computing@computingonline.net
www.computingonline.net

ISSN 1727-6209
International Journal of Computing

A DECISION-THEORETIC APPROACH TO MAINTAIN TRUST IN UBIQUITOUS DISPLAYS ENVIRONMENTS

Katja Kurdyukova, Elisabeth André, Karin Leichtenstern

Faculty of Applied Informatics, Augsburg University, D-86159 Augsburg, Germany
{kurdyukova,andre,leichtenstern}@informatik.uni-augsburg.de
http://mm-werkstatt.informatik.uni-augsburg.de

Abstract: *In this paper, we present a decision-theoretic approach to trust management for ubiquitous display environments that assesses the user's trust in a system, monitors it over time and applies appropriate measurements to maintain trust in critical situations. The approach has been applied to two interactive applications that have been developed as part of a university-wide ubiquitous displays management system. The two applications run on public display located in public rooms at Augsburg University. They can be operated and assisted by mobile phones. In the paper, we define decision policies for the two applications and investigate their impact on relevant trust factors, such as privacy, comfort of use, transparency and controllability.*

Keywords: *Ubiquitous Displays, Adaptive Systems, Trust Management, Decision-Theoretic Approach, Man-Machine Communication.*

1. INTRODUCTION

Recent years has brought about a large variety of interactive displays that are installed in many public places. Apart from simply providing information (e.g. news or weather) to people in public places, such as coffee bars or airports, public displays make it possible for passing individuals to view, edit and exchange specific data between each other. Mobile phones represent a popular interaction device for interacting with these displays since they have been widely adopted by people as an everyday companion and can be customized to individual interaction preferences.

The interaction with large screens comes with a lot of benefits (e.g. usage of full screen mode) but also with a lot of risks, such as the loss of data due to unstable transmission technologies. Bluetooth is often used for the communication between mobile phones and a ubiquitous display environment; see, for example, [3]. Typical problems of Bluetooth emerge in the discovery process and the data transmission because they can unexpectedly require more time or even fail completely. Such a behavior can seriously affect trust in a system since it is no longer considered as reliable and secure. The problem is aggravated by the fact that people usually interact with public displays on a short-term basis without having the possibility to verify the security of the underlying infrastructure.

In addition, the social setting with the possibility to view personalized information in the presence of other people inevitably raises privacy issues. Röcker and colleagues [11] found that users wish to take advantage of large displays in public settings, however, they are worried about the protection of their data. Further, the high dynamics and unpredictability of such environments may have a negative impact on the user's trust. People may approach and leave a public display at any time requiring the systems to permanently adapt to a new situation. Due to the high complexity of the adaption process, the user may no longer be able to comprehend the rationale behind the system's decisions. For example, interviews with users of an adaptive digital signage system that automatically adapts to the assumed interest of an audience revealed that some users did not understand the adaption mechanism, but rather had the impression that the system was presenting randomized information, see [10]. Finally, ubiquitous display environments are characterized by a high degree of autonomy which may leave the users with the feeling that they have no longer any control over the system. It is evident that a limited amount of transparency and controllability will eventually lead to a loss of trust. Summing up, there is an enormous need for sophisticated trust management in ubiquitous display environments in order to ensure that such environments will find acceptance among

users.

While a lot of research has been devoted on improving the security and the reliability of ubiquitous display environments, work on the user experience factor of trust is still scarce. In a user study, we investigated user experience and trust in different mobile interaction technologies [12]. Surprisingly, the users found the interaction via the mobile phone's NFC reader much more trustworthy compared to other mobile technologies (e.g. Bluetooth scanning) due to the short distance between the mobile phone and the physical target object. Obviously, trust of a user in a computer system is not only influenced by technological aspects, but also by perceived or assumed characteristics of the computer system.

The objective of this paper is the development of a trust management system for ubiquitous display environments that assesses the user's trust in a system, monitors it over time and applies appropriate measurements to maintain trust in trust-critical situations [15].

