Telcordia

A Secure Low-cost WLAN Localization Scheme

Santosh Pandey (1), Farooq Anjum (2), Byungsuk Kim (2) and Prathima Agrawal (1)

(1) Auburn University, USA

(2) Telcordia Technologies, USA

Motivation

- Location based services are expected to be the next “killer” application. Examples of applications using location information are:
  - Emergency service such as E911.
  - Location based access control.
  - Implementation of company policies.
  - Improve the performance of mesh networks or 802.11 MAC using location information of network clients.

Motivation

- An adversary (attacker or intruder) may try to deceive the localization system by using special hardware, power variation etc.
- A localization scheme that will be resilient against such attacks to provide correct location information of the end user is hence needed. Such schemes are called *secure localization schemes*.
- The objective of this work is to introduce a low-cost secure localization scheme for WLAN and compare its performance with existing signal strength (SS) based scheme. We assume a simple threat model; a single attacker with no advance hardware.

Scheme Description

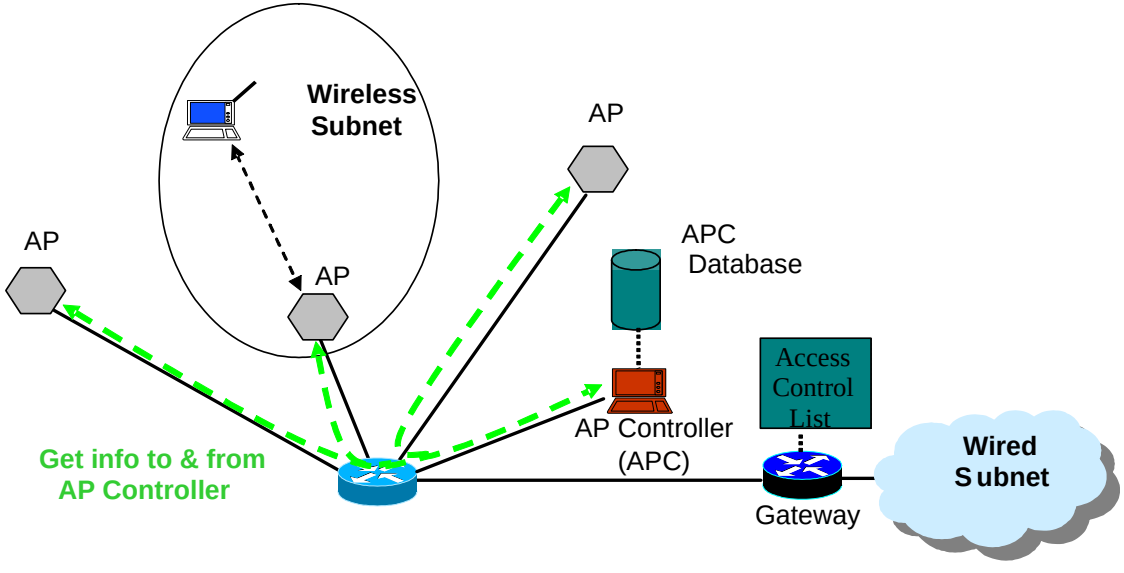

FIGURE 1: Architecture of proposed localization system

Scheme Description

- Messages Nij are transmitted at different power levels by neighboring APs.
  - $Nij = E_k\{N_o|AP_i|P_j\}$
    Nij: Message corresponding to the j^{th} power level (P_j) from the i^{th} AP (AP_i),
    N_o: Nonce

