TDOA-ENHANCED DISTANCE BOUNDING

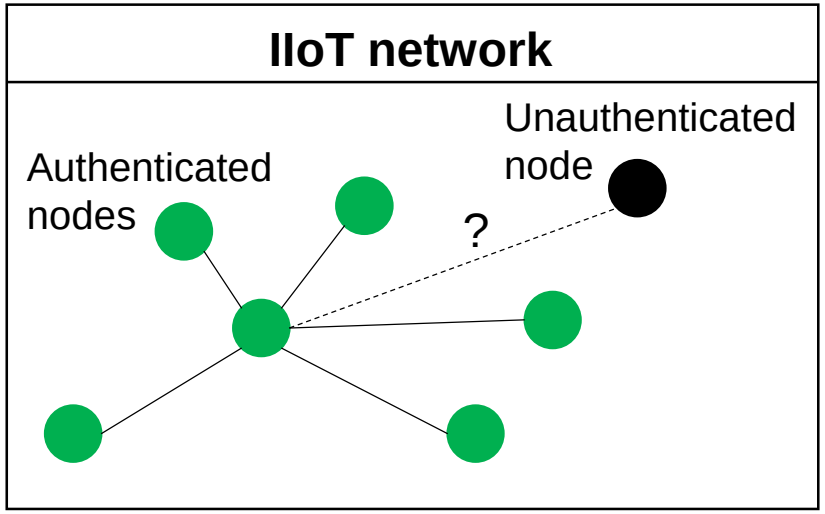
Núria Ballber Torres, nuria.ballber_torres@jku.at

Doctoral School 5G Internet of Things - Workshop 7-8 Sep 2021

- **Motivation - Security in Industrial Internet Of Things (IIoT)**
- **Authentication**
  - Distance bounding
  - Non Ideal Distance Bounding
- **Our Approach**
- **Time Difference of Arrival (TDOA)**
- **Simulations**
  - TDOA-location ambiguity without measurement noise
  - TDOA-location ambiguity with measurement noise
- **Attacks exploring location uncertainty**
- **Summary and Future Work**

