Usable security from ecocentric videos, implicit Fuzzy pairing and Device-free activity recognition

Stephan Sigg

Aalto University, Communications and Networking

June 27, 2016

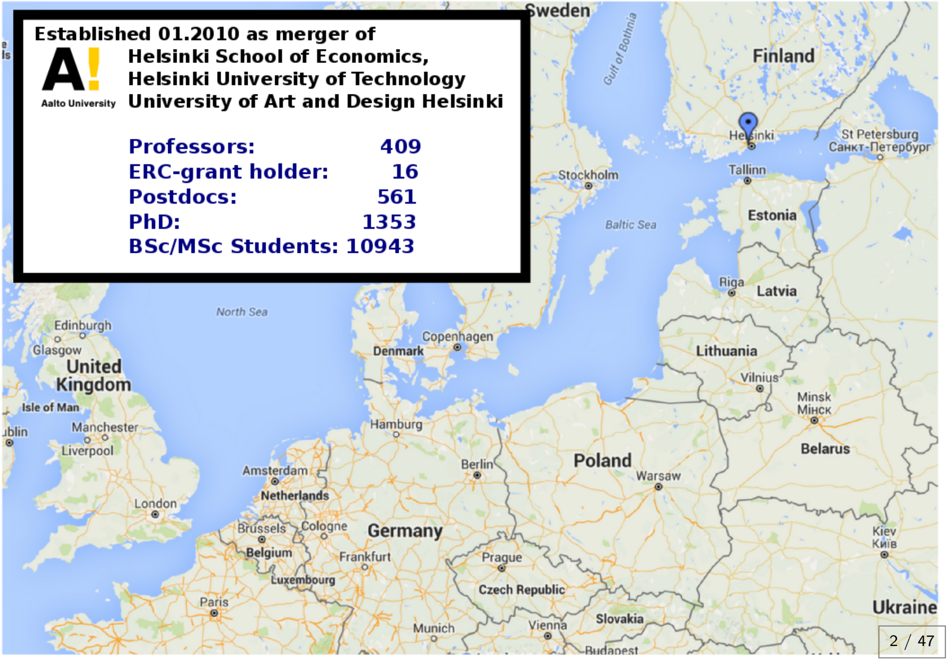

Sweden
Gulf of Bothnia
Norway
Finland
Helsinki
St Petersburg
Санкт-Петербург
Oslo
Stockholm
Tallinn
Estonia
Baltic Sea
Riga
Latvia
North Sea
Edinburgh
Glasgow
United Kingdom
Copenhagen
Denmark
Lithuania
Vilnius
Minsk
Минск
Isle of Man
Manchester
Liverpool
Hamburg
Belarus
Amsterdam
Berlin
Poland
Warsaw
Netherlands
London
Brussels
Cologne
Germany
Kiev
Київ
Belgium
Frankfurt
Prague
Luxembourg
Czech Republic
Paris
Slovakia
Ukraine
Munich
Vienna
Budapest

Established 01.2010 as merger of

Aalto University

Helsinki School of Economics,
Helsinki University of Technology
University of Art and Design Helsinki

Professors:	**409**
ERC-grant holder:	**16**
Postdocs:	**561**
PhD:	**1353**
BSc/MSc Students:	**10943**

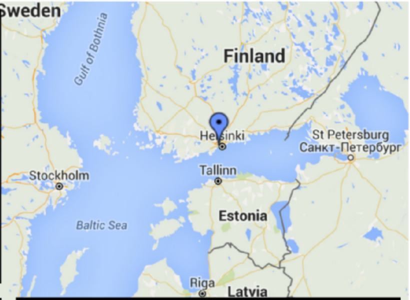


Established 01.2010 as merger of

Aalto University

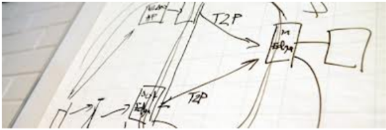
Helsinki School of Economics,
Helsinki University of Technology
University of Art and Design Helsinki

Professors:	**409**
ERC-grant holder:	**16**
Postdocs:	**561**
PhD:	**1353**
BSc/MSc Students:	**10943**



Comnet

- Personnel: ~115
- 11 + 2 Professors
- budget ~7.8 M€
  - ~ 60% external funding
- ~ 55 M.Sc thesis annually
- ~ 8 D.Sc thesis annually



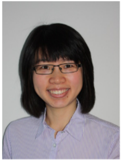
Comnet is a multi-disciplinary unit of research and higher education covering communications and networking technology, networking business and human aspects of communications. In its area, Comnet is the largest unit in Finland.

http://comnet.aalto.fi/en/

Aalto University
School of Electrical Engineering

Comnet
6/8/16
2

Professors



Xiao Yu
Networking software and applications

Stephan Sigg
Ubiquitous computing

Antti Oulasvirta
Human-Computer Interaction
(User Interfaces)

Heikki Hämmäinen
Network Economics

Juuso Töyli
Network economics
Adjunct Prof.

Jarno Limnell
Cyber security
PoP

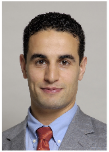
Patric Östergård
Information theory

Olav Tirkkonen
Communications theory

Riku Jäntti
Commuications Engineering
Head of department

Jyri Hämäläinen
Radio communications
Dean of ELEC

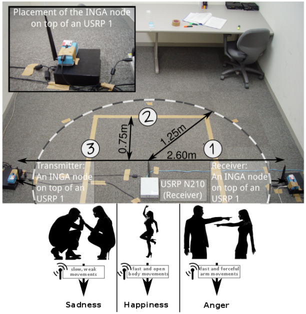
Raimo Kantola
Networking technology
Routing, trust, and privacy

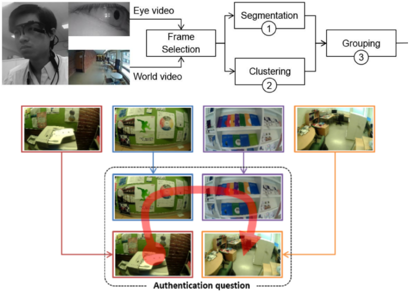


Tarik Taleb
Mobile Core Networks
Network Function Virtualization and Cloud Communications

Jukka Manner
Internet technologies
Transport

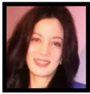
Ambient Intelligence





Stephan Sigg

Randomized Algorithms, Optimization, Usable security, Activity recognition, Machine learning, Pervasive Computing



Bahareh Gholampooryazdi

Signal processing, RF-based Device-free activity recognition

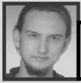
Le Ngu Nguyen

Usable Security, Activity recognition, Machine learning, Mobile applications

Muneeba Raja

Sentiment sensing, Device-Free RF-based Activity recognition, Pervasive Computing

Visitors



Dominik Schuermann

Security in DTN, Anonymity in decentralized networks, Authenticated Key Exchange, Usable security

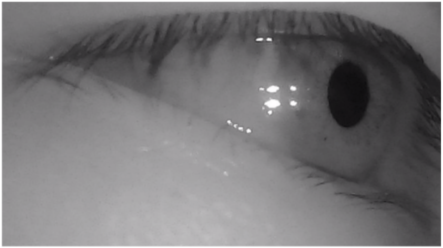
Arne Bruesch

Machine learning, Information systems, Ad-hoc secure device pairing, Inertial sensors

