GEORG-AUGUST-UNIVERSITÄT
GÖTTINGEN

Advanced Topics in Mobile Communications

Wireless Security

- Session: Location -

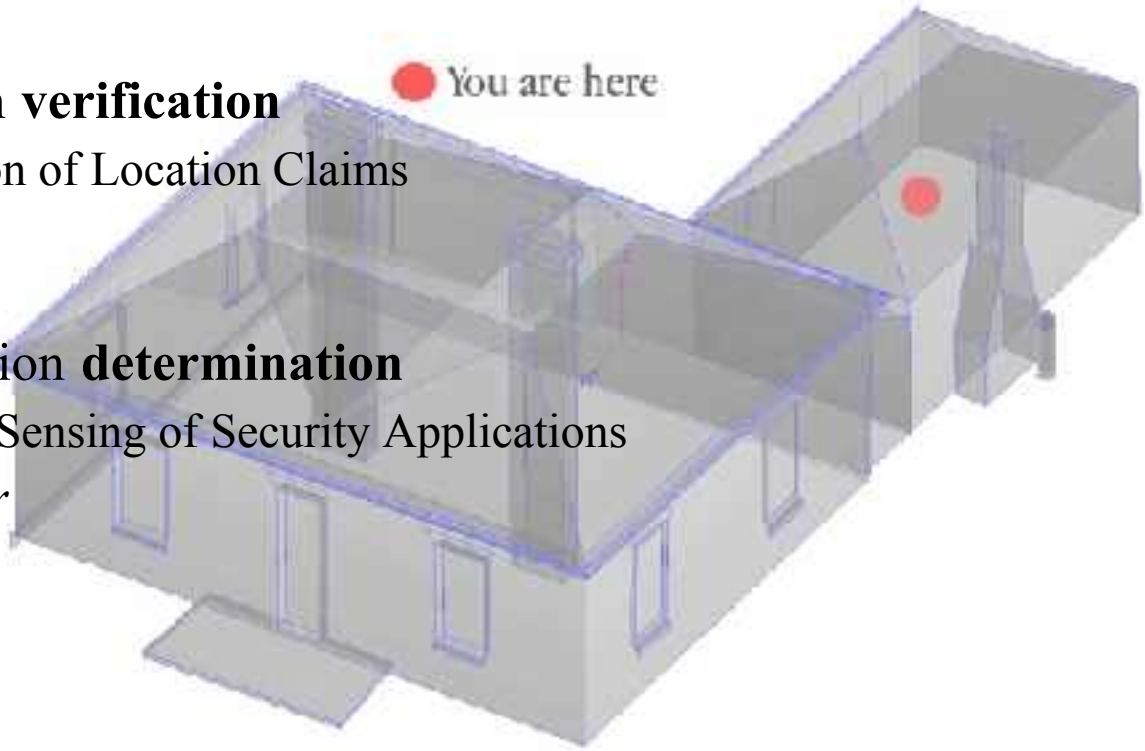
Alexander Willner, 20109435
mail@AlexanderWillner.de

Telematics Group
Institute for Informatics

University of Göttingen, Germany

Overview | what is this presentation about

- Motivation
  - Why do we need location based systems?
  - Location verification vs. location determination
- First issue: Secure location **verification**
  - Paper: Secure Verification of Location Claims
  - Protocol: *Echo*
- Second issue: Secure location **determination**
  - Paper: WLAN Location-Sensing of Security Applications
  - Protocol: based on *Radar*
- Conclusion
- Future directions



Motivation | location systems

- **Topic:** How to *secure* locate the position of a target (e.g. mobile device)?

- **Why**
  - First example: Provide useful user functionality based on the location. E.g. gain special services for free to visitors of a football match *after* enter the stadium. Otherwise they have to pay for the service if they are outside of the building.
  - Second example: Locate a malicious mobile device in order to remove it.
  - A lot of more areas of application are possible

- The field of location-aware computing deals with two principal tasks
  - Determine and track the position of a mobile device
  - Provide useful user functionality based on the location