MOTIVATION – SECURITY IN INDUSTRIAL INTERNET OF THINGS

- **Node authentication**

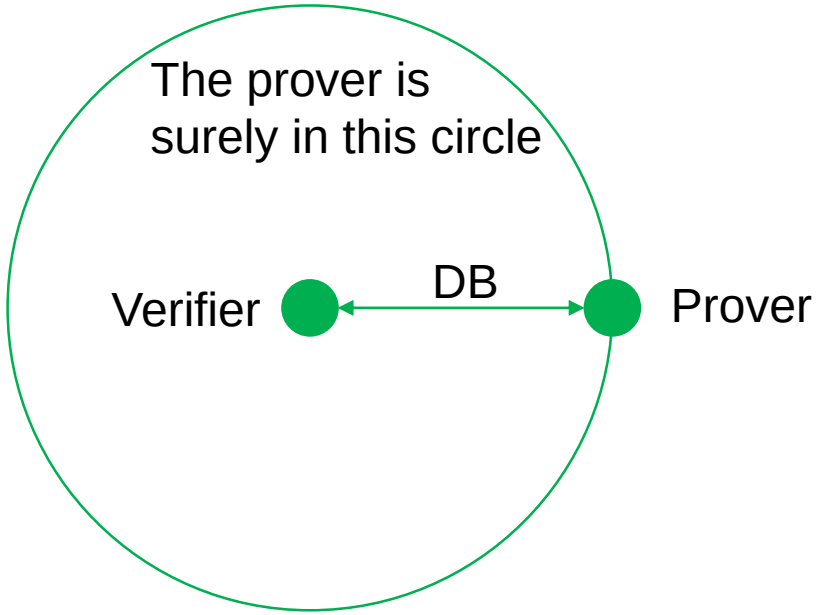


- **Distance bounding protocol:**

Authentication by establishing a distance upper bound

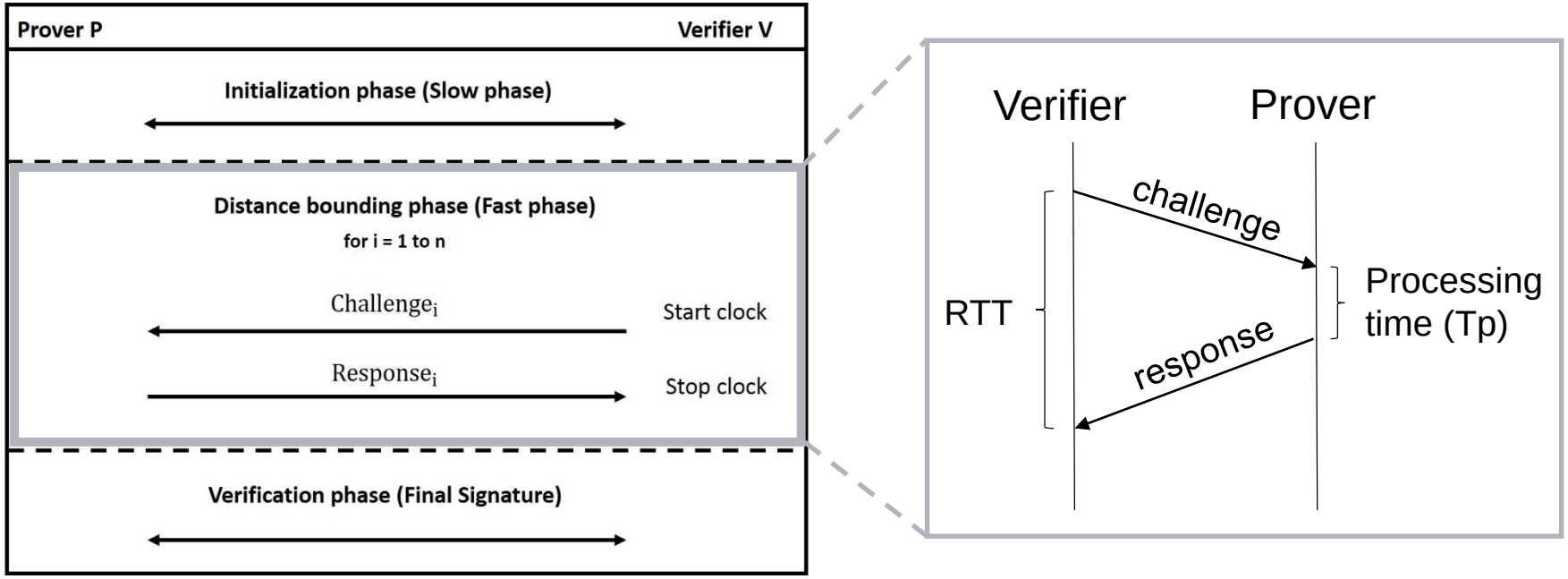
DISTANCE BOUNDING

- Authenticate an IIoT device by verifying its proximity



Source: https://redshift.autodesk.de/industrielles-internet-internet-der-dinge/

DISTANCE BOUNDING



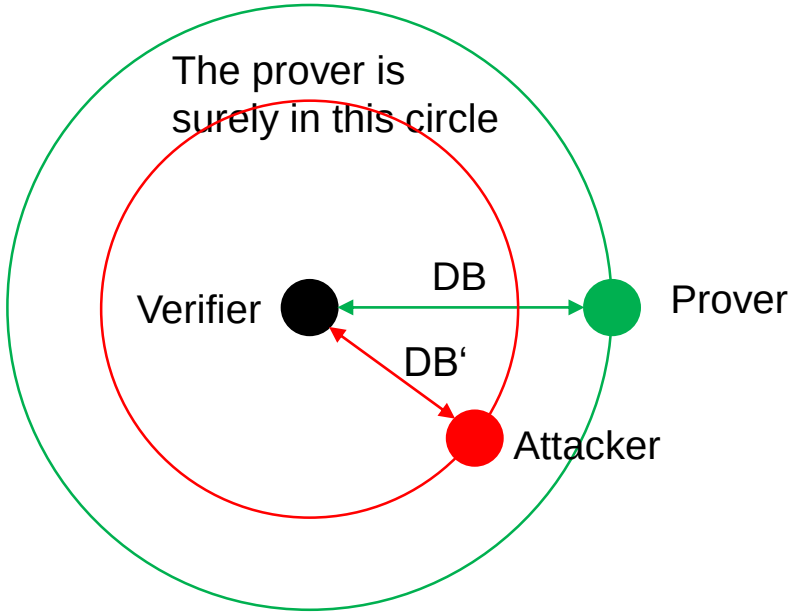
- A signal cannot go faster than light
- The prover cannot broadcast a valid response before receiving the challenge
- Elapsed time can be artificially increased, but not shortened

