Final report:

Implicit situation awareness of a wireless sensor network utilising channel quality estimations

February 5, 2013

Stephan Sigg

National Institute of Informatics (NII)
Information Systems Architecture Science Research Division
2-1-2 Hitotsubashi
Chiyoda-ku
101-8430 Tokyo
Japan
Abstract

This document summarises the achievements in the project 'Implicit situation awareness of a wireless sensor network utilising channel quality estimations'. We first describe the project proposal and its goals and then discuss the results achieved regarding the various research questions. After briefly discussing central achievements during the project we briefly and discuss (subjective) the research and living conditions at the National Institute of Informatik and in Tokyo.

1 Project goal and research achievements

The research on the DAAD-FIT project 'Implicit situation awareness of a wireless sensor network utilising channel quality estimations' was officially started in December 2010. Preliminary studies were undertaken since about autumn 2010. In 2011, a proposal for an extension of the project was accepted. The general aim of the project was the study of approaches to utilise environmental data in Ubiquitous or Internet of Things environments. We considered RF- and audio-based secure spontaneous device pairing, device free RF-based activity recognition as well as mathematical calculations on the wireless channel.

During the project, 19 full papers have been accepted at international peer-reviewed venues and journals. Additionally, three papers are currently under review at various journals and further three papers are currently being prepared.

In the scope of the project, six students have been involved in research tasks as exchange students (NII internship program) and participated in publications. Additionally, 1 PhD student currently conducts her studies in a related topic and three external researchers have been invited for cooperation to the NII. In the following, the workpackages of the project are sketched.

First year of the research project (December 2010 through November 2011)

PJ1–WP1 Context classification based on channel quality measurements

PJ1–WP2 Experimental measurements of context related channel qualities

PJ1–WP3 Context prediction

PJ1–WP4 Installation and evaluation

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Dec - Feb</th>
<th>Mar - May</th>
<th>Jun - Aug</th>
<th>Sep - Nov</th>
</tr>
</thead>
<tbody>
<tr>
<td>PJ1–WP1</td>
<td></td>
<td></td>
<td></td>
<td>2.4</td>
</tr>
<tr>
<td>WP1.1</td>
<td>0.6</td>
<td>0.4</td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>WP1.2</td>
<td>0.4</td>
<td>0.2</td>
<td>0.4</td>
<td>0.6</td>
</tr>
<tr>
<td>WP1.3</td>
<td></td>
<td>0.4</td>
<td>0.6</td>
<td>0.8</td>
</tr>
<tr>
<td>PJ1–WP2</td>
<td></td>
<td></td>
<td></td>
<td>0.6</td>
</tr>
<tr>
<td>PJ1–WP3</td>
<td></td>
<td></td>
<td></td>
<td>0.6</td>
</tr>
<tr>
<td>PJ1–WP4</td>
<td></td>
<td></td>
<td></td>
<td>0.4</td>
</tr>
<tr>
<td>Sum</td>
<td>1.0</td>
<td>1.0</td>
<td>1.0</td>
<td>4.0</td>
</tr>
</tbody>
</table>

Second year of the research project (December 2011 through November 2012)

PJ2–WP1 In-network context processing

PJ2–WP2 Ad-hoc secure communication

PJ2–WP3 Instrumentation and case studies
Figure 1: Encoding maps message \( a \in \mathcal{A} \) to codeword \( c \in \mathcal{C} \). Decoding maps several \( \tilde{c} \in \mathcal{C} \), \( \mathcal{C} = \{c, c', c'', \ldots\} \) to one \( a \in \mathcal{A} \).

