …



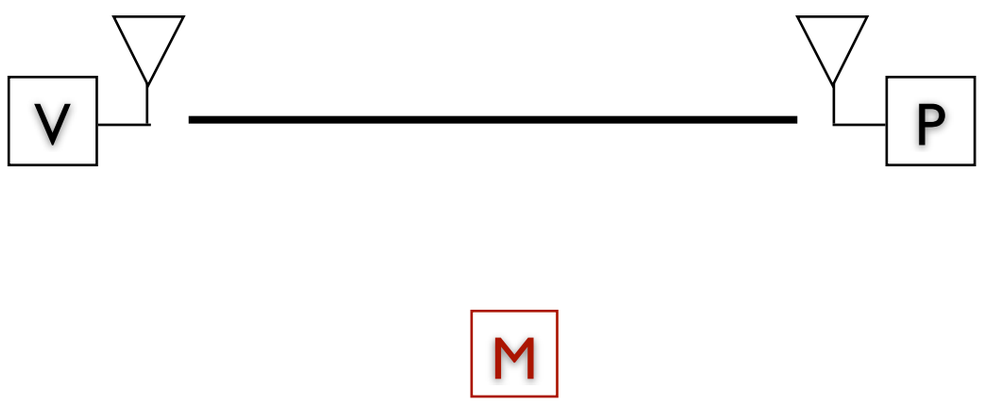


Are *we* physically close?

ETH Zürich

Are *you* physically close to *me*?

Is this *message* coming from close by?

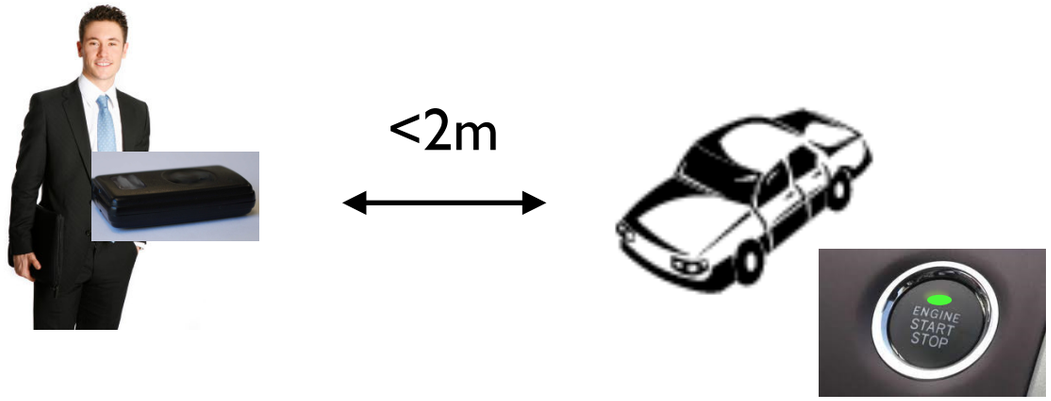


V,P: are we close?

Secure Ranging:

*Compute a 'correct' range to a **trusted** device in the presence of an attacker.*

Example: *Passive Keyless* Entry and Start Systems (PKES)



Entry: Key fob needs to be ***close*** for the car to open

Start: Key fob needs to be ***in the car*** to start the car

No need for human action:
(no button pressing, fob can be in purse)

PKES protocol

K

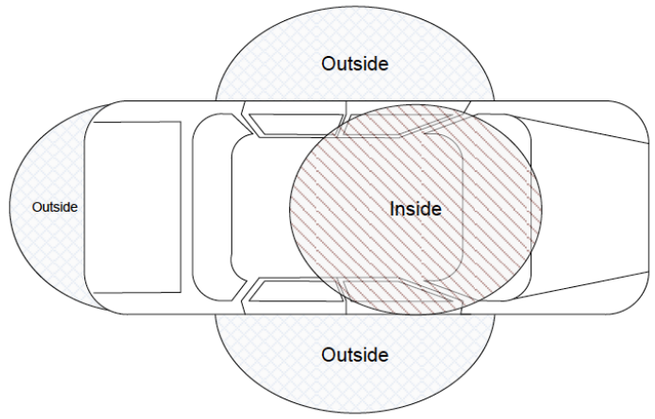
short range (<2m)
Fresh Challenge
(LF, 120-135 KHz)

K

Authentic Reply
(UHF, 315-433 MHz)
long range (<100m)

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

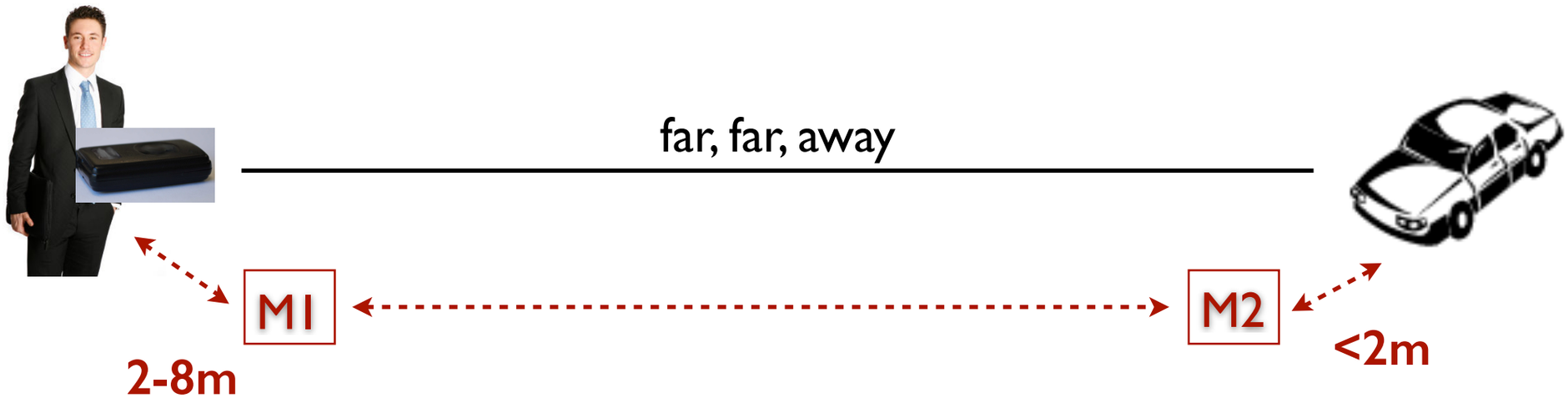
then:
- open door / start car



The main assumption:
communication implies proximity

But it doesn't! (in adversarial settings)

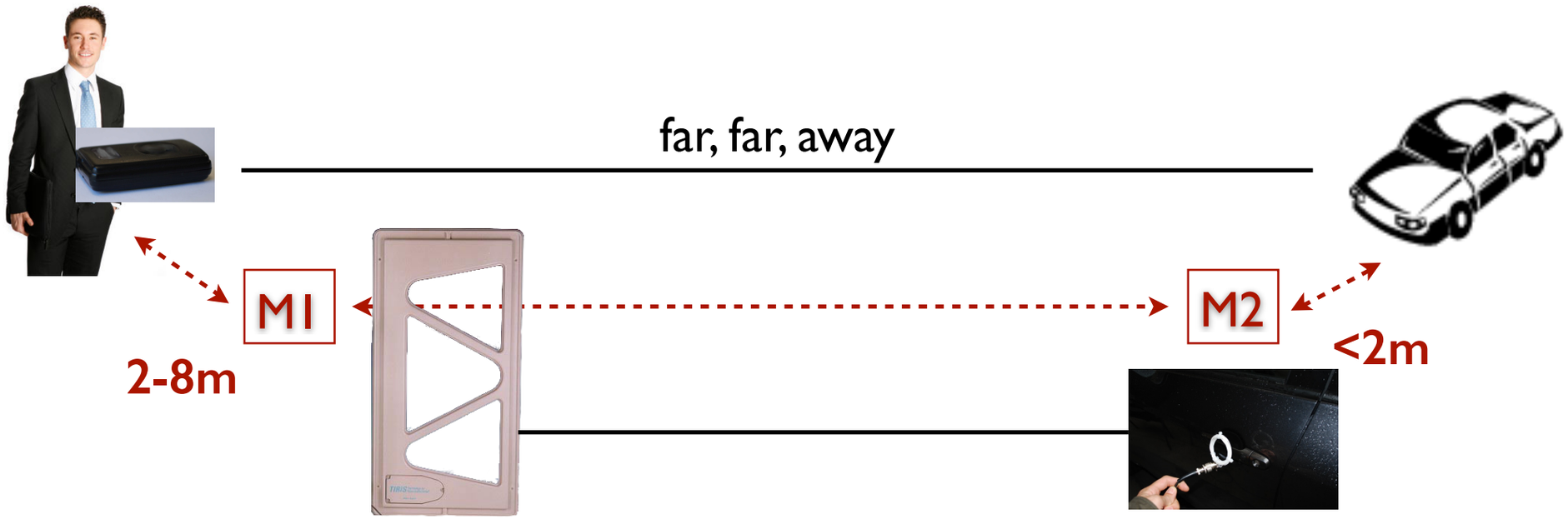
Relay attack on PKES *(wired)* [1]



[1] Aurelien Francillon, Boris Danev, Srdjan Capkun
Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars
NDSS 2011

ETH Zürich

Relay attack on PKES *(wired)* [1]

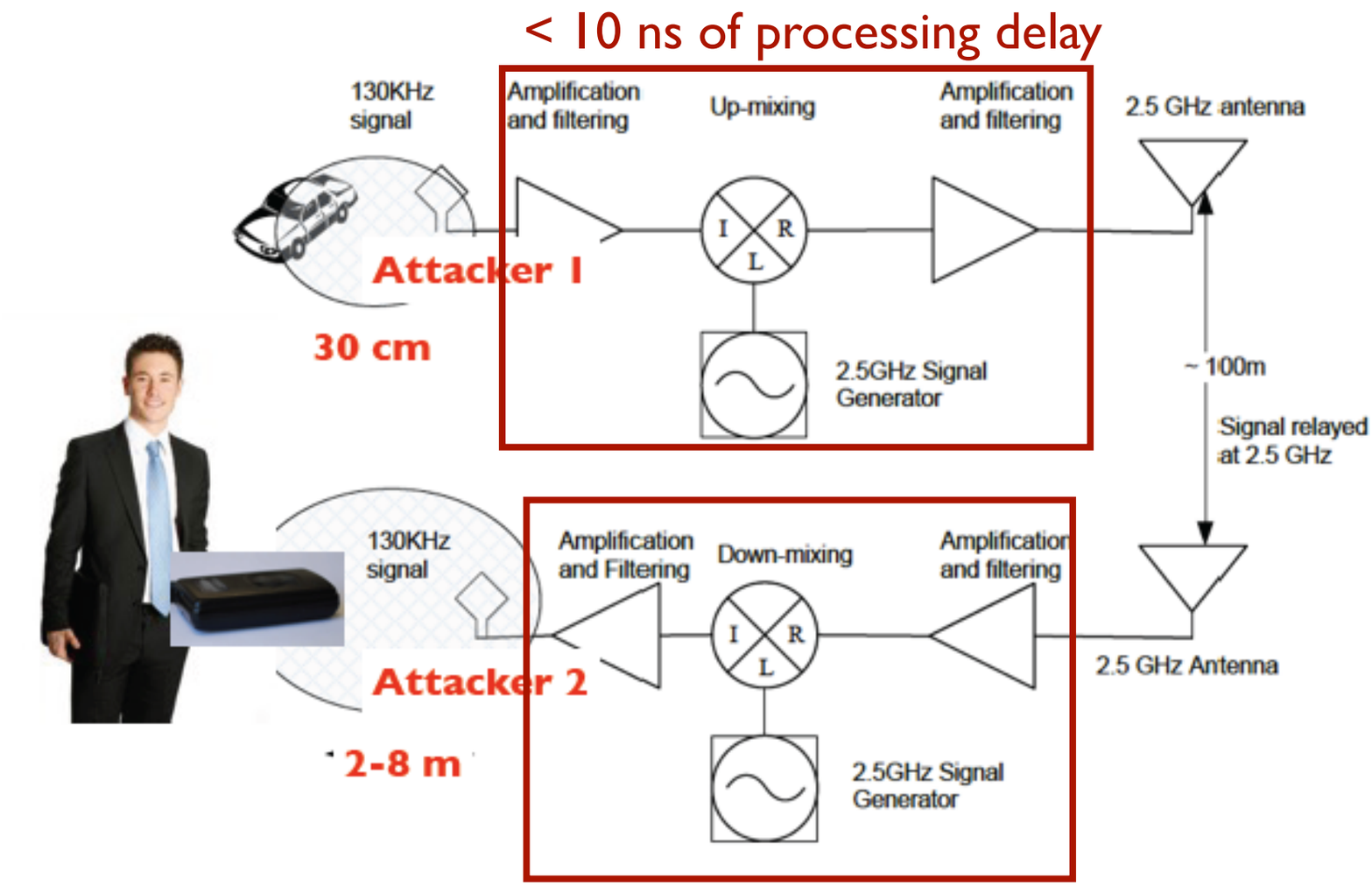


"Wired" attack: 60m wire between M1 and M2 and some antennas

Result: car opened and started

- did not stop after relay broken
- worked in through house windows

Relay attack on PKES *(wireless)* [1]



Distance of *attacker to key* (owner)

Car model	Relay cable						Key to antenna distance (m)			
	7 m		30 m		60 m		No Amplifier		With Amplifier	
	open	go	open	go	open	go	open	go	open	go
Model 1	✓	✓	✓	✓	✓	✓	2	0.4	*	*
Model 2	✓	✓	A	A	A	A	0.1	0.1	2.4	2.4
Model 3	✓	✓	✓	✓	✓	✓	-	-	-	-
Model 4	✓	✓	-	-	-	-	-	-	-	-
Model 5	✓	✓	✓	✓	✓	✓	2.5	1.5	6	5.5
Model 6	✓	✓	A	A	A	A	0.6	0.2	3.5	3.5
Model 7	✓	✓	A	A	-	-	0.1	0.1	6	6
Model 8	✓	A	✓	A	-	-	1.5	0.2	4	3.5
Model 9	✓	✓	✓	✓	✓	✓	2.4	2.4	8	8
Model 10	✓	✓	✓	✓	-	-	-	-	-	-

Maximum Delay not detected by the car

Car model	Max. Delay	Key Response Time (std dev)	Key Response Time Spread
Model 1	500 μs	1782 μs (± 8)	21 μs
Model 2	5 ms	11376 μs (± 15)	47 μs
Model 4	500 μs	-	-
Model 5	1 ms	5002 μs (± 4)	11 μs
Model 6	10-20 ms	23582 μs (± 196)	413 μs
Model 7	620 μs	1777 μs (± 12)	25 μs
Model 8	620 μs	437 μs (± 70)	162 μs
Model 9	2 ms	1148 μs (± 243)	436 μs
Model 10	35 μs	2177 μs (± 8)	12 μs

Distance of *attacker to key* (owner)

Car model	Relay cable						Key to antenna distance (m)			
	7 m		30 m		60 m		No Amplifier		With Amplifier	
	open	go	open	go	open	go	open	go	open	go
Model 1	✓	✓	✓	✓	✓	✓	2	0.4	*	*
Model 2	✓	✓	A	A	A	A	0.1	0.1	2.4	2.4
Model 3	✓	✓	✓	✓	✓	✓	-	-	-	-
Model 4	✓	✓	-	-	-	-	-	-	-	-
Model 5	✓	✓	✓	✓	✓	✓	2.5	1.5	6	5.5
Model 6	✓	✓	A	A	A	A	0.6	0.2	3.5	3.5
Model 7	✓	✓	A	A	-	-	0.1	0.1	6	6
Model 8	✓	A	✓	A	-	-	1.5	0.2	4	3.5
Model 9	✓	✓	✓	✓	✓	✓	2.4	2.4	8	8
Model 10	✓	✓	✓	✓	-	-	-	-	-	-

Maximum Delay not detected by the car

Car model	Max. Delay		Key Response Time (std dev)		Key Response Time Spread	
Model 1	500	μs	1782	μs (±8)	21	μs
Model 2	5	ms	11376	μs (±15)	47	μs
Model 4	500	μs	-		-	
Model 5	1	ms	5002	μs (±4)	11	μs
Model 6	10-20	ms	~~23582~~	~~μs (±196)~~	~~413~~	~~μs~~
Model 7	620	μs	1777	μs (±12)	25	μs
Model 8	620	μs	437	μs (±70)	162	μs
Model 9	2	ms	1148	μs (±243)	436	μs
Model 10	35	μs	~~2177~~	~~μs (±8)~~	~~12~~	~~μs~~

1500 km

5 km

ETH Zürich

Immediate countermeasures

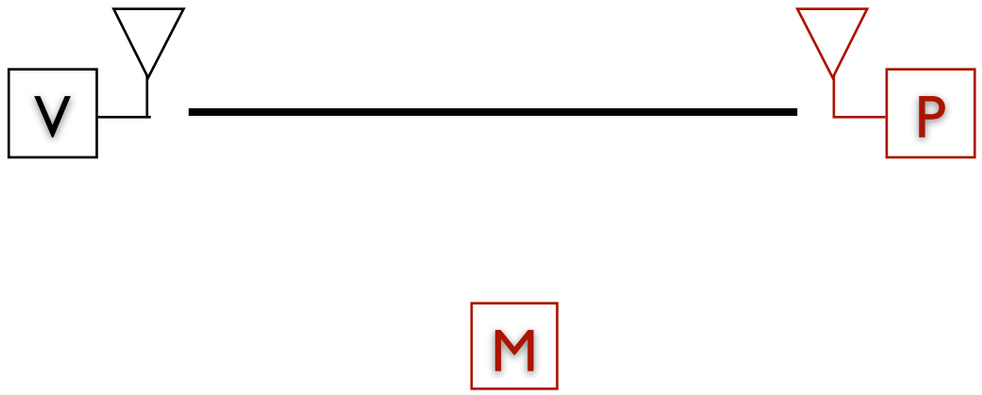
- Shield the key
- Remove the battery from the key

Lesson learnt: *communication does not imply proxir*

- no control over attackers antenna gain, transmission power, ...
- assumptions on attacker's processing speed are hard to make

Way forward:

- Build a new system that securely *verifies proximity through precise timing*
- Industry is already working on this (e.g., 3DB Access)



V,P: are we close?

