Introduction

Panel

Citizen Mobility and Crowd Behavior

Chair
Prof. Dr. Sandra Sendra
Universitat Politècnica de València, Spain

Mobility, Sensing, Inside, Outside, IoT

- Large spectrum
  - Mobility (citizens, devices, services)
  - Sensing (location, path tracking, health status, body-networks)
  - Inside/Outside mobility monitoring
  - Mass monitoring
  - Personalized monitoring

- Technologies
  - Accuracy
  - Target Speed
  - Real-time
  - Safety
  - Privacy
  - IoT, AI, G5/G6, Cognitive Monitoring

Overview

Chair

Sandra Sendra, Universitat Politècnica de València, Spain

Panelists

- **Pascal Urien**, Telecom Paris, France
    - Can we Trust Internet of Things without Software Integrity Insurance?
- **Mayank Maheshwari**, Hughes Systique Corporation, India
    - Wi-Fi Device Localization in an Indoor Environment
- **Michael Spranger**, Hochschule Mittweida, Germany
    - Group Dynamics in a Networked World and their Influence on Real Events
- **Sergio Ilarri**, University of Zaragoza, Spain
    - Data Management to Help Citizens in Their Daily Life

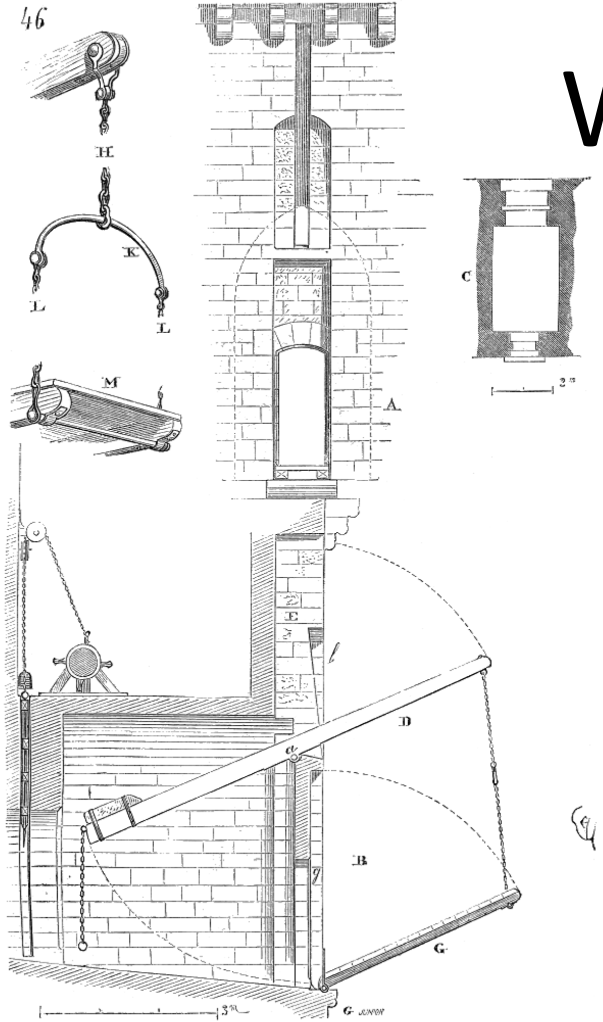
Can you trust internet of things without software integrity insurance?

Pascal.Urien@Telecom-Paris.fr

About the Internet of Things (IoT)

- Pretz, K. (2013). “The Next Evolution of the Internet”

The ***Internet of Things*** (IoT) is a ***network*** *of* ***connected things***.



What is a Thing?

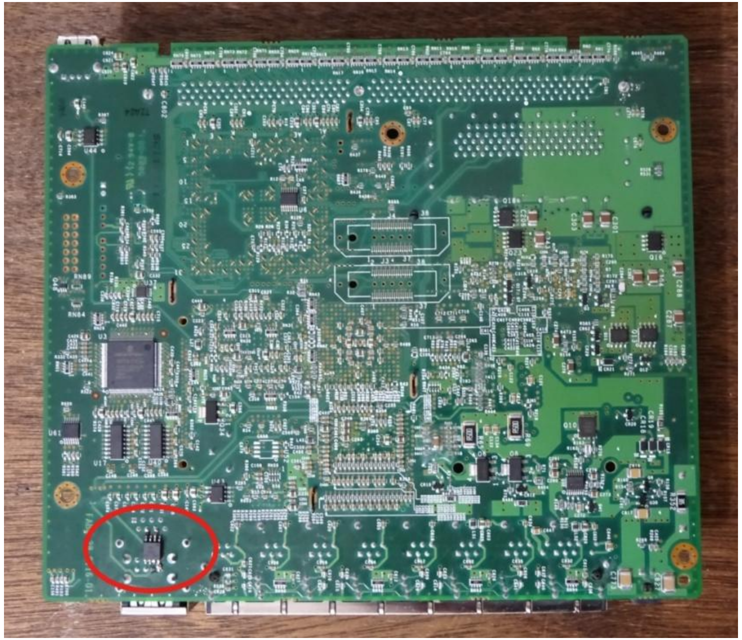
- A computer
  - CPU
  - Memories (RAM, ROM, EEPROM, FLASH…)
  - IO buses
- With at least one network interface
  - Wi-Fi, Bluetooth, ZigBee…
- Equipped with sensors and actuators

How to you know that a thing is the thing you believe it is ?

- Hardware Integrity
- Software Integrity

Giuseppe Arcimboldo,
The Greengrocer 1585

IMPLANT



MALWARE

MIRAI WORM, 2016
145.607 cameras,
1 terabit/s
35,000/50,000 HTTP request/s
25,000 IP adresses, More than 100 countries

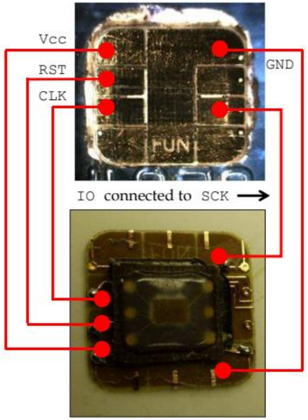
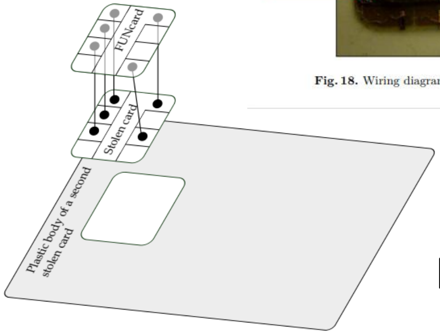


Fig. 18. Wiring diagram of the forgery.



RELAY

Monta Elkins, Nation-State Supply Chain Attacks for Dummies and You Too, CS3sthlm, 2020

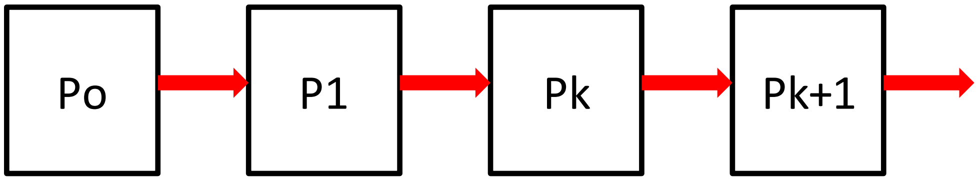
"When Organized Crime Applies Academic Results A Forensic Analysis of an In-Card Listening Device"
Houda Ferradi, Rémi Géraud, David Naccache, and Assia Tria, October 2015, Journal of Cryptographic Engineering

Software Integrity

- Local Attestation: is it possible for a software to self check its integrity ?
- Can you solve h(P) = h(prefix | h(P) | suffix) ?
- Can you trust secure boot ?

Who check Po ?

Pk: Check P_{k+1} hash
Load P_{k+1}



Remote Attestation

- *R~~emote attestation~~ bMAC is a process whereby a trusted entity (verifier) ~~remotely~~ measures internal state of a untrusted possible compromised device (prover).*
- *The ~~ICE~~ bMAC verification function is a self-check ~~summing~~ hash code, i.e. a sequence of instructions that compute a ~~checksum~~ fingerprint over themselves in a way that the ~~checksum~~ MAC would be wrong or the computation would be slower if the sequence if instruction is modified*
- bMAC computes a fingerprint of a set of memories (m) such as FLASH, SRAM, EEPROM, according to a pseudo random order, fixed by a permutation P.

$$bMAC(P) = h(\,A(P(0)\,||\,A(P(1)||\ldots||\,A\big(P(i)\big)\ldots||\,A(P(m-1)\,)$$

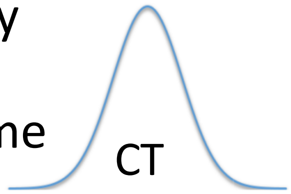
Asokan, N. et al. "ASSURED: Architecture for Secure Software Update of Realistic Embedded Devices.". IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 37.11 (2018): 2290-2300.

