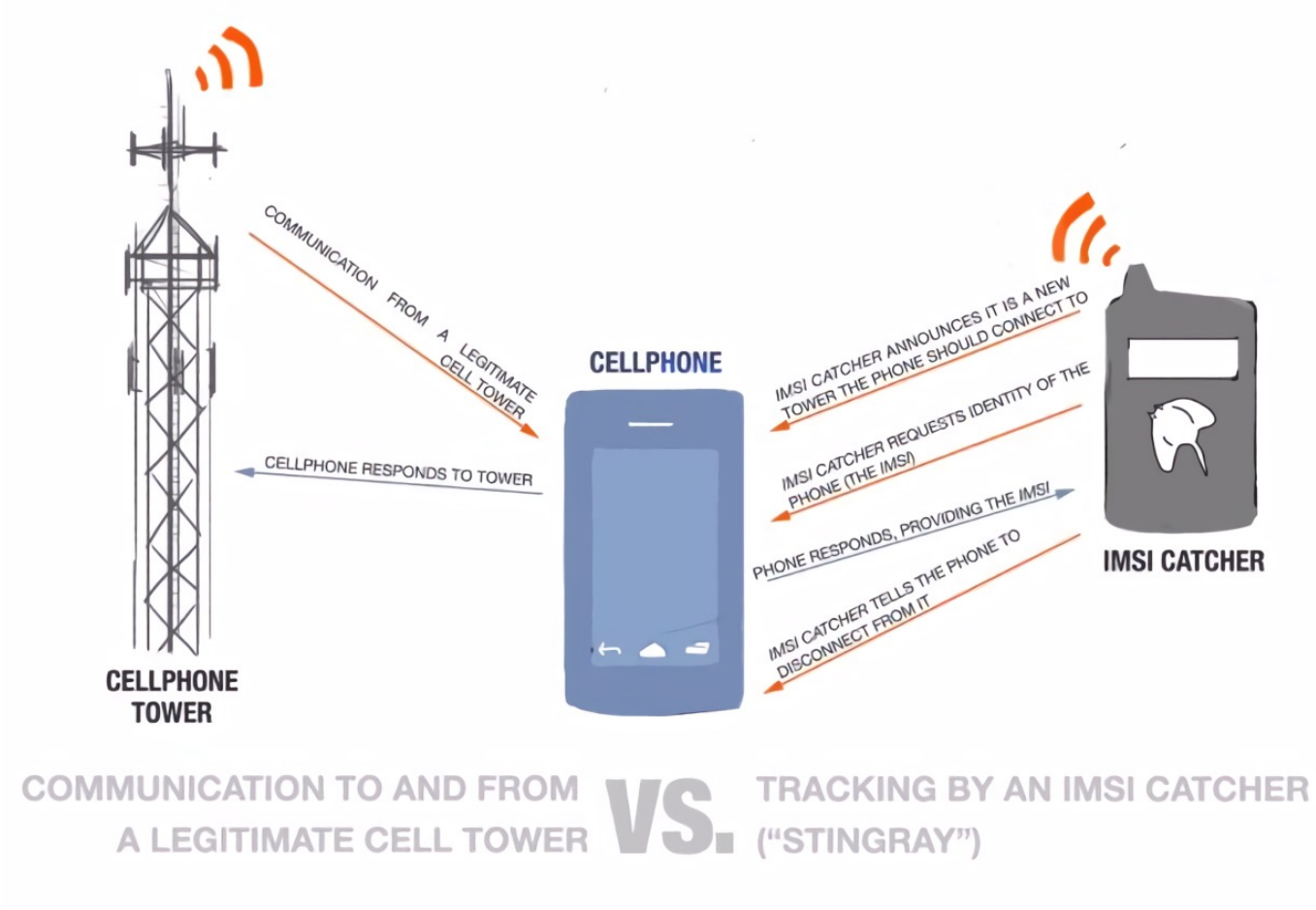
Detection of Malicious Handover in Mobile Networks Using Dead-reckoning

Tianchang Yang (tianchang.yang@psu.edu)

Yilu Dong (yiludong@psu.edu)

FBS attacks (IMSI Catcher)

