Location-Leaking in Mobile Augmented Reality

Gabriel Meyer-Lee; Swarthmore College
Jiacheng Shang, Jie Wu; Temple University

Outline

- Motivation and Context
- Attack Model
- Analysis and Results
- Conclusions

Motivation and Context

The emergence of mobile augmented reality and the unaddressed security and privacy concerns.

Mobile Augmented Reality

- Interactive virtual content situated in the real world.
  - Broader term "mixed reality"
- Location-based AR ties virtual content to geophysical location
- Projected to reach $85-90 billion by 2022
  - Mostly games

powerhour.at
O Malleys Irish Pub
139 m
20:00-04:00 Biere 2.30 Euro, Cider 0.5l Nimm 4 zahl 3, Spritzer 1.80 Euro, Shots 2.00 Euro
details

AR Security/Privacy

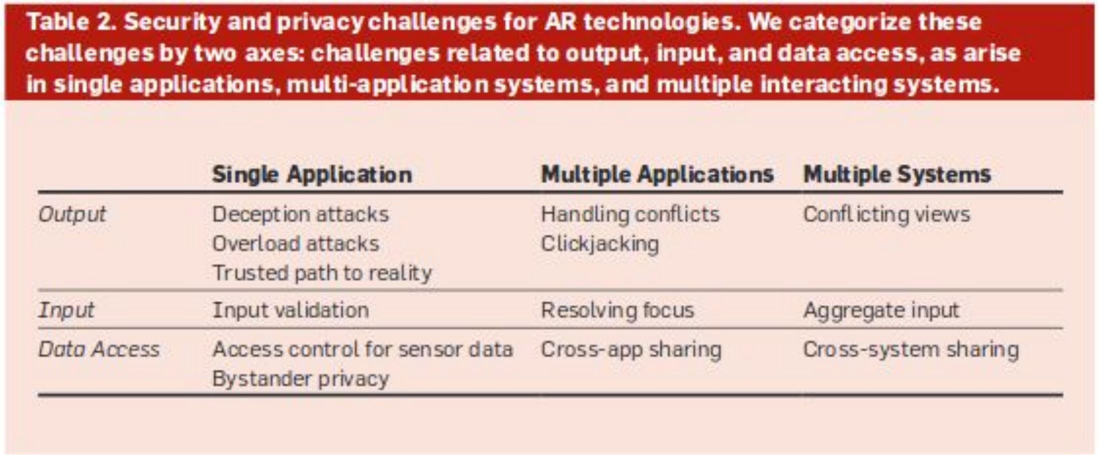
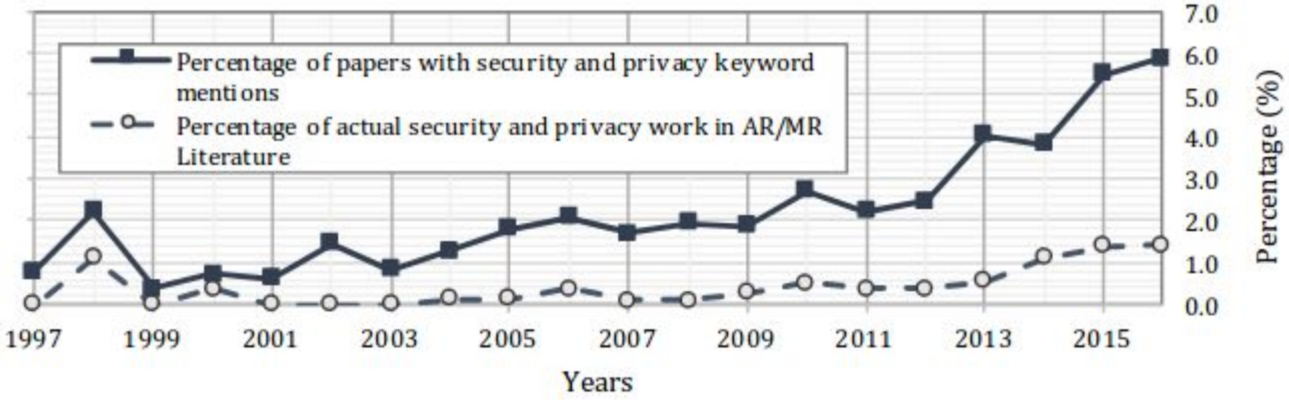


Table 2. Security and privacy challenges for AR technologies. We categorize these challenges by two axes: challenges related to output, input, and data access, as arise in single applications, multi-application systems, and multiple interacting systems.