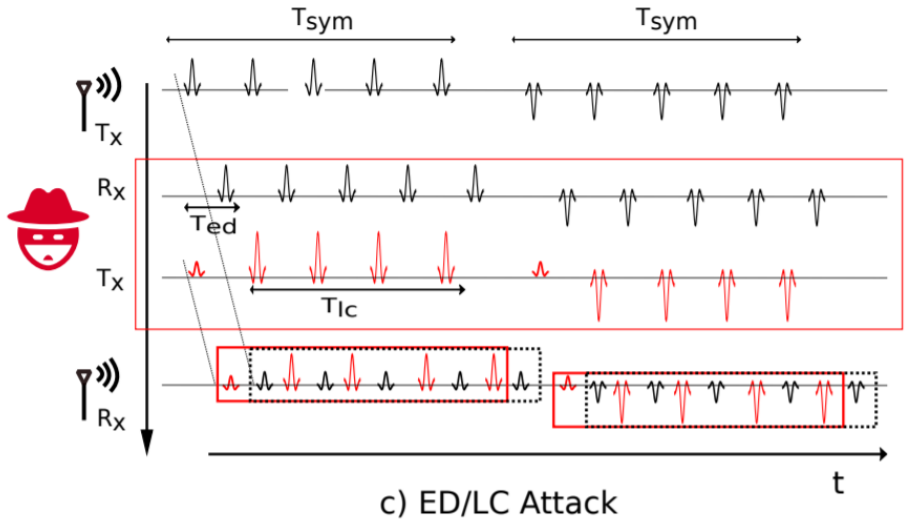
Distance upper bound

$$D = (RTT - Tp) * \frac{c}{2}$$

NON IDEAL DISTANCE BOUNDING

- Real-world communications
- Early detect attack
  - Early detection of the received bit
- Late commit attack
  - Early transmission of the bit



