Abstract

Personal communication and relationships within spatially distributed or separated groups can be difficult to establish and maintain. A promising approach investigated with respect to this problem are ambient intelligence and smart environments equipped with perception and communication technology. These technologies require a standardized way to access sensors, actuators, and to develop applications for them to be usable. Furthermore, they have to address concerns like privacy in order to be accepted. We propose a middleware based on a distributed reasoning concept and a qualitative spatial privacy aware representation to address these requirements.

Introduction

Personal and casual communication and interaction play a central role for general wellbeing, productivity, and social identity in groups. If working teams are colocated such communication and interaction occurs on a spontaneous and day-to-day basis: Colleagues pass each other on an office floor, have lunch together, or meet at social places like coffee dispensers. However, today’s work settings prevent this as teams are more often spatially distributed across cities, countries, and continents. Examples include branches of companies or members of research projects that are located at different sites. Furthermore, this holds also true in private life as families are often at least temporally separated when children move to different cities to study or work, or a parent works and lives in a different place during the week.

An approach to address this problem that is pursued is to deploy and use ambient intelligence and smart environments (AISE). This includes systems like Media Spaces (Stults, Harrison, and Harper 2009) that provide ubiquitous and pervasive sensors and communication devices.

As such environments use distributed sensor and actuator nets, a middleware is required to facilitate access to sensors, actuators and allow data-distribution within the environment. Furthermore, in order to make a system acceptable for users, privacy concerns have to be addressed, too.

In this paper we introduce the Spatial Interaction Laboratory (SIL) as a smart environment based on common components and describe its middleware. Furthermore, we propose a privacy aware representation for such environments based on qualitative spatial reasoning (see (Cohn and Hazarika 2001; Cohn and Renz 2008)) and the use consistency-checking to identify privacy violations.

Related Work

Research on Media Spaces started in the 1980s. These are environments that allow multimedia communication by technology that is integrated as part of the environment. Examples are the RAVE (Ravenscroft Audio Video Environment) project (Gaver et al. 1992; MacKay 1999), the Portholes project (Dourish and Bly 1992), the Telemurals project (Karahalios and Donath 2004), the Family Window project (Judge, Neustaedter, and Kurtz 2010), and the ASTRA project (Romero et al. 2006). For an introduction and description of the history, projects and findings in the research field of Media Spaces the interested reader is directed to (Dewan et al. 1999; Stults, Harrison, and Harper 2009). The results of these Media Space projects were promising, but current research seems to move away from these settings.

In order to create and deploy such environments a standardized way to access sensors and actuators, as well as to develop and deploy software providing desired functional-
ity is required. An approach pursued to solve this is the development of so called middlewares. That is, software providing an interface to the underlying systems. This field of research is just as diverse as are the possibilities to use middleware systems. Examples are middlewares for service-oriented computing (Al-Jaroodi and Mohamed 2012; Gaddah and Kunz 2003), for sensor networks (Wang et al. 2008; Molla and Ahamed 2006), or for context-aware systems (Bettini et al. 2010; Hung et al. 2003; Kjær 2007; Saeed and Waheed 2010).

An introduction and overview of the research field of qualitative spatio-temporal representation and reasoning is provided in (Cohn and Hazarika 2001; Cohn and Renz 2008). In this work we make use of the RCC representation described in (Cohn et al. 1997). We use the RCC-8 version with the eight base relations \(\{dc, ec, po, eq, tpp, ntpp, tpp^{-1}, ntpp^{-1}\}\) (see Figure 1) as a foundation for our representation. To simplify the notation we use a RCC-6 version combining the RCC-8 relations \(tpp\) and \(ntpp\) to \(pp\) and respectively \(pp^{-1}\) and \(ntpp^{-1}\) to \(pp^{-1}\). That is, we regard the border of a region as belonging to the interior of a region. The RCC-6 relation \(pp\) in turn is mapped to the RCC-8 relation \(\{tpp, ntpp\}\) and respectively \(pp^{-1}\) to \(\{tpp^{-1}, ntpp^{-1}\}\). Thus we are able to use RCC-8 as an underlying representation and its implementation in the SparQ software (Dylla et al. 2006; Wallgrün et al. 2010) for experimental evaluations, i.e., consistency checking using algebraic closure (a-closure), which to our knowledge is not yet proven to decide consistency for RCC-6.

