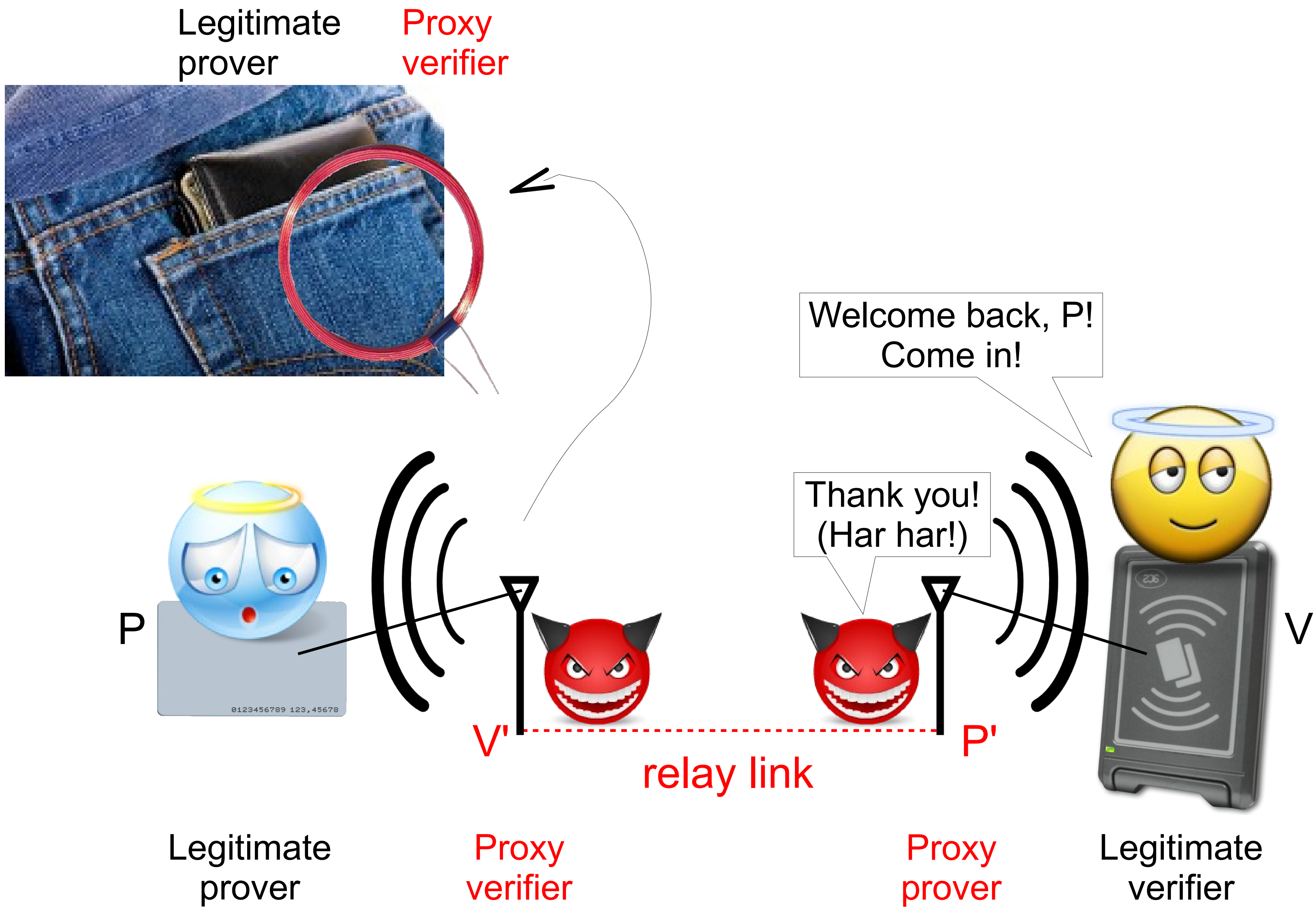
Distance enlargent against IEEE802.15.4a distance bounding

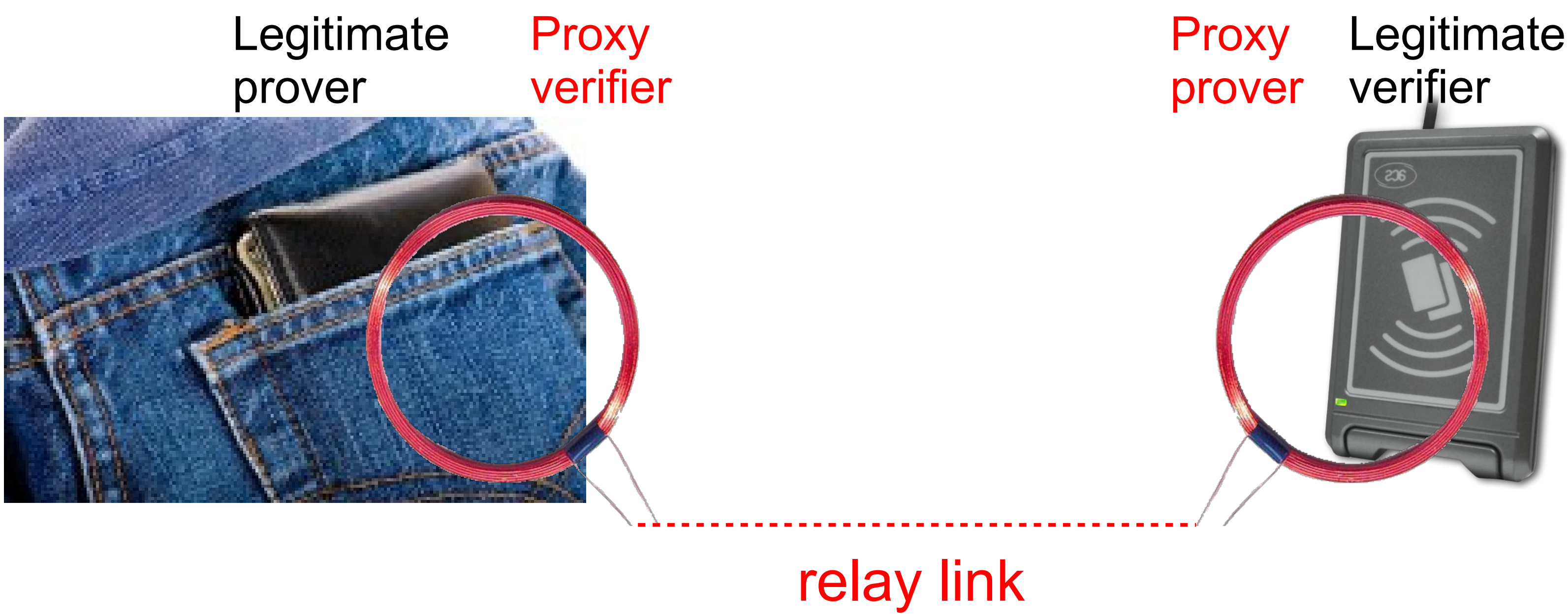
Mafia fraud

- Mafia fraud is an attack against a generic authentication protocol
- A verifier (V) checks for the identity of a prover (P) and then opens a door (access control)
- An adversary establishes a relay link between two far away honest parties (P and V)
- The prover correctly authenticates to the verifier and the door opens
- The adversary enters the door