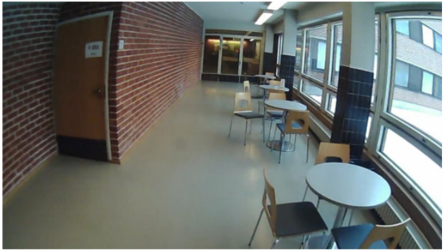
Project:

Secure authentication from an Egocentric Camera

Secure authentication from Egocentric camera



b)

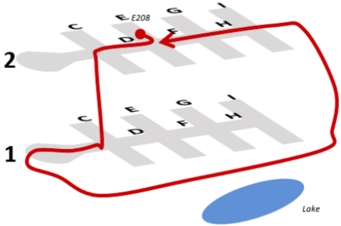


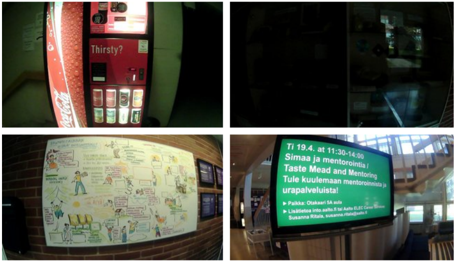
PassFrame video

Device-authentication from egocentric videos

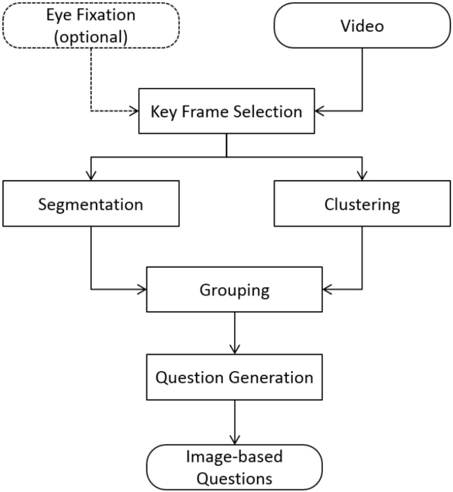
Try and break it:

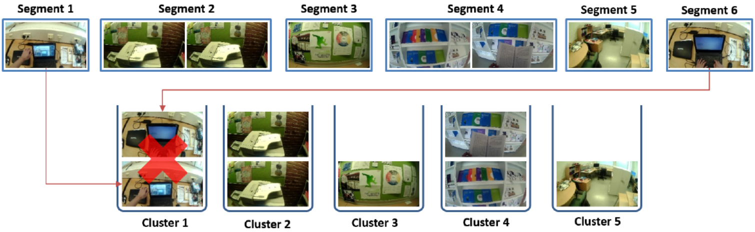
http://ambientintelligence.aalto.fi/passframe/





Overview (Frame selection and challenge generation)





Segmentation

Figure 3. Images selected by eye fixations (bottom) and frame sampling (top)

clustering

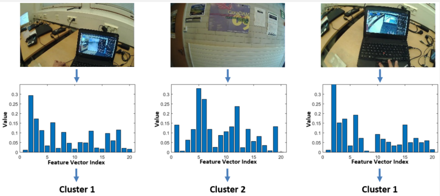


Figure 6. Feature values extracted from video frames (We only show absolute values of a part of feature vectors for better visualization)

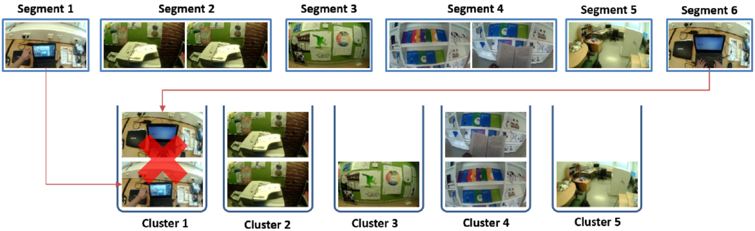
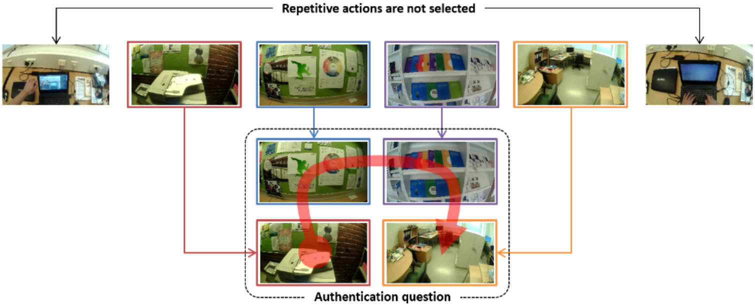
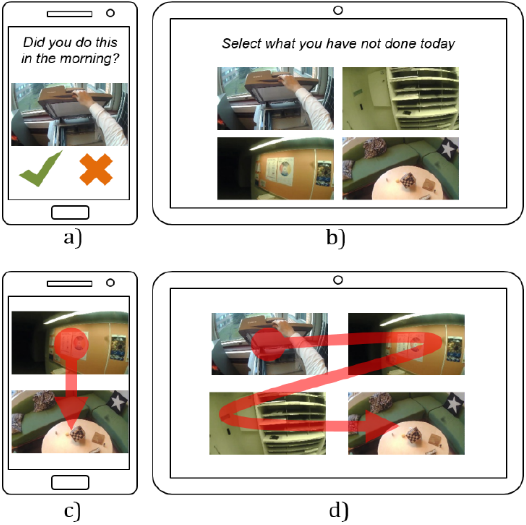


Figure 5. Non-informative images discarded from small clusters

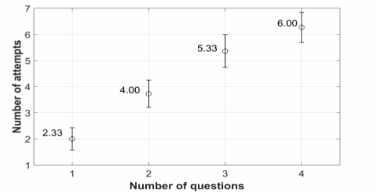
Secure authentication from Egocentric camera



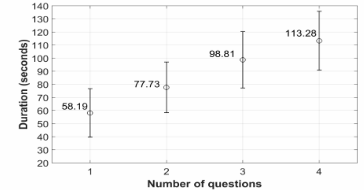
Alternative Autentication schemes



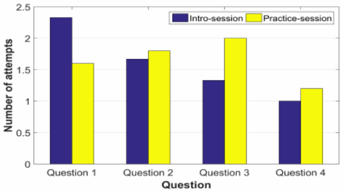
Performance of subjects



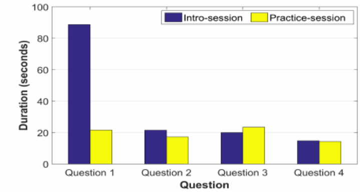
(a) Number of attempts to answer the challenges



(b) Time duration spent on answering the challenges



(c) Average number of attempts on each challenge



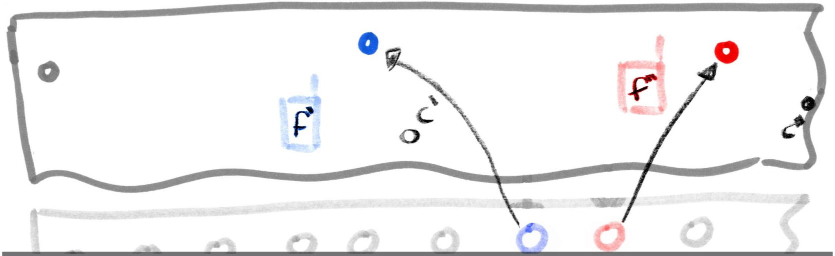
(d) Average thinking duration on each challenge