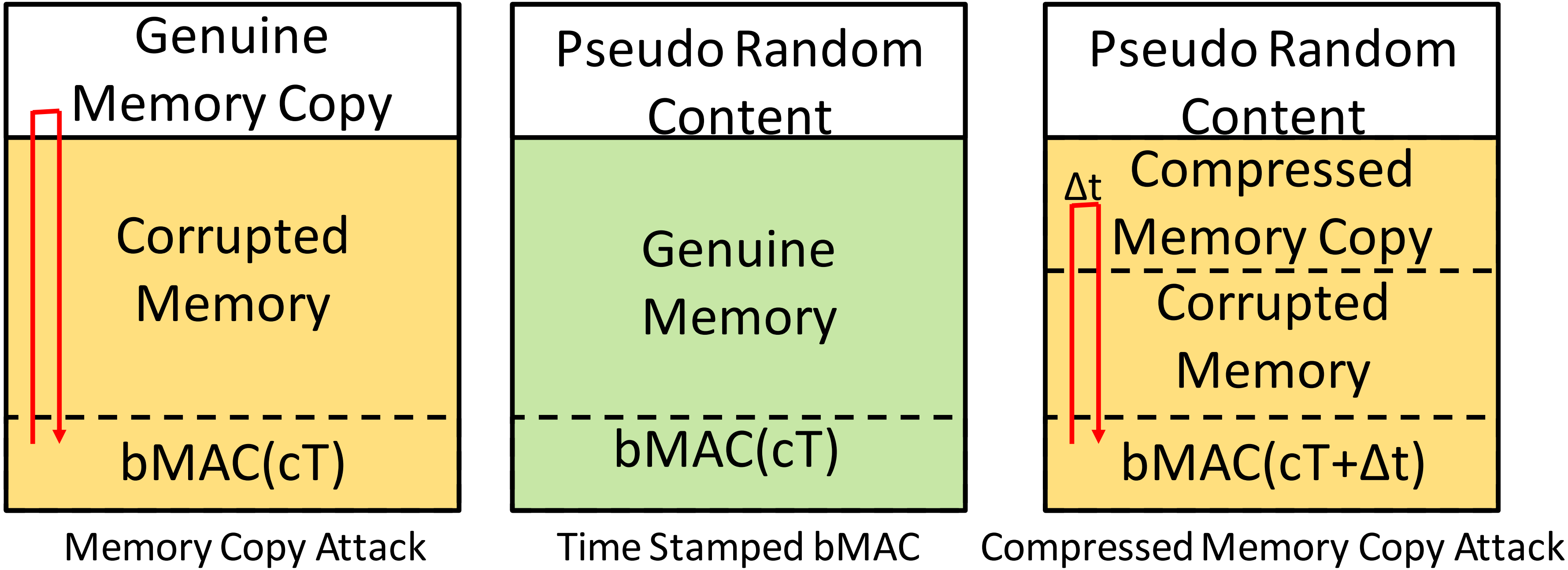
Seshadri, A. et al. "SCUBA: Secure Code Update By Attestation in sensor networks.", in Radha Poovendran & Ari Juels, ed., "'Workshop on Wireless Security" , ACM, , pp. 85-94 (2006).

Urien, P "Proving IoT Devices Firmware Integrity with Bijective MAC Time Stamped", IEEE WF-IOT-2020

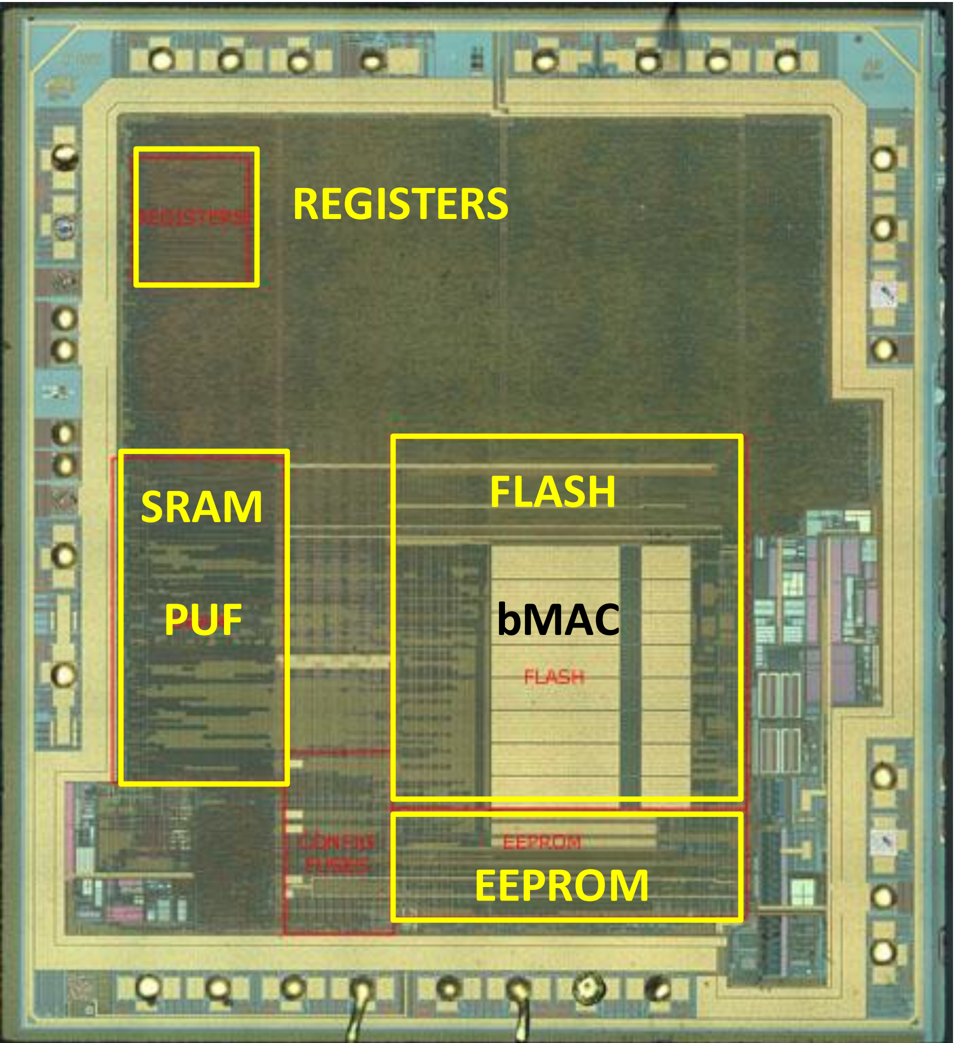
bMAC Security & Time Stamped bMAC

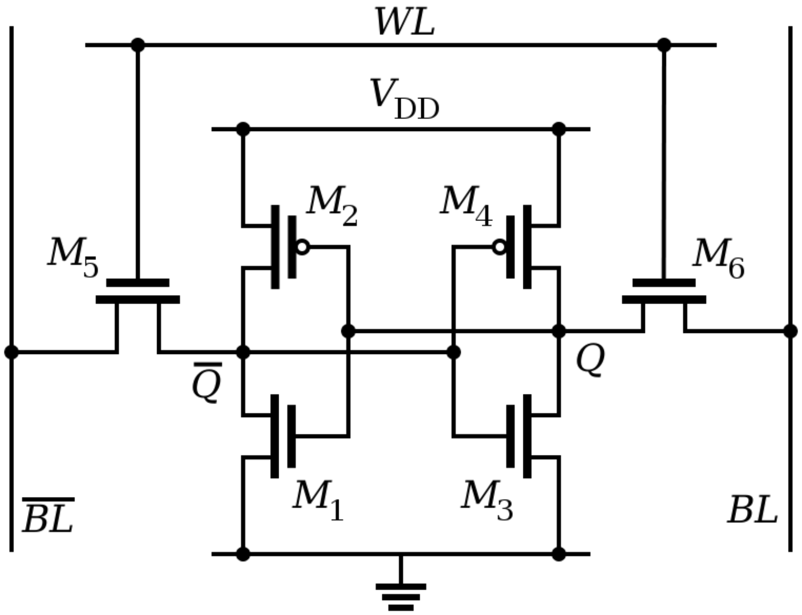
- bMAC fills all unused memories (FLASH, SRAM, EEPROM,...) by pseudo random content
- bMAC_TS = Time Stamped bMAC = bMAC exor ComputingTime = bMAC exor cT





