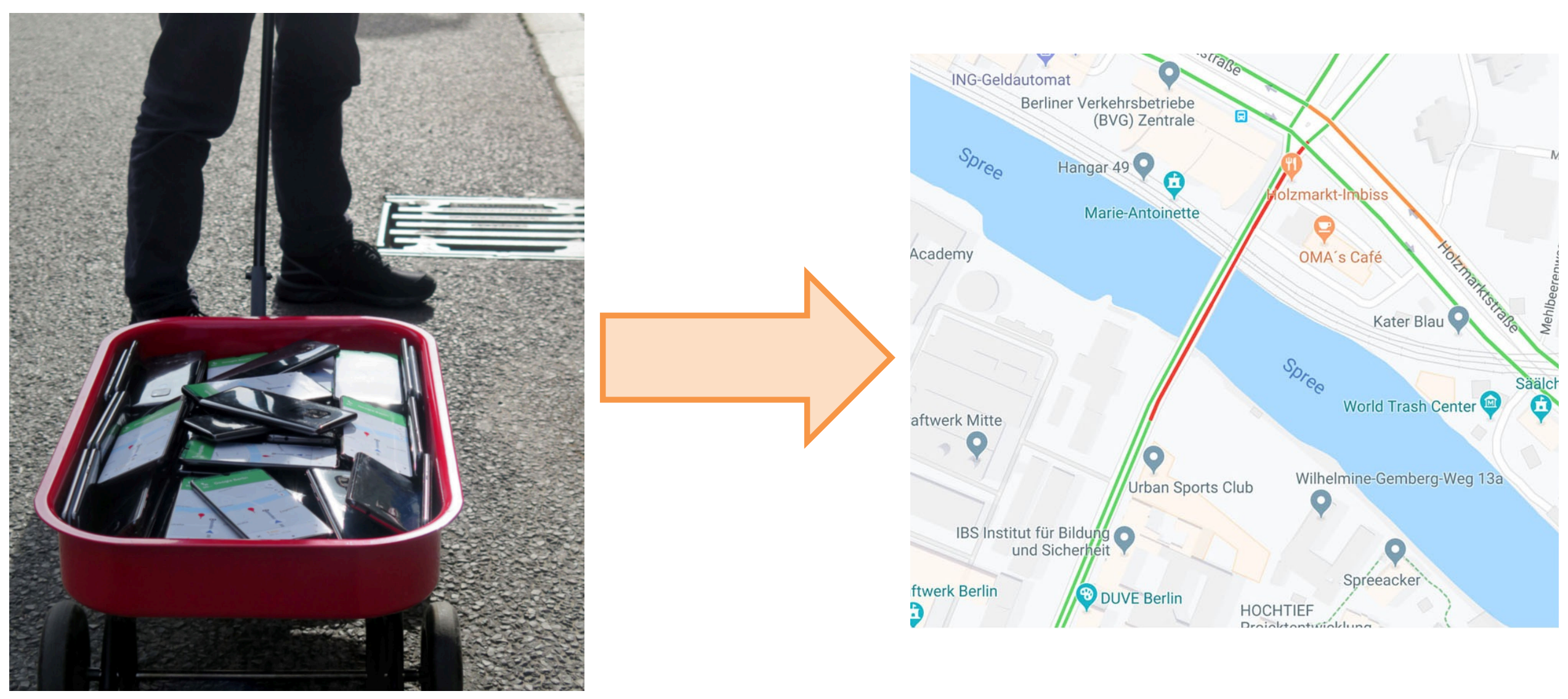
ARGUS: Preventing Sybils for Mobile Crowdsensing User Registration

Cihan Eryonucu
KTH Royal Institute of Technology
Networked Systems Security (NSS) Group, www.eecs.kth.se/nss
Supervisor: Panos Papadimitratos