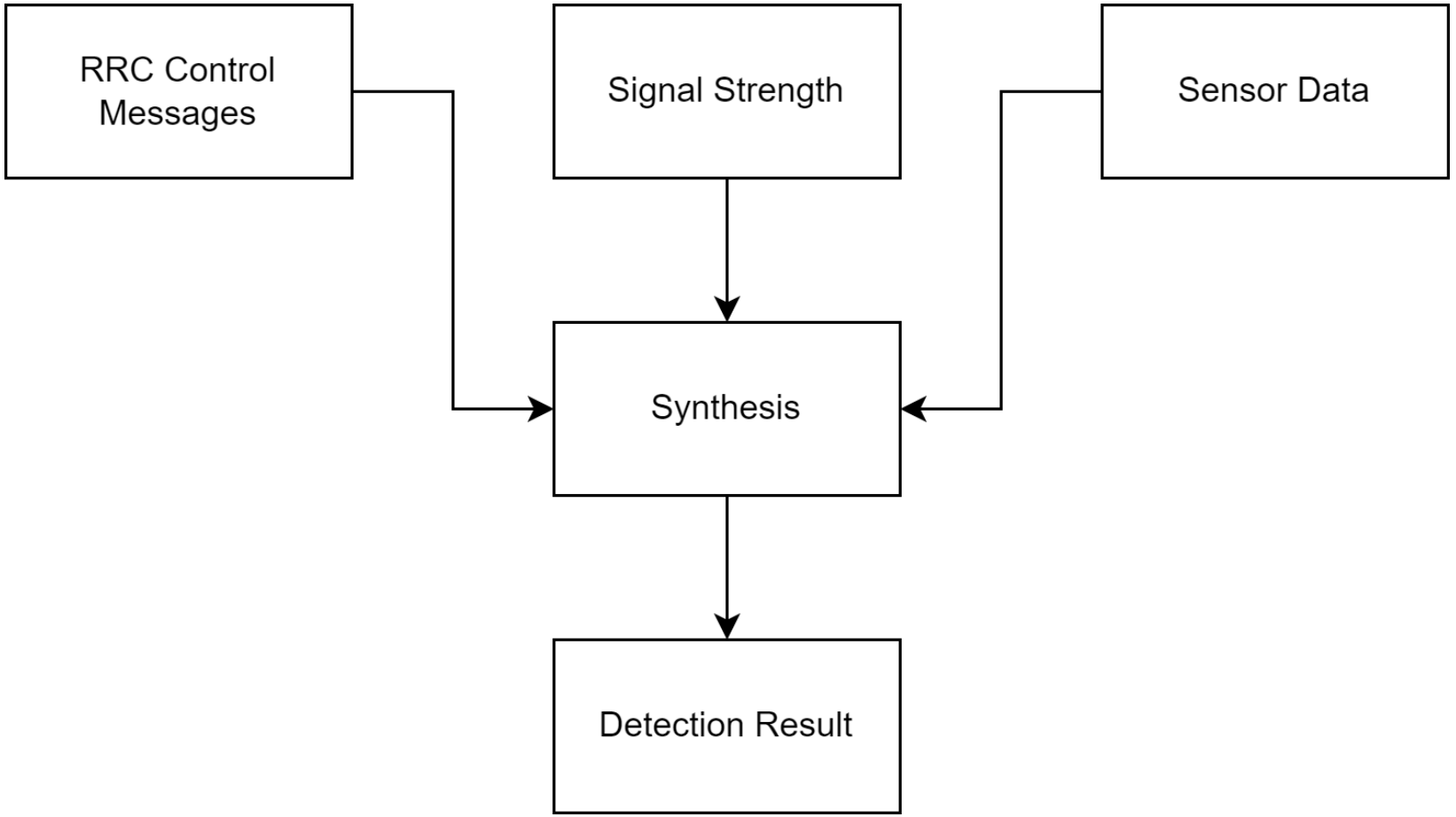
- Unique Identifier
- No or optional encryption
- Track user location



Identify Malicious Handover

- FBSs usually use high transmitting power to attract phones -> Signal Strength
- FBSs will behave differently than a normal base station (i.e., send slightly different RRC control messages) -> analyze RRC control messages
- Usually, the handover will occur when the user moved from one cell to another -> detect user movement
- All the above can be done on a phone