AISE requires environmental data as input to provide functionality. This poses a potential privacy issue as stated in (Wright 2005; Friedewald et al. 2007). If we want to deploy AISE and have general public acceptance, these privacy concerns have to be addressed explicitly. However, even as privacy has been recognized as an important issue, it remains to be an open problem. Often the respective users of a system have to take care of their personal privacy or privacy enforcement is limited to specific aspects (Stults, Harrison, and Harper 2009). We approach this problem by proposing a new notion of privacy understanding and a respective representation.

The SIL Environment

In this section we introduce the hardware and software used to create the Spatial Interaction Laboratory (SIL). The SIL is installed at the University of Bremen. It serves as an experimental platform for AISE. It is based on an embedded computer based on the following hardware specifications:

- 1.2GHz CPU
- 1GB RAM
- 8GB Flash HDD
- touchscreen
- web cam
- stereo speakers

Figures 2 and 3 provide an impression of the physical environment and how the doorplates are embedded within it. A doorplate together with the respective software is called a peer. These peers provide the possibility to perceive the environment by modalities of vision and audio, and have a display supporting a touchscreen for user interaction. Figure 4 provides a visual impression of what the cameras of the SIL are able to perceive.

The SIL Middleware

In order to enable fast prototyping of functionality within the SIL environment, we created a middleware infrastructure. It provides possibilities to develop applications as plug-ins to provide new functionality which can include or depend on other existing plug-ins. It also provides a standard way of communication between plug-ins. It makes no difference if the plug-ins are part of the same peer or part of different ones of a connected environment.

The software is written in C++ and based on the Qt 4.8 framework\(^1\). We use Ubuntu\(^2\) as the underlying operating system.

The middleware adopts the distributed reasoning concept introduced in (van de Ven et al. 2010) (see Figure 5). It divides distributed reasoning into three layers: (1) the environment layer, (2) the perception and interaction layer, and

\(^1\)http://qt-project.org
\(^2\)http://www.ubuntu.com
(3) the reasoning layer, including local reasoning and group reasoning. This allows to understand ambient intelligence as a network of single connected peers, that individually facilitate perception, action, and local reasoning. The environment is then defined through the available connections between individual peers as depicted in Figure 6. Based on this topology of individual peers and connection based groups, the differentiation between local reasoning and group reasoning can be defined.

Local reasoning addresses the interpretation and artificial decision making with data that is located and limited to one individual peer. It is restricted to data and information regarding only this peer. Distributed reasoning addresses propagation and distribution of data and information within a group of peers. However, actual decision making resides to each individual peer, but also includes data and information about and from other connected peers.

Our software implements the architecture presented in Figure 5. This architecture is based on the distributed reasoning concept. But instead of addressing the different layers of reasoning, it organizes the information flow. Thus, the GroupComCtrl component resembles the communication of the distributed reasoning layer, the LocalComCtrl resembles the communication of the local reasoning layer, and the PluginServiceCtrl together with the Plug-ins resemble the perception and interaction and environment layer as well as the actual reasoning functionality. The components of the architecture are now described in more detail.

The LocalComCtrl Component
The LocalComCtrl component is concerned with controlling and coordinating communication within one peer. That is, it relays messages from one plug-in to another on the same peer. Furthermore, it provides access to some common data and information, e.g., configurations, of an individual peer. The actual decision if a message is meant for this or a different peer is also made within this component. This allows to introduce a system wide communication restriction policy and by this a certain form of privacy, later on. Some basic logging functionality is implemented in this component and provides all other components with one central log-file or other log-method.

