Data-Driven Model-Based Detection of Malicious Insiders via Physical Access Logs

Carmen Cheh

January 2017

Submitted to DSN last month

Motivation

- Insider threats are always approached from cyber aspect but physical security is also very important.
- Current building access controls are static and over-permissive
- We need a world view of the physical domain (e.g., location, movement behavior).

Threat Model

- Goal is to physically tamper with assets in room
- Users who have gained access to legitimate access control device (e.g., card, badge)
- Access control device has been granted access to room
- Assume that adversary access of room for malicious intent will deviate from typical work flow

Contribution

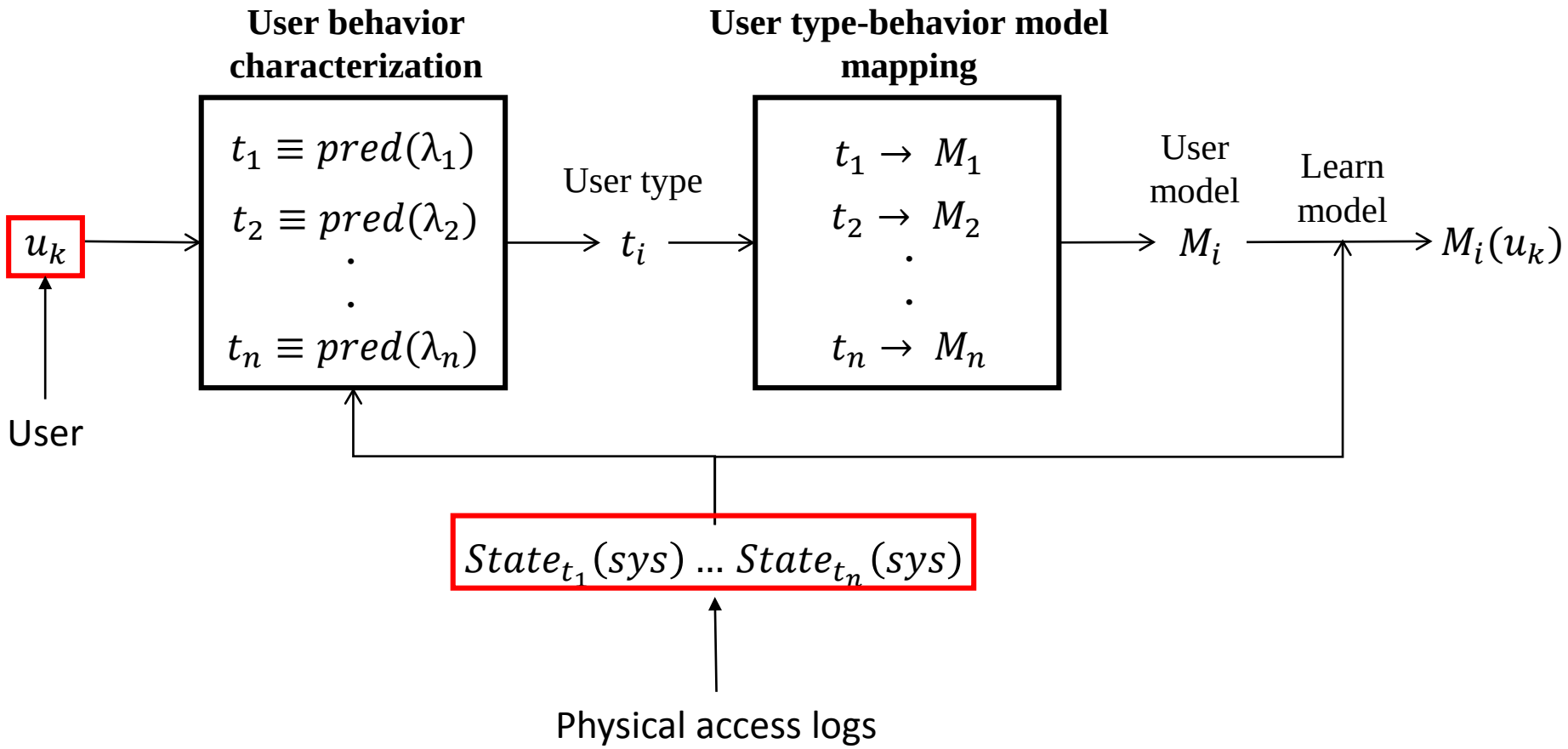
- Use domain knowledge to
  - Choose correct model
  - Establish context of movement in terms of location
- Create updatable world view of physical behavior

- Questions to answer
  - Can we characterize user’s movement behavior in a complex real-world system?
  - How can we model movement behavior?
  - Can we perform online-based detection and what factors affect the detection capability?