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Dec - Feb</th>
<th>Mar - May</th>
<th>Jun - Aug</th>
<th>Sep - Nov</th>
<th>Sum</th>
</tr>
</thead>
<tbody>
<tr>
<td>PJ2–WP1</td>
<td></td>
<td></td>
<td></td>
<td>2.0</td>
<td></td>
</tr>
<tr>
<td>WP1.1</td>
<td>0.5</td>
<td></td>
<td></td>
<td>0.7</td>
<td>1.4</td>
</tr>
<tr>
<td>WP1.2</td>
<td>0.5</td>
<td>0.2</td>
<td></td>
<td>1.0</td>
<td>2.0</td>
</tr>
<tr>
<td>WP1.3</td>
<td></td>
<td>0.3</td>
<td></td>
<td>0.3</td>
<td>0.8</td>
</tr>
<tr>
<td>PJ2–WP2</td>
<td></td>
<td></td>
<td></td>
<td>1.4</td>
<td></td>
</tr>
<tr>
<td>WP2.1</td>
<td></td>
<td></td>
<td>0.5</td>
<td>0.5</td>
<td>0.5</td>
</tr>
<tr>
<td>WP2.2</td>
<td></td>
<td></td>
<td>0.2</td>
<td>0.6</td>
<td>0.8</td>
</tr>
<tr>
<td>WP2.3</td>
<td></td>
<td></td>
<td></td>
<td>0.3</td>
<td>0.3</td>
</tr>
<tr>
<td>PJ2–WP3</td>
<td></td>
<td></td>
<td></td>
<td>0.6</td>
<td></td>
</tr>
<tr>
<td>WP3.1</td>
<td></td>
<td></td>
<td>0.3</td>
<td>0.3</td>
<td>0.3</td>
</tr>
<tr>
<td>WP3.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.3</td>
</tr>
<tr>
<td>Sum</td>
<td>1.0</td>
<td>1.0</td>
<td>1.0</td>
<td>1.0</td>
<td>4.0</td>
</tr>
</tbody>
</table>

Generally, the project can be divided into three main parts, namely:

1. Ad-hoc spontaneous device authentication (PJ2–WP2, PJ2–WP3)
2. RF-based Device-free activity recognition (PJ1–WP1, PJ1–WP2, PJ1–WP3, PJ1–WP4)
3. Mathematical operations on the wireless channel (PJ2–WP1, PJ2–WP3)

In the following, we discuss the progress achieved in these aspects.

### 1.1 Spontaneous context-based device authentication

For spontaneous device authentication among previously unacquainted devices, we proposed the use of fuzzy cryptography techniques [5, 4, 1, 2, 6, 9]. In particular, we utilised ambient audio recorded on devices in proximity as a basis to a common secret between these devices. Devices agree on a recording time, capture audio, generate an audio fingerprint for the captured sequence with the Haitsma and Kalker audio fingerprinting approach [3] and account for possible differences in the created fingerprints by Reed-Solomon error correcting codes [7]. The procedure is depicted in figure 1.

Devices in proximity experience some correlation in the audio signals they observe and will create a similar audio-fingerprint within a code-space \( \mathcal{C} \). Let the fingerprint on one device be \( c' \) in the figure. By Reed-Solomon decoding, any fingerprint within \( \mathcal{C} \) is mapped to the same message \( a \) in the message space. By decoding this message again, the sequence \( c \) will be achieved. At this point, devices in proximity have, without disclosing any information on the wireless channel, computed an identical common secret that can be utilised as a seed for a cryptographic key.
Devices which are farther away, however, are unlikely to compute the same key since the audio observed and hence the audio fingerprint created considerably differs.

We published a prototypical implementation of this method, demonstrated its feasibility to separate proximate devices from a remote attacker in case studies in office environments, outdoor scenarios and a canteen and verified the entropy of the generated audio fingerprints with the die harder set of statistical tests. The results were published in [26, 27, 20, 22]. Furthermore, we implemented the described approach for android mobile devices [25]. Due to hardware-specific unpredictable delays on the mobile phones, we had to restrict the generation of a fingerprint to a specific band in the audio spectrum and introduced a synchronisation based on the smith-waterman approximate pattern matching [8] in order to mitigate the timing offsets experienced in the recordings. With this approach, we could achieve a synchronisation accuracy of less than 10 milliseconds. The results on these studies are published in [13, 12].

Currently, we consider the vulnerability of the protocol against an active attacker. Such an attacker might send a strong signal that overlays the signals at the legitimate communication partners such that the generation of common keys can be affected. We could show that an active attacker can with the Haitsma and Kalker fingerprinting approach indeed greatly impact the generated fingerprint and even dictate the generated key to great extent for both, audio and RF-signals. However, we also observed that the smaller fluctuations of the received signal can not be impacted by a remote attacker for RF. For audio, similar studies are currently conducted. We propose to apply a filter on the received signal before generating the fingerprint that ignores all signal fluctuation that exceeds a certain threshold in signal strength. A publication containing these results is currently prepared.

1.2 RF-based Device-free activity recognition

We considered the classification of activities from individuals not equipped with a transmit or receive device from fluctuations observed on the RF-channel by a receiver in proximity. The RF-signal of a receiver is composed of all signal components that arrive at the receive antenna from various directions. A subject in the proximity of the receive antenna will block and reflect the incoming signal components and therefore alter the composition of signal components at the receiver. This, in turn, induces a fluctuation in the received signal envelope. We assert that specific activities by subjects in proximity of a remote receiver induce characteristic patterns in the fluctuation of the received signal and that these patterns can be identified and classified for the respective activities.