Issues

- Similar images

Figure 11. Some images that are difficult for the users to recall

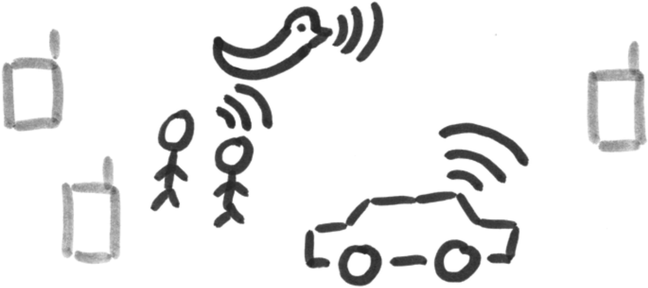
- Robustness against an active attacker



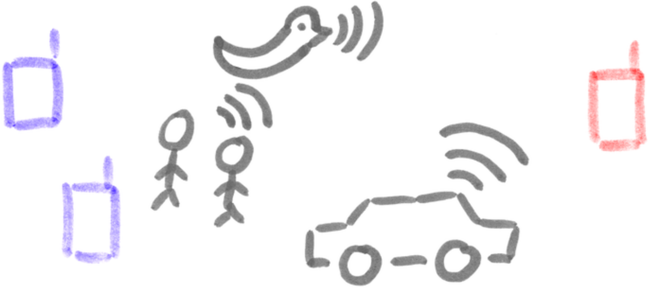
Secure spontaneous authentication from ambient audio

Spontaneous audio-based device pairing

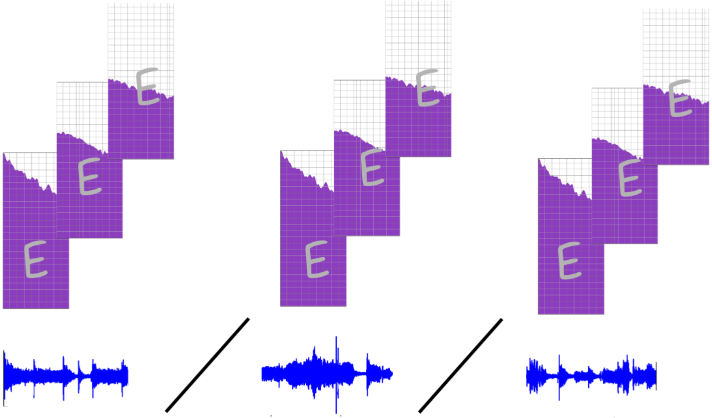
Spontaneous audio-based device pairing



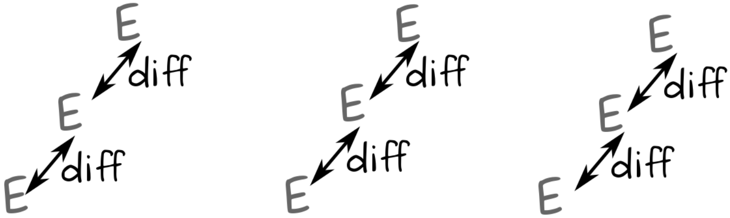
Spontaneous audio-based device pairing



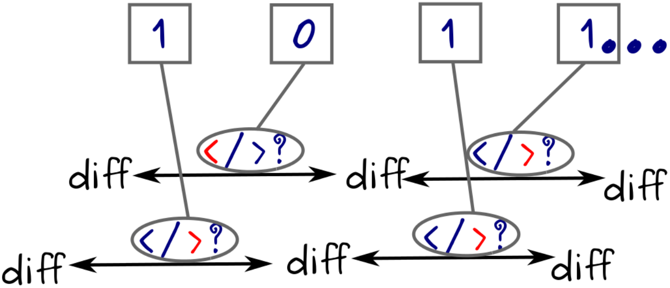
Spontaneous audio-based device pairing



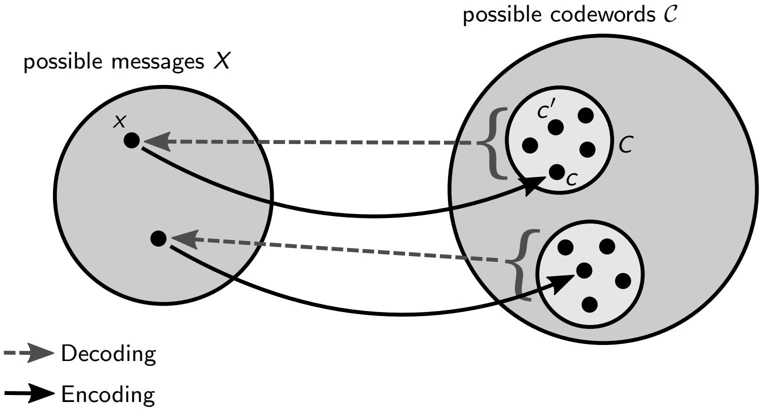
Spontaneous audio-based device pairing



Spontaneous audio-based device pairing



Secure pairing from noisy data

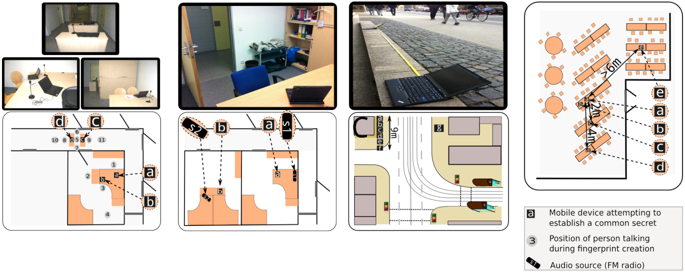


Security from environmental stimuli

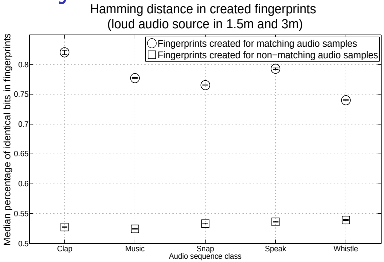
Audio-based ad-hoc secure pairing[a]

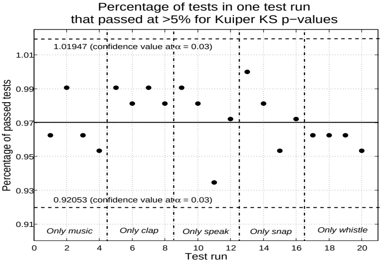
[a] S. Sigg et al., Secure Communication based on Ambient Audio, IEEE Transactions on Mobile Computing, vol. 12, no. 2, 2013