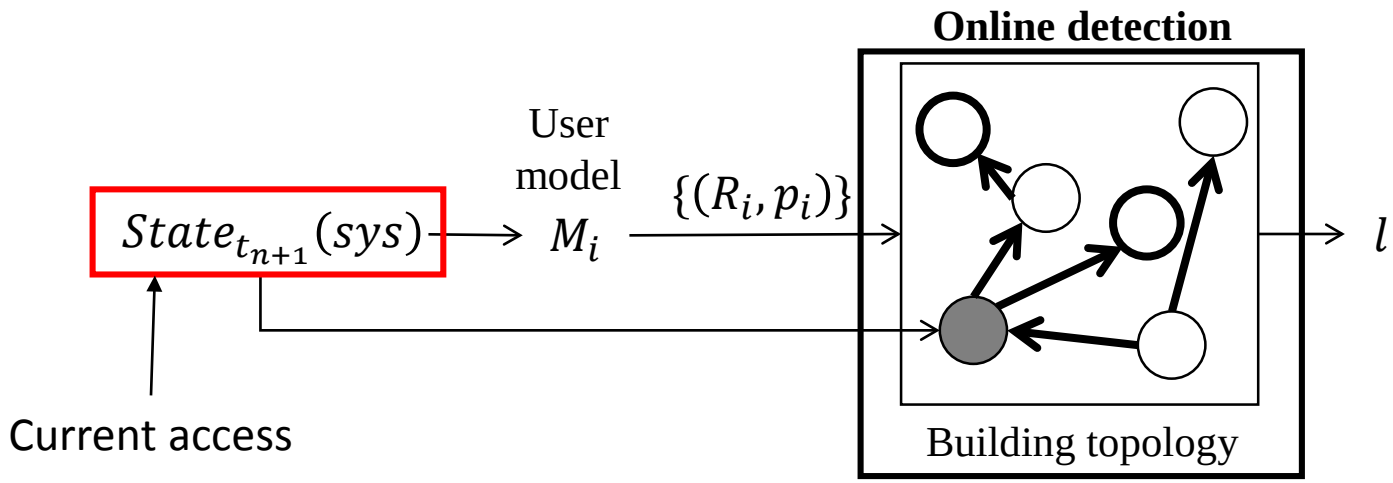
Our Approach

- Systematic, contextual solution to analyze system and its users
- Offline phase
  - Characterizes user based on past movement pattern
  - Learns appropriate model using past movement pattern
- Online phase
  - Utilize learned model from offline phase, together with building topology to detect anomalies