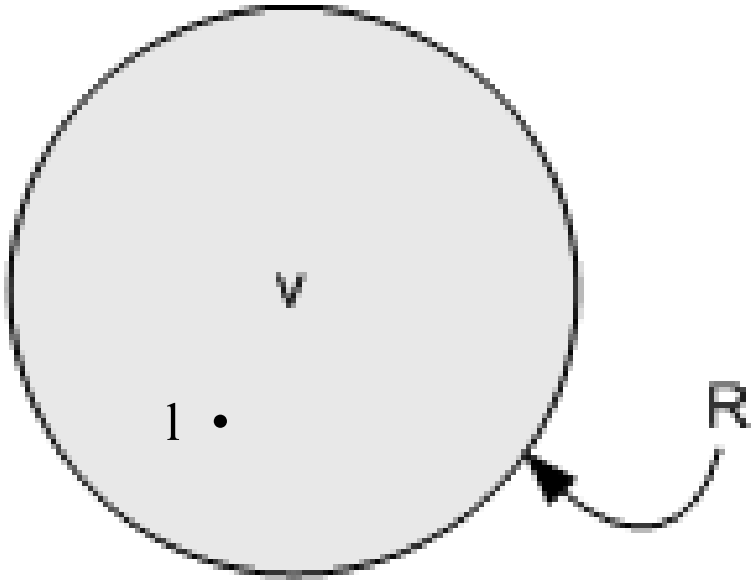
- **How:** Two different issues to locate the position of a target
  - Location *verification*: The system verifies the location the target stated (active)
  - Location *determination*: The system is determining the location of a target (passive)

Location verification

- **Topic:** How to *secure* locate the position of a target (e.g. mobile device)?
- **Why**
  - First example: Provide useful user functionality based on the location. E.g. gain special services for free to visitors of a football match after enter the stadium. Otherwise they have to pay for the service if they are outside of the building.
  - Second example: Locate a mobile malicious device in order to remove it.
  - A lot of more areas of application possible
- The field of location-aware computing deals with two principal tasks
  - Determine and track the position of a mobile device
  - Provide useful user functionality based on the location
- **How:** Two different issues to locate the position of a target
  - Location *verification*: The system verifies the location the target stated (active)
  - Location *determination*: The system is determining the location of a target (passive)

Location verification | introduction

- First simplification of the problem: secure in-region verification



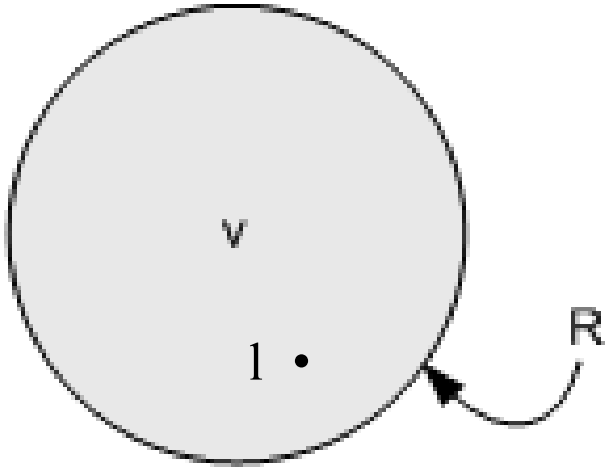
- l: location of the prover p (the user)
- v: verifier node
- R: region of interest

Location verification | design principles

- Work primarily initiated in the context of nodes in sensor networks
- Resulted constraints to the hardware
  - Small cheap nodes
  - Minimum computation (e.g. no public-key technique possible)
  - Variety of environmental sensors
- Requirements to the location system
  - Make few resource demands on the prover and verifier
  - No prearranged setup required
  - Quantitative guarantees
- Simplification of the problem
  - Only “local” regions
  - Verify hole regions, not points
  - **Use of special hardware**

Location verification | idea

- The idea is older than 60 mill. years: Similar to the system of bats
- Use both radio frequency (RF) and sound (ultrasound)
- Speed of sound waves: approx. 330 m/s (light/RF: approx. 300.000.000 m/s)