Idea Overview

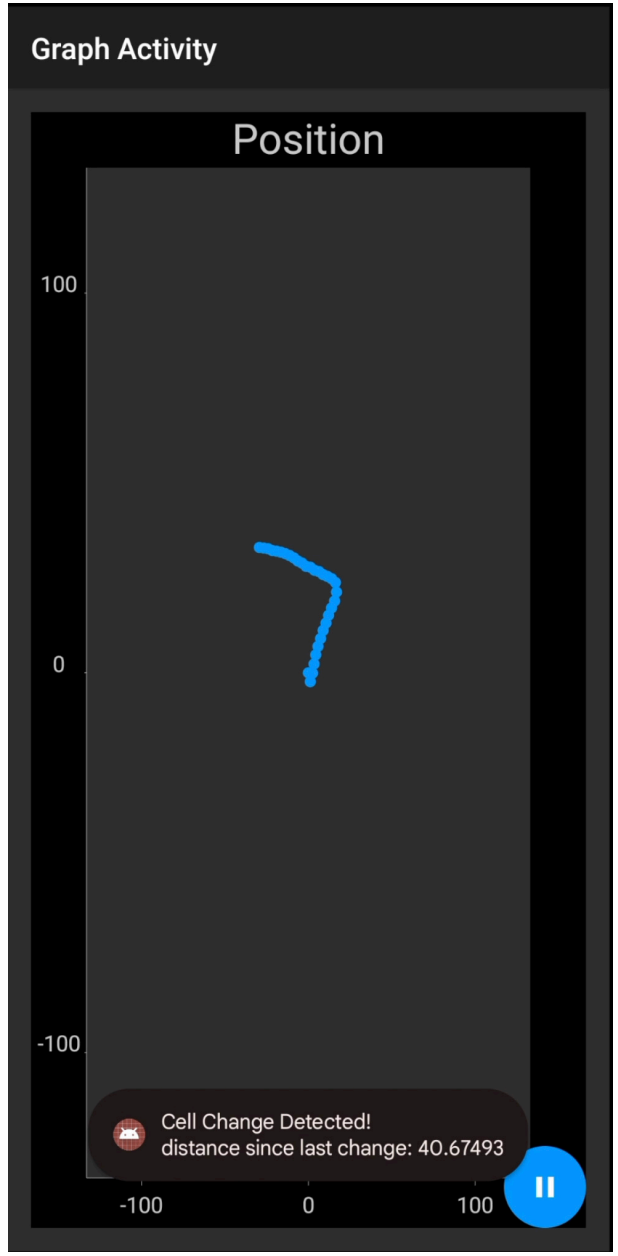


Why Dead-Reckoning?