Secure Ranging:

Compute a ‘correct’ range of a **trusted** device in the presence of an attacker.

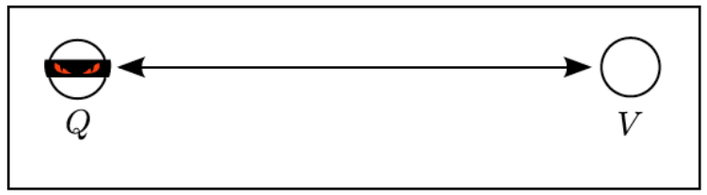
V: is P close?

Proximity Verification:

Verify the correctness of a proximity claim of an **untrusted** device.

More Properties

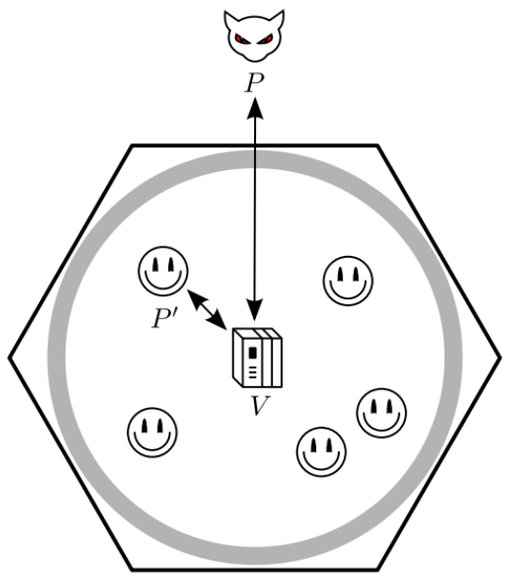
Distance Fraud



Terrorist Fraud

Mafia Fraud

Distance Hijacking [2]

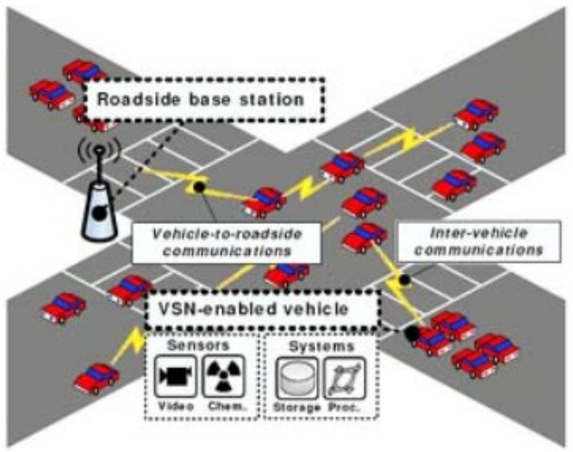


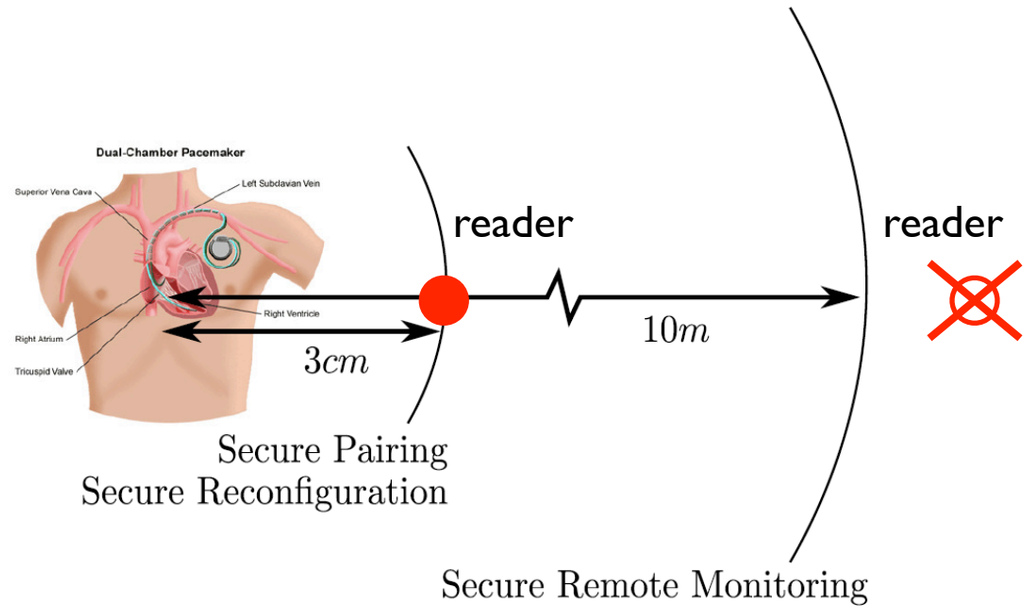
[2] Cas Cremers, Kasper Bonne Rasmussen, Benedikt Schmidt, Srdjan Capkun
Distance Hijacking Attacks on Distance Bounding Protocols, IEEE S&P 2012

ETH Zürich

Systems Affected (current and future)

- NFC payments: proximity => authorization to pay
- Buildings/Offices: proximity => authorization to enter
- Implants: proximity => access control to data / configuration
- WiFi: proximity => access to network
- Key establishment: proximity => intention to pair devices
- PKES: proximity => authorization to enter / drive
- …





Lesson learned:

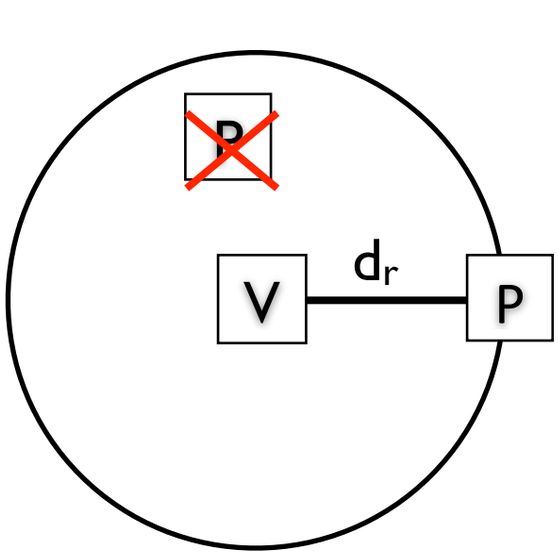
Authenticated communication

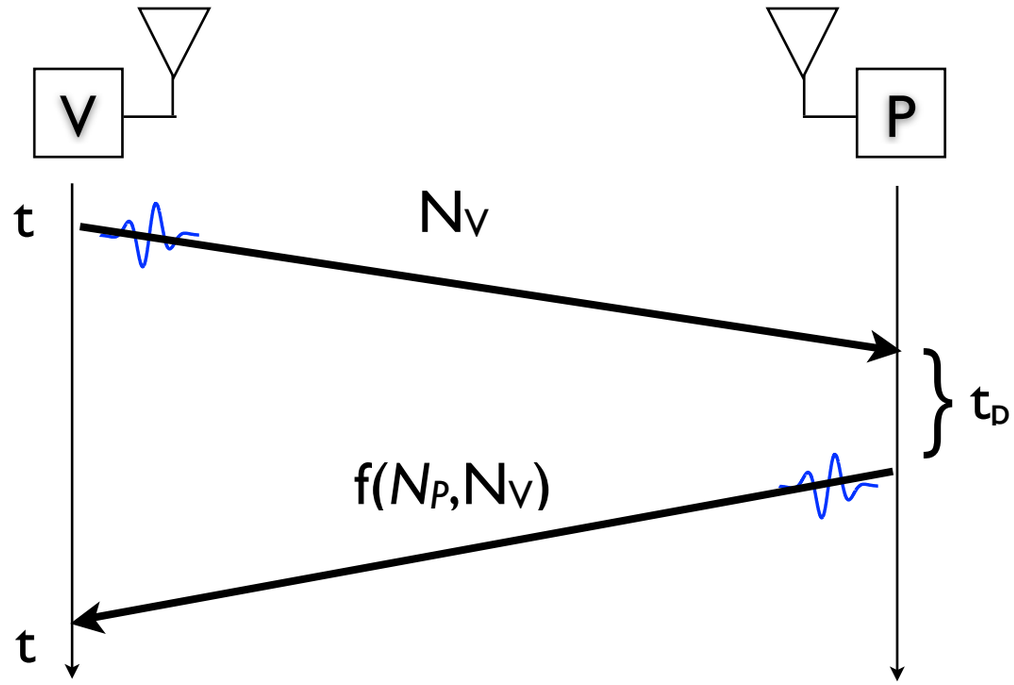
***doesn't** imply proximity!*

We need to build different primitives:

Distance Bounding Protocols

Secure Proximity Verification using Distance Bounding Protocols [3]





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

***V**: is P close?*

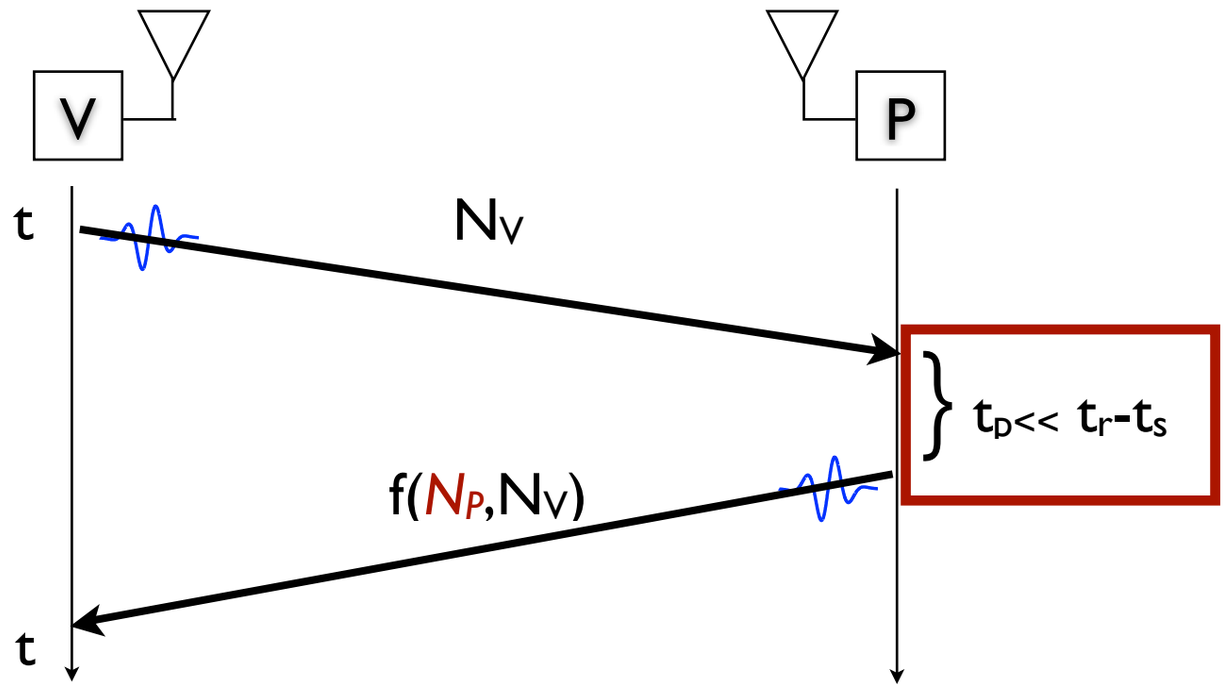
[3] Stefan Brands, David Chaum: **Distance-bounding protocols**, Eurocrypt '93.

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



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

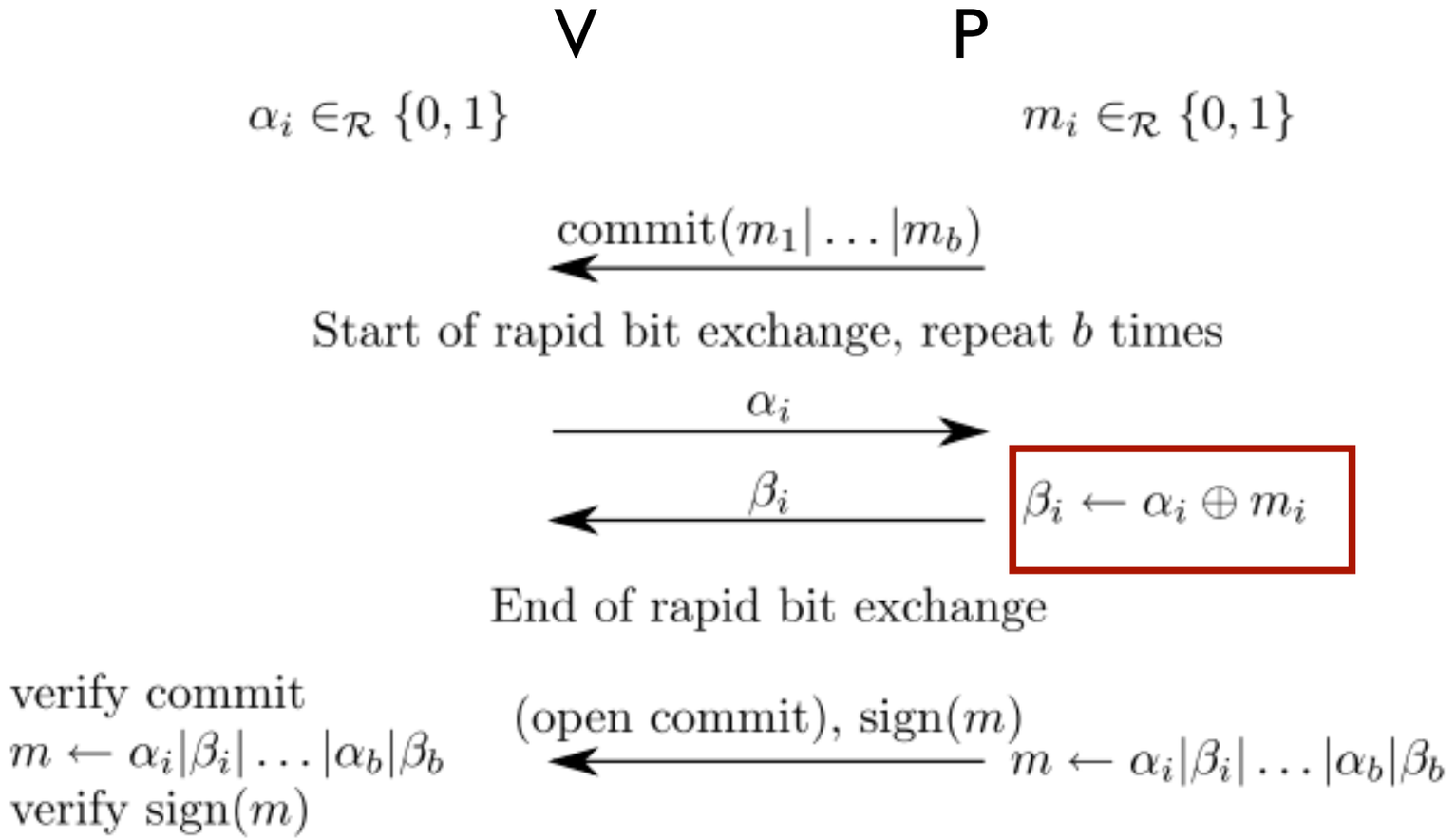
Distance Bounding: *f() and t_p*

[4] sign(), h(), mac(), E(), ... => t_p >> ns

[3] *XOR* => t_p = ?