Motivation & Research Goals

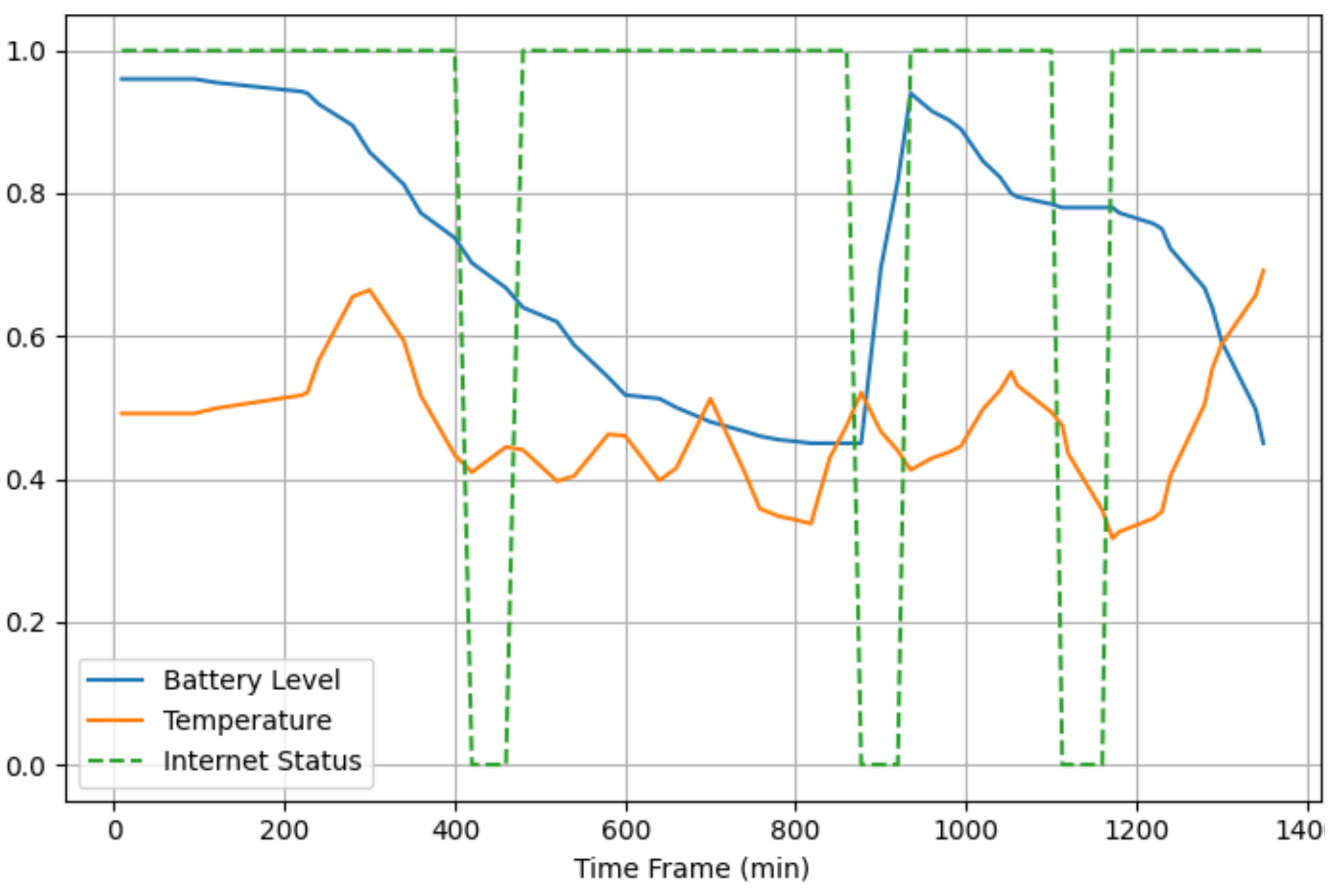
- Mobile Crowdsensing (MCS) relies on large-scale participation via mobile sensing platforms
- Sybil attackers can manipulate and deceive MCS by injecting huge amount bogus data [1]
- MCS should only accept actual users with an actual devices
- We propose ARGUS to stop such Sybil attackers during the registration phase [2]
  - Distinguishing between legitimate vs fake/emulate/farm device
- Balancing security with ease of use
  - Legitimate users are not burdened while maintaining a high bar for potential attackers