The GroupComCtrl Component
The GroupComCtrl component is concerned with facilitating communication with other peers. That is, providing the actual data transmission and also handling incoming communications. Furthermore, the possibility to directly relay a message is provided. If the message is directed to the current peer, it is sent to the LocalComCtrl component for processing.

The PluginServiceCtrl Component
The PluginServiceCtrl component is concerned with the control and management of plug-ins. That is, it detects and loads plug-ins and is able to relay messages received from the LocalComCtrl component to a specified plug-in. Furthermore, it provides possibilities to dynamically start and stop the actual execution of specific plug-ins.

Plug-ins
The plug-ins provide the actual functionality. This includes perception by providing sensor control and data interpretation. For example, access to a connected microphone and calculation of the present dB value or access to a connected camera and detection and tracking of faces. This also includes reasoning on the local layer as well as the group layer or interaction by providing access to actuators, e.g., presenting content on a display. These plug-ins are not limited with respect to their functionality and have a simple and standard way of communication with one another, either on the local peer or even across multiple peers. Thus providing new functionality for the SIL environment requires to implement a plug-in and deploying it to all desired peers of the environment.

Towards a Privacy Aware Representation
In order to use and store data perceived by the environment, we propose a representation based on RCC-6 as previously introduced. RCC-6 provides a set of six base relations: \( \text{Rel} = \{ \text{dc, ec, po, eq, pp, pp}^{-1} \} \). To be able to use the SparQ software and a-closure for deciding consistency, we use a translation of RCC-6 to RCC-8 by substituting \( \text{pp} \) with \( \text{tpp, ntpp} \) and \( \text{pp}^{-1} \) with \( \text{tpp}^{-1}, \text{ntpp}^{-1} \), respectively.

Furthermore, we make the following assumptions:

(A1) Everything can be represented as a (conceptual) spatial region.

(A2) Privacy can be understood as spatio-temporal restrictions of perceivability and availability. This is a hypothesis derived from the observation, that people are often
concerned with where information about them can be accessed and by whom.

(A3) The represented spatial environment, especially the regions describing it, are static.

The proposed representation is called Qualitative Spatio-Temporal Privacy Aware Representation (QSTPAR). Within this document a first conceptual approach to this representation is proposed. This also includes the following additional assumptions:

(A4) One single temporal snapshot (static / unchanged world)

(A5) Full world knowledge (all facts, regions, and relations are known)

**Definition of QSTPAR**

QSTPAR is described by the tuple \((P, N, C, I, E, O, L)\) for which the following definitions are provided:

(D1) \(P = \{p_0, \ldots, p_a\}\) with \(a \in \mathbb{N}\) is the set of all spatial regions in the environment that can be observed by a sensor, e.g., field of view of a camera.

(D2) \(N = \{n_0, \ldots, n_b\}\) with \(b \in \mathbb{N}\) is the set of all spatial regions in the environment that can not be observed by a sensor.

(D3) \(C = \{c_0, \ldots, c_d\}\) with \(d \in \mathbb{N}\) is the set of all conceptual spatial regions in the environment, e.g., a floor or lounge area.

(D4) \(I = \{i_0, \ldots, i_f\}\) for \(f \in \mathbb{N}\) is the set of conceptual regions representing perceptions and other facts.

(D5) \(S = P \cup N \cup C\) is the set of all spatial regions available.

(D6) \(A = S \cup I\) is the set of all available regions.

(D7) A relation \(r\) within QSTPAR is a tuple \(r = (x_r, R_r, y_r)\) with \(x_r, y_r \in A\) and \(R_r \subseteq \text{Rel} = \{\text{dc, ec, po, eq, pp, pp}^{-1}\}\).