[5] *bit comparison* => t_p = ?

> 30 proposed protocols



[3] Stefan Brands, David Chaum: **Distance-bounding protocols**, Eurocrypt '93.

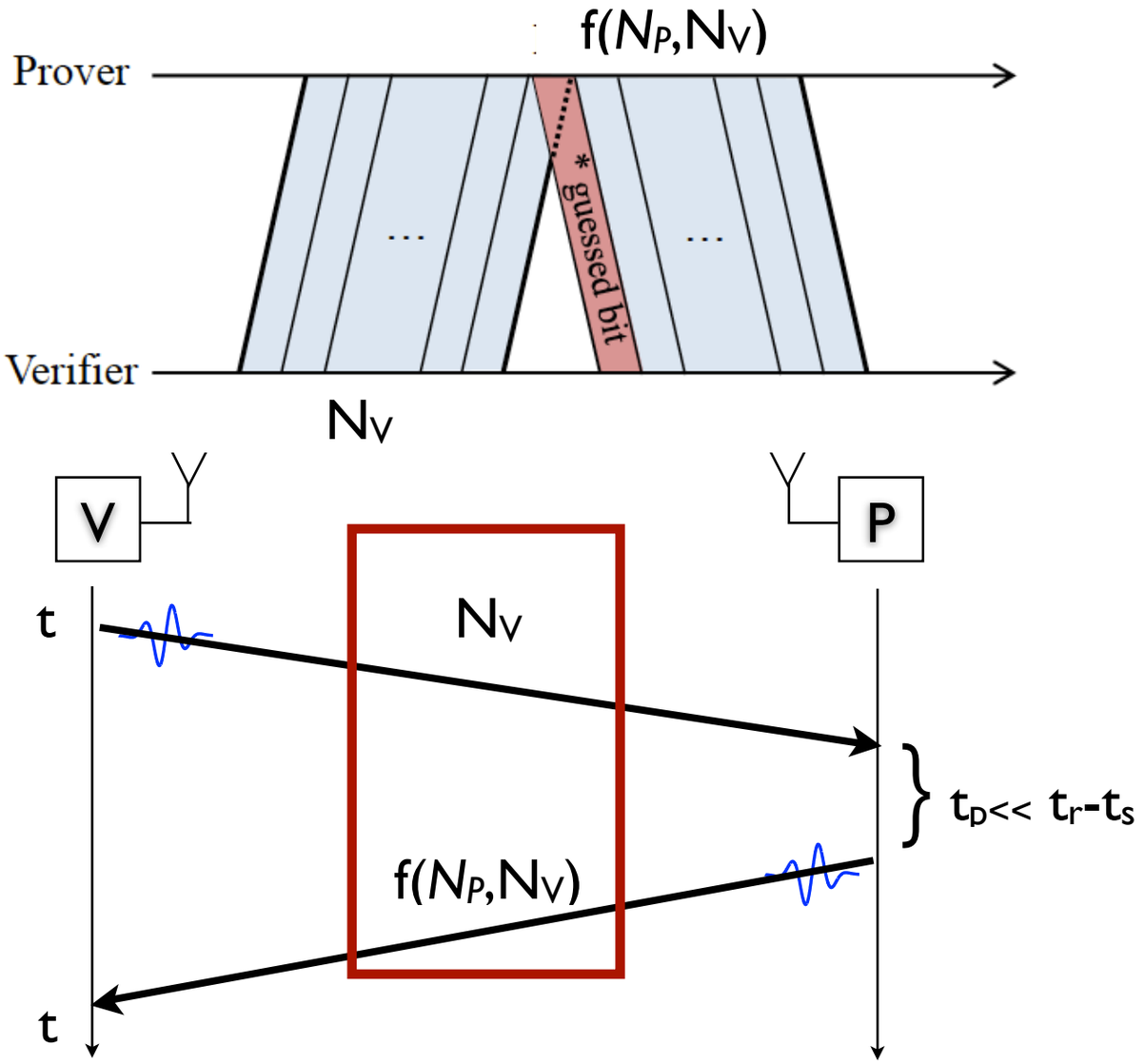
[4] Thomas Beth and Yvo Desmedt. **Identification tokens - or: Solving the chess grandmaster problem**, CRYPTO ’90:

[5] Gerhard Hancke, Markus Kuhn: **An RFID distance-bounding protocol**, SecureComm 2005

Distance Bounding: N_v length

N_V and f(NV,NP) should be "short" in the # of bits [6]

- short compared to the required accuracy / security

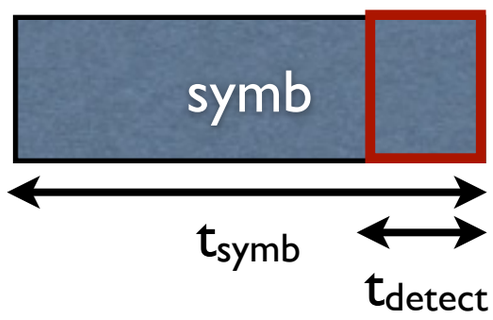


[6] Jolyon Clulow, Gerhard P. Hancke, Markus G. Kuhn, and Tyler Moore.
So near and yet so far: Distance-bounding attacks in wireless networks, ESAS, 2006

Distance Bounding: *symbols*

Assuming $|N_V|$=1bit, the symbols should be short as well [6]

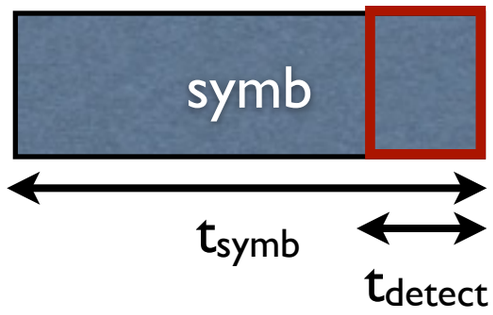
- short compared to the required accuracy / security
- Early Detection
- Late Commit
- Note: *channel spread does not help*
- Ideal: short (<1ns) UWB pulses

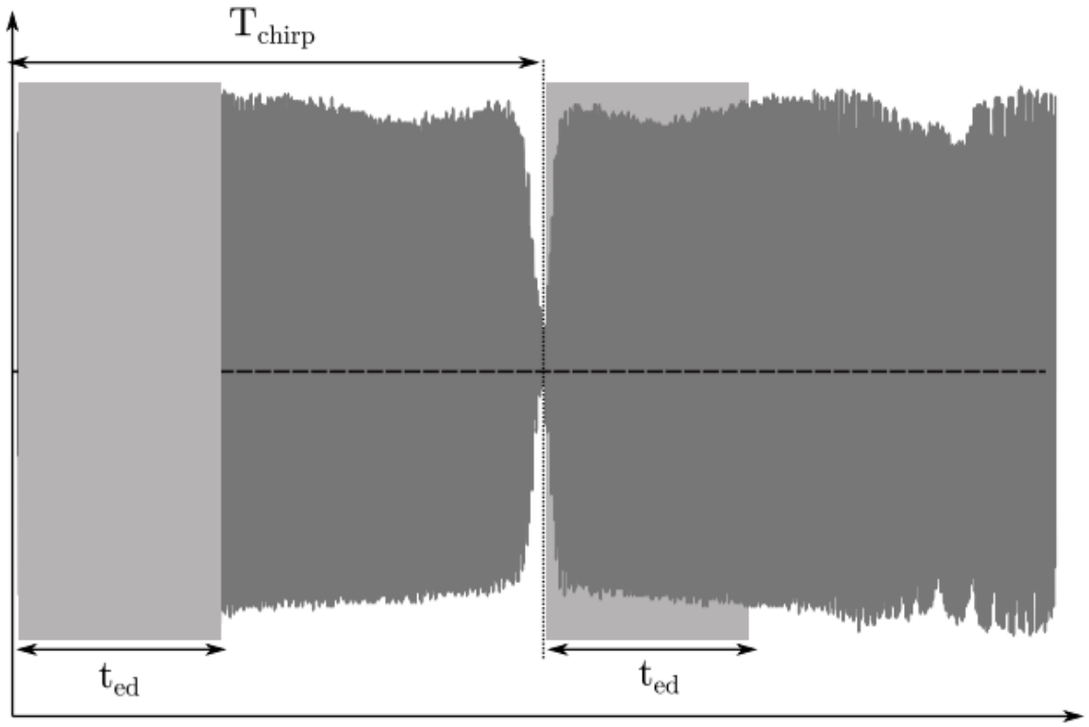


Distance Bounding: *symbols*

Example: Chirp SS ranging (802.15.4) systems strongly affected

- long symbol lengths allow for simple ED and LC attacks
- Early Detection
- Late Commit
- Attacks on CSS ranging system successful [7]





(a) Signal properties of early detect.

[7] Aanjhan Ranganathan, Boris Danev, Aurélien Francillon, Srdjan Capkun,
Physical-Layer Attacks on Chirp-based Ranging Systems
In Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (**WiSec**), 2012

Thus in order to build a DB system ..

We need:

- prover to receive, process and send in few nseconds
- robust logical and *physical-layer* protocol design

=>

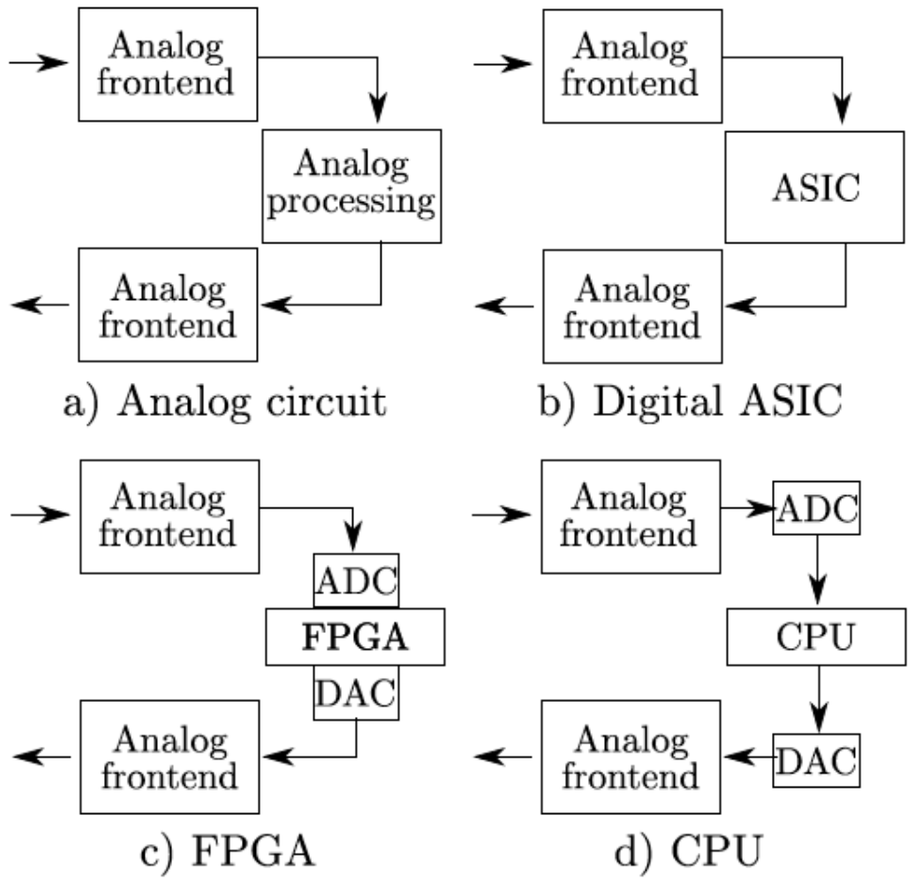
- a fast ***processing function*** (order of ns)
- appropriate ***modulation*** (i.e., short symbol lengths)
- high precision ***ranging system***
- DB protocols

Different choices will lead to *different security guarantees:*

- distance by which the attacker can cheat
- types of attacks that the system resists
  (mafia, distance, terrorist, hijacking)

Main Design Choices

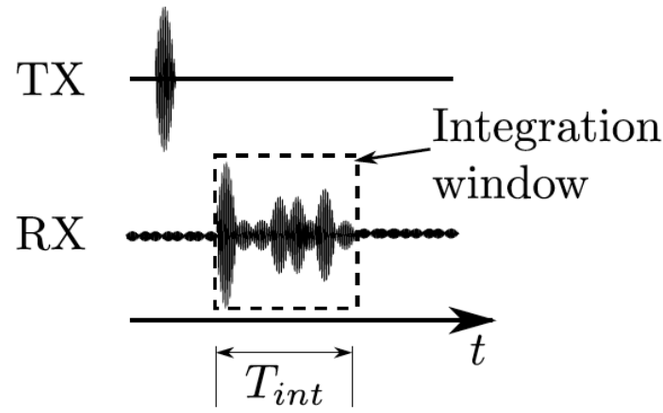
- Digital transceiver [8]
  - longer processing times
  - broader choice of functions
  - easier protocol design
- Analog transceiver [9]
  - shorter processing times
  - limited set of functions
  - more restricted protocol design

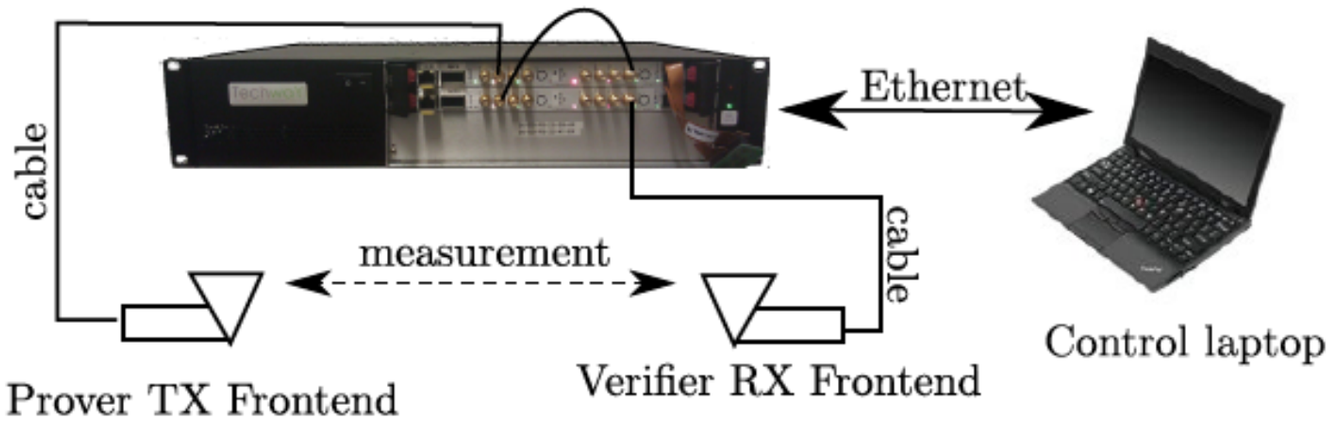


[8] Nils Ole Tippenhauer
Physical-Layer Security Aspects of Wireless Localization, PhD Thesis, ETH Zurich, 2012
[9] Kasper Bonne Rasmussen, Srdjan Capkun
Realization of RF Distance Bounding, **USENIX Security Symposium**, 2010

Digital [8]

- f() = XOR
- UWB-based ranging (1ns pulses)
- Special modulation (SEM), a form of PPM
- Protocols: many protocols can work on top
- ***< 70ns processing delay => 10m distance reduction***