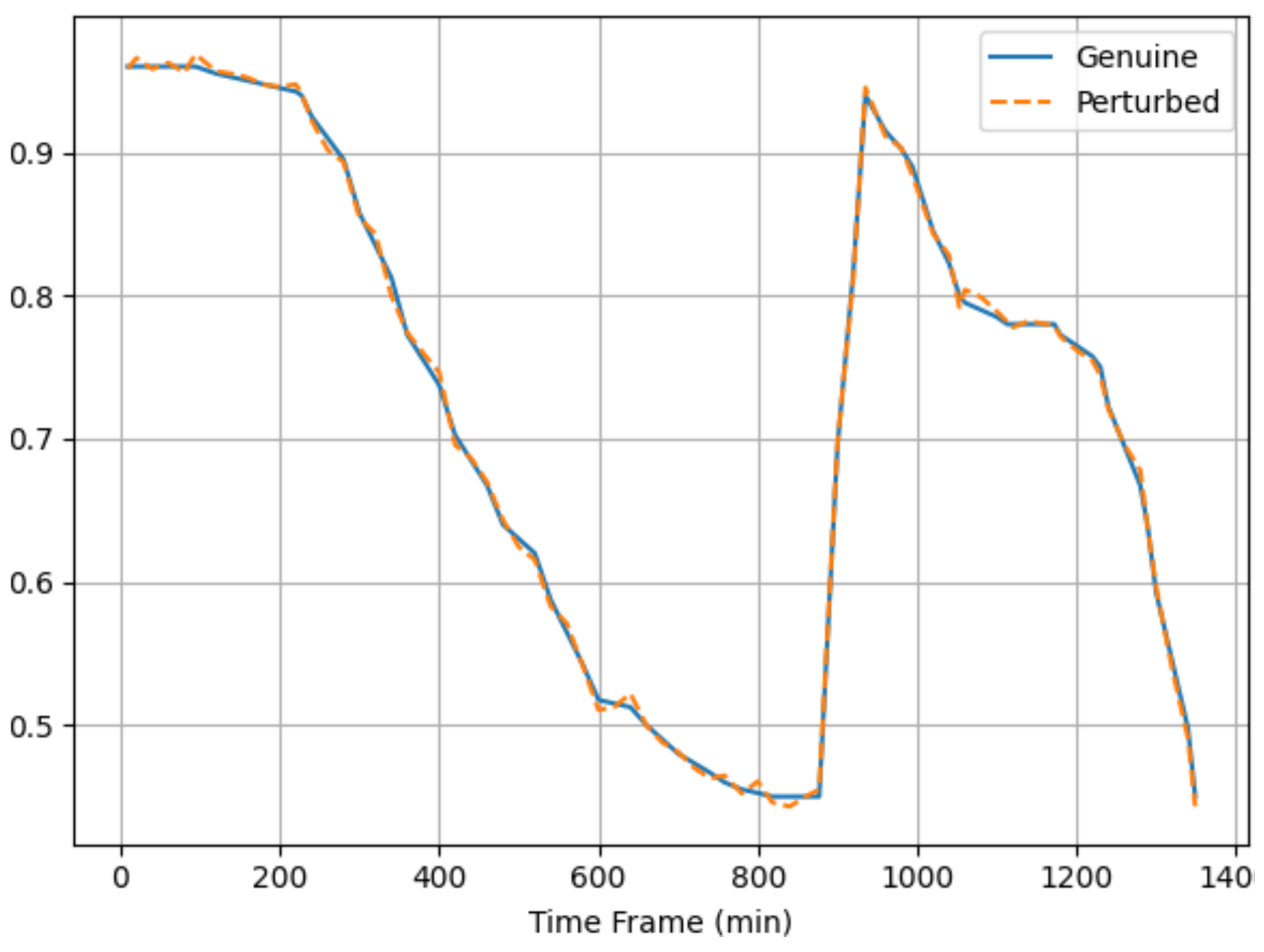


Objectives

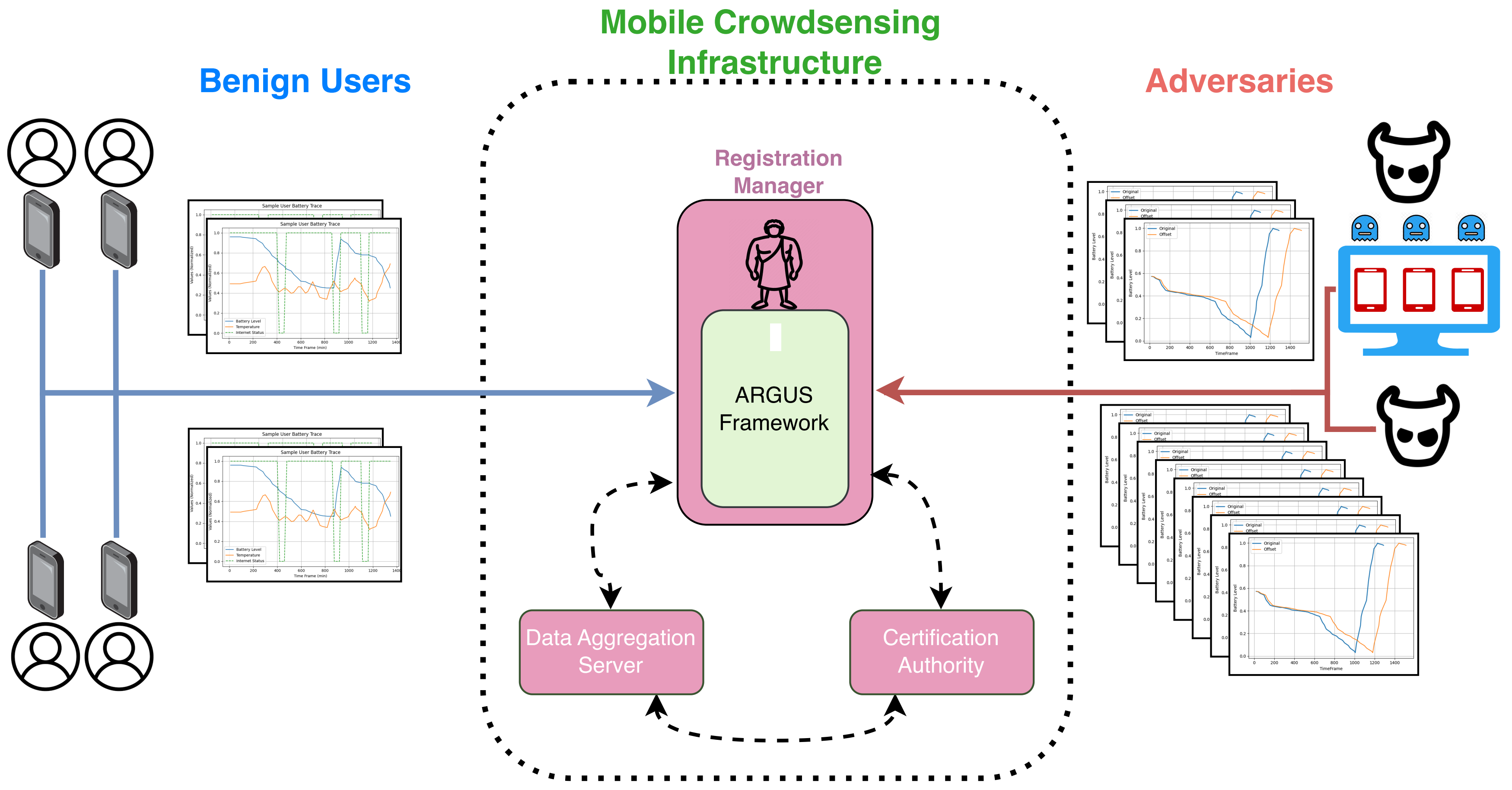
Smartphone battery traces detect Sybils without invading user privacy [3]

- Battery level, temperature, internet and charging status
