Detecting Rogue AP with the Crowd Wisdom

Tongqing Zhou, Zhiping Cai, Bin Xiao, Yueyue Chen, Ming Xu

zhoutongqing@nudt.edu.cn

National University Of Defense Technology, China
The Hong Kong Polytechnic University, Hong Kong

Content

- Background
- Motivation
- The CRAD approach
- Evaluation

Background 1/2

Openness of such places

Weak Security Mechanism

Personal Information

Background 2/2

- Rogue APs are easy to launch[1]
- 20% of all APs in enterprise WLANs are in fact rogue APs[2]

ITV REPORT 21 January 2015 at 1:54pm

7-year-old girl takes just 10 minutes to hack into public WiFi network and access stranger's laptop

Some public WiFi hotspots are so unsecure they can be hacked into by primary school children - as seven-year-old Betsy Davies proved as part of a new experiment.

[1] Public wi-fi hacked by seven year old in 10 minutes, http://www.welivesecurity.com/.
[2] Beyah, R., Venkataraman, A. (2011). Rogue-access-point detection: Challenges, solutions, and future directions. IEEE Security & Privacy.

Motivation

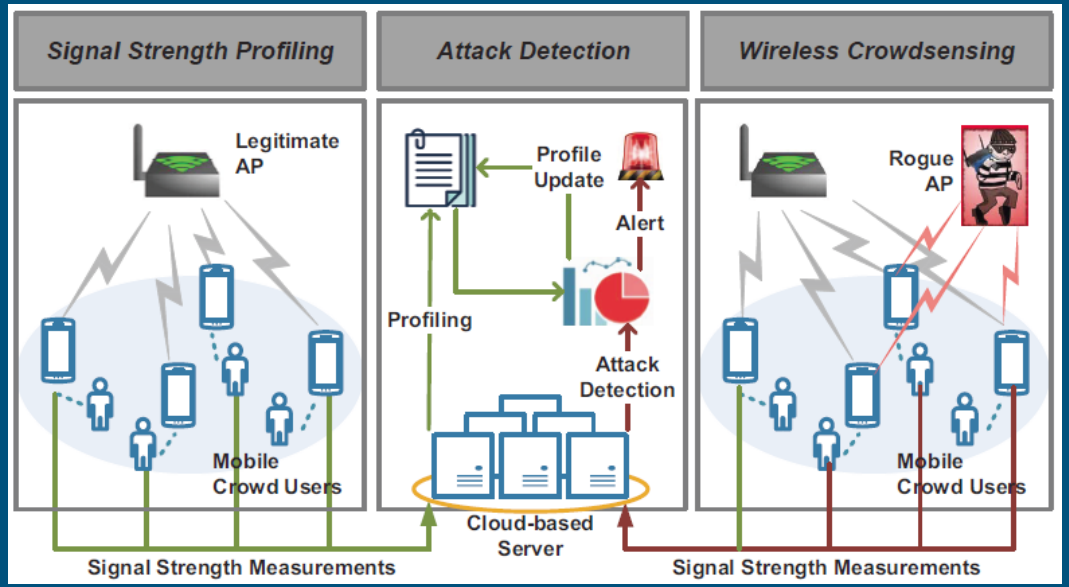
- Limitations of existing rogue AP detection approaches:
  - Time-based approaches assume rogue APs relay their traffic via legitimate APs.
  - Fingerprinting-based approaches require custom hardware for monitoring.

Can we design an approach that is:

1. **Effective to all the RAP threats (especially replacement attack);**
2. **Requiring non-specialized hardware.**

The CRAD approach -- Overview

❖ Crowd based Rogue AP Detection



Exploiting the RSS measurements (instead of time factors) sensed and reported by mobile devices of the crowd (instead of specific hardware) for rogue AP detection.