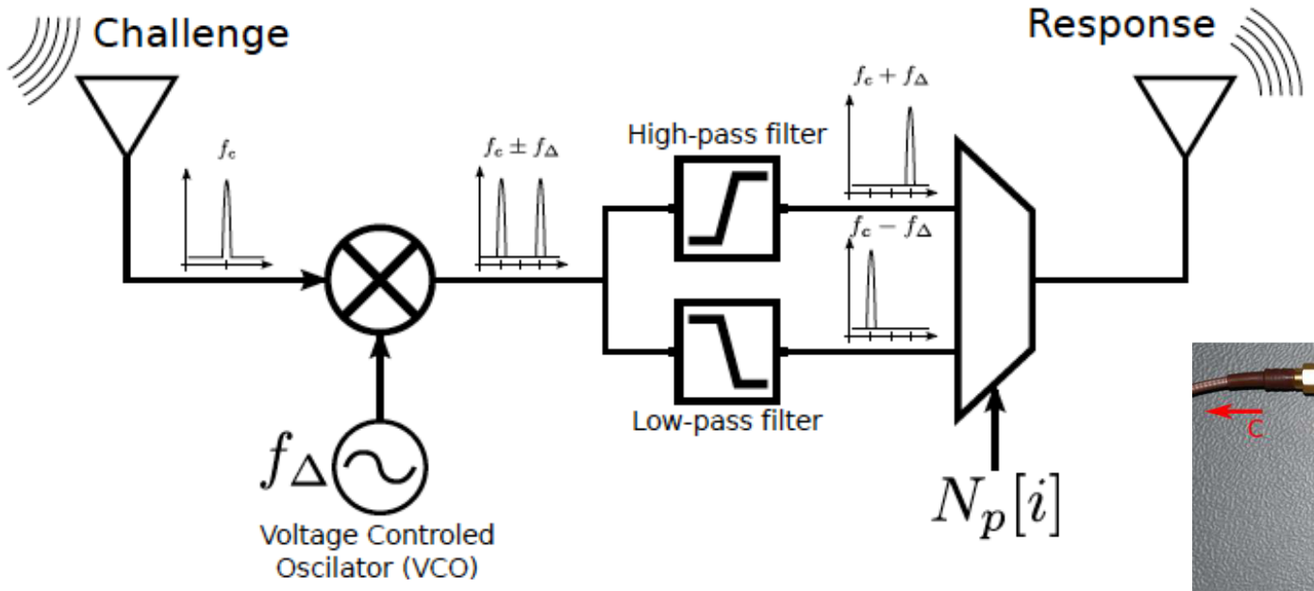




Analog [9]

Challenge Reflection with Channel Selection

- Prover does not interpret Nv (only reflects it)
- All *time-critical* processing is done in *analog*
- Verifier does “all the work”
- ***1ns of processing delay => 15cm of distance reduction***



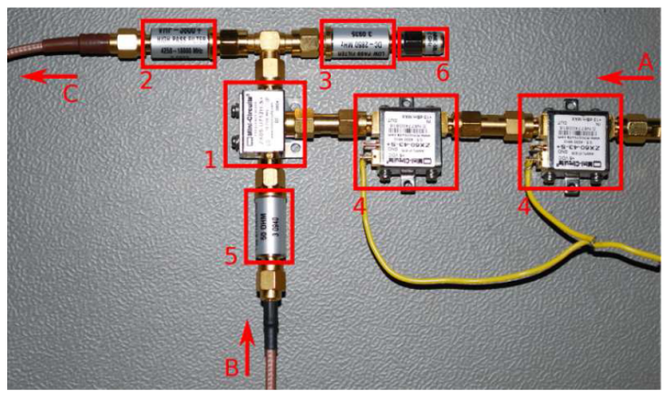


Figure 6: This picture shows the prototype implementation of the prover. It consists of a mixer (1), a high-pass filter (2), a low-pass filter (3), four amplifiers (4) (only two visible), a 1dB attenuator (5) and a terminating resistor (6). The signal from the receiving antenna (A) is mixed with the local oscillator (B) and sent to the transmitting antenna (C). The yellow wires are power (+5V).

ETH Zürich

Main Design Choices

- Digital transceiver [8]
  - longer processing times (70 ns => 10m); (upd 2013: 40ns)
  - broader choice of functions (XOR, comparison, ...)
  - easier protocol design
  - Broader application:
    Distance, Mafia, Terrorist, Hijacking - resilient
- Analog transceiver [9]
  - shorter processing times (1ns => 15cm)
  - limited set of functions (analog)
  - more restricted protocol design
  - More narrow application:
    Distance, Mafia - resilient
- Analog transceiver with Terrorist Fraud Resilience [7]
  - compromise on the processing time (0.5m, 4.51m)

Formal Analysis of Distance Bounding

Authentication and Key Establishment protocols

- analyzed in the Dolev-Yao model
- no notions of location, channel characteristics, (or time)
- the same frameworks cannot analyze DB protocols

New frameworks can capture physical properties *(time, location, physical layer) e.g.,* [10]

- Model based on experiments with real systems
- Enables formal analysis of DB protocols
- Captured new attacks on DB that we missed in the informal analysis

[10] Patrick Schaller, Benedikt Schmidt, David Basin, Srdjan Capkun
Modeling and Verifying Physical Properties of Security Protocols for Wireless Networks, IEEE CSF 2009

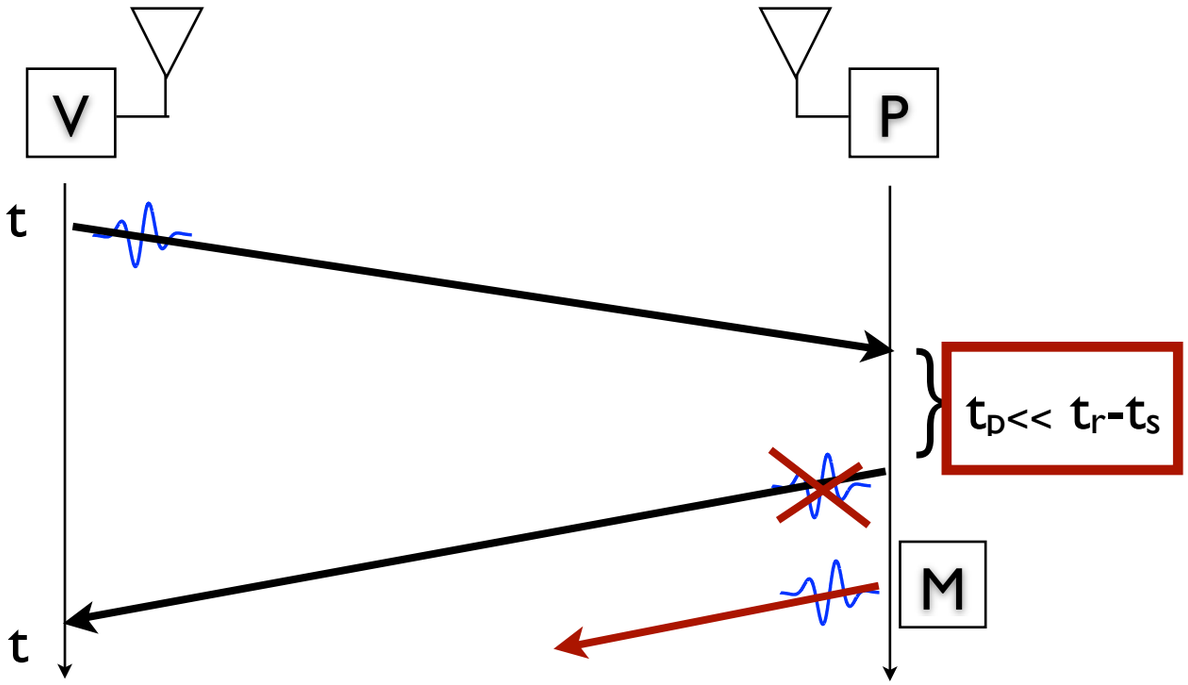
From Ranges to Locations

Distance Bounding

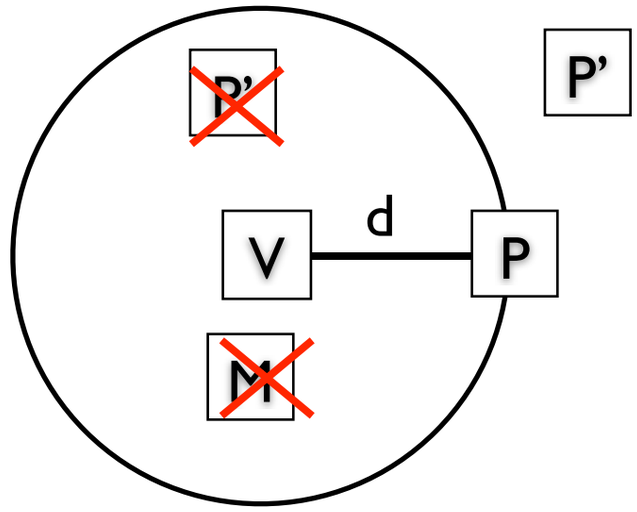
- P can always pretend to be further from V
- M can always convince P and V that they are further away

*=> Distance **enlargement is easy, distance reduction is prevented** using distance bounding protocols*

Ranging



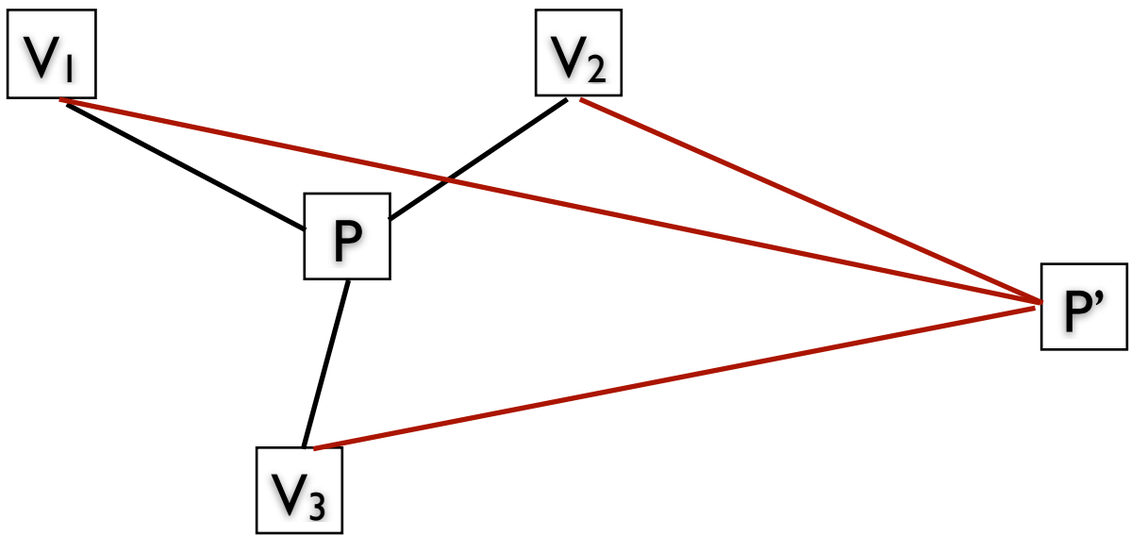
$d = (t_r - t_s - t_p)c/2$



From Ranges to Locations?

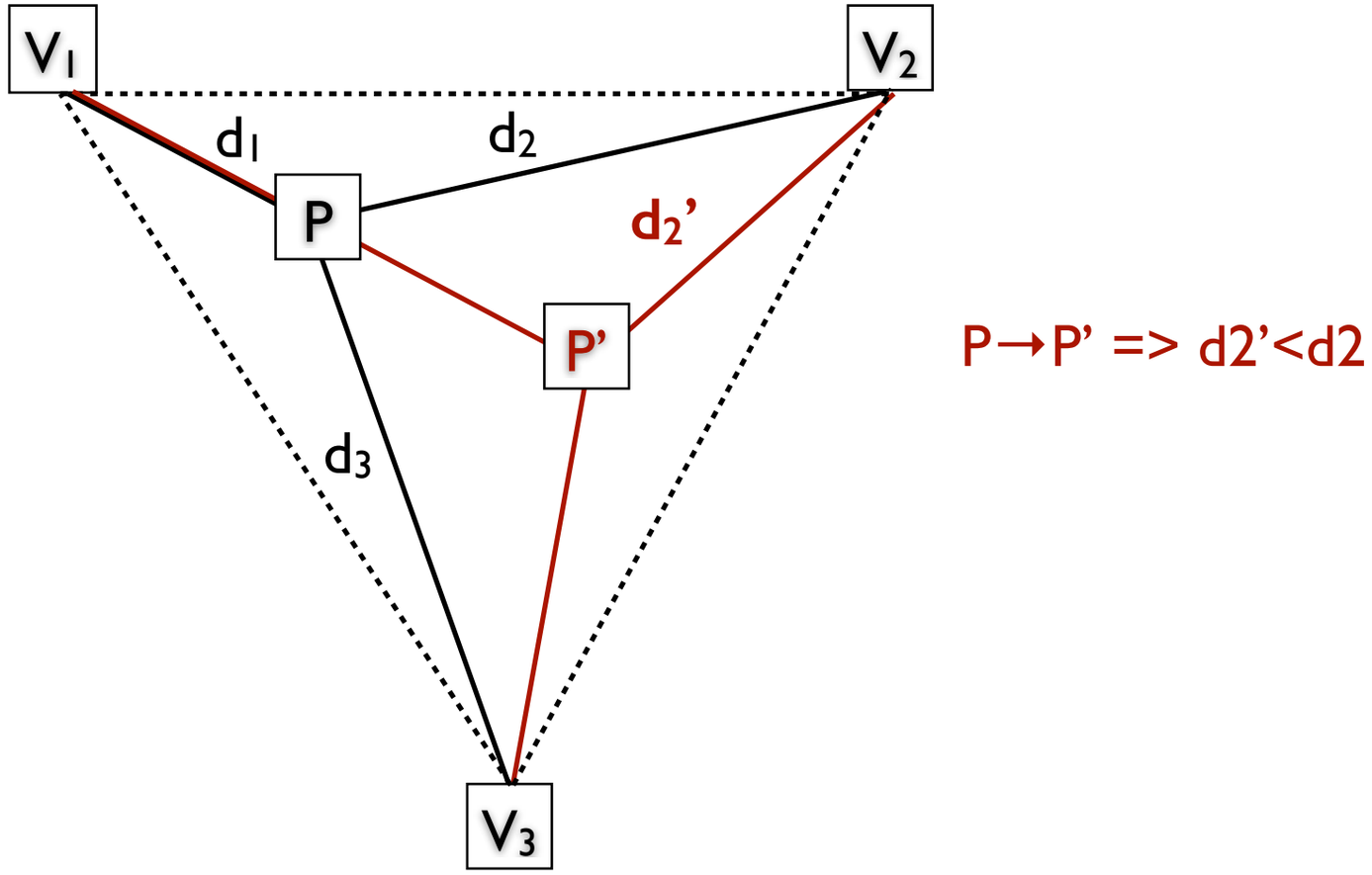
Distance enlargement is easy, distance reduction is prevented using distance bounding protocols

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



Verifiable Multilateration [12]

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.*

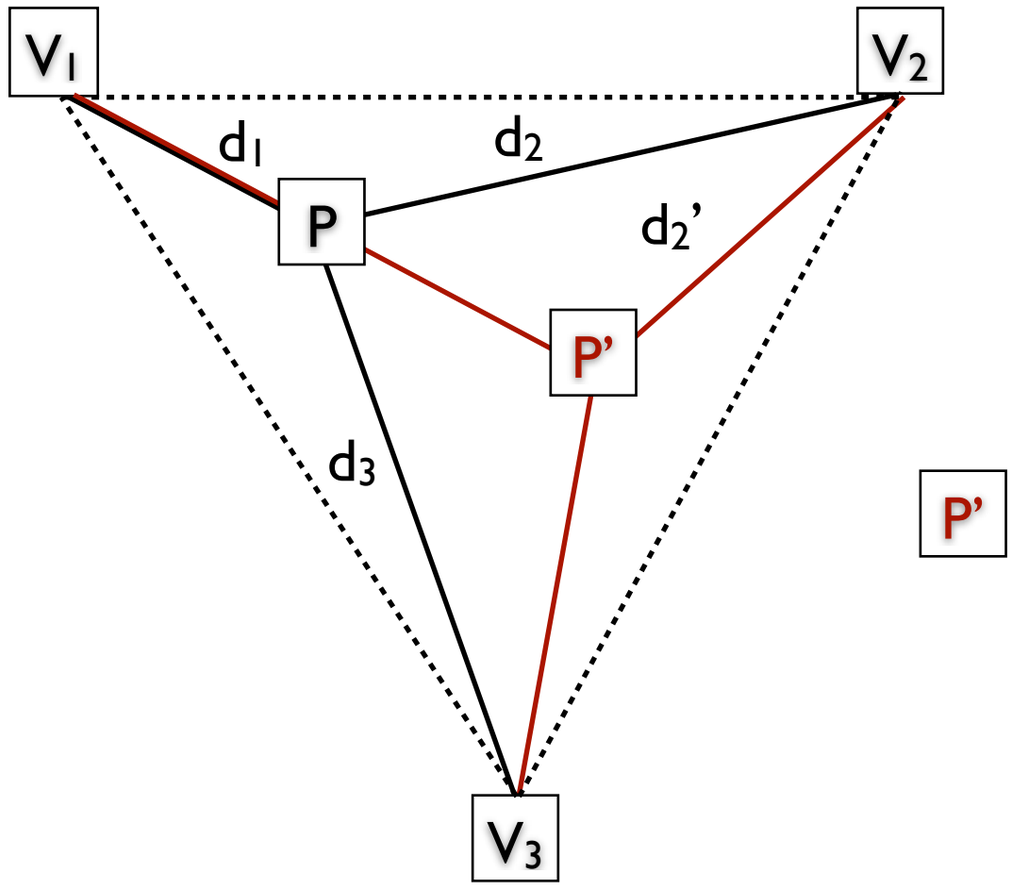


[12] S.Capkun, J.P. Hubaux,
Secure positioning of wireless devices with application to sensor networks, INFOCOM 2005