- Sparsely collected over 24h
- Generic enough, obscures user behavior
- Sufficient to verify device legitimacy





System Model



Adversary Model

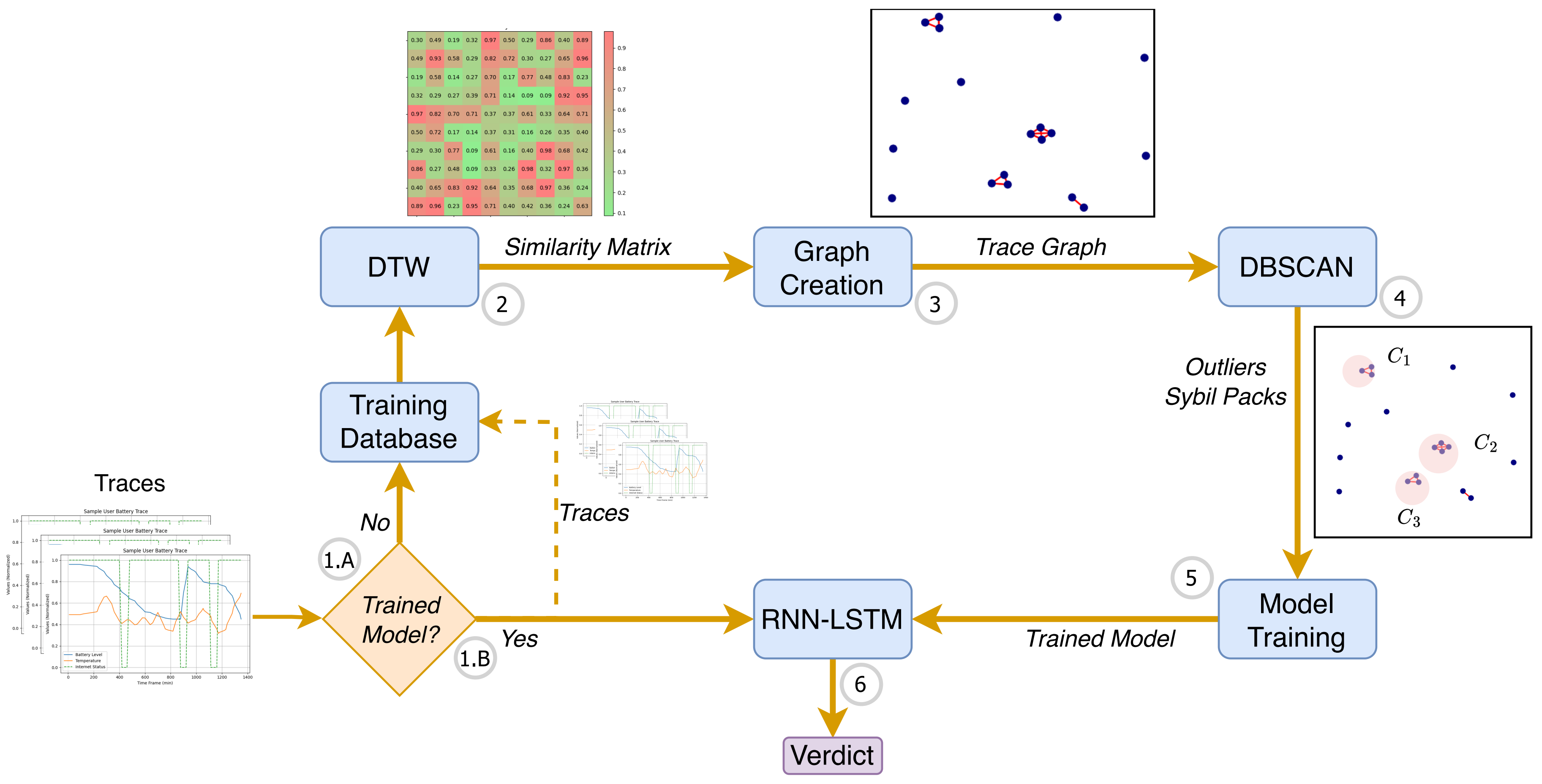
Attack that adversaries can employ:

1. Generate and submit high volume of synthetic traces
2. Generate a pack of fake traces by adding noise to a genuine trace
3. Train a generative model with actual traces
4. Slowly gather traces and submit.

References

1. C. Eryonucu and P. Papadimitratos, “Sybil-Based Attacks on Google Maps or How to Forge the Image of City Life,” ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec), May 2022
2. C. Eryonucu and P. Papadimitratos, “Security and Privacy for Mobile Crowdsensing: Improving User Relevance and Privacy”, *ESORICS SECPRE 2023*, September 2023
3. C. Eryonucu and P. Papadimitratos, “ARGUS: Preventing Sybils for Mobile Crowdsensing User Registration”, manuscript in submission

Framework and Results



DTW: Measures similarity between traces

- Finds replayed and similar traces
- Creates similarity matrix for traces

DBSCAN: Identifies clusters of Sybils

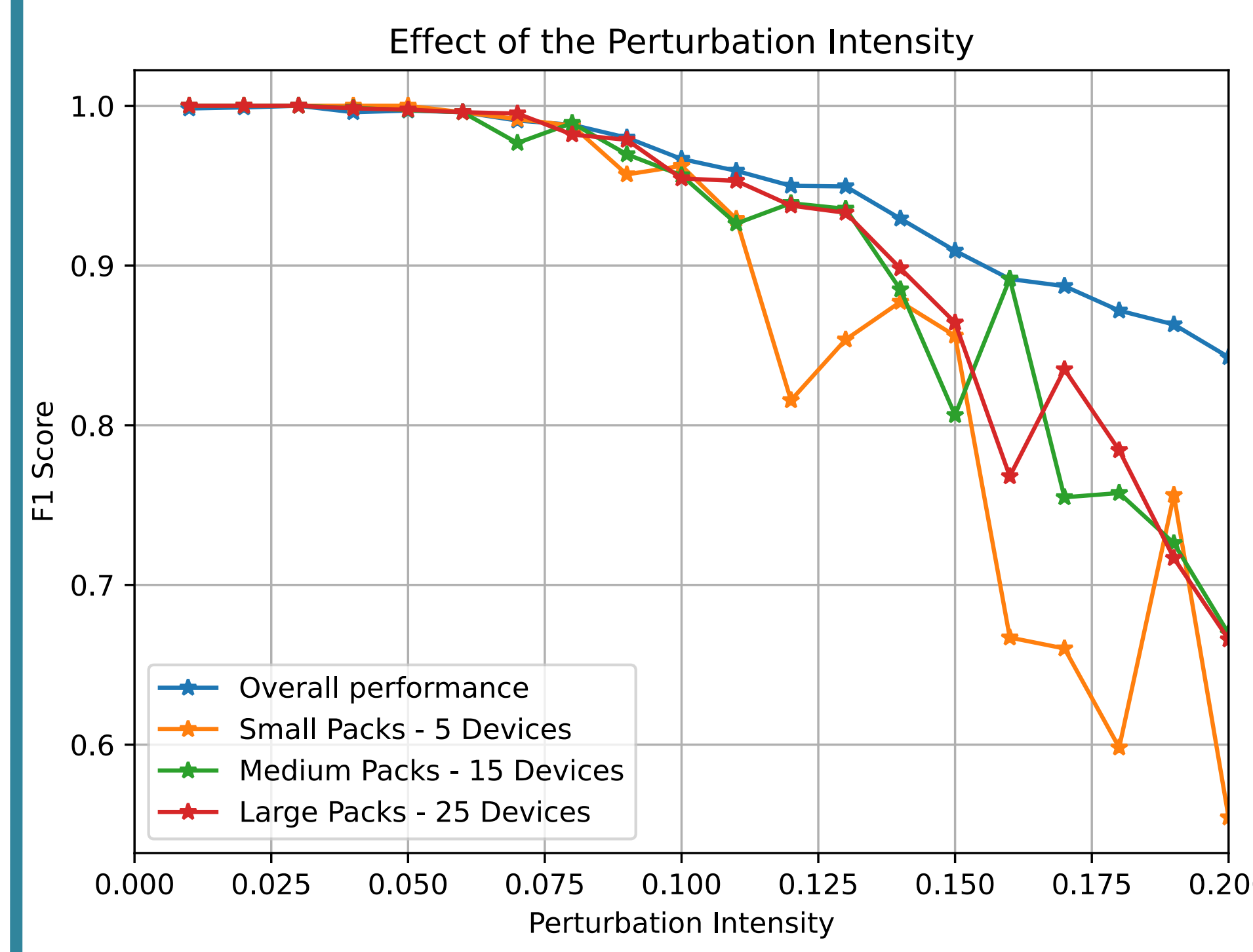
- Clusters traces via DTW scores
- Detecting clusters of Sybil accounts
- Outliers are likely genuine users