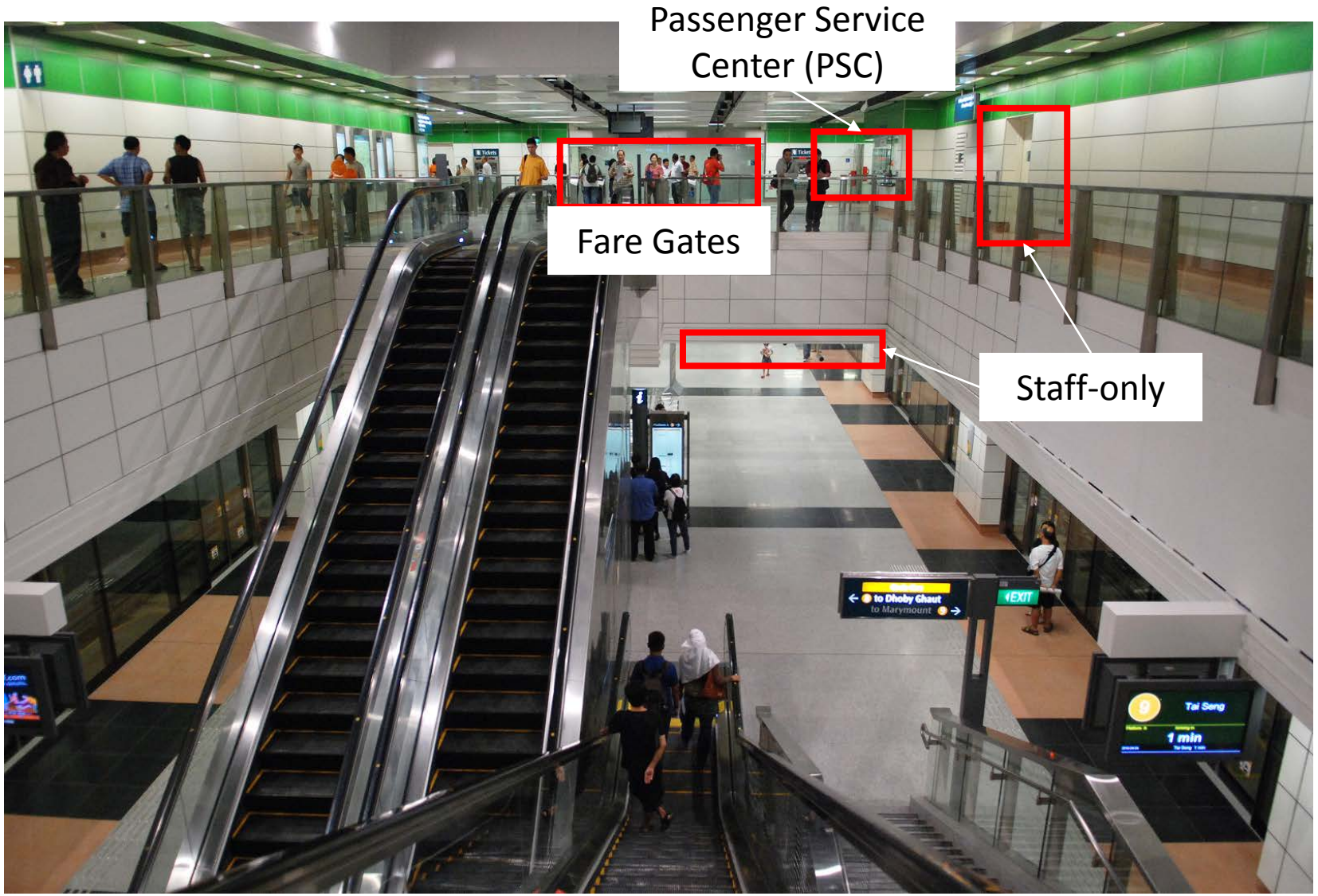
Offline phase



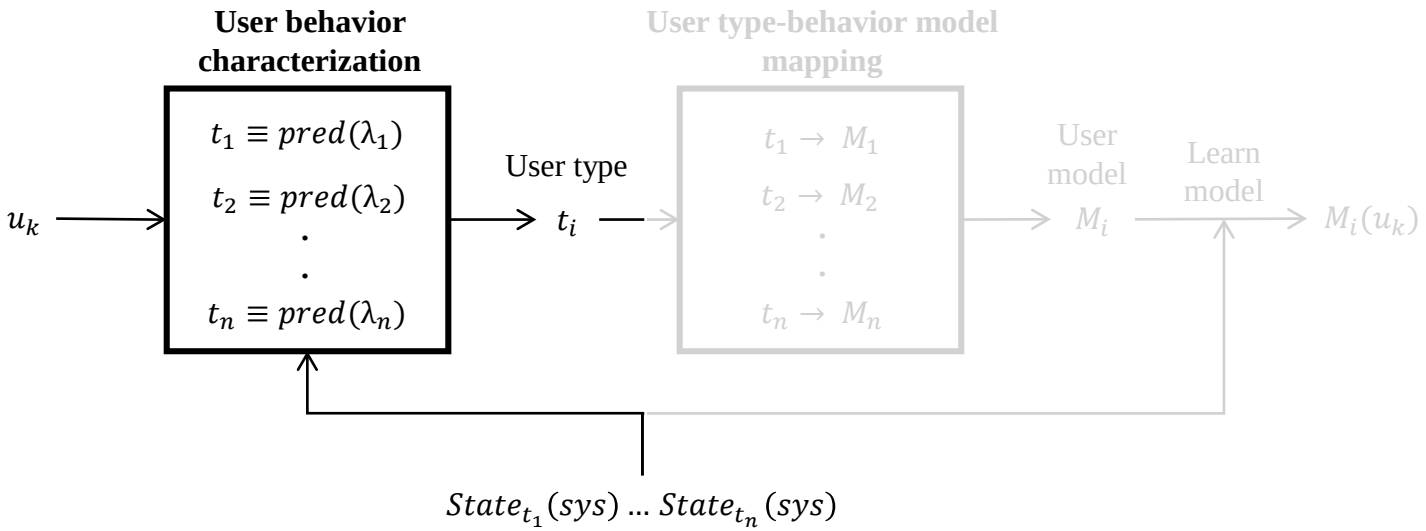
Online phase



Use Case – Railway Transit System

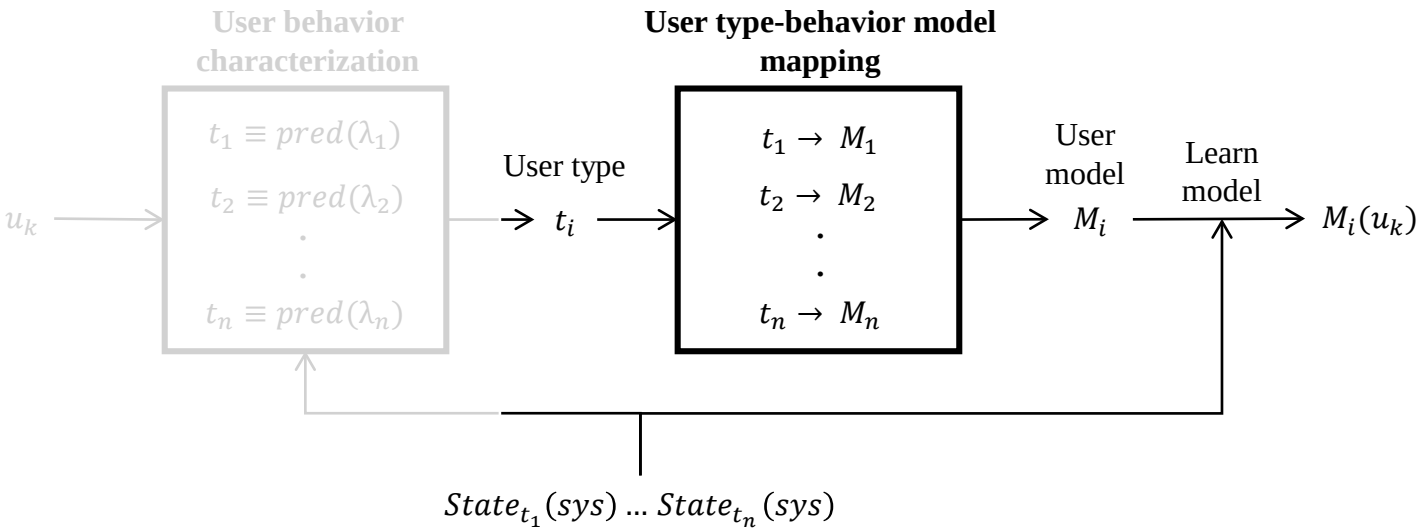


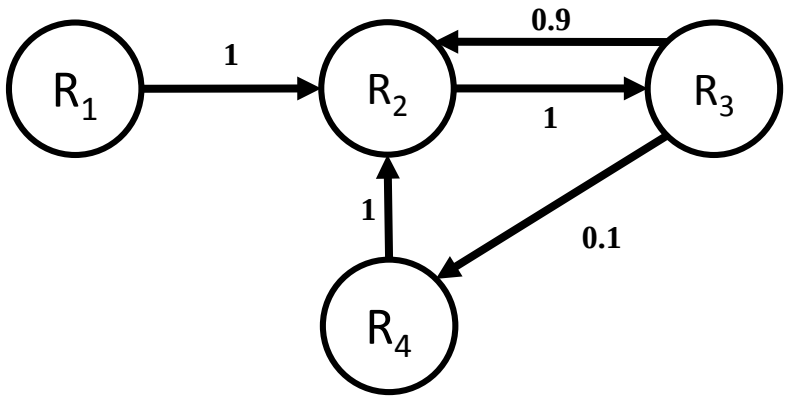
Offline phase – user type



- Two types of users
  - t_1 – fixed shift, regular behavior (e.g., station operators)
  - t_2 – moves on-demand based on event occurring in system (e.g., maintenance staff)
- We can measure regularity by defining λ as entropy of time series of previous movement ($R_1 \rightarrow R_2 \rightarrow R_3 \rightarrow R_1$)
  - $t_1 = (\lambda < \mathbf{E})$

