Fault Tolerant Positioning using WLAN Signal Strength Fingerprints

C. Laoudias, M. P. Michaelides and C. G. Panayiotou

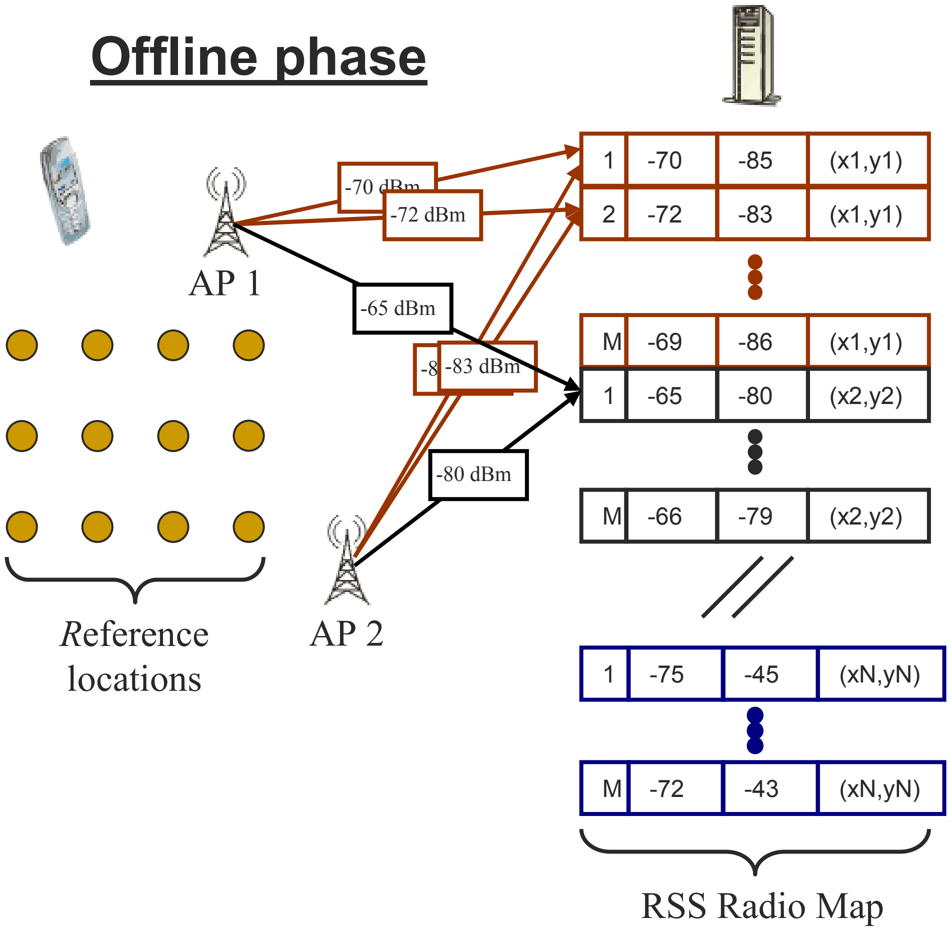
KIOS Research Center for Intelligent Systems and Networks
Department of Electrical & Computer Engineering
University of Cyprus

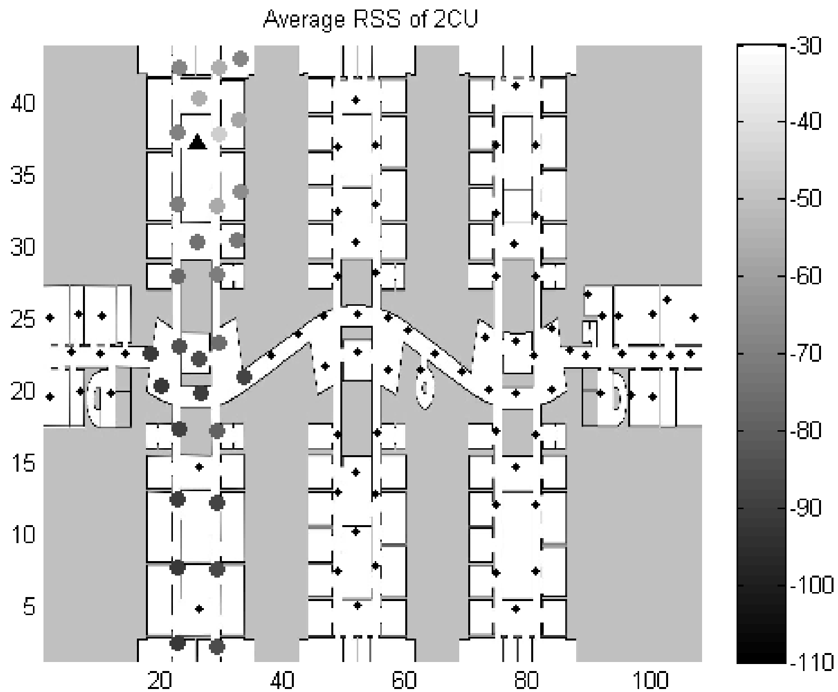
International Conference on Indoor Positioning & Indoor Navigation, 15 September 2010