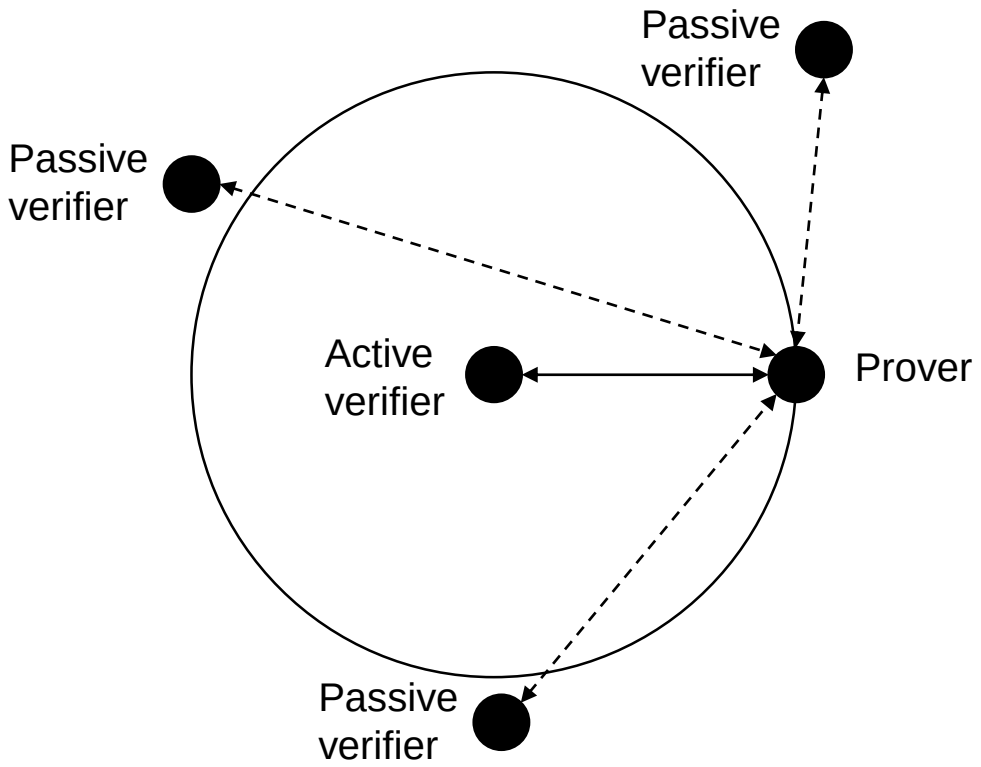


[1] M. Singh, P. Leu, and S. Capkun, “Uwb with pulse reordering: Securing ranging against relay and physical layer attacks,” tech. rep., Cryptology ePrint Archive, Report 2017/1240, 2017. https://eprint. iacr.org/2017/1240.

JKU

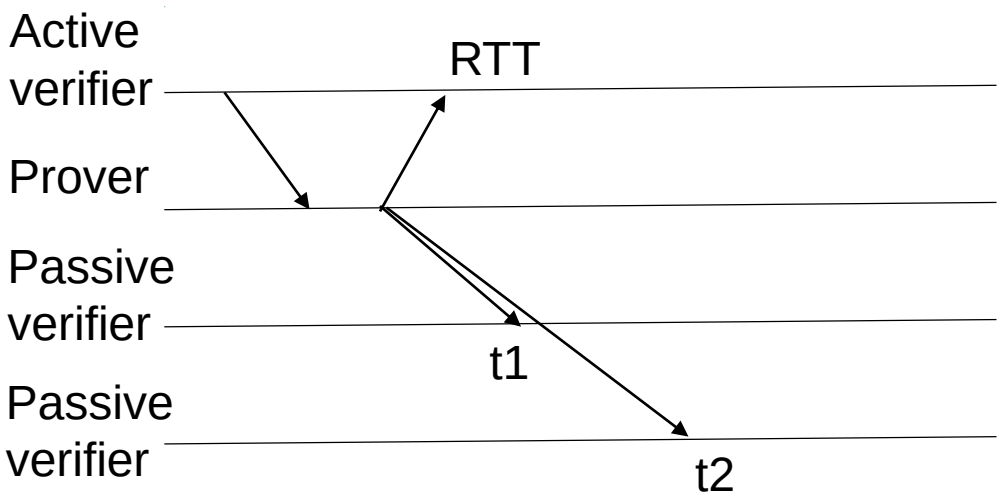
OUR APPROACH

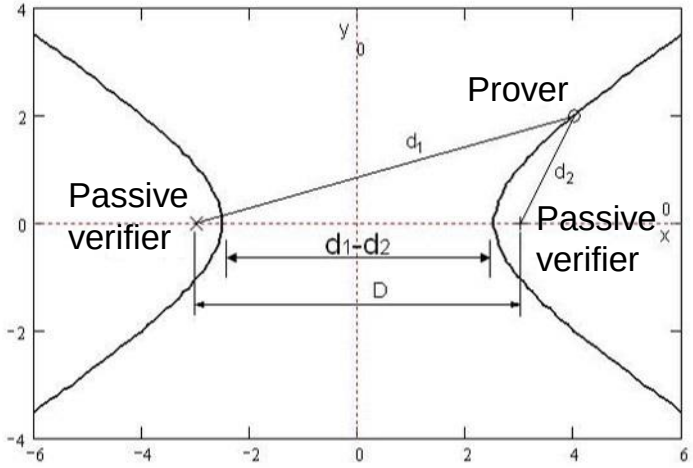
- Active verifier performing DB
- Addition of 3 passive verifiers performing TDOA



JKU

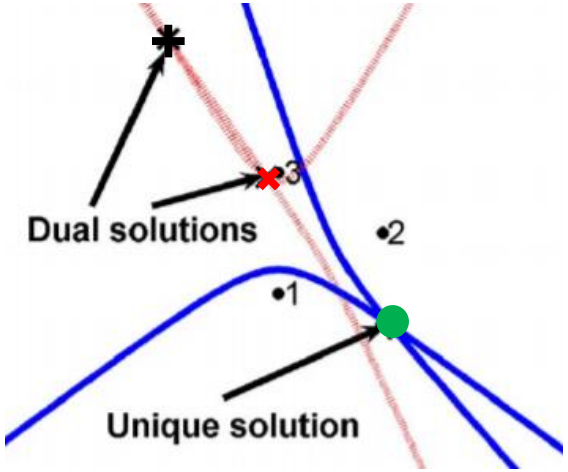
TIME DIFFERENCE OF ARRIVAL (TDOA)