Verifiable Multilateration [12]

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

Lessons learned:

With distance bounding we can enable

Secure Localization (prevent spoofing)

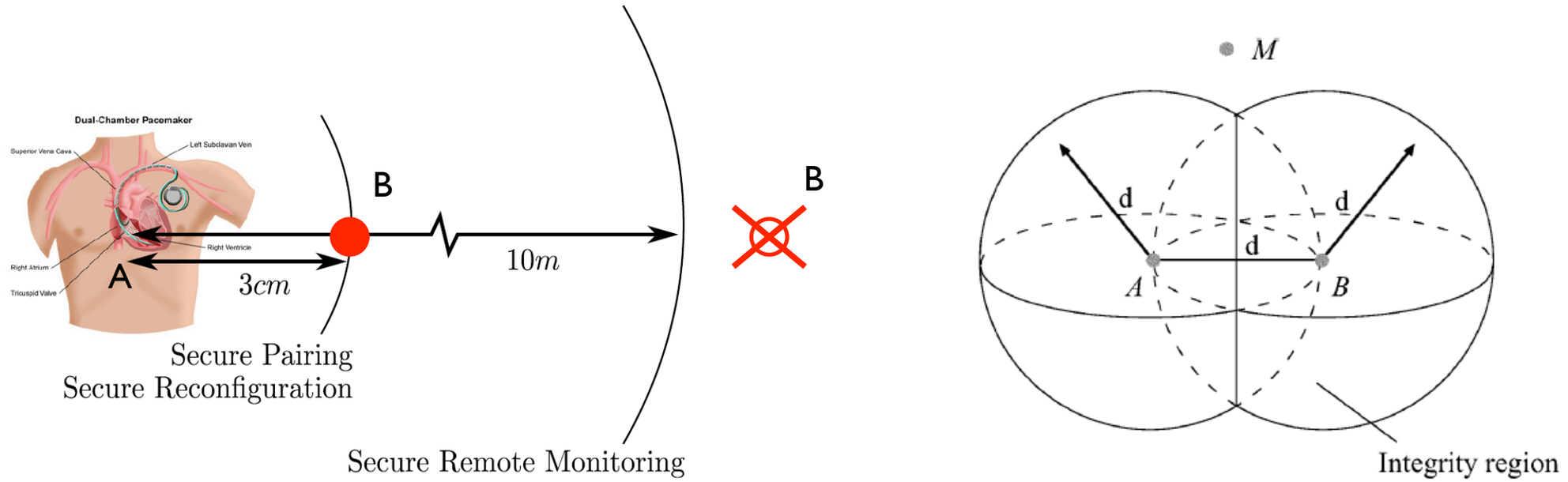
and Location Verification

Location Verification remains vulnerable to attackers with several carefully placed devices.

now that we have Distance Bounding ...

Message Authentication

Based on *Absence* Awareness

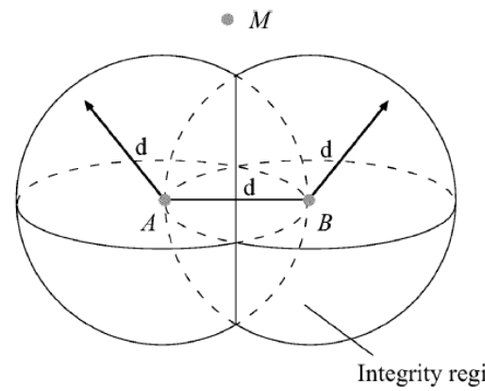


The protocol needs to ensure that **(derived) *key is bound to distance***. [11]

[11] Kasper Bonne Rasmussen, Claude Castelluccia, Thomas S. Heydt-Benjamin, Srdjan Capkun
Proximity-based Access Control for Implantable Medical Devices, ACM CCS 2009

ETH Zürich

Diffie-Hellman with Distance Bounding



Alice		Bob
Given ID_A, g^{X_A}		Given ID_B, g^{X_B}
Pick $N_A, R_A \in_U \{0,1\}^k$		Pick $N_B, R_B \in_U \{0,1\}^k$
$m_A \leftarrow 0 \Vert ID_A \Vert g^{X_A} \Vert N_A$		$m_B \leftarrow 1 \Vert ID_B \Vert g^{X_B} \Vert N_B$
$(c_A, d_A) \leftarrow \text{commit}(m_A)$		$(c_B, d_B) \leftarrow \text{commit}(m_B)$
$(c'_A, d'_A) \leftarrow \text{commit}(0 \Vert R_A)$		$(c'_B, d'_B) \leftarrow \text{commit}(1 \Vert R_B)$
	$c_A, c'_A \rightarrow$	
	$\leftarrow c_B, c'_B$	
	$d_A \rightarrow$	$\hat{m}_A \leftarrow \text{open}(\hat{c}_A, \hat{d}_A)$
$\hat{m}_B \leftarrow \text{open}(\hat{c}_B, \hat{d}_B)$	$\leftarrow d_B$	Verify 0 in $\hat{m}_A$; $i_B \leftarrow N_B \oplus \hat{N}_A$
Verify 1 in $\hat{m}_B$; $i_A \leftarrow N_A \oplus \hat{N}_B$		
— distance-bounding phase —		
The bits of R_A are $R_{A1}, R_{A2}, \ldots, R_{Ak}$		The bits of R_B are $R_{B1}, R_{B2}, \ldots, R_{Bk}$
The bits of i_A are $i_{A1}, i_{A2}, \ldots, i_{Ak}$		The bits of i_B are $i_{B1}, i_{B2}, \ldots, i_{Bk}$
$\alpha_1 \leftarrow R_{A1} \oplus i_{A1}$	$\alpha_1 \rightarrow$	
	$\leftarrow \beta_1$	$\beta_1 \leftarrow R_{B1} \oplus i_{B1} \oplus \hat{\alpha}_1$
	...	
$\alpha_i \leftarrow R_{Ai} \oplus i_{Ai} \oplus \hat{\beta}_{i-1}$	$\alpha_i \rightarrow$	Measure delay between β_{i-1} and $\hat{\alpha}_i$
Measure delay between $\hat{\beta}_i$ and α_i	$\leftarrow \beta_i$	$\beta_i \leftarrow R_{Bi} \oplus i_{Bi} \oplus \hat{\alpha}_i$
	...	
$\alpha_k \leftarrow R_{Ak} \oplus \hat{\beta}_{k-1}$	$\alpha_k \rightarrow$	Measure delay between β_{k-1} and $\hat{\alpha}_k$
Measure delay between $\hat{\beta}_k$ and α_k	$\leftarrow \beta_k$	$\beta_k \leftarrow R_{Bk} \oplus \hat{\alpha}_k$
— end of distance-bounding phase —		
	$d'_A \rightarrow$	$0 \Vert \hat{R}_A \leftarrow \text{open}(\hat{c}'_A, \hat{d}'_A)$
$1 \Vert \hat{R}_B \leftarrow \text{open}(\hat{c}'_B, \hat{d}'_B)$	$\leftarrow d'_B$	
$\hat{i}_{Bi} \leftarrow \alpha_i \oplus \hat{\beta}_i \oplus \hat{R}_{Bi} \quad (i = 1, \ldots, k)$		$\hat{i}_{A1} \leftarrow \hat{\alpha}_1 \oplus \hat{R}_{A1}$
Verify $i_A \stackrel{?}{=} \hat{i}_B$		$\hat{i}_{Ai} \leftarrow \hat{\alpha}_i \oplus \beta_{i-1} \oplus \hat{R}_{Ai} \quad (i = 2, \ldots, k)$
		Verify $i_B \stackrel{?}{=} \hat{i}_A$

Alice and Bob visually verify that there are no other users/devices in their "integrity region".

Lessons learned:

Absence awareness can enable authentication.

Presence awareness can enable authentication.
(not covered in this talk)

What about GPS?

- Satellites broadcast navigation signals
- GPS ***RECEIVERS*** (i.e., not intended to transmit signals back to the satellites)
- One cannot use distance bounding to protect this navigation system

some time ago ...

French secret services accused of dirty tricks in Tank deal.

A £1bn tank bid to supply the Greek government with Challenger 2 tanks has raised suspicions that the French secret services used dirty tricks to scupper the British bid. French and British teams were among four countries in competition for the tender to supply 250 Tanks. The other countries being Germany and America.

During the tests the British Challenger tanks had difficulty with navigation and were unable to work out exactly where they were. The British use the satellite global positioning system, GPS, for navigation, whilst the French had no such problems with their navigation.

The Americans also claimed that their navigation suffered difficulty and it was later alleged that the French were covertly interfering with a GPS signal.

Investigations showed that a signal was transmitted blocking the signal from one satellite. Since the GPS system needs the signal from 3 or more satellites for accuracy the loss of just one signal means errors in navigation in excess of 100 yards.

In 1995 an American Institute think-tank estimated that France was devoting a third of its secret service budget to economic intelligence. This may well be true since agents from the DST, Direction et Surveillance du Territoire, [French Internal Security Service] removed documents from a hotel in Tolouse where British Aerospace executives were staying.

The Greek officials found the whole event to be most amusing and discounted the dirty-tricks in their decision making processes, eventually selecting the German made Leopard 2A5 Tank as their choice.

ENIGMA 2000 Newsletter - Issue 2

January 2001
Articles, newsreports and Items of interest : e2k_news@hotmail.com

and more recently ...

'We hacked U.S. drone': Iran claims it electronically hijacked spy aircraft's GPS and tricked aircraft into landing on its soil

- **RQ-170 Sentinel drone has been seen on display by Iran's gloating military**
- **Engineer claims Iran downed drone by using fake signals to confuse it**
- **Claimed GPS signals are easy to hack without cracking U.S. control codes**
- **Alleges aircraft's GPS weakness was long known to U.S. military officials**

and more recently ...

29 June 2012 Last updated at 10:54 GMT

Researchers use spoofing to 'hack' into a flying drone

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).

Drones are mostly used for military operations

A University of Texas at Austin team used "spoofing" - a technique where the drone mistakes the signal from hackers for the one sent from GPS satellites.

The same method may have been used to bring down a US drone in Iran in 2011.

Analysts say that the demo shows the potential danger of using drones.

Drones are unmanned aircraft, often controlled from a hub located thousands of kilometres away.

Related Stories

Tests begin on 'unmanned' plane

Drones: What are they

Global Positioning System

GPS specs:

- 1.57542 GHz (L1) and 1.2276 GHz (L2), CDMA SS
- The C/A code (civilian use) 1.023 Mchips/s, P code
- L1 carrier is modulated by both C/A and P codes,
  L2 only modulated by P code; P can be encrypted P(Y)
- Navigation data rate: 50 b/s

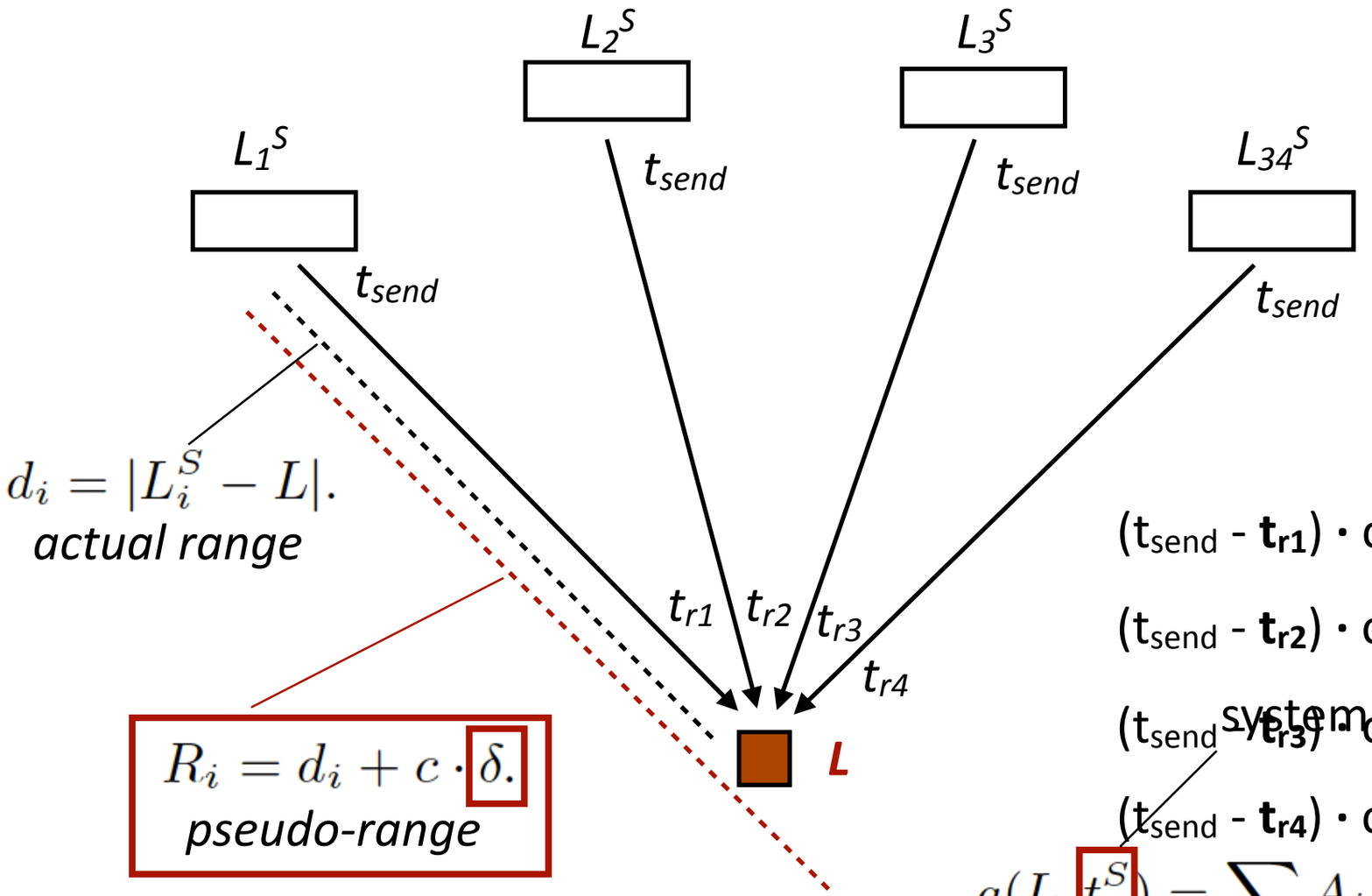
GPS security:

- Today, anyone can generate (civilian) GPS signals (public data and public spreading codes)
- Military GPS uses secret spreading codes
  - Code distribution prevents the use of military GPS
  - In large % of operations agencies still use civilian GPS

Global Positioning System

Receiver computes its location and synchs to the satellite clocks

- Satellites are (mutually) tightly synchronized (t^S)



$(t_{send} - \mathbf{t_{r1}}) \cdot c = R_1 = |L\text{-}L_1^S| + c \cdot \delta$

$(t_{send} - \mathbf{t_{r2}}) \cdot c = R_2 = |L\text{-}L_2^S| + c \cdot \delta$

$(t_{send} - \mathbf{t_{r3}}) \cdot c = R_3 = |L\text{-}L_3^S| + c \cdot \delta$

$(t_{send} - \mathbf{t_{r4}}) \cdot c = R_4 = |L\text{-}L_4^S| + c \cdot \delta$

system (satellite time)