Static RAM PUF

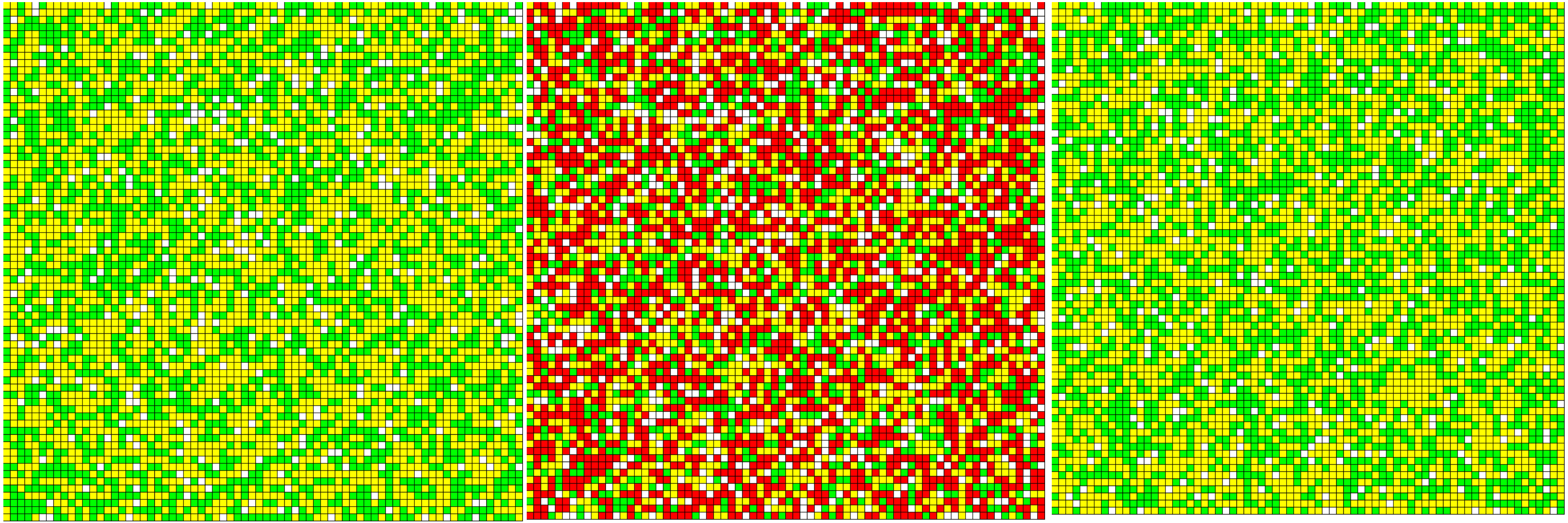




4823 bits (93%)
1: 45% - 0:55%

Common Domain 4517 bits
Match: 2324 (51 %) – NoMatch: 2193 (49%)

4856 bits (93%)
1:46% - 0: 54%

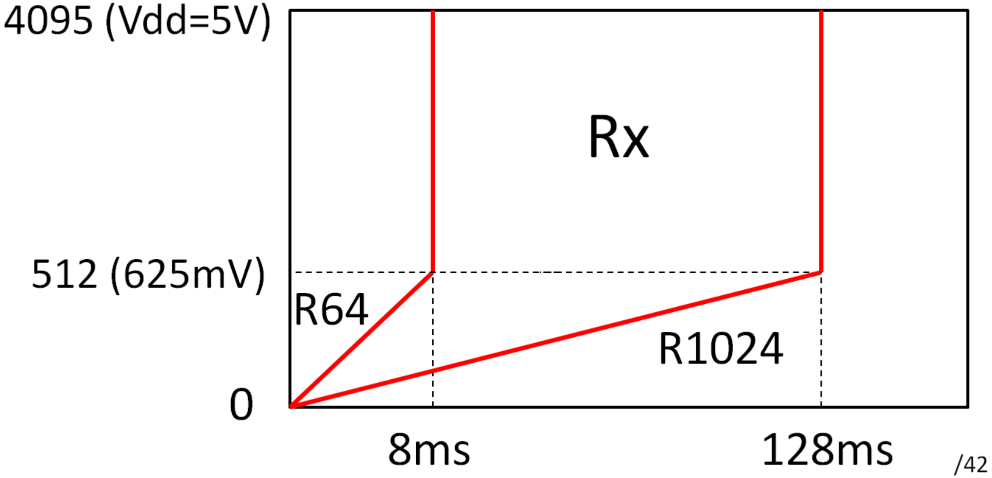


DEVICE#1
250 MEASURES

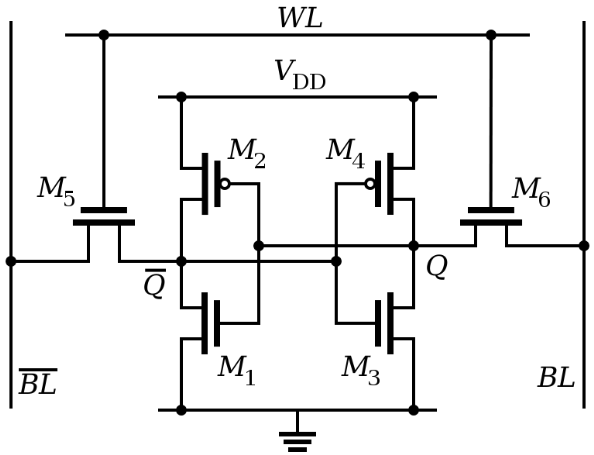
Flipping bits, red
H match, green
L match, yellow
Other, white

DEVICE#2
250 MEASURES

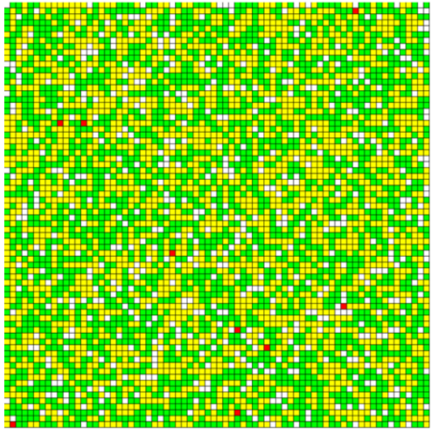
Dynamic PUF



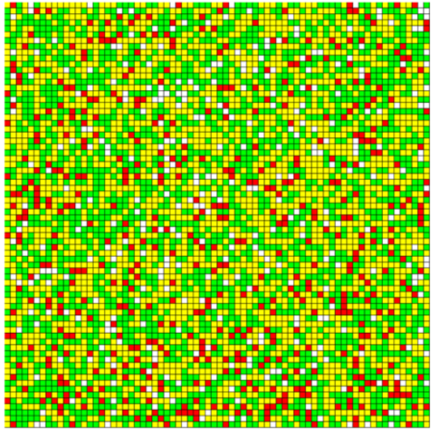
Power-Up Waveform



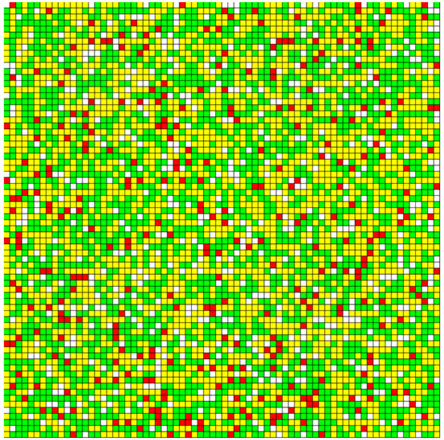
Some PUF bits are dependant on the power-up rising time



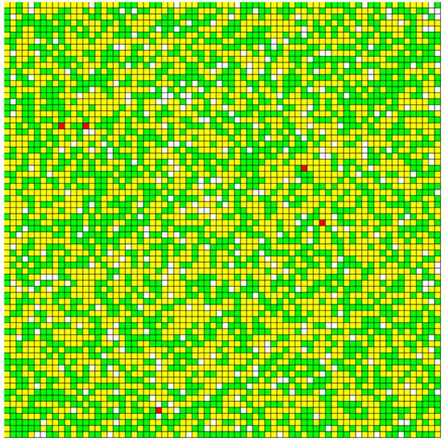
R^{1}_{64} / S^{250}_{64}



R^{1}_{64} / S^{250}_{1024}



R^{1}_{1024} / S^{250}_{64}



R^{1}_{1024} / S^{250}_{1024}

Luke has SRAM contents for two Rx power-up waveforms: R64 and R1024.

The R64 SRAM content has about 200 flipping-bits.

These contents are determined at low voltage (512mV), before Luke and Vador have a digital life.

Vador and Leia know these SRAM contents. In order to authenticate Luke, Leia uses power-up waveforms either R64 or R1024, in a random order.