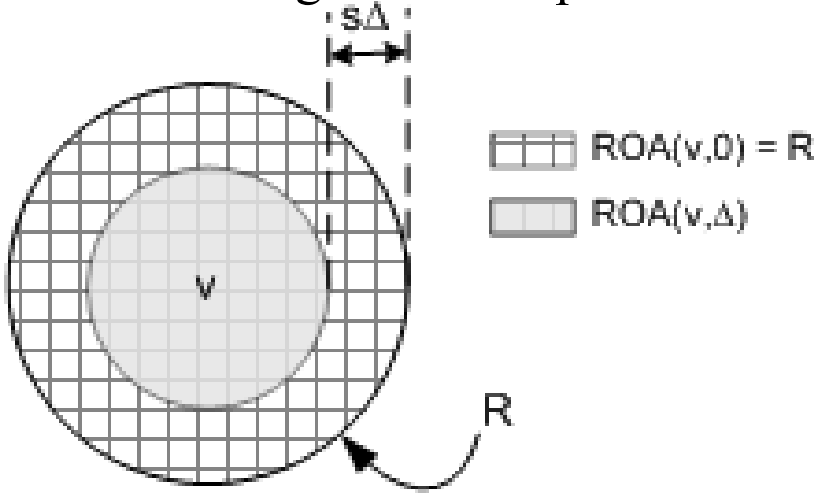
1. $p \xrightarrow{\text{radio}} v : \ell$
2. $v \xrightarrow{\text{radio}} p : N$
3. $p \xrightarrow{\text{sound}} v : N$

v accepts if $\ell \in R$ and
elapsed time $\leq d(v, \ell) \cdot (c^{-1} + s^{-1})$.

- The *Echo* protocol
  - **p** sends a request to **v** via RF
  - **v** sends an arbitrary value **N** to **p** via RF
  - **p** sends the arbitrary value **N** back to **v** via sound
  - **v** checks the response time and calculates the distance

Location verification | first problem

- Processing delay reduces the region of acceptance



ROA: Region of Acceptance

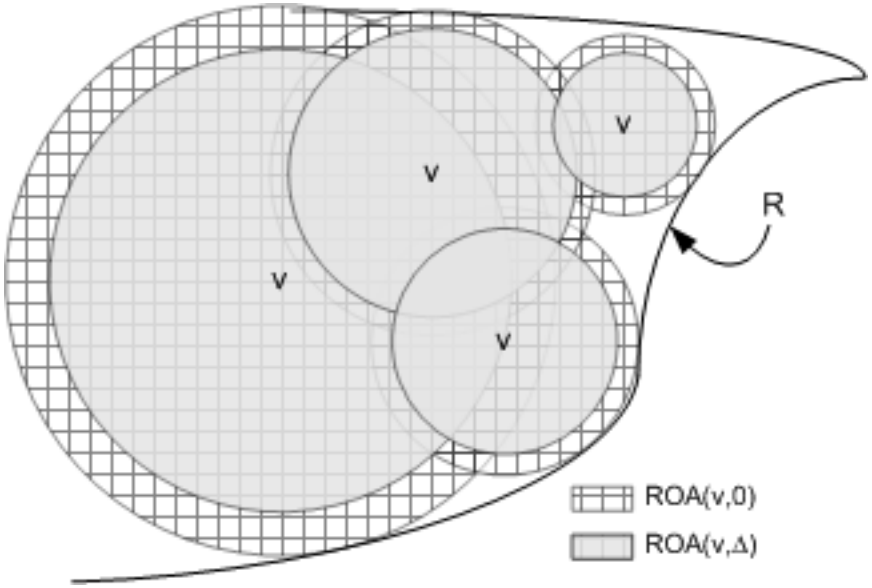
- In an ideal case the prover can respond immediately after receive the value
  - ROA (v, 0) -> first slide
- In practice the prover needs a processing delay of at least sΔ seconds
  - ROA (v, sΔ)
- **Remember**: **v** checks the response time (*now with the added processing delay)* and calculates the wrong distance
- **Possible attack:** No attack possible since the calculation is based on physical laws

Location verification | second problem

- Packet transmission time
  - Start timing either before the first bit or after the last bit?
  - Stop timing before the first bit or after the last bit?
- **Remember**: **v** checks the response time (*now with the added transmission delay)* and calculates the distance
- **Possible attack:** Exploit the transmission delay to launch an attack
  - The attacker could simply guess the first (or last) few bits of the nonce and send them preemptively
- **Example**: Suppose the verifier stops its timer upon receiving the first bits. The attacker could start sending a few randomly guessed bits
  - **Effect: v** calculates a too small distance
- **Solution:** Verifier should start timing before sending first bit and stop after receiving last bit to avoid this problem

Location verification | third problem

- Non-circular regions



- Since the we assume that our communications equipment is omnidirektional and signals travel at the same time the ROA **must** be a circle
- **Possible attack**: If the ROA is to bigger than R an attacker can naturally be in ROA without being in R
- **Example**: See black board
- **Solution**: Use more than one verifier with different ranges of coverage