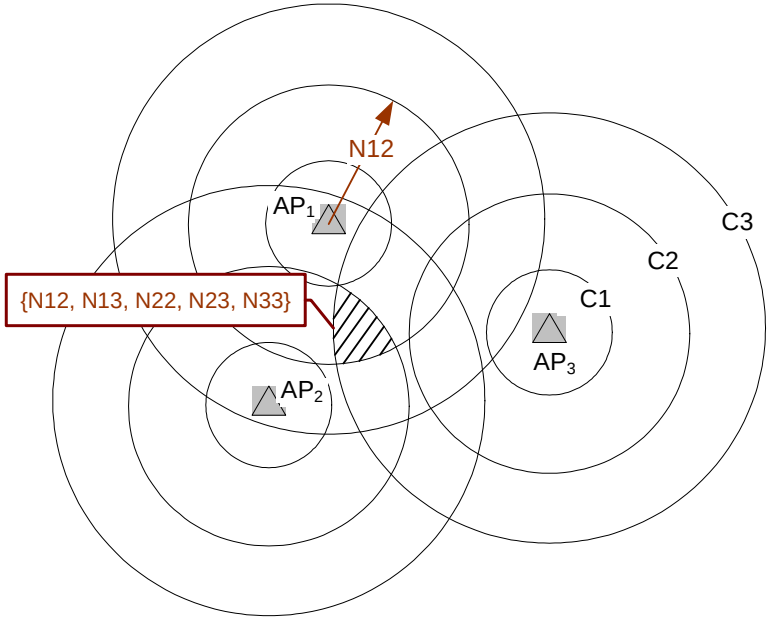

FIGURE 2: Three access points with 3 transmission power levels

Preliminary measurements

- Different power levels $\Rightarrow$ Sufficiently different transmission ranges.
- The transmission range is almost circular in open spaces and irregularly shaped in closed spaces.
- ‘k out of N’ scheme: For different values of k and N, k=60% of N gave a sharp cut off.
- Boundary varied over discrete time periods throughout the day and not instantaneously.

