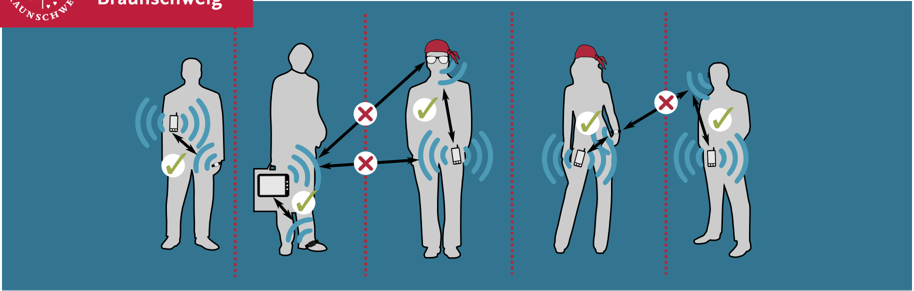
Technische Universität Braunschweig

Aalto University



BANDANA

Body Area Network Device-to-device Authentication using Natural gAit

Dominik Schürmann*, Arne Brüsch*, Stephan Sigg†, Lars Wolf*, 2017-03-15

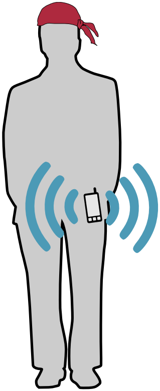
*Institute of Operating Systems and Computer Networks, TU Braunschweig
†Ambient Intelligence, Comnet, Aalto University

Waking up on Hawaii...

- Jet lag
- Awesome sunrise
- Let’s go jogging

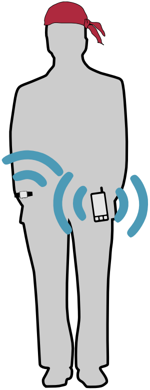
Waking up on Hawaii...

- Quantified self



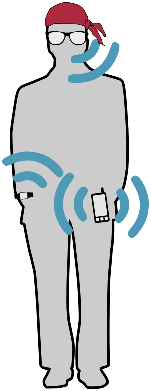
Waking up on Hawaii...

- Putting on your wearables



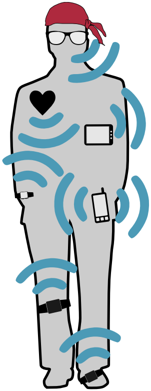
Waking up on Hawaii...

- Putting on all your wearables



Waking up on Hawaii...

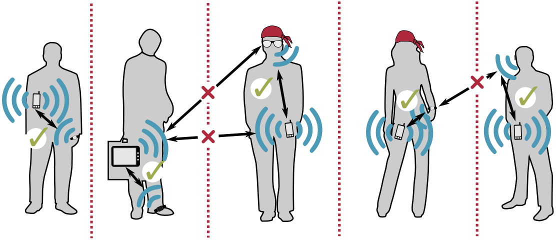
- Putting on **all** your wearables



Device-to-Device Authentication

Bluetooth Authentication

- "Just works" profile
- Still pressing buttons
- DH key exchange
- No MitM protection



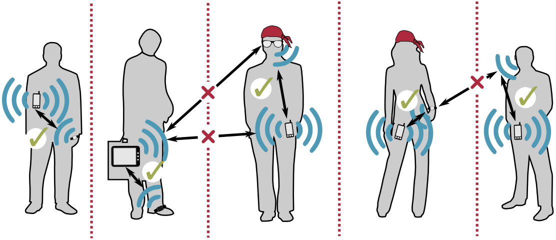
Device-to-Device Authentication

Bluetooth Authentication

- “Just works” profile
- Still pressing buttons
- DH key exchange
- No MitM protection

BANDANA

- Person’s gait (walking pattern)
- Zero interaction
- Independent of on-body location
- MitM protection



