Aalto University
School of Electrical
Engineering

Aspects of Pervasive Sensing: Perception and Security from ambient noise

Stephan Sigg

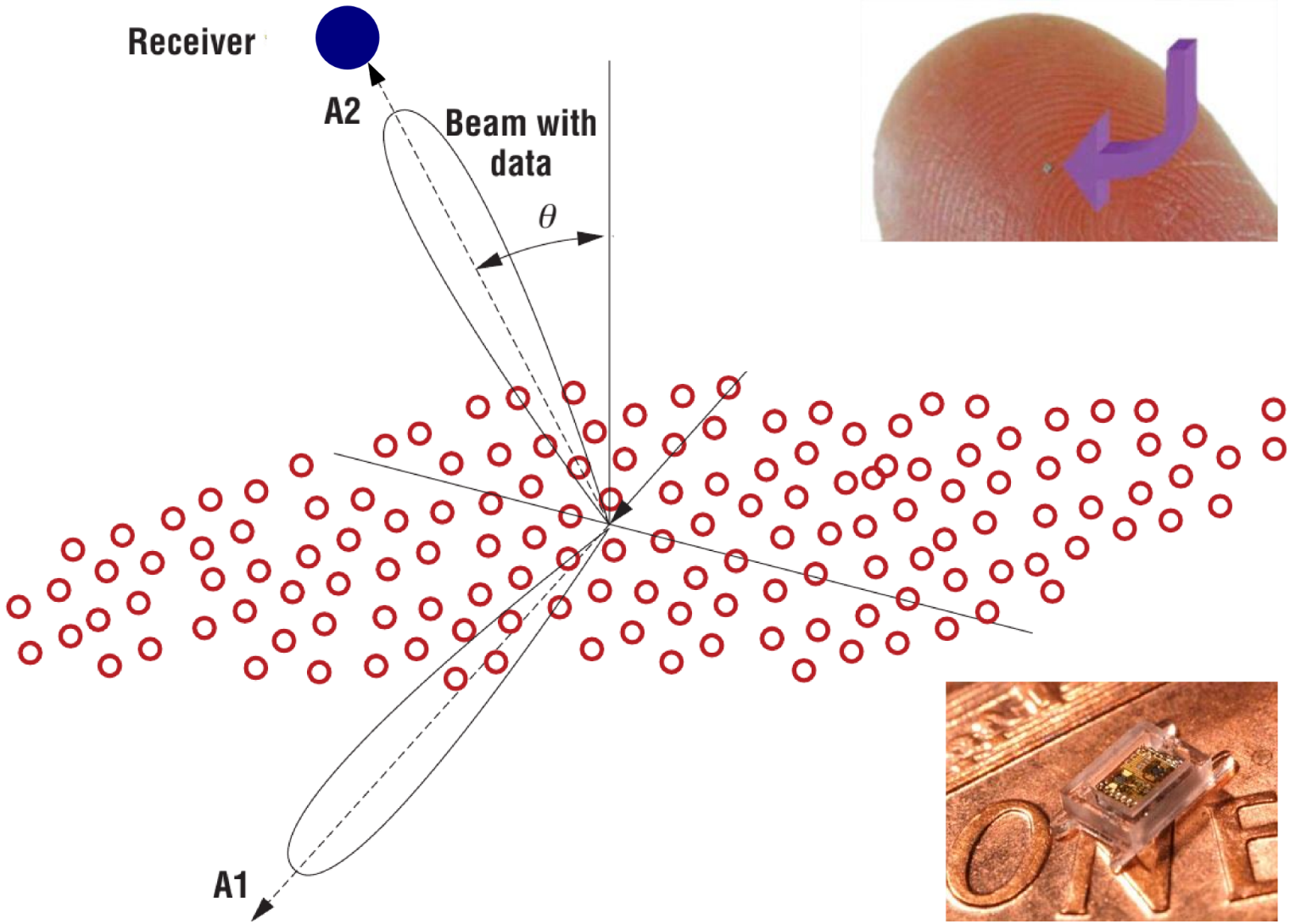
Department of Communications and Networking
Aalto University, School of Electrical Engineering
stephan.sigg@aalto.fi

TU-BS, 27.04.2017

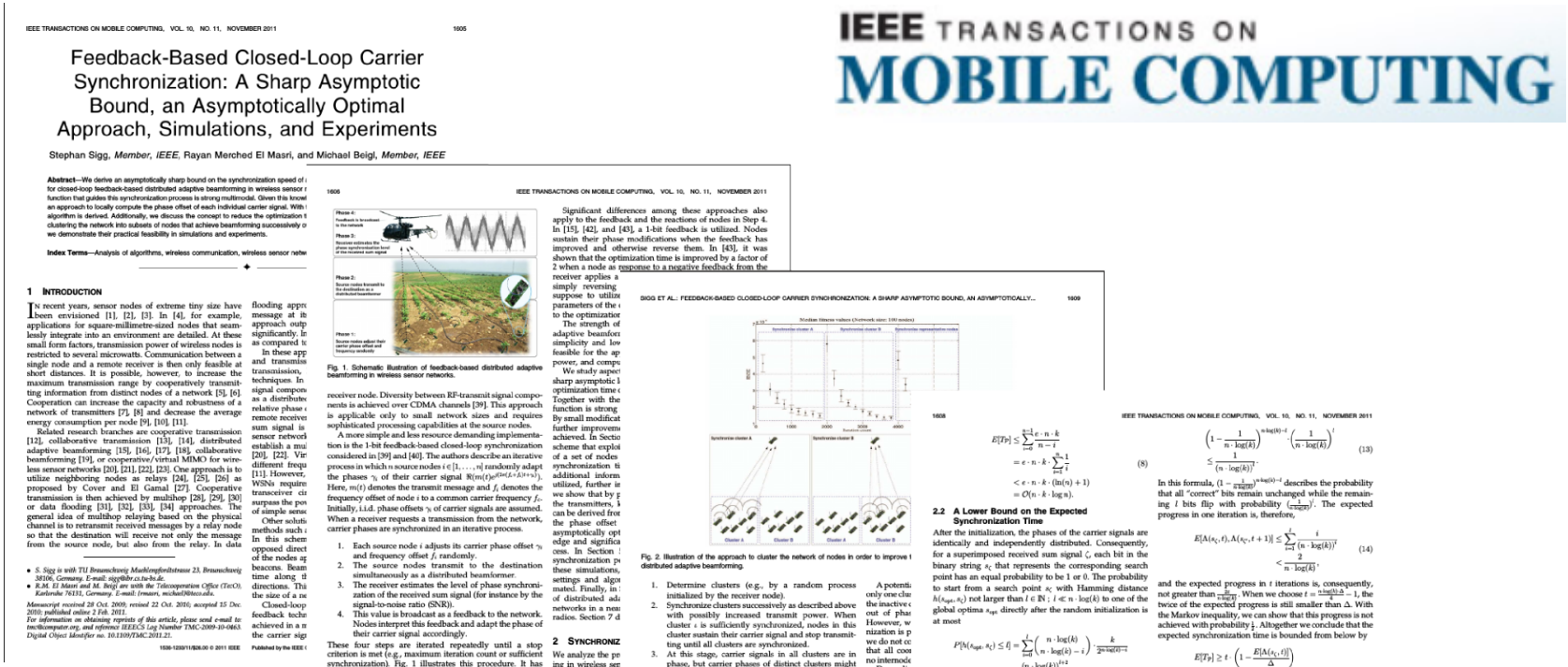
Cheap collaboration

Radio Vision

Security from ambient signals


Receiver
A2
Beam with
data
θ
A1

Feedback-based distributed adaptive beamforming



IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 10, NO. 11, NOVEMBER 2011 1605

Feedback-Based Closed-Loop Carrier Synchronization: A Sharp Asymptotic Bound, an Asymptotically Optimal Approach, Simulations, and Experiments

Stephan Sigg, *Member, IEEE*, Rayan Merched El Masri, and Michael Beigl, *Member, IEEE*

Abstract—We derive an asymptotically sharp bound on the synchronization speed of … for closed-loop feedback-based distributed adaptive beamforming in wireless sensor … function that guides this synchronization process is strong multimodal. Given this knowl… an approach to locally compute the phase offset of each individual carrier signal. With … algorithm is derived. Additionally, we discuss the concept to reduce the optimization t… clustering the network into subsets of nodes that achieve beamforming successively o… we demonstrate their practical feasibility in simulations and experiments.

Index Terms—Analysis of algorithms, wireless communication, wireless sensor netw…

1 Introduction

In recent years, sensor nodes of extreme tiny size have been envisioned [1], [2], [3]. In [4], for example, applications for square-millimetre-sized nodes that seamlessly integrate into an environment are detailed. At these small form factors, transmission power of wireless nodes is restricted to several microwatts. Communication between a single node and a remote receiver is then only feasible at short distances. It is possible, however, to increase the maximum transmission range by cooperatively transmitting information from distinct nodes of a network [5], [6]. Cooperation can increase the capacity and robustness of a network of transmitters [7], [8] and decrease the average energy consumption per node [9], [10], [11].

Related research branches are cooperative transmission [12], collaborative transmission [13], [14], distributed adaptive beamforming [15], [16], [17], [18], collaborative beamforming [19], or cooperative/virtual MIMO for wireless sensor networks [20], [21], [22], [23]. One approach is to utilize neighboring nodes as relays [24], [25], [26] as proposed by Cover and El Gamal [27]. Cooperative transmission is then achieved by multihop [28], [29], [30] or data flooding [31], [32], [33], [34] approaches. The general idea of multihop relaying based on the physical channel is to retransmit received messages by a relay node so that the destination will receive not only the message from the source node, but also from the relay. In data flooding appro… message at th… approach outp… significantly. In… as compared t… In these app… and transmiss… transmission, … techniques. In… signal compon… as a distributive… relative phase … remote receive… sum signal is … sensor networ… establish a mu… [20], [22]. Vir… different frequ… [11]. However, … WSNs require… transceiver cir… surpass the po… of simple sens… Other soluti… methods such … In this schem… opposed direct… of the nodes ag… beacons. Beam… time along t… directions. Thi… the size of a n… Closed-loop … feedback techn… achieved in a n… the carrier sig…

- *S. Sigg is with TU Braunschweig Muehlenpfordtstrasse 23, Braunschweig 38106, Germany. E-mail: sigg@ibr.cs.tu-bs.de.*
- *R.M. El Masri and M. Beigl are with the Telecooperation Office (TecO), Karlsruhe 76131, Germany. E-mail: {rmasri, michael}@teco.edu.*

Manuscript received 20 Oct. 2009; revised 22 Oct. 2010; accepted 15 Dec. 2010; published online 2 Feb. 2011.
For information on obtaining reprints of this article, please send e-mail to: tmc@computer.org, and reference IEEECS Log Number TMC-2009-10-0463.
Digital Object Identifier no. 10.1109/TMC.2011.21.

1536-1233/11/$26.00 © 2011 IEEE Published by the IEEE …

1606 IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 10, NO. 11, NOVEMBER 2011

Fig. 1. Schematic illustration of feedback-based distributed adaptive beamforming in wireless sensor networks.

receiver node. Diversity between RF-transmit signal components is achieved over CDMA channels [39]. This approach is applicable only to small network sizes and requires sophisticated processing capabilities at the source nodes.

A more simple and less resource demanding implementation is the 1-bit feedback-based closed-loop synchronization considered in [39] and [40]. The authors describe an iterative process in which n source nodes $i \in [1, \ldots, n]$ randomly adapt the phases γ_i of their carrier signal $\Re(m(t)e^{\mathbb{I}2\pi(f_c t + \gamma_i)})$. Here, $m(t)$ denotes the transmit message and f_c denotes the frequency offset of node i to a common carrier frequency f_c. Initially, i.i.d. phase offsets γ_i of carrier signals are assumed. When a receiver requests a transmission from the network, carrier phases are synchronized in an iterative process.

1. Each source node i adjusts its carrier phase offset γ_i and frequency offset f_i randomly.
2. The source nodes transmit to the destination simultaneously as a distributed beamformer.
3. The receiver estimates the level of phase synchronization of the received sum signal (for instance by the signal-to-noise ratio (SNR)).
4. This value is broadcast as a feedback to the network. Nodes interpret this feedback and adapt the phase of their carrier signal accordingly.

These four steps are iterated repeatedly until a stop criterion is met (e.g., maximum iteration count or sufficient synchronization). Fig. 1 illustrates this procedure. It has been studied by different authors [41], [42], [43], [13]. The distinct approaches proposed differ in the implementation of the first and the fourth step specified above. The authors of [43] show that it is possible to reduce the count of transmitters in a random process and still achieve sufficient synchronization among all nodes.

In [41], [42], and [43], a process is described in which each node alters its carrier phase offset γ_i according to a normal distribution with small variance in Step 1. In [13], a uniform distribution is utilized instead, but the probability for one node to alter the phase offset of its carrier signal is low. We show in Section 5 that both approaches achieve a similar performance. Only in [42] not only the phase, but also the frequency is adapted.

Significant differences among these approaches also apply to the feedback and the reactions of nodes in Step 4. In [15], [42], and [43], a 1-bit feedback is utilized. Nodes sustain their phase modifications when the feedback has improved and otherwise reverse them. In [43], it was shown that the optimization time is improved by a factor of 2 when a node as response to a negative feedback from the receiver applies a… simply reversing… suppose to utilize… parameters of the … to the optimization… The strength of… function is strong… By small modificat… further improvem… achieved. In Sectio… scheme that explo… of a set of nodes… synchronization ti… additional inform… utilized, further i… we show that by … the transmitters, … can be derived fro… the phase offset … asymptotically opt… edge and significa… cons. In Section … synchronization p… these simulations, … settings and algo… mated. Finally, in … of distributed ad… networks in a nea… radios. Section 7 d…

2 Synchroniz…

We analyze the pe… ing in wireless sen… and assume that … probability $\frac{1}{2}$ for … uniformly at rando… feedback of the re… phase of their carr… reversed. If, depe… improved or not. … the superimposed …

$$\zeta_{\text{sum}} = \Re($$

to a real-valued fi… received signal st…

SIGG ET AL.: FEEDBACK-BASED CLOSED-LOOP CARRIER SYNCHRONIZATION: A SHARP ASYMPTOTIC BOUND, AN ASYMPTOTICALLY… 1609

Fig. 2. Illustration of the approach to cluster the network of nodes in order to improve t… distributed adaptive beamforming.