Location verification | summary

- Introduced an in-region verification problem
- Echo is an provable secure and lightweight protocol
- Its security rests on physical properties of sound and RF signals
- It does not require an cryptography, time synchronization or any prior agreements
- Therefore it is suitable for low-cost devices such as those in sensor networks
- It could guarantee in-region verification for 80-90% of legitimate location claims
- It is based on specific hardware

Location determination

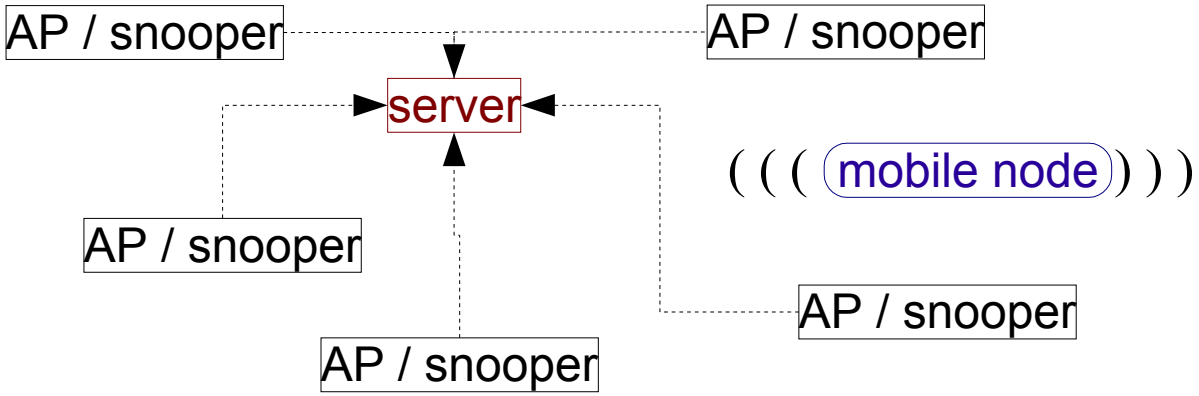
- **Topic:** How to *secure* locate the position of a target (e.g. mobile device)?
- **Why**
  - First example: Provide useful user functionality based on the location. E.g. gain special services for free to visitors of a football match after enter the stadium. Otherwise they have to pay for the service if they are outside of the building.
  - Second example: Locate a mobile malicious device in order to remove it.
  - A lot of more areas of application possible
- The field of location-aware computing deals with two principal tasks
  - Determine and track the position of a mobile device
  - Provide useful user functionality based on the location
- **How:** Two different issues to locate the position of a target
  - Location *verification*: The system verifies the location the target stated (active)
  - Location *determination*: The system is determining the location of a target (passive)

Location determination | idea

- **Idea:** The system is based on the following association
  - Use the signal strength / transmission power of WLAN equipment
  - Calculate the position with an implementation of a Markov localization algorithm and the signal strength
- **Status quo**: Typically the *Radar* protocol is used to localize targets in a 802.11 environment inside buildings without their cooperation
  - e.g. locate the position of an malicious mobile device in order to remove it
- **Advantage**: Does not require any modifications to the hardware or software