(D8) \(E = \{r_{e_0}, \ldots, r_{e_g}\}\) with \(g, h \in \mathbb{N}\), \(r_{e_h} = (x_{e_h}, R_{e_h}, y_{e_h})\), and \(0 \leq h \leq g\) and \(x_{e_h}, y_{e_h} \in S\) and the constraint

\[
x_{e_h} \in (P \cup N), \forall y_{e_h} \in C \Rightarrow R_{e_h} \subseteq \{dc, ec, po, eq, pp\}
\]

\[x_{e_h} \in (P \cup N) \land y_{e_h} \in C \Rightarrow R_{e_h} \subseteq \{dc, ec, po, eq, pp\}\]  

\[(D9) O = \{r_{o_0}, \ldots, r_{o_j}\}\) with \(j, u \in \mathbb{N}\), \(r_{o_u} = (x_{o_u}, R_{o_u}, y_{o_u})\), and \(0 \leq u \leq j\) and the constraint

\[
x_{o_u} \in I, y_{o_u} \in A \Rightarrow R_{o_u} \subseteq \{pp, eq, po\}
\]

is the set of relations representing the spatial environment.

(D10) \(L = \{r_{l_0}, \ldots, r_{l_w}\}\) with \(w, z \in \mathbb{N}\), \(r_{l_z} = (x_{l_z}, R_{l_z}, y_{l_z})\), and \(0 \leq z \leq w\) and the constraint

\[
x_{l_z}, y_{l_z} \in A \Rightarrow R_{l_z} \subseteq \{dc, po, pp\}
\]

is the set of relations defining a privacy policy by restricting spatial perceivability and availability of information.

Figure 7 shows a depiction of an environment and is used to provide an example for a QSTPAR instance. Due to space limitations we omitted relations that either are the converse (denoted by \(\sim\)) to presented ones or have the form \((x, \{dc\}, y)\). These are the resulting sets for the provided example:

\[
P = \{p_1, p_2, p_3, p_4, p_5\}
\]

\[
N = \{n_1, n_2, n_3, n_4\}
\]

\[
C = \{c_1, c_2\}
\]

\[
I = \{i_1\}
\]

\[
O = \{\langle i_1, \{pp\}, p_1 \rangle, \langle i_1, \{pp\}, c_1 \rangle\}
\]

\[
E = \{\langle p_1, \{pp\}, c_1 \rangle, \langle n_1, \{pp\}, c_1 \rangle, \langle p_2, \{pp\}, c_1 \rangle, \langle p_1, \{ec\}, n_1 \rangle, \langle n_1, \{ec\}, p_2 \rangle, \langle p_5, \{pp\}, c_2 \rangle, \langle n_2, \{pp\}, c_2 \rangle, \langle p_3, \{pp\}, c_2 \rangle, \langle n_3, \{pp\}, c_2 \rangle, \langle p_4, \{pp\}, c_2 \rangle, \langle n_4, \{pp\}, c_2 \rangle, \langle p_5, \{ec\}, n_2 \rangle, \langle n_2, \{ec\}, p_3 \rangle, \langle p_3, \{ec\}, n_3 \rangle, \langle n_3, \{ec\}, p_4 \rangle, \langle p_3, \{po\}, p_4 \rangle, \langle p_4, \{ec\}, n_4 \rangle\}
\]

Given a specific QSTPAR instance \((P, N, C, I, E, O, L)\), the hypothesis is that consistency-checking of the set of relations of the combined sets \(E, O, L\) allows to determine violations against the privacy policy defined by \(L\). Let the function \(\Phi(X) = true\) iff the set \(X\) of relations is consistent.

Consistency does determine privacy, because the set \(L\) restricts the possibilities of how an informational fact may be related to a spatial region. And where it can be perceived or is available. Thus, if assumption (A2) is correct, \(L\) can ensure that specific relations do not hold, i.e., the set \(X\) is not consistent. It follows, that as long as the relations contained in set \(L\) describe the privacy policy, the described policy holds iff the set of relations in \(L\) is consistent in combination with the environment defined by \(E\) and the accessible information defined by \(O\). The interpretation of a relation between an informational fact and a spatial region is related to perceivability and availability. That is, a relation \(r_p = (i_p, R_p, s_p)\) with \(i_p \in I, s_p \in S, R_p \subseteq \{po, eq, pp\}\) means that the informational fact \(i_p\) is perceivable or available.