Luke will always produce the right response, while Vador will make a random choice; so after n tries so probability of zero error for Vador will be 1/2^n…

Wi-Fi Device Localization in an Indoor Environment Using Graph Mapping

Abheek Saha
Abheek.saha@hsc.com
Hughes Systique Corporation

Mayank Maheshwari
Mayank.maheshwari@hsc.com
Hughes Systique Corporation

Abheek Saha

Interested in applications of mathematical modelling and optimization in the real world

Mayank Maheshwari

Interested in Wi-Fi and Bluetooth based Indoor positioning systems

Motivation

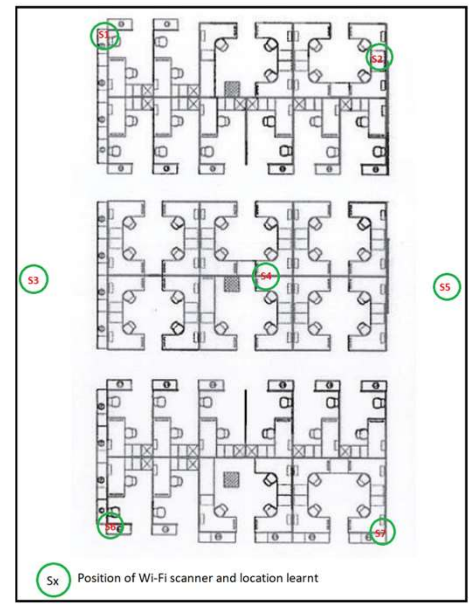
- What are we doing here?
  - Our interest is in the study of crowds in indoor locations using sampled position data
- Key points
  - Why crowds?
    - Security
    - Distancing in the era of CoVID 19
    - Modeling of crowd movement
    - Identification of 'hotspots' and 'coldspots'
  - Mass behavior
    - We are not interesting in collecting movement of individual users
    - We don't want to track or keep data regarding individuals

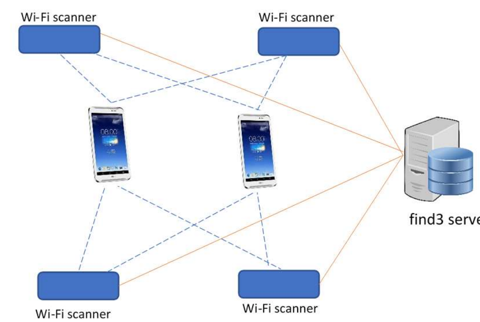
Prior Art

- Cellular Based
  - Accuracy is low, generally in the range of 50-20 meter
- Bluetooth
  - Smaller range as compared to Wi-Fi
- UWB
  - High accuracy
  - Not available in most of the mobile phones so not suitable for crowd tracking
- Wi-Fi based lateration techniques
  - Time of Arrival and Time Difference of Arrival
    - Requires time synchronization between Wi-Fi transmitter and receiver or among receivers
    - Very accurate measurement of time of Time of arrival or Time difference of arrival
  - RSSI Propagation loss model
    - RSSI propagation loss model is used to calculate distance between transmitter and receiver
    - Distance between transmitter and three or more receiver is used to find the location of the transmitter
    - These techniques do not work very well because of multipath in the indoor environment

Location patterning using RSSI fingerprinting

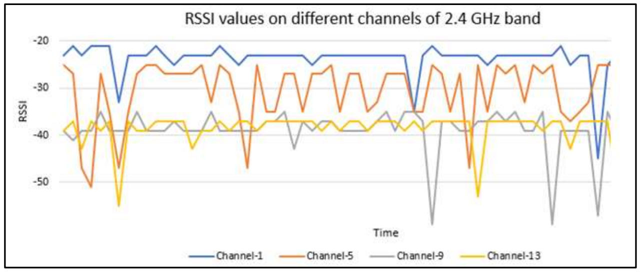
- Location patterning technique is based on the sampling and recording of radio signal patterns in specific environments
- Location patterning techniques fundamentally assumes that each potential device location ideally possesses a distinctly unique RF “signature”
- Location patterning solutions typically base such signatures on received signal strength (RSSI). This technique involves two phases
- Calibration
  - RSSI data is collected to determine the RF signatures of desired locations
  - RSS values associated with the device are recorded into a database known
  - Because of fading and other phenomena, the observed RSSI of a device at a location is not static but vary over time. As a result, multiple samples of RSSI for a device are collected during the calibration phase.
  - RSSI signature DB is used to training various ML classifier algorithms
- Tracking
  - Group of receiving sensors provide signal strength measurements of tracked the mobile device and forwards that information to a location tracking server
  - The location server uses a trained ML algorithms and the RSSI signature to estimate the location of the device

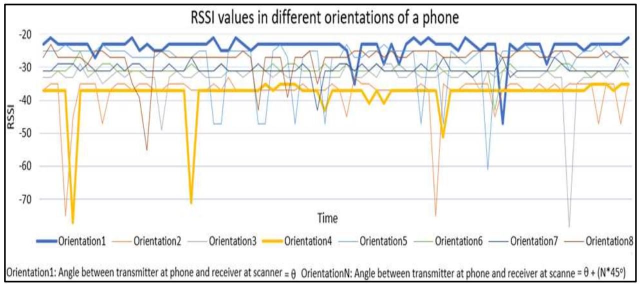


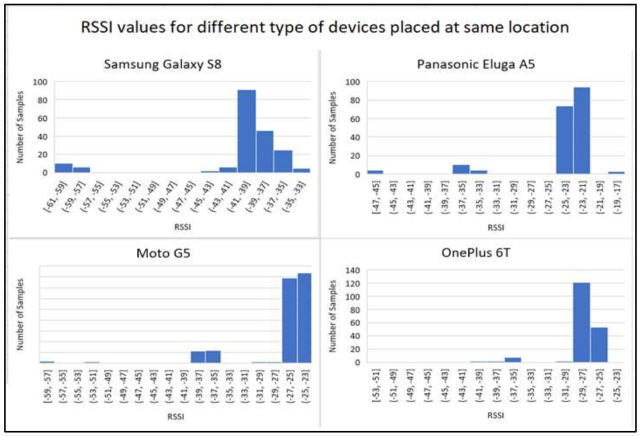


Challenges of Indoor Position Determination

- Dependency on Wi-Fi Channel
  - Considerable difference in RSSI values of probes on different channels, even when the location of the Wi-Fi transmitter and Wi-Fi receiver remains the same
  - So Wi-Fi RSSI based indoor localization system should account for RSSI differences on different Wi-Fi channels.
- Dependency on device orientation
  - RSSI values change significantly with the change in device orientation without any change in device location
  - The angle between Orientation1 and Orientation4 was 180^0, and RSSI values on these two orientations differ by about 18 dB
- Dependency on device orientation
  - RSSI values change significantly with change in Wi-Fi device type. Graph shows that average RSSI value from OnePlus 6T (-27 dB) and average RSSI value from Motorola G5(-39 dB) differ by about -12 dB
  - If the type of the device used during calibration is different from device used during tracking, the accuracy of the prediction deteriorate







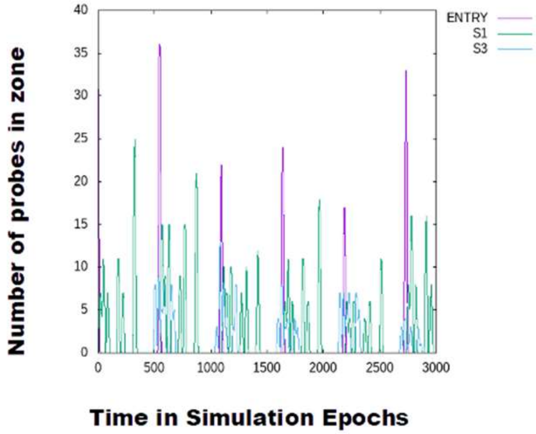
ML Algorithms

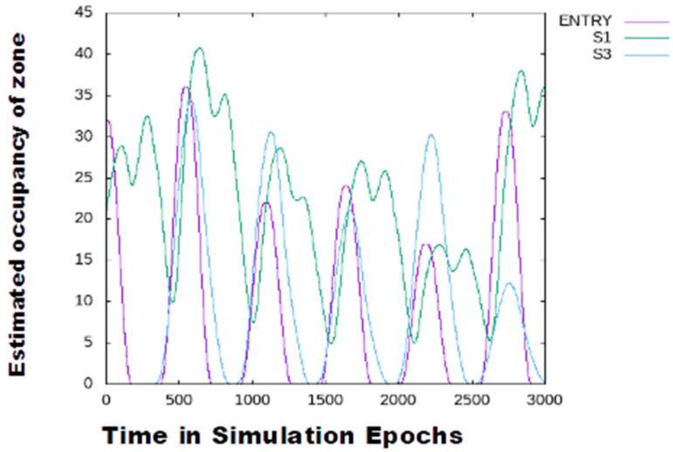
- We used the Machine Learning package find3 for location prediction
- The find3 package runs multiple machine learning algorithms in parallel then chooses the best among them using the Youden's J statistic diagnostic metric
- Algorithms used include include the K-nearest neighbor, linear SVM, Decision tree, Random Forest, and Extend Naive Bayes
- Using the labeled data provided, each algorithm is trained with a subset of the data and then tested using the remaining part of the data. The prediction is in the form of a probability factor *PL* for each location *L*. Based on the predictions by ML algorithms Youden's J statistic is calculated for each location and each ML algorithm
- We obtained more than 80% prediction accuracy on all of these devices, within a 3 meter radius of the calibration positions
- In future we would like to refine the algorithm to handle incomplete input i.e. the situation when a probe request is not received by all the Wi-Fi scanners
- Retraining of the ML for each change in interior topology is CPU intensive and slow; hence, we would like to find ways to augment existing algorithms for minor changes, rather than retrain the entire ML