1. Determine clusters (e.g., by a random process initialized by the receiver node).
2. Synchronize clusters successively as described above with possibly increased transmit power. When cluster ι is sufficiently synchronized, nodes in this cluster sustain their carrier signal and stop transmitting until all clusters are synchronized.
3. At this stage, carrier signals in all clusters are in phase, but carrier phases of distinct clusters might differ. Determine representative nodes from all clusters and synchronize these.
4. Nodes in all clusters alter their carrier phase by the phase offset experienced and broadcast by the corresponding representative node. Let

$$\zeta_i = \Re(m(t)\text{RSS}_i e^{\mathbb{I}2\pi f_c t(\gamma_i + \alpha_i + \omega_i)})$$

and $\zeta_i' = \Re(m(t)\text{RSS}_i e^{\mathbb{I}2\pi f_c t(\gamma_i' + \alpha_i + \omega_i)})$ be the carrier signals of representative node i from cluster ι before and after synchronization between representative nodes were achieved. A node h from cluster ι alters its carrier signal $\zeta_h = \Re(m(t)\text{RSS}_h e^{\mathbb{I}2\pi f_c t(\gamma_h + \alpha_h + \omega_h)})$ to $\zeta_h' = \Re(m(t)\text{RSS}_h e^{\mathbb{I}2\pi f_c t(\gamma_h + \alpha_h + \omega_h - \bar{\omega})})$. Under ideal conditions, all nodes are now in phase.
5. To account for synchronization errors, a final synchronization phase in which all nodes participate concludes the overall synchronization process.

Fig. 2 illustrates this procedure. The crucial idea of this approach is applied in Step 4. Since nodes inside a cluster have already been synchronized, they are still in phase after all applying an identical phase offset. Because this offset is the phase alteration the representative nodes experienced during their synchronization, all nodes should be synchronized after this step.

A potenti… only one clu… the inactive … out of pha… However, w… nization is p… we do not co… that all coo… no internode… Dependir… stage might … energy cons… depth and t… participating … assume that … size. This r… network size … depths, and … demonstrate … arbitrarily s… number of t… depth and … $\mathcal{O}(n^2)$ (cf. Ap… Society [Digi… org/10.1109… time is dep… hierarchy de… the original … be composed … clusters.

4 An As…

Since no loc… strong multi…

1608 IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 10, NO. 11, NOVEMBER 2011

$$\begin{aligned} E[T_P] &\leq \sum_{i=0}^{n-1} \frac{e \cdot n \cdot k}{n-i} \\ &= e \cdot n \cdot k \cdot \sum_{i=1}^{n} \frac{1}{i} \\ &< e \cdot n \cdot k \cdot (\ln(n) + 1) \\ &= \mathcal{O}(n \cdot k \cdot \log n). \end{aligned} \tag{8}$$

2.2 A Lower Bound on the Expected Synchronization Time

After the initialization, the phases of the carrier signals are identically and independently distributed. Consequently, for a superimposed received sum signal ζ, each bit in the binary string s_ζ that represents the corresponding search point has an equal probability to be 1 or 0. The probability to start from a search point s_ζ with Hamming distance $h(s_{\text{opt}}, s_\zeta)$ not larger than $l \in \mathbb{N}$; $l \ll n \cdot \log(k)$ to one of the global optima s_{opt} directly after the random initialization is at most

$$\begin{aligned} P[\Lambda(s_{\text{opt}}, s_\zeta) \leq l] &= \sum_{i=1}^{l} \binom{n \cdot \log(k)}{n \cdot \log(k) - i} \cdot \frac{k}{2^{n \cdot \log(k) - i}} \\ &\leq \frac{(n \cdot \log(k))^{l+2}}{2^{n \cdot \log(k) - l}}. \end{aligned}$$

In this formula,

$$\binom{n \cdot \log(k)}{n \cdot \log(k) - i} \tag{9}$$

is the count of possible configurations with i bit errors to a given global optimum, $\frac{1}{2^{n \cdot \log(k)}}$ represents the probability for all these bits to be correct, and k is the count of global optima. This means that with high probability (w.h.p.) the Hamming distance to the nearest global optimum is at least l. We use the method of the expected progress to calculate a lower bound on the optimization time.

Let $\Lambda(s_\zeta, t)$ denote the situation that search point s_ζ is achieved after t iterations of the algorithm. We assume a progress measure $\Lambda : \mathbb{B}^{n \cdot \log(k)} \to \mathbb{R}_0^+$ such that $\Lambda(s_\zeta, t) < \Delta$ represents the case that a global optimum was not found in the first t iterations. For every $t \in \mathbb{N}$, we have

$$\begin{aligned} E[T_P] &\geq t \cdot P[T_P > t] \\ &= t \cdot P[\Lambda(s_\zeta, t) < \Delta] \\ &= t \cdot (1 - P[\Lambda(s_\zeta, t) \geq \Delta]). \end{aligned} \tag{10}$$

With the help of the Markov inequality, we obtain

$$P[\Lambda(s_\zeta, t) \geq \Delta] \leq \frac{E[\Lambda(s_\zeta, t)]}{\Delta}, \tag{11}$$

and, therefore,

$$E[T_P] \geq t \cdot \left(1 - \frac{E[\Lambda(s_\zeta, t)]}{\Delta}\right). \tag{12}$$

This means that we can obtain a lower bound on the optimization time by providing the expected progress after t iterations. The probability for l bits to correctly flip is at most

$$\left(1 - \frac{1}{n \cdot \log(k)}\right)^{n \log(k) - l} \cdot \left(\frac{1}{n \cdot \log(k)}\right)^{l} \leq \frac{1}{(n \cdot \log(k))^{l}}. \tag{13}$$

In this formula, $(1 - \frac{1}{n \log(k)})^{n \log(k) - l}$ describes the probability that all "correct" bits remain unchanged while the remaining l bits flip with probability $(\frac{1}{n \log(k)})^{l}$. The expected progress in one iteration is, therefore,

$$\begin{aligned} E[\Lambda(s_\zeta, t), \Lambda(s_\zeta, t+1)] &\leq \sum_{i=1}^{l} \frac{i}{(n \cdot \log(k))^{i}} \\ &< \frac{2}{n \cdot \log(k)}, \end{aligned} \tag{14}$$

and the expected progress in t iterations is, consequently, not greater than $\frac{2 \cdot n \log(k) \cdot \Delta}{n \log(k)} - 1$. When we choose $t = \frac{2 \cdot n \log(k) \cdot \Delta}{n \log(k)} - 1$, the twice of the expected progress is still smaller than Δ. With the Markov inequality, we can show that this progress is not achieved with probability $\frac{1}{2}$. Altogether we conclude that the expected synchronization time is bounded from below by

$$\begin{aligned} E[T_P] &\geq t \cdot \left(1 - \frac{E[\Lambda(s_\zeta, t)]}{\Delta}\right) \\ &\geq \frac{n \cdot \log(k) \cdot \Delta}{4} \cdot \left(1 - \frac{2 \cdot n \log(k) \cdot \Delta}{4 \cdot n \log(k)}\right) \\ &= \Omega(n \cdot \log(k) \cdot \Delta). \end{aligned} \tag{15}$$

With $\Delta = k \cdot \frac{\log(n)}{\log(k)}$, we obtain a lower bound in the same order as the upper bound derived in Section 2.1 and, consequently, an asymptotically sharp bound of

$$E[T_P] = \Theta(n \cdot k \cdot \log(n)). \tag{16}$$

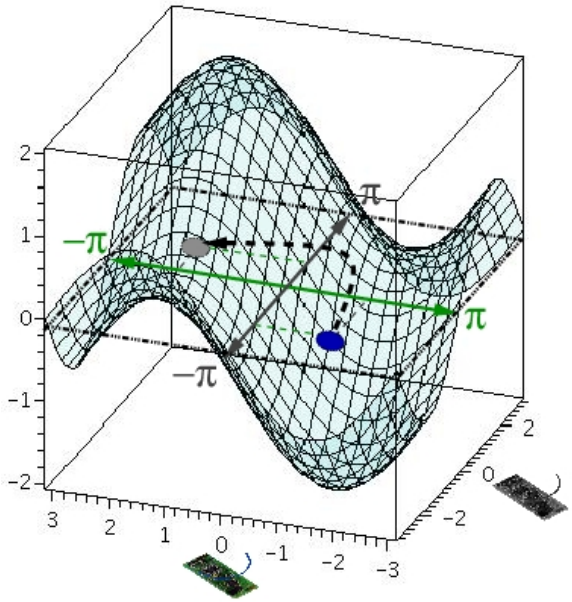
Note that in [41], an upper bound on the expected asymptotic synchronization time was derived that scales linearly in the number of nodes n when the probability distribution is optimally altered repeatedly during the synchronization. However, simulation results derived for a fixed uniform distribution in this study also indicate a logarithmic factor in the synchronization time of 1-bit feedback-based synchronization.

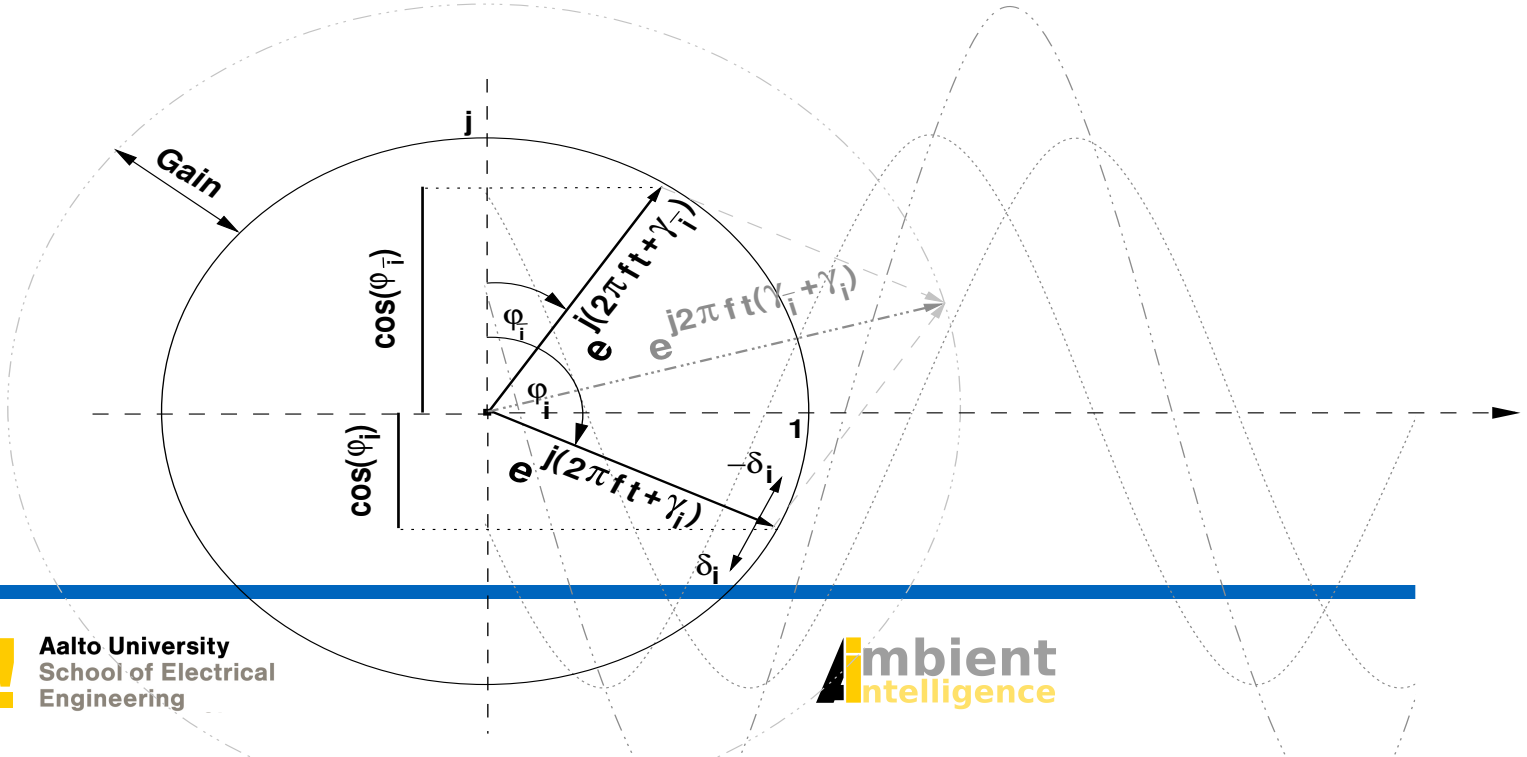
3 Hierarchical Clustering

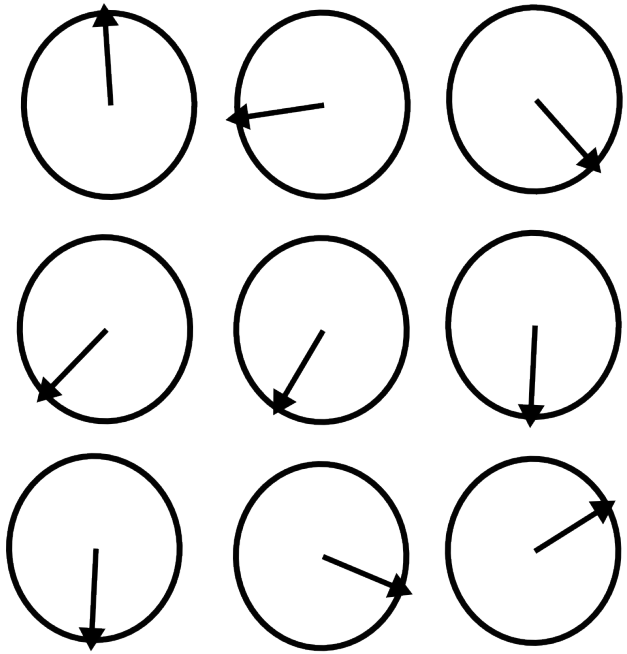
A further improvement of the synchronization time can be achieved by synchronizing smaller clusters of nodes separately. Since this bound on the synchronization time grows faster than linearly with the network size n, but the received signal strength RSS_{sum} of the received superimposed signal grows linearly with n, the overall energy consumption and synchronization time might be reduced when fewer nodes transmit for a shorter time, but with an increased transmission power. Note that currently most low-cost radios are not capable of altering their transmission power and, therefore, are not able to exploit this property. More sophisticated radios could, however, achieve carrier phase synchronization more efficiently when this fact is utilized. We propose the following hierarchical clustering scheme that synchronizes all transmit nodes iteratively in clusters of reduced size.