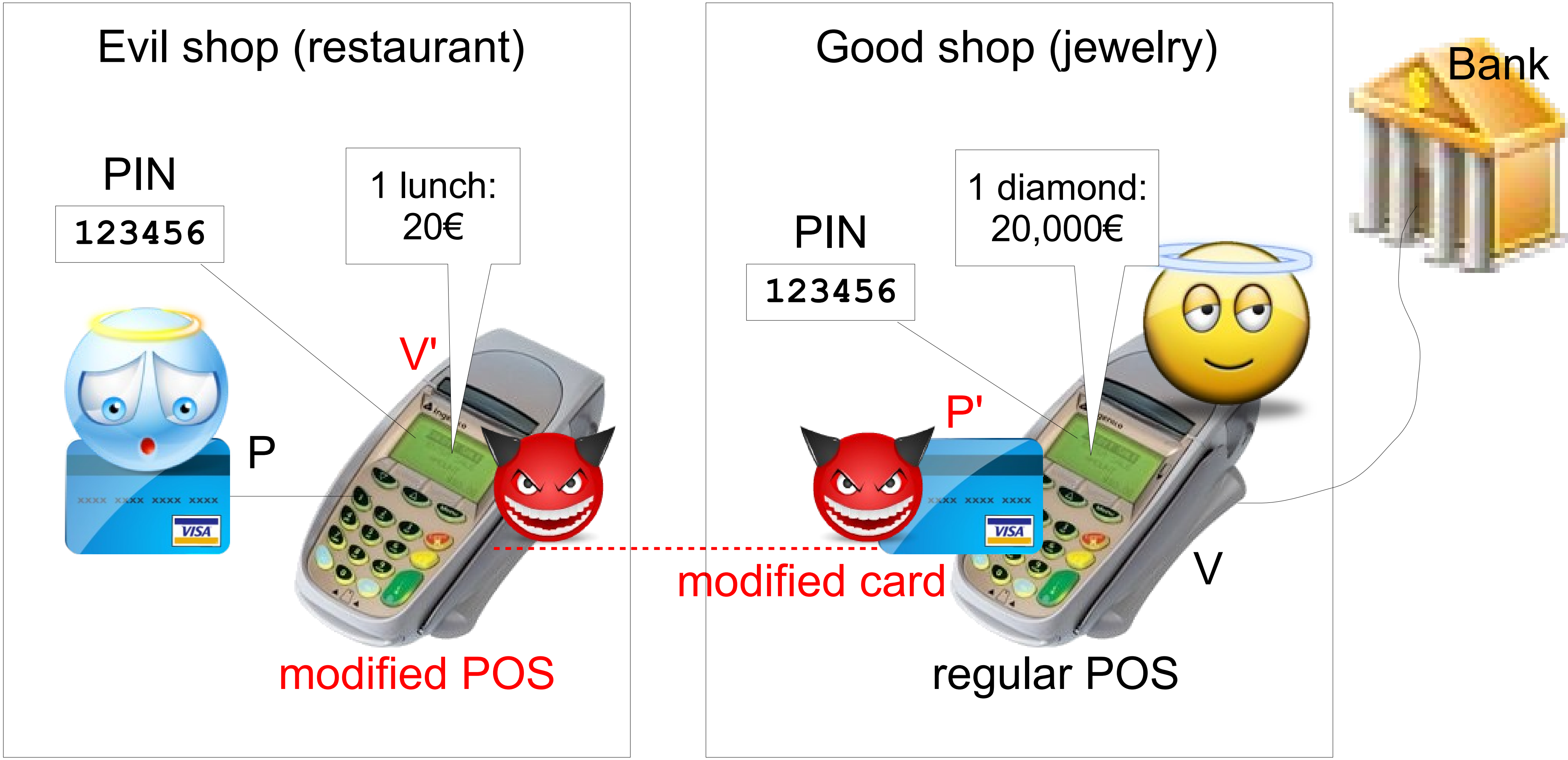
Mafia fraud


Legitimate prover
Proxy verifier
Welcome back, P! Come in!
Thank you! (Har har!)
P
V
V'
P'
relay link
Legitimate prover
Proxy verifier
Proxy prover
Legitimate verifier

Mafia fraud

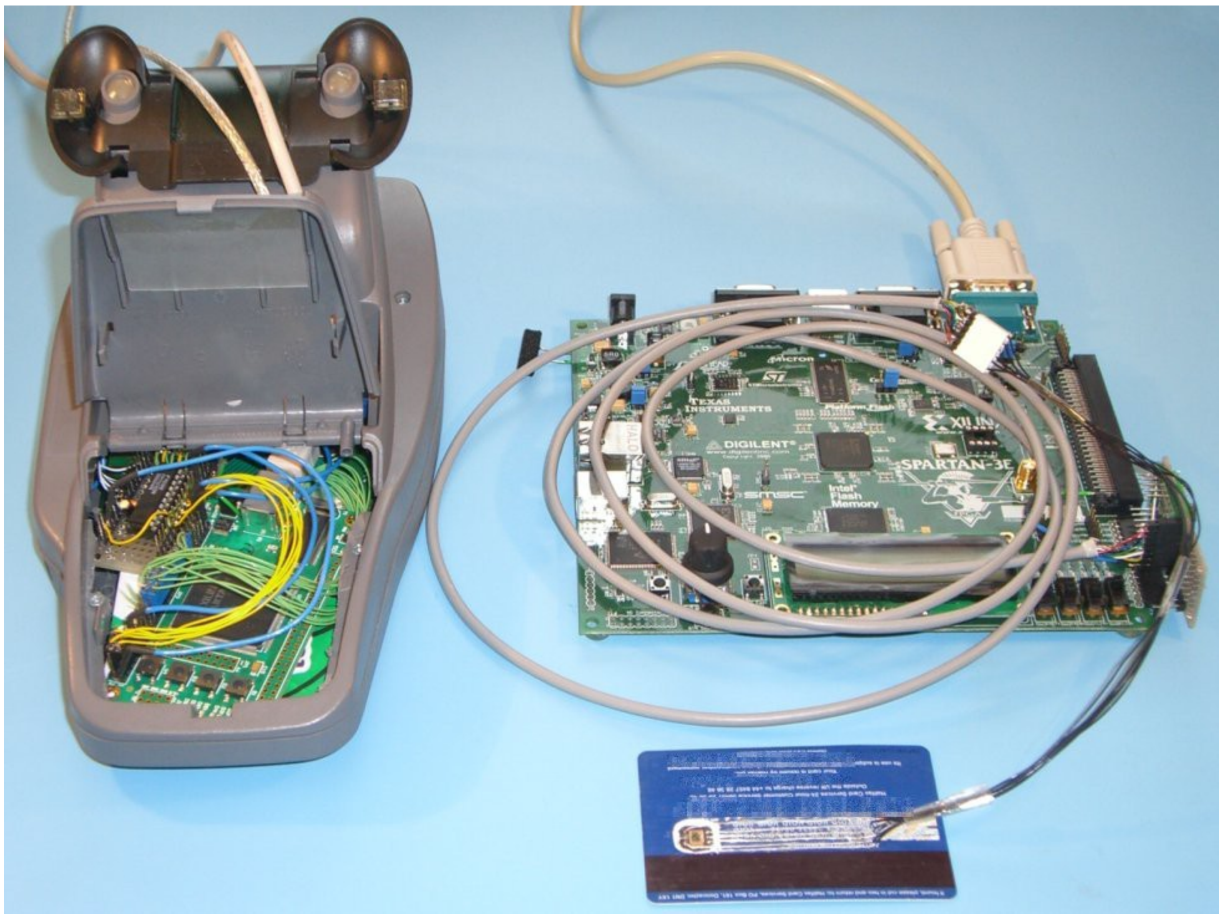

Legitimate prover
Proxy verifier
Proxy prover
Legitimate verifier
relay link

Mafia fraud



Evil shop (restaurant)
PIN
123456
1 lunch:
20€
V'
P
modified POS
Good shop (jewelry)
Bank
PIN
123456
1 diamond:
20,000€
P'
modified card
V
regular POS

Mafia fraud


TEXAS INSTRUMENTS
DIGILENT
SPARTAN-3E
Intel Flash Memory
SMSC


MENU
CANCEL
CLEAR
ENTER

Mafia fraud against PKES

- Passive Keyless Entry and Start

Mafia fraud against PKES

Mafia fraud against PKES

Car model	Relay cable					
	7 m		30 m		60 m	
	open	go	open	go	open	go
Model 1	✓	✓	✓	✓	✓	✓
Model 2	✓	✓	A	A	A	A
Model 3	✓	✓	✓	✓	✓	✓
Model 4	✓	✓	-	-	-	-
Model 5	✓	✓	✓	✓	✓	✓
Model 6	✓	✓	A	A	A	A
Model 7	✓	✓	A	A	-	-
Model 8	✓	A	✓	A	-	-
Model 9	✓	✓	✓	✓	✓	✓
Model 10	✓	✓	✓	✓	-	-

