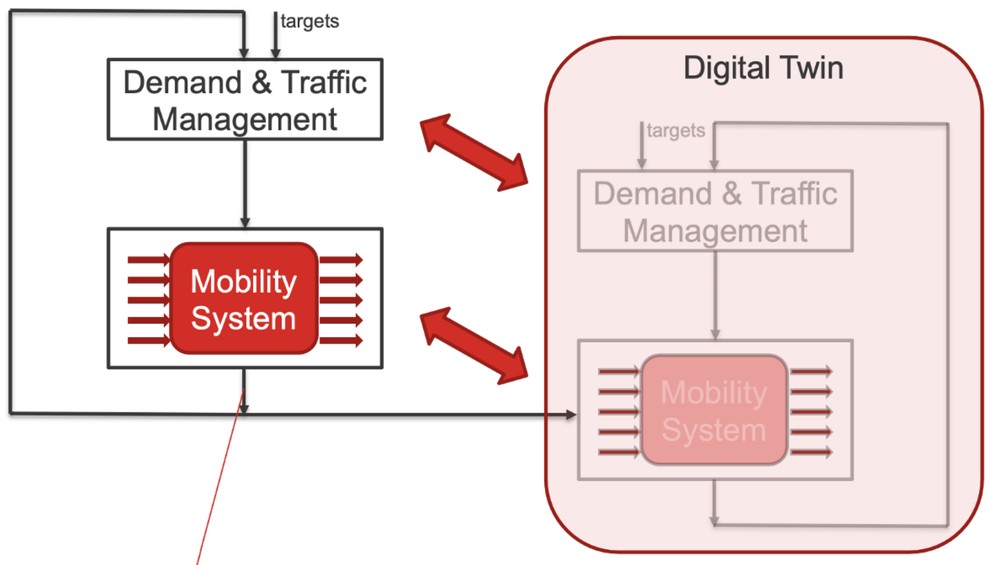
Privacy-Preservising Mobility Data Collection

Fatemeh Marzani, Thijs van Ede, Geert Heijenk and Maarten van Steen

University of Twente, The Netherlands

Overview

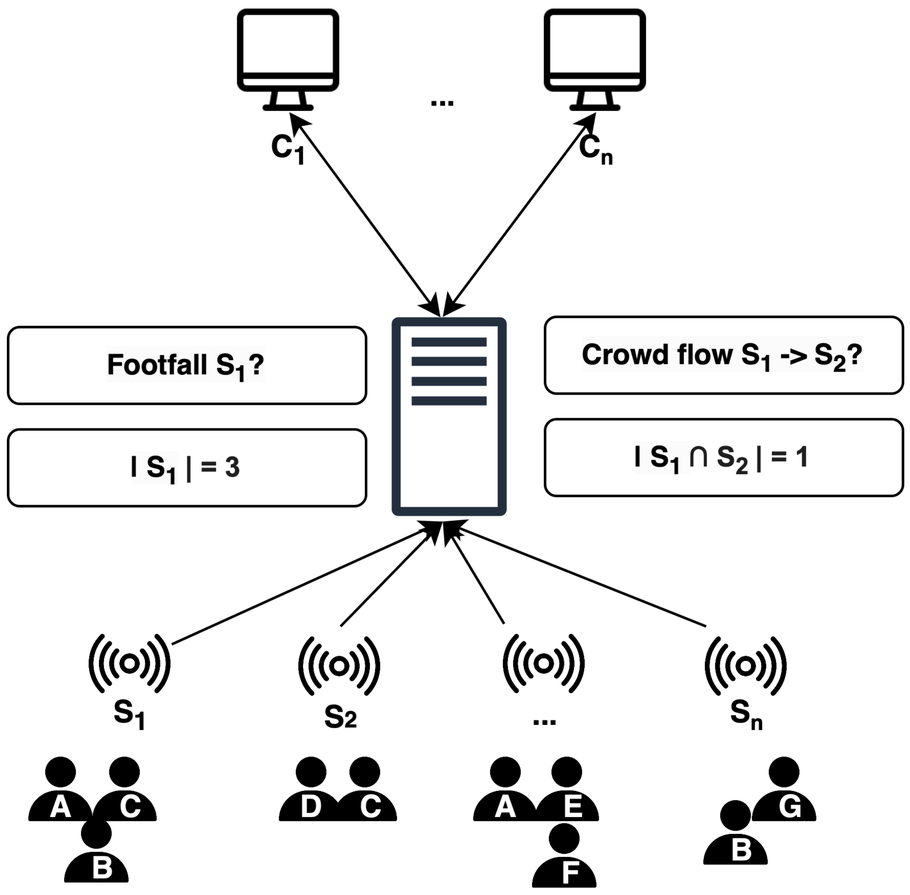


Massive privacy-preserving mobility data collection and aggregation.

Types Mobility Data

Problem: What type of identifier can be used to detect pedestrians?
Idea: Sniffing cellphone MAC addresses to collect pedestrian data.

Mobility Data Collection



Data Privacy VS. Data Protection

Data protection is concerned with who can access data!
Data privacy concerns with what can be learned from data!

Privacy Violation in Aggregation

Mobility data can be linked with auxiliary data to reveal personal details.
Providing auxiliary data for small group is easier $\rightarrow$ re-identification is easier.
Measuring footfall at s_1 = 1 and if we know s_1 is Alice's office $\rightarrow$ Alice is at s_1.

Random Data Sampling

Random sampling helps protect data privacy.
When the population is small, sampled data is less reliable but reduces the risk of re-identification.
When the population is large, sampling provides reliable and representative data.

Conclusions and Future Work

Current Approach: Collecting MAC addresses to collect pedestrian data while ensuring privacy protection.
Problem: MAC addresses are dynamically changed, making them unreliable.
Idea: Can we generate **anonymous IDs** from face data to compute footfall and crowd flow while preserving privacy?
Challenges: IDs must be irreversible and consistent for each person.
IDs must be discriminative between different individuals.

UNIVERSITY OF TWENTE.

DACS Design and Analysis of Communication Systems

f.marzani@utwente.nl