We have shown that it is feasible to detect changed environmental conditions such as opened or closed doors, locations and count of individuals from amplitude fluctuation of RF-signals in [15, 14]. Furthermore, in [17], we have at the same time distinguished a person walking, an opened or closed door or an ongoing phone call. In these studies, an active device free activity recognition (DFAR) system was utilised in which the system also contained a transmitting device.

This is the easiest case for RF-based DFAR, since the system has complete control also over the incoming signal. A comprehensive study of an active system for the indoor recognition of an office room where a single person walking, crawling, standing or lying in proximity of the receive antenna is currently under review by IEEE Transactions on Mobile Computing.

In [19, 18], we also considered the classification accuracy of a passive system utilising environmental FM-radio for the same activities in an indoor scenario. We could identify suitable features and reached a classification accuracy of about 0.7 to 0.8 for a two-staged classification approach with k-nearest neighbour and decision tree classifiers.

Recently, we compared the classification accuracy of a passive FM-based system to active systems and also to accelerometer-based systems. In these experiments, a similar classification accuracy could be reached. Additionally, we demonstrated that by utilising several receive antennas, this accuracy can be further increased, investigated the impact of distance between the receive antenna and the location where the activity was conducted and reached similar accuracy.

---

1Submitted January 2012
in multiple scenarios with the same set of features. These results are currently submitted to a special issue on ‘Non-cooperative Localization Networks’ of the IEEE Journal of Selected Topics in Signal Processing\(^2\).

In all the above cases, we utilised USRP Software defined radio nodes. However, contemporary mobile nodes commonly not provide such a wide access to the wireless channel. More likely, as we have discussed in [16] the Received Signal Strength Indicator (RSSI) is the only information available at mobile nodes. The RSSI is transmitted with each packet over a wireless channel. Its granularity is much lower than the information available from SDR nodes and the sampling frequency is dependent on the count of packets received. We analysed active and passive systems utilising INGA sensor nodes\(^3\) and a common WiFi receiver. In the former case, a slightly reduced classification accuracy of about 0.7 could be observed for the above mentioned classes. The latter case, however, could only distinguish between activities in close proximity of a WiFi antenna. We currently prepare a submission covering these results.

1.3 Mathematical operations on the wireless channel

In the Internet of Things, devices will be sharply restricted in their computational capabilities but likely provide an access to the wireless channel. We study the computational capabilities of the wireless channel when signals are transmitted simultaneously to reach a superimposition.

In [10, 11], we have considered an efficient communication scheme for distributed nodes. It is possible to combine a high count of values from RFID or other resource restricted nodes in non-synchronised simultaneous transmission on the wireless channel by utilising suitable random binary sequences. We generally considered encodings of data sequences that allow with a high probability to identify individual sequences from an unsynchronised superimposition of a high number of physical signals at a remote receiver. The submission was rewarded with the best paper award at the 7th International Conference on Intelligent environments [10]. We consider in-network processing in intelligent environments which are currently implemented with standard wireless sensor network technologies using conventional connection-based communications. Since, however, connection-based communications may impede progress towards intelligent environment scenarios involving high mobility or massive amounts of sensor nodes, we present a novel approach based on collective transmission for item level tagging using printed organic electronics, which implements robust, collective, approximate read-out of large numbers of simple tags. Figure 1.3 depicts the experimental setup and results achieved. Our approach uses mechanisms for calculation by simultaneous transmission. We detailed the collective transmission approach, discussed its implementation in the organic printed label scenario, and showed first results of experiments conducted with our smart label test bed.

In [23] we considered the simultaneous operation of complex functions in a network of cooperating wireless nodes. In particular, we build a virtual Neural Network overlay over a collection of wireless nodes and show that the network is capable of conducting arbitrary mathematical operations. This was feasible by combining a set of nodes as a distributed beamformer in order to be able to simultaneously process operations through the neural network without inter-node interference.

Following another line of thought, we utilised in [21] a characteristic representation of data as rotated vector on a Bloch sphere in order to allow simultaneous distributed computation of an operation and the arbitrary computation at any intermediate state.

Distinct values are represented by multiples of unique rotations of a vector. The rotations that represent distinct feature classes are required to be no multiple of each other and no multiple of a full rotation so that, after combining rotations of distinct vectors, the resulting rotation still uniquely represents a valid and unique representation of the combined measurements. Figure 3 illustrates this concept. The order in which rotations are applied can be arbitrary and combination of only a

---

\(^2\)Submitted January 2013
\(^3\)http://www.ibr.cs.tu-bs.de/projects/inga/
The experimental setup consists of 21 transducers and one receiver connected to a PC.