✓ Without amplification

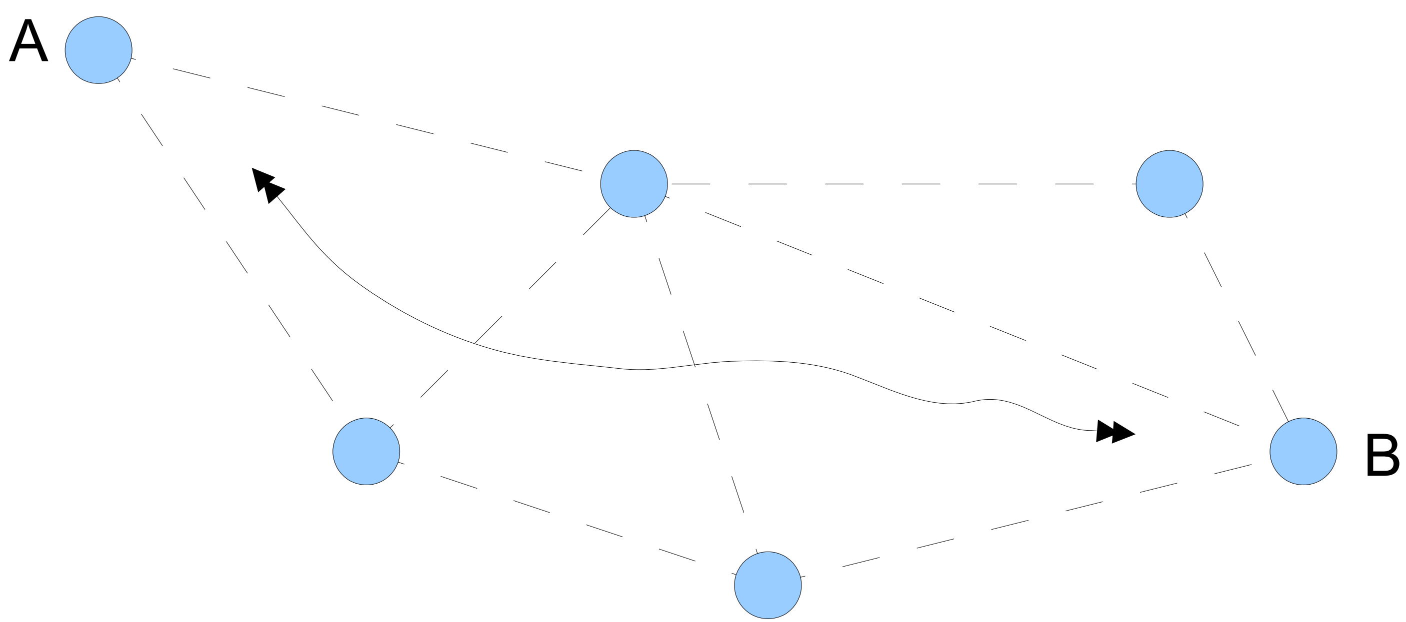
A With amplification

– Not tested

2010

Wormhole attack

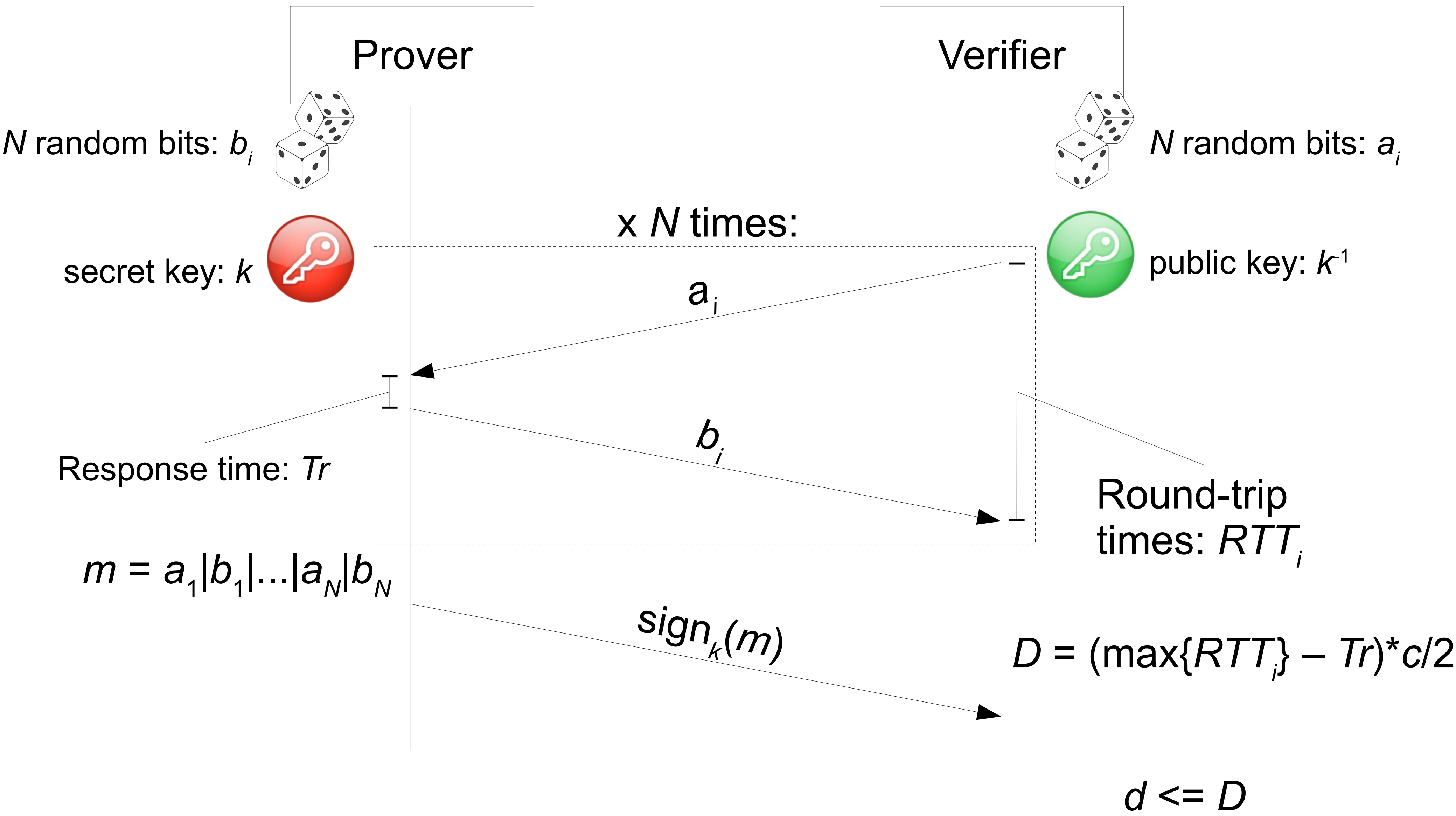
- False assumption: "if A hears an (authenticated) beacon message from B, then B and A are in the proximity"
- The adversary establishes a (wireless) link between two far away nodes (the wormhole)



Distance bounding protocol

- *Countermeasure:* precisely measure the round trip-time between a challenge and a response messages
- If the round-trip time is too large, reject the authentication (a mafia fraud could be present!)
- The challenges and the responses must be *externally unpredictable*

Brands-Chaum protocol (type I)



Distance bounding protocol

2009 implementation

Distance bounding protocol

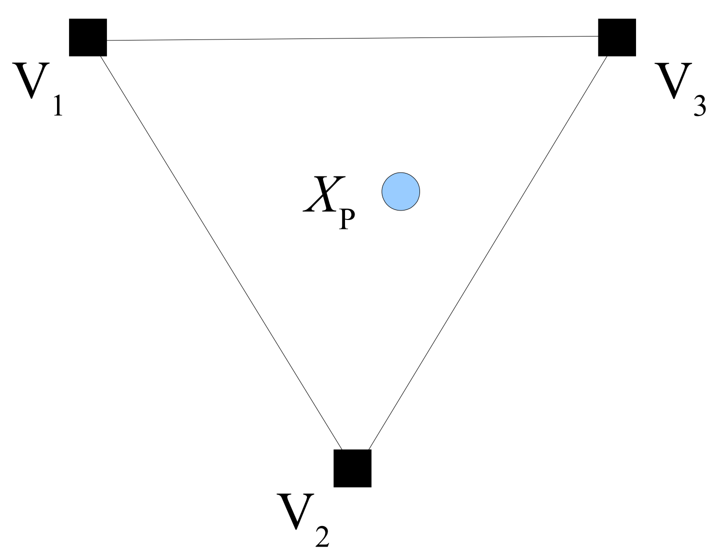
- *Distance reduction attack*: make the distance appear shorter than real
- Infeasible with distance bounding

Secure positioning

- Measure the position of a device (e.g. a wireless sensor) in presence of an adversary
- Useful for securing a lot of applications
  - geographic routing
  - robot/drone guidance
  - position based security/authentication

Verifiable multilateration

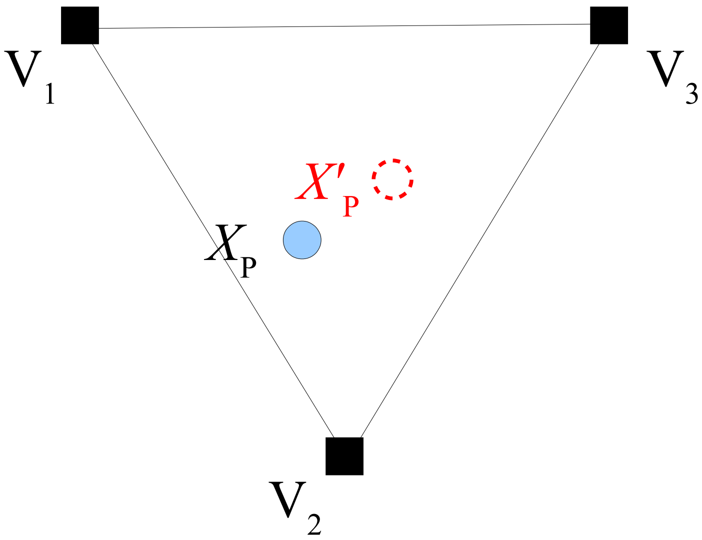
- Multilaterate a device by means of wireless distance bounding
- Check if the measured distance is inside the verifiers' polygon (*in-polygon check*)