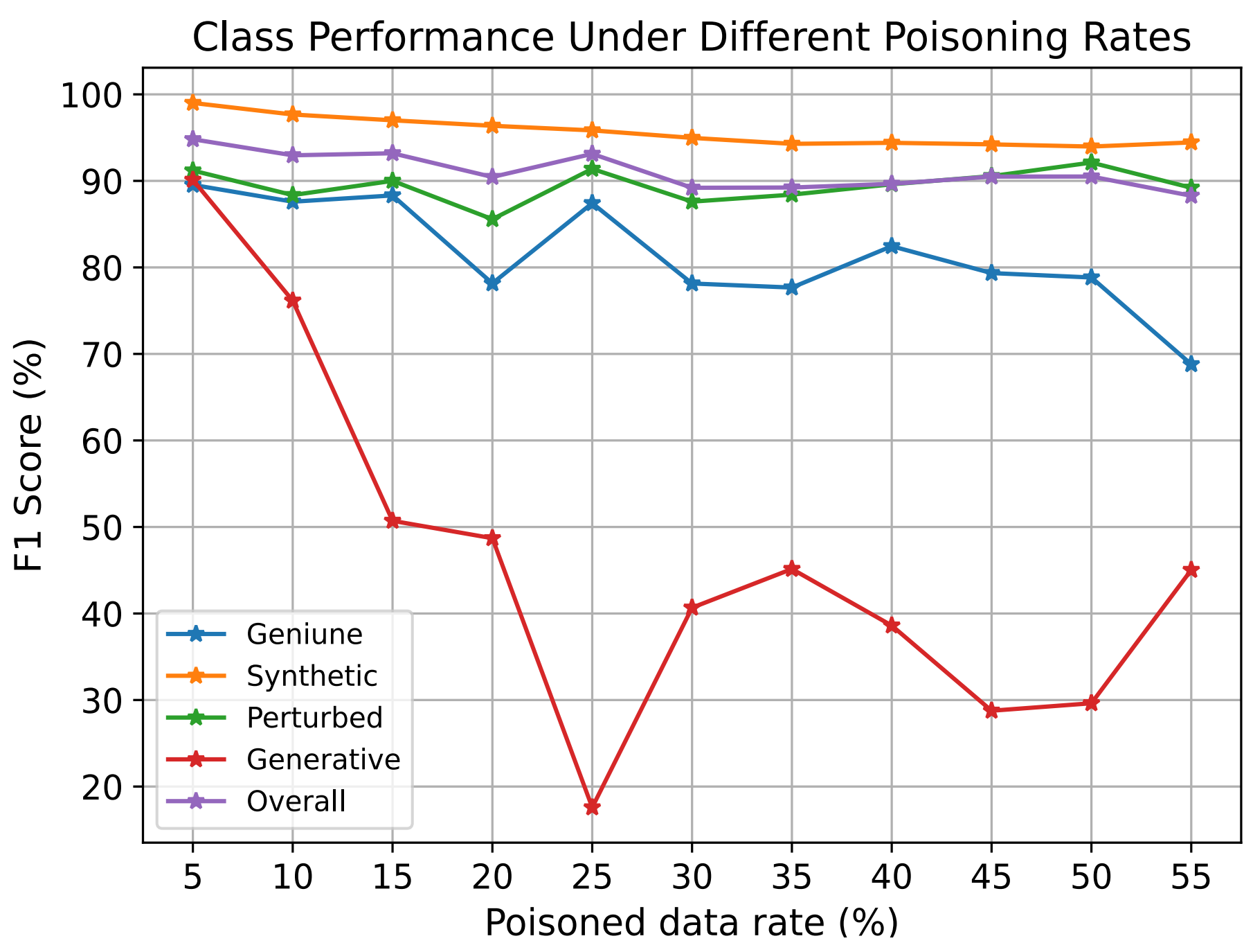
VAEs: Trained to detect generative traces