Experimental results

Figure 2: Experimental setup and results for our case study on in-network processing

<table>
<thead>
<tr>
<th>Setting</th>
<th>Number of Trials</th>
<th>Correctly Identified Msg.</th>
<th>Average Error Sum</th>
<th>Average Error Mean p. Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>10</td>
<td>88.57%</td>
<td>12.38%</td>
<td>1.77%</td>
</tr>
<tr>
<td>18.3</td>
<td>10</td>
<td>89.05%</td>
<td>11.90%</td>
<td>1.70%</td>
</tr>
<tr>
<td>15.6</td>
<td>10</td>
<td>91.90%</td>
<td>8.37%</td>
<td>1.22%</td>
</tr>
<tr>
<td>12.9</td>
<td>10</td>
<td>97.62%</td>
<td>2.38%</td>
<td>0.34%</td>
</tr>
<tr>
<td>15,3,3</td>
<td>10</td>
<td>90.00%</td>
<td>10.95%</td>
<td>1.56%</td>
</tr>
<tr>
<td>12,6,3</td>
<td>10</td>
<td>89.05%</td>
<td>11.43%</td>
<td>1.63%</td>
</tr>
<tr>
<td>9,9,3</td>
<td>10</td>
<td>89.05%</td>
<td>10.95%</td>
<td>1.56%</td>
</tr>
<tr>
<td>9,6,6</td>
<td>10</td>
<td>82.38%</td>
<td>17.62%</td>
<td>2.52%</td>
</tr>
<tr>
<td>12,3,3,3</td>
<td>10</td>
<td>82.86%</td>
<td>17.62%</td>
<td>2.52%</td>
</tr>
<tr>
<td>6,6,6,3</td>
<td>10</td>
<td>82.38%</td>
<td>17.14%</td>
<td>2.45%</td>
</tr>
<tr>
<td>9,3,3,3</td>
<td>10</td>
<td>80.95%</td>
<td>18.10%</td>
<td>2.59%</td>
</tr>
<tr>
<td>6,3,3,3</td>
<td>10</td>
<td>80.00%</td>
<td>21.90%</td>
<td>3.13%</td>
</tr>
<tr>
<td>3,3,3,3</td>
<td>10</td>
<td>80.95%</td>
<td>20.95%</td>
<td>2.99%</td>
</tr>
</tbody>
</table>

Figure 3: Representation of a situation representation on a sphere and applications of rotations to a vector.
subset of vectors represents a partial computation that can be combined with partial computation of other parts of the network.

Actual mathematical operations on the wireless channel could then be conducted in [28]. We utilised Poisson distributed burst-sequences in order to add values during simultaneous transmission on the wireless channel. By employing logarithm laws, all four basic mathematical operations could be conducted. We demonstrated the successful operation utilising sensor nodes in [24].

We believe that further mathematical operations are feasible when other random distributions are employed.

2 Research at the NII for DAAD researchers

The National Institute of Informatics (NII) is the only nationally funded research institute for computer sciences in Japan. It is well supported by the government and features a high share of international researchers. The NII provides a good environment for scientific research. DAAD-founded researchers at NII are independent in their research and cooperation. The DAAD-FIT grant comprises an additional research budget that can be spent for professional travel expenses within Japan, hardware or internship students. The NII has a very active internship program. From my personal experience, this research budget is best invested in internship students.

The DAAD also provides support for up to two international conference travels. For a research grant, I believe that this support of conference travels should be significantly extended. In its current implementation, the grantee should be prepared to cover travel costs to international venues privately. In some cases, it might be possible that NII covers some conference travel expenses. Another option is the application for a research project, for instance at the JSPS, that might cover travel grants.

A critical aspect of the research grant is the return to Germany. If a postdoctoral position is intended after the grant, first discussions regarding such an appointment with the corresponding institute or Professor before the start of the grant are suggestive. Applications for Professor positions or as research group leader likely require an application at least one year in advance. NII will normally not employ DAAD researchers after their grant to respect the interest of DAAD.

Apartments in Japan are generally at a lower standard compared to Germany (heating, windows). Good apartments at reasonable cost are available in the Tokyo International Exchange Center. Since the application process for these flats consumes several months, a timely application is suggestive.

The working environment and equipment at NII is very good. In contrast to Germany, an office is typically occupied by ten or more researchers.
Publications by other authors


Own publications in the scope of the project