	Single Application	Multiple Applications	Multiple Systems
Output	Deception attacks Overload attacks Trusted path to reality	Handling conflicts Clickjacking	Conflicting views
Input	Input validation	Resolving focus	Aggregate input
Data Access	Access control for sensor data Bystander privacy	Cross-app sharing	Cross-system sharing



Figures from Roesner (2014), de Guzman (2018)

Network Traffic Analysis

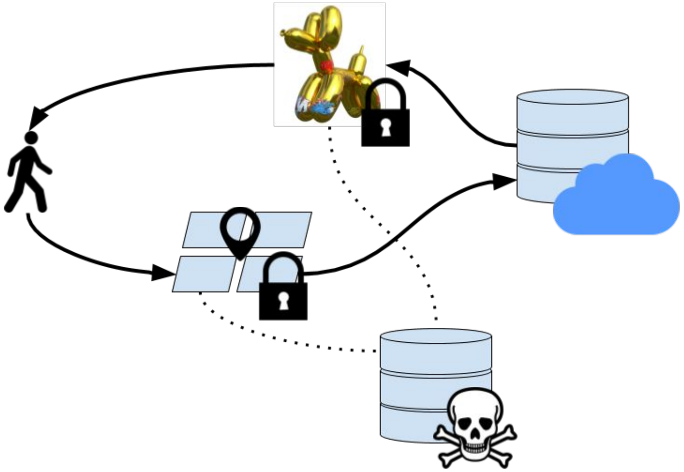
- Web sites are vulnerable to side-channel attacks because as a byproduct of common web design practices
  - Low-entropy inputs
  - Stateful communications
  - Significant traffic distinction
- All of these are also applicable to the design of mobile AR applications
- Website Fingerprinting →Location Fingerprinting

The Attack

Side-channel attack to reveal user's location through network traffic analysis

Overview of the attack

- Three separate sets of digital content
- User downloads content when within visible radius
- User's network traffic is monitored
- User is located based on their network traffic patterns