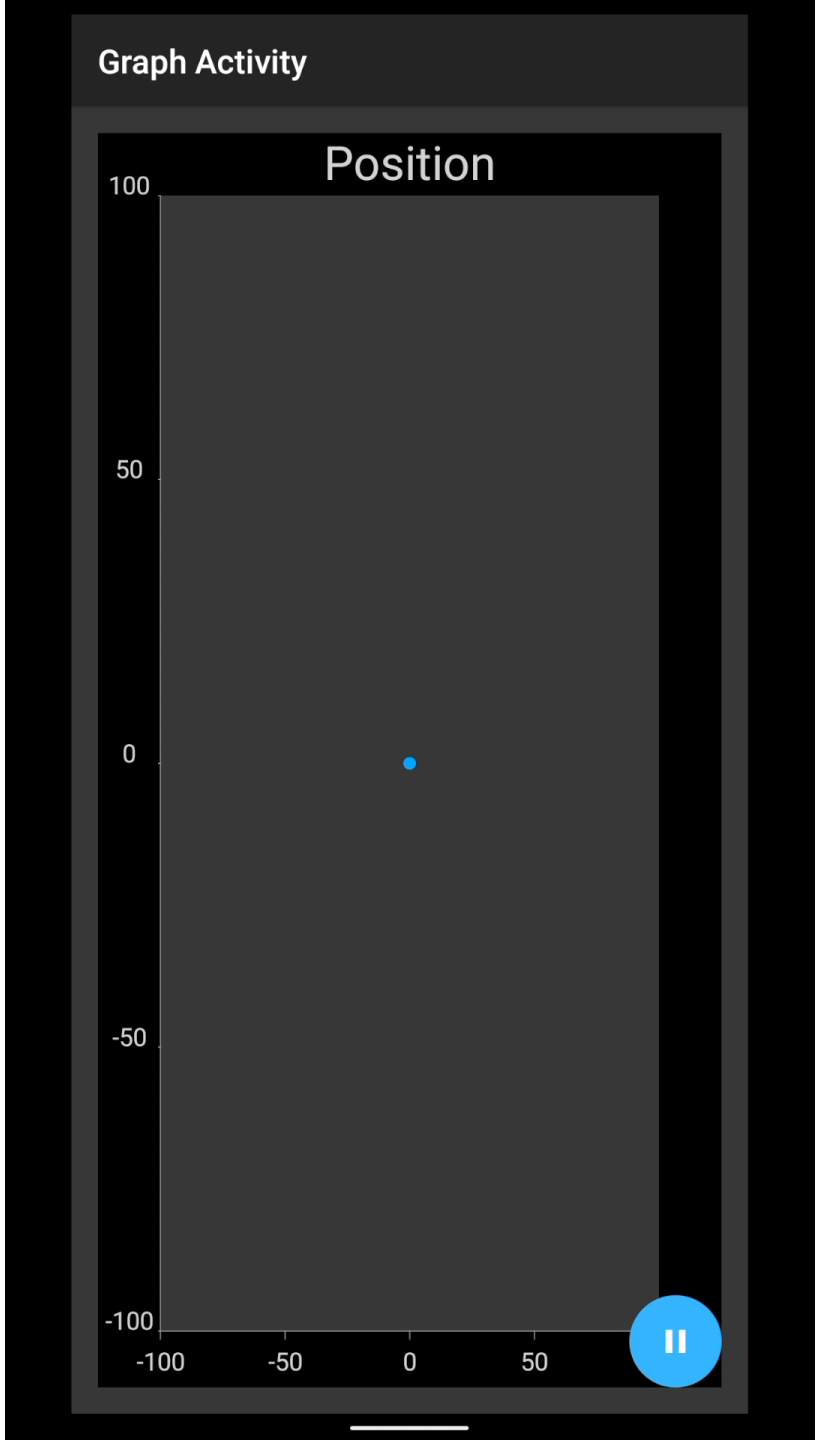
- Collecting GPS information requires special permission, which pose privacy concerns.
- Work for indoor locations
- We don’t require a very precise location estimate to achieve our goal.