Location determination | design

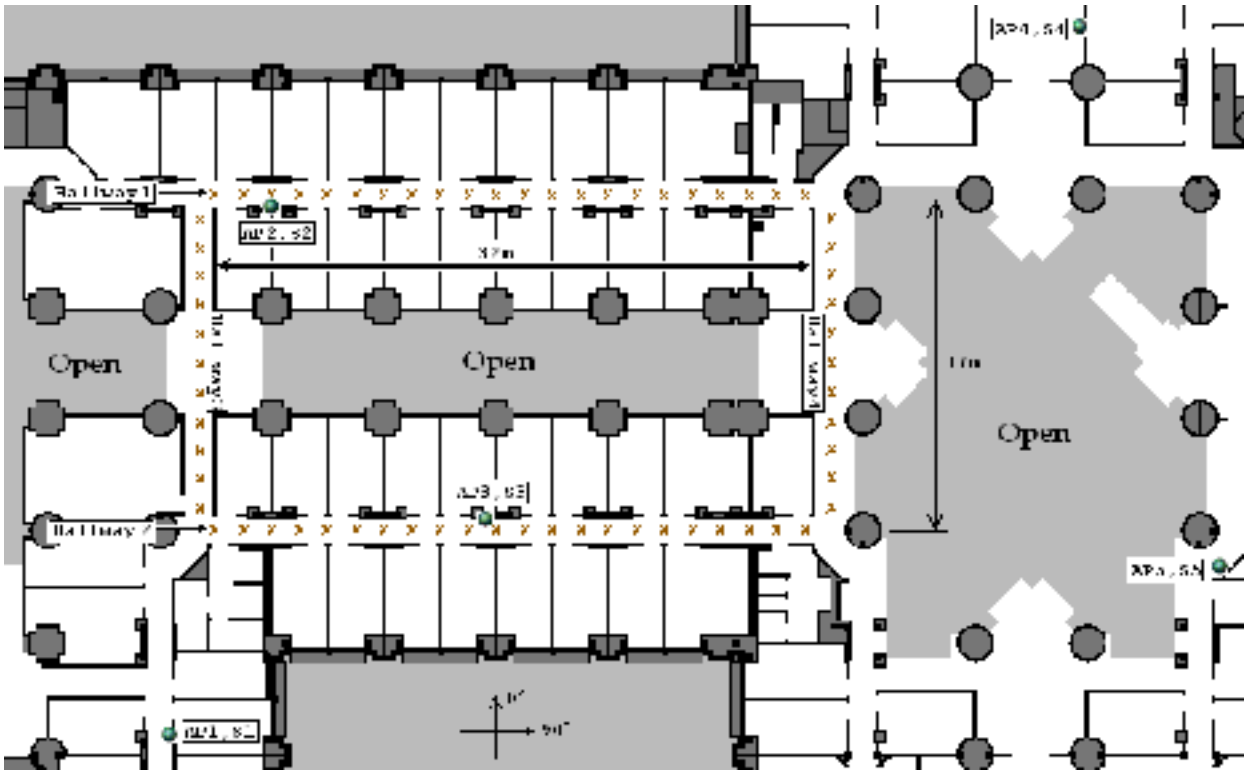
- Server-side architecture



- Snooper
  - Observes the signal strength
  - Upon request it temporarily switches the channel and measures the target station´s strength of packets
- Server
  - Collects signal strengths
  - Contains the Bayesian network and calculates the relative position

Location determination | training mode

- **Preparation**: The system has to be trained at first!
  - Sample sensor readings from different known positions