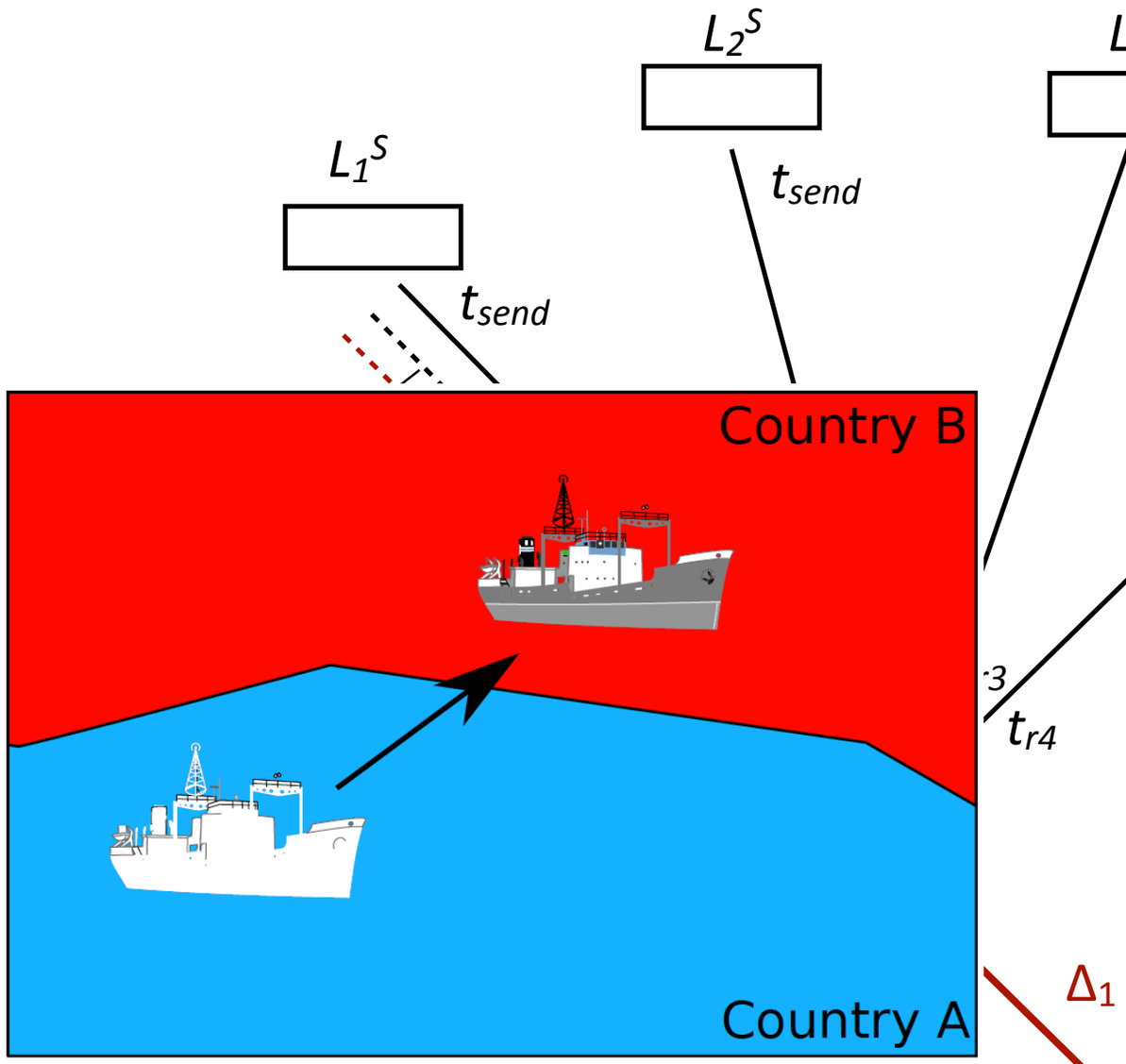
local (receiver time)

$$g(L, t^S) = \sum_i A_i s_i \left(t - \frac{d_i}{c} - \delta \right) + n(L, t^S)$$

$$t = t^S + \delta$$

GPS *Spoofing*

*Receiver **computes its location L from arrival times** =>*
if attacker can influence arrival times (pseudo ranges) it can spoof



$$(t_{send} - \mathbf{t_{r1}}) \cdot c + \Delta_1 = R_1 = |L - L_1^S| + c \cdot \delta$$

$$(t_{send} - \mathbf{t_{r2}}) \cdot c + \Delta_2 = R_2 = |L - L_2^S| + c \cdot \delta$$

$$(t_{send} - \mathbf{t_{r3}}) \cdot c + \Delta_3 = R_3 = |L - L_3^S| + c \cdot \delta$$

$$(t_{send} - \mathbf{t_{r4}}) \cdot c + \Delta_4 = R_4 = |L - L_4^S| + c \cdot \delta$$

GPS *Spoofing*

Attacker can

- generate GPS signals (civilian)
- re(p)lay GPS signals (military)

Legitimate GPS signals are therefore ***overshadowed***

- with signals from different locations or with signals from a “GPS satellite simulator”
- GPS signal weak at surface (10^{-15} W)
- *the original signal appears as noise in the attacker’s signal*

GPS *Spoofing*

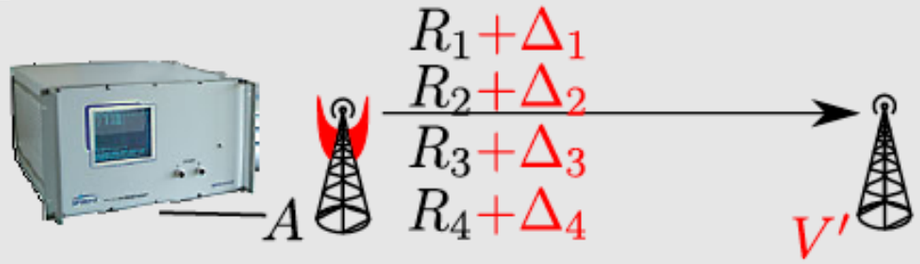
GPS signal spoofing

- Attack is at the physical layer
  (not a software/application layer attack).
- Fake GPS signals are transmitted at a higher power.
- The signals are crafted such that they are identical to the satellite signals potentially received at the spoofed location.

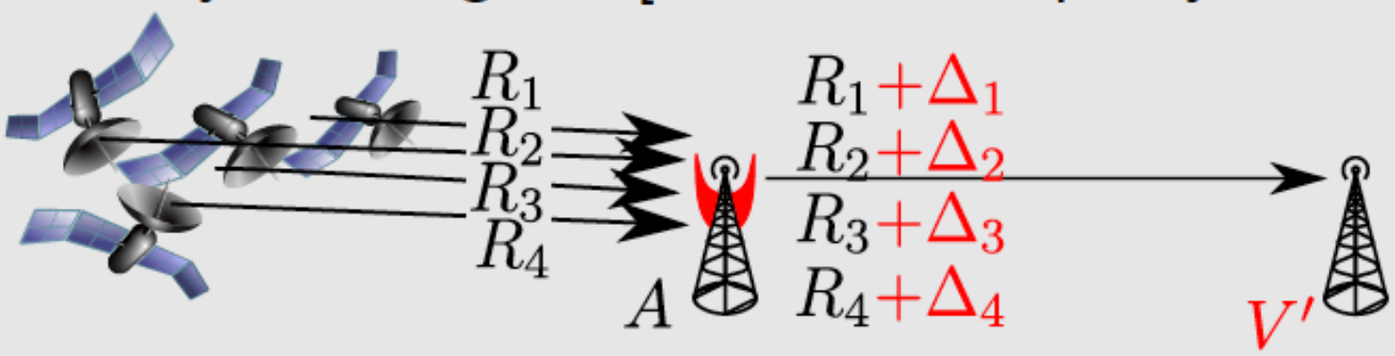
GPS *Spoofing*

How can the attacker create signals:

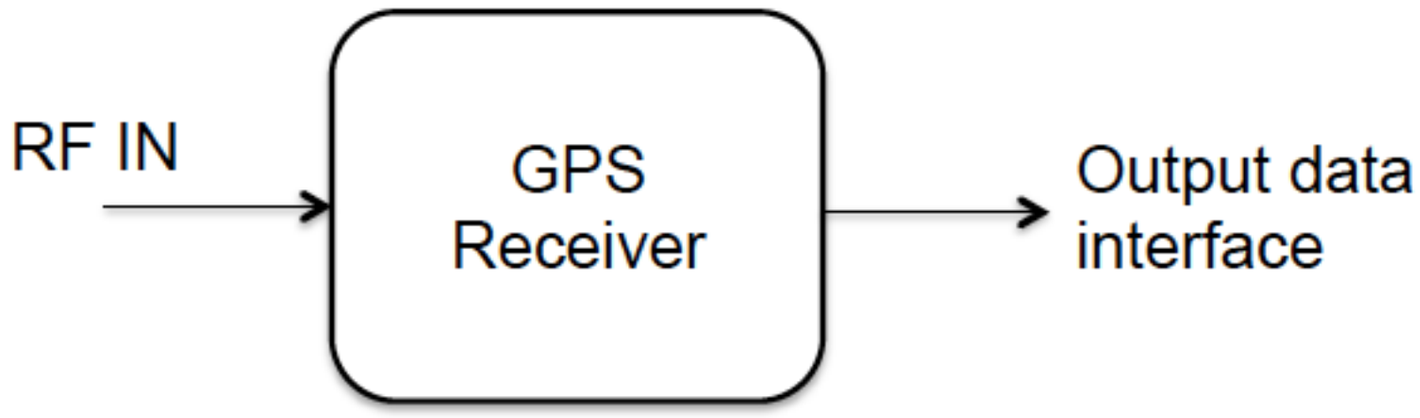
- **GPS satellite simulator:** the attacker can use a commercial or self constructed simulator to generate (non-authenticated) civilian GPS signals [Warner02,Warner03,Johnston03].



- **Relay of GPS signals:** the attacker can pick up and forward legitimate signals with appropriate delays applied. This even works for (authenticated) military GPS signals [Kuhn04,Humphreys08,Papadimitratos08,Ledvina10].

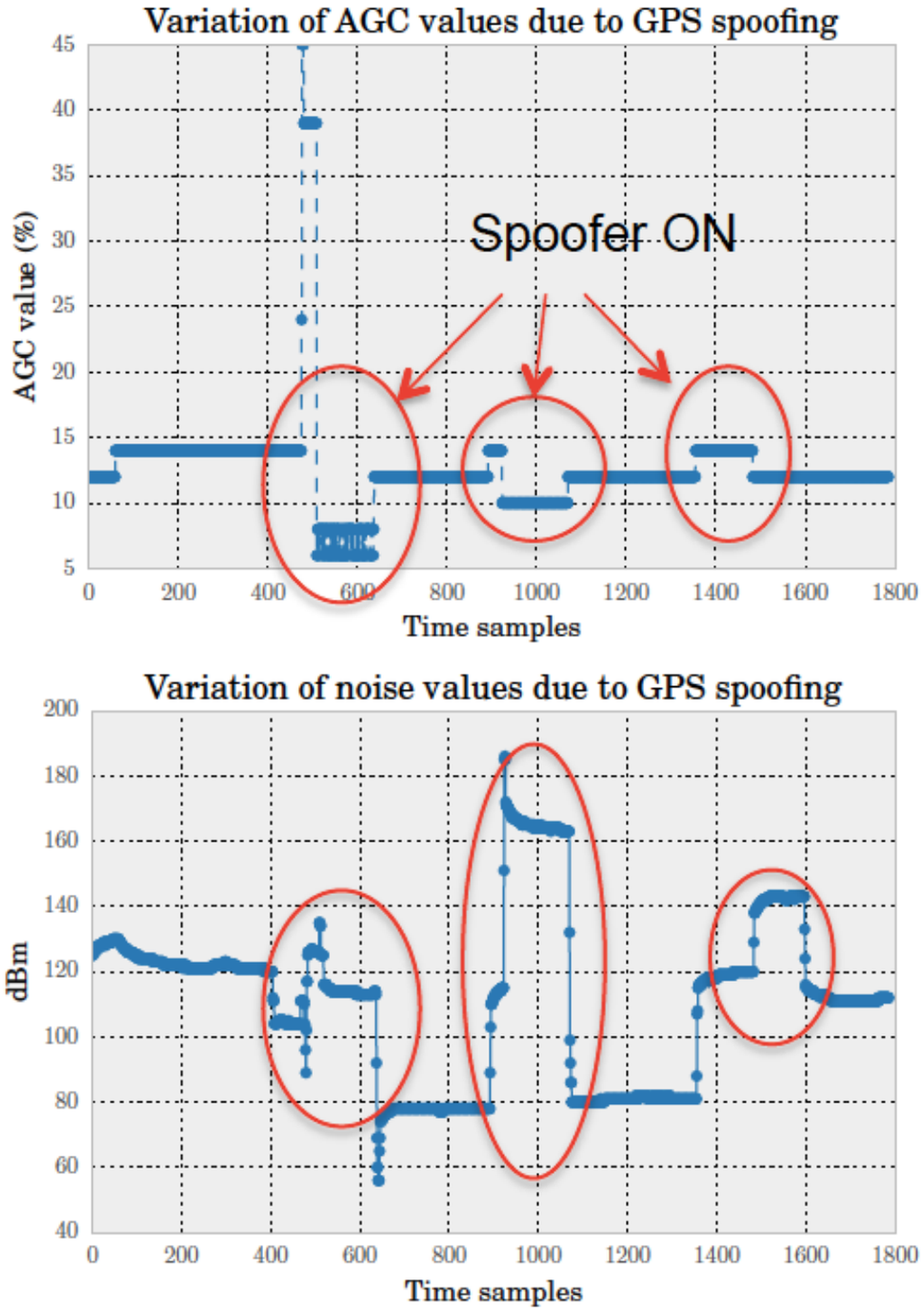


GPS *Spoofing* Detection



- **Based on Common Receiver Observables:**
  - Standardized data exchange format (e.g., NMEA) outputs e.g.: position, #visible satellites, time and date, RSSI from satellites
  - Several detection schemes based on the above have been proposed.
- **Based on Enhanced Receivers:**
  - Estimating Angle of arrival, carrier phase based detection (introducing random antenna motion)…
  - Requires modification to the receiver signal processing HW

GPS *Spoofing* Detection



AGC varies the gain of the internal amplifier so as to account for the dynamic nature of GPS input signal.

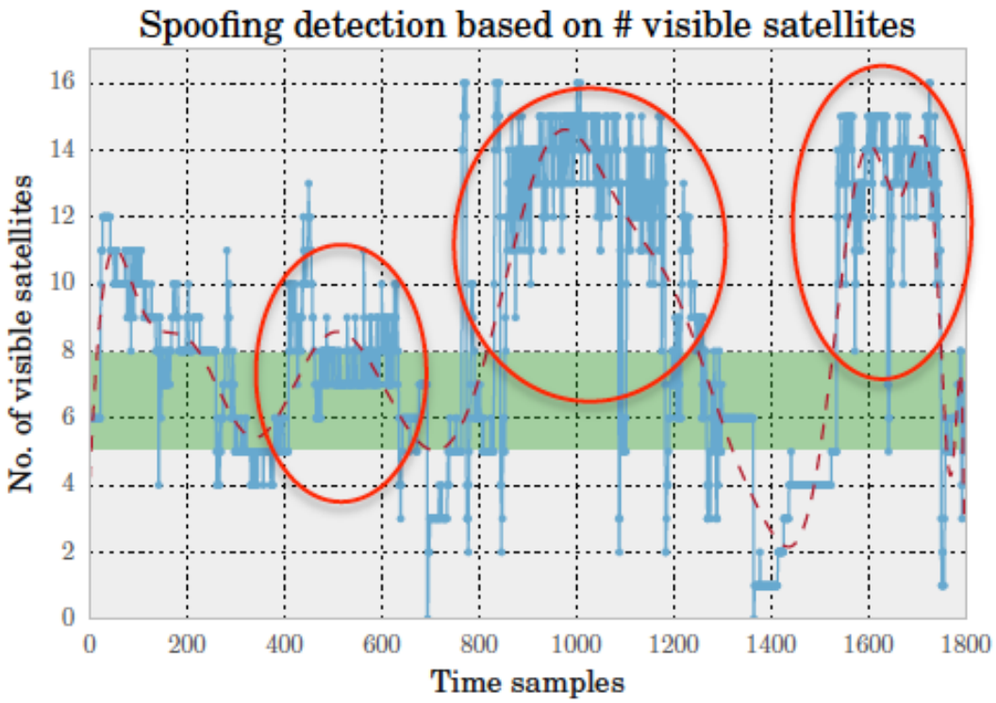
Gain is increased for weak input signals and reduced for stronger signals.

Typical noise floor level is around -120 dBm. Presence of a nearby spoofer could cause distinct changes to the observed noise level.

* Who's Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC), Dennis M Akos., Journal of Navigation.