Secure Location Algorithm

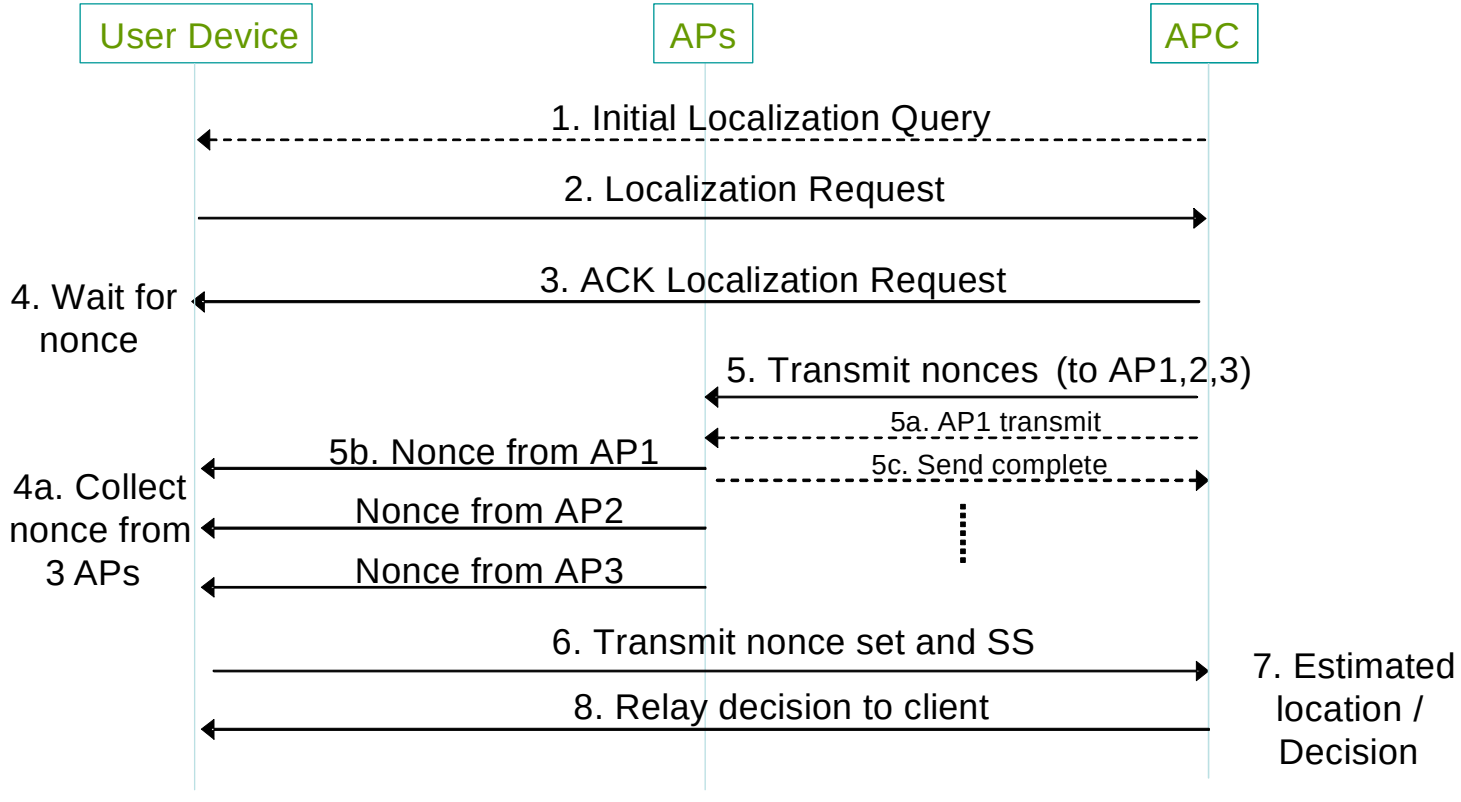

FIGURE 3: Timeline

Secure Location Algorithm

- Let N_t = the number of attempts,

  N_c = the maximum number of trials to locate a user and

  $N(L_p)$ = the number of successive values of L_p.

  - If $N_t \leq N_c$ and $N(L_p) < \delta$ then $N_t = N_t + 1$
  - else if $N_t \leq N_c$ and $N(L_p) \geq \delta$ then the user location is L_p
  - else reinitiate query.