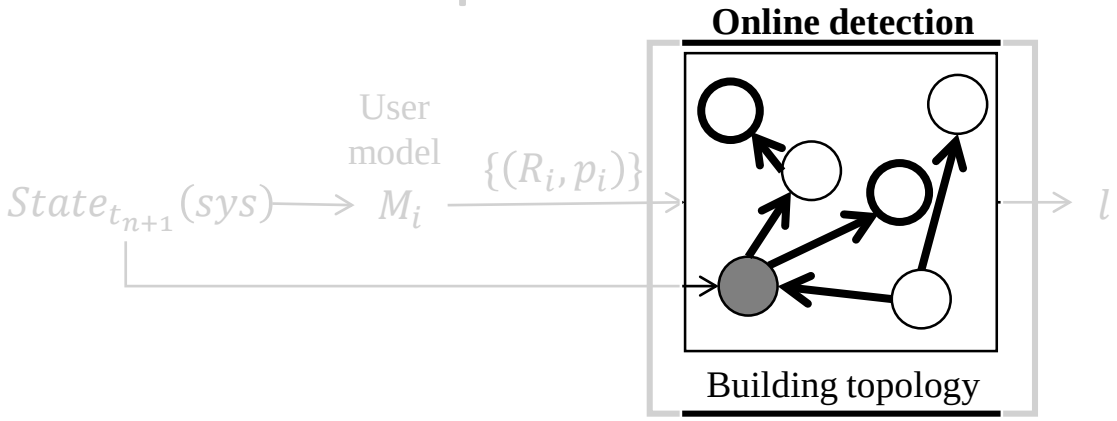
Offline phase – behavior model

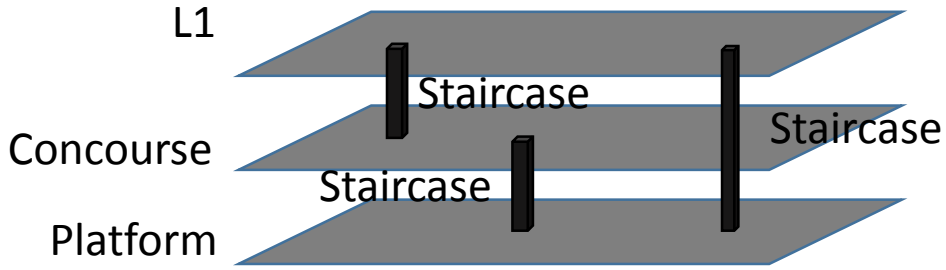


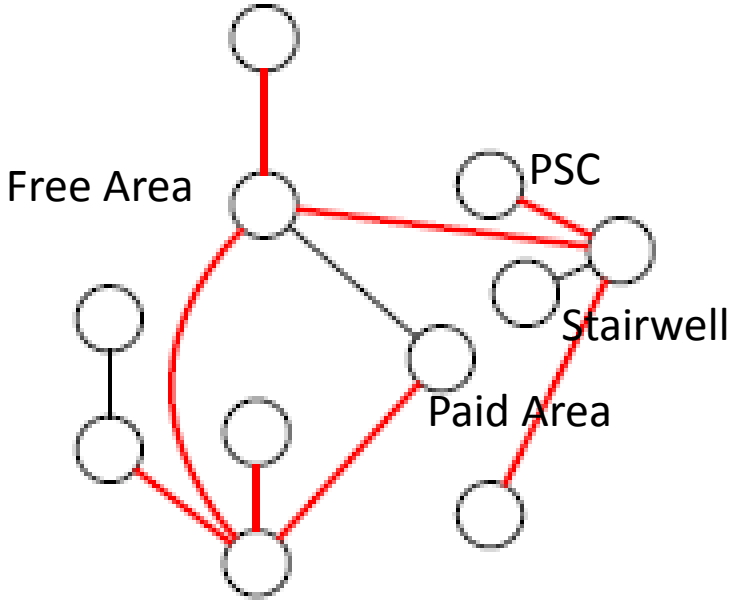


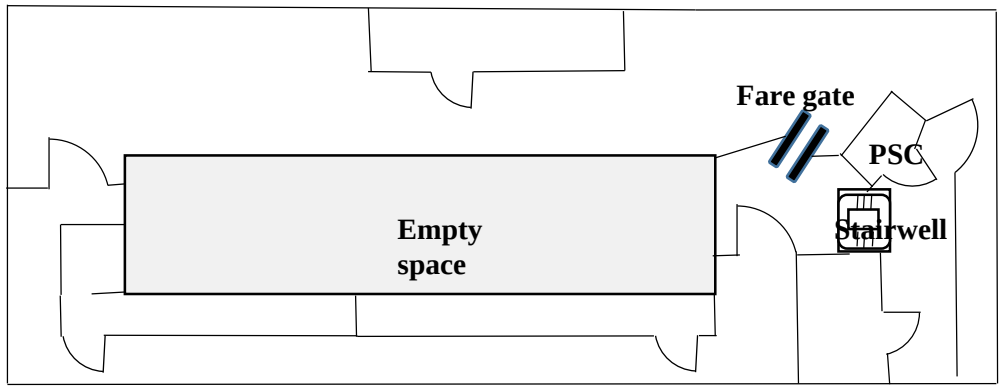
- t_1
  - Markov model (states are rooms, transition rates are frequency)