Model of the side-channel attack

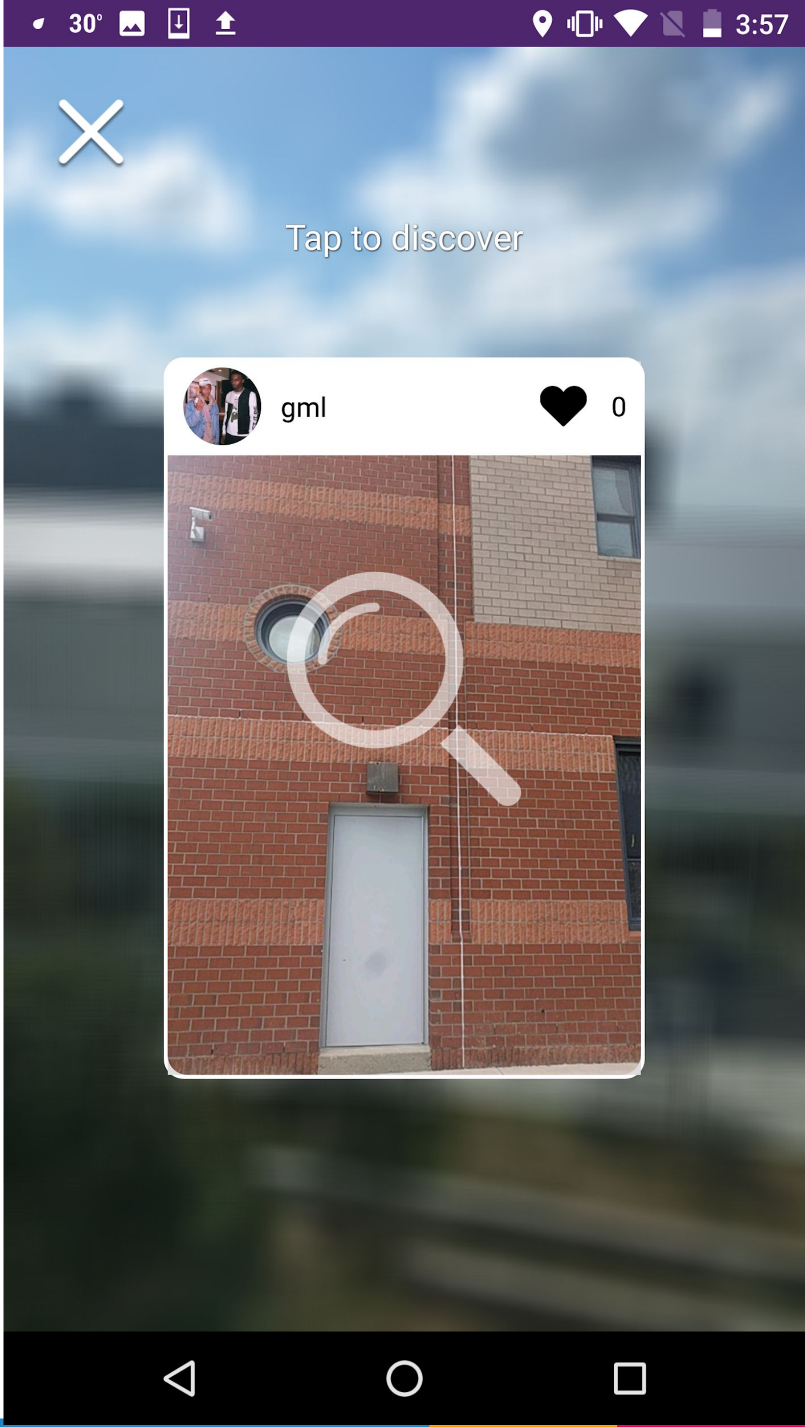
Monitoring network traffic

- Network sniffing
  - Typical method for network traffic analysis attack
  - Applicable to mobile user in urban center or university campus, but requires access point coverage
- **Spyware on Device**
  - Coarseness of user permissions makes over-permissioning inevitable
  - Most Android users do not pay attention to or comprehend permissions