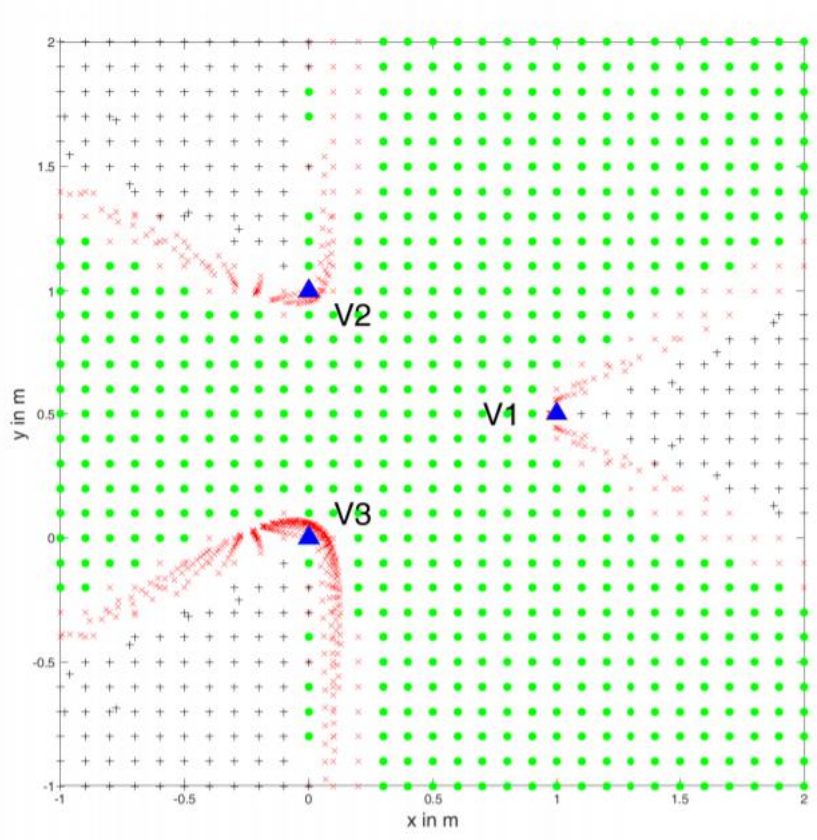




Time Difference of Arrival	Round trip time
$((t_{V1} - tr) - (t_{V2} - tr)) * c = d_{V1P} - d_{V2P}$ $d_{V1P} = \sqrt{(x - x_1)^2 + (y - y_1)^2}$ $d_{V2P} = \sqrt{(x - x_2)^2 + (y - y_2)^2}$ $P = (x, y) \quad V_i = (x_i, y_i)\ i = 1,2$	$D = (RTT - tr - Tp) * \frac{c}{2}$