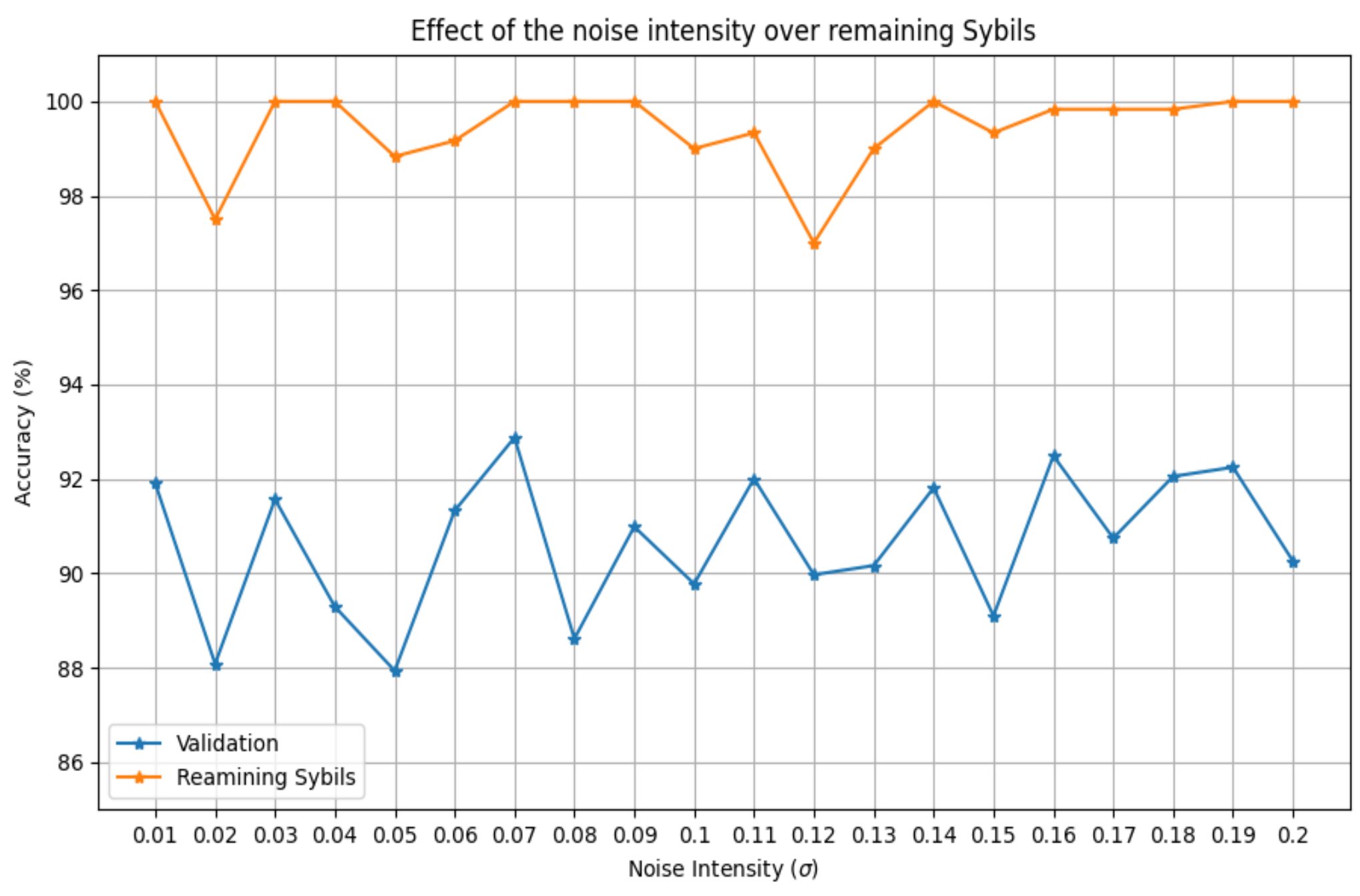
- Create generative traces for the training