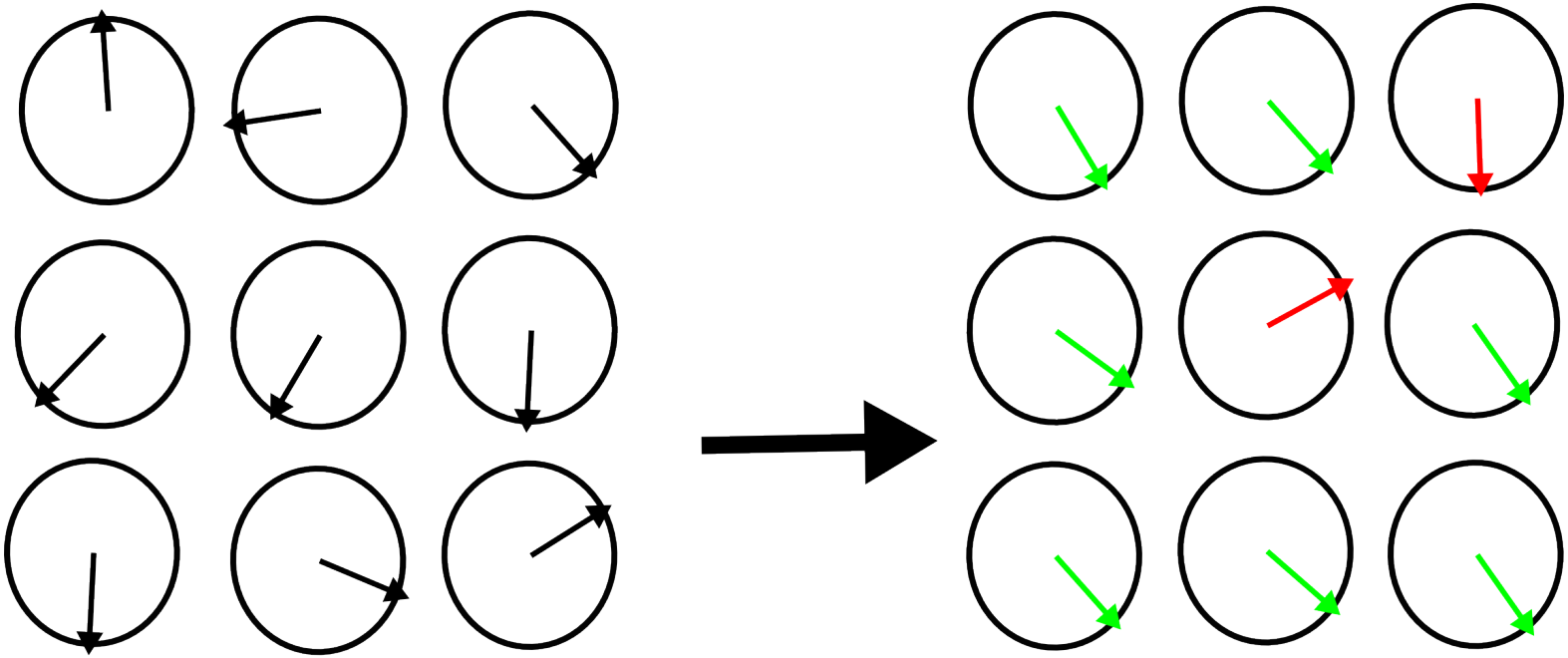
Feedback-based distributed adaptive beamforming

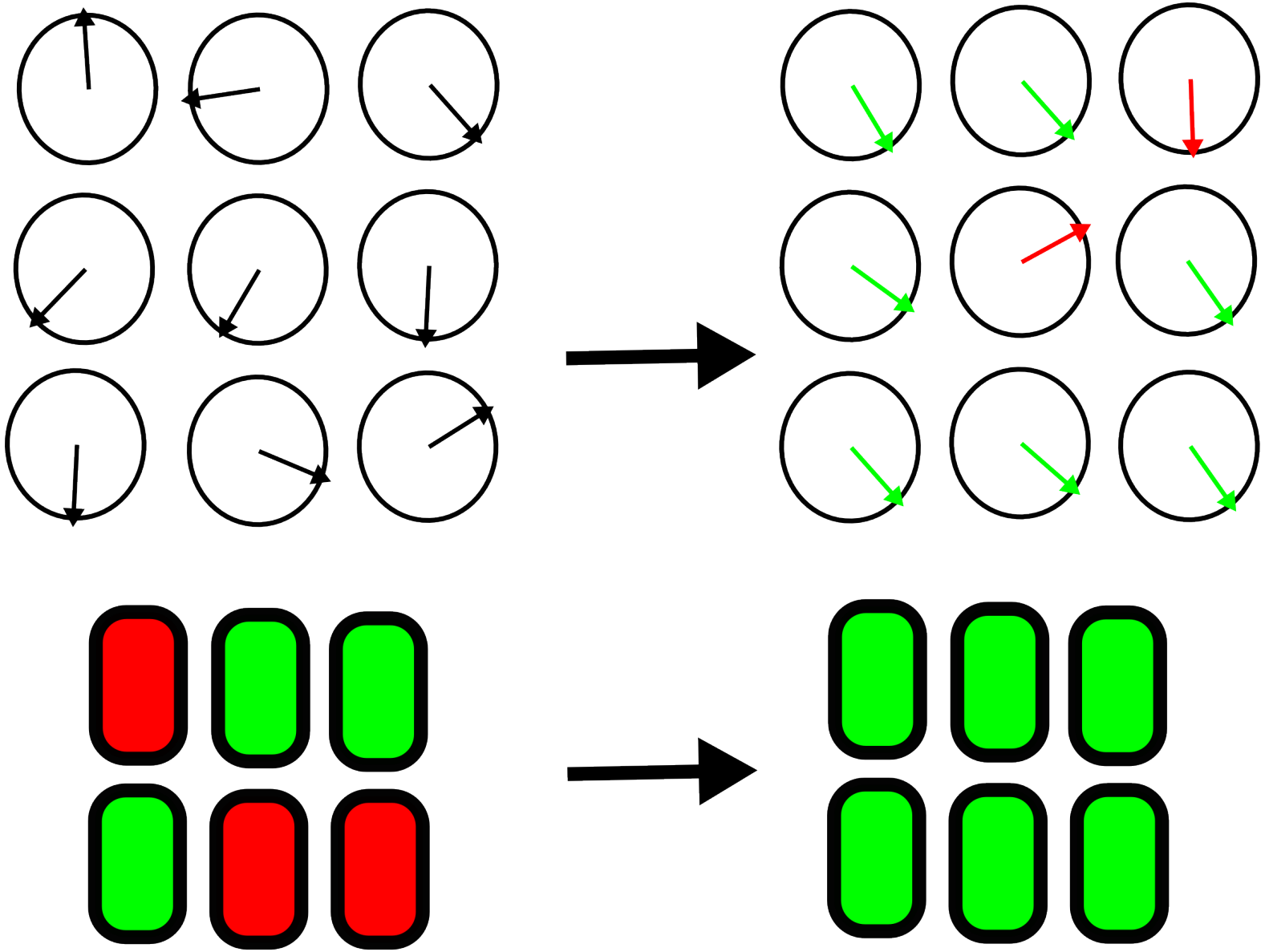
- Weak multimodal fitness function
- Single local=global optimum





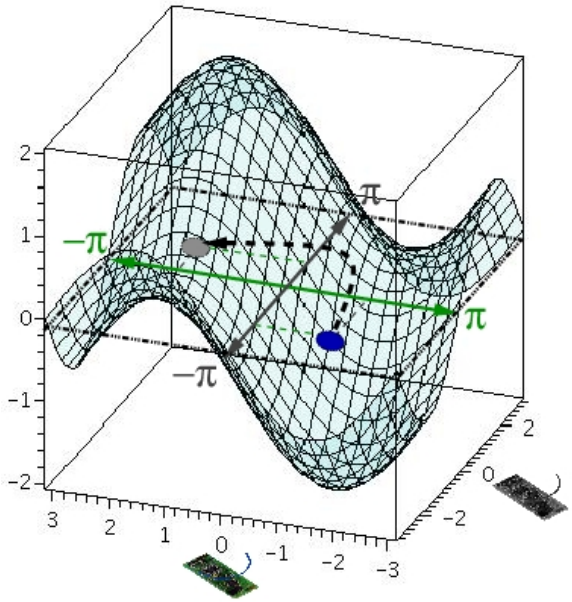


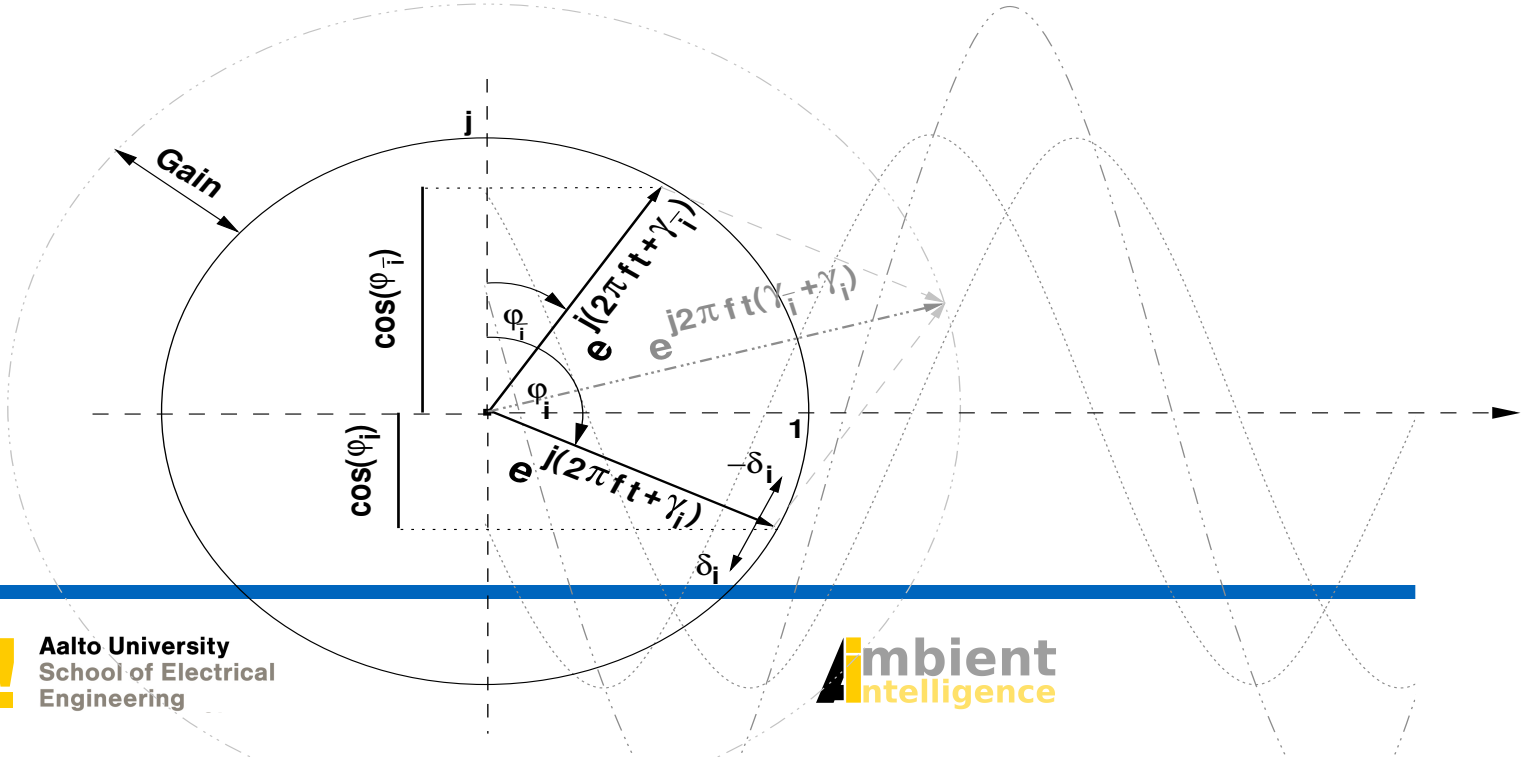




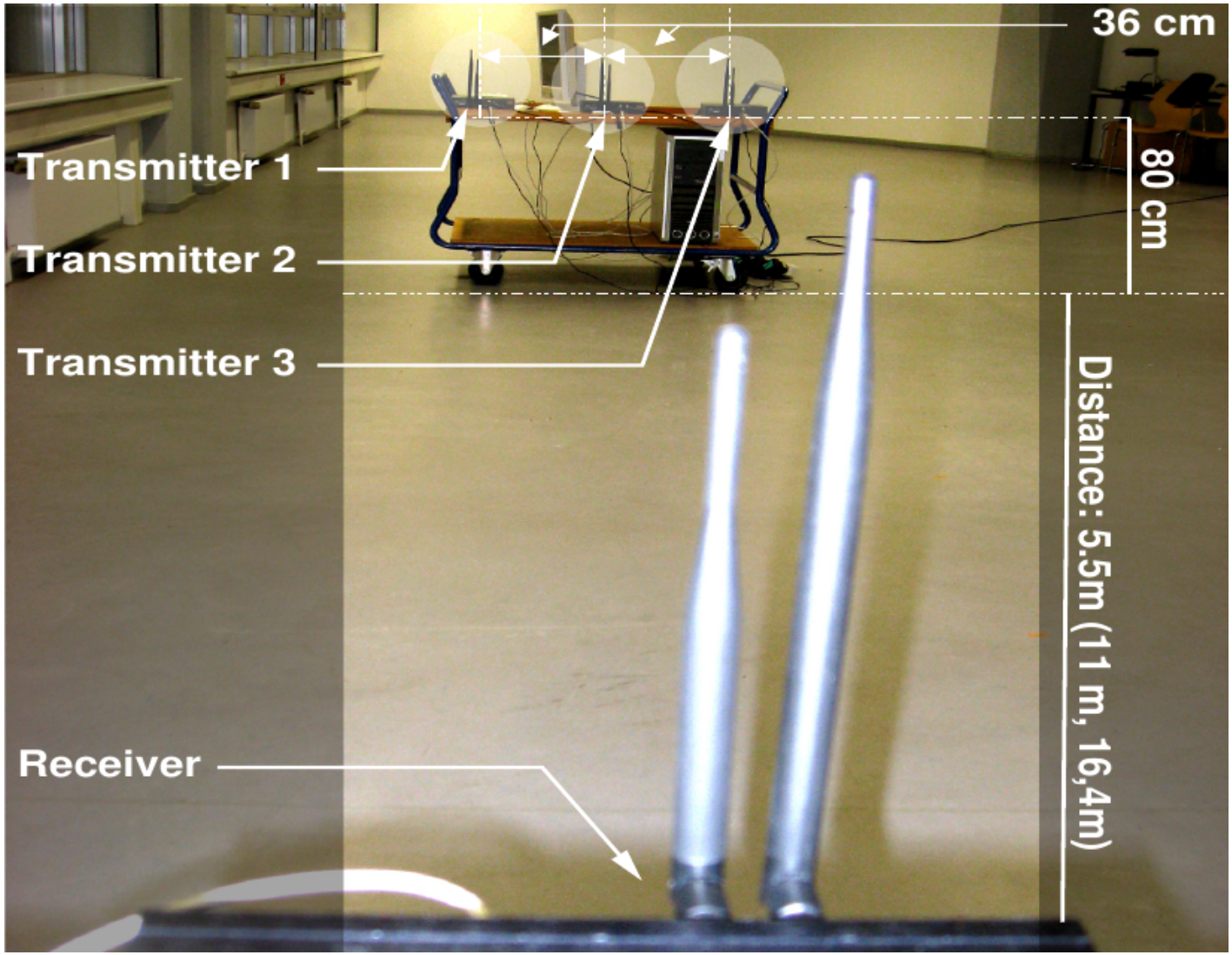
Feedback-based distributed adaptive beamforming