Outline

- Fault Models
- Nearest Neighbor method
- Performance Evaluation
  - Measurement Setup
  - Experimental Results
- Conclusions

Region of Coverage (RoC)





RoC: Subset of reference locations where a specific AP is detected in the offline phase

Fault Tolerance

- The focus of positioning methods so far has been on improving accuracy
- In real world, WLAN APs can fail or exhibit erroneous behaviour, thus compromising performance
  - APs may be unavailable during positioning due to unpredicted failures, e.g. power outages
  - Positioning methods are susceptible to attacks that corrupt the expected RSS values
- We treat failures and attacks in a unified framework, because they both inject faults during positioning
- Assume that the reference data are not corrupted and study RSS attacks and failures in the online phase

AP Failure model

- Effect
  - Several APs used in the offline phase are not available during positioning
- Feasibility
  - Unpredicted AP failures, e.g. power outages, WLAN system maintenance, AP firmware upgrades
  - Adversary cuts off the power supply of an AP or uses specialized equipment to jam the communication channel
- Simulation
  - Remove the RSS values of the faulty APs in the original test fingerprints

False Negative model

- Effect
  - The faulty AP is no longer detected in some locations inside its original RoC
- Feasibility
  - Block the propagation path, e.g. furniture or equipment, so that AP signal cannot be detected in locations where it was previously weak
- Simulation
  - Ignore valid RSS readings for a set of APs in a number of test fingerprints
  - The AP Failure model is an extreme case of this model

False Positive model

- Effect
  - The faulty AP is detected during positioning in locations outside its original RoC
- Feasibility
  - Remove obstructions, e.g. heavy objects or equipment, from the propagation path so that AP signal can travel further
  - Under attack, a rogue AP is deployed and programmed to replicate an existing AP
- Simulation
  - Inject random RSS values to the test data for a set of APs that would otherwise be undetected in those locations where the respective test fingerprints are collected

AP Relocation model

- Effect
  - The faulty AP is detected during positioning inside an area that is different than the expected one
- Feasibility
  - An AP is moved to a new location, e.g. for network operation reasons
  - The attacker physically relocates an AP or launches a joint attack i.e. impersonates an AP and at the same time eliminate the AP signals through jamming
- Simulation
  - Replace the RSS readings of the corrupted AP in the test data with the values of another randomly selected AP

RSS Attack models

Linear Attack model[1]

- Effect
  - RSS values of an AP are amplified or attenuated
- Feasibility
  - Increase the AP transmit power or place a material, e.g. glass, metal, foil, in front of the AP antenna
- Simulation
  - Perturb the original RSS values in the test data by a constant attenuation or amplification factor

Additive Gaussian Noise model[2]

- Effect
  - RSS values of an AP have higher noise variance
- Simulation
  - Perturb the original RSS values with additive Gaussian noise

Nearest Neighbor method

$$\hat{\ell}(s) = \arg\min_{\ell_i} D_i \qquad D_i = \sum_{j=1}^{n} \left(r_{ij} - s_j \right)^2$$

$$D_i^{median} = \operatorname*{med}_{j=1}^{n} \left(r_{ij} - s_j \right)^2$$

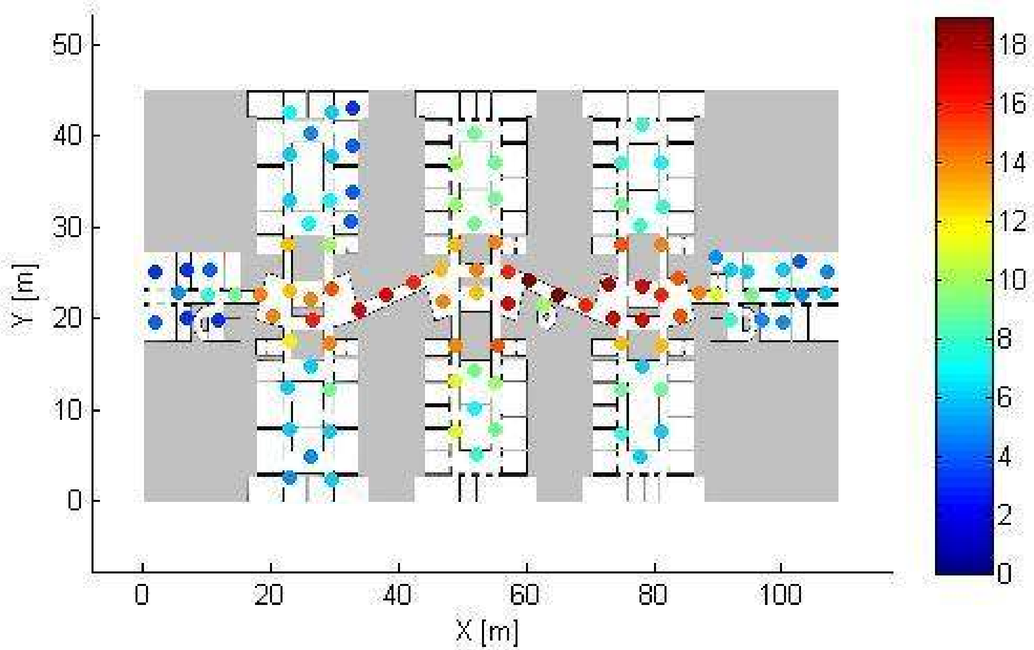
$$D_i^0 = \sum_{j \in R_i \cap S} d_{ij} + \sum_{j \in R_i \setminus S} d_{ij} + \sum_{j \in S \setminus R_i} d_{ij} \qquad d_{ij} = \left(r_{ij} - s_j \right)^2$$