Evaluation

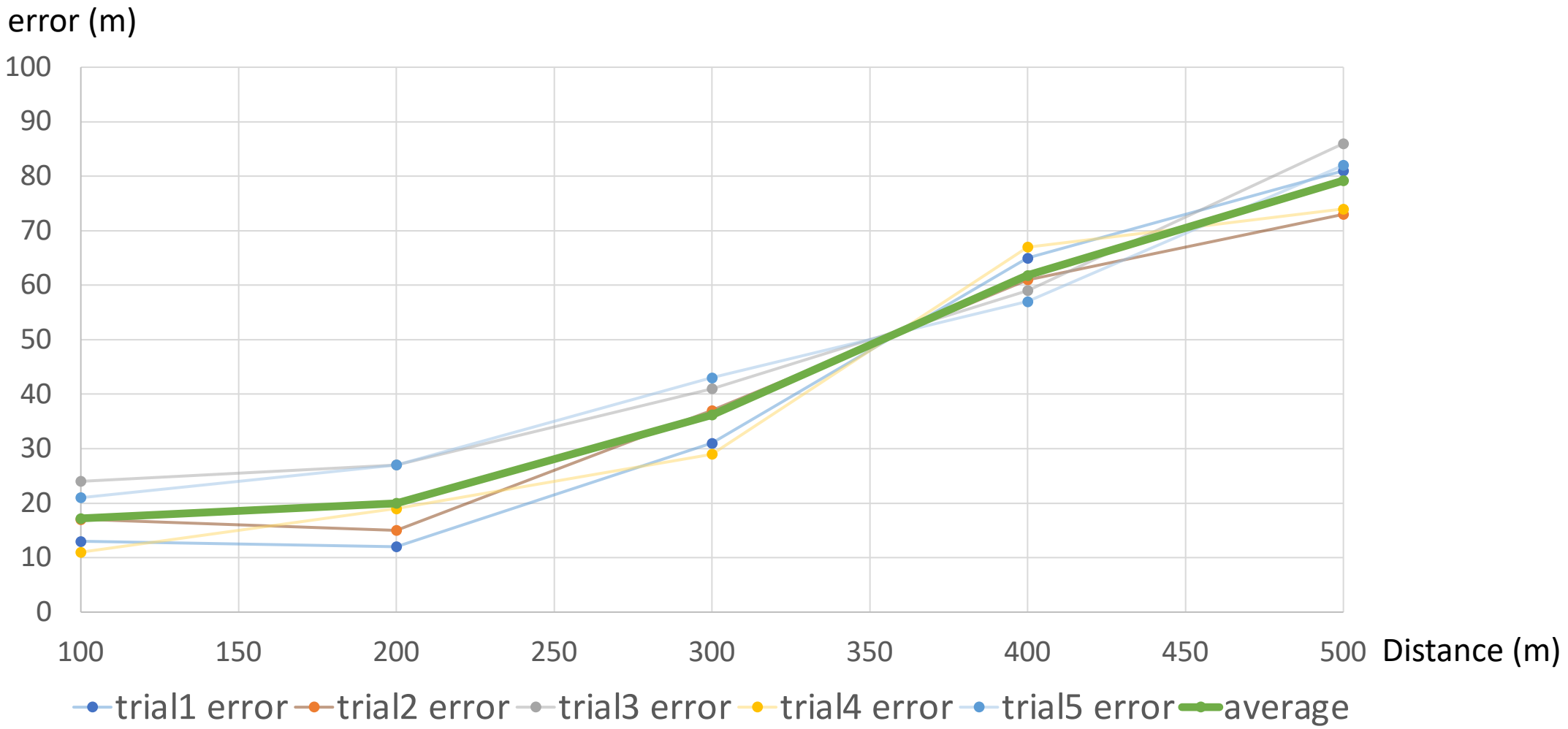
- Pixel 6 and Pixel 7 pro running Android 12
- Sensor data:
  - Accelerometer: steps
  - Gyroscope: heading information
  - Magnetometer: translate direction to global frame
- Cell information



Demo



Evaluation

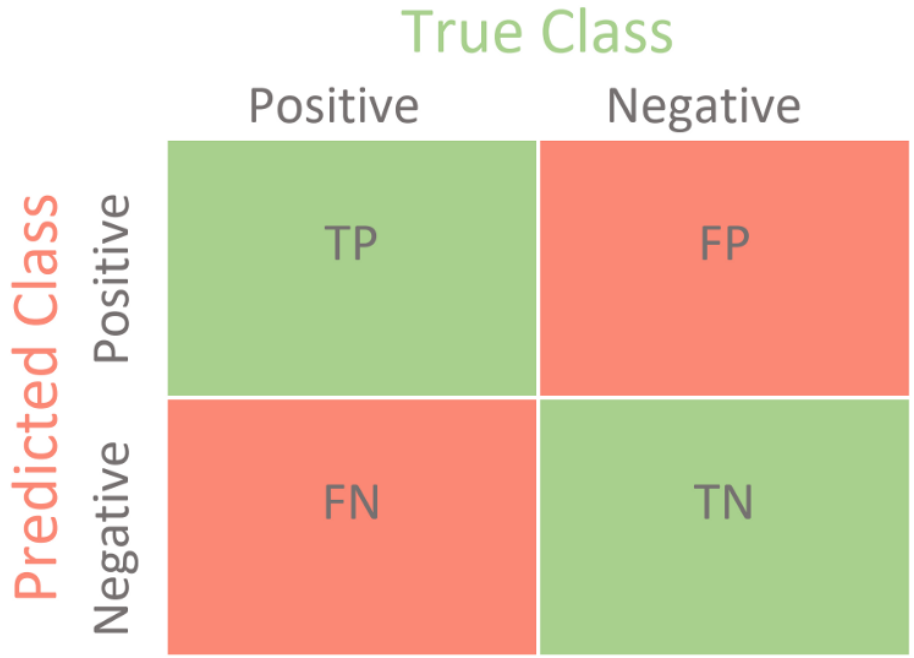

error (m)
100
90
80
70
60
50
40
30
20
10
0
100
150
200
250
300
350
400
450
500
Distance (m)
trial1 error
trial2 error
trial3 error
trial4 error
trial5 error
average