In the remaining paper, we first discuss related work to increase the user's trust in ubiquitous display environments by appropriate interface design. We then describe two applications that are part of a university-wide public displays environment and serve as a test bed for our research. After that, we present a model of a trust management system based on Bayesian Networks and influence diagrams and how this model has been used within our applications. Finally, we present first results of a user study.

2. RELATED WORK

Most work that investigates trust issues in the context of ubiquitous displays environments focuses on the distribution of private and public data over various displays. Often mobile phones are used as private devices that protect the personal component of interaction from public observation.

Röcker and colleagues [11] conducted a user study to identify privacy requirements of public display users. Based on the study, they developed a prototype system that automatically detects people entering the private space around a public display using infrared and RFID technology and that adapts the information that is visible based on the privacy preferences of the users. An evaluation of the system revealed that users are willing to use public displays in case there is a mechanism for privacy protection.

Based on the evaluation of two mobile guides, Graham and Cheverst [5] analyze several types of mismatch between the users' physical environment and information given on the screen and their influence on the formation of user trust. Examples of mismatches include situations where the system is not able to correctly detect the user's current location or situations where the system conveys a wrong impression about the accuracy of its descriptions. To help users form trust, Graham and Cheverst suggest employing different kinds of guide, such as a chaperone, a buddy or a captain, depending on characteristics of the situations, such as accuracy and transparency. For example, the metaphor of a buddy is supposed to be more effective in unstable situations than the chaperone or the captain.

Cao and colleagues [1] introduce the notion of crossmodal displays that enable users to access personalized information in public places while ensuring their anonymity. The basic idea is to publicly display the main information, but to add cues for individual users to prompt them to information that is relevant to them.

All in all, there is a vivid research interest in the design of novel user interfaces for heterogeneous display environments. However, the few approaches that address the user experience factor of trust in such environments do not attempt to explicitly model the user experience of trust as a prerequisite for a trust management system. A number of approaches have been presented to model trust in computational systems. Especially in the area of multi-agent systems (MAS), trust models have been researched thoroughly (see, e.g., Castelfranchi's and Falcone's introduction [2] to a formal modeling of trust theory and its applications in agent-based systems). However, these approaches either focus on trust in software components or aim at modeling trust in human behavior.

3. A PUBLIC DISPLAYS ENVIRONMENT

As a test bed for our research, we employ two applications that have been developed as part of a university-wide displays management system. The two applications run on public displays located in public rooms at Augsburg University. They can be operated and assisted by mobile phones.

The first application, Friend Finder, is an interactive campus map that shows the current location and status of the user's friends. Since many students have difficulties in orienting themselves on the campus (especially in new buildings), Friend Finder also supports a routing function, showing a detailed path to a selected friend (see Fig. 1).

The second application, Media Wall, fosters exchange between the students. It represents a gallery of media items (pictures or videos) uploaded by students or scientific staff. Users can rank the media items, upload new items, and view their favorite ones (see Fig. 2).

Both applications require sophisticated

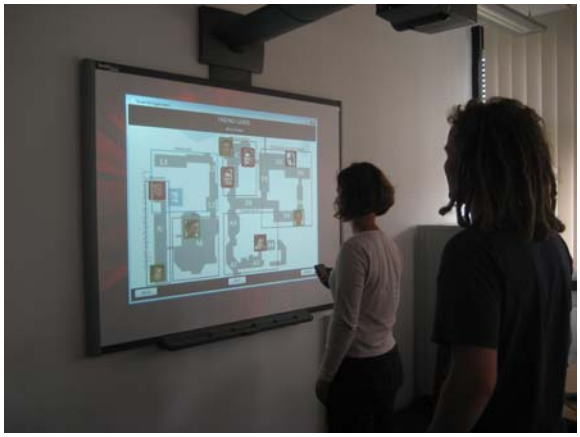

Fig. 1 – Users interacting with Friend Finder

Fig. 2 - User interacting with the Media Wall

mechanisms to adapt to various trust-critical events.