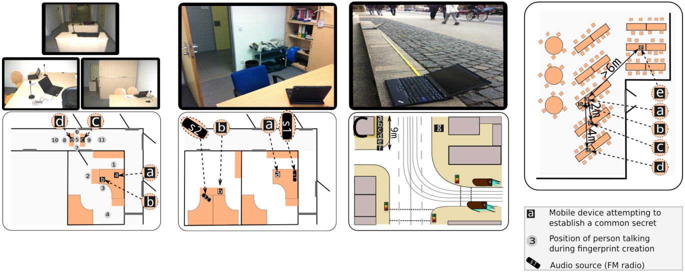
- Audio as common context source
- Fuzzy cryptography

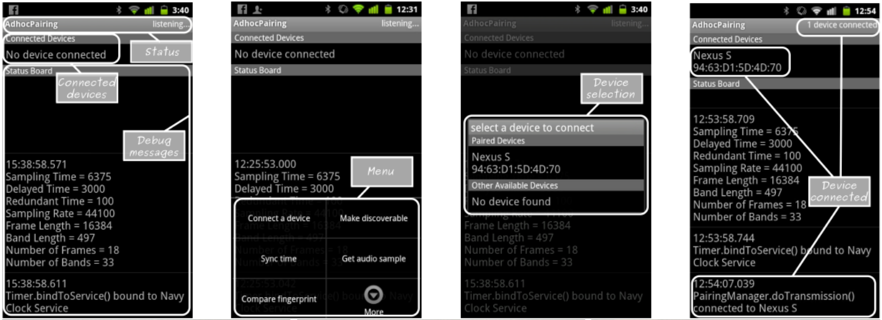


Security from environmental stimuli







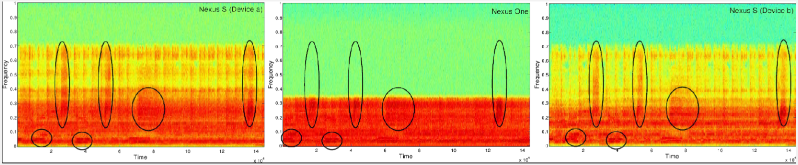

AdhocPairing
listening...
Connected Devices
No device connected
Status
Status Board
Connected devices
Debug messages
15:38:58.571
Sampling Time = 6375
Delayed Time = 3000
Redundant Time = 100
Sampling Rate = 44100
Frame Length = 16384
Band Length = 497
Number of Frames = 18
Number of Bands = 33
15:38:58.611
Timer.bindToService() bound to Navy Clock Service
Menu
12:25:53.000
Connect a device
Make discoverable
Sync time
Get audio sample
Compare fingerprint
More
Device selection
select a device to connect
Paired Devices
Nexus S
94:63:D1:5D:4D:70
Other Available Devices
No device found
1 device connected
12:53:58.709
Device connected
12:53:58.744
12:54:07.039
PairingManager.doTransmission() connected to Nexus S

Security from environmental stimuli

Real-time implementation on android mobile phones[a]

[a] Stephan Sigg, et al., AdhocPairing: Spontaneous audio-based secure device pairing for Android mobile devices, IWSSI 2012

- Hardware noise cancellation on some phones
- Hardware originated synchronisation offset



Security from environmental stimuli

How to synchronise audio without disclosing information?

No data shall be transmitted among devices

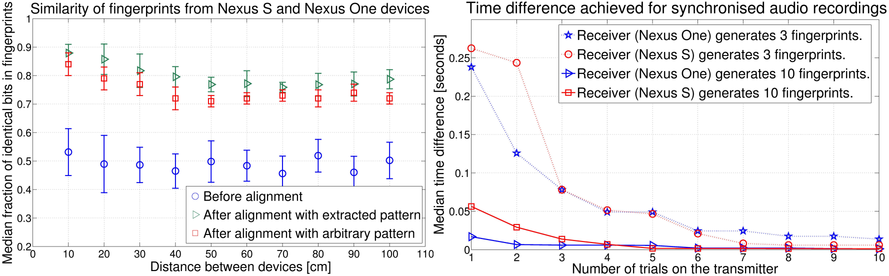
Hardware-originated synchronisation offset

- Approximate pattern matching with arbitrary common sequence [a]

[a] T. F. Smith and M. S. Waterman. Identification of common molecular subsequences. Journal of molecular biology, 147(1):195â197, Mar. 1981

Security from environmental stimuli

Hardware-originated synchronisation offset



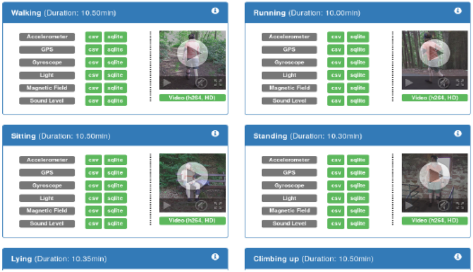
- Synchronisation in the order of 3ms possible
- No additional data transmitted among devices[1] [2]

[1] N. Nguyen, S. Sigg, A. Huynh and Y. Ji: Pattern-based Alignment of Audio Data for Ad-hoc Pairing, ISWC, 2012

[2] N. Nguyen, S. Sigg, A. Huynh and Y. Ji: Using ambient audio in secure mobile phone communication, PerCom, 2012

Unobtrusive Ad-Hoc Pairing for Body Area Networks

- 15 Subjects
- 8 Actions
- 7 Sensor-positions
- 6 Sensors



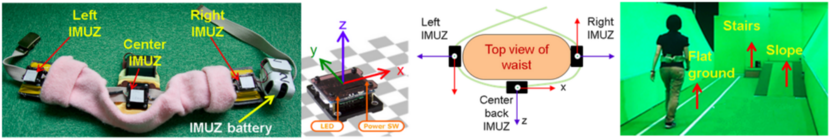
Sztyler et al.:*On-body Localization of Wearable Devices [...]*

Osaka University (OU-ISIR Gait database)

- 460 participants aged between 8 and 78
- gender ratio almost 50:50
- max. 8 gait cycles
- Sensorpositions: Waist right, left, back
- 3D-Accelerometer and Gyroskope (100Hz)

URL: http://www.am.sanken.osaka-u.ac.jp/BiometricDB/SimilarActionsInertialDB.html

Sensor Setup



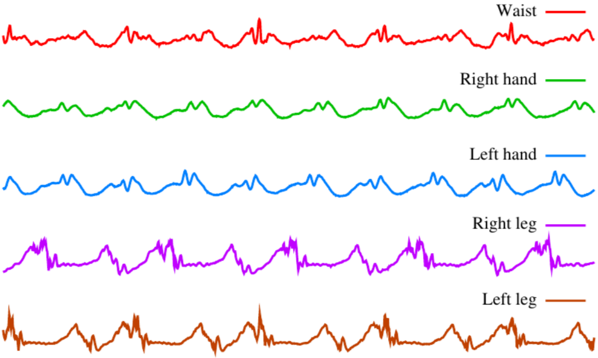
(a) Uncovered 3 IMUZ sensors on a belt (b) IMUZ (c) Sensor attachment (d) Subject wearing a belt in the scene

Thanh Trung Ngo, Yasushi Makihara, Hajime Nagahara, Yasuhiro Mukaigawa,Yasushi Yagi, "Similar gait action recognition using an inertial sensor," Pattern Recognition Vol.48 (4), pp. 1289-1301, 2015