Novelty

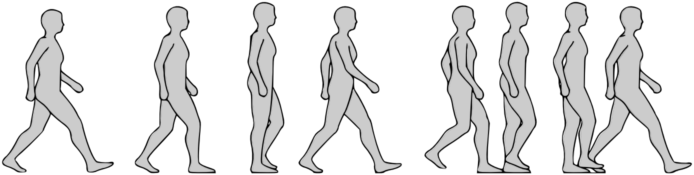
Unlock smartphones

- Muaaz et al. 2015
- Hoang et al. 2015

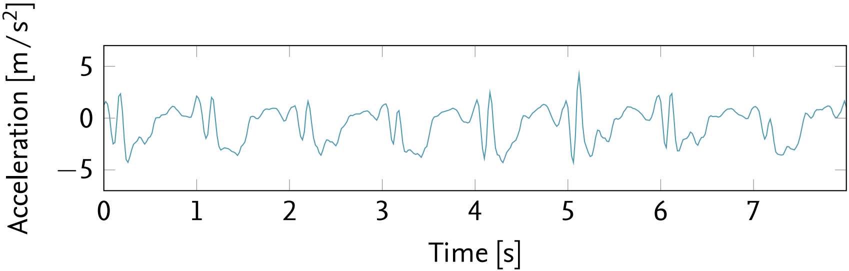
Device2Device Authentication

- No init procedure with templates
- Fresh secrets for each D2D authentication

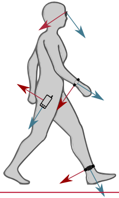
Gait Cycle



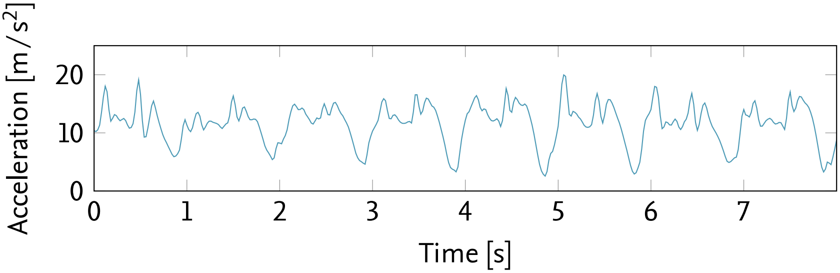
Accelerometer Reading



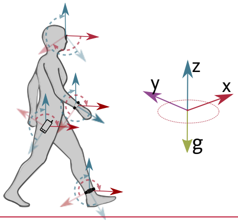
- Accelerometer reading on z-axis only



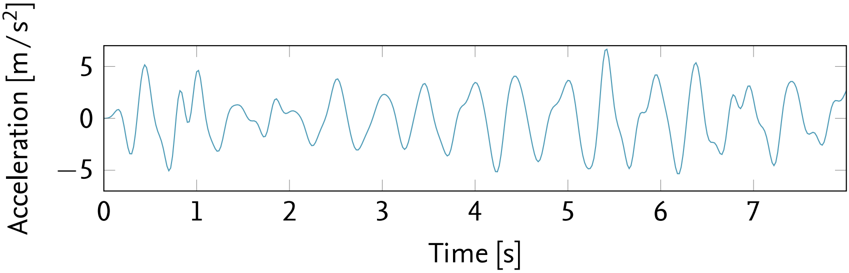
Rotated Signal



- Orientation relative to ground using Madgwick's Algorithm
  - Notice influence of gravity *g*

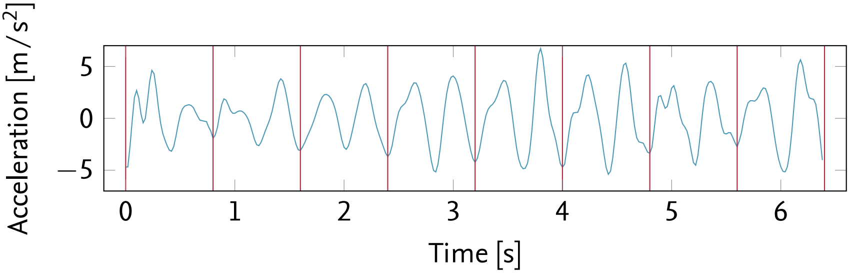


Noise-Reduced Signal



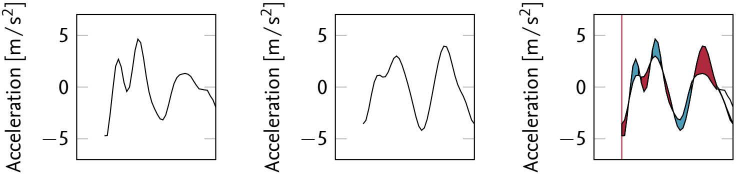
- Apply a bandpass filter to keep frequencies between 0.5 and 12 Hz