- Spoofing a position inside the polygon *always* requires a distance reduction

Verifiable multilateration

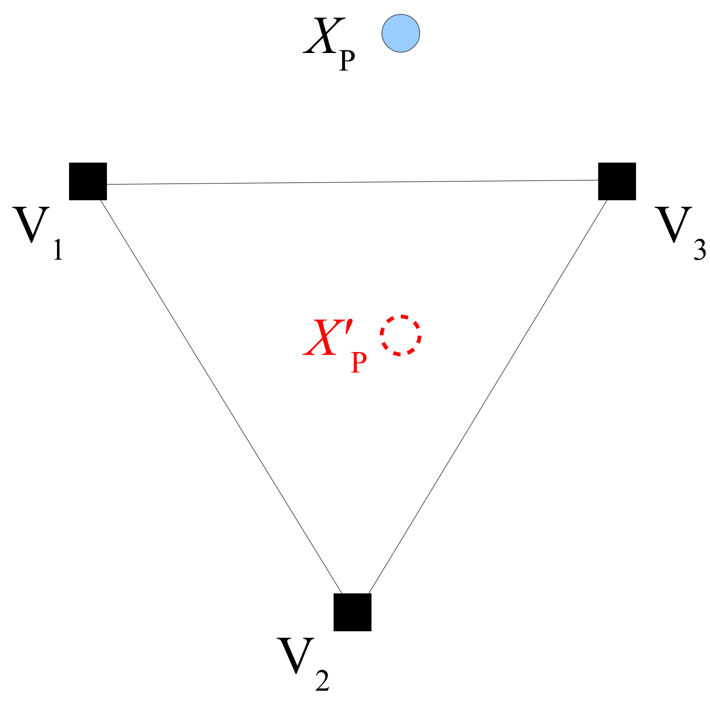
- Case of “inside-inside” spoofing



- Distance reduction against V_3 (impossible)

Verifiable multilateration

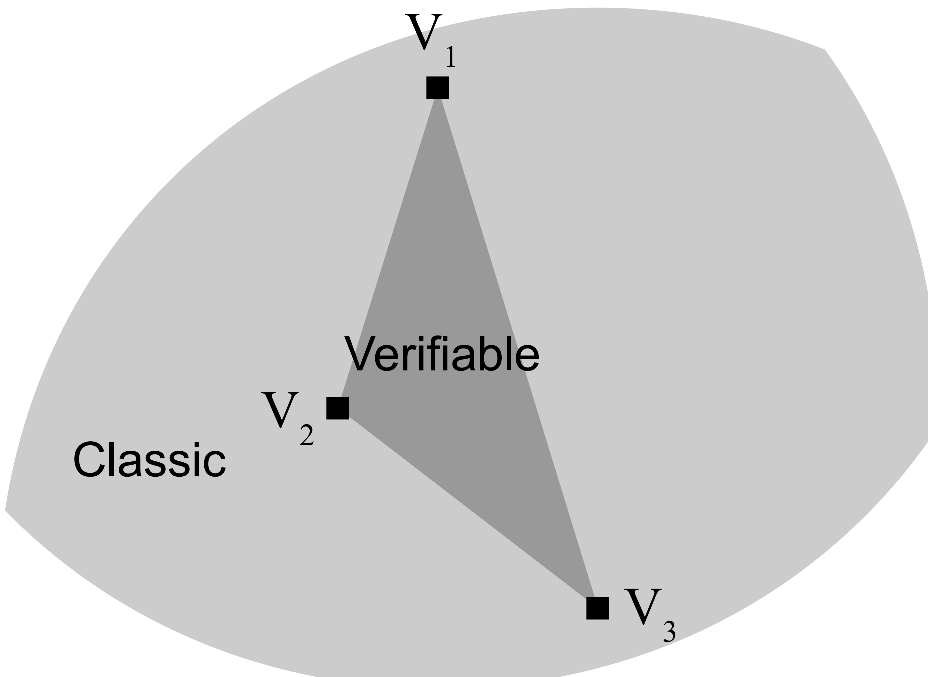
- Case of “outside-inside” spoofing



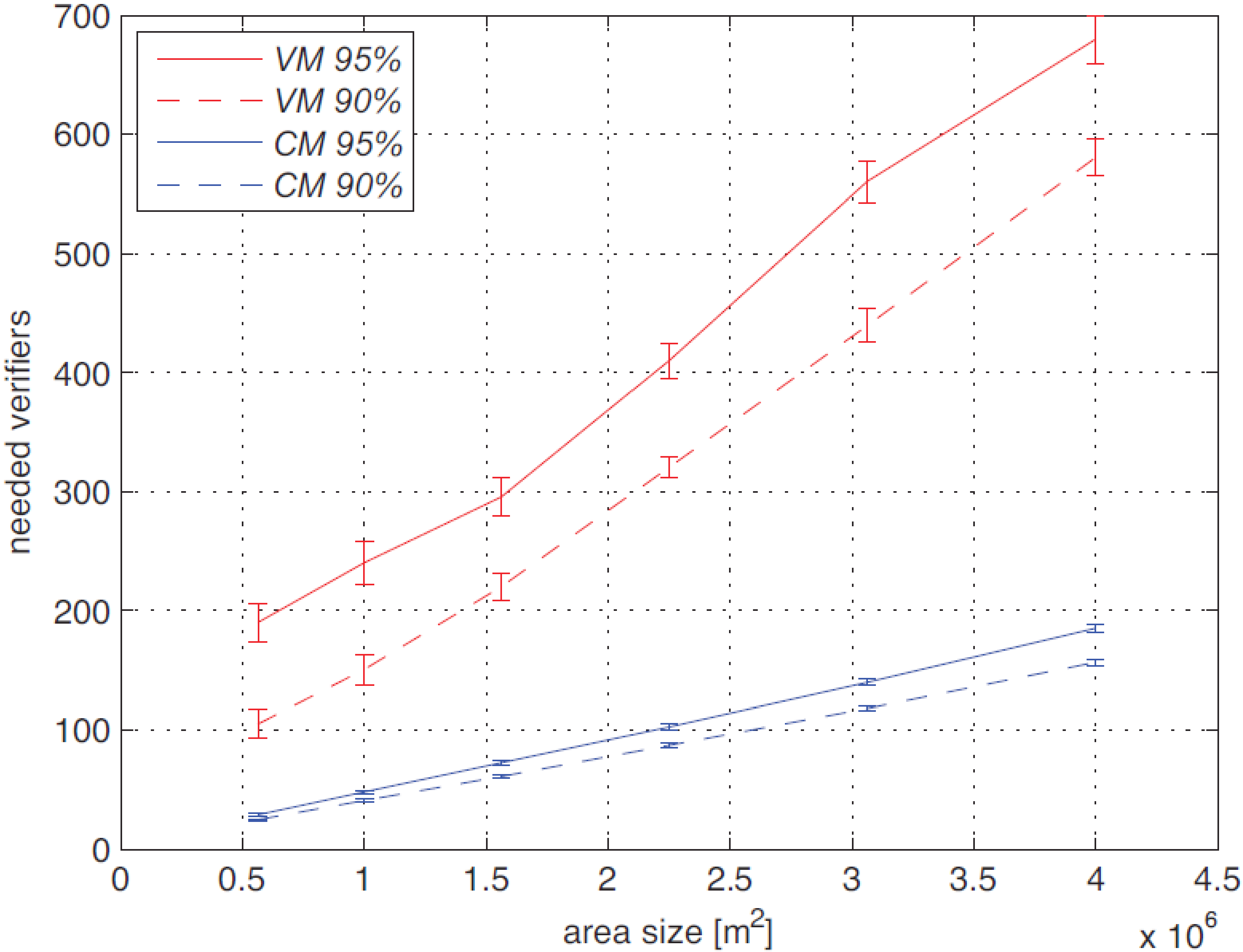
- Distance reduction against V_2 (impossible)