Dartmouth

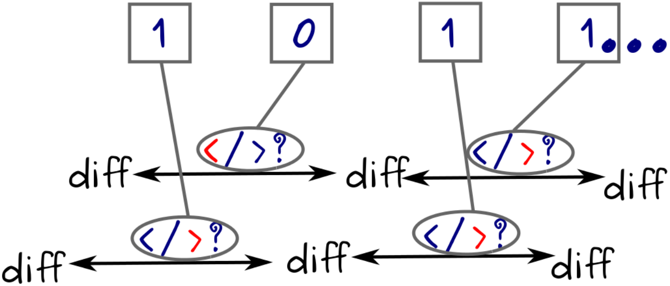
- 7 Subjects
- 5 Accelerometers - no Gyroscopes
- 13 hours at 255Hz
- waist, left wrist, right wrist, left ankle, right ankle

http://www.cs.dartmouth.edu/~dfk/papers/cornelius-same-body.pdf



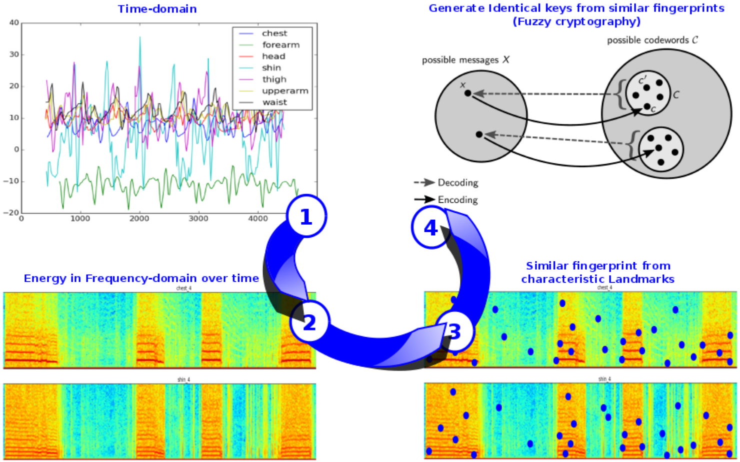
Cory Cornelius and David Kotz. 2011. Recognizing whether sensors are on the same body. In Proceedings of the 9th international conference on Pervasive computing (Pervasive'11), Kent Lyons, Jeffrey Hightower, and Elaine M. Huang (Eds.). Springer-Verlag, Berlin, Heidelberg, 332-349.

Audio Fingerprinting (Haitsma & Kalker, ISMIR 2002)



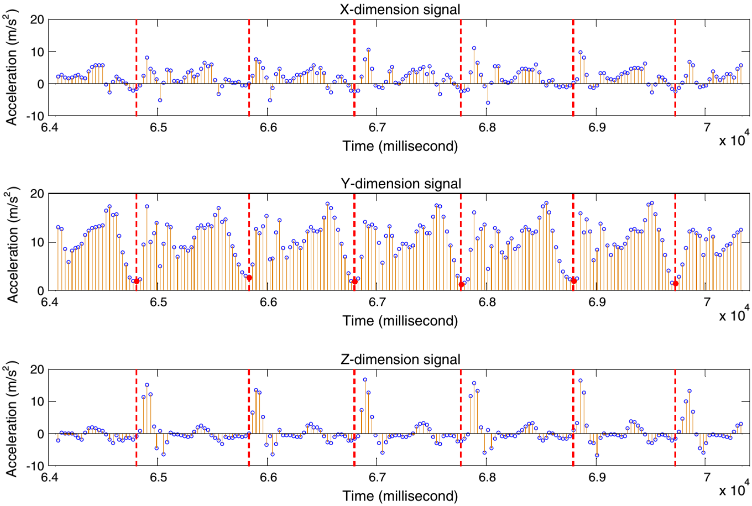
Haitsma, Kalker: A highly robust audio fingerprinting system. ISMIR. 2002.

Audio Landmarks (Wang, ISMIR 2003)

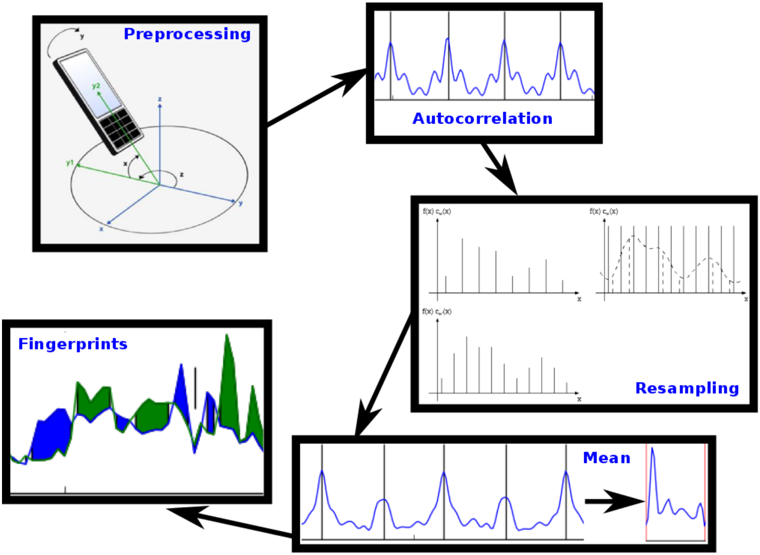


Wang: An Industrial Strength Audio Search Algorithm. ISMIR. 2003.

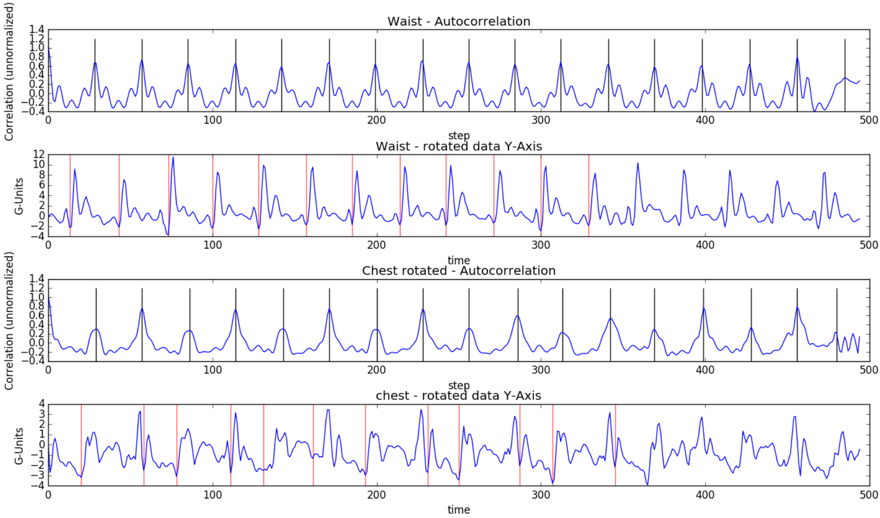
Gait recognition (Hoang & Choi & Nguyen, IJIS 2015)