$$D_i^1 = \sum_{j \in R_i \cap S} d_{ij} + \sum_{j \in S \setminus R_i} d_{ij}$$

$$D_i^2 = \sum_{j \in R_i \cap S} d_{ij} + \sum_{j \in R_i \setminus S} d_{ij}$$

Measurement Setup

- Area 110x45m on the 2nd floor @ VTT Research Center, Finland
- 107 reference locations with 2-3m spacing
- 31 WLAN APs (9.7 APs detected on average)



Training data

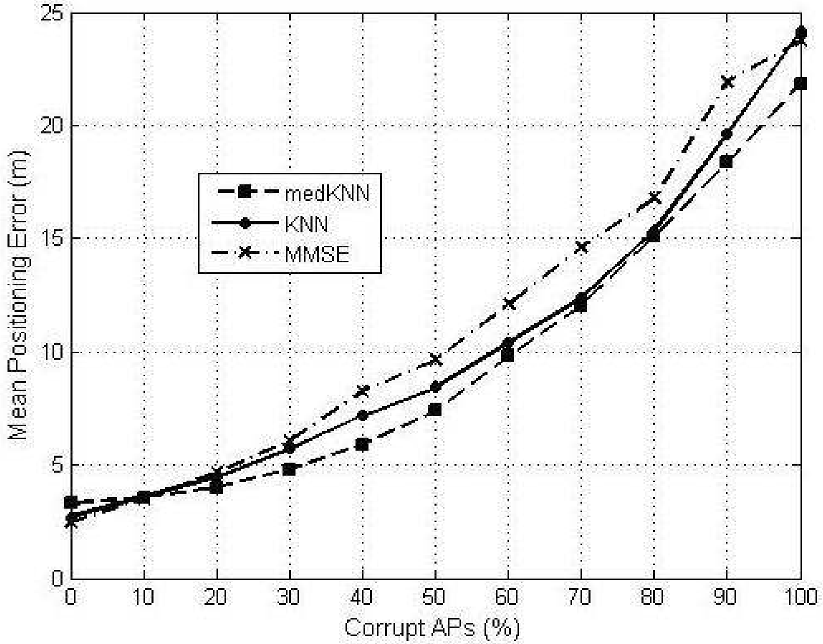
- 30 fingerprints per reference location (3210 fingerprints in total)

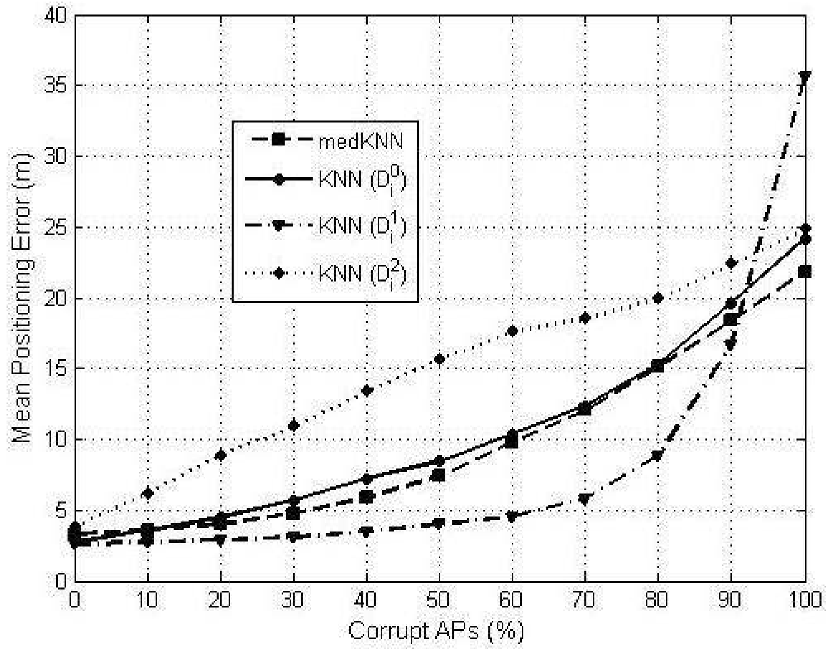
Testing data

- Route of 192 locations sampled 3 times (576 fingerprints in total)