Since Friend Finder may disclose private information about user's social network, it should be able to intelligently adapt to the surrounding social context in order to avoid possible privacy threats. For example, the user in Fig. 1 might not feel comfortable to view personal data on the public display in the presence of the passer-by behind her.

Ranking the media on Media Wall again may threaten the user's privacy in case of observation. Several users may interact with Friend Finder simultaneously, rendering their networks on the same campus map. Therefore, the system should be able to accommodate the data and interaction coming from multiple users.

4. CHARACTERISTICS OF TRUST

Much of the original research on trust comes from the humanities. Psychologists and sociologists have tried for a very long time to get a grasp of the inner workings of trust in interpersonal and interorganisational relationships. Other fields, such as economics and computer science, relied on their findings, but adapted them to the special requirements of their respective fields and the new context they are applied to.

There is consensus that trust depends on a variety of trust dimensions. However, there is no fixed set of such dimensions. Trust dimensions that have been researched in the context of internet applications and e-commerce include reliability, dependability, honesty, truthfulness, security, competence, and timeliness; see, for example, the work by Grandison and Sloman [6] or Kini and Choobineh [7]. More sociologically inclined authors, such as Tschannen-Moran and Hoy [14], introduce willing vulnerability, benevolence, reliability, competence, honesty, and openness as the constituting facets of trust. Researchers working on adaptive user interfaces consider transparency and controllability as major facets of trust; see, for example, the work by Glass and colleagues [4].

In our case the factors have been determined based on interviews with twenty students of computer science who were asked to indicate properties of user interfaces that they felt contributed to their assessment of trustworthiness. The choice of participants was motivated by the envisioned applications, which address students at a university. The most frequent mentions felt into the following categories: comfort of use ("should be easy to handle"), transparency ("I need to understand what is going on"), controllability ("want to use a program without automated updates"), privacy ("should not ask for private information"), reliability ("should run in a stable manner"), security ("should safely transfer data"), credibility ("recommendation of friends") and seriousness ("professional appearance").

Trust depends on experience and is subject to change over time. Lumsden [9] distinguishes between immediate trust dimensions and interaction-based trust dimensions. Immediate trust dimensions, such as seriousness, come into effect as soon as a user gets in touch with a software system while interaction-based trust dimensions, such as transparency of system behavior, influence the users' experience of trust during an interaction.

There is a consensus that trust is highly subjective. A person who is generally confiding is also more likely to trust a software program. Furthermore, users respond individually to one and same event. While some users might find it critical if software asks for personal information, others might not care.

5. USING A DECISION-THEORETIC APPROACH FOR TRUST MANAGEMENT

To model trust, we decided to apply a decision-theoretic approach. The basic idea is to define factors that have an influence on the user's feelings of trust and to investigate how these factors can be influenced by particular system actions.

We have chosen to model the users' feelings of trust by means of Dynamic Bayesian Networks [13]. The structure of a Bayesian Network is a directed, acyclic graph (DAG) in which the nodes represent random variables while the links or arrows connecting nodes describe the direct influence in terms of conditional probabilities.

Bayesian Networks enable us to model the influence of different trust dimensions on the user's trust in a rather intuitive manner. For example, it is rather straightforward to model that reduced transparency leads to a decrease of user trust. The exact probabilities are usually difficult to determine. However, the conditional probabilities can also be (partially) derived from the user data (see our earlier work where we presented an experiment to collect data for this purpose [8]. In Fig. 3, a small portion of a Bayesian Network is shown that we use for modeling trust in our two applications.