TDOA-LOCATION AMBIGUITY WITHOUT MEASUREMENT NOISE





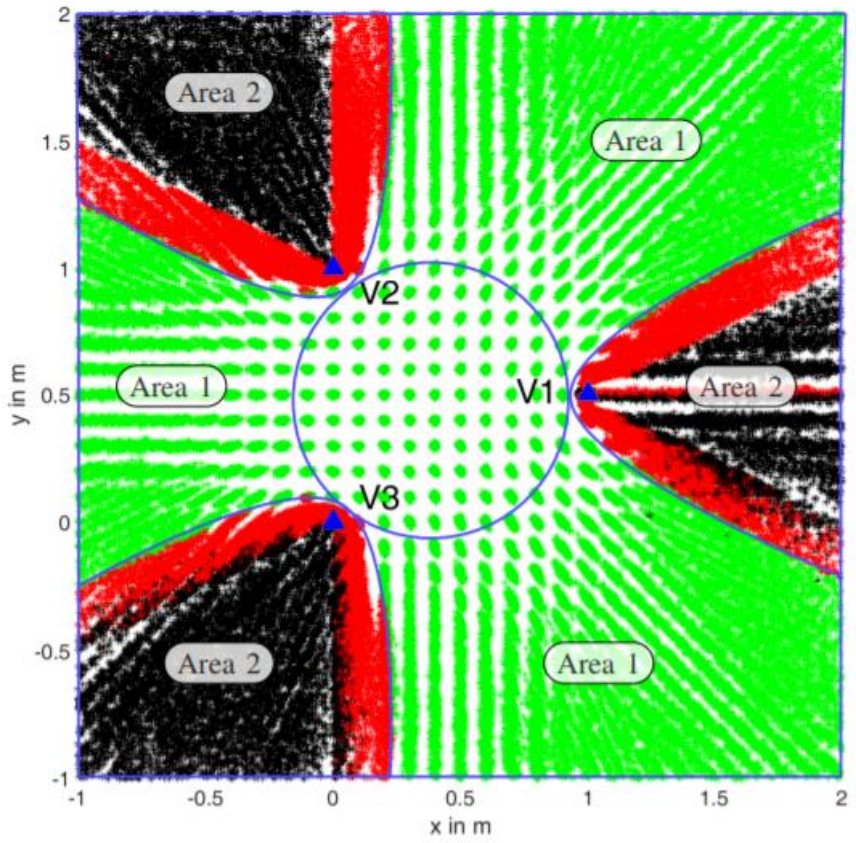
+ , x	●
Two possible solution areas	Single solution areas

[2] S. Spencer, “The two-dimensional source location problem for time differences of arrival at minimal element monitoring arrays,” *The Journal of the Acoustical Society of America*, vol. 121, pp. 3579–94, 2007.

