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
Feedback-based distributed adaptive beamforming
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

Mean gain in the signal strength - 16.4 meters distance

- Normal distributed phase offset, variance $0.25\pi$, Mutation probability: 0.33
- Normal distributed phase offset, variance $0.25\pi$, Mutation probability: 0.66
- Normal distributed phase offset, variance $0.25\pi$, Mutation probability: 1.0

Iterations
Feedback-based distributed adaptive beamforming
Cheap collaboration

Radio Vision

Security from ambient signals
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

Activities recognized:
- Walking
- Lying
- Standing
- Empty
- Crawling
### RF-based device-free activity recognition

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

<table>
<thead>
<tr>
<th>Ground truth</th>
<th>Classification</th>
<th>ly</th>
<th>st</th>
<th>wa</th>
<th>cr</th>
</tr>
</thead>
<tbody>
<tr>
<td>ly</td>
<td>.976</td>
<td>.024</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>st</td>
<td>1.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>wa</td>
<td>.955</td>
<td>.045</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cr</td>
<td>.253</td>
<td>.748</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Ground truth</th>
<th>Classification</th>
<th>ly</th>
<th>st</th>
<th>wa</th>
<th>cr</th>
</tr>
</thead>
<tbody>
<tr>
<td>ly</td>
<td>.904</td>
<td>.096</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>st</td>
<td>.096</td>
<td>.898</td>
<td>.006</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wa</td>
<td>.013</td>
<td>.962</td>
<td>.025</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cr</td>
<td>.038</td>
<td>.212</td>
<td>.75</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Ground truth</th>
<th>Classification</th>
<th>ly</th>
<th>st</th>
<th>wa</th>
<th>cr</th>
</tr>
</thead>
<tbody>
<tr>
<td>ly</td>
<td>.882</td>
<td>.118</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>st</td>
<td>.12</td>
<td>.869</td>
<td>.007</td>
<td>.004</td>
<td></td>
</tr>
<tr>
<td>wa</td>
<td>.953</td>
<td>.047</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cr</td>
<td>.01</td>
<td>.439</td>
<td>.551</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Ground truth</th>
<th>Classification</th>
<th>ly</th>
<th>st</th>
<th>wa</th>
<th>cr</th>
</tr>
</thead>
<tbody>
<tr>
<td>ly</td>
<td>1.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>st</td>
<td>.056</td>
<td>.98</td>
<td>.022</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wa</td>
<td>.023</td>
<td>.874</td>
<td>.102</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cr</td>
<td>.044</td>
<td>.144</td>
<td>.811</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Cheap collaboration

Radio Vision

Security from ambient signals
Motivation
Motivation

Trust and proximity
We will use audio as a source of common information in proximity
6
Security from environmental stimuli

Real-time implementation on android mobile phones

*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

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

Hamming distance in created fingerprints
(loud audio source in 1.5m and 3m)

<table>
<thead>
<tr>
<th>Audio sequence class</th>
<th>Median percentage of identical bits in fingerprints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clap</td>
<td>0.5</td>
</tr>
<tr>
<td>Music</td>
<td>0.55</td>
</tr>
<tr>
<td>Snap</td>
<td>0.6</td>
</tr>
<tr>
<td>Speak</td>
<td>0.65</td>
</tr>
<tr>
<td>Whistle</td>
<td>0.7</td>
</tr>
</tbody>
</table>

Percentage of tests in one test run that passed at >5% for Kuiper KS p-values

<table>
<thead>
<tr>
<th>Test run</th>
<th>Only music</th>
<th>Only clap</th>
<th>Only speak</th>
<th>Only snap</th>
<th>Only whistle</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0.91</td>
<td>0.93</td>
<td>0.95</td>
<td>0.97</td>
<td>0.99</td>
</tr>
<tr>
<td>2</td>
<td>0.93</td>
<td>0.95</td>
<td>0.97</td>
<td>0.99</td>
<td>1.01</td>
</tr>
<tr>
<td>4</td>
<td>0.95</td>
<td>0.97</td>
<td>1.01</td>
<td>1.03</td>
<td>1.05</td>
</tr>
</tbody>
</table>

S. Sigg et al., Secure Communication based on Ambient Audio, IEEE Transactions on Mobile Computing
Secure pairing from noisy data

possible messages $X$

possible codewords $C$

$X \rightarrow$ Decoding

$\rightarrow$ Encoding
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 $g$
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

- Acceleration [m/s²]

**Forearm:**
- 0111
- 1000
- 1001
- 0101
- 1000
- 1100
- 1011
- 1000

**Waist:**
- 0110
- 1000
- 1001
- 0001
- 1001
- 1001
- 1100
- 1010

Graph showing acceleration at different locations.
Evaluation

Intra-body:
- chest: 0.2
- forearm: 0.4
- head: 0.6
- shin: 0.8
- thigh: 1.0
- upperarm: 0.8
- waist: 0.6

Inter-body:
- Similarity range from 0 to 1
Cheap collaboration

Radio Vision

Security from ambient signals
Thank you!

Stephan Sigg
stephan.sigg@aalto.fi