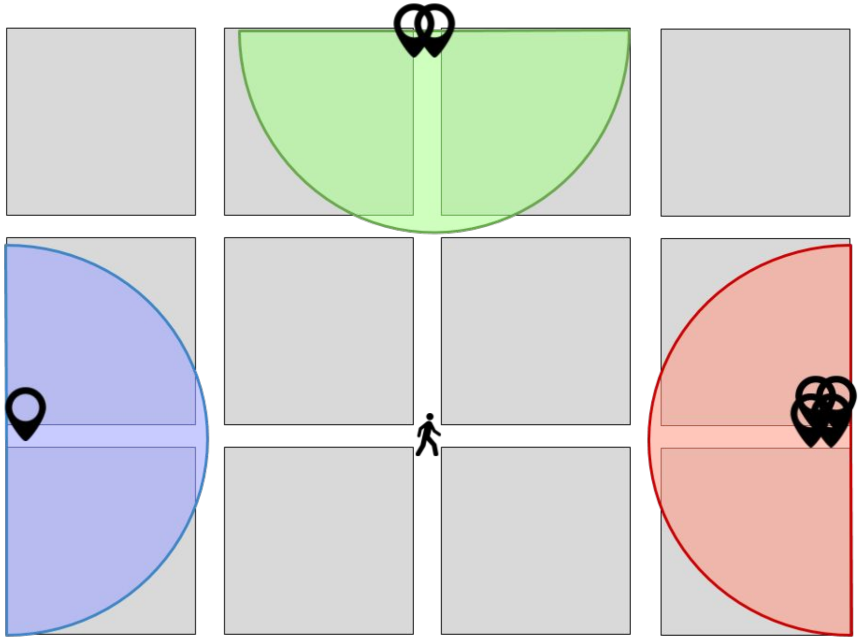
WallaMe

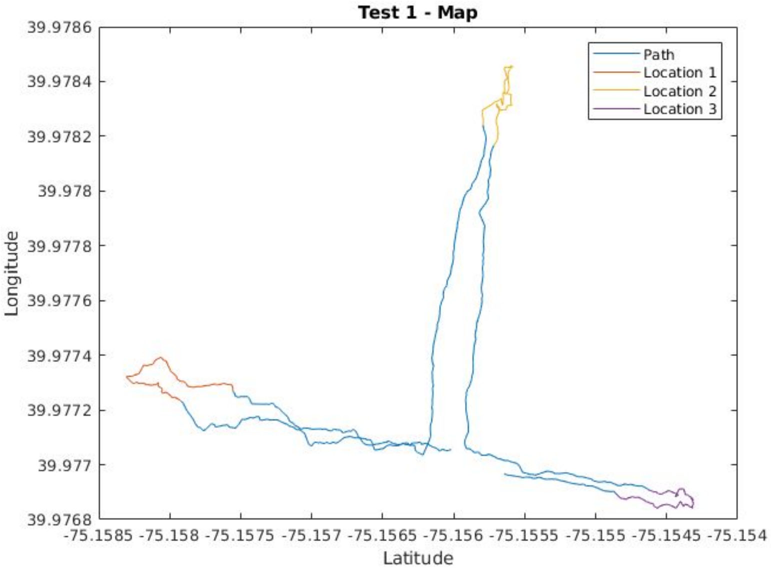
Digital graffiti AR app available for iOS and Android