**Algorithm 1: Function \(\omega(S, E, O, L)\)**

```
input : The sets S, E, O, L
output: The set X of relations
1 EL ← E;
2 foreach x, y ∈ S : (x, R_e, y) ∈ E ∧ (x, R_t, y) ∈ L do
3     EL ← EL/(x, R_e, y);
4     if (y, R_e, x) ∈ EL then
5         EL ← EL/(y, R_e, x);
6     X ← EL ∪ O ∪ L;
```

32
within the spatial region \( s_p \). A relation \( r_h = (i_h, R_h, s_h) \) with \( i_h \in I, s_h \in S, R_h \subseteq \{dc, ec\} \) means that the informational feature \( i_h \) is not perceivable or available within the spatial region \( s_h \). However, a differentiation between spatial (\( P \cup N \)) and conceptual spatial (\( C \)) regions has to be made. Real spatial regions are static and their relation to other spatial regions can not be changed, as they are based in the real physical world. Conceptual spatial regions are regarded as static, following assumptions (A3) and (A4). However, we regard them as more flexible as physical regions as the borders are not always crisp.

Thus, in order to check consistency of a QSTPAR instance, the consistency of the combined relations of the sets \( E, O \), and \( L \) have to be determined. Lets assume a simple unification of the sets \( E, O \), and \( L \), it follows that if \( \Phi(E \cup O \cup L) = \text{true} \) implies that the environment itself enforces the privacy policy \( L \) because it holds:

\[
\forall x_i, x_j, y_i, y_j \in A, \forall r_e \in (E \cup O), \forall r_i \in L : \\
r_e = (x_e, R_e, y_e) \land r_i = (x_i, R_i, y_i) \land x_i = x_j \land y_i = y_j \rightarrow R_e \subseteq R_i
\]

Alternatively, one could algorithmically combine the three sets \( E, O, \) and \( L \) and thus determine if a given privacy policy holds, even if the environment itself does not ensure its enforcement. A first approach is removing all spatial relations of the environment for which different relations are provided within the policy (see function \( \omega(S, E, O, L) \) provided in Algorithm 1).

It holds that if \( \Phi(\omega(S, E, O, L)) = \text{true} \), i.e., the constraint set generated by \( \omega(S, E, O, L) \) is consistent, states that the privacy policy is not violated, i.e., all relations defined in \( L \) hold. However, \( \Phi(\omega(S, E, O, L)) = \text{false} \) does not necessarily imply that the privacy policy is violated (see example \( E_2, O_w, L_2 \) in Table 1 and example scenario \( E_2, O_w \)). Thus the algorithm is refined to duplicate physical spatial and information regions and all according relations to other regions (see function \( \Omega(S, C, I, E, O, L) \) provided in Algorithm 2). This allows a more flexible relationship between physical spatial regions and conceptual spatial regions.

Still, if \( \Phi(\Omega(S, C, I, E, O, L)) = \text{true} \), i.e., the constraint set generated by \( \omega(S, C, I, E, O, L) \) is consistent, it is ensured that the privacy policy is not violated, i.e., all relations defined in \( L \) hold. However, \( \Phi(\Omega(S, C, I, E, O, L)) = \text{false} \) does imply that the privacy policy is violated. Analyzing the inconsistency also allows to locate the spatial region where the violation occurred, thus making it possible to address possible future violations. However, this in itself is a hard problem as for example stated in (Wallgrüen and Dylla 2010a; 2010b).