Find3 -https://github.com/schollz/find3

From Raw Data to Occupancy

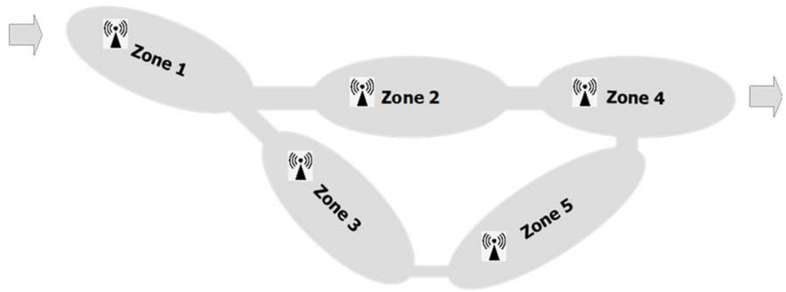
- Despreading
  - Converting sampled time-series data to continuous measures
- Modelling
  - Parameter identification
  - Identification of the state space
  - Modelling of mass behaviour
- Verification
  - Mapping of mathematical model against real world data
  - Boundary conditions

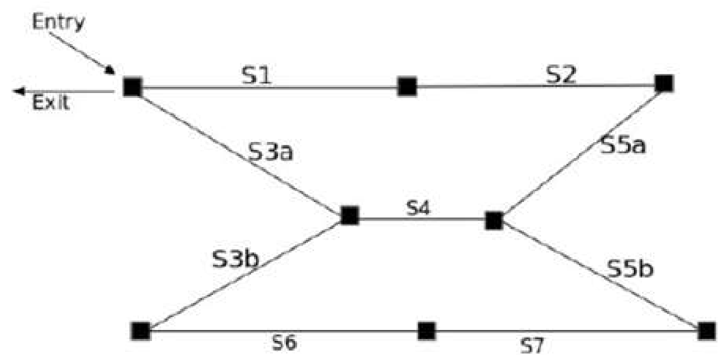




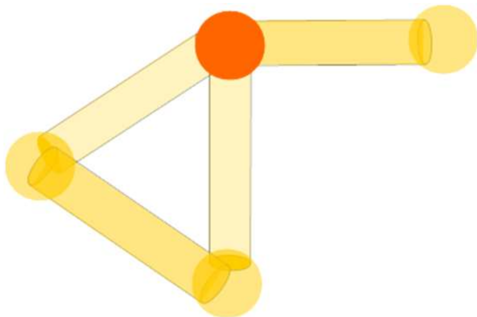
Crowd Modelling in an Indoor Area

- Methodology
  - We consider an indoor arena as a set of zones connected by passages
  - The obvious mathematical model is a graph
    - Position is always measured in terms of a specific zone
    - To increase the zones, we increase the number of Access Points
    - We will predict crowd behaviour in terms of occupancy of edges
      - A zone maps to an edge
      - A hotspot is when an edge contains a large number of people etc.
  - Transition matrix ensures Kirchoff transition conditions at the nodes



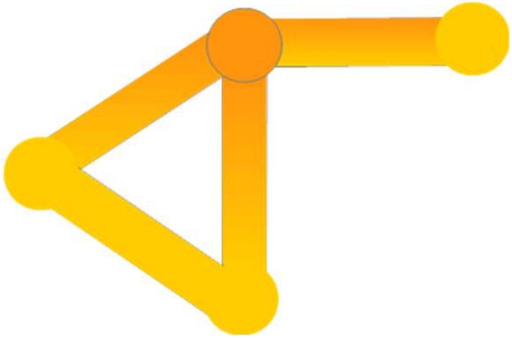


Heat Diffusion Model



Initial State: Single junction heated

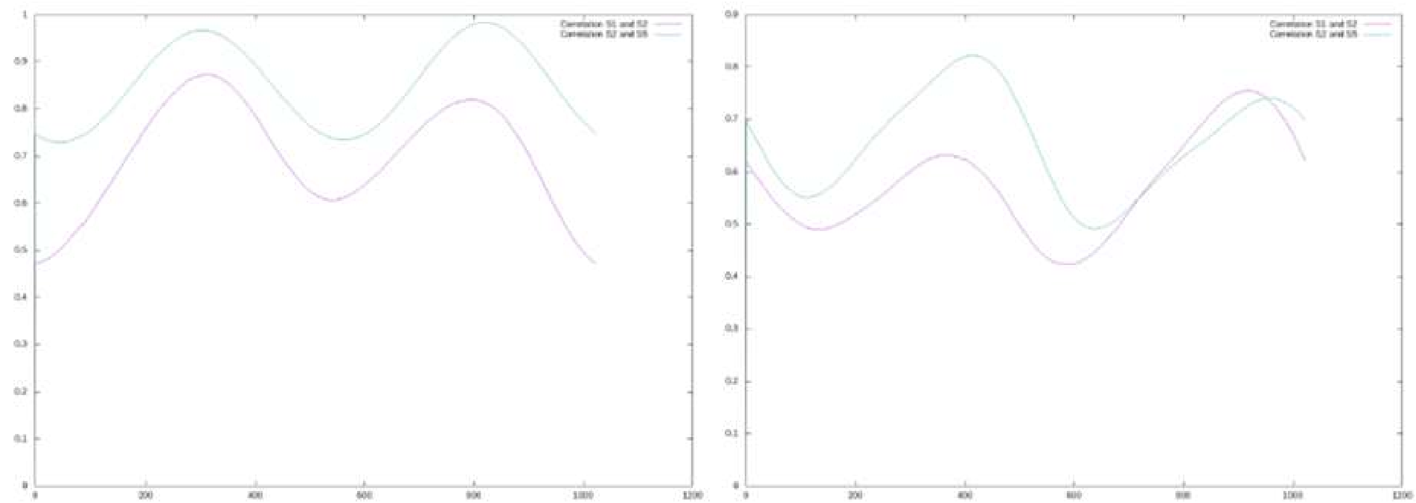
As diffusion takes place



- Crowd entering through a door is equivalent to a single junction being heated.
- The dispersion model shows us how the intensity dissipates over time.
- Its natural to dissipate from higher to lower intensity

$$\nabla^2 x^i + \eta^i \frac{\partial x^i}{\partial t} + g(x^j) = 0, j \in Inc(i)$$

Mass behaviour



(a). Correlation between adjacent edges - phone always on (b). Correlation between adjacent edges - random probing intervals

- We track correlation between occupancy of adjacent paths
  - For each path in the graph we can compare predicted occupancy vs actual occupancy over time.

