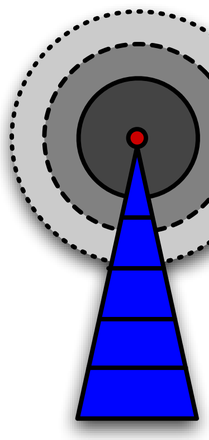
Fine-Grained Secure Localization for 802.11 Networks

Patrick Traynor, Patrick McDaniel, Thomas La Porta, Farooq Anjum

Location-Based Access Control

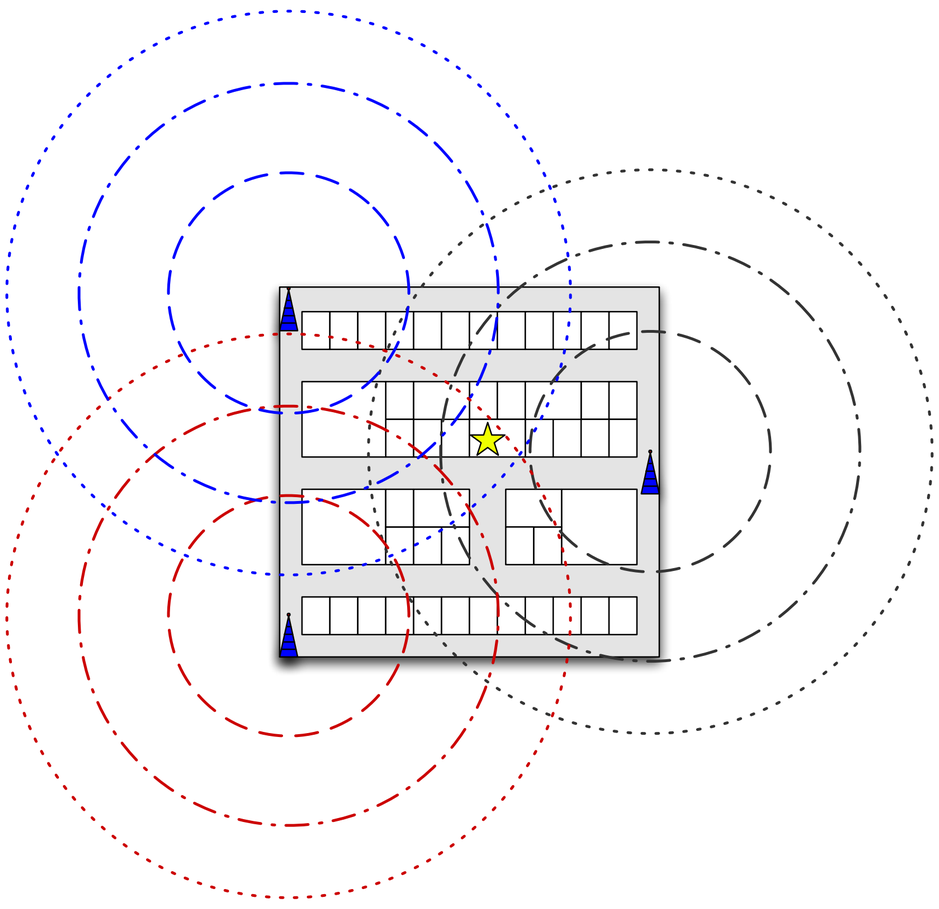
- The combination of inexpensive hardware and wireless networking have helped to erode traditional network perimeters.
- Whereas it was once reasonable to assume that a user would always log in from the same physical point, such an assumption is no longer valid.
- Accordingly, it may no longer be sufficient for a user to simply identify themselves - they may also need to identify their location.



- Current methods, which are dependent upon signal strength measurements, are subject to location spoofing.
- Our scheme is based on a client reporting a series of received tokens. These tokens appear semantically meaningless, but help the network to determine the location of the client.
- To ensure that we find location with a high degree of accuracy, we perform localization at multiple scales.

Macro-Localization

- An *Access Point Controller* (APC) generates a series of pseudo-random tokens.
- Each connected *Access Point* (AP) receives a token and a set of parameters indicating the power with which each token should be transmitted.
- A client, signified here by the star, records the tokens it hears.
- At the end of the phase, the client tells the APC which tokens it has received.
- The APC compares these tokens against a list of tokens that should have been received at each location and then picks the corresponding general or macro location.

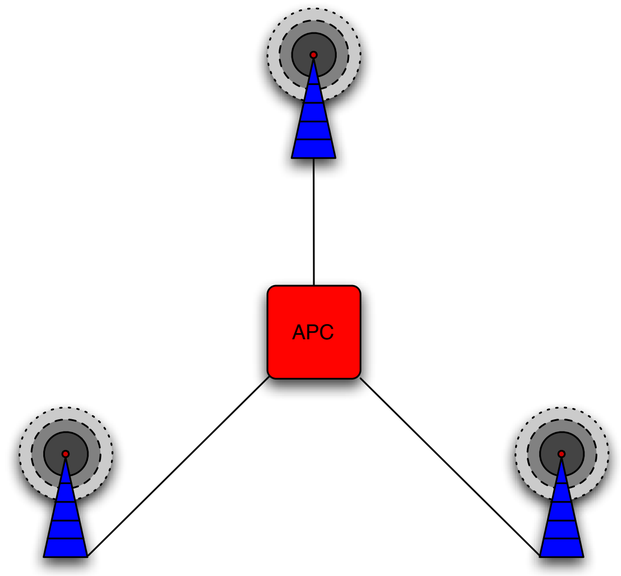


Pico-Localization

- Macro-Localization gives us a general area for the client's location. We may need to know the specific office.
- The APC relaunches the localization phase, but this time it asks for a little help from deployed hardware.
- Desktop computers throughout the office are equipped with USB 802.11 wireless cards. These inexpensive attachments (<$30 each) allow PCs to act as local APs.
- At a single low power, each PC (known as a "Pico-AP" broadcasts a new set of pseudo-random tokens generated by the APC.
- Upon receiving the second token report, the APC can determine a more exact location for the client.

Location Mapping Mode

- Developing maps of wireless coverage for an area is time consuming using traditional means.
- More importantly, wireless coverage is constantly changing, so static representations are not realisitic.
- It is therefore critical to be able to dynamically generate accurate representations of coverage.
- We have created a mapping mode - an automatic means of characterizing the coverage of each AP for a given environment.
- Mapping mode is similar to the standard operation of the localization tool.
- APs broadcast a series of tokens generated by the APC.
- The Pico-APs then report the tokens they hear back to the APC, which compares these tokens against the ones it sent out.
- Over time, the APC can develop statistical maps of regions, such that it can anticipate with a high probability the tokens a client should hear.



Performance Evaluation

msec	TokenGen	Transmit	Policy	Comm Setup
avg	1.098475	11.05223	0.041914	0.076046
stddev	0.181283	29.63134	0.257622	0.666688452
confidence	0.000359	0.058758	0.000511	0.001322018

- We perform a preliminary evaluation of system performance.
- The most expensive operation, by an order of magnitude, is transmission.
- Early results indicate that such a system can efficiently be implemented and run in an enterprise setting.

Future Work

- This system is being deployed across the PSU CSE building.
- Data will be gathered over a three month period and to create statistical coverage maps.
- A paper detailing this work and our experience with the system will be submitted to the USENIX Security Symposium.

Sponsored by: Telcordia Technologies