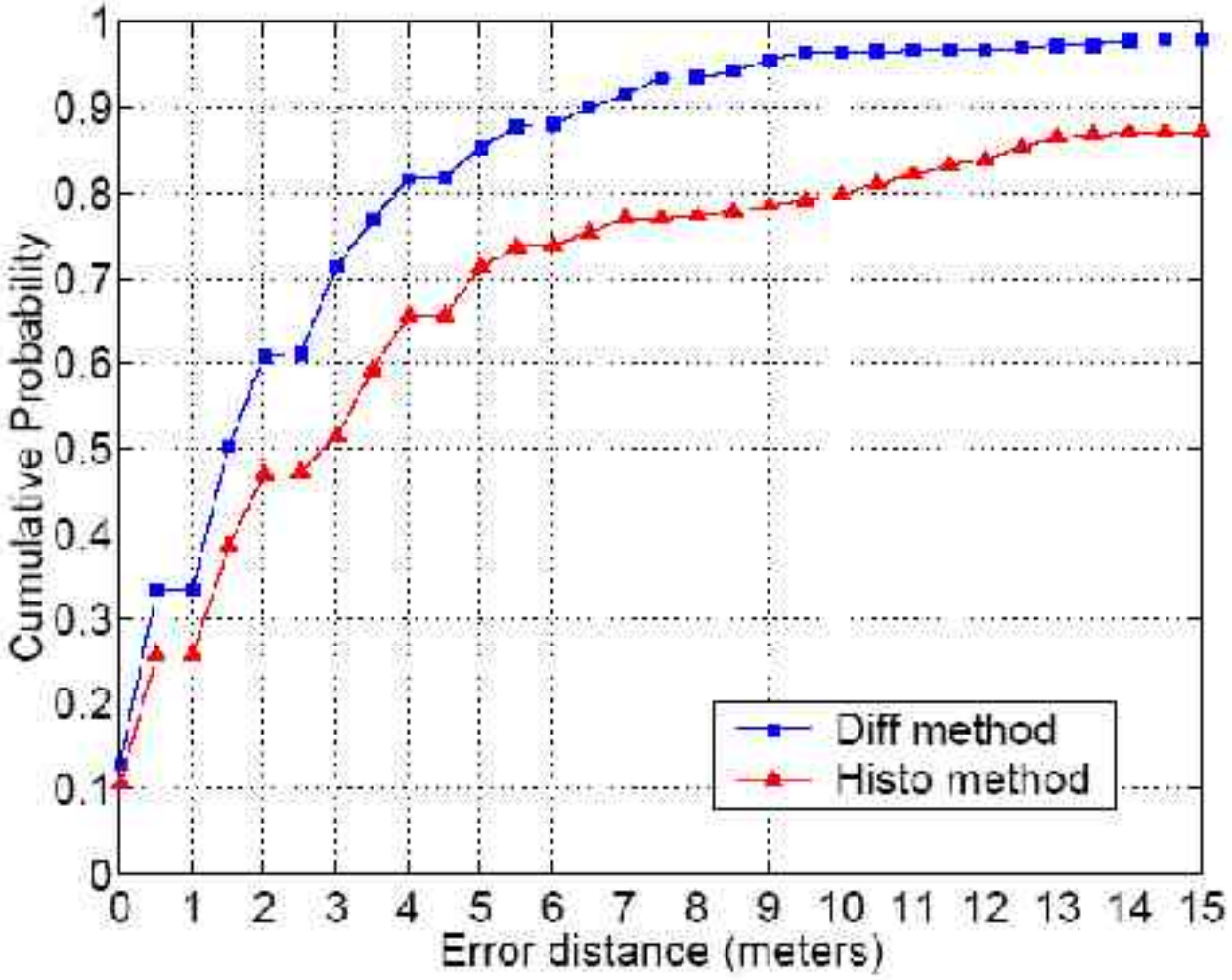
x : tested location

Location determination | security enhancement

- There are two main security enhancements to the *Radar* protocol
- Signal strengths
  - The signal strength was observed by the mobile device (client-side)
    - **Possible attack**: An malicious device could send wrong informations in order to hide its true position
  - **Solution**: Get the signal strength from the APs/snoopers (server-side)
- Localization algorithms
  - Histogram method was developed in the prior work
    - **Possible attack**: This method is vulnerable to alternate signal strengths. Rough machines could variate the transmission power while sending packets.
  - **Solution**:
    - Difference method is a mathematical more resistant algorithm.
    - Use the mathematical mean of two signal strengths measured by two APs