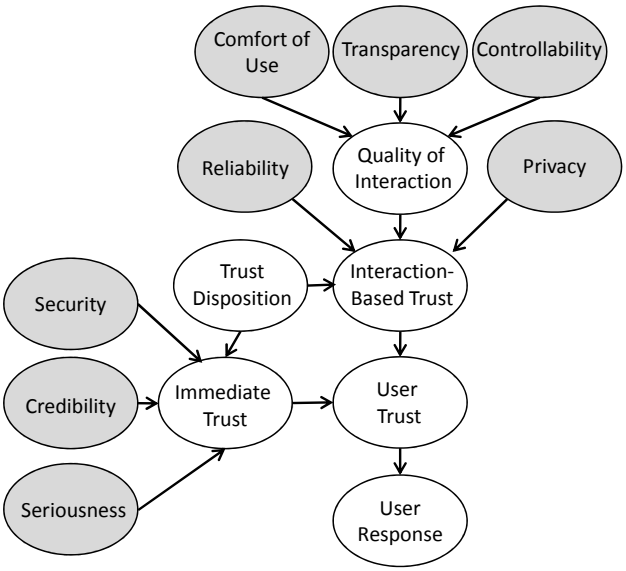

Fig. 3 – Small portion of a Bayesian Network with trust dimensions (trust dimensions in gray)

Dynamic Bayesian Networks allow us, in addition, to model the dependencies between the current states of variables and earlier states of variables. In particular, we are able to represent how the user's current level of trust is influenced by earlier levels of trust. To keep things simple, we only consider the user's level of trust at time t_{i-1} when determining the user's level of trust at time t_i(see the extension to a Dynamic Bayesian Network in Fig. 4).

To use the Bayesian Network formalism for decision-making, it has to be extended to an influence diagram by adding a decision node and a utility node. The decision node represents all system action that the system can perform while the utility node encodes the utilities of all possible outcomes.

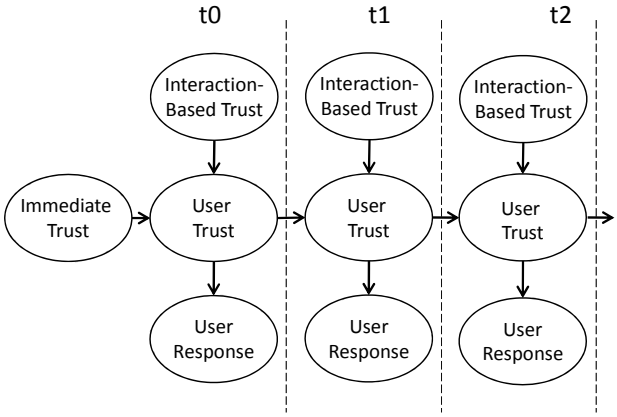

Fig. 4 – Dynamic Bayesian Network

To take a decision, the system evaluates the utility of all possible options in terms of user trust and chooses the action with the highest utility.

In Fig. 5, a small portion of the influence diagram is shown. We illustrate the basic idea by means of one trust dimension, namely privacy.

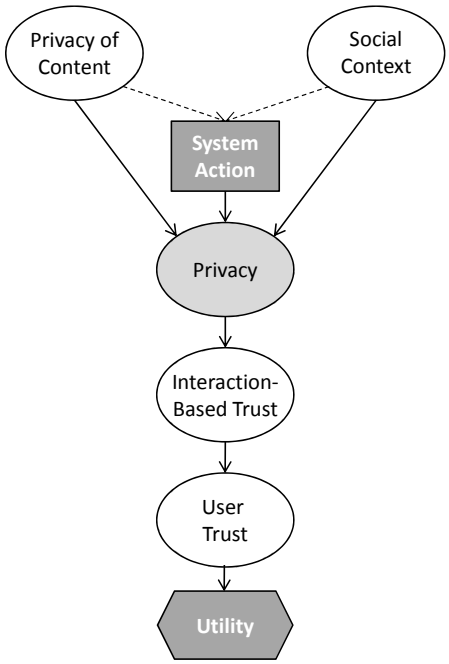

Fig. 5 – Small portion of an influence diagram

Privacy is handled as a hidden variable with three discrete values low, medium and high. That is its value cannot be directly observed, but has to be inferred from observables variables, such as *Privacy of Content* and *Social Context*. For example, the likelihood that the variable *Privacy* has the value *Low* would be high if *Personal Content* has the value *Private* and *Social Context* has the Value *People Approaching*. These dependencies are indicated by the arrows going from *Social Context* and *Privacy of Content* to *Privacy*. Associated with the decision node *System Action* is a table which describes the system's decision policy for each

combination of the variables *Social Context* and *Privacy of Content*. The arrow going from *System Action* to *Privacy* represents the impact a particular system action, for example, the masking of private information, has on privacy.