Coverage

- The coverage area is smaller than (classic) multilateration

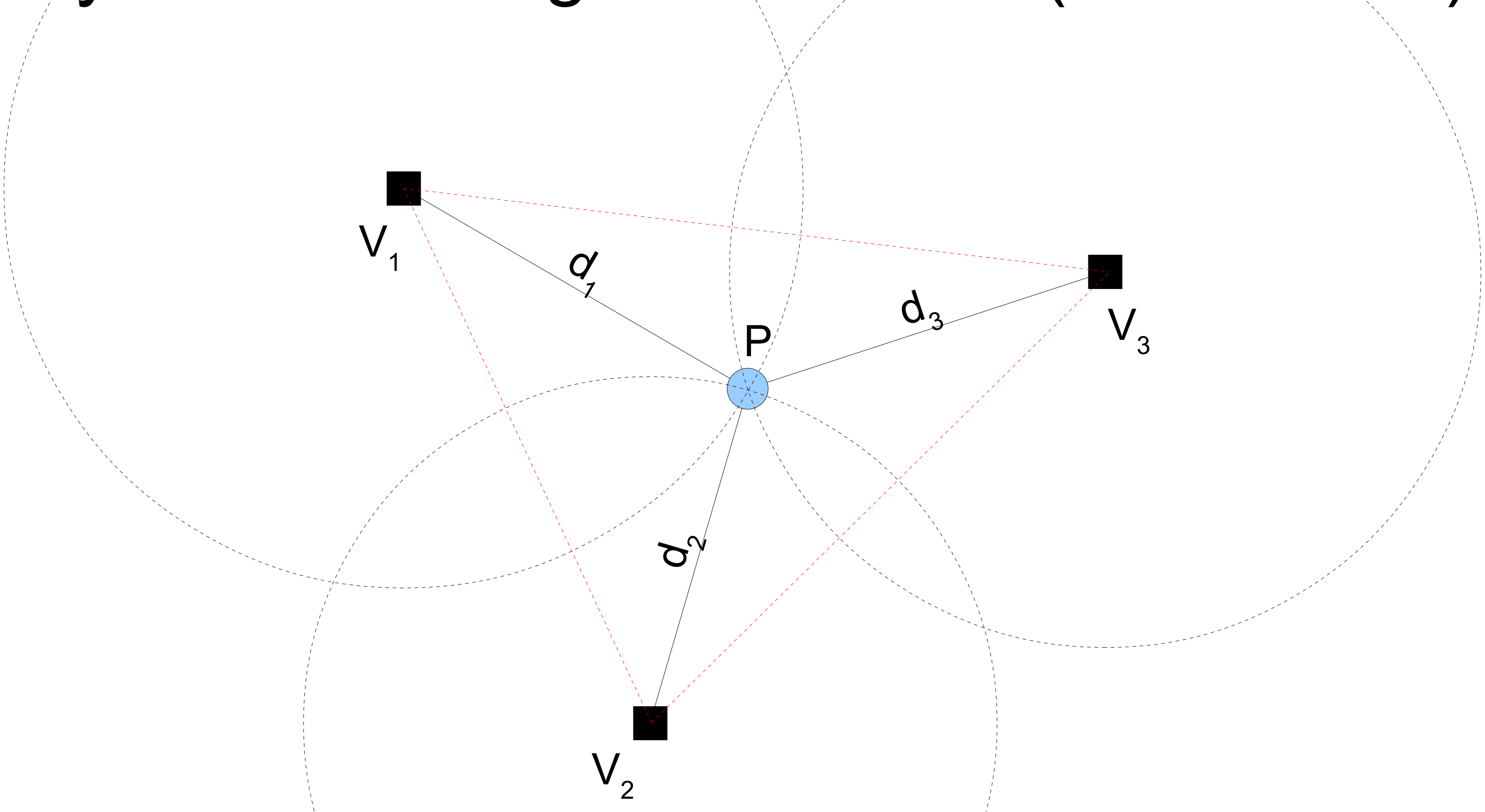


Coverage


VM 95%
VM 90%
CM 95%
CM 90%
needed verifiers
0
100
200
300
400
500
600
700
0
0.5
1
1.5
2
2.5
3
3.5
4
4.5
area size [m2]
x 10^6

Verifiable multilateration

- Multilateration by means of wireless distance bounding protocols
- Only the red triangle is covered (not outside)



Enlargement attacks

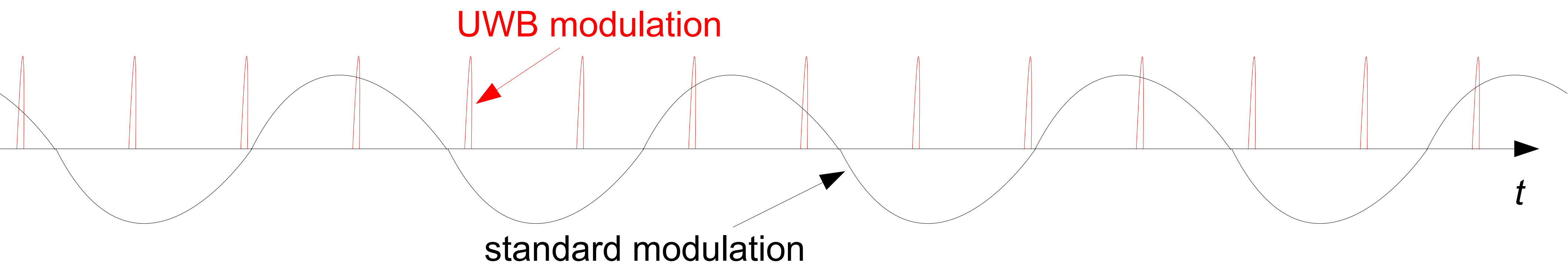
- The problem is that reduction attacks are impossible, but *enlargement attacks* are (considered) possible
  - The adversary waits for a legitimate protocol execution
  - She jams the response and repeats it just after
  - The round-trip time (and consequently the measured distance) is *enlarged*

What is the real feasibility of performing an enlargement attacks?

- The feasibility of an enlargement attack highly depends on the PHY protocol
- We studied the feasibility of enlargement attacks within the standard PHY modulation IEEE 802.15.4a

IEEE 802.15.4a UWB

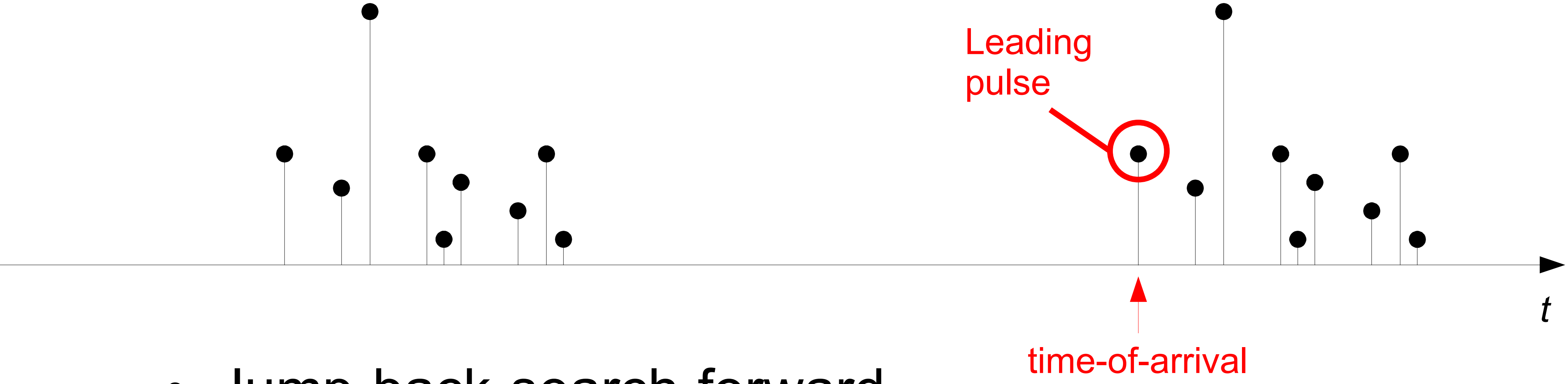
- Impulse-radio ultra-wide band (IR-UWB)



- >= 500MHz bandwidth (each channel)
- The instant of pulse arrival is precisely measurable
- In a multi-path environment, the replicas remain distinct

IEEE 802.15.4a UWB

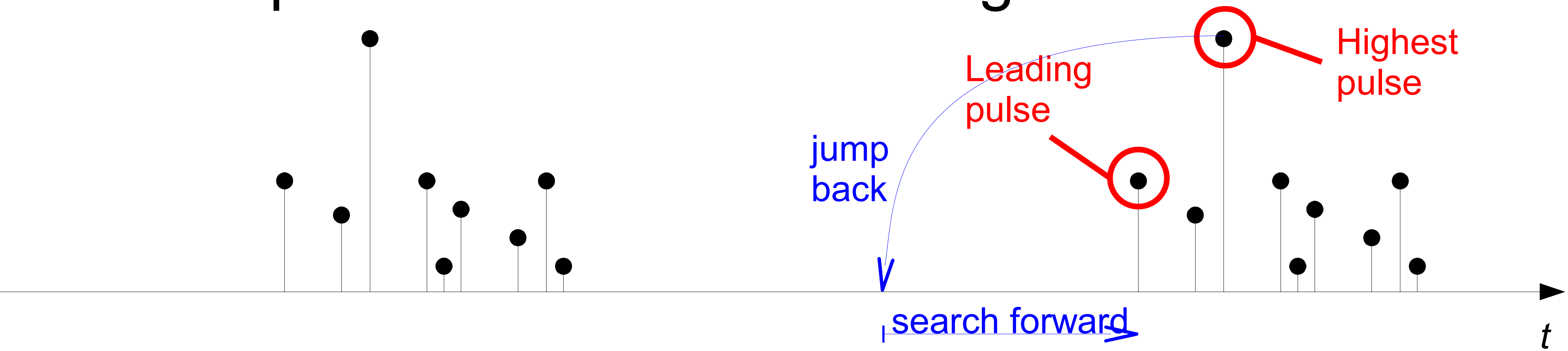
- Time-of-arrival (ToA) estimation algorithm