ETH Zürich

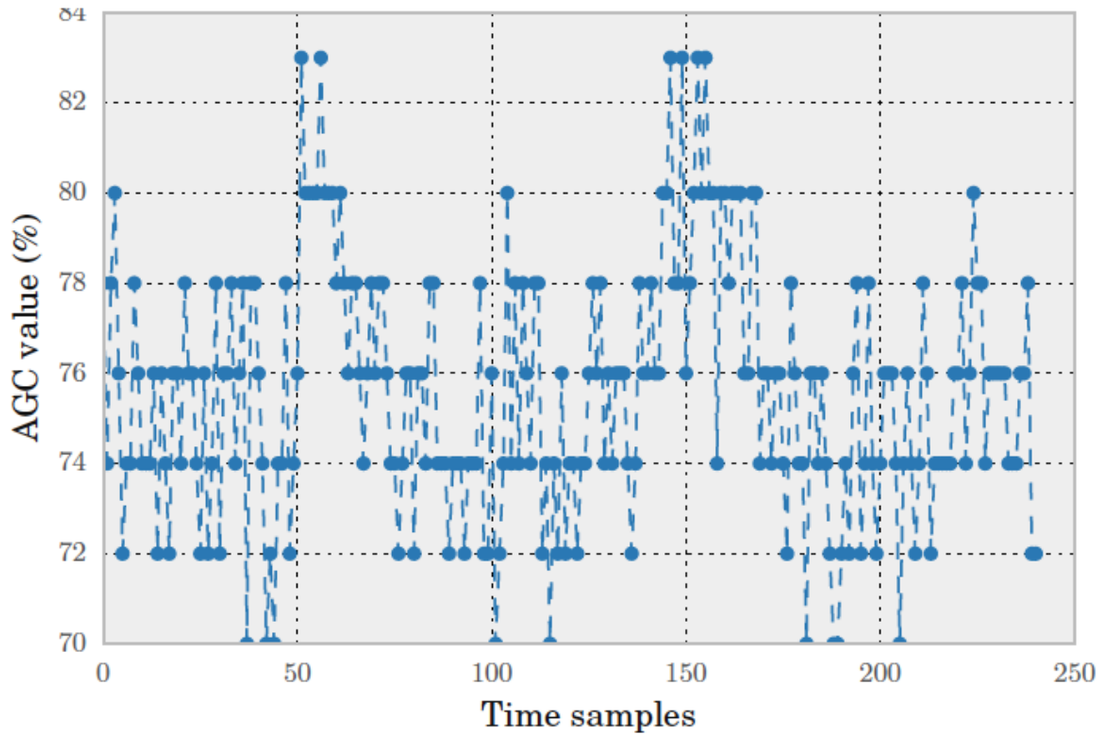
GPS *Spoofing* Detection



During spoofing, the number of visible satellites can increase beyond a certain threshold.

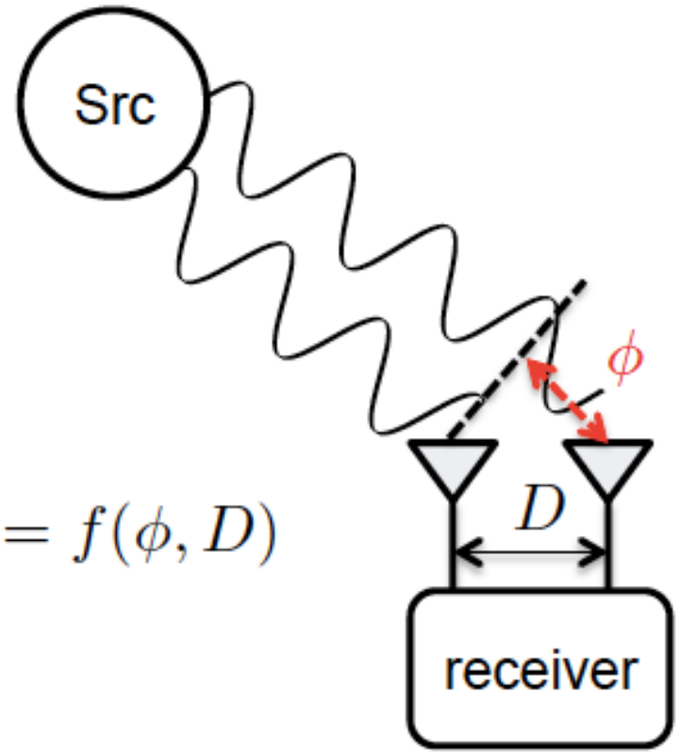
Typically, 4-8 satellites are visible.

But, in mobile / urban environments:



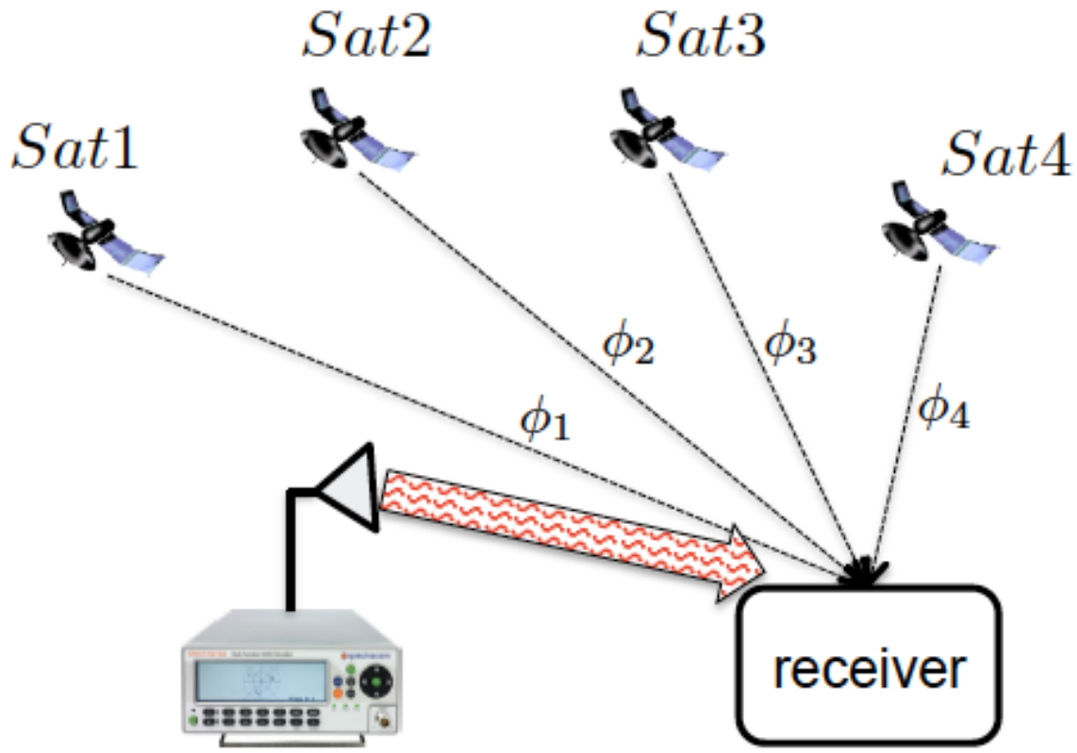
GPS *Spoofing* Detection

AoA-based Detection



$$\theta = f(\phi, D)$$

Angle of arrival is a function of the measured signal phase difference (Φ) at both the antennas and their separation D.



Spoofed scenario: $\phi_1 \sim \phi_2 \sim \phi_3 \sim \phi_4$

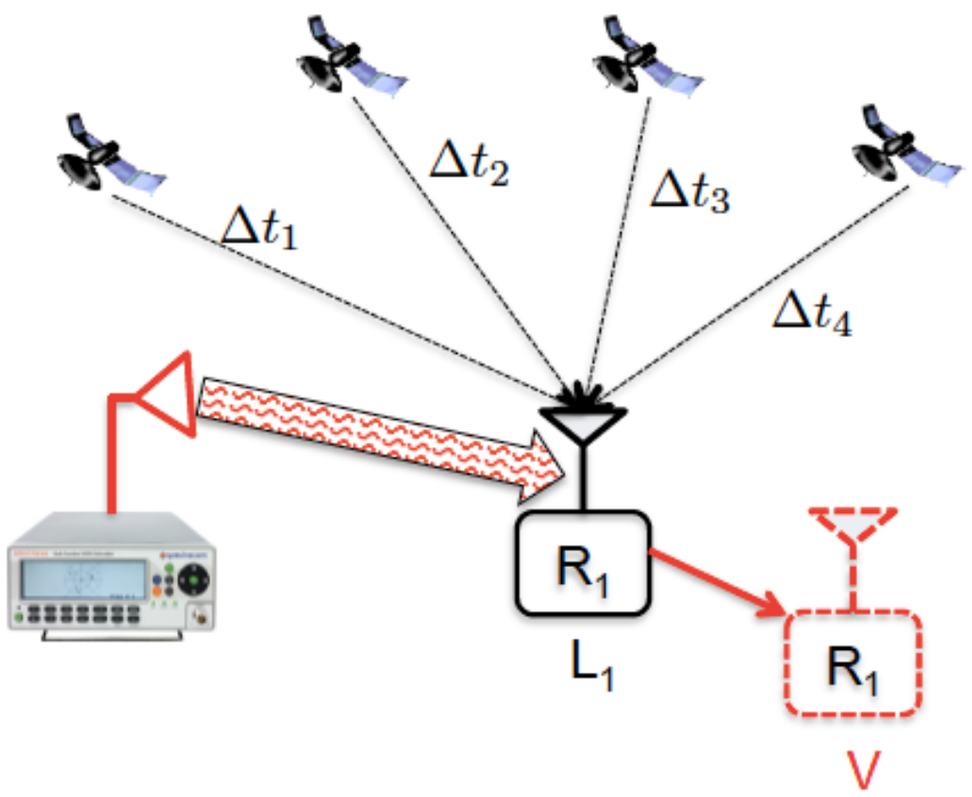
Phase measurement is computationally expensive and requires receiver hardware modifications.

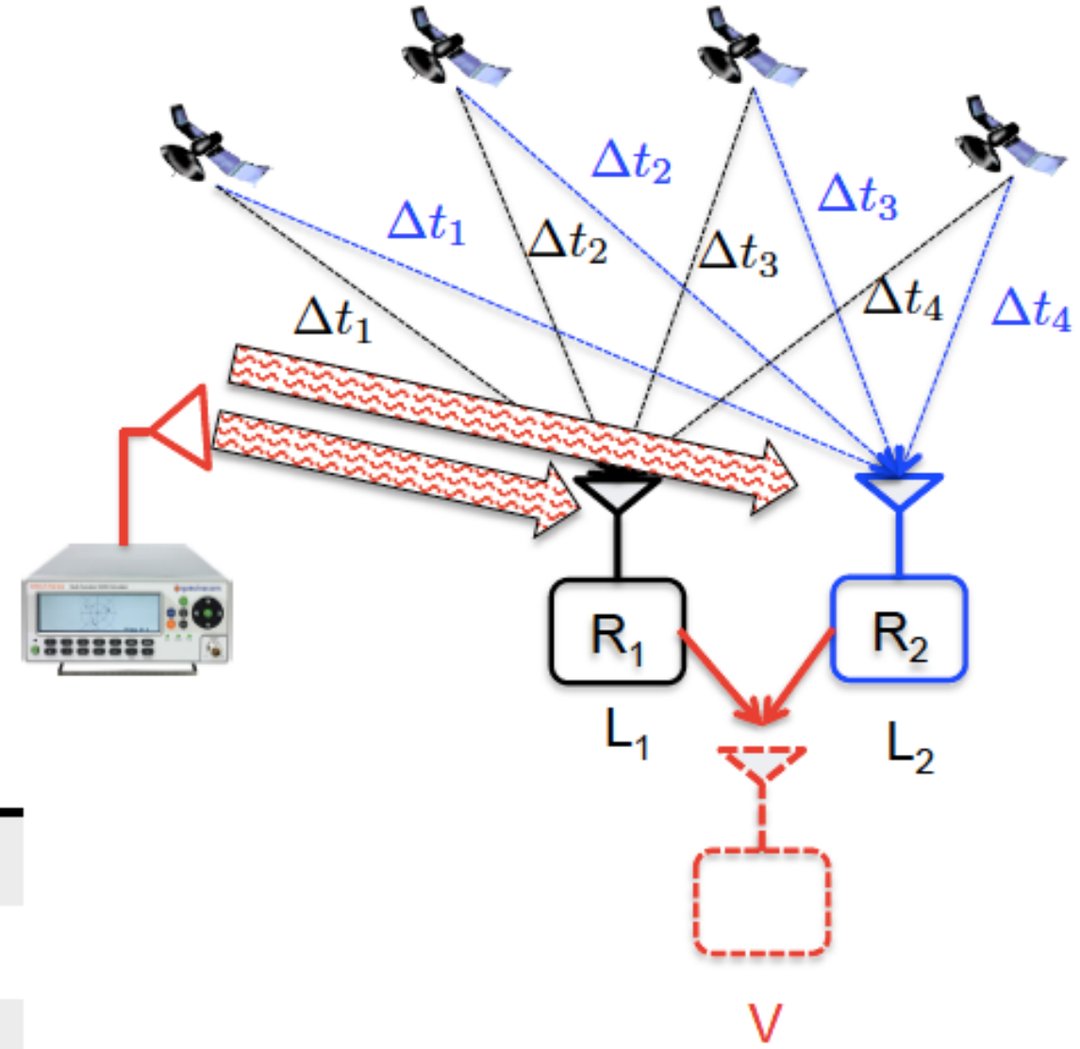
Montgomery, P.Y., T.E. Humphreys, B.M. Ledvina, ***"A Multi-Antenna Defense Receiver-Autonomous GPS Spoofing Detection,"*** *InsideGNSS, 2009.*

ETH Zürich

GPS *Spoofing* Detection

Prevent Spoofing Using Multiple Receivers





Δt_i	Signal transit times
L_i	Receiver locations
V	Spoofed location

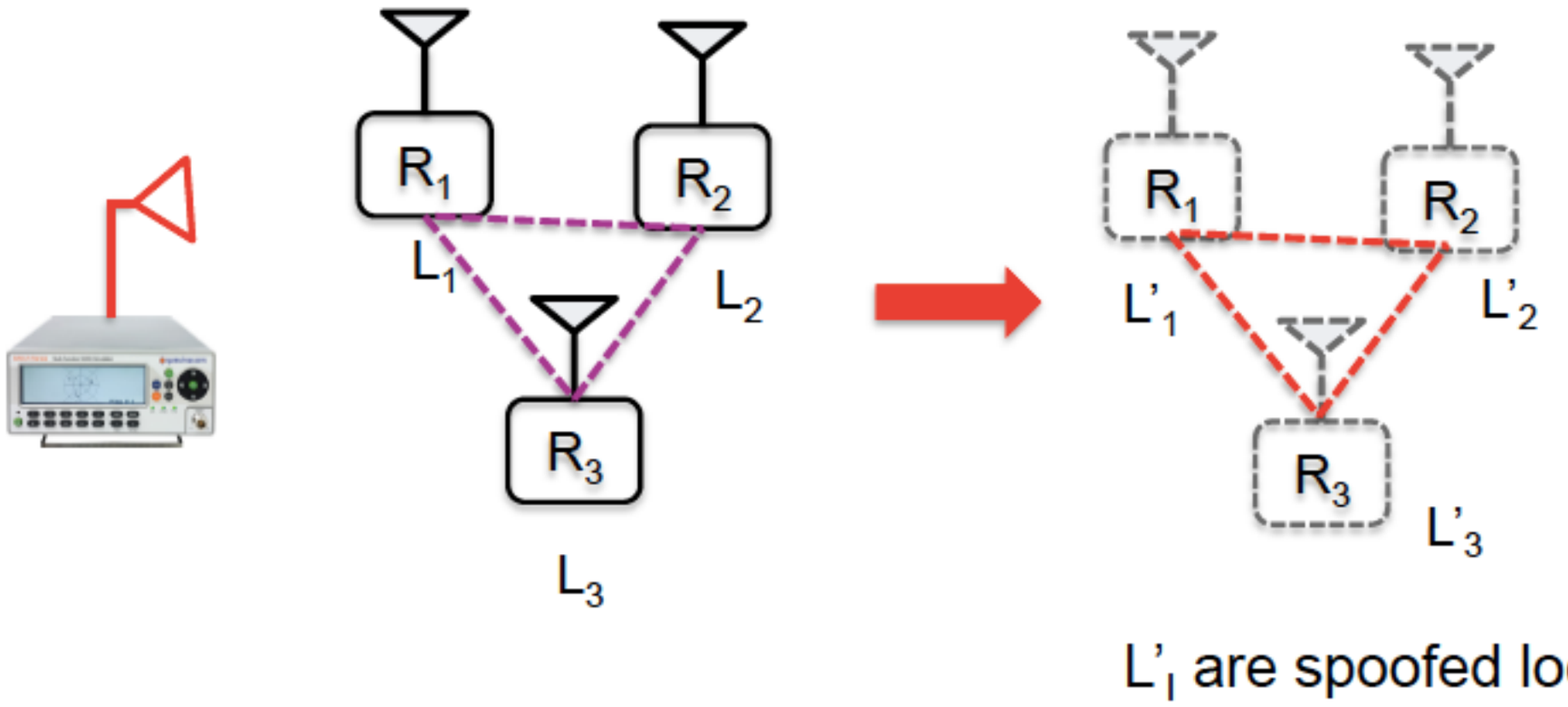
Nils Ole Tippenhauer, Christina Pöpper, Kasper Bonne Rasmussen, Srdjan Capkun, "**On the Requirements for Successful GPS Spoofing Attacks**", In Proceedings of the ACM Conference on Computer and Communications Security (CCS), 2011