Experimental Results

AP Failure model

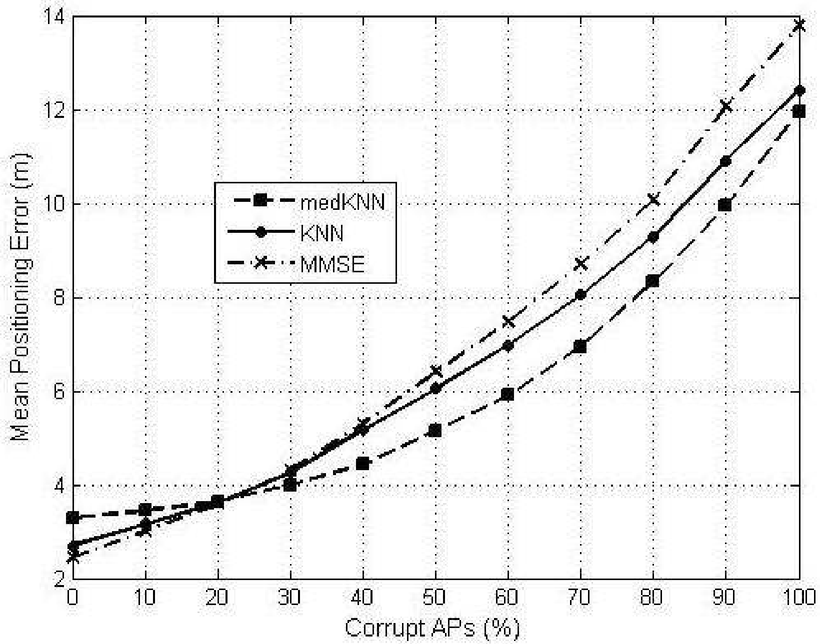


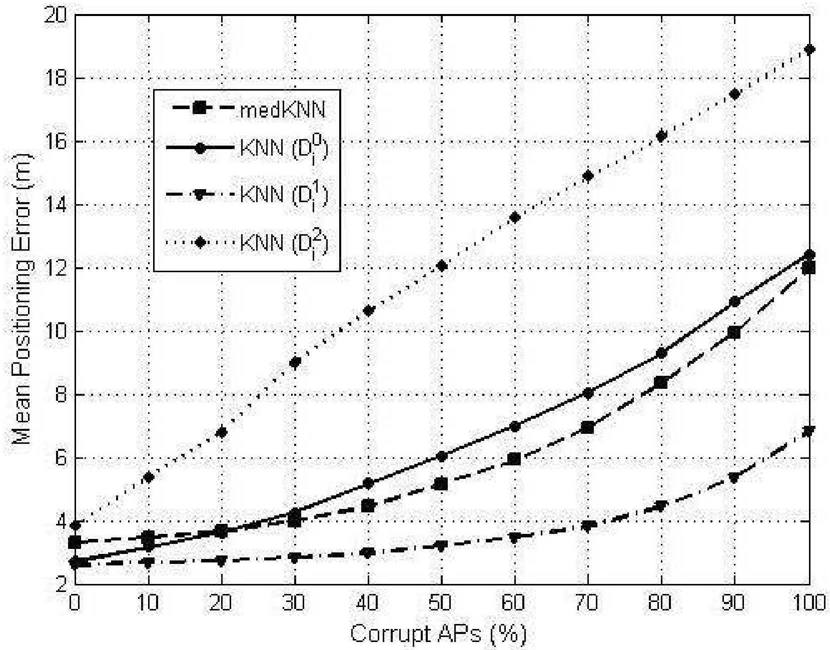


- The median-based KNN (medKNN) performs slightly better than the standard KNN method
- KNN (D^1) method can tolerate up to 65% failed APs, contrary to 35% for medKNN (Mean Error 5m)