- Weak multimodal fitness function
- Single local=global optimum

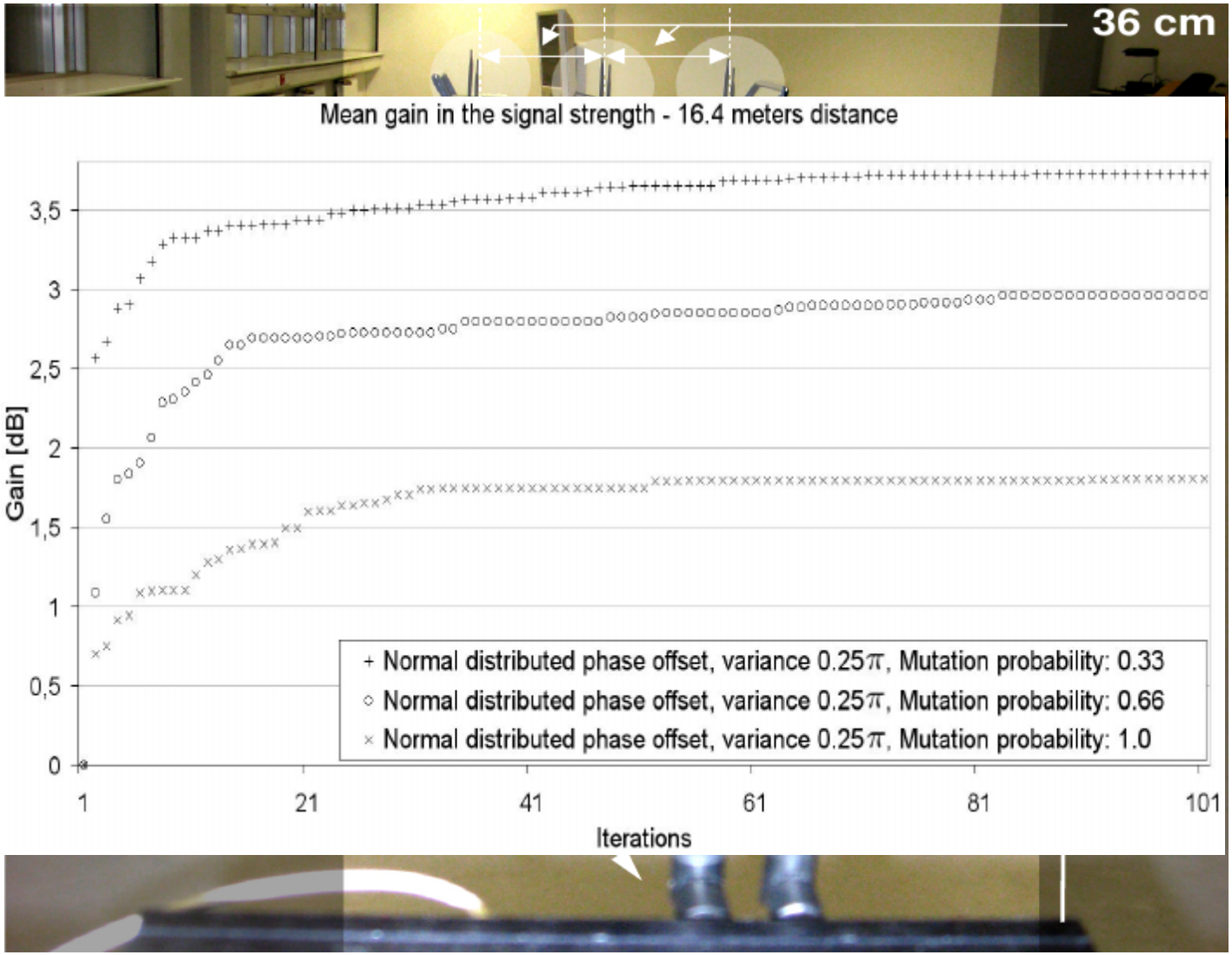




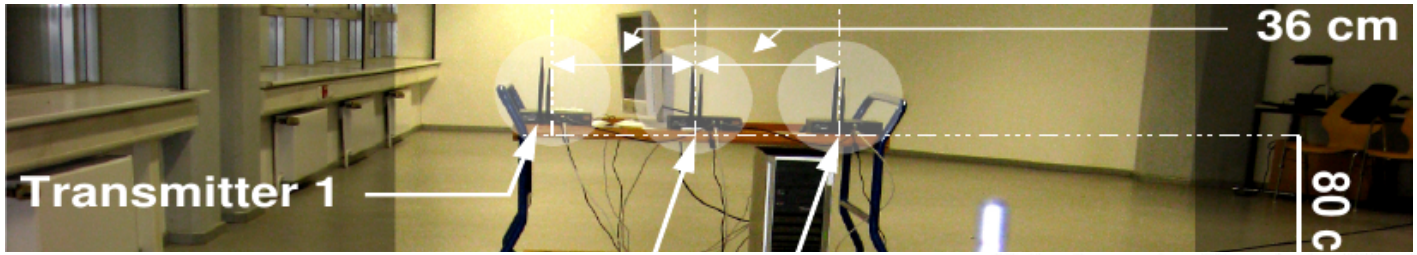
Feedback-based distributed adaptive beamforming



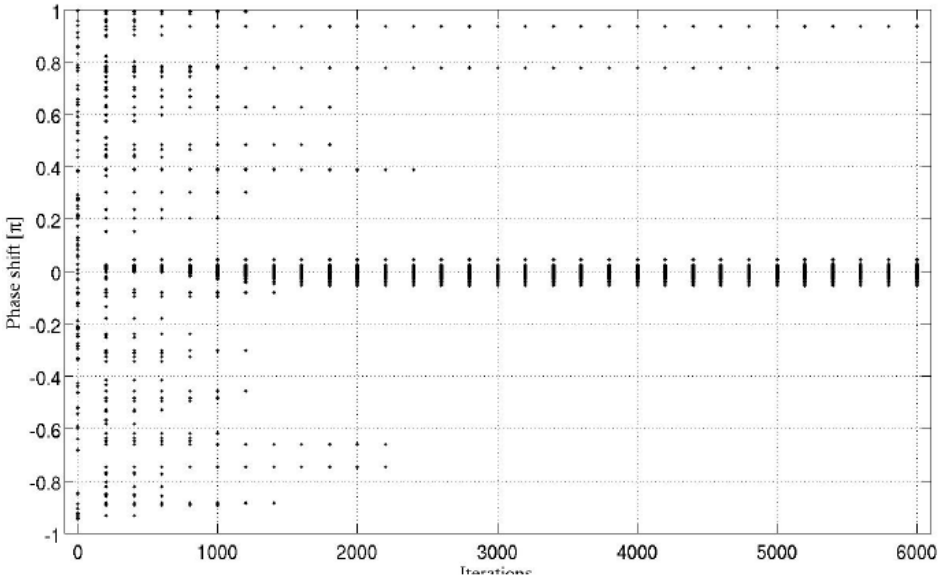
Feedback-based distributed adaptive beamforming



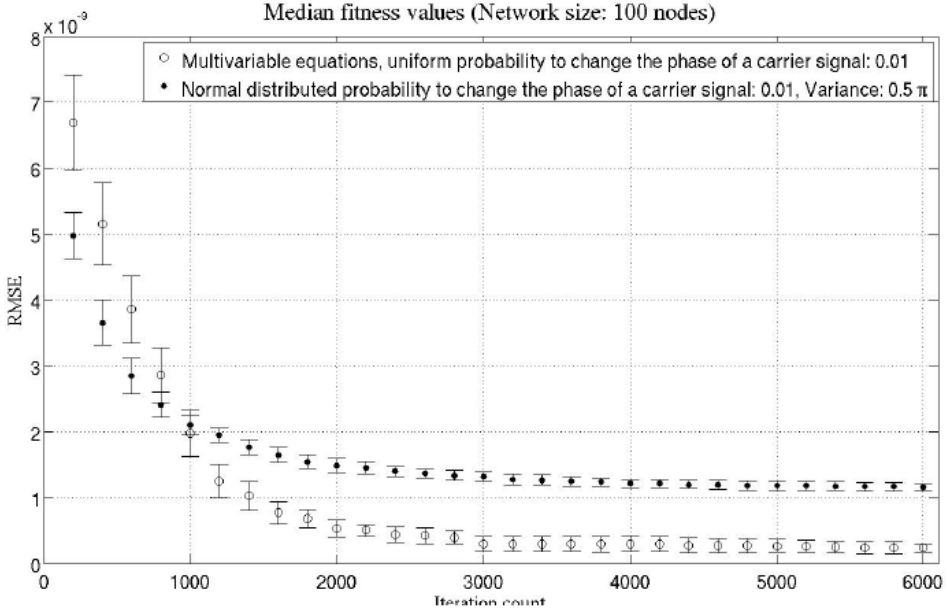
Feedback-based distributed adaptive beamforming

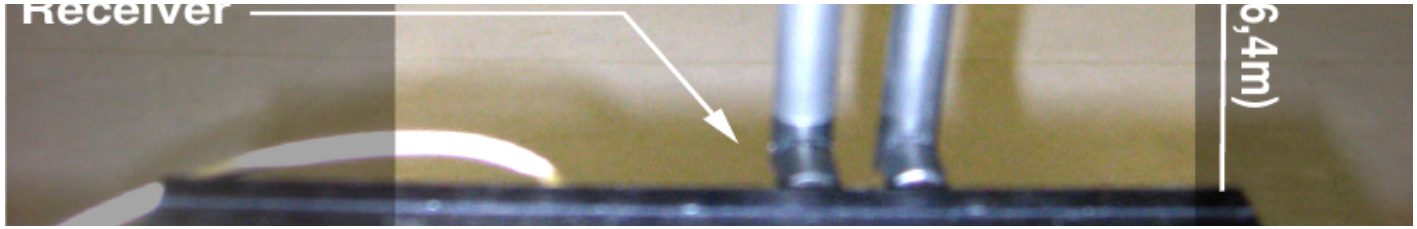


Relative phase shift (Network size: 100)



Median fitness values (Network size: 100 nodes)





Cheap collaboration

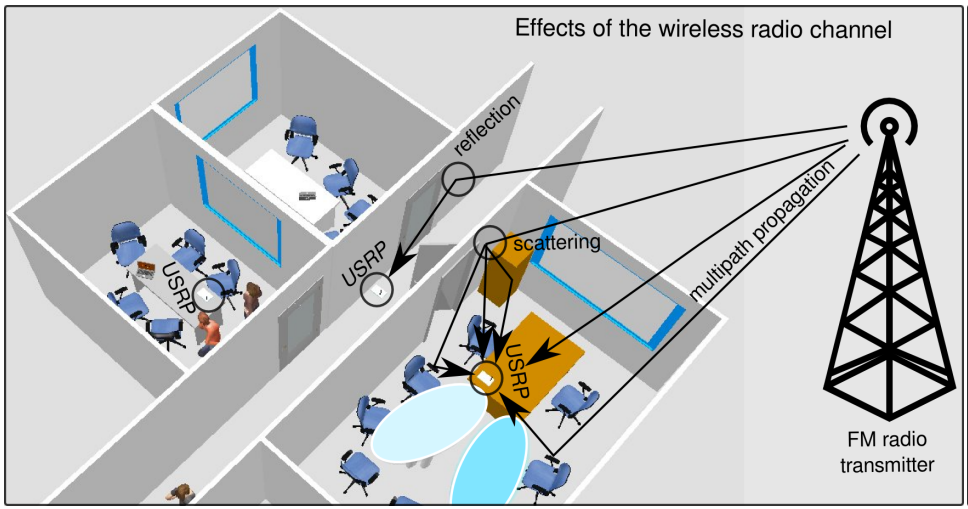
Radio Vision

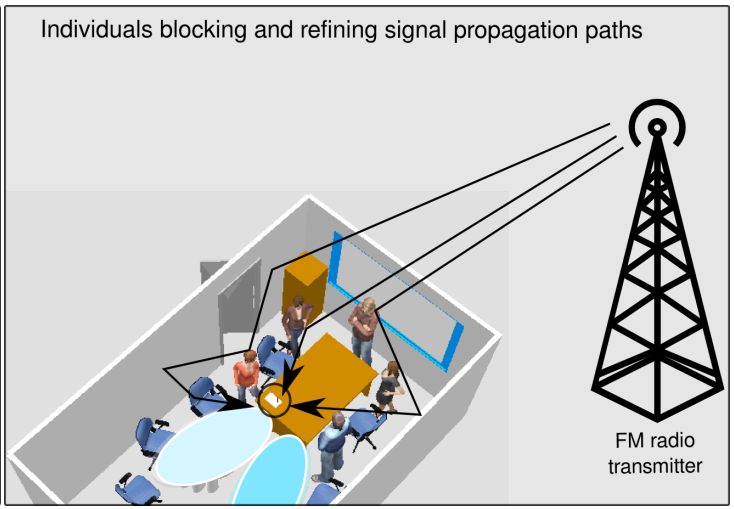
Security from ambient signals

g

RF-sensing for environmental perception

- Multi-path propagation
- Signal superimposition
- Scattering
- Signal Phase
- Reflection
- Blocking of signal paths
- Doppler Shift
- Fresnel effects