Online phase

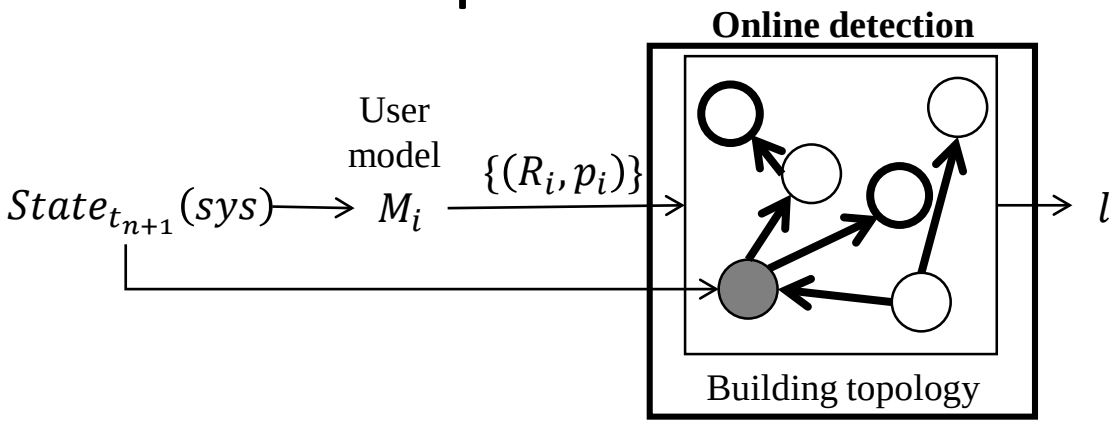




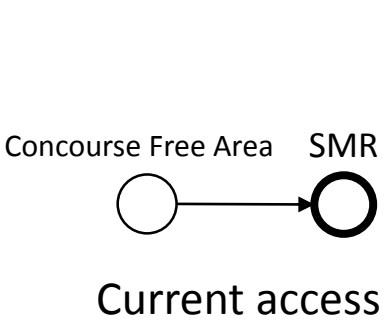


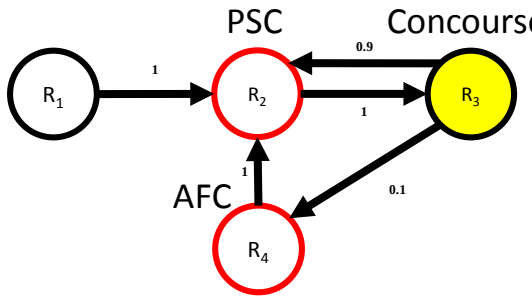


Online phase

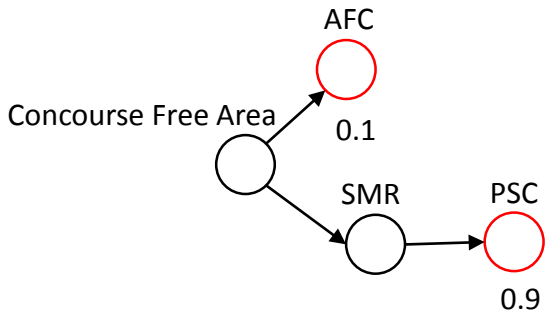


- General algorithm





Update model and return probability of entering next room



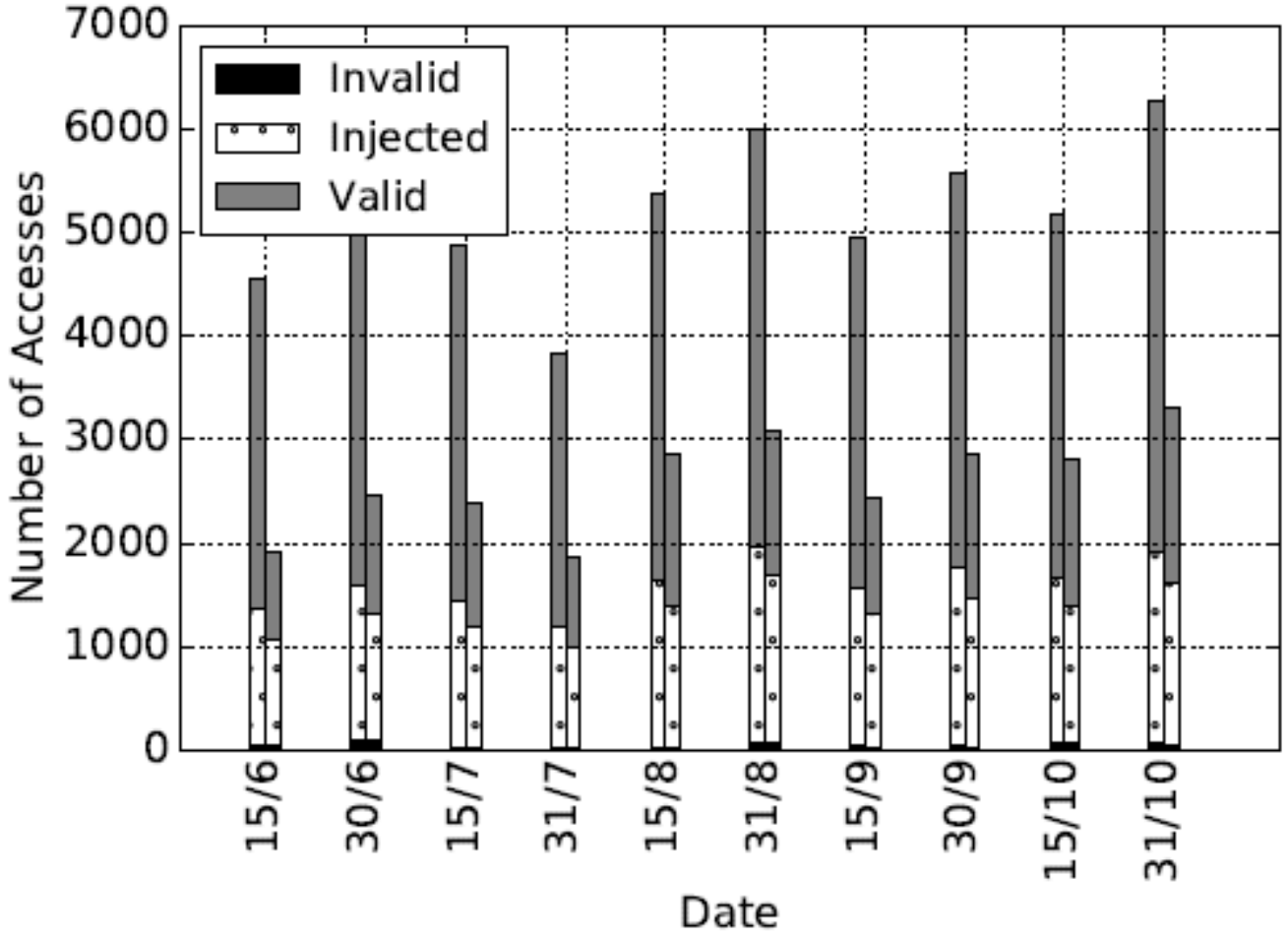
Is it likely for the user to move to this room if he moved to SMR?