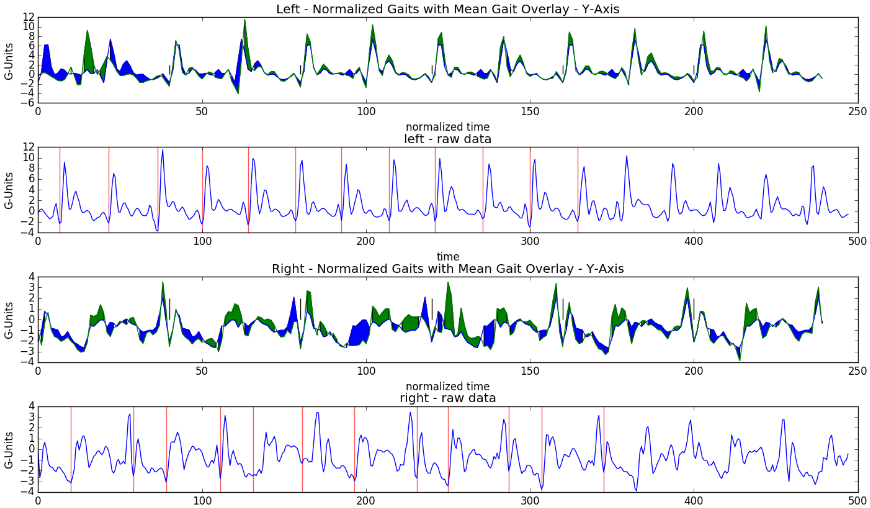
Hoang, Choi, Nguyen: Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment


Preprocessing
Autocorrelation
Resampling
Mean
Fingerprints

Results

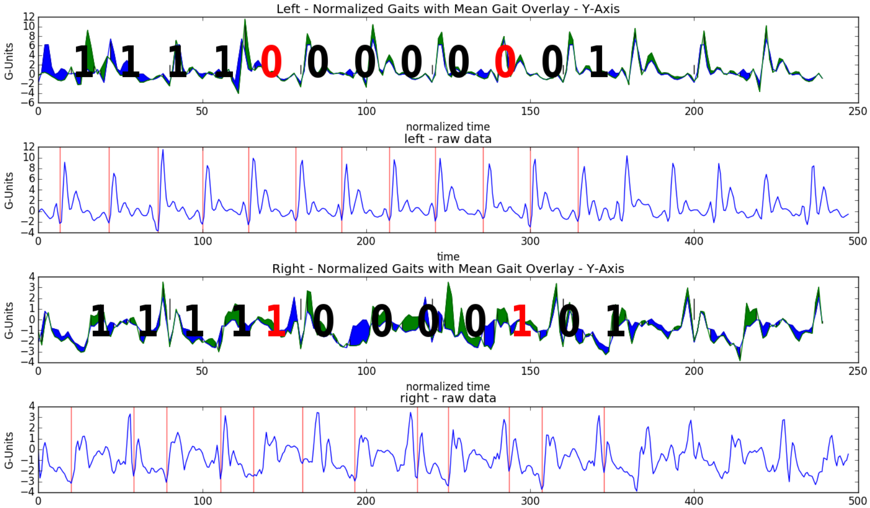

Waist - Autocorrelation
Correlation (unnormalized)
step
Waist - rotated data Y-Axis
G-Units
time
Chest rotated - Autocorrelation
Correlation (unnormalized)
step
chest - rotated data Y-Axis
G-Units
time

Results



Left - Normalized Gaits with Mean Gait Overlay - Y-Axis
G-Units
normalized time
left - raw data
G-Units
time
Right - Normalized Gaits with Mean Gait Overlay - Y-Axis
G-Units
normalized time
right - raw data
G-Units

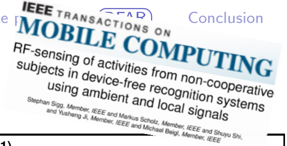
Results

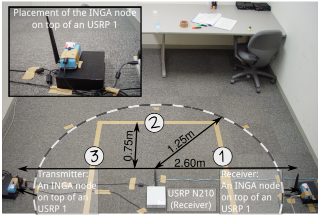

Left - Normalized Gaits with Mean Gait Overlay - Y-Axis
G-Units
normalized time
1 1 1 1 0 0 0 0 0 0 0 1
left - raw data
time
Right - Normalized Gaits with Mean Gait Overlay - Y-Axis
1 1 1 1 1 0 0 0 0 1 0 1
right - raw data

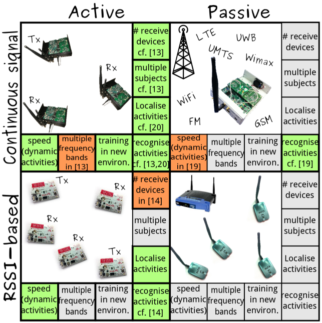
Project:

RF-based device-free activity recognition

RF-based device-free activity recognition


IEEE TRANSACTIONS ON MOBILE COMPUTING
RF-sensing of activities from non-cooperative subjects in device-free recognition systems using ambient and local signals
Stephan Sigg, Member, IEEE and Markus Scholz, Member, IEEE and Shuyu Shi, and Yusheng Ji, Member, IEEE and Michael Beigl, Member, IEEE





Active SDR-based DFAR (USRP1)
Frequency: 900MHz (RFX900 board), Vert900 Antenna), 4dBi antenna gain
Signal: Sine signal, continuously modulated onto the carrier
Sample rate: 80 Hz

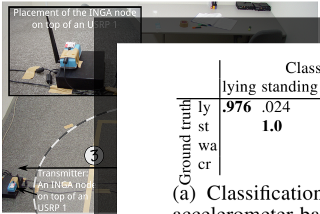
Passive SDR-based DFAR (USRP N210)
Frequency: 82.5MHz (WBX board), Vert900 Antenna, 4dBi antenna gain
Signal: Environmental FM radio captured from a nearby radio station
Sample rate: 64Hz

Active RSSI-based DFAR (INGA wsn nodes, v1.4)
Frequency: 2.4GHz IEEE802.15.4, PCB High Gain-Antenna
Signal: RSSI samples from packets transmitted between nodes
Sample rate: Transmission of 100 packets per second

Accelerometer-based activity recognition (Iphone 4)
Signal: 3-axis accelerometer
Sample rate: 40 Hz

Walking Lying standing empty Crawling

RF-based device-free activity recognition



Active SDR-based DFAR (USRP1)
Frequency: 900MHz (RFX900 board), Vert900 Antenna), 4dBi antenna gain

Ground truth	lying	standing	walking	crawling
ly	**.976**	.024		
st		**1.0**		
wa			**.955**	.045
cr			.253	**.748**

(a) Classification accuracy for accelerometer-based activity recognition by a k-NN

Ground truth	lying	standing	walking	crawling
ly	**.904**	.096		
st	.096	**.898**	.006	
wa		.013	**.962**	.025
cr		.038	.212	**.75**

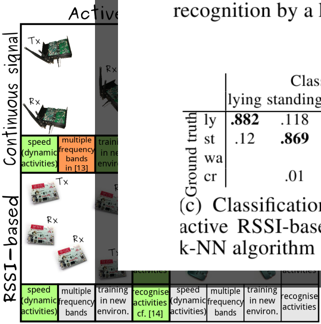
(b) Classification accuracy for active SDR-based DFAR by a k-NN algorithm