Experimental Results

False Negative model

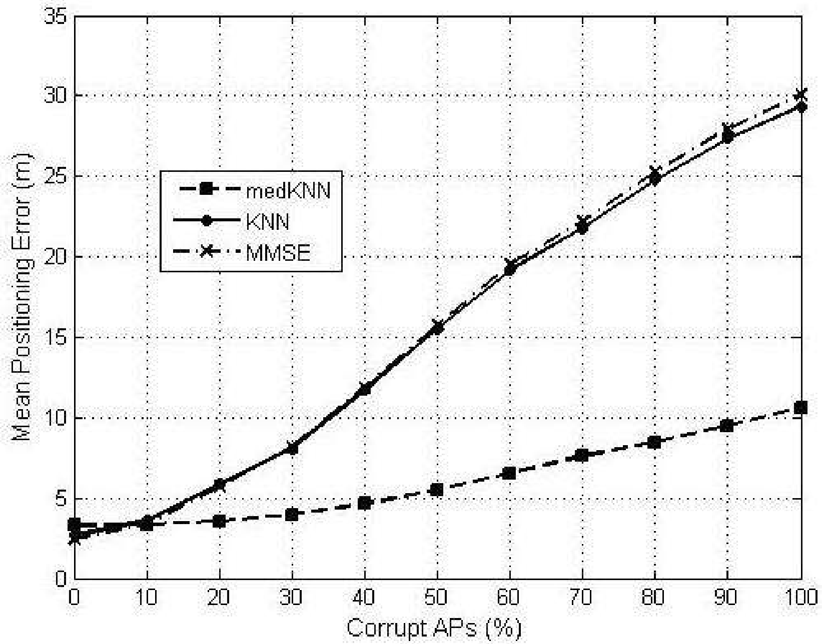


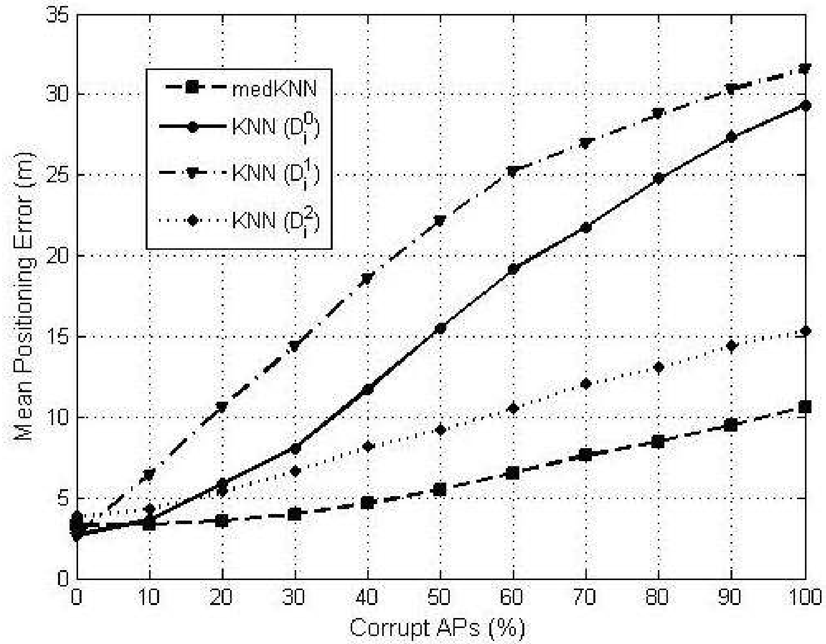


- medKNN performs better than the standard KNN method, followed by MMSE
- KNN (D^1) method can tolerate up to 85% faulty APs, contrary to 45% for medKNN (Mean Error 5m)