Gait-Cycle Detection



- Partition data into gait cycles
- Resample gait cycles to equal length
- Calculate average gait cycle

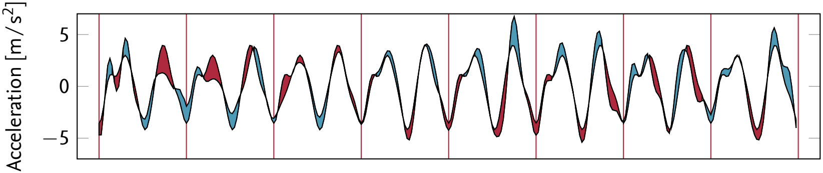
Quantization



Cycle Average Cycle 1 0 0 1

- Average gait cycle overlaid on each original gait cycle
- 4 bits per cycle

Quantization



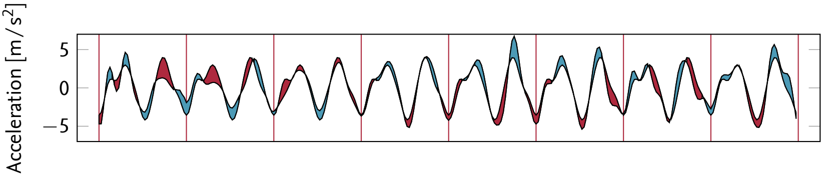
a) 1001 0100 1001 1010 1010 1001 0101 0110

b) 1001 0100 1001 1010 1010 1001 0101 0110

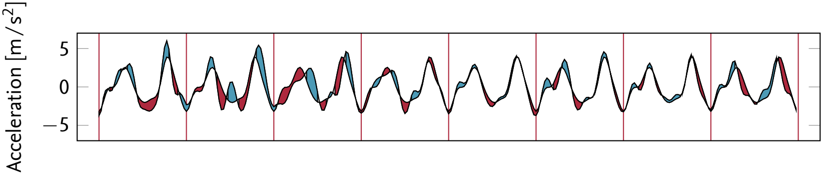
c) 0111 1000 1001 0101 1000 1100 ~~1011~~ ~~1000~~