Ground truth	lying	standing	walking	crawling
ly	**.882**	.118		
st	.12	**.869**	.007	.004
wa			**.953**	.047
cr		.01	.439	**.551**

(c) Classification accuracy for active RSSI-based DFAR by a k-NN algorithm

Ground truth	lying	standing	walking	crawling
ly	**1.0**			
st	.056	**.98**	.022	
wa	.023		**.874**	.102
cr	.044		.144	**.811**

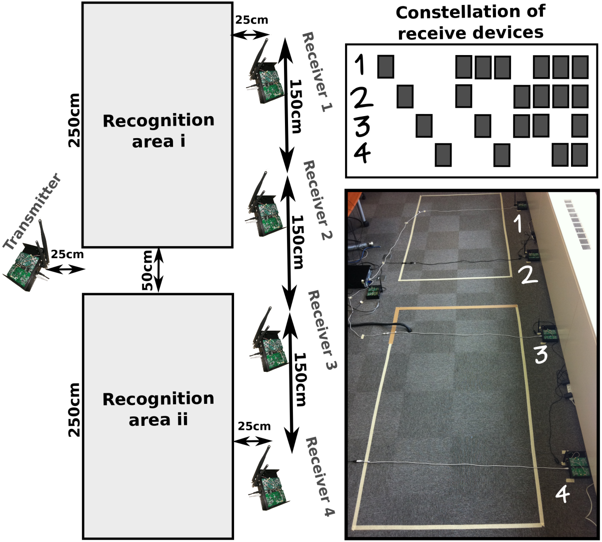
(d) Classification accuracy for passive SDR-based DFAR by a k-NN algorithm



Recognition of multiple activities simultaneously

standing
walking
crawling
lying
empty

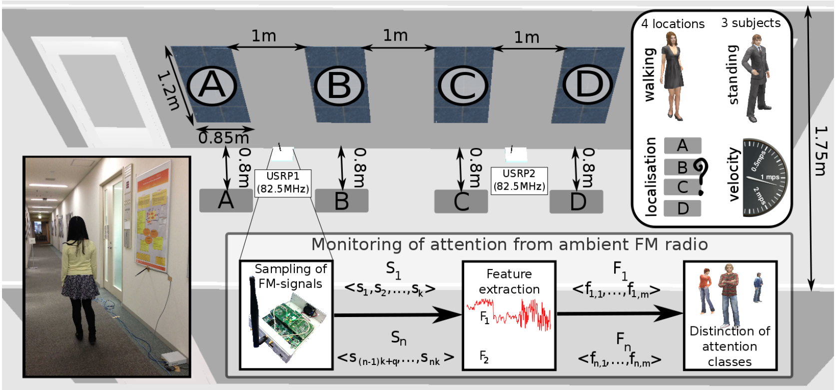
5x5=25



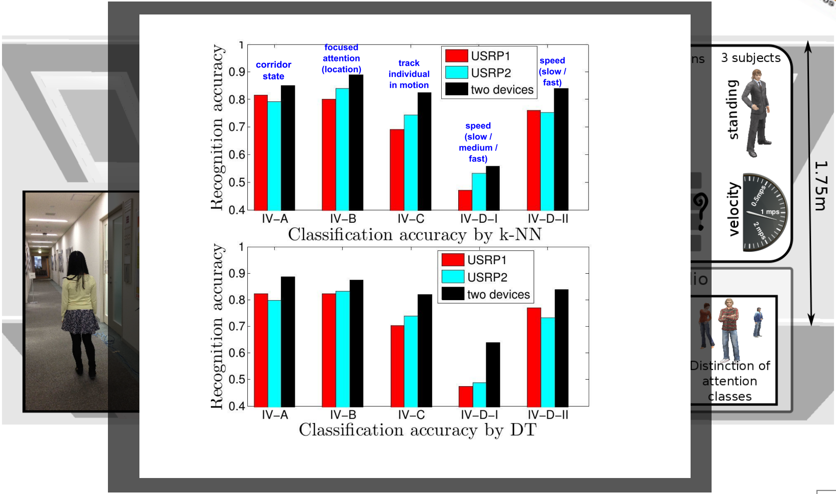
	Constellation of receive devices						
	1,2	1,3	1,4	2,3	1,2,3	1,2,4	1,2,3,4
CA	.697	.749	.726	.730	.787	.754	.838
IS	1.49	1.64	1.57	1.57	1.7	1.65	1.86
Brier	.421	.355	.388	.390	.318	.343	.229
AUC	.930	.946	.939	.928	.958	.960	.980