Experimental Results

False Positive model

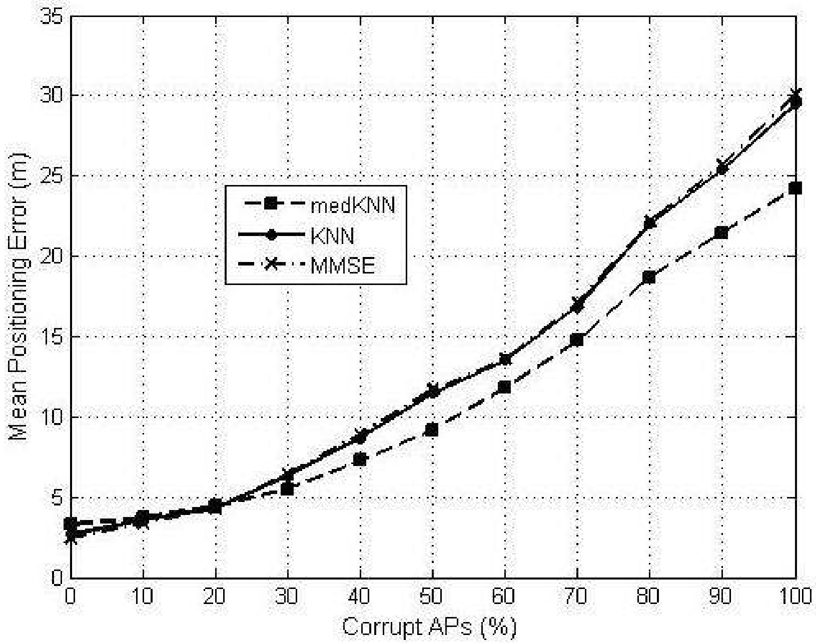


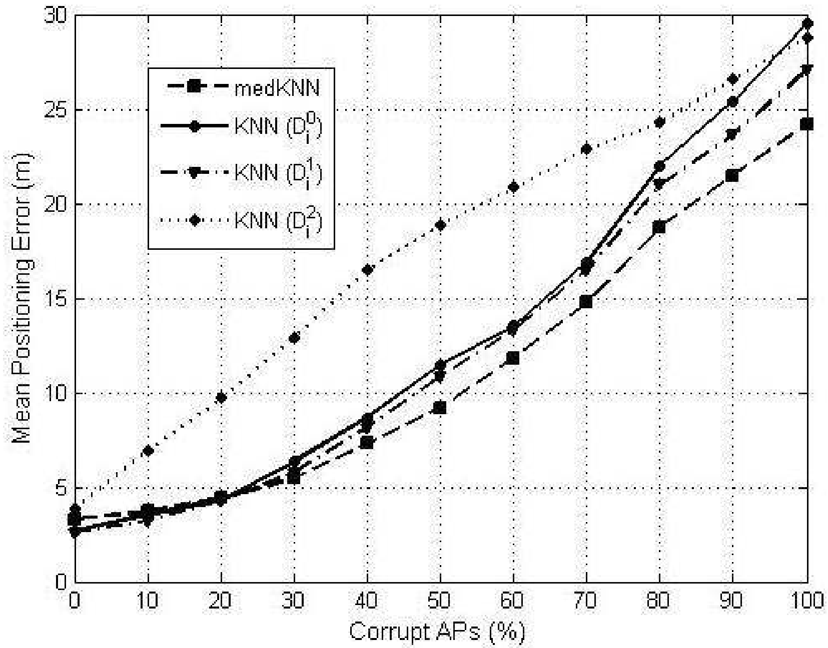


- medKNN has the best performance and can tolerate up to 45% faulty APs compared to 15% for KNN and MMSE
- Using metric D^2 greatly improves the performance of KNN method, but cannot achieve the fault tolerance of medKNN

Experimental Results

AP Relocation model

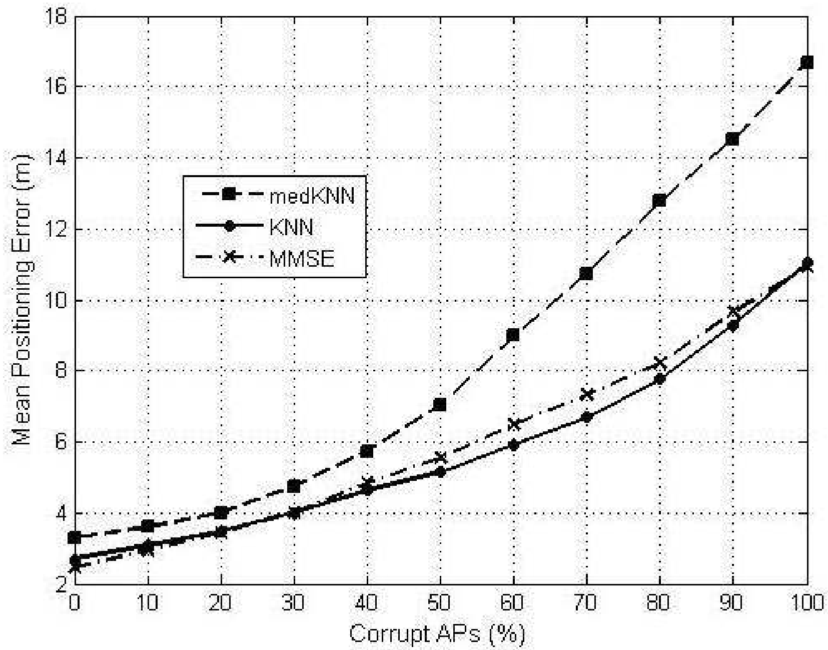


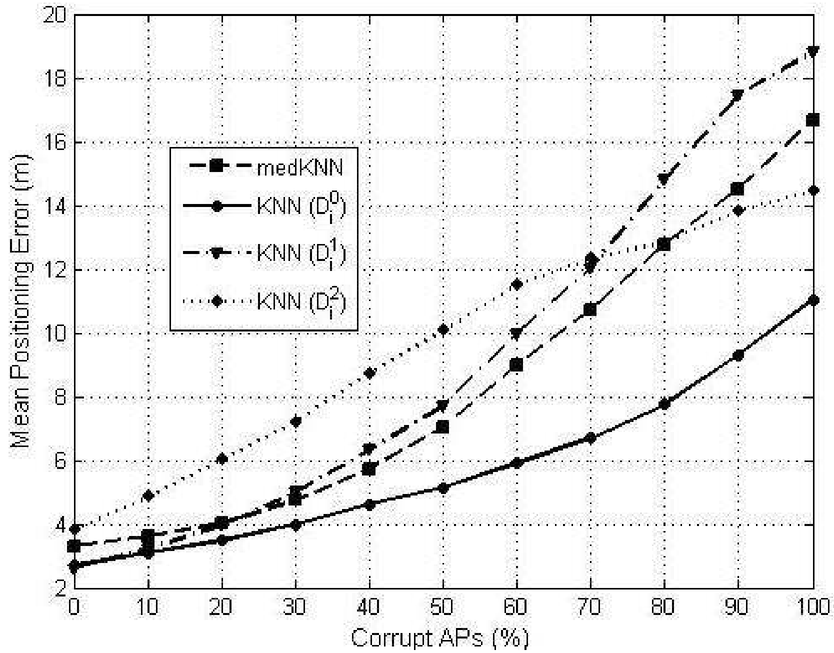


- All methods perform equally well for <30% corrupt APs, but medKNN is better for >30% corrupt APs
- Performance of KNN is only marginally improved with D^1, while D^2 causes severe degradation