- Average gait cycle overlaid on each original gait cycle
- 4 bits per cycle

Comparison between Locations

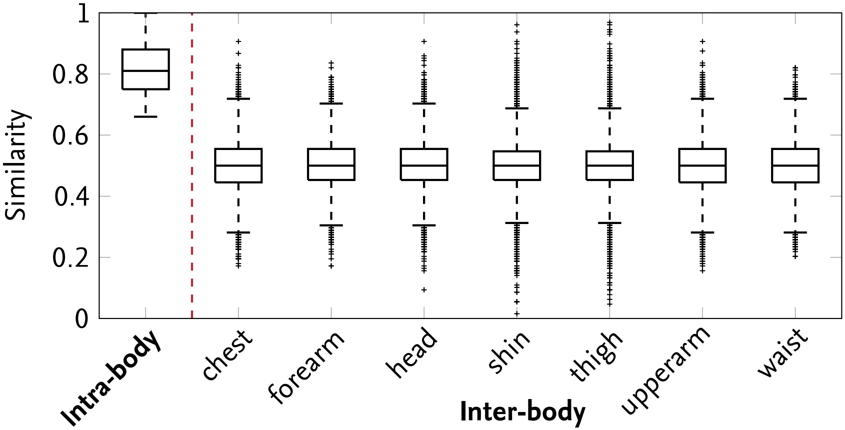


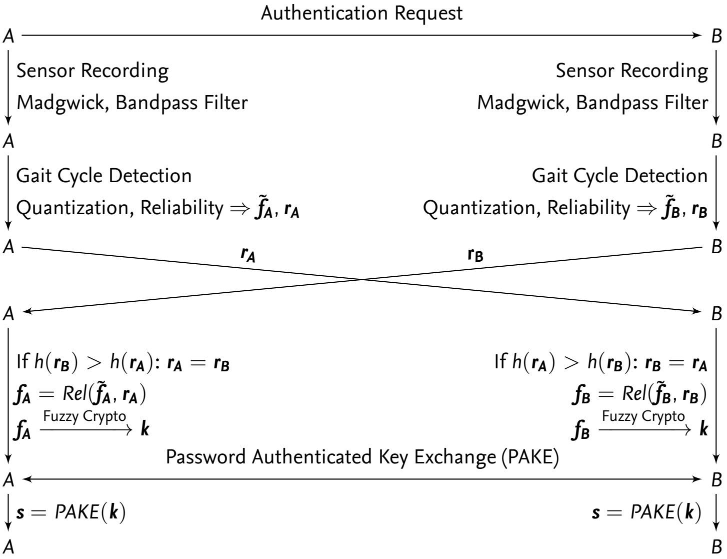
forearm: 0111 1000 1001 0101 1000 1100 ~~1011~~ ~~1000~~



waist: 0110 1000 1001 0001 1001 1001 ~~1100~~ ~~1010~~

Evaluation


Similarity
1
0.8
0.6
0.4
0.2
0
Intra-body
chest
forearm
head
shin
thigh
upperarm
waist
Inter-body



Authentication Request

$A \longrightarrow B$

Sensor Recording

Madgwick, Bandpass Filter

Sensor Recording

Madgwick, Bandpass Filter

Gait Cycle Detection

Quantization, Reliability $\Rightarrow \tilde{\boldsymbol{f}}_{\boldsymbol{A}}, \boldsymbol{r}_{\boldsymbol{A}}$

Gait Cycle Detection

Quantization, Reliability $\Rightarrow \tilde{\boldsymbol{f}}_{\boldsymbol{B}}, \boldsymbol{r}_{\boldsymbol{B}}$

$\boldsymbol{r}_{\boldsymbol{A}}$

$\boldsymbol{r}_{\boldsymbol{B}}$

If $h(\boldsymbol{r}_{\boldsymbol{B}}) > h(\boldsymbol{r}_{\boldsymbol{A}})$: $\boldsymbol{r}_{\boldsymbol{A}} = \boldsymbol{r}_{\boldsymbol{B}}$

$\boldsymbol{f}_{\boldsymbol{A}} = Rel(\tilde{\boldsymbol{f}}_{\boldsymbol{A}}, \boldsymbol{r}_{\boldsymbol{A}})$

$\boldsymbol{f}_{\boldsymbol{A}} \xrightarrow{\text{Fuzzy Crypto}} \boldsymbol{k}$

If $h(\boldsymbol{r}_{\boldsymbol{A}}) > h(\boldsymbol{r}_{\boldsymbol{B}})$: $\boldsymbol{r}_{\boldsymbol{B}} = \boldsymbol{r}_{\boldsymbol{A}}$

$\boldsymbol{f}_{\boldsymbol{B}} = Rel(\tilde{\boldsymbol{f}}_{\boldsymbol{B}}, \boldsymbol{r}_{\boldsymbol{B}})$

$\boldsymbol{f}_{\boldsymbol{B}} \xrightarrow{\text{Fuzzy Crypto}} \boldsymbol{k}$

Password Authenticated Key Exchange (PAKE)

$A \longleftrightarrow B$

$\boldsymbol{s} = PAKE(\boldsymbol{k})$

$\boldsymbol{s} = PAKE(\boldsymbol{k})$

Conclusion

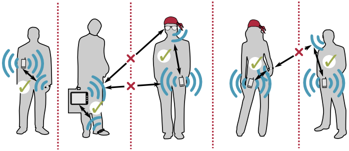
- Device-to-Device authentication for Body Area Networks
- Zero-interaction based on human gait pattern
- For 128 bit keys, 192 bit fingerprints are generated (48 cycles), disregarding 64 unreliable bits
- Worst-case duration: 96 s
- 80 % similarity required for fuzzy cryptography
  ⇒ 103-bit security level for the PAKE password.