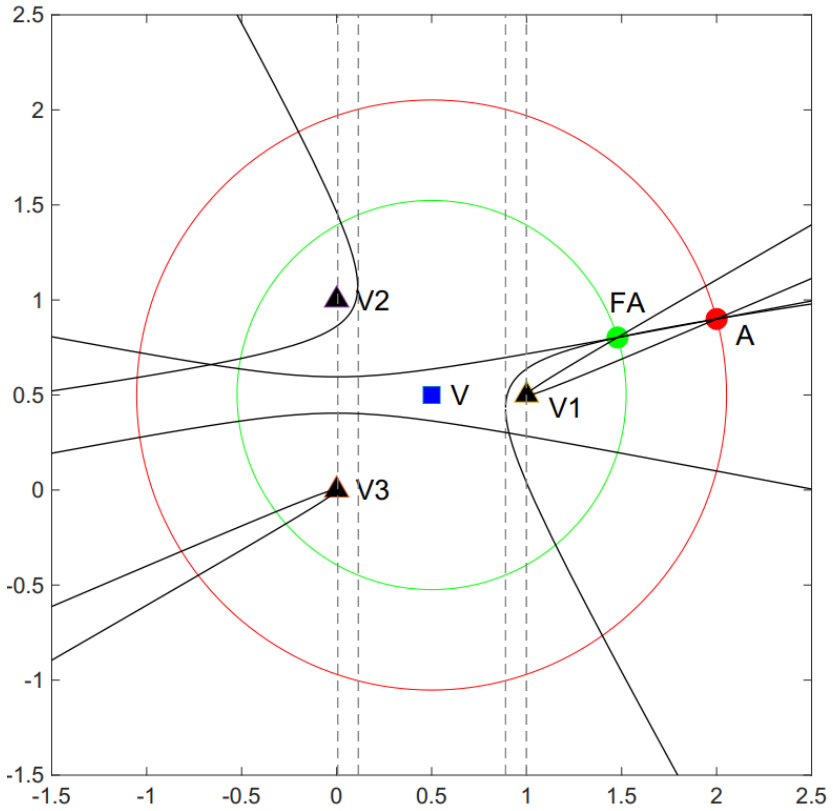
TDOA-LOCATION AMBIGUITY WITH MEASUREMENT NOISE

- Normal distributed noise
  - 0.16 ns standard deviation
  - 5 cm of accuracy

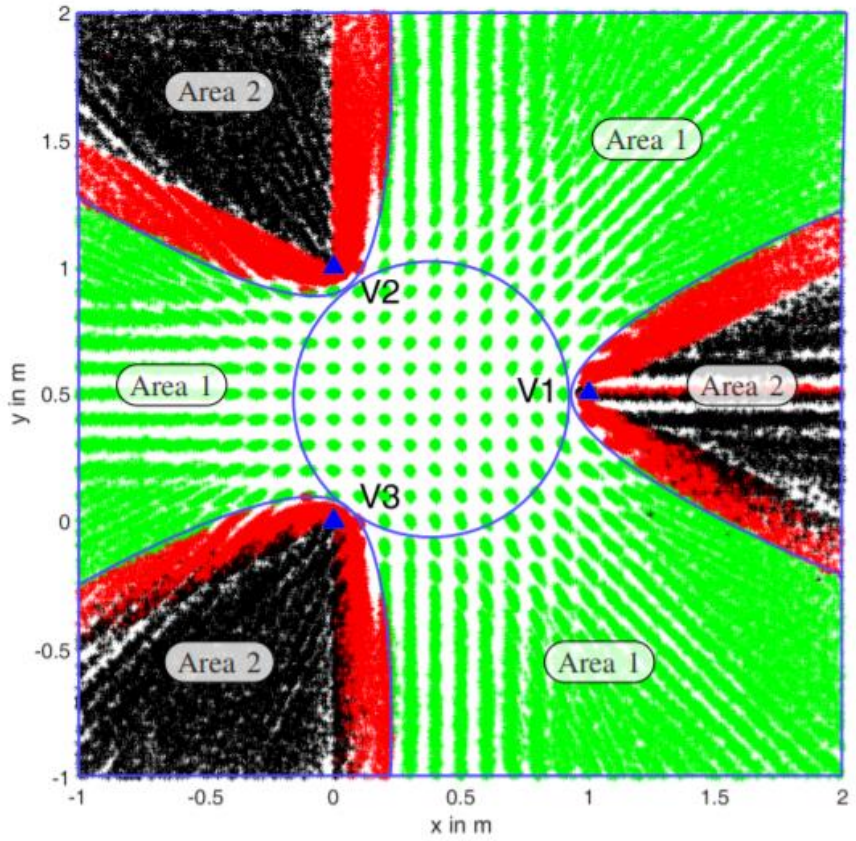
- Area 1: High uncertainty
- Area 2: Two possible solutions