Experimental Results

Linear Attack model (-20dBm)

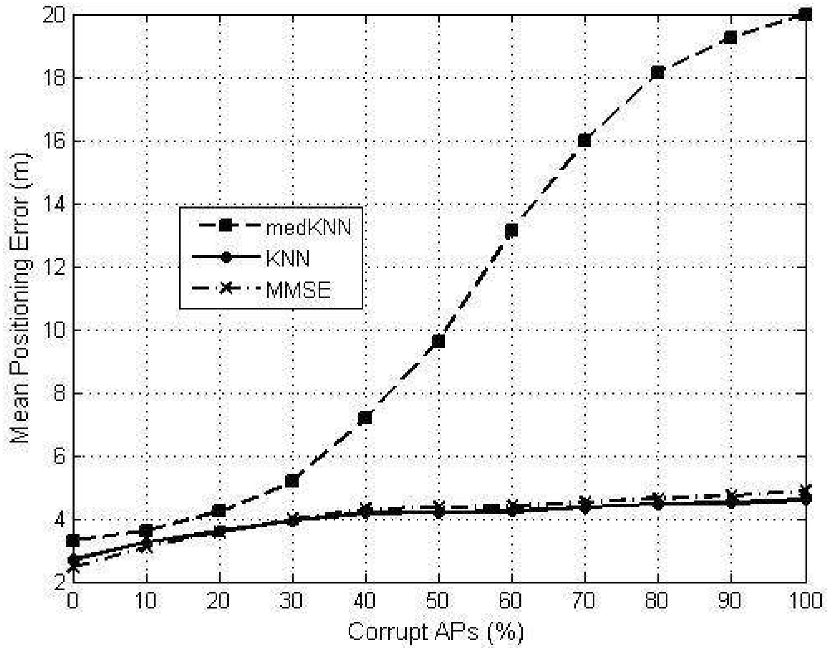


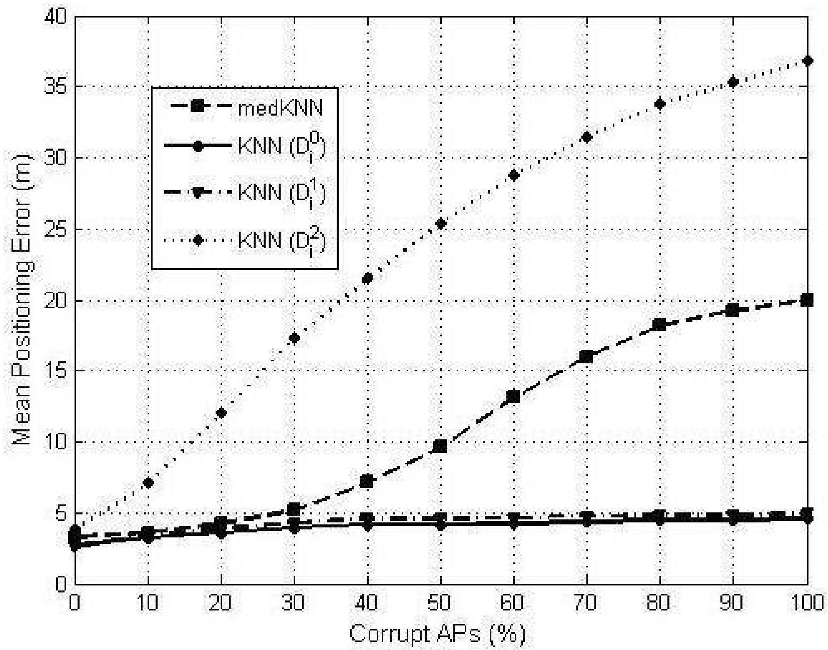


- KNN has the best performance, followed by MMSE. Mean Error increases rapidly for medKNN, especially if we have >50% faulty APs
- Metrics D^1 or D^2 do not improve fault tolerance over the standard KNN method (D^0)

Experimental Results

Linear Attack model (+20dBm)