Users post walls for other users to discover the art on

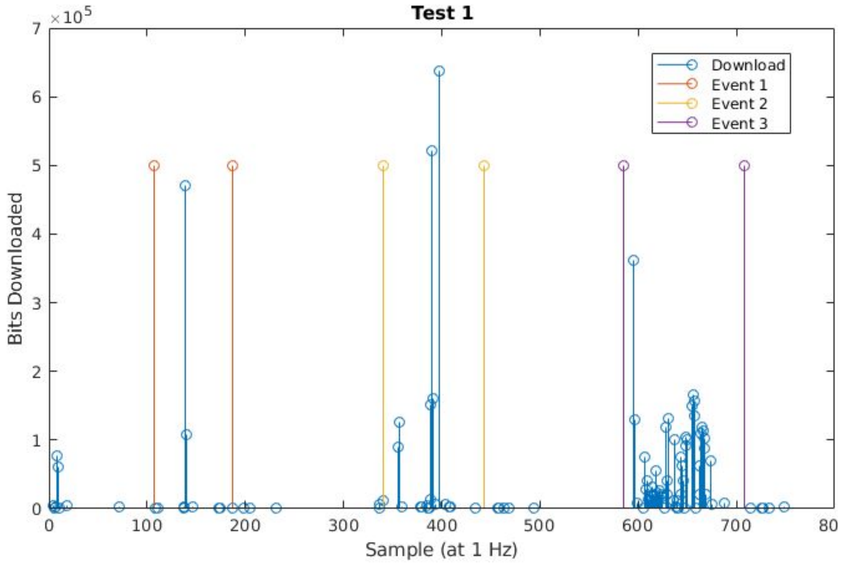


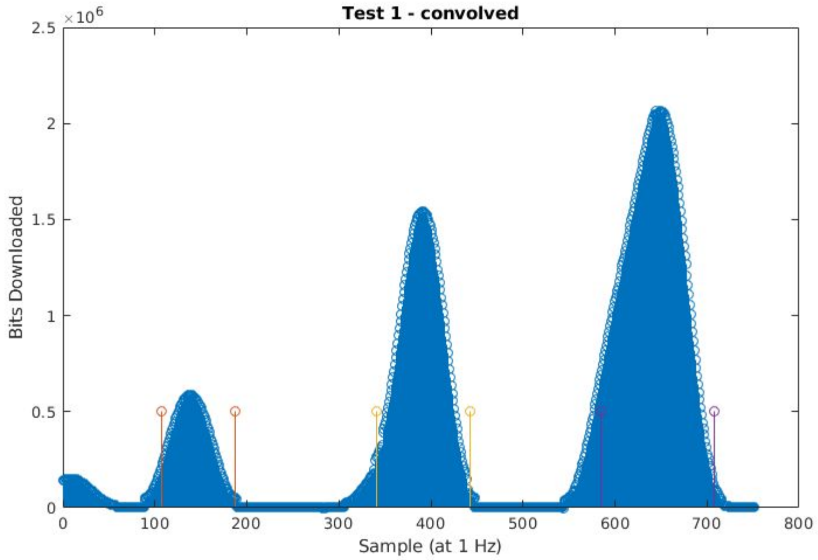
Scenario One:
Non-overlapping duplicates