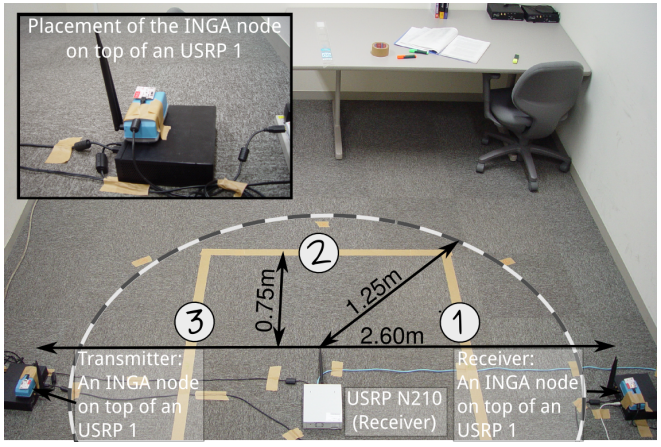


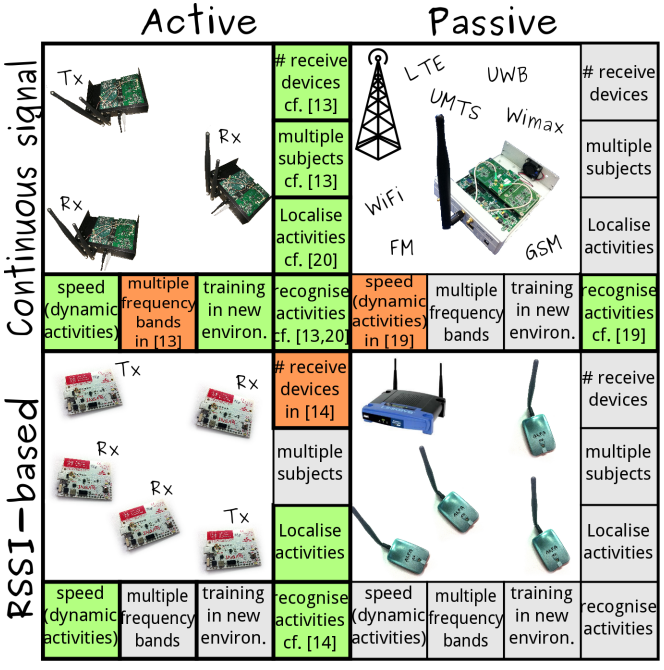


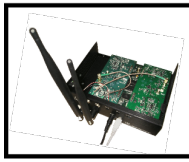
RF-based activity recognition

Sensewaves Video

RF-based device-free activity recognition







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

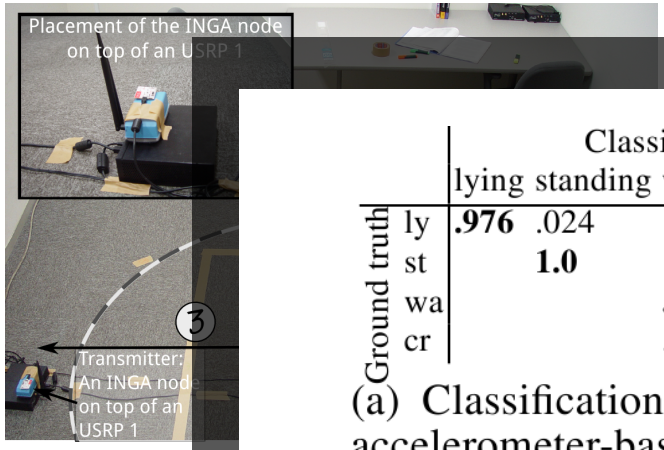
Passive SDR-based DFAR (USRP N210)
Frequency: 82.5MHz (WBX board), Vert900 Antenna, 4dBi antenna gain
Signal: Environmental FM radio captured from a nearby radio station
Sample rate: 64Hz

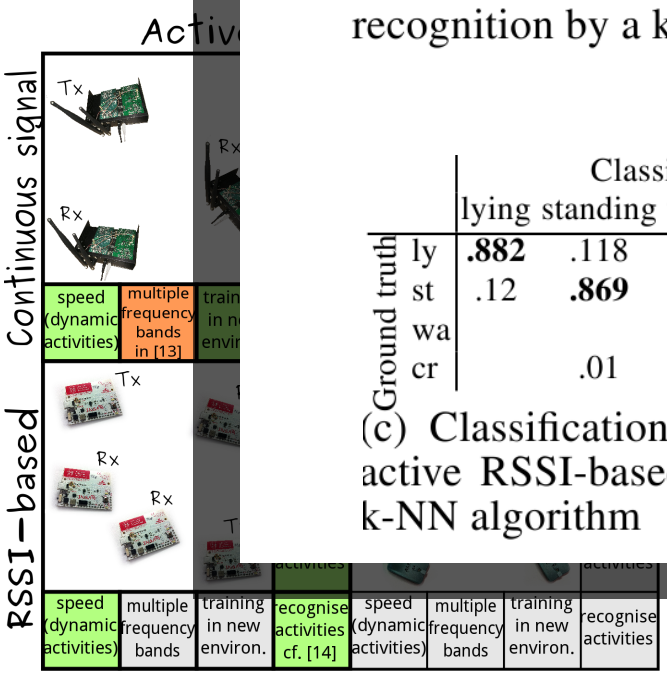
Active RSSI-based DFAR (INGA wsn nodes, v1.4)
Frequency: 2.4GHz IEEE802.15.4, PCB High Gain-Antenna
Signal: RSSI samples from packets transmitted between nodes
Sample rate: Transmission of 100 packets per second

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

walking
standing
Crawling
Lying
empty

RF-based device-free activity recognition





Ground truth	Classification: ly	st	wa	cr
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	Classification: ly	st	wa	cr
ly	**.904**	.096		
st	.096	**.898**	.006	
wa		.013	**.962**	.025
cr		.038	.212	**.75**

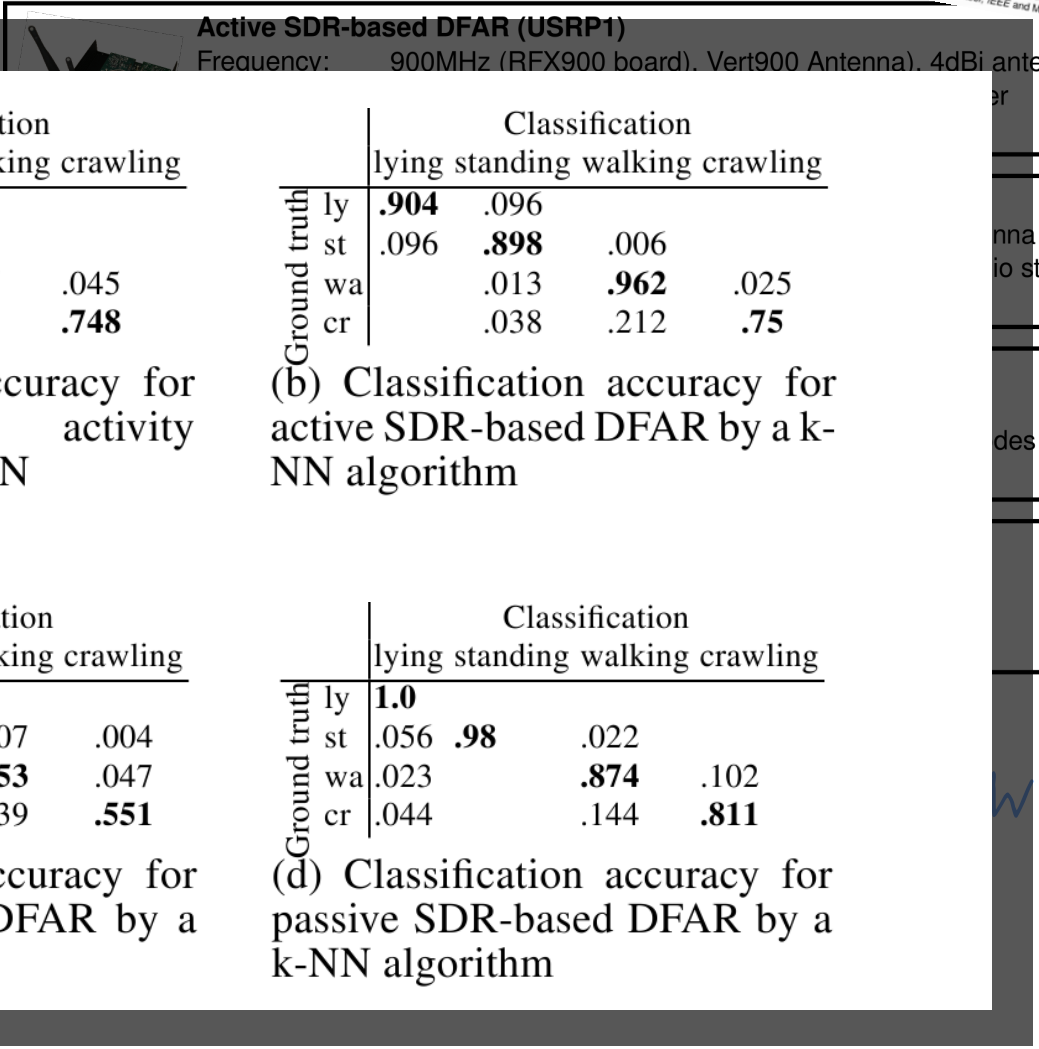
(b) Classification accuracy for active SDR-based DFAR by a k-NN algorithm

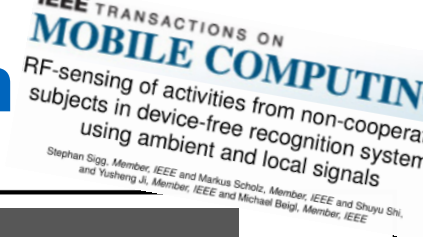
Ground truth	Classification: ly	st	wa	cr
ly	**.882**	.118		
st	.12	**.869**	.007	.004
wa			**.953**	.047
cr		.01	.439	**.551**

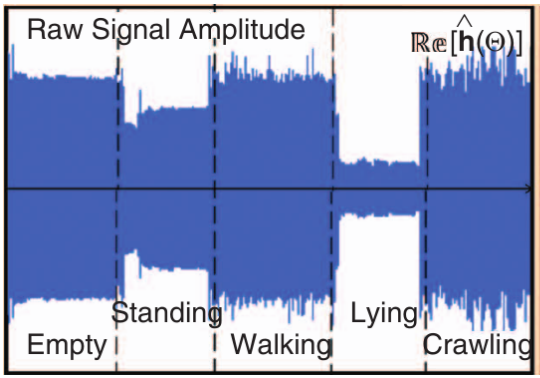
(c) Classification accuracy for active RSSI-based DFAR by a k-NN algorithm

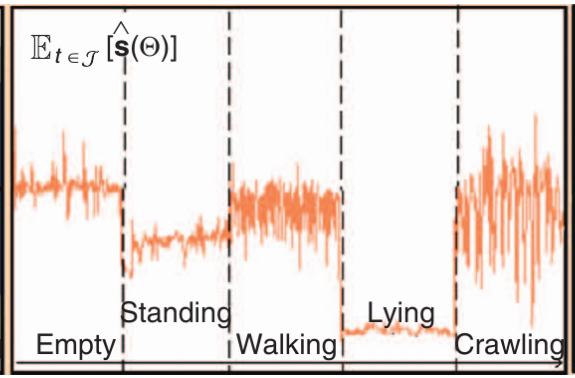
Ground truth	Classification: ly	st	wa	cr
ly	**1.0**			
st	.056	**.98**	.022	
wa	.023		**.874**	.102
cr	.044		.144	**.811**

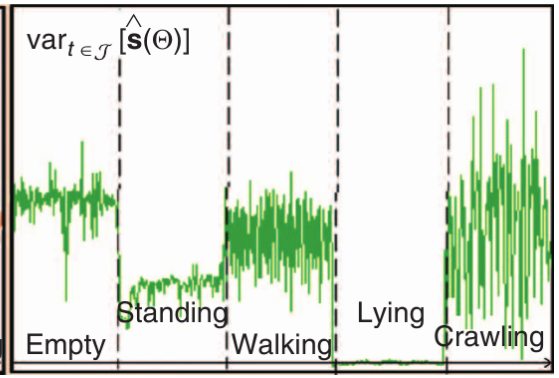
(d) Classification accuracy for passive SDR-based DFAR by a k-NN algorithm



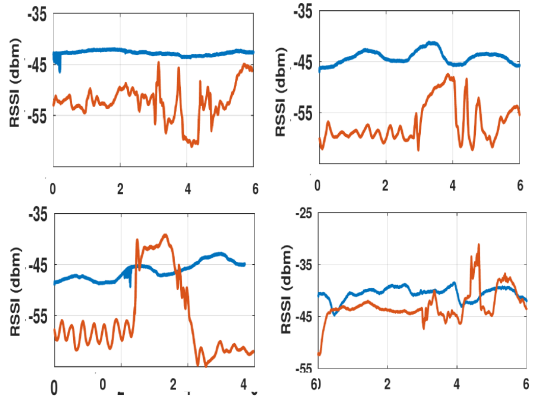



Raw Signal Amplitude
$\mathbb{R}\mathrm{e}[\hat{\mathbf{h}}(\Theta)]$
Empty
Standing
Walking
Lying
Crawling

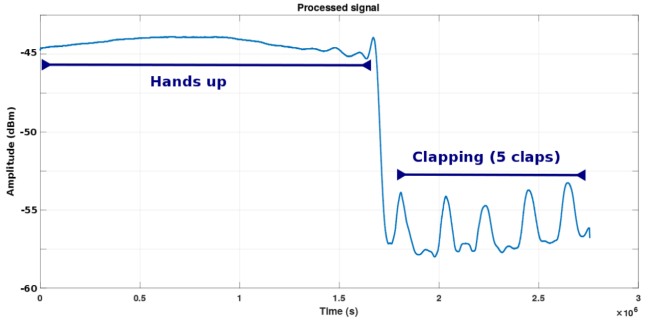

$\mathbb{E}_{t\in\mathcal{T}}[\hat{\mathbf{s}}(\Theta)]$
Empty
Standing
Walking
Lying
Crawling