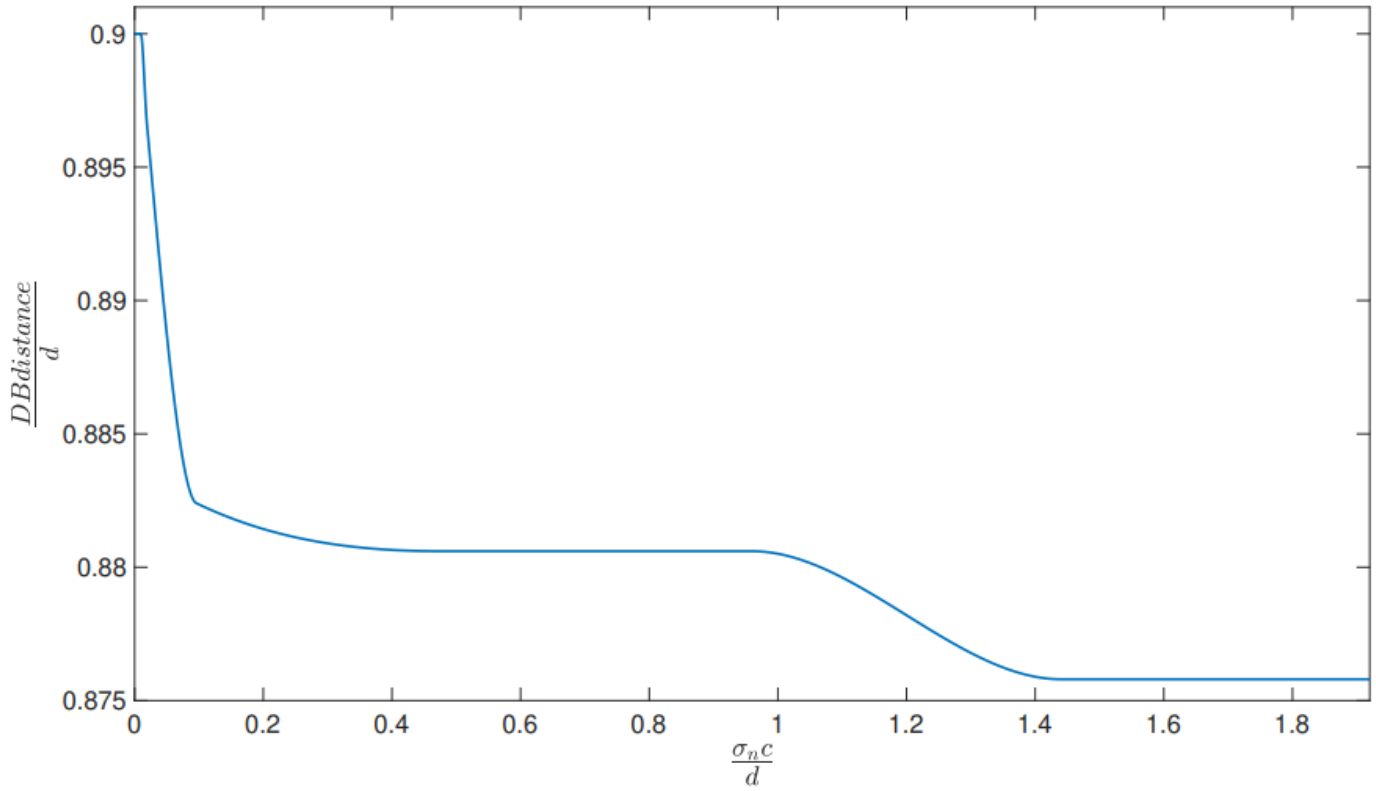
ATTACKS EXPLORING LOCATION UNCERTAINTY



PASSIVE VERIFIER PLACEMENT FOR SECURING DB



PASSIVE VERIFIER PLACEMENT FOR SECURING DB



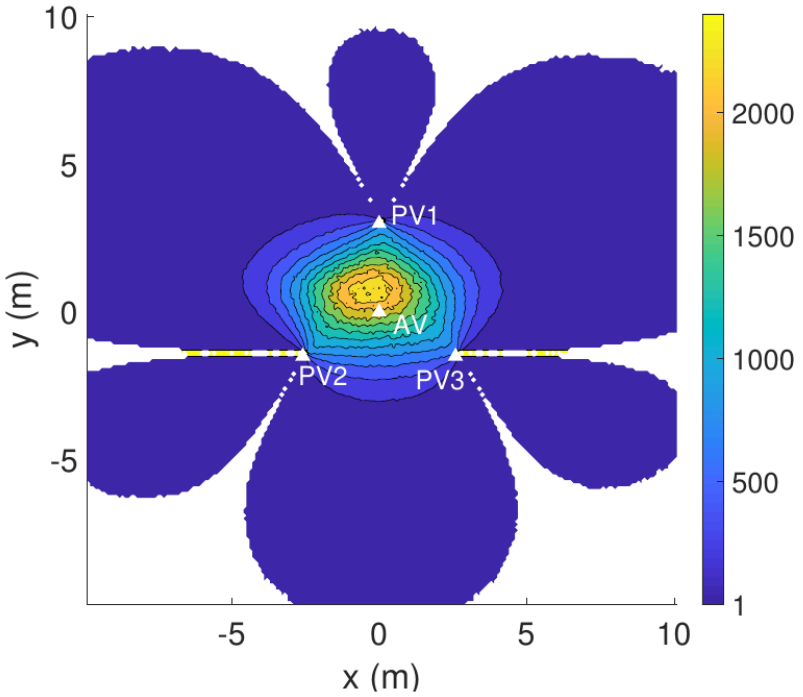
JKU

SUMMARY

- Addition of TDOA-localization to non-ideal DB
- Improvement of the resilience against ”early detect” and ”late commit” attacks
- Attacks exploiting uncertainty in the location estimation or in location ambiguity

CURRENT & FUTURE WORK

- Perform TDOA real-life measurements
- Define secure areas in TODA-based Distance Bounding and RTT-based Distance Bounding



JOHANNES KEPLER
UNIVERSITÄT LINZ

THANK YOU FOR YOUR ATTENTION

Questions?

JOHANNES KEPLER
UNIVERSITÄT LINZ
Altenberger Straße 69
4040 Linz, Österreich
www.jku.at