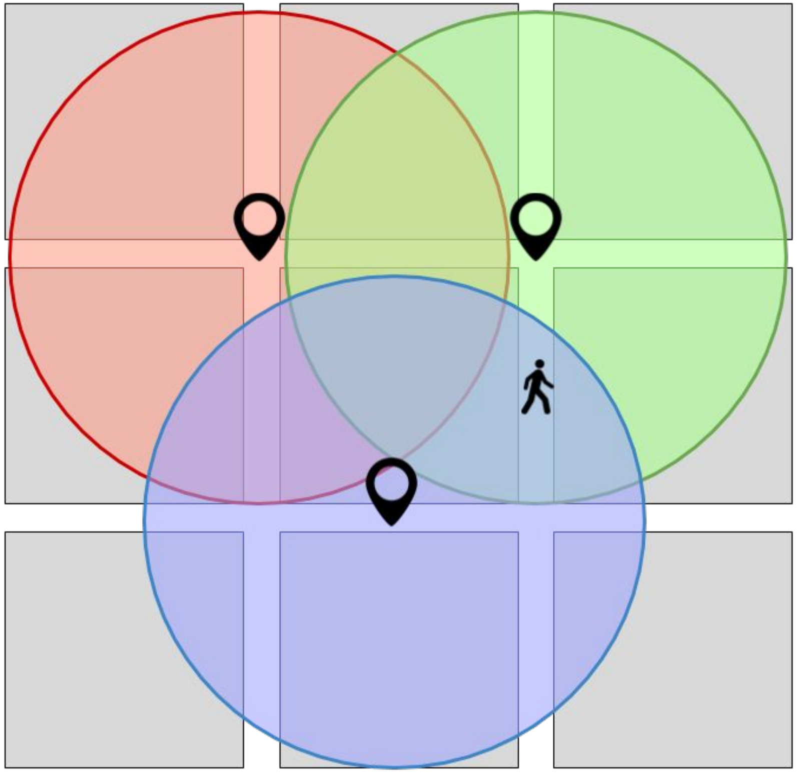


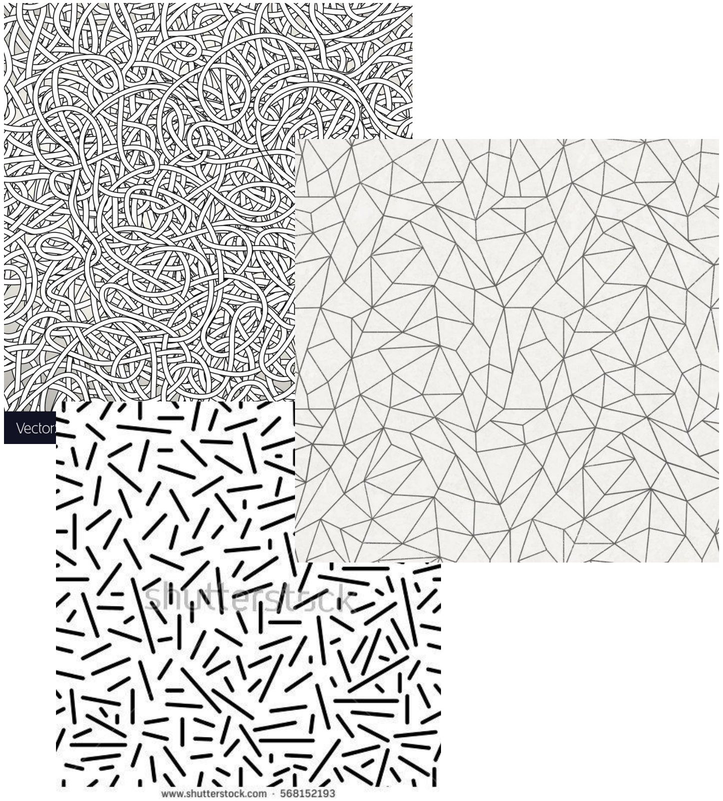
Scenario One: Non-overlapping duplicates