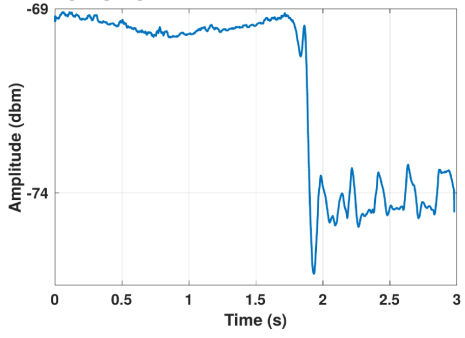

$\mathrm{var}_{t\in\mathcal{T}}[\hat{\mathbf{s}}(\Theta)]$
Empty
Standing
Walking
Lying
Crawling

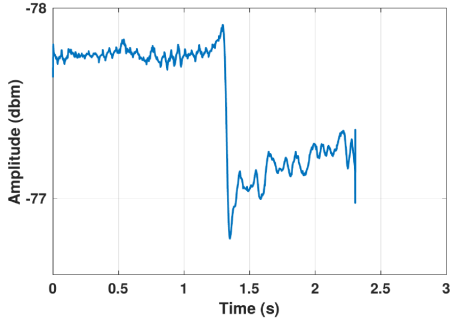

Angry, agitated driving


RSSI (dbm)

– Video –


Processed signal
Hands up
Clapping (5 claps)
Amplitude (dBm)
Time (s)


Amplitude (dbm)
Time (s)


Amplitude (dbm)
Time (s)

Cheap collaboration

Radio Vision

Security from ambient signals

Motivation

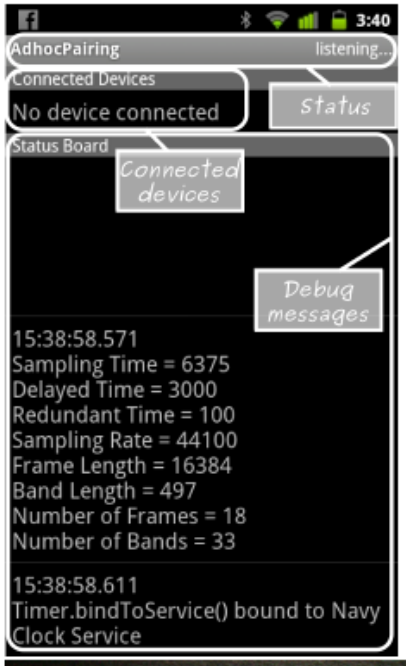
6

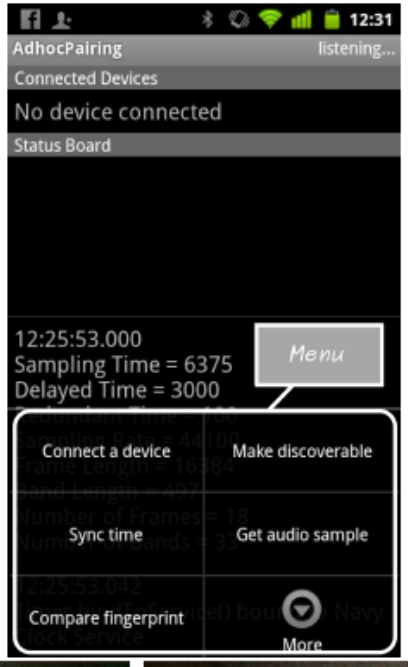
Motivation

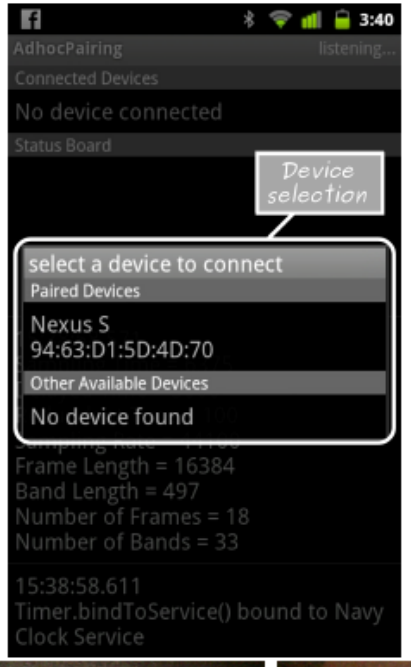
Trust and proximity

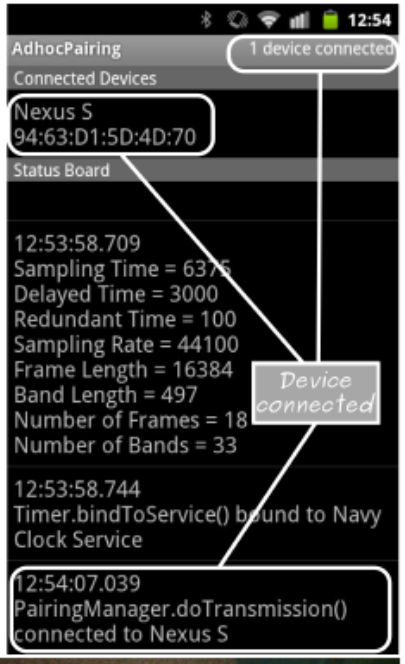
We will use audio as a source of common information in proximity

6


3:40
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


12:31
AdhocPairing
listening...
Connected Devices
No device connected
Status Board
12:25:53.000
Sampling Time = 6375
Delayed Time = 3000
Menu
Connect a device
Make discoverable
Sync time
Get audio sample
Compare fingerprint
More


3:40
AdhocPairing
listening...
Connected Devices
No device connected
Status Board
Device selection
select a device to connect
Paired Devices
Nexus S
94:63:D1:5D:4D:70
Other Available Devices
No device found
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

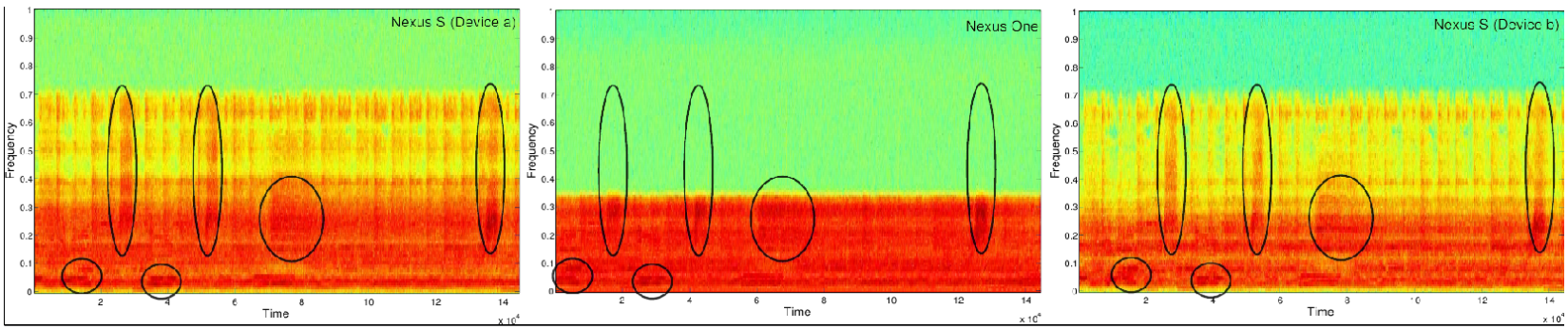

12:54
AdhocPairing
1 device connected
Connected Devices
Nexus S
94:63:D1:5D:4D:70
Status Board
12:53:58.709
Sampling Time = 6375
Delayed Time = 3000
Redundant Time = 100
Sampling Rate = 44100
Frame Length = 16384
Band Length = 497
Number of Frames = 18
Number of Bands = 33
Device connected
12:53:58.744
Timer.bindToService() bound to Navy Clock Service
12:54:07.039
PairingManager.doTransmission()
connected to Nexus S

Security from environmental stimuli

Real-time implementation on android mobile phones[a]

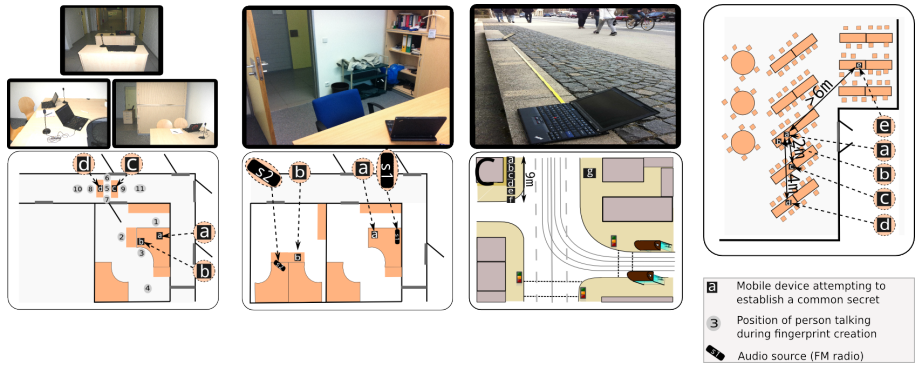
[a] Stephan Sigg, et al., AdhocPairing: Spontaneous audio-based secure device pairing for Android mobile devices, IWSSI 2012

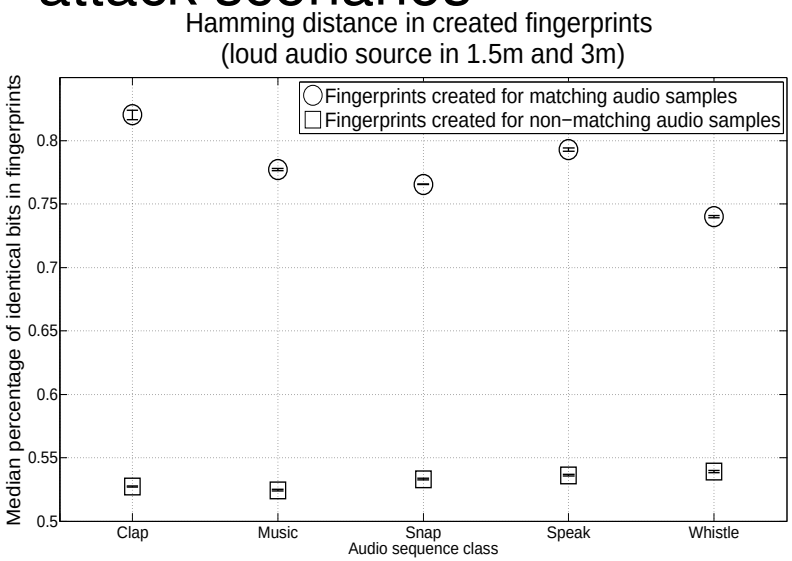
- Hardware noise cancellation on some phones
- Hardware originated synchronisation offset

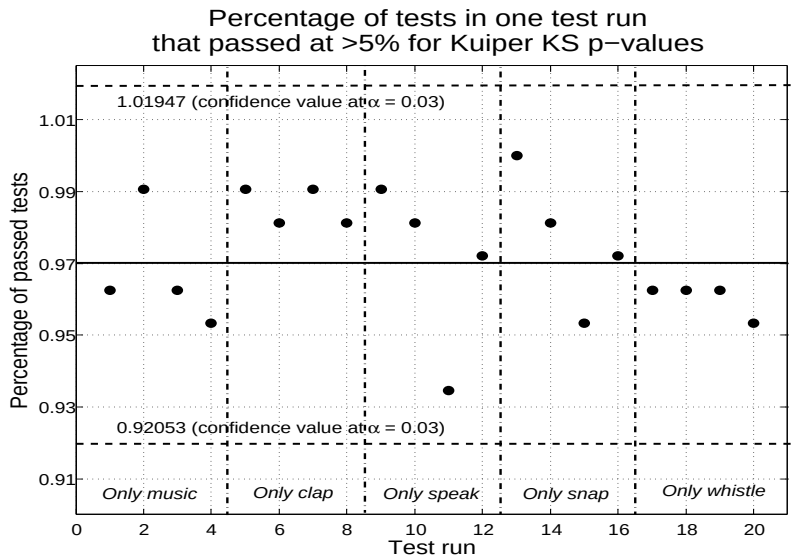


Audio-based ad-hoc secure pairing[1]

- Use audio to generate secret key
- high Entropy, fuzzy cryptography, case studies, attack scenarios