Thank you

HOCHSCHULE
MITTWEIDA
University of Applied Sciences

Panel Datasys 2020

Group Dynamics in a Networked World and their Influence on Real Events

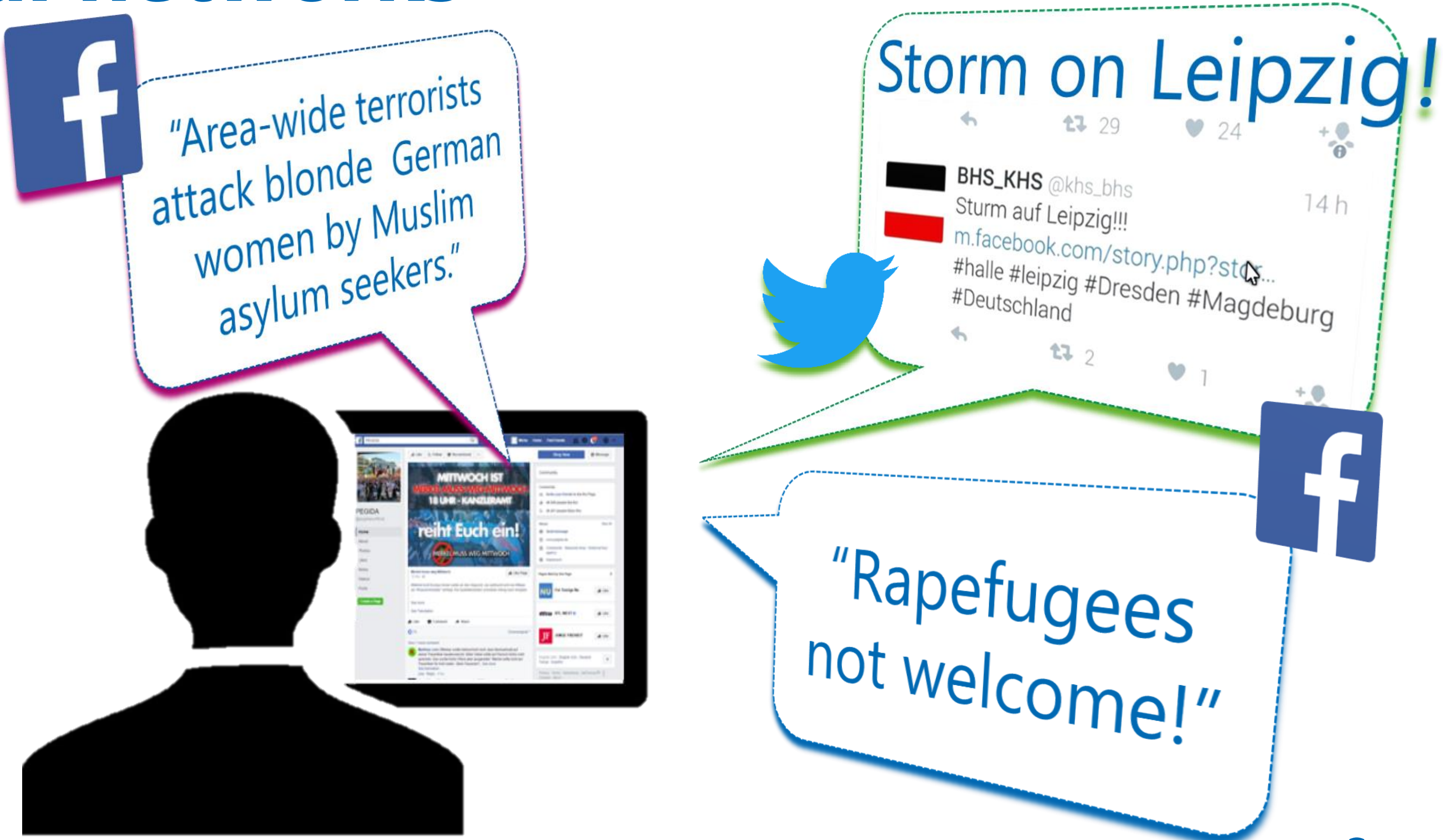
Michael Spranger

Real and Virtual World are Connected

Rioting in the wake of demonstrations, sporting events or as a result of political dissatisfaction often becomes **apparent in advance in the social media**.

Terrorists often **recruit** their future **assassins** via **social networks**. **Amok** runners often **signal** their readiness in **social networks**.

Rioters often announce themselves in social networks

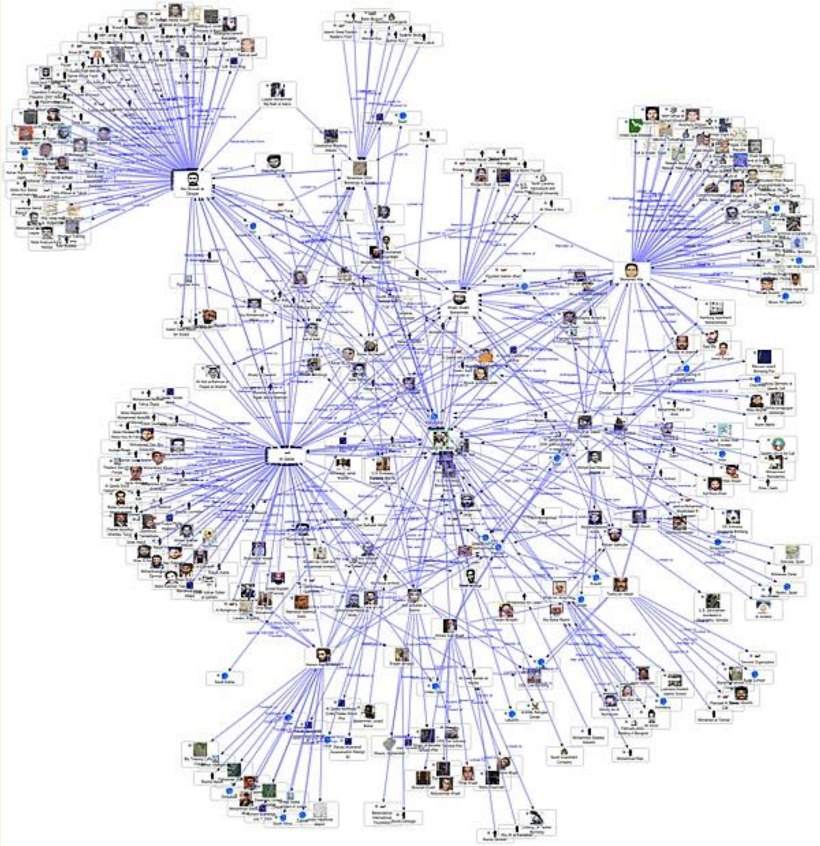


HOCHSCHULE MITTWEIDA

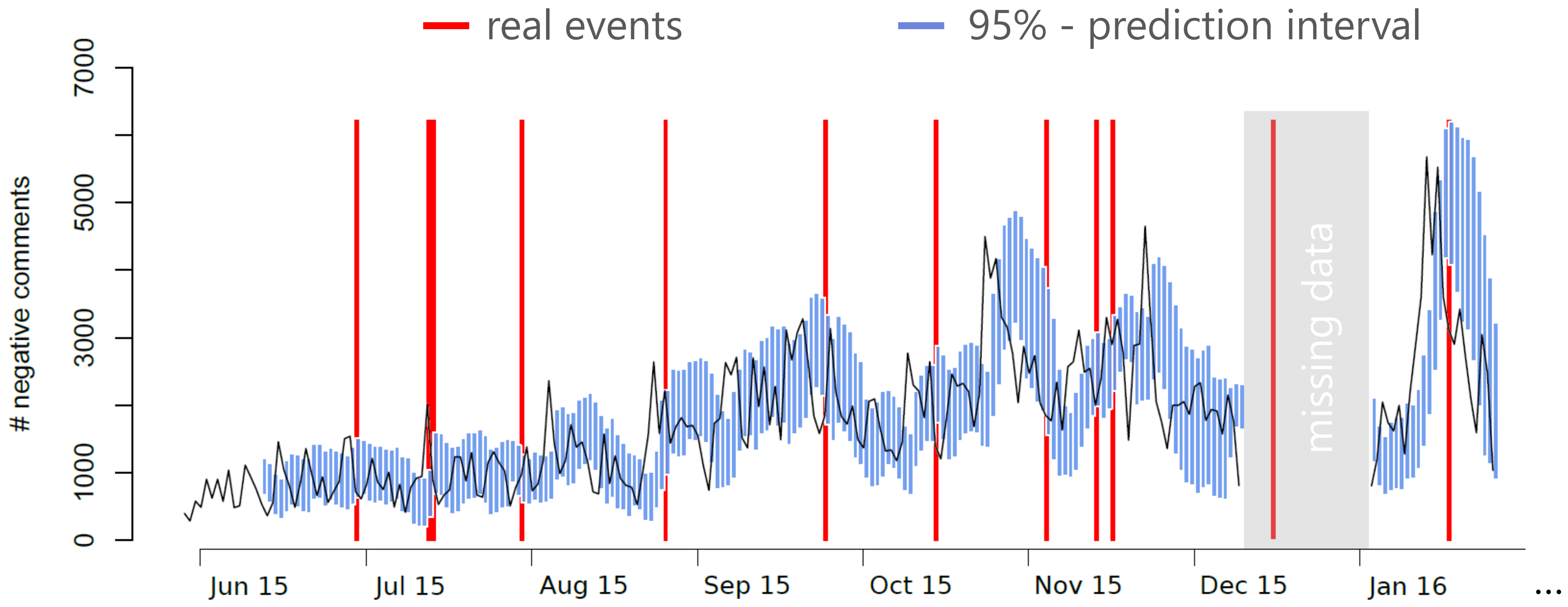
Virtual Communities

- no physical contact necessary
- larger networks through a higher range
- fast, immediate accessibility
- supposed anonymity enables more open communication
- faster growth of emotions