Scenario Two:
Overlapping, distinct





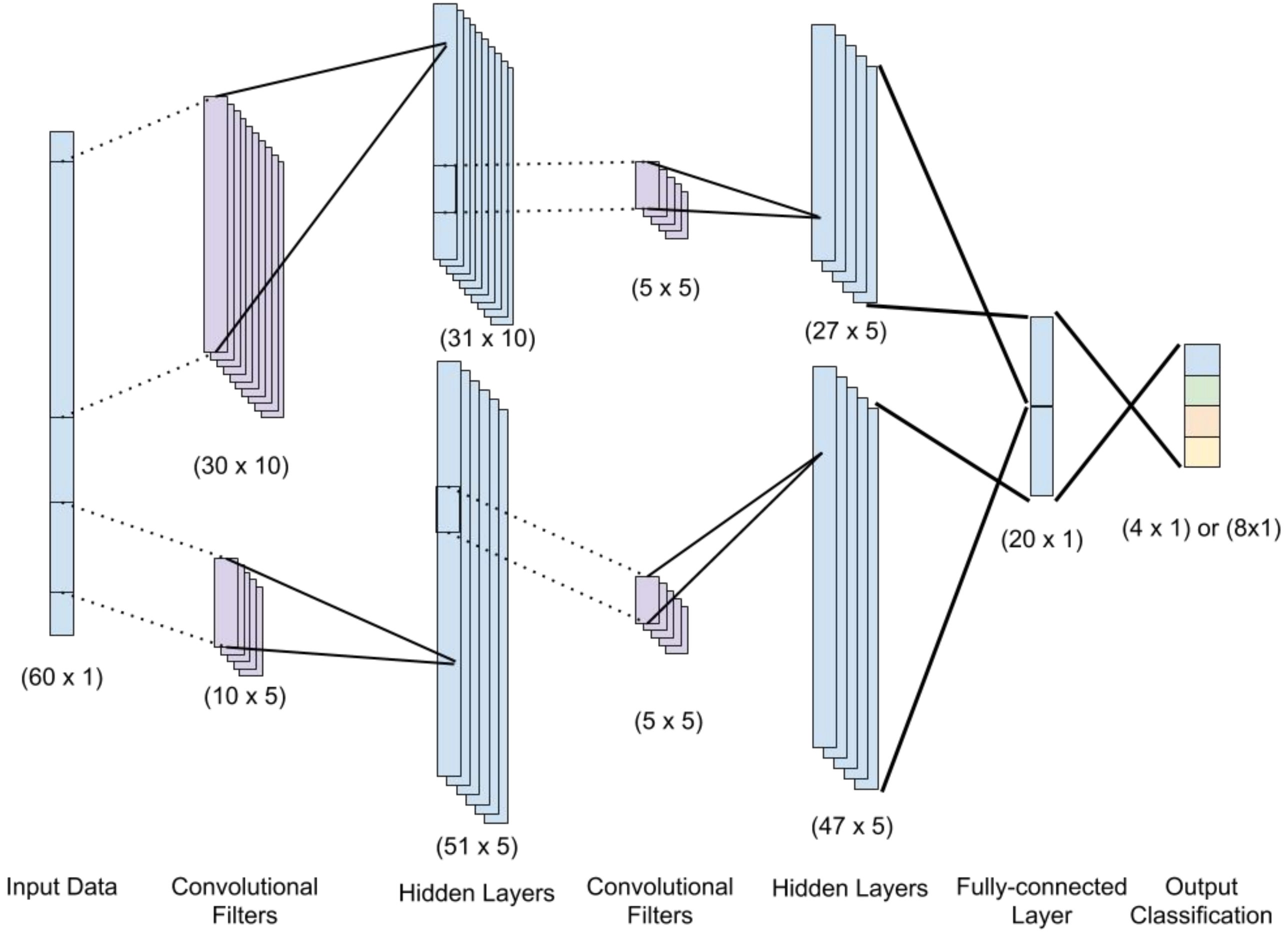
Analysis and Results

CNN-based data processing pipeline and classification accuracy

Analysis

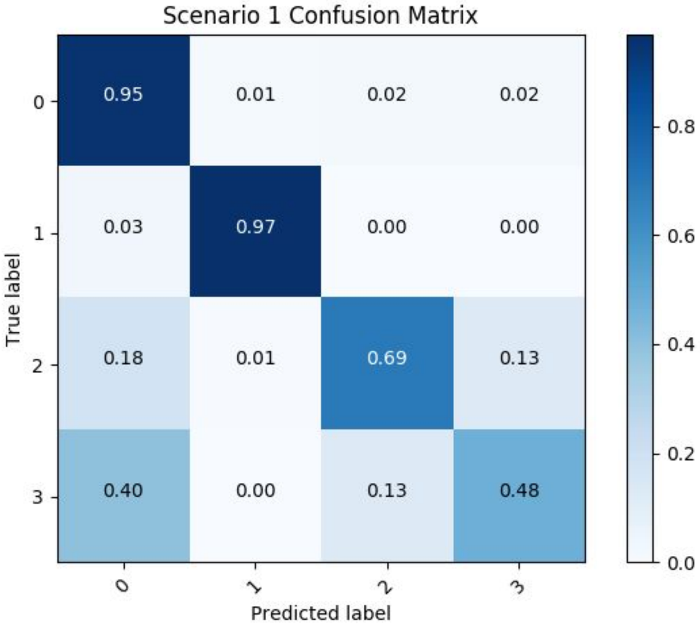
- Past WF algorithms have utilized SVM, kNN, random forest
- We require an algorithm that supports:
  - Near real time location updates, allowing an online attack.
  - No reliance on sequential pattern of input location-encoded data
- Our method:
  - Window network download data to 60s
  - Manually label location regions of recorded data
  - Train 1D CNN