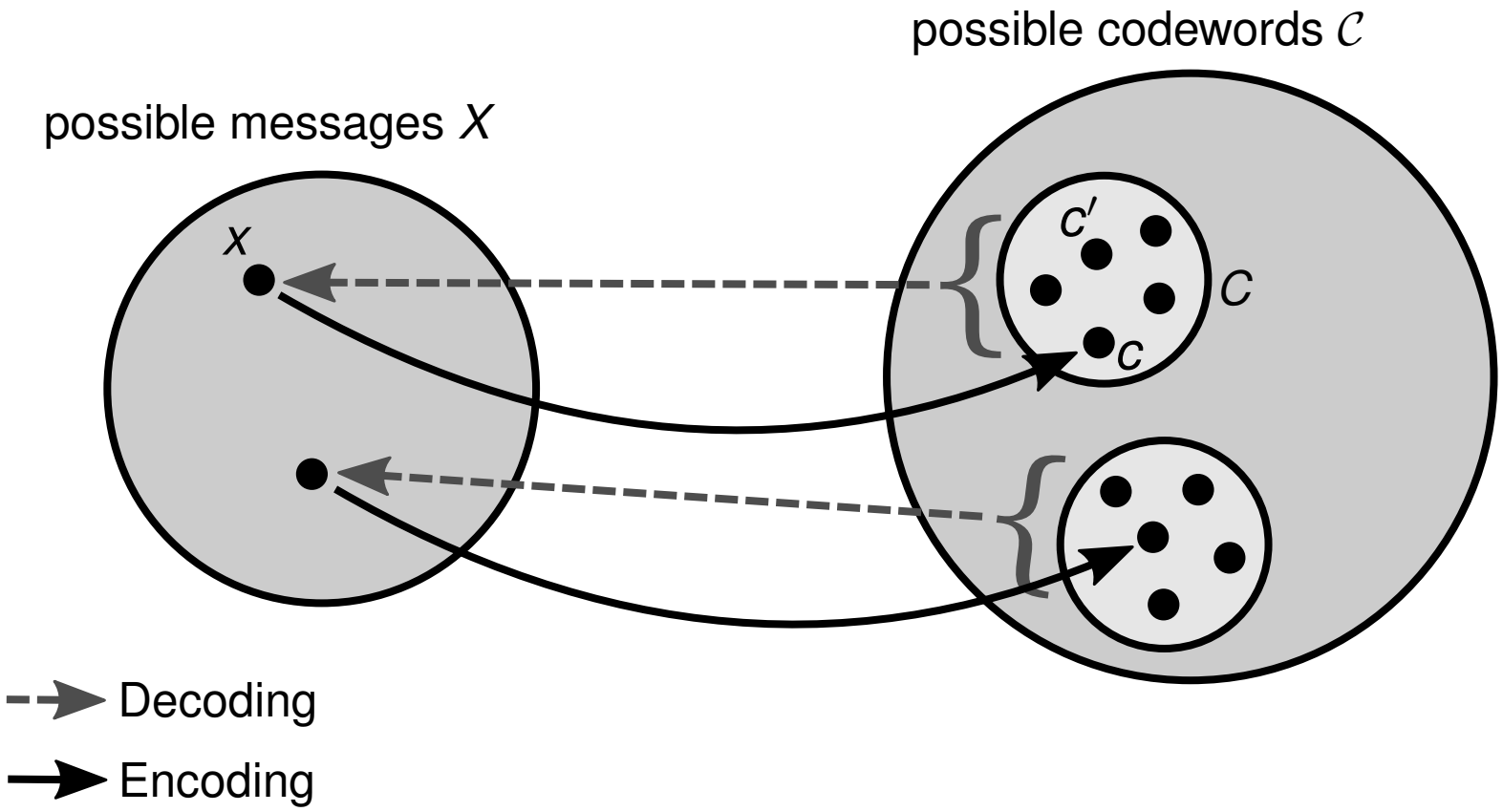




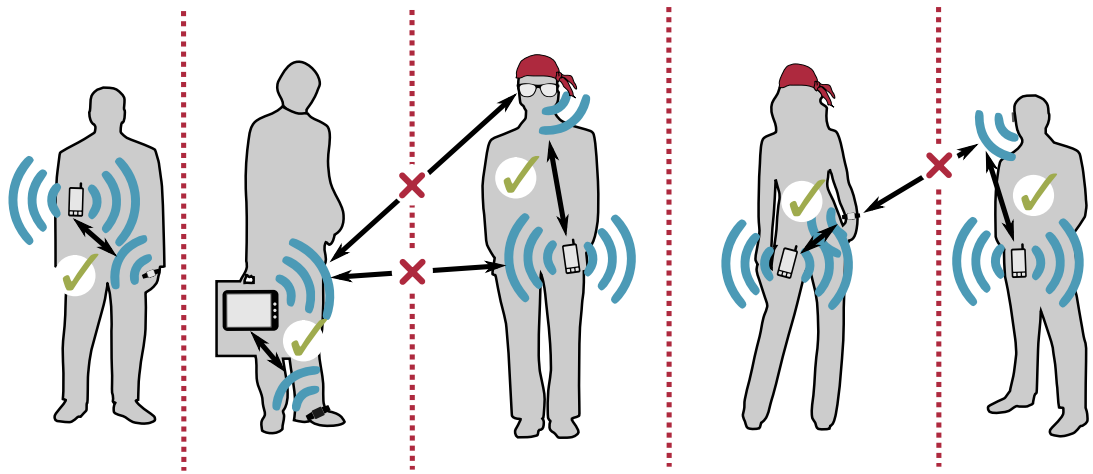


[1] S. Sigg et al., Secure Communication based on Ambient Audio, IEEE Transactions on Mobile Computing