Table 5: Overall performance of the k-NN classifier

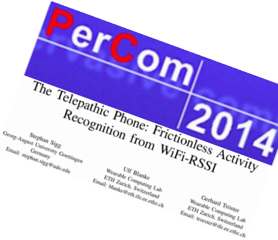
Monitoring attention from RF

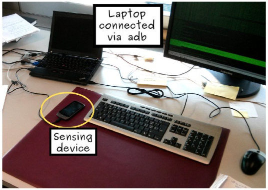


Monitoring attention from RF

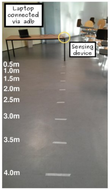


Situation and gestures from passive RSSI-based DFAR

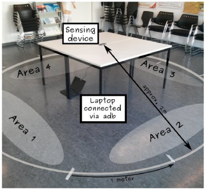




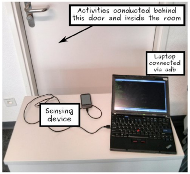
(a) Office environment at ETH



(b) Lecture room at TU-BS

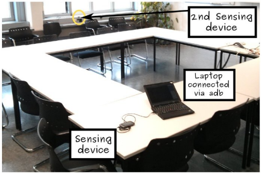


(c) Scenario for the distinction of walking speed

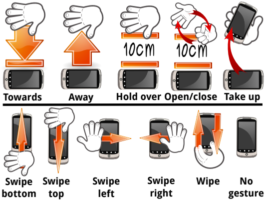


(d) Activities conducted behind a closed door

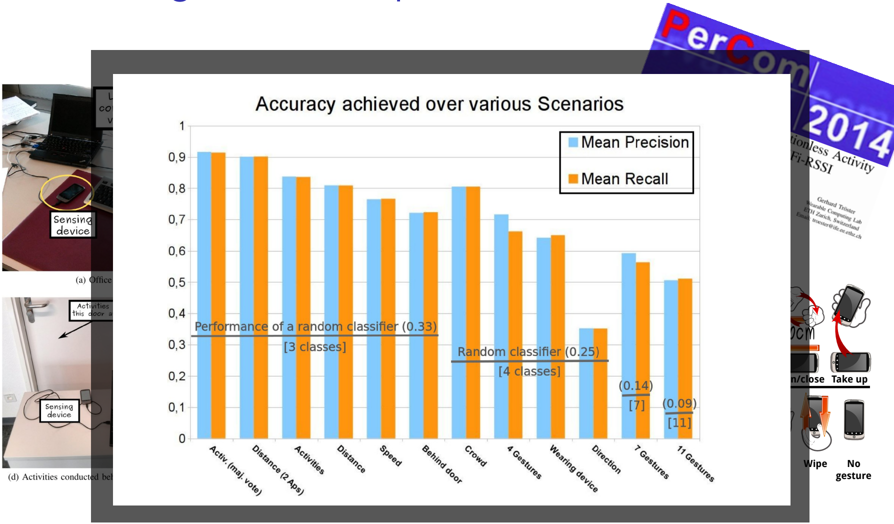
(e) Sensing device inside pocket



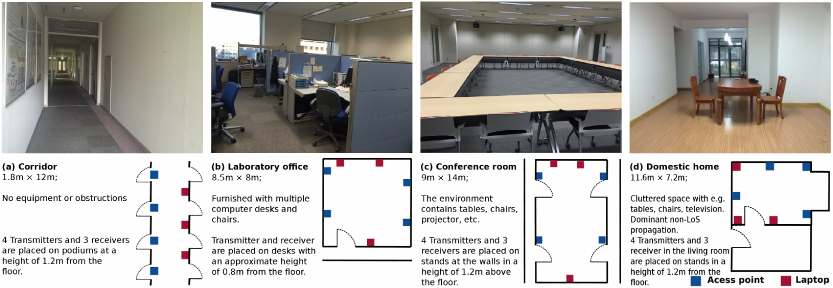
(f) Meeting room at ETH



Situation and gestures from passive RSSI-based DFAR

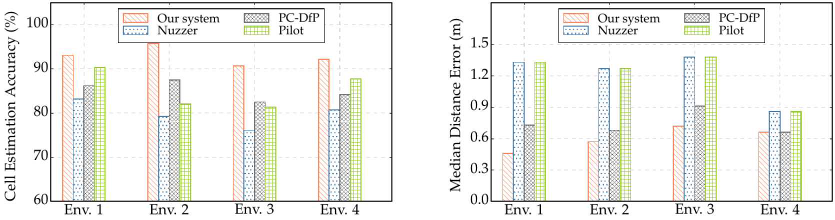


Modelling CSI vectors via multivariate gaussian distribution



We model the amplitude of every CSI reading at location 'y' to approximately follow a multivariate Gaussian Distribution. Location is then predicted via the maximum likelihood estimate.

Modelling CSI vectors via multivariate gaussian distribution

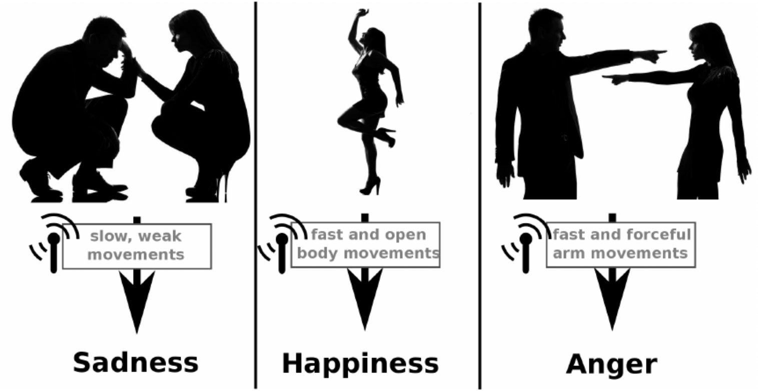


We model the amplitude of every CSI reading at location 'y' to approximately follow a multivariate Gaussian Distribution. Location is then predicted via the maximum likelihood estimate.

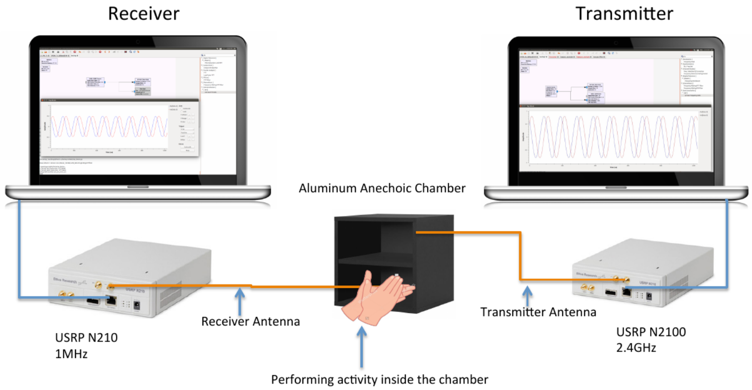
Nuzzer: Seifeldin, Saeed, Kosba, El-keyi, Youssef. Nuzzer: A large-scale device-free passive localization system for wireless environments. IEEE Transactions on Mobile Computing, 2013.
Pilot: Xiao, Wu, Yi, Wang, Ni. Pilot: Passive device-free indoor localization using channel state information. ICDCS, 2013.

PC-DfP: Xu, Firner, Zhang, Howard, Li, Lin. Improving rf- based device-free passive localization in cluttered indoor environments through probabilistic classification

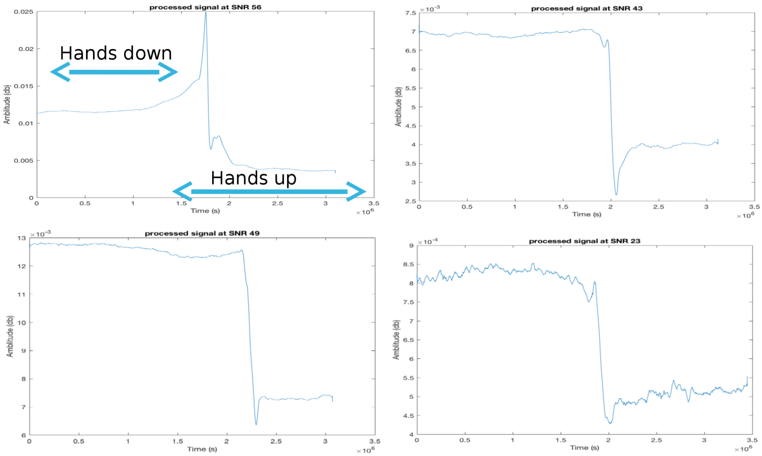
Emotion recognition from RF



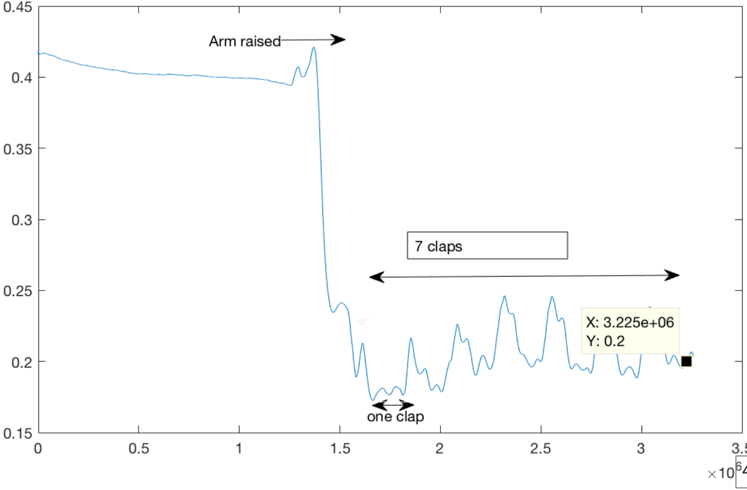
Emotion recognition from RF



Emotion recognition from RF



Emotion recognition from RF



Thank you!

Stephan Sigg
stephan.sigg@aalto.fi