Evaluation - dataset

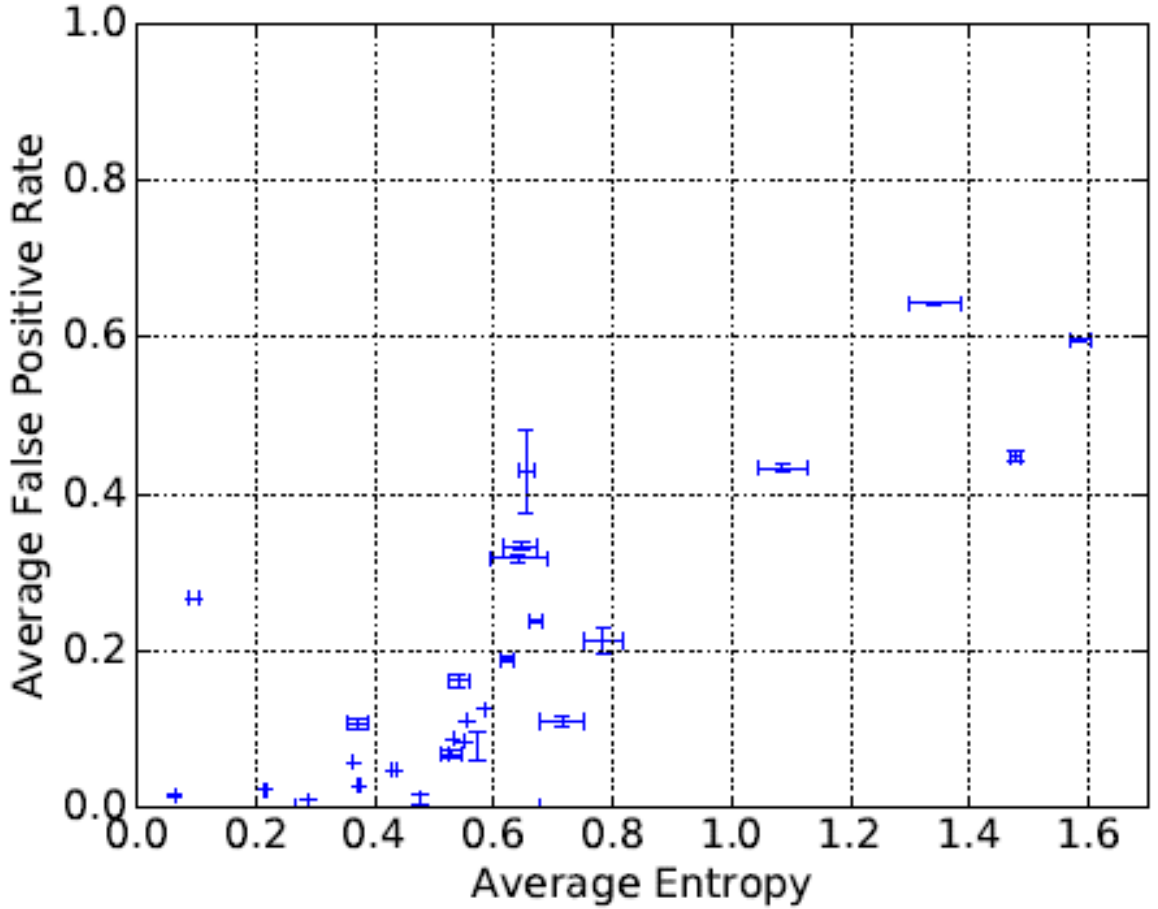
- June to October 2016
- One small station, one interchange station
- Data:
  - 1234, 00:11:22 6/4/2016, Door1, Access
  - 1234, 00:12:22 6/4/2016, Door2, Card Not Valid