The CRAD approach -- Profiling phase

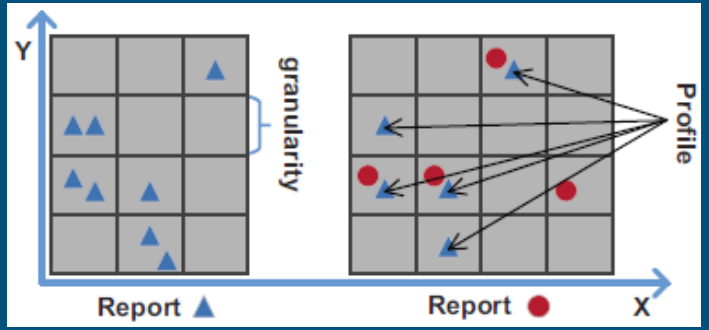
❖ Profiling the legitimate AP with RSS measurements of the crowd devices

➢ Using a grid-based profiling method

✓ Recording every location is not practical;

✓ RSS within certain distance are similar.

➢ Calculating the granularity based on spatial relations of the collected RSS measurements.



The CRAD approach -- Detection phase

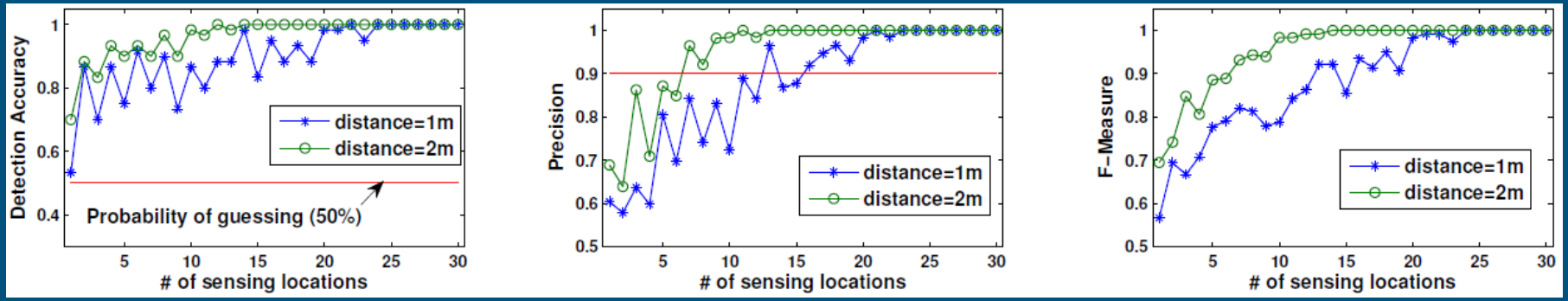
- Identifying rogue AP by matching crowd observed RSS with the profile
  - Comparing new coming RSS samples to their grid neighbors in the profile
    - ✓ Temporal Correlation: RSS measured at one location are similar to each other;
    - ✓ Spatial Correlation: Locations near each other would observe similar RSS.
  - Majority voting for rogue detection
    - ✓ Positive, if more than half samples are significantly different (difference bigger than a threshold) from the profile records.
    - ✓ Negative, otherwise.

Evaluation -- Prototype

- Evaluating the performance of CRAD based on a prototype
  - One legitimate AP, and two rogue APs (with a distance of 1m and 2m to the legitimate one) are launched.
  - An android application is developed to perform RSS measuring and recording.

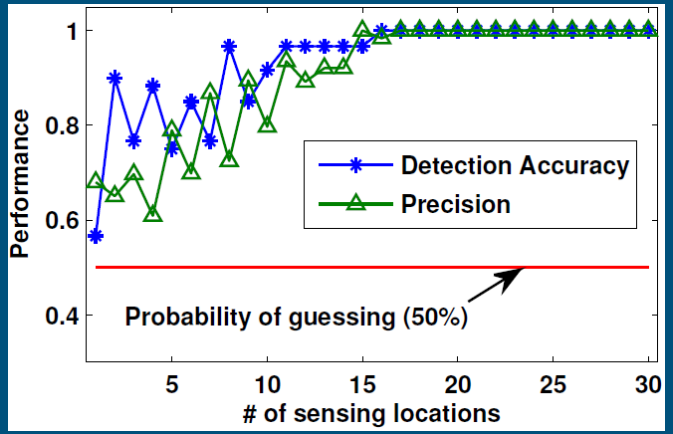
Evaluation -- Results 1/2

- Rogue AP detection accuracy, precision, and F-Measure (Replacement attack, distance =1m & 2m)



Evaluation -- Results 2/2

- Rogue AP detection accuracy, precision (Coexistence attack, distance = 2m)



Thank you !

Email: zhoutongqing@nudt.edu.cn