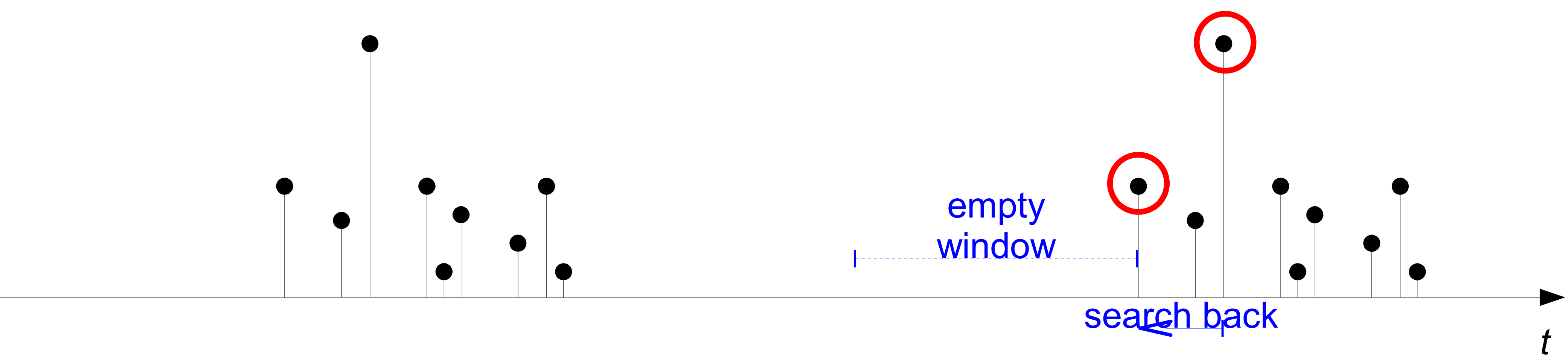
  - Jump-back-search-forward
  - Search-back

ToA estimation algorithm

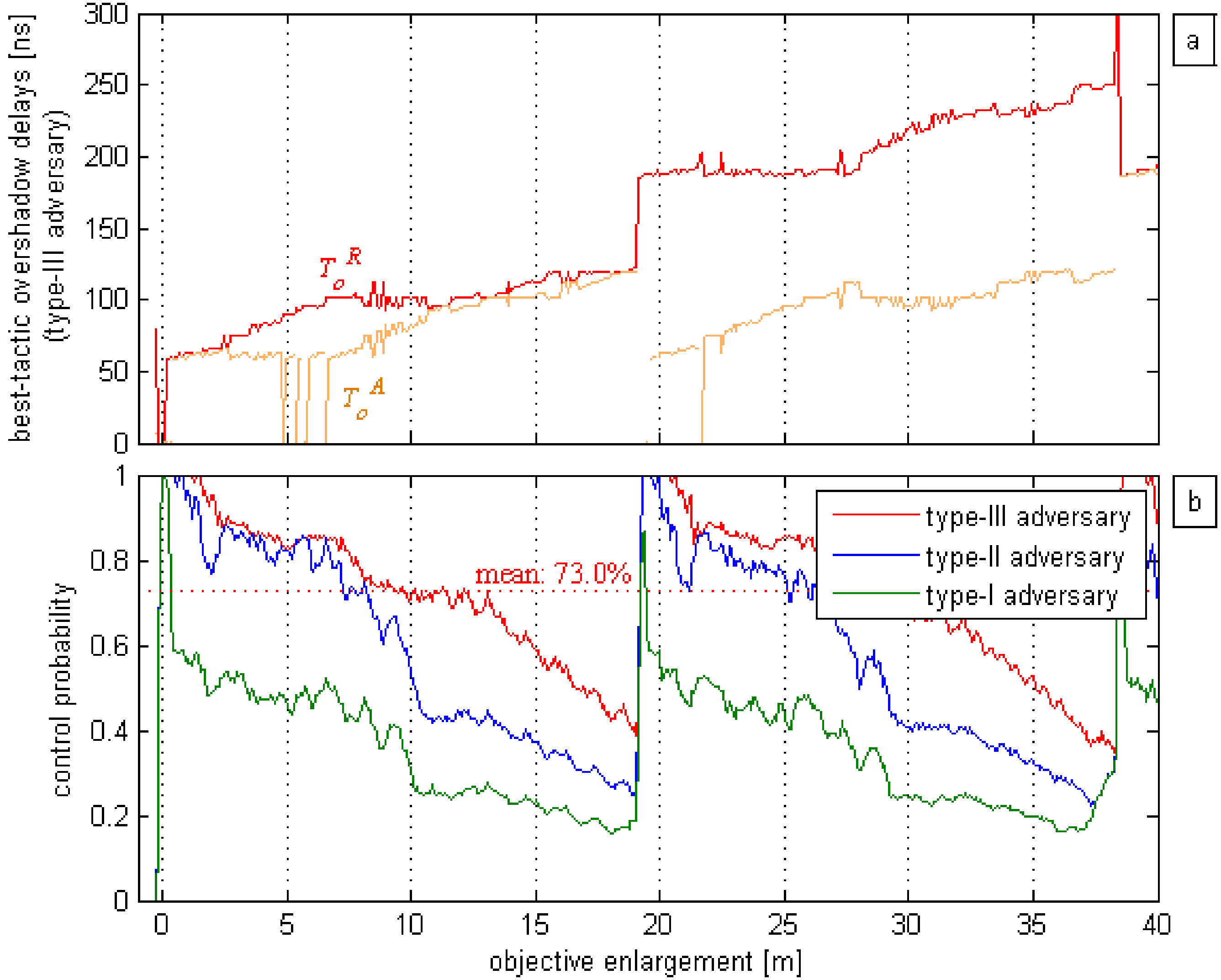
- Jump-back-search-forward algorithm:



- Search-back algorithm:

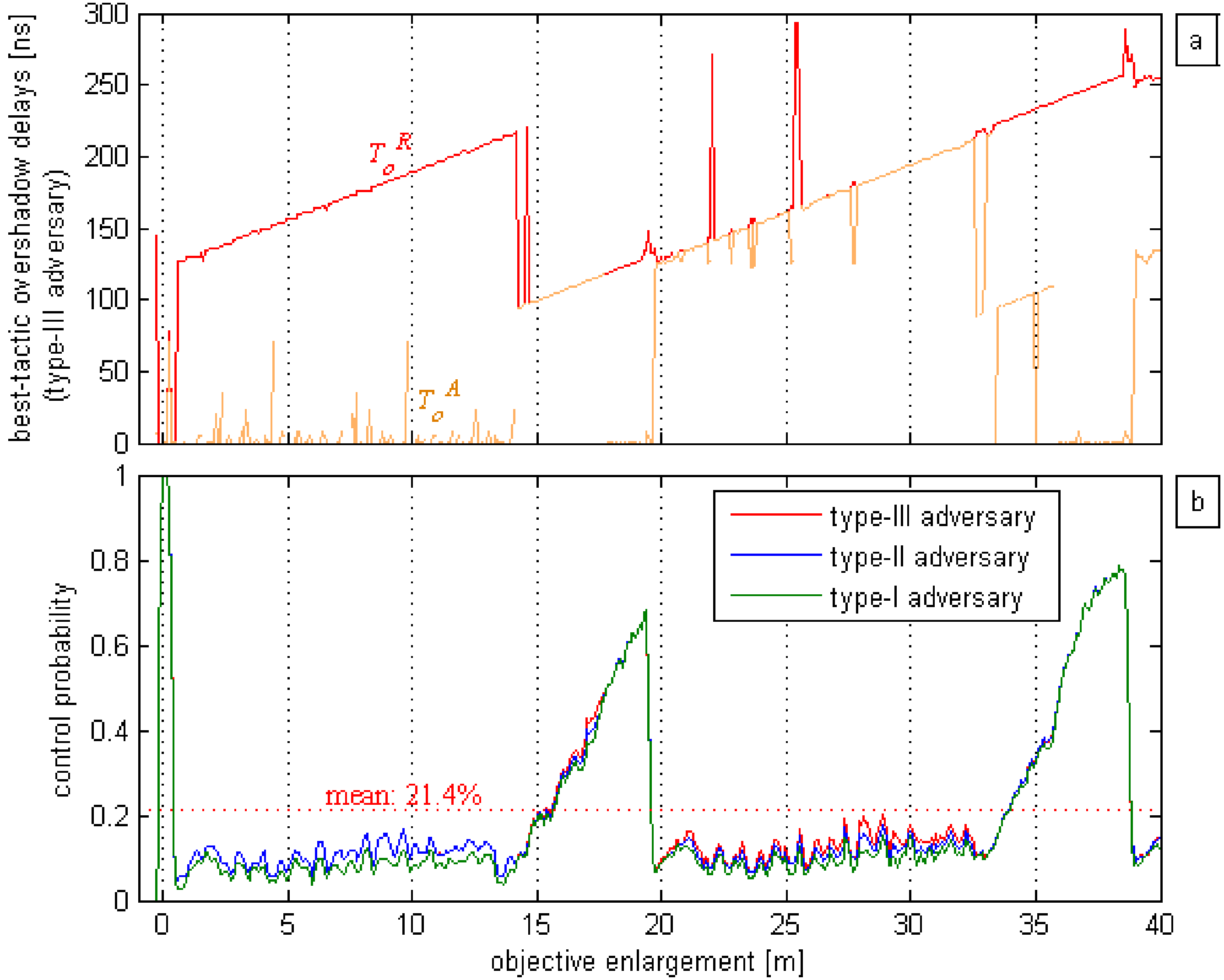


Enlargement attack best tactics



against jump-back-search-forward algorithm

Enlargement attack best tactics



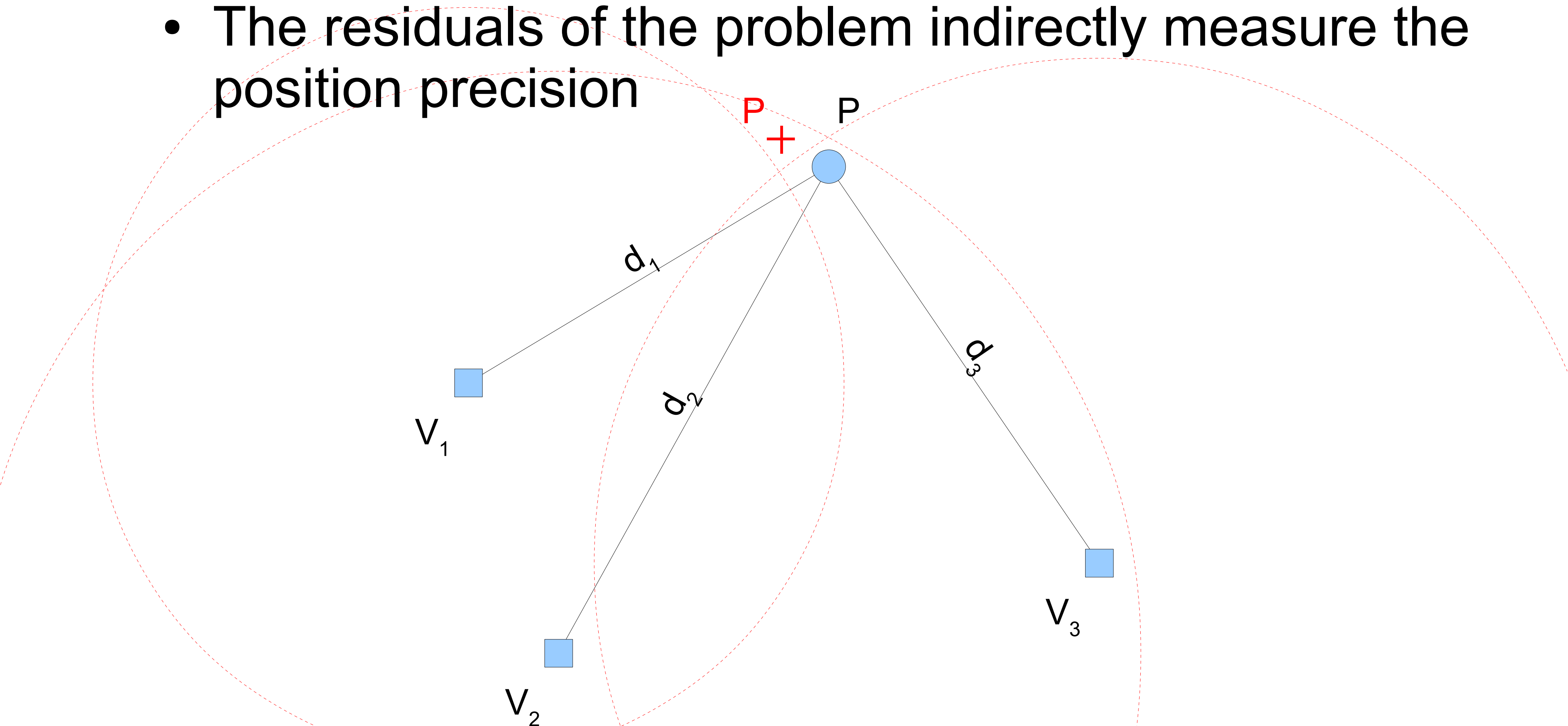
against search-back algorithm

EMCD-ML

- Enlargement-miscontrol detection multilateration
- *Idea*: detect an attack by detecting the imprecision of the adversary in enlargement attacks

(Real-life) multilateration

- In presence of ranging errors: *least-squared-error solution* (LSE)
    - The residuals of the problem indirectly measure the position precision

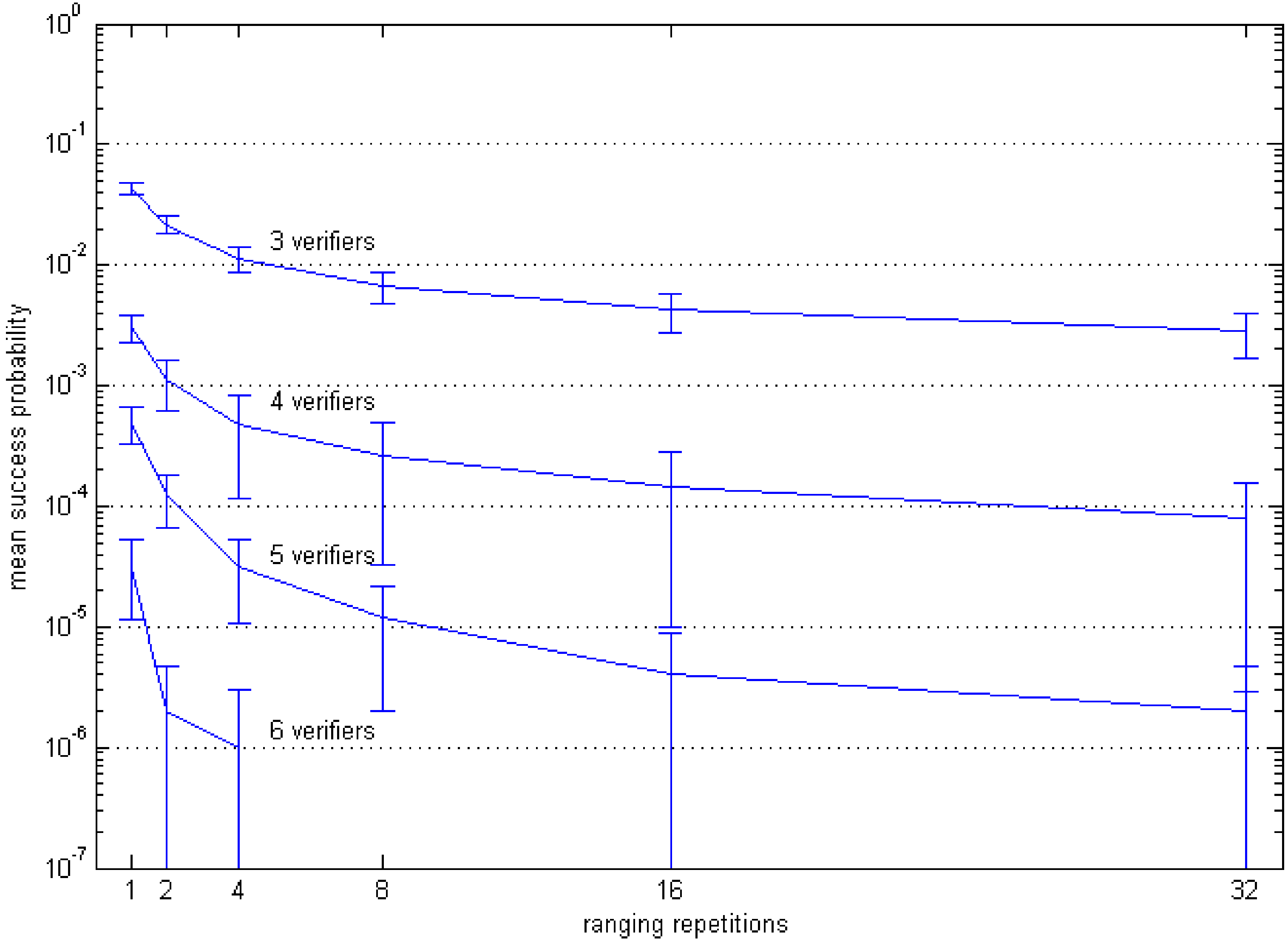


EMCD-ML

- Repeat each distance bounding *K* times and average the results
  - The adversary has to enlarge *K* times in a coherent manner
  - The honest system gets more precise, and we can detect more easily the small imprecisions of the adversary