emotional, public discussion



Prediction of events through sentiment analysis

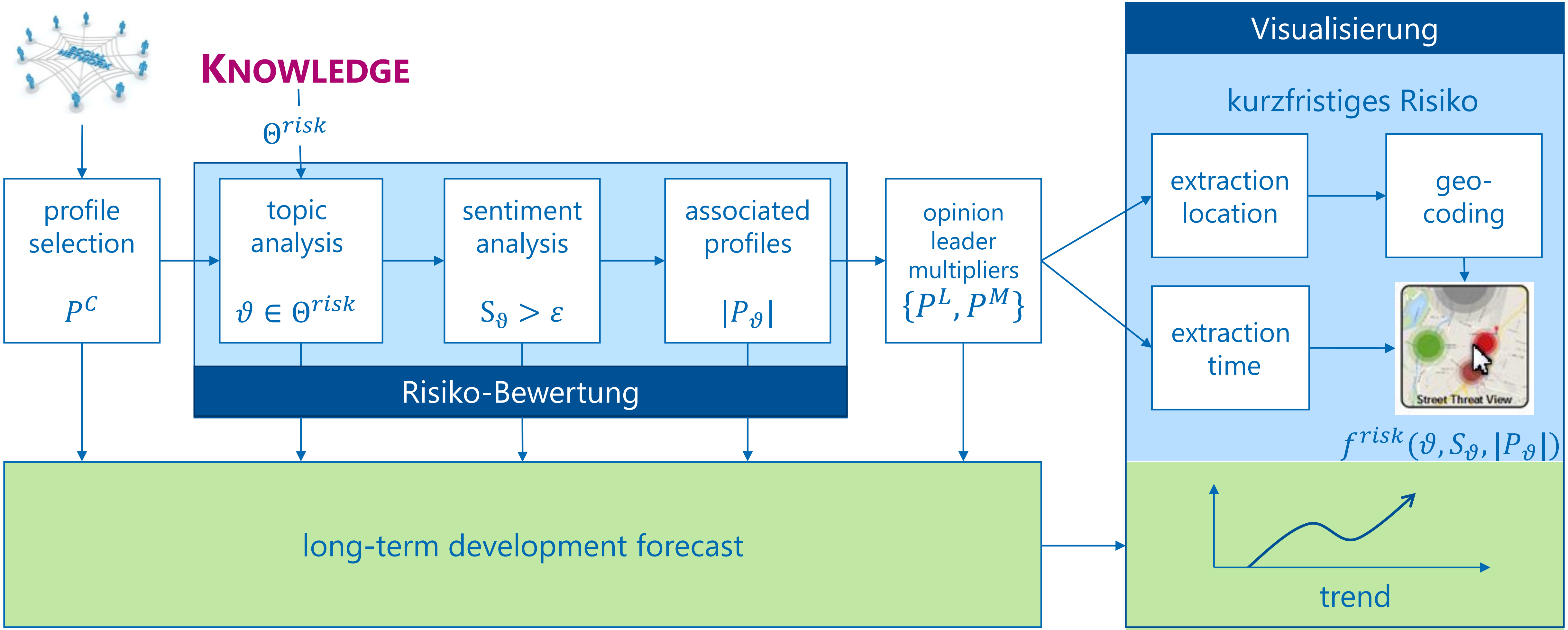


Sentiment scores of the Facebook page of Pegida e.V.

Cooling phases often mark real events

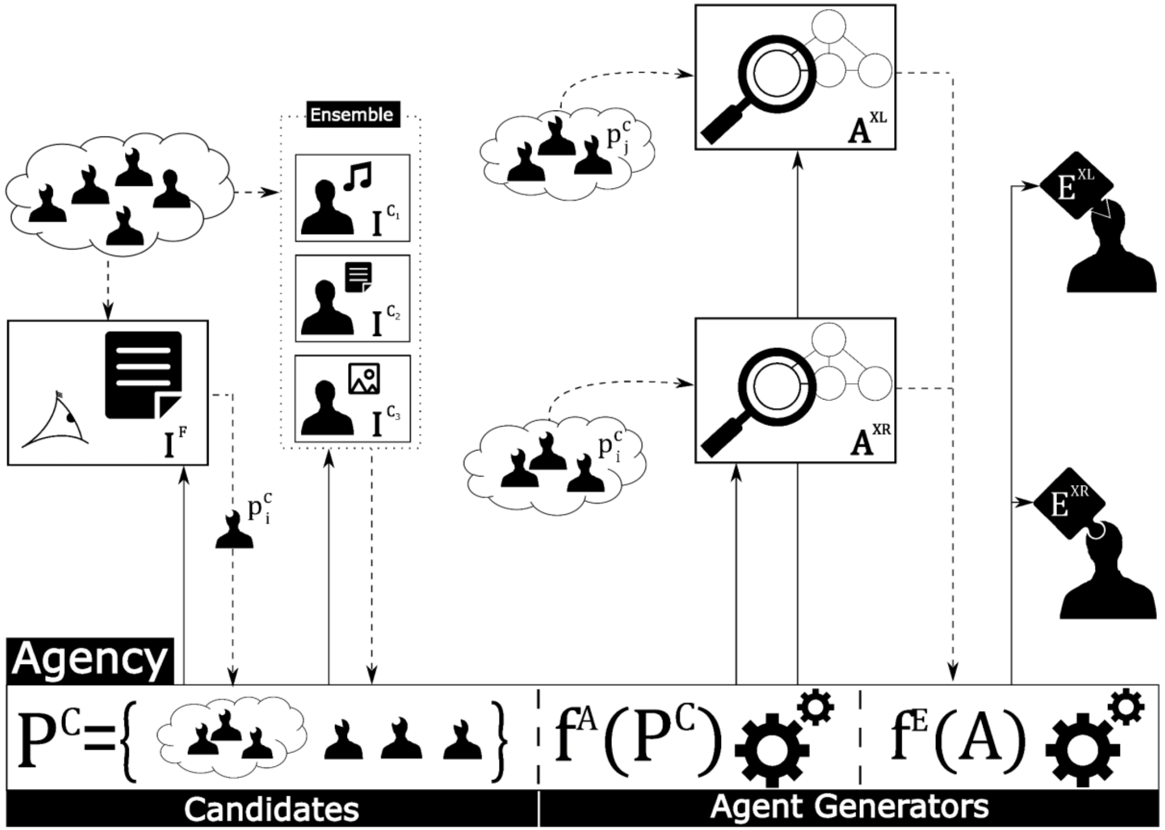
HOCHSCHULE MITTWEIDA

Process model for hazard prediction



HOCHSCHULE MITTWEIDA

Agent-based analysis of social networks



Actors of an artificial immune system for social networks

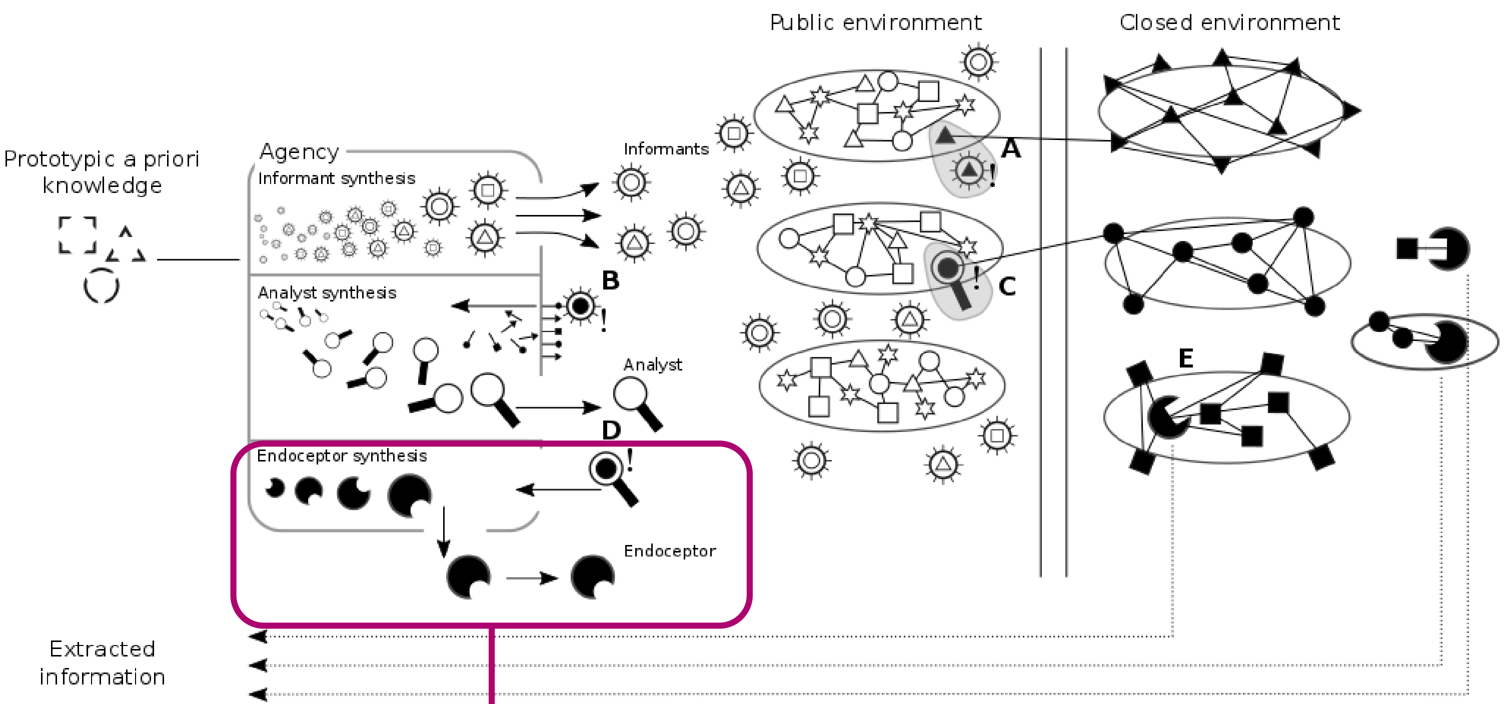
Scoring function

$$r(p_i^c) = \lambda \frac{count(I^o, p_i^c)}{\sum_{p_j \in P^c} count(I^o, p_j^c)} + (1-\lambda)\frac{1}{|I^{c_j}|}\sum_{j=1}^{|I^{c_j}|} w_j I^{c_j}(p_i^c)$$