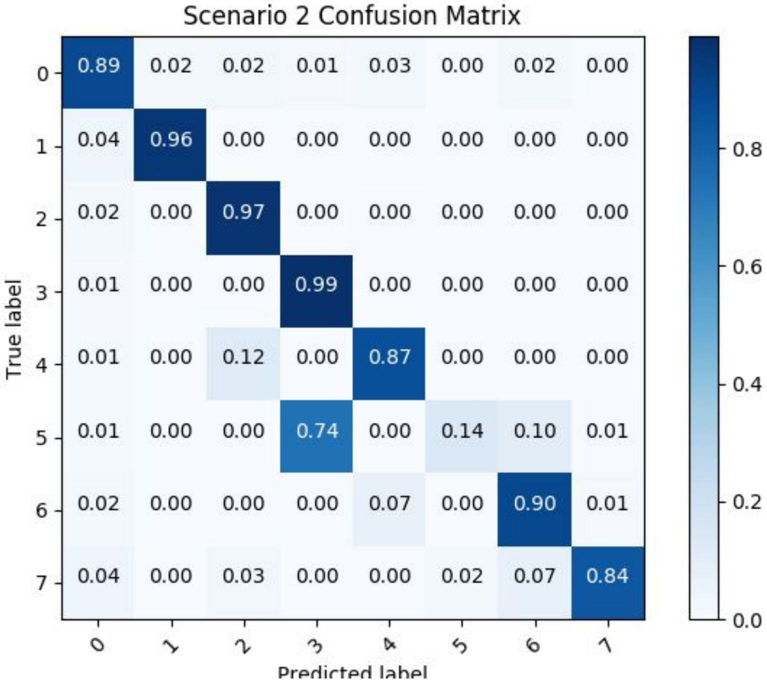
CNN Design


(60 x 1)
(30 x 10)
(10 x 5)
(31 x 10)
(51 x 5)
(5 x 5)
(5 x 5)
(27 x 5)
(47 x 5)
(20 x 1)
(4 x 1) or (8x1)
Input Data
Convolutional Filters
Hidden Layers
Convolutional Filters
Hidden Layers
Fully-connected Layer
Output Classification

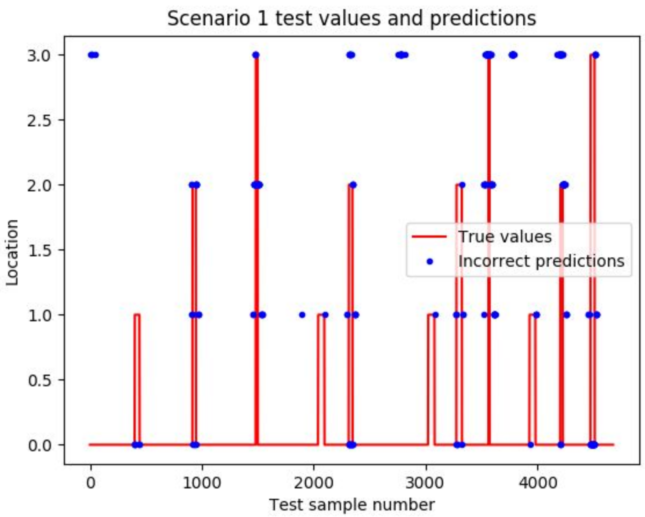
Results

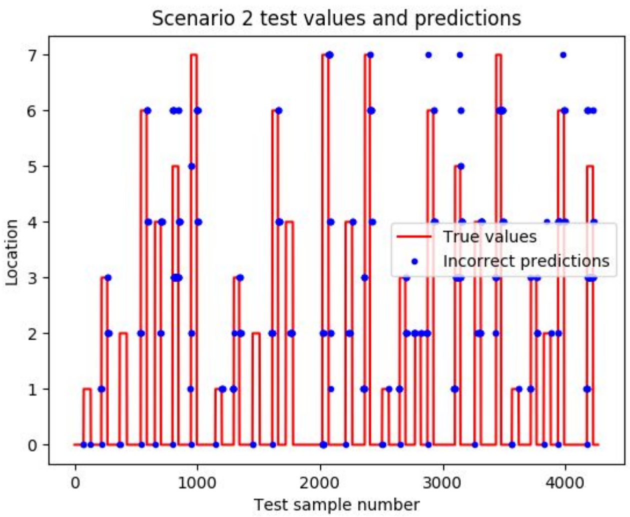
Scenario	Test Accuracy
1	93.8%
2	87.6%





Moving Frame Error





	Scenario 1	Scenario 2
Raw Accuracy	93.8%	87.6%
Error due to moving frame	56.3%	58.2%
Accuracy excl moving frame	97.3%	94.8%

Conclusion

Potential avenues for mitigation and final conclusion

Mitigation

- Irregular user behavior
- Secure app design
  - Padding
  - Probabilistic location loading

Conclusion

- You don’t have to worry about playing Pokemon Go for now
- Network traffic patterns in AR apps can in fact leak location information
- Future AR developers must include network privacy breaches among the risks they account for