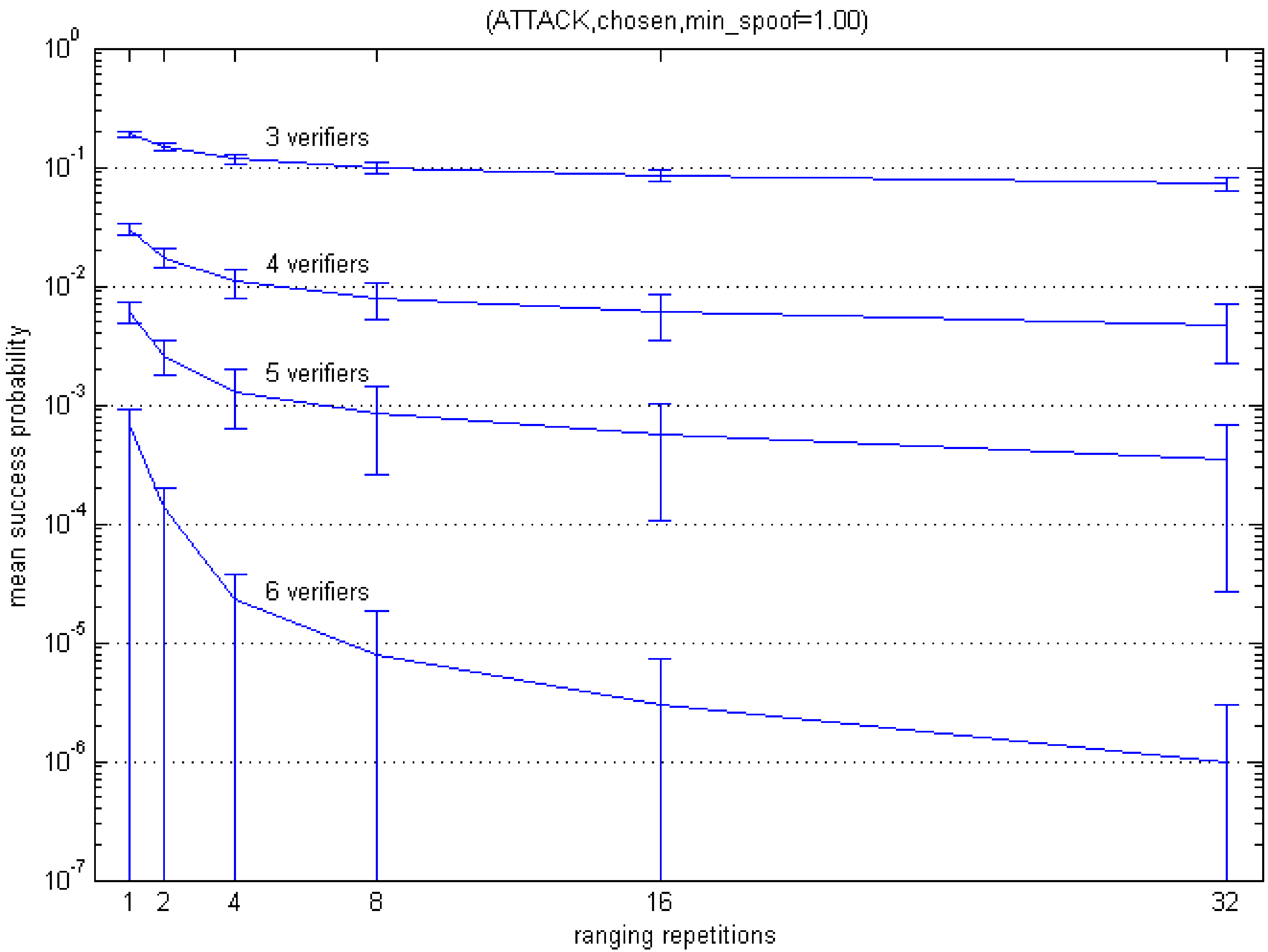
EMCD-ML

Random-objective adversary: the adversary chooses a random objective

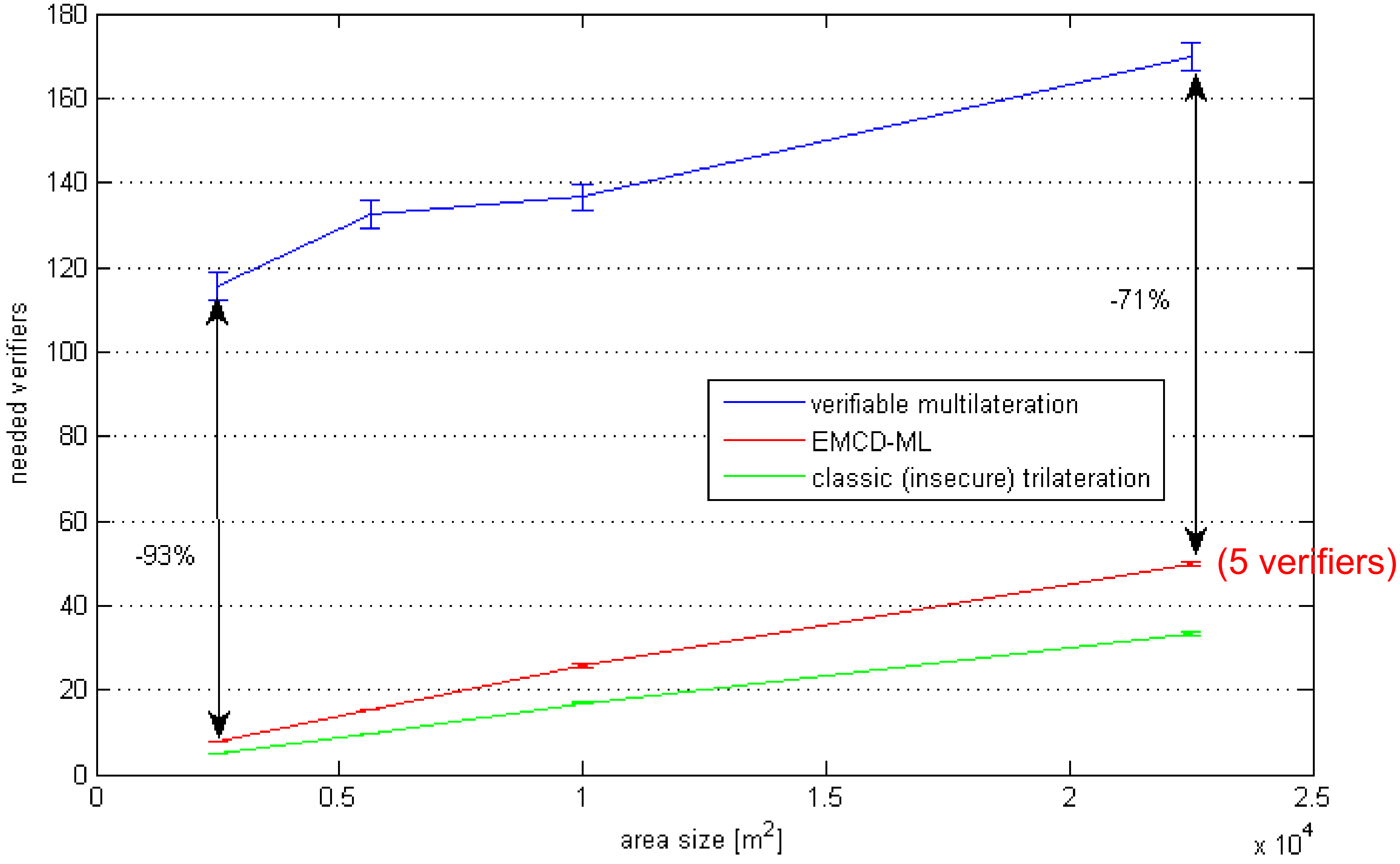


EMCD-ML

Chosen-objective adversary: the adversary chooses the easiest objective



EMCD-ML



180
160
140
120
100
80
60
40
20
0
0
0.5
1
1.5
2
2.5
x 10^4
area size [m^2]
needed verifiers
-71%
-93%
(5 verifiers)
verifiable multilateration
EMCD-ML
classic (insecure) trilateration