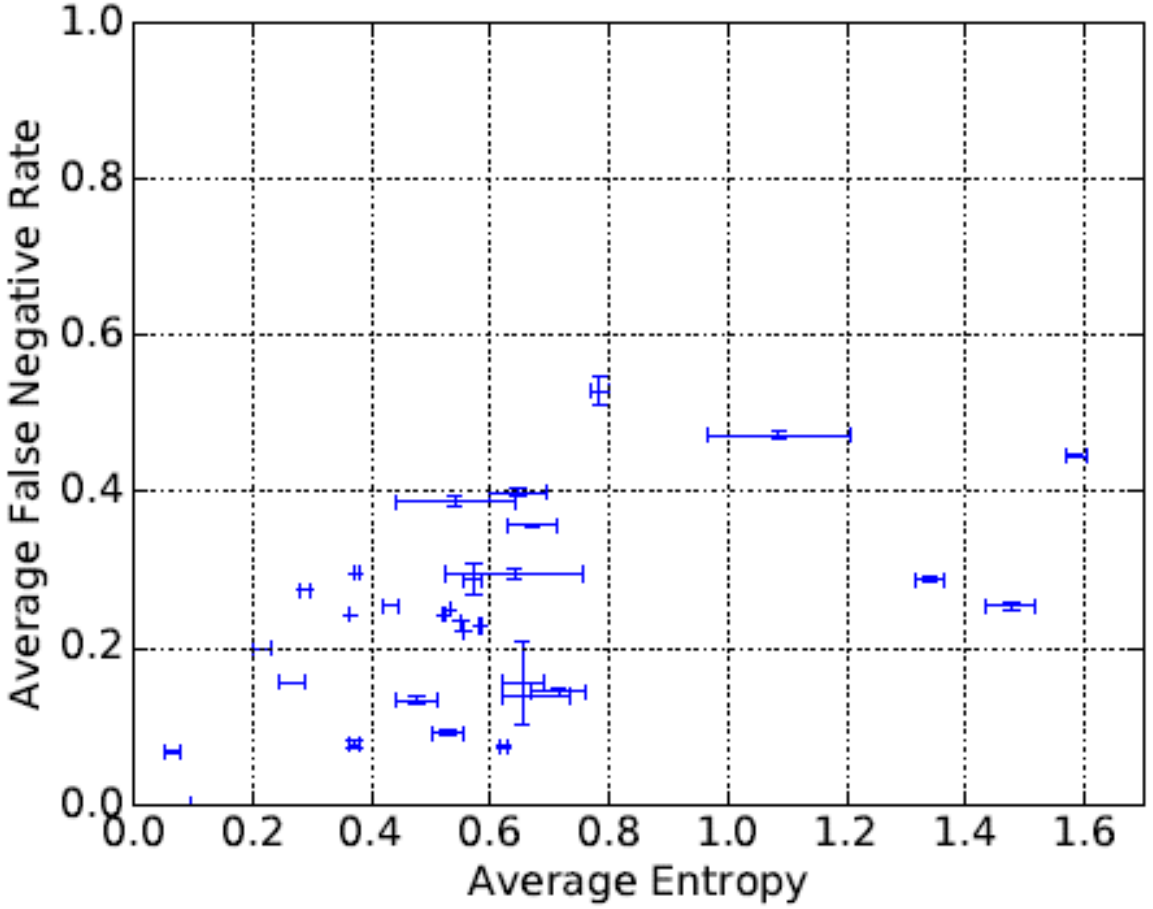
	Small station	Interchange station
# Users	366	490
# Accesses	85670	151025
# Rooms	62	55

Results – detection capability



Results – user characterization





Results – online detection

- We detect most malicious movements after their second door access
- Station layout, and user's physical movement behavior affect online detection results

Conclusion

- There is no single world view of a system
- We explore ways to model the system by using domain knowledge in combination with past data to decide the best model
- We update the model in an online manner