Implementation

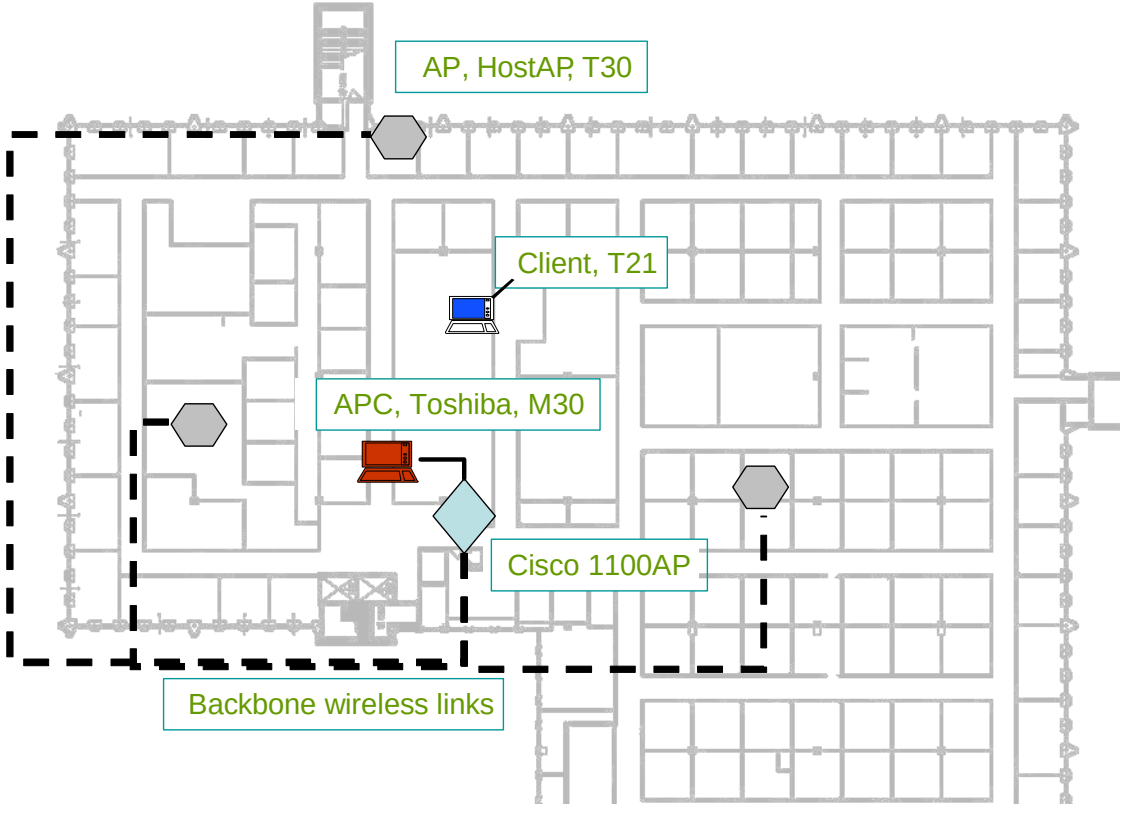

FIGURE 4: Testbed setup

Implementation

- The testbed was implemented using `Python` in an area of about 150 x 120 ft. (18,000 sq. ft.).
- The user device in testbed was a Linux laptop with Prism II wireless card.
- HostAP drivers were employed to convert Linux based laptops into APs.
- Wireless links were used instead of the backbone wired links between APC and APs.

Implementation

- The APC is also a Linux based laptop and can control several parameters such as:
  - The number of APs to involve in localization.
  - The number of transmission power levels for each AP.
  - The number (N) of sub-messages to be transmitted.
  - The power level at which each sub-message is to be transmitted. Different APs can transmit at completely different power levels.
  - Other parameters such as k, N_c, δ which are decided based on the policies at the APC.