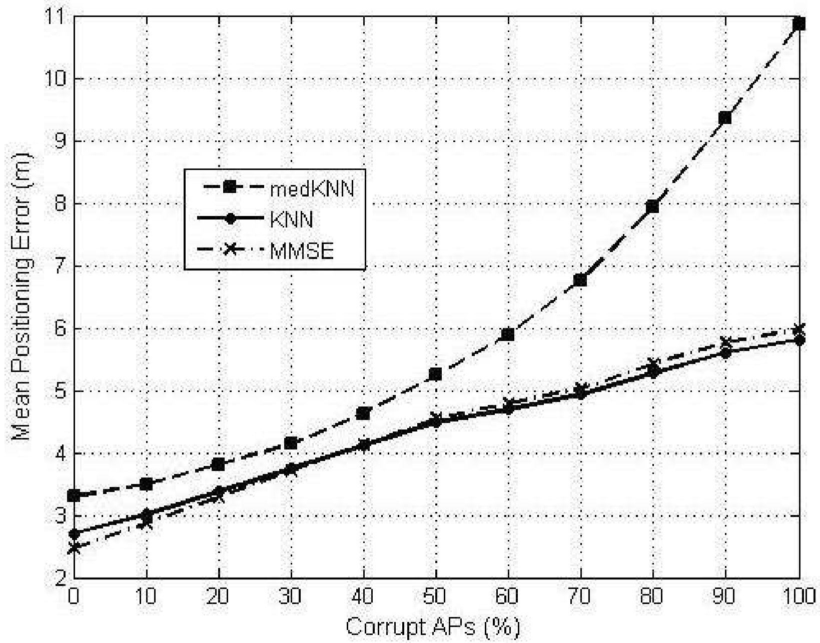


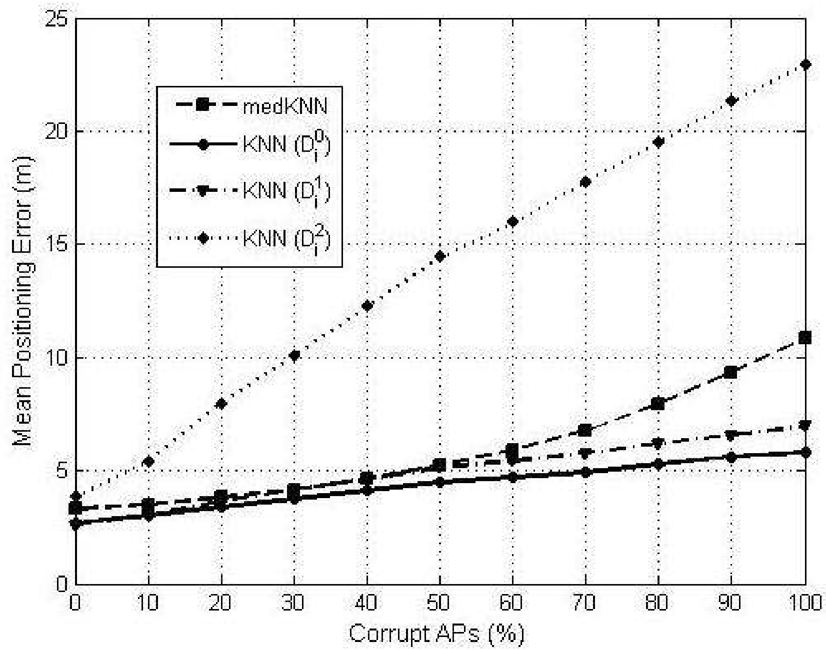


- For KNN and MMSE Mean Error is <5m even for 100% faulty APs, while medKNN degrades sharply
- Using D^2 is not a good option as the Mean Error explodes, while D^1 performance is similar to D^0

Experimental Results

Additive Gaussian Noise model (σ_n=20dBm)





- For Mean Error <5m KNN and MMSE methods can tolerate 70% faulty APs, compared to 45% for medKNN
- Standard KNN (D^0) exhibits higher fault tolerance than the variants using the distance metrics D^1 or D^2

Summary

	medKNN	KNN (D^0)	KNN (D^1)	KNN (D^2)
AP Failure	+	+	++	--
False Negative	+	+	++	--
False Positive	++	-	--	+
AP Relocation	+	-	-	--
Attenuation	-	++	-	--
Amplification	-	++	++	--
Gaussian Noise	-	++	+	--

Conclusions

- Fault tolerance of positioning methods is important, but has received little attention because the focus has been on improving accuracy
- We introduced several realistic fault models to capture the effect of fails or attacks and described how to simulate them using real test data
- We analyzed the distance metric in KNN method, discussed alternative metrics and studied the performance of the variants in the presence of faults
- Future work: Develop robust detection schemes to decide the type of the fault/attack in order to select the appropriate distance metric

References

[1] Y. Chen, K. Kleisouris, X. Li, and R. P. Martin, “The robustness of localization algorithms to signal strength attacks: a comparative study,” in *International Conference on Distributed Computing in Sensor Systems (DCOSS)*, 2006, pp. 546–563.

[2] A. Kushki, K. Plataniotis, and A. Venetsanopoulos, “Sensor selection for mitigation of RSS-based attacks in wireless local area network positioning,” in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2008, pp. 2065–2068.

[3] Z. Li, W. Trappe, Y. Zhang, and B. Nath, “Robust statistical methods for securing wireless localization in sensor networks,” in *International Symposium on Information Processing in Sensor Networks (IPSN)*, 2005, pp. 91–98.

Thank you

Contact

Christos Laoudias
KIOS Research Center for Intelligent Systems and Networks
Department of Electrical & Computer Engineering
University of Cyprus

Email: laoudias@ucy.ac.cy