Activation function

$$\alpha_A(p_i^c) = \begin{cases} 1, & if\ r(p_i^c) > \epsilon \\ 0, & sonst \end{cases}$$

An Artificial Immune System



Activities in an artificial immune system for social networks (process view)

Which profiles should be contacted ?

Profiles with a high CompetenceRank!

Conclusion

- **Connection** between real and virtual world
- Virtual groups can mobilize **larger numbers of individuals in less time**
- Discussions are **emotionally charged**
- Emotions are **measurable**
- **Transfer to the real world** observable
- Usable for the development of **prediction tools**
- Ultimate goal -> an **artificial immune system for social networks**

Questions?

Feel free to contact me:
spranger@hs-mittweida.de

HOCHSCHULE MITTWEIDA
University of Applied Sciences

Data Management to Help Citizens in Their Daily Life

Sergio Ilarri

silarri@unizar.es

University of Zaragoza (Spain)
COS2MOS Group (http://cos2mos.unizar.es/)

DataSys 2020 Panel "Citizen Mobility and Crowd Behavior (Tracking, Safety, Heath)"

Introduction

- The development of suitable data management techniques to help citizens in their daily life is more important than ever
  - Lots of data, mobility challenges, our society is changing (impact of COVID-19), …
- In this panel, I will provide a high-level overview of some of the efforts that we are developing at the University of Zaragoza
  - Project “Data 4.0: Challenges and Solutions”
    - Project TIN2016-78011-C4-3-R (AEI/FEDER, UE)
  - Project “TRAFAIR: Understanding Traffic Flows to Improve Air Quality”
    - Project 2017-EU-IA-0167, co-financed by the Connecting Europe Facility of the European Union
  - COSMOS research group
    - Government of Aragon (Group Reference T64_20R)

Project Data 4.0

- Data 4.0: the 4th revolution in data management
  - "big" and/or "smart" + requirements of new processing solutions and exploitation in demanding scenarios of a whole new range of applications
- Participation of 4 universities:
  - University of A Coruña
  - Polytechnic University of Madrid
  - University of the Basque Country
  - University of Zaragoza

Project Data 4.0

- Team at the University of Zaragoza:

  Focus on mobile computing:

  1. Data exploitation in mobile environments
     - Obtaining and exploiting useful information in wireless computing contexts
       - Evaluate the relevance of the data produced and filter them based on the user's context (location, activity being carried out, etc.)
  2. Management of the semantic heterogeneity of the data
     - Creating mechanisms that discover and make the meaning of the data explicit
       - Help users to express the type of information they seek, and consider the meaning of data to answer queries

Help users to find exactly the information they need

Mobile CARS

- Recommender systems (RS) can alleviate the user's overload
- Focus on mobile Context Aware RS (CARS)
  - They consider the context of the user (location + other context attributes) and mobile computing aspects
- Our current work on mobile CARS:
  - Push-based and pull-based RS architectures
  - Use of spatial database techniques (Re-CoSKQ)
  - Exploitation of text mining techniques
  - Prototypes
  - Generation of datasets and simulation of scenarios for evaluation

Help mobile users by suggesting them relevant items

VANETs

- Interest in the development of information systems for drivers
- Sharing and retrieval of useful information
  - Accidents, obstacles on the road, available parking spaces, etc.
- Exploitation of mobile P2P networks to exchange data directly among the vehicles + other communication technologies
- Our current work on VANETs:
  - Use of mobile agent technology for distributed data management
  - Exploitation of spatial crowdsourcing techniques
  - Development of driver-assistance systems to find available parking spaces

Help drivers to obtain the information they need

TRAFAIR

- Raising awareness among citizens and public administrations about the air quality within an urban environment and the pollution caused by traffic
- 4 academic organizations, 4 public administrations, a regional in-house providing company, and a research center: https://trafair.eu/consortium/
- Main goals:
  1. Monitoring urban air quality by using sensors in 6 European cities
     - Zaragoza (600,000 inhabitants), Florence (382,000), Modena (185,000), Livorno (160,000), Santiago de Compostela (95,000), and Pisa (90,000)
  2. Making urban air quality predictions
     - Weather forecasts and traffic flows → simulation models

Raise awareness about air quality, help citizens and public administrations

http://trafair.eu/

TRAFAIR

- Examples of tasks tackled in TRAFAIR:
  - Installation and calibration of air quality sensors and LoRaWAN antennas
  - Development of a traffic model
    - E.g., in Zaragoza: SUMO traffic simulator + historical traffic data
  - Prediction of pollutants using VEIN (Vehicular Emissions Inventories) and GRAL (Lagrangian particle model)
  - Interpolation algorithms
  - Interpolation Maps and Interactive Map Visualization
  - Development of 2 mobile apps (Android, iOS)
    - For the cities of Zaragoza, Santiago de Compostela and Modena

http://trafair.eu/

TRAFAIR

TRAFAIR Forecast

Zaragoza Trafair Team Health & Fitness

PEGI 3

Add to Wishlist

Install

The TRAFAIR Forecast application shows forecast air quality information (concerning the next 48 hours), mainly about the concentration of nitrogen oxides (NOx), for the cities of Zaragoza, Santiago de Compostela and Modena. In addition, the application offers the possibility of consulting real-time information about the concentration of other pollutants, such as CO, NO2, NO and O3. Moreover, the app includes an interactive map which allows the user to check NOx concentration in the desired city area for the next 2 days.

Acknowledgments:
-TRAFAIR project 2017-EU-IA-0167, co-financed by the Connecting Europe Facility of the European Union.
-Project TIN2016-78011-C4-3-R (AEI/FEDER, UE).

https://play.google.com/store/apps/details?id=eu.traffair.forecastapp

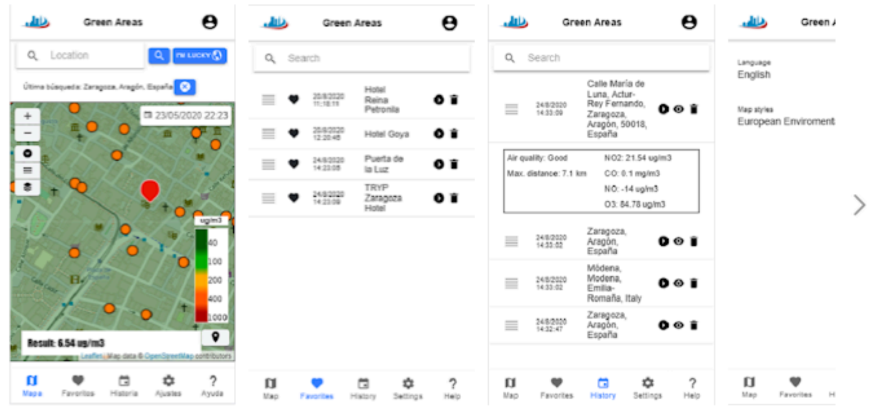
TRAFAIR Green Areas

Zaragoza Trafair Team Health & Fitness

PEGI 3

Add to Wishlist

Install



The TRAFAIR Green Areas application shows real-time information of the concentration of different air pollutants, such as NO2, CO, O3 and NO in a point of interest in three European cities: Zaragoza, Santiago de Compostela and Modena. This allows the user to know an approximation of the air quality in the desired city area. For an easier consultation of the data, it is possible to store a list of points of interest for the user as favorites, as well as to choose between different scales of colors and values for an easier visualization of the data.

Acknowledgments:
-TRAFAIR project 2017-EU-IA-0167, co-financed by the Connecting Europe Facility of the European Union.
-Project TIN2016-78011-C4-3-R (AEI/FEDER, UE).

https://play.google.com/store/apps/details?id=eu.trafair.greenareas

THANK YOU...

COS2MOS
COMPLEXITY MANAGEMENT