Performance Analysis

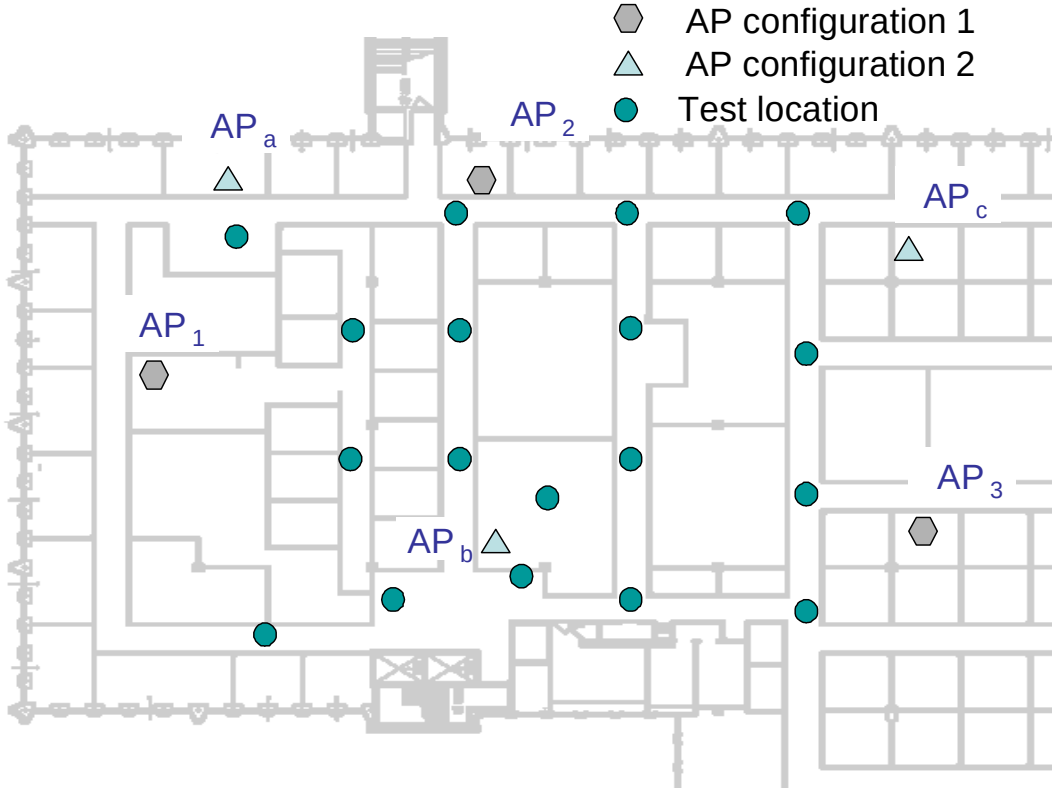

FIGURE 5: Test locations and AP configurations

Performance Analysis

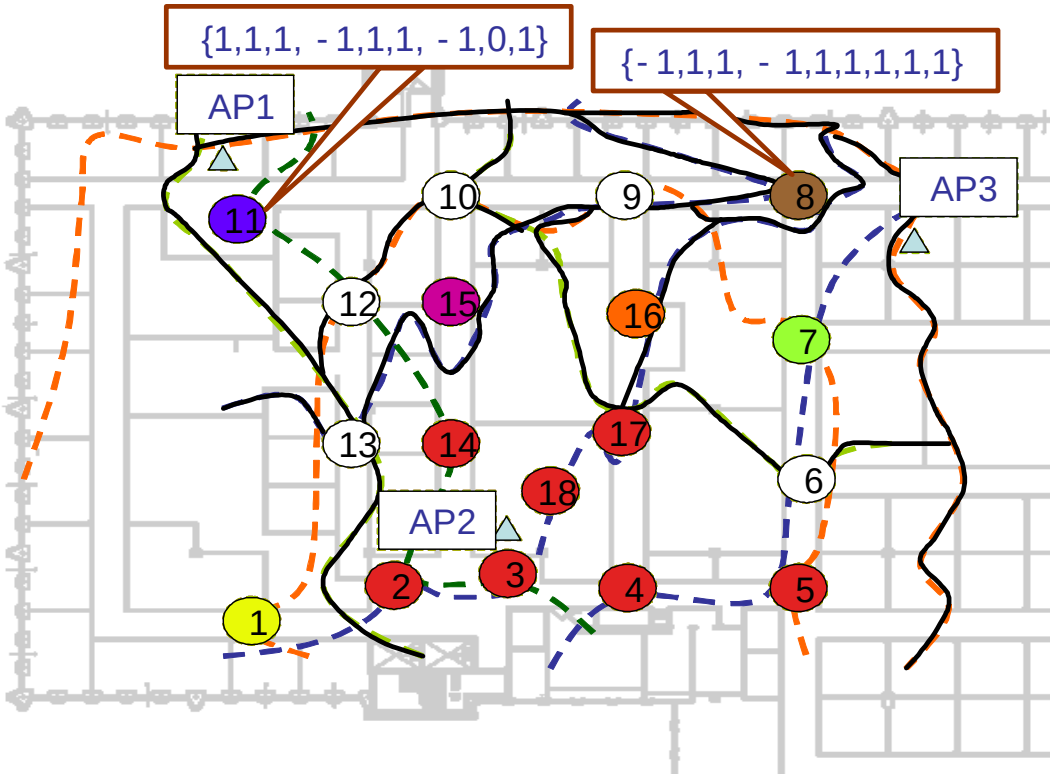

FIGURE 6: Sub-regions for AP configuration 1

Performance Analysis

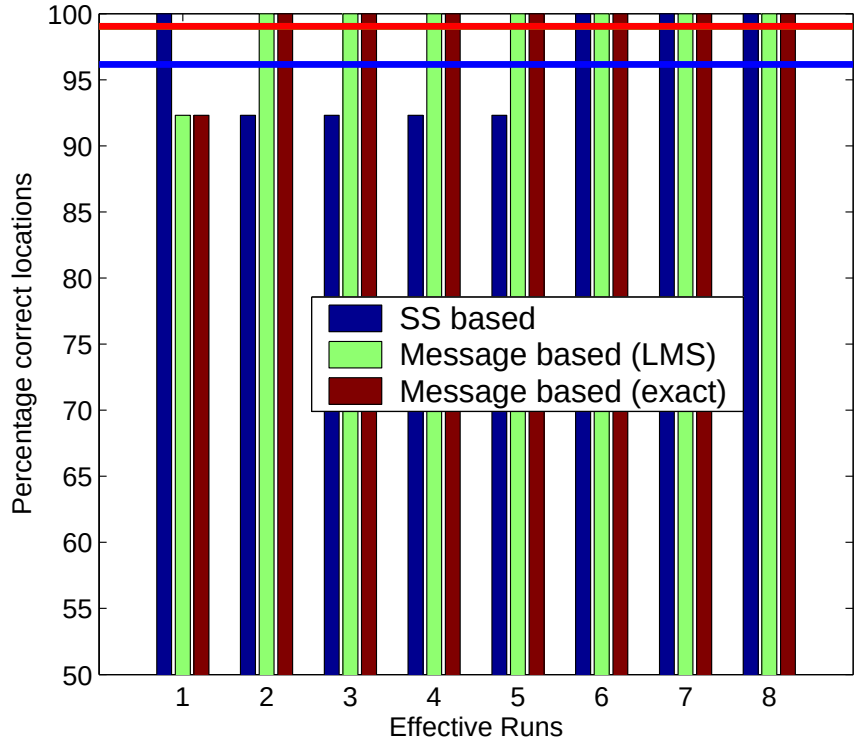

FIGURE 7: Percentage correct location for SS, message (LMS) and message (exact) with N_c=3, δ=2 (AP configuration 1)

Performance Analysis

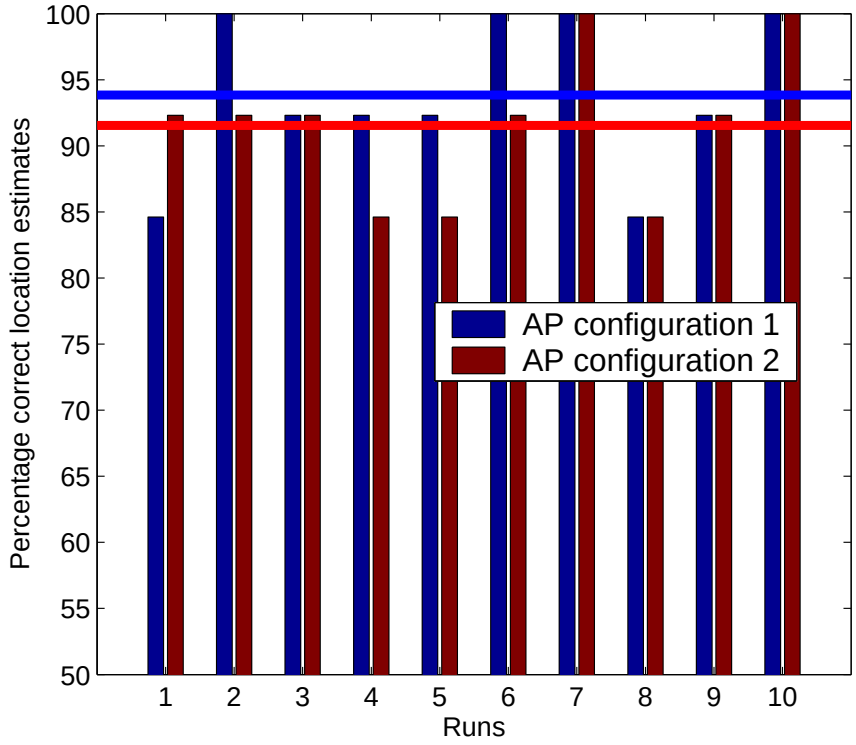

FIGURE 8: Percentage correct estimates for the test setup with AP configuration 1 and 2 for the exact message based scheme

Performance Analysis

- The accuracy is affected by AP placement.
- The value of δ and N_c decide the trade-off between security and performance of our scheme.
- A single localization query could be completed in about 1.5 secs.
- The throughput at AP dropped marginally from 4.8 Mbps to 4.7 Mbps due to localization overhead.

Security Features

- Unlike the SS based scheme, the attacker cannot build a lookup table in this case. The APC chooses the set of power level and corresponding unique set of messages for each AP for each localization query.
- The APs transmit messages using spoofed MAC addresses and hence it is difficult for the attacker to identify the message source.
- Further, even with the lookup table, the probability of dropping appropriate messages for location spoofing was found to be low, especially given the fact that all these messages are encrypted.

Conclusion

- The proposed scheme has several attractive security properties and performs better than existing SS based localization schemes.
- Future work:
  - Combine with SS scheme.
  - AP placements and “message map” generation.
  - Avoid unnecessary handoffs.
  - Distributed APC.