Conclusion

- Device-to-Device authentication for Body Area Networks
- Zero-interaction based on human gait pattern
- For 128 bit keys, 192 bit fingerprints are generated (48 cycles), disregarding 64 unreliable bits
- Worst-case duration: 96 s
- 80 % similarity required for fuzzy cryptography
  $\Rightarrow$ 103-bit security level for the PAKE password.

Any questions?

Dominik Schürmann <schuermann@ibr.cs.tu-bs.de>



Backup Slides

Spectral Coherence

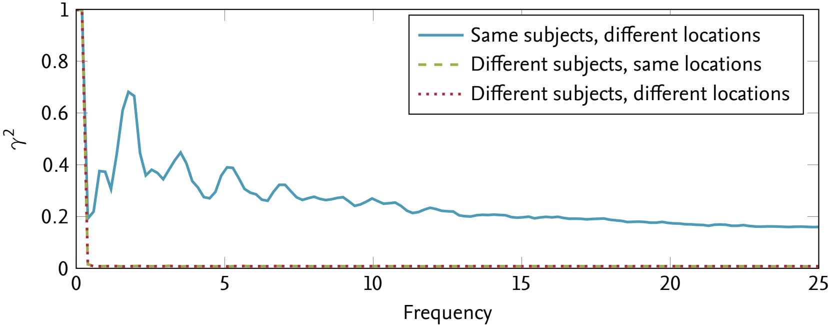


Figure: Average spectral coherence over full sensor readings of the Mannheim dataset for same and different subject.

Reliability

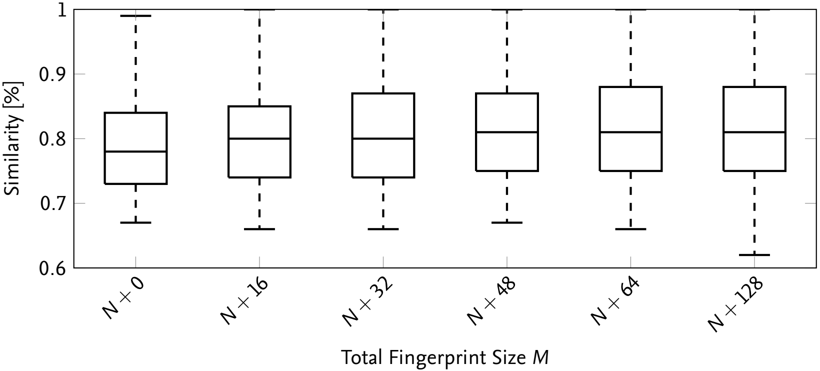


Figure: Fingerprint similarity of different sizes M with cutoff at $N = 128$ to evaluate the influence of $Rel()$.

Fingerprint Similarity

Table: Fingerprint similarity between locations on the same body (intra-body). Shown is the mean over all 15 subjects.

	chest	forearm	head	shin	thigh	upperarm	waist
chest	1.0	0.82	0.74	0.78	0.78	0.88	0.81
forearm	0.82	1.0	0.8	0.81	0.88	0.89	0.89
head	0.74	0.8	1.0	0.8	0.76	0.77	0.78
shin	0.78	0.81	0.8	1.0	0.77	0.78	0.8
thigh	0.78	0.88	0.76	0.77	1.0	0.85	0.84
upperarm	0.88	0.89	0.77	0.78	0.85	1.0	0.88
waist	0.81	0.89	0.78	0.8	0.84	0.88	1.0

Entropy

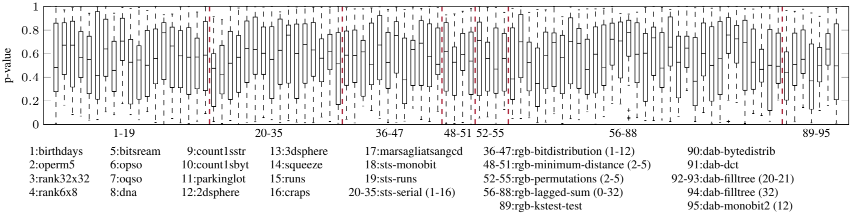


Figure: Distribution of p-values achieved for 128 bit keys (fingerprint length $M = 192$, 64 unreliable bits removed) in 21 runs of the various statistical tests of the dieHarder set of statistical tests.