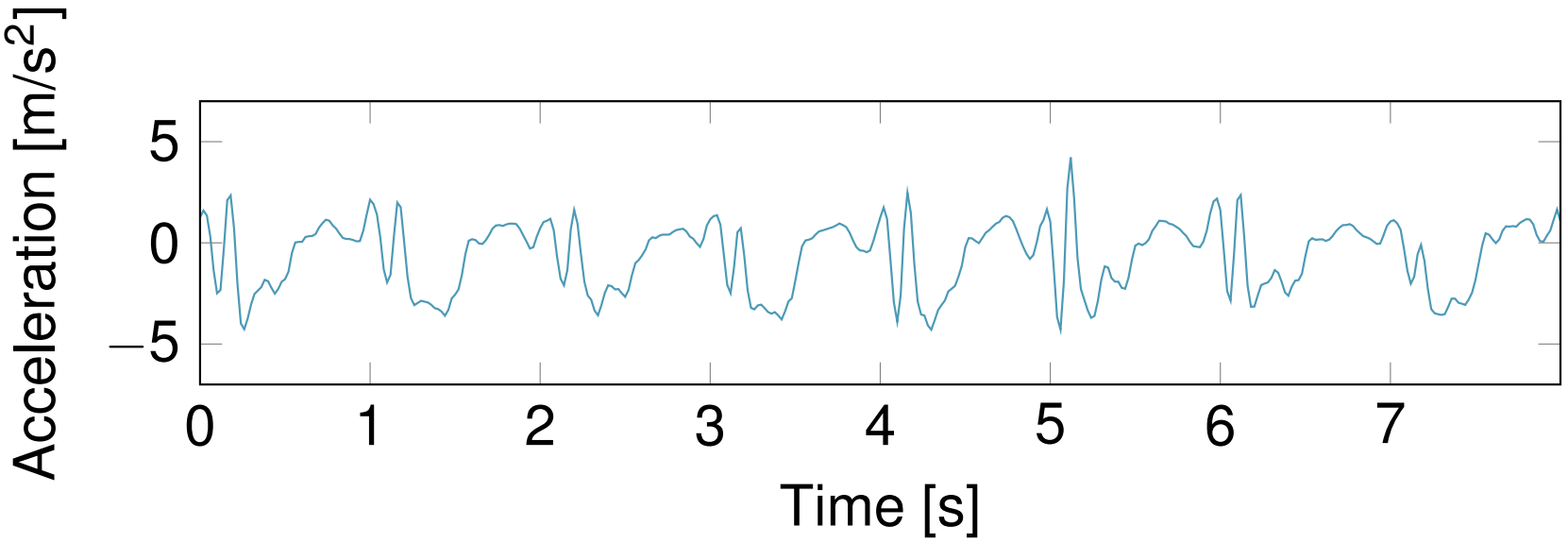
Secure pairing from noisy data



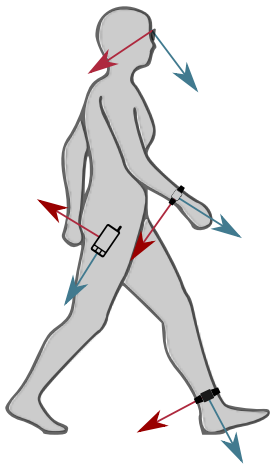
Device-to-Device Authentication



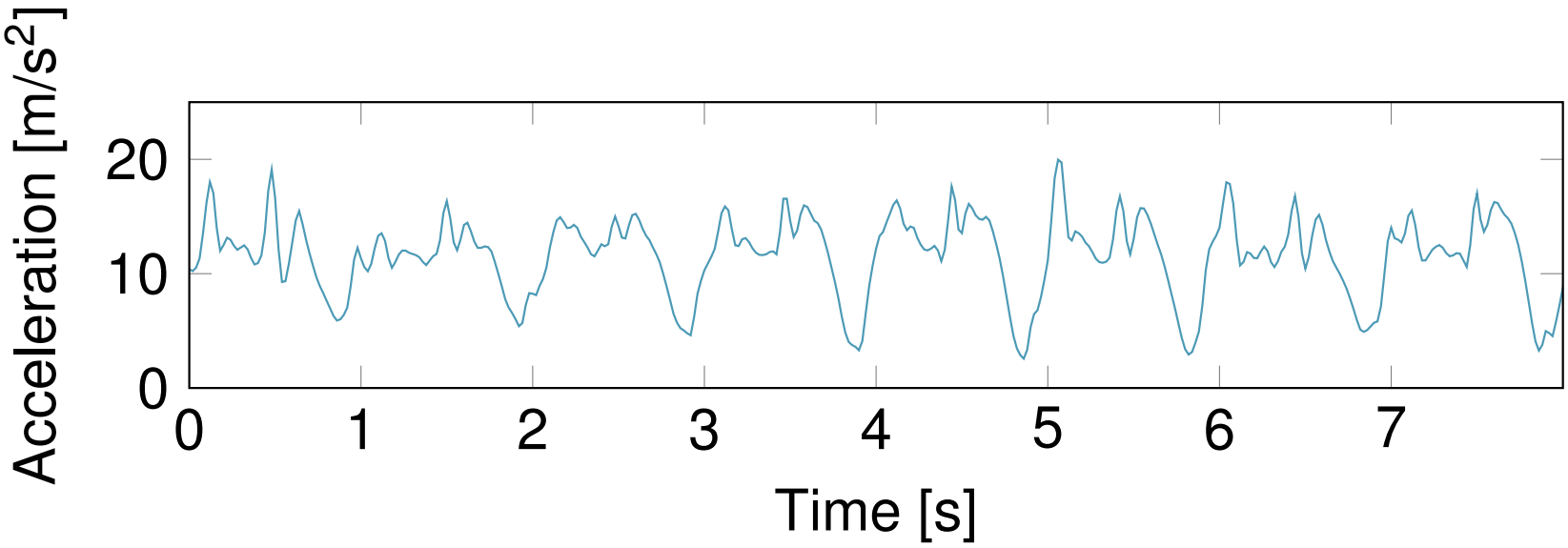
Accelerometer Reading



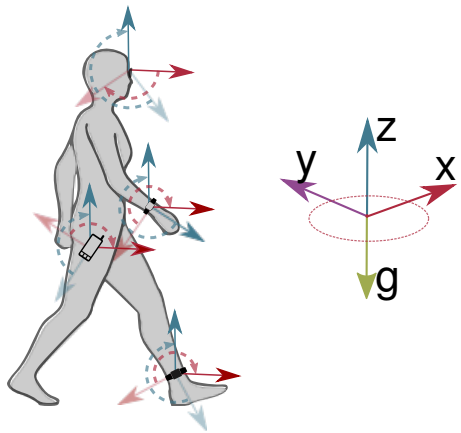
- Accelerometer reading on z-axis only



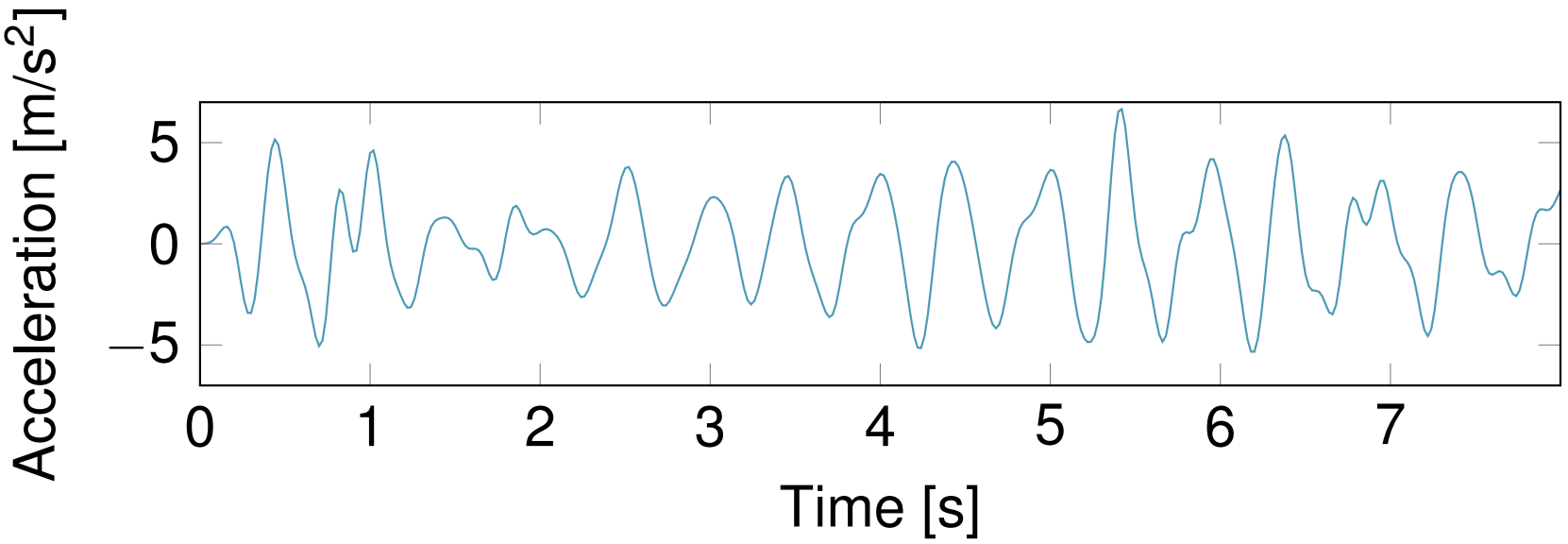
Rotated Signal



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

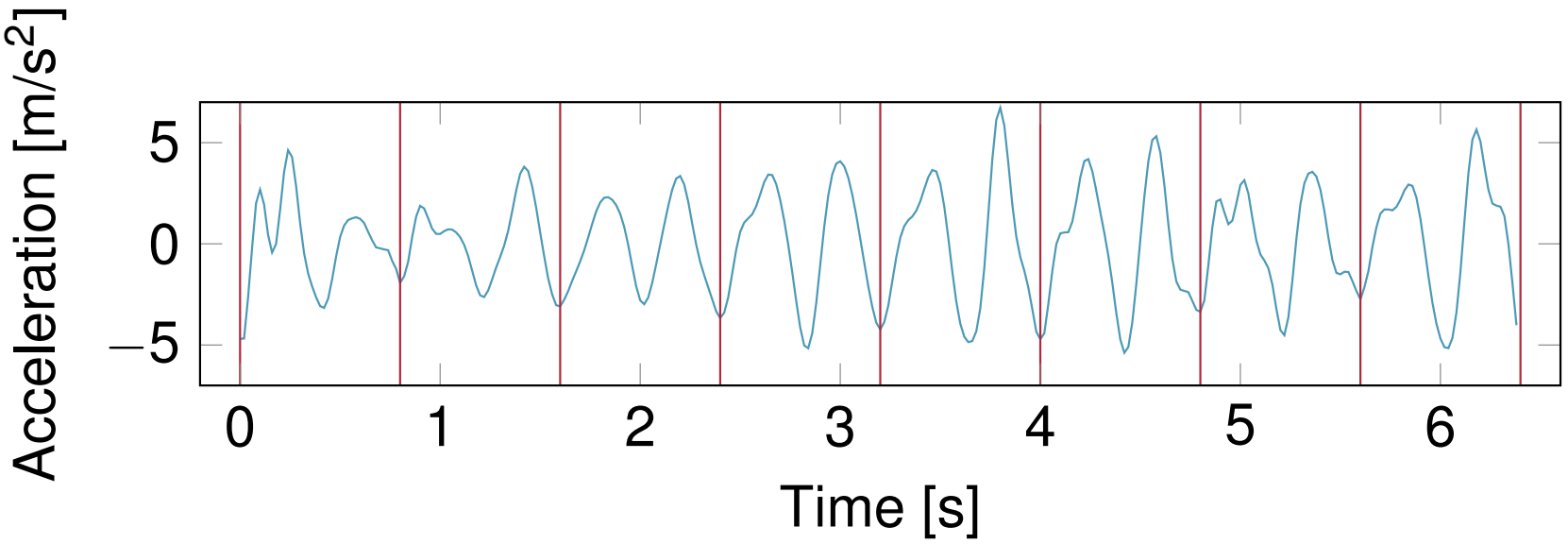


Noise-Reduced Signal



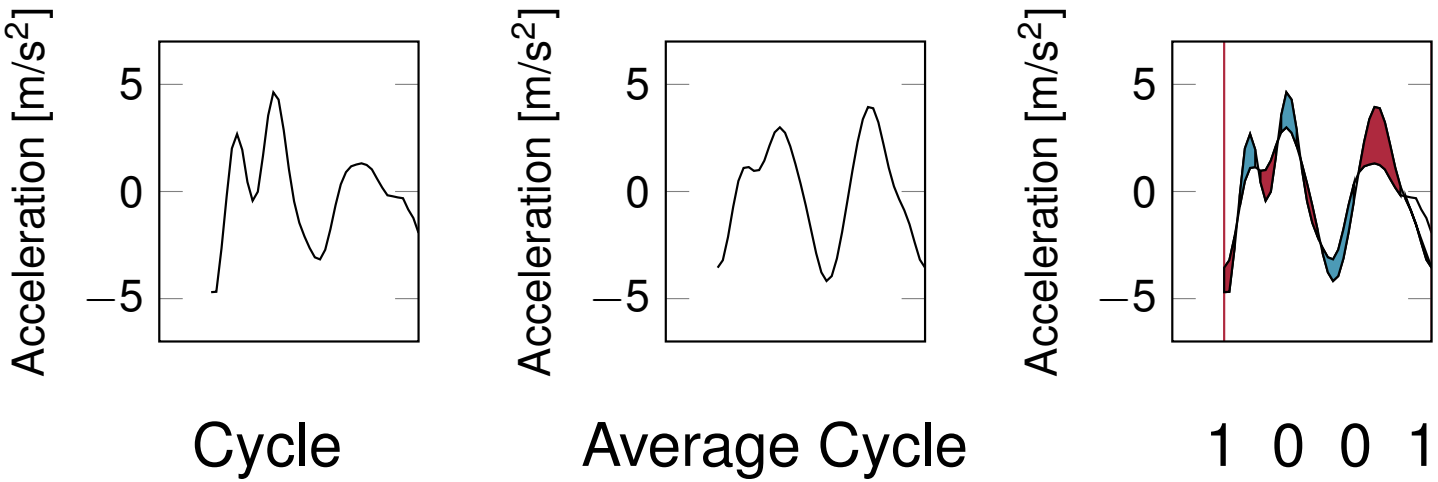
- Apply a bandpass filter to keep frequencies between 0.5 and 12 Hz

Gait-Cycle Detection



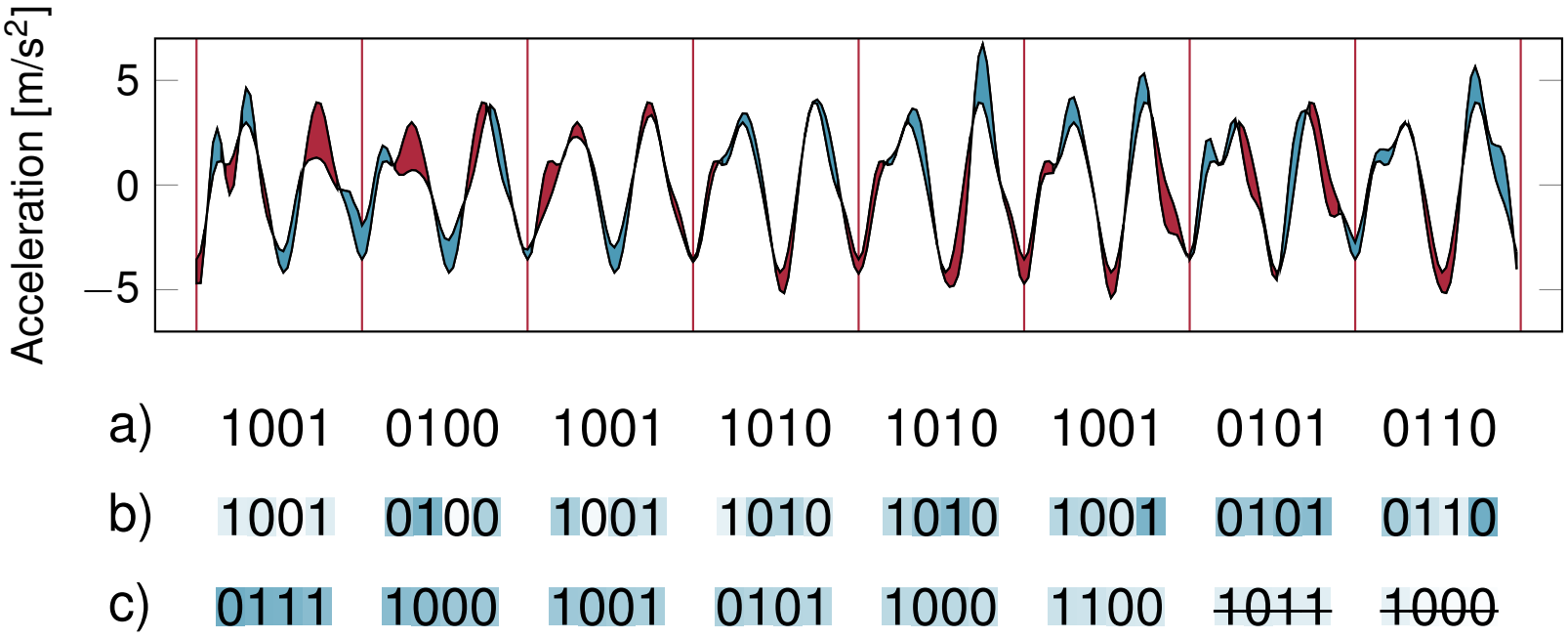
- Partition data into gait cycles
- Resample gait cycles to equal length
- Calculate average gait cycle

Quantization



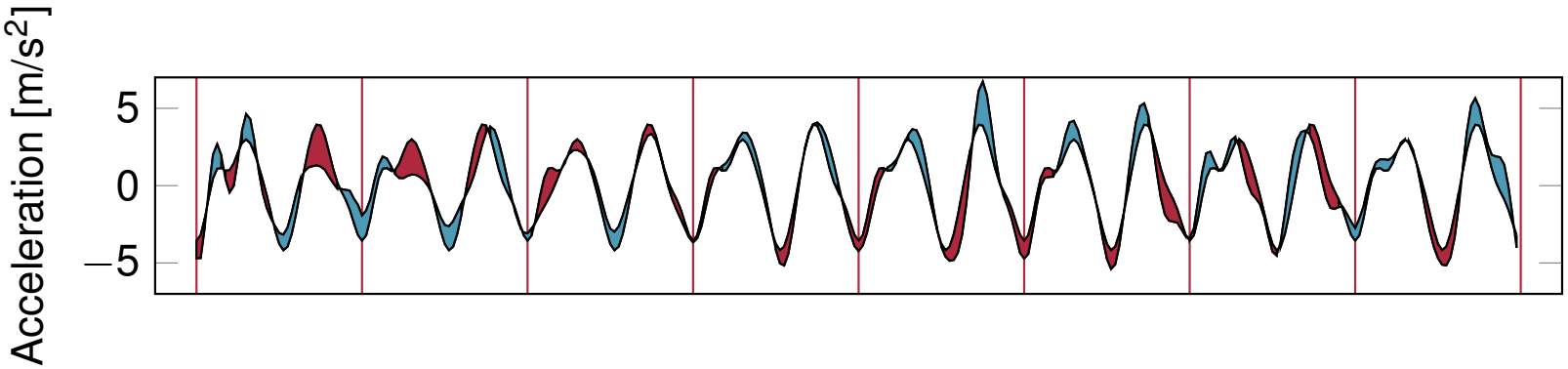
- Average gait cycle overlaid on each original gait cycle
- 4 bits per cycle

Quantization

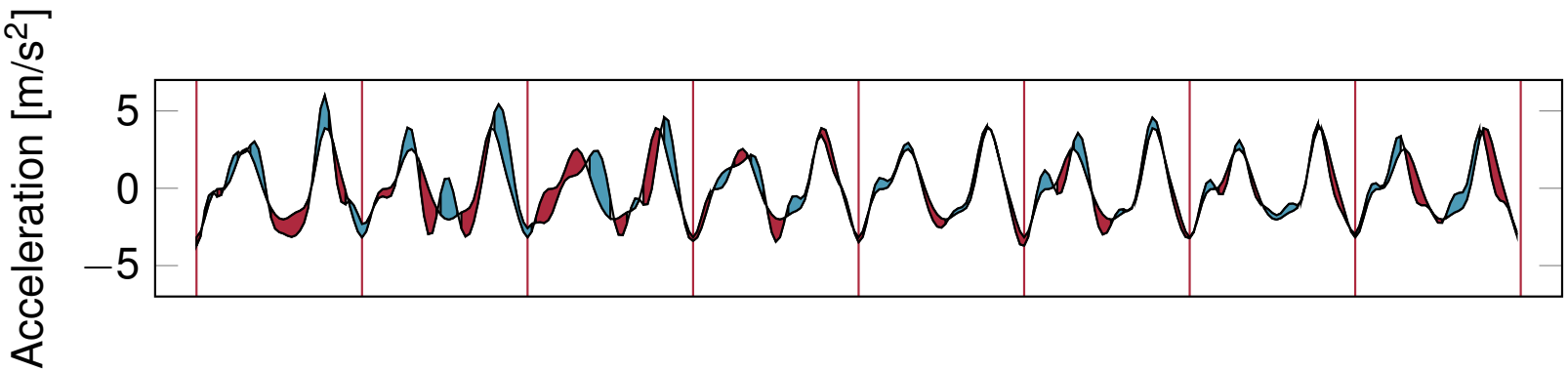


- Average gait cycle overlaid on each original gait cycle
- 4 bits per cycle

Comparison between Locations

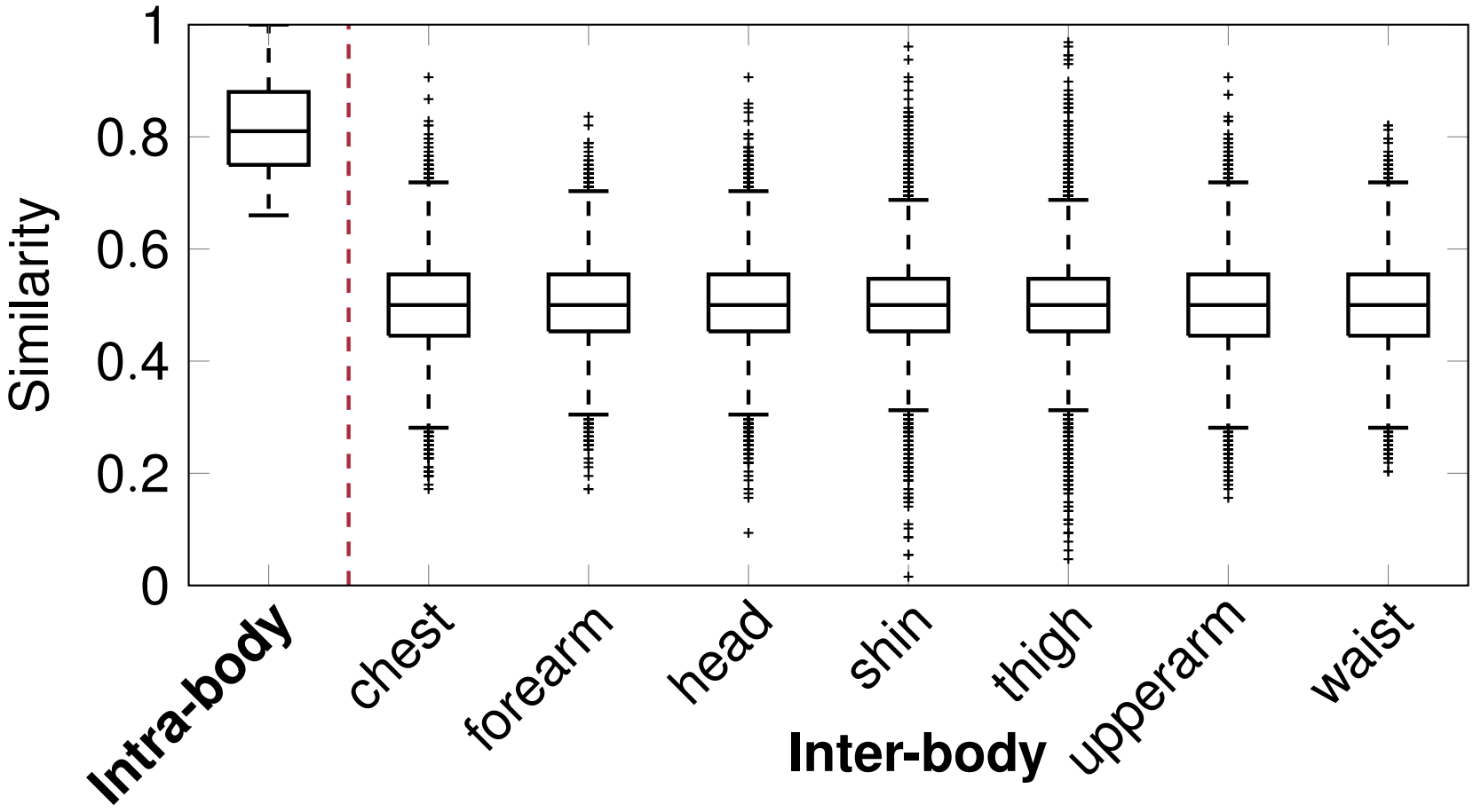


forearm: 0111 1000 1001 0101 1000 1100 ~~1011~~ ~~1000~~



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

Cheap collaboration

Radio Vision

Security from ambient signals

Thank you!

Stephan Sigg
stephan.sigg@aalto.fi