ETH Zürich

GPS *Spoofing* Detection

Prevent Spoofing Using Multiple Receivers

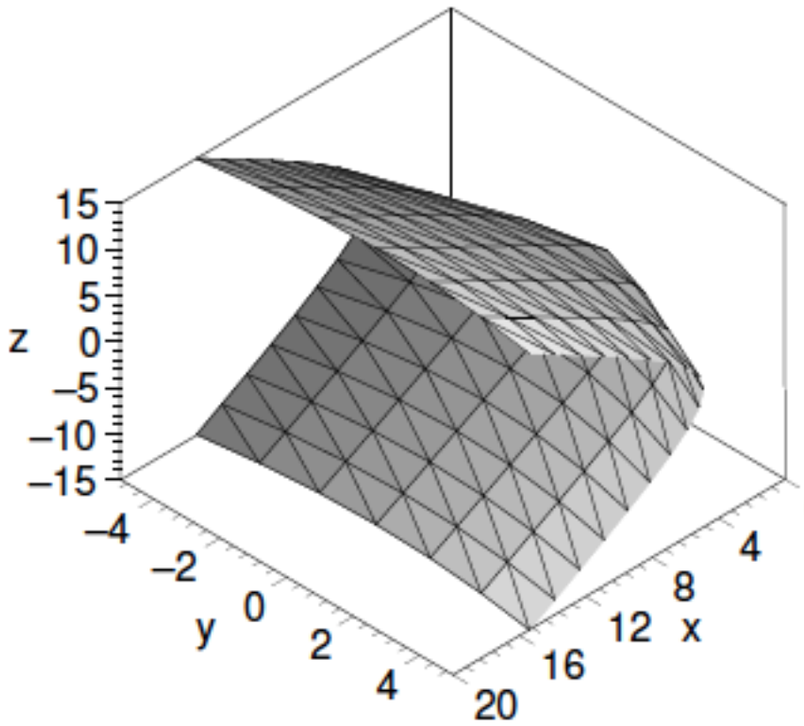
"*The* GPS Group Spoofing Problem is the problem of finding combinations of GPS signals (sent by the attacker), transmission times (when the spoofing signals are sent), and physical transmission locations (from where the attacker transmits) such that the location or time of each victim is spoofed to the desired location."



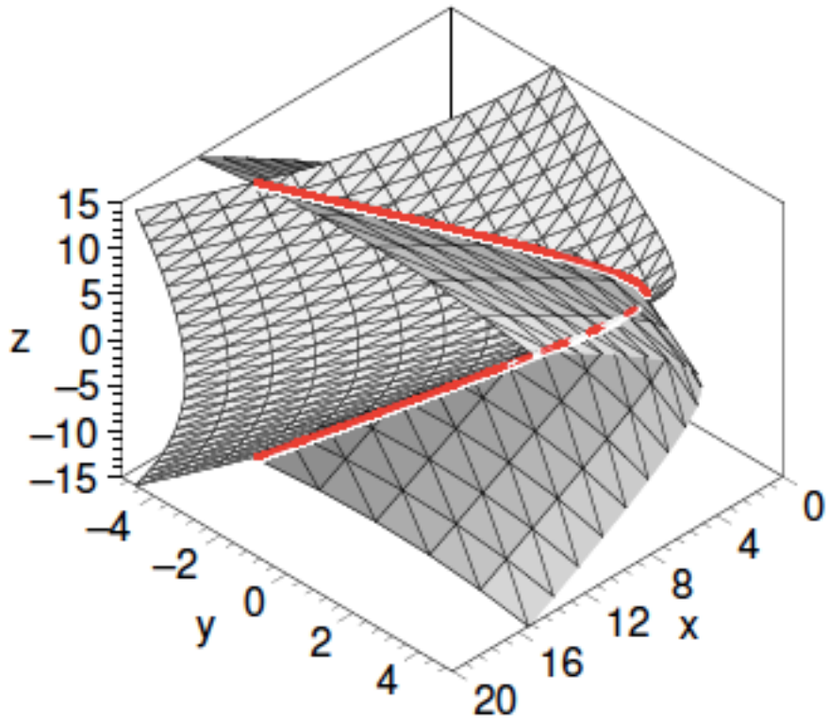
L'_i are spoofed locations

GPS *Spoofing* Detection

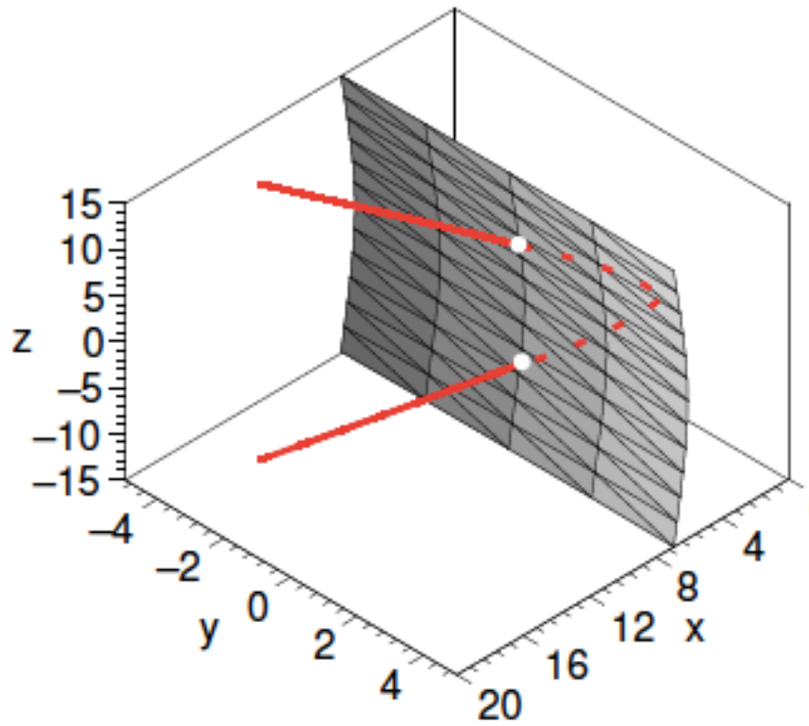
Prevent Spoofing Using Multiple Receivers



(a) 2 receivers



(b) 3 receivers



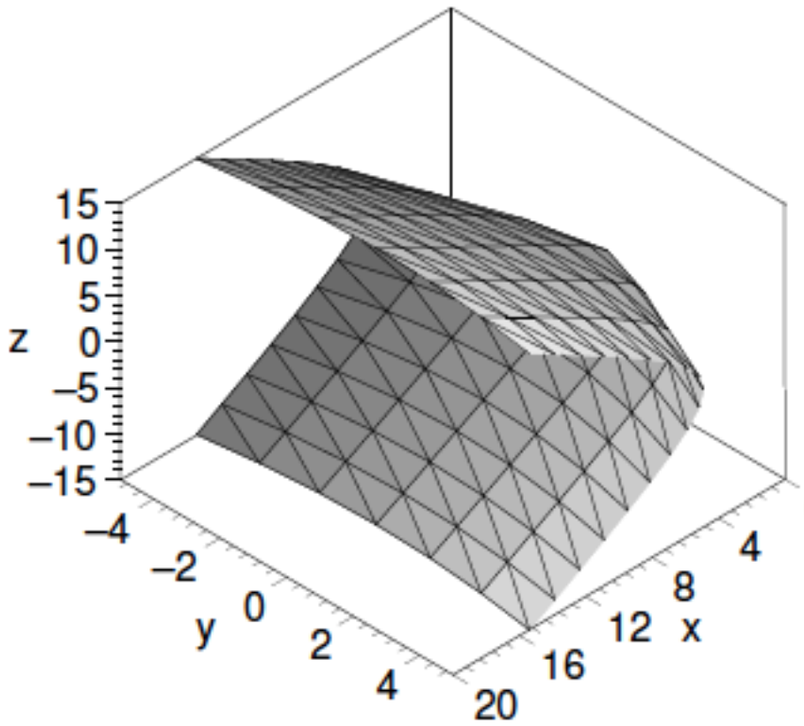
(c) 4 receivers

	Spoofing to one location	Spoofing to multiple locations (preserved formation)	
n	Civ. & Mil. GPS	Civilian GPS	Military GPS
1	$P_i^A \in \mathbb{R}^3$	-	-
2	$P_i^A \in \mathbb{R}^3$	set of hyperboloids	one hyperboloid
3	$P_i^A \in \mathbb{R}^3$	set of intersections of two hyperboloids	intersection of two hyperboloids
4	$P_i^A \in \mathbb{R}^3$	set of 2 points	2 points
≥ 5	$P_i^A \in \mathbb{R}^3$	set of points	1 point

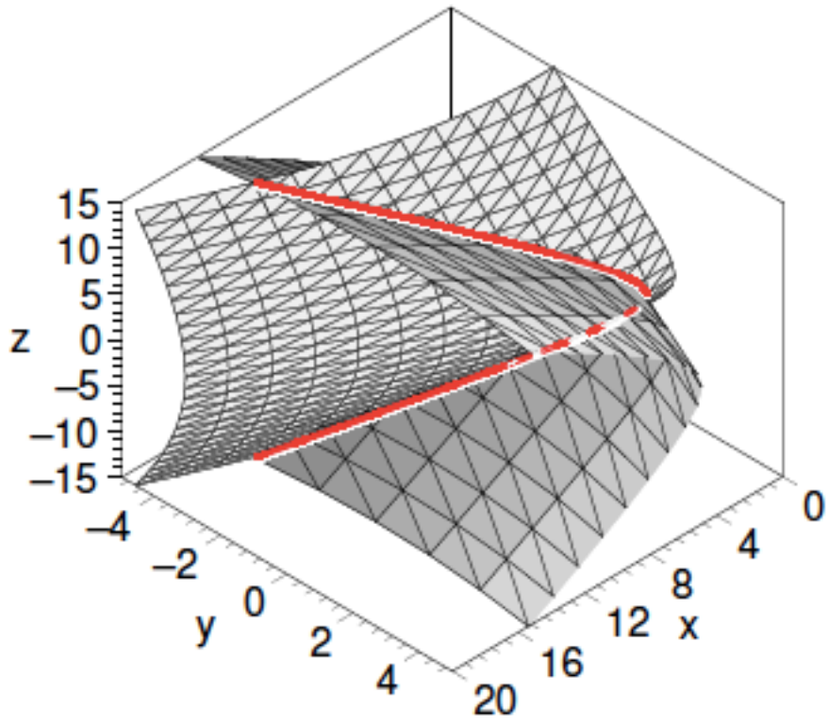
ETH Zürich

GPS *Spoofing* Detection

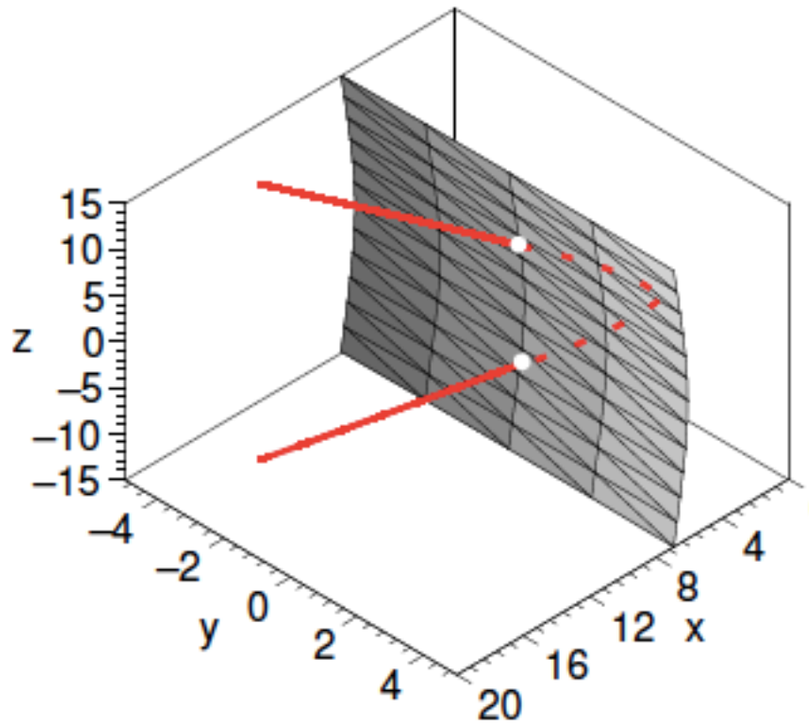
Prevent Spoofing Using Multiple Receivers



(a) 2 receivers



(b) 3 receivers



(c) 4 receivers

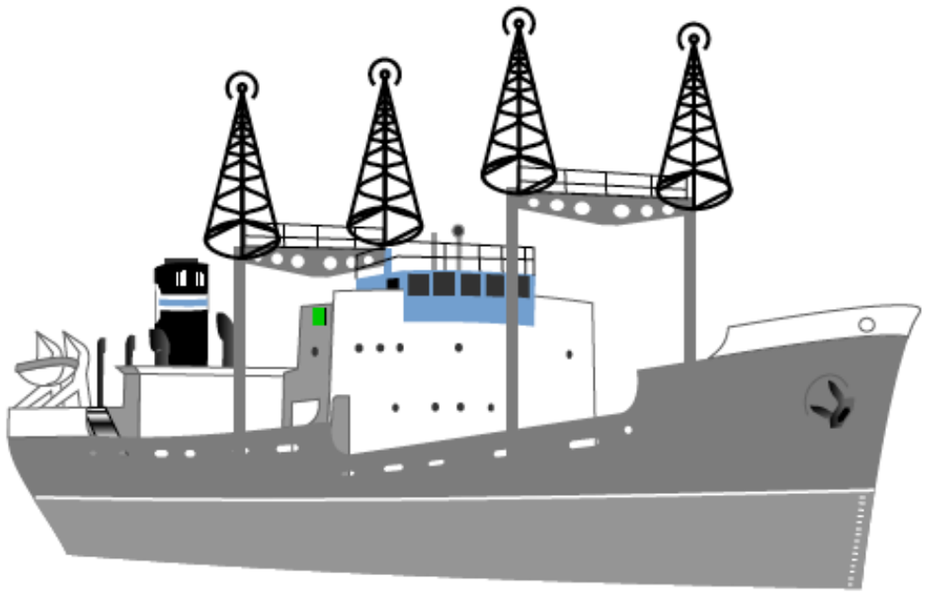
	Spoofing to one location	Spoofing to multiple locations (preserved formation)	
n	Civ. & Mil. GPS	Civilian GPS	Military GPS
1	$P_i^A \in \mathbb{R}^3$	-	-
2	$P_i^A \in \mathbb{R}^3$	set of hyperboloids	one hyperboloid
3	$P_i^A \in \mathbb{R}^3$	set of intersections of two hyperboloids	intersection of two hyperboloids
4	$P_i^A \in \mathbb{R}^3$	set of 2 points	2 points
≥ 5	$P_i^A \in \mathbb{R}^3$	set of points	1 point

ETH Zürich

GPS *Group Spoofing*: Implications

A victim can use 4 (or more) GPS receivers in a known static formation to detect spoofing attacks.

- If their reported positions do not fit their formation, suspect attack
- The attacker must translate/rotate his antennas if victims are moving



- *GPS precision influences how distant receivers need to be for the detection to be effective.*

ETH Zürich

Lesson learned:

With spatial diversity and several COTS receivers we can significantly limit attacker's spoofing ability

Conclusion

- Secure Localization / Location Verification is a fascinating area
- Brings up interesting cross-layer interactions
  between logical and physical layers
- New protocol designs, radio designs, new security insights,
  new challenges in formal protocol analysis

- Numerous Applications
  - Physical and Logical Access Control, Anti-Spoofing,
    Protection of Networking Functions, …

- http://www.syssec.ethz.ch
- capkuns@inf.ethz.ch

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

- Aanjhan Ranganathan
- Christina Popper
- Nils Tippenhauer
- Kasper Rasmussen
- Boris Danev
- Aurelien Francillon
- …