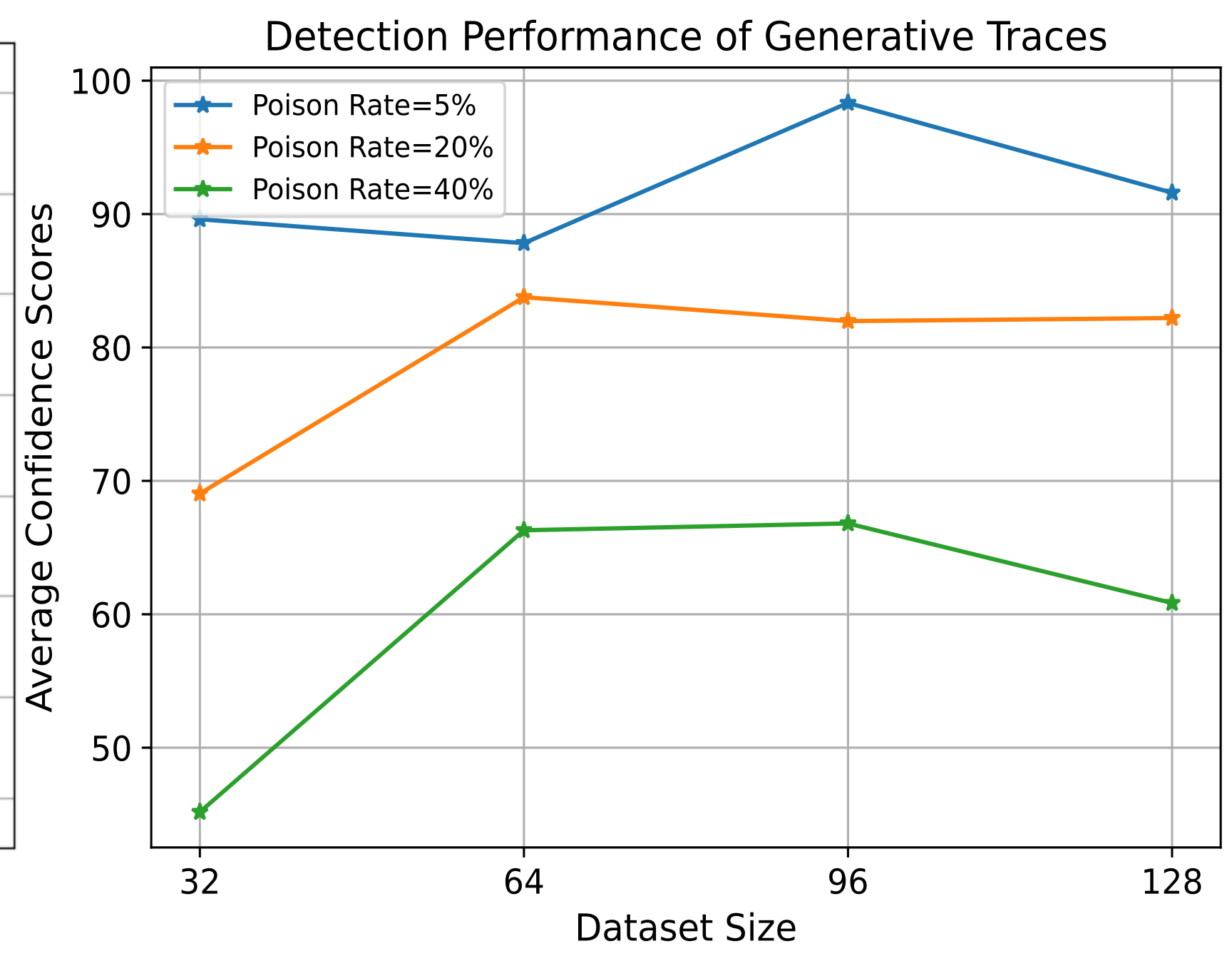
RNN-LSTM: Final verdict

- Identify synthetic and generative traces
- Finds traces that is missed by the DBSCAN









WASP | WALLENBERG AI, AUTONOMOUS SYSTEMS AND SOFTWARE PROGRAM