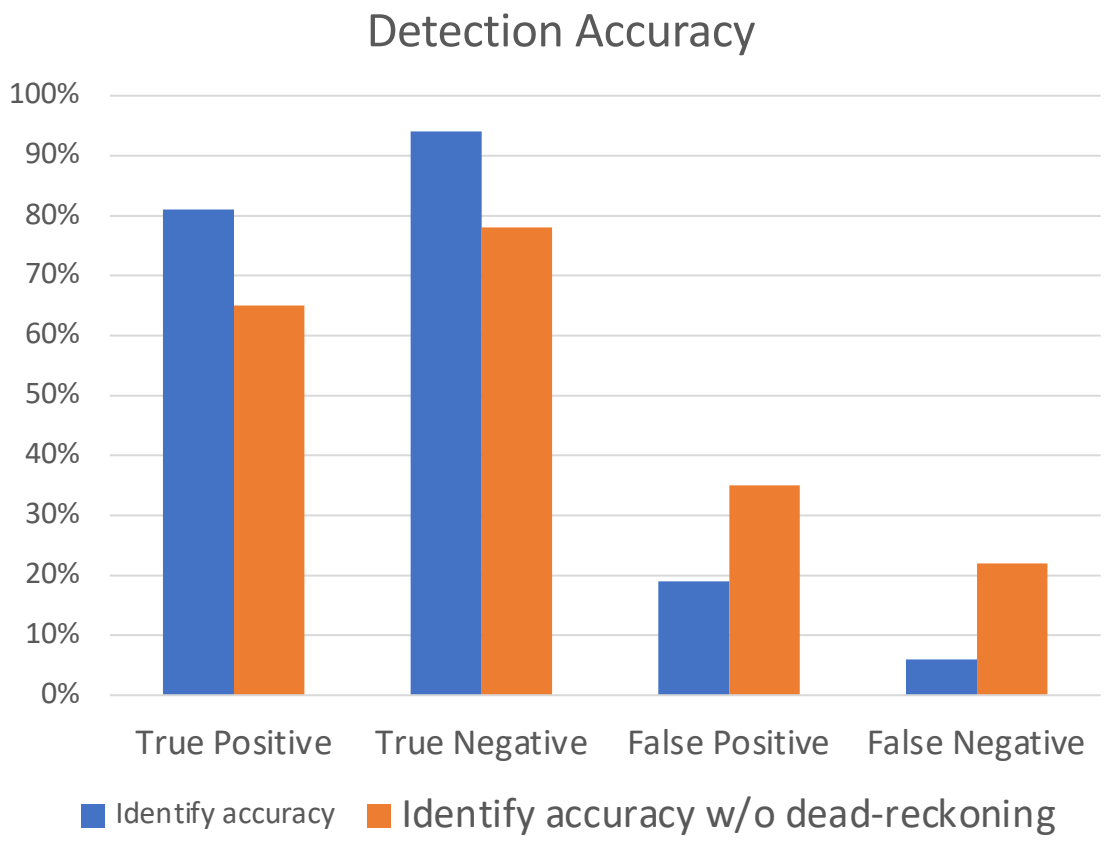
Future Work

- Take more information into consideration
  - E.g., Handover commands, signal strength, messaging sequences
- Take into consideration more movement patterns
  - Biking, running, etc.
- Using machine learning techniques to raise malicious handover alerts

Future Evaluations

The positive rate for identifying fake base station





References

- A. Dabrowski, N. Pianta, T. Klepp, M. Mulazzani, and E. Weippl, “IMSI-catch me if you can,” *Proceedings of the 30th Annual Computer Security Applications Conference*, 2014.

- H. Wang, S. Sen, A. Elgohary, M. Farid, M. Youssef, and R. R. Choudhury, “No need to war-drive: unsupervised indoor localization,” *Proceedings of the 10th international conference on Mobile systems, applications, and services - MobiSys '12*, 2012.

- Nisargnp, “NISARGNP/deadreckoning: Real-time localization on Android phones using inertial sensors (accelerometer, Compass, gyro),” *GitHub*. [Online]. Available: https://github.com/nisargnp/DeadReckoning. [Accessed: 14-Dec-2022].

Thanks! Questions?