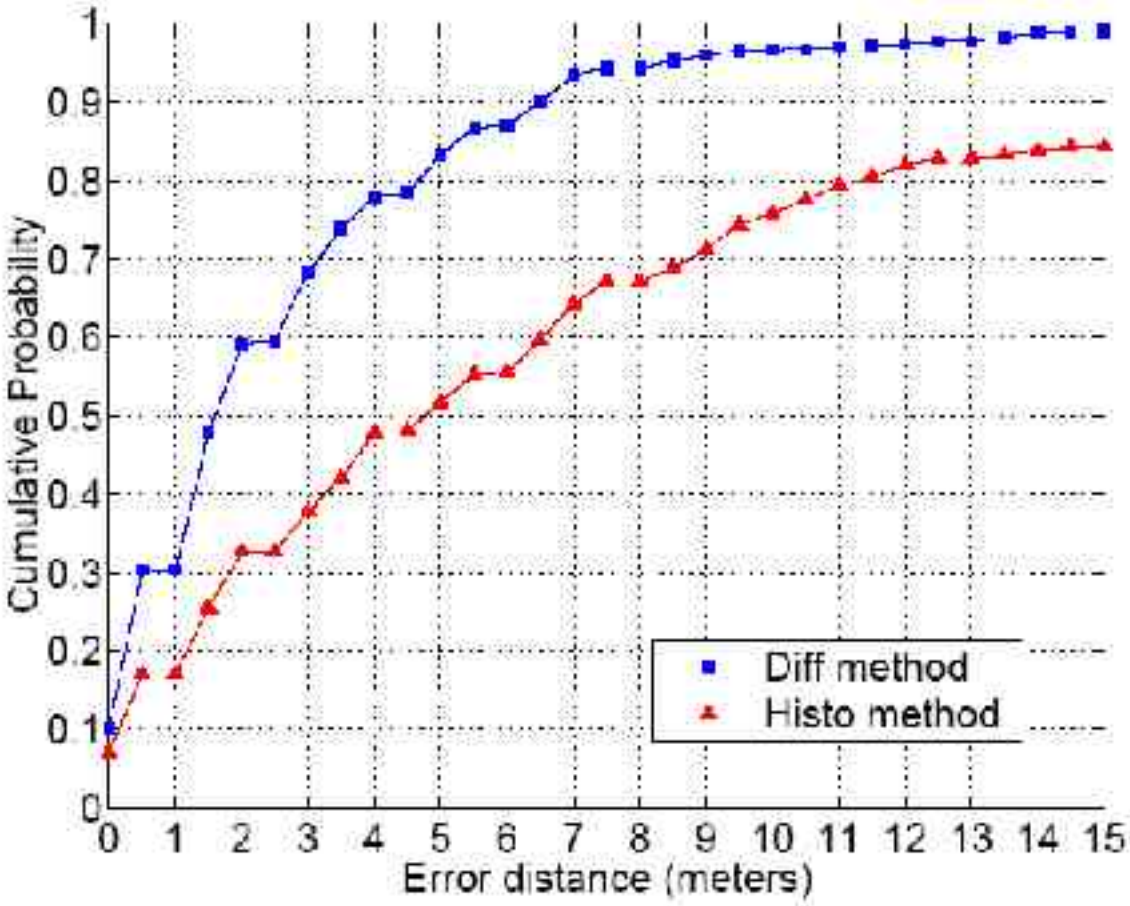
Location determination | result 1

- Accuracy of the location in meters using a friendly device



Location determination | result 2

- Accuracy of the location in meters where transmission power level is reduced for every packet by an malicious device



Location determination | summary

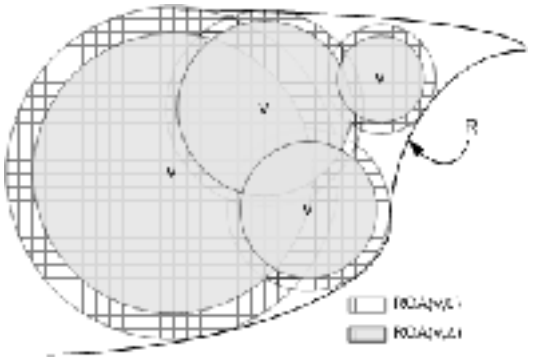
- Introduced a server-side indoor location-sensing system
- It is based on popular 802.11 hardware (no modifications to the hardware or software needed)
- The area of interest (similar to the ROA) have to be trained in an off-line phase
- Secure enhancement of traditional localization method (see result 1 and result 2)

Conclusion

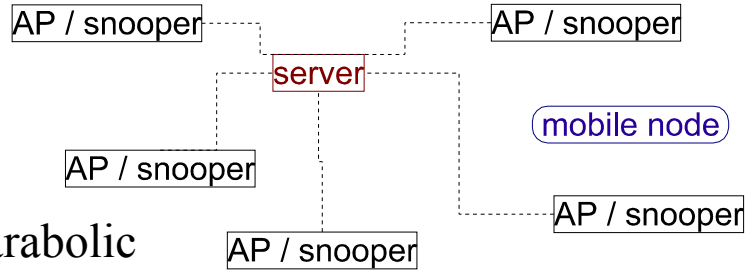
- Both systems could gain a user services and specific informations based on his/her physical position
- They are different issues and areas of application
  - Echo protocol: Localize targets just in a range in an active way with special hardware
  - Radar protocol: Localize targets to points in a passive way with popular used hardware
- Both issues are just able to locate a target in a specific (trained) local range
- Different possible attacks to both systems were mentioned and solved

Future directions

- **Location verifications (Echo protocol)**
  - Enhancement: Intersection
    - A more precise region verification could be done when using e.g. Triangulation
    - Status quo: **v1** and **v2** do not communicate with each other



  - Enhancement: Keyed Echo protocol (pre-shared keys)
    - If **v** and **p** previously exchanged a key it can be used to verify that a *particular* prover is inside a region
- **Location determination (Radar protocol)**
  - Enhance filters for a better accuracy
  - Sensor fusion (Intersection)
  - This issue raises interesting privacy issues
  - Compass the direction to an attacker with parabolic or other non-standard antennas
  - Enhance robustness against different hardware and nodes outside the trained area



Thank for your attention...