**Examples**

Two spatial example scenarios \( E_1 \) and \( E_2 \) will be used (depicted in Figures 8 and 9) to illustrate the proposed representation. Each is evaluated using combinations of observations and limitation constraints (privacy policies). The example

![Figure 8: QSTPAR example scenario E1](image-url)

observation sets used are:

\[
\begin{align*}
O_1 &= \{(i_1, pp, p_1), (i_1, pp, c_1)\} \\
O_2 &= \{(i_1, pp, p_3), (i_1, pp, p_4), (i_1, pp, c_2)\} \\
O_{3E1} &= \{(i_1, pp, p_2), (i_1, pp, c_1)\} \\
O_{3E2} &= \{(i_1, pp, p_2), (i_1, pp, c_2)\} \\
O_w &= \{(i_1, pp, p_2), (i_1, pp, c_1), (i_1, pp, c_2)\}
\end{align*}
\]

The example privacy policies are:

\[
\begin{align*}
L_1 &= \{(c_1, \{po\}, c_2)\} \\
L_2 &= \{(c_1, \{de\}, c_2)\} \\
L_3 &= \{(p_3, \{de\}, p_4)\}
\end{align*}
\]

Table 1 gives an overview of the ground truth (GT) and results of evaluating example combinations using the SparQ software. A √ states that no inconsistency was found, ×
states that an inconsistency was found. A $×*$ states that the provided set contains contradicting relations and SparQ can not compute this set. This is regarded as inconsistent. The weakness of the $\omega$-function for generating the set of combined relations is shown by example $E_2, O_w, L_2$. A selection of the examples is addressed in more detail to provide a better understanding of QSTPAR.

**Example E$_1$, O$_2$** This example gives an idea of how informational facts are represented as spatial regions within QSTPAR. A depiction of the example scenario is provided in Figure 10. The shaded circular region $i1$ represents a single informational fact, perceivable or available in the spatial regions $p3$, $p4$, and $c2$. As the informational fact is purely contained in $c2$ the privacy policies defined by $L_1$ and $L_2$ can not be violated. However, the policy $L_3$ states that no information may be shared between $p3$ and $p4$ and thus is always violated in this scenario, as they are physical spatial regions and thus are crisp and cannot be disconnected.

**Example E$_2$, O$_{1E2}$** This example has an informational fact $i1$ represented within the spatial regions $p2$ and $c2$. And the region $p2$ partly overlaps both conceptual spatial regions $c1$ and $c2$. Thus, only the privacy policies $L_1$ and $L_2$ can be affected. In both cases the actual privacy constraints are not violated for the example scenario depicted in Figure 11.

**Example E$_2$, O$_w$** This example is designed to expose the weakness of using $\Phi(\omega(S, E, O, L))$ to determine privacy violations. A depiction of the scenario is provided in Figure 12. It holds one informational fact $i1$ within the spatial region $p2$ and the conceptual spatial regions $c1$ and $c2$. Thus, this information is actually allowed to exist in both conceptual regions as $p2$ is part of both and thus, the sensor readings are available to both regions $c1$ and $c2$. This means that the scenario does not violate the privacy policies defined by $L_1$ and $L_2$. However, $\Phi(\omega(S, E_2, O_w, L_2)) = false$ states that the privacy policy $L_2$ is violated. The core of this problem is that the boundaries of conceptual spatial regions are not always crisp. That is, a given physical spatial region can belong to an office floor and a lounge area connected to this floor. We solve this problem by duplicating the respective regions and their relations (see Algorithm 2). However, this might not always be the right solution depending on the setting requirements.

### Conclusion

In this paper, a first approach to a Qualitative Spatio-Temporal Privacy Aware Representation (QSTPAR) has been presented. Furthermore, the proposed representation in combination with the SparQ software has been used to model and analyze example scenarios regarding violations of privacy policies. In addition, the Spatial Interaction Laboratory (SIL) has been introduced as a foundation to develop, deploy, and evaluate ambient intelligence applications.

Next steps are to relax the assumption A4 and A5 to in-

### Acknowledgements

We acknowledge and are thankful for funding by the German Research Foundation (DFG) via the Spatial Cognition Research Center (SFB/TR 8).
References