6. APPLYING THE APPROACH TO UBIQUITOUS DISPLAYS

In the previous section, we described the general structure of an influence diagram as the basis for the implementation of a trust management system. In the following, we illustrate how to set the probabilities for concrete applications.

In an earlier paper [8], we described how build up conditional tables for modeling user trust based on an experiment where users had to rate trust and trust factors for prototypes they got confronted with. For this reason, we will not explain the modeling of trust in detail here, but focus on how to set the probabilities for the decision-making process.

One possibility is to learn influence diagrams based on collected user data. Another option is to set up the influence diagrams based on informed guesses. For example, probabilities that represent the influence of actions on trust factors referring to the quality of interaction may be assessed by considering usability guidelines. Since the acquisition of data is rather time-consuming and can in most cases not directly be transferred from one application to the other, we decided to follow the second approach.

In the following, we analyze the impact of various system reactions to typical trust-critical situations on relevant trust factors, providing illustrations from Friend Finder and Media Wall.

Let us assume that the user is viewing private data on the public screen as other users pass by. Such a situation may occur in Friend Finder when users load a map of the university campus with friends on a public screen. The locations and pictures of friends are considered as private information, not supposed to be observed by any one. Within the influence diagram shown in Fig. 5, this situation is described by the values of the variables *Social Context* and *Privacy of Content*.

In Table 1, four possible responses to the described situation are listed. Basically, the system has to decide whether it should trust the user takes appropriate steps herself (Option 1), whether it should adapt the display of information to the changed social context (Option 2 and 3) or whether it should ask the user for confirmation first (Option 4). Within the influence diagram shown in Fig. 5, the available options are represented by the decision node *System Action*.

Fig. 6 shows Friend Finder's implementations of Option 3. The photos of the user's friends are masked with icons and the private data migrates to the mobile screen. Fig. 7shows the implementations of option 3 in Media Wall. Here, the system masks the ranking and moves it to the mobile phone.

Option 1 bears the risk that the user might expect the system to protect her privacy and is upset if no appropriate actions are taken. Options 2 and 3 have the limitations that they cause an interruption of the user's work flow and might give her the feeling that she has the system no longer under control. The drawback of Option 4 is that there might not be enough time for the user to confirm the adaptations proposed by the system.

Compared to Option 2, Option 3 has the

Table 1. Possible system reactions to changing social context

Situation	Possible System Action
User interacts with some private data on a public display. Another user approaches the display and starts to interact as well. Other people are around the display.	1. Do not take any action 2. Move all data from the public display to the mobile display 3. Mask private data on the public display and move the data to the mobile screen 4. Notify the user about potential privacy issues and offer options to protect data

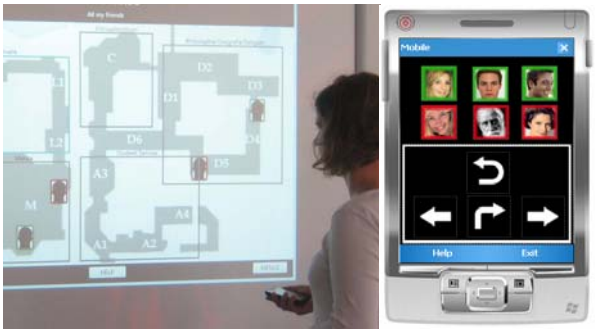

Fig. 6 - Friend Finder: System masks private data on public display and display the private details on the mobile screen (Option 3)

Fig. 7 - Ranking on Media Wall: the system masks user ranking and moves it to the mobile phone

advantage that the user is still able to execute desired actions. Thus on Friend Finder the user can select a desired friend and get a route to his or her destination. In this case, the user still profits from the large real estate of the public screen, while preserving personal information. Furthermore, the Option 3 allows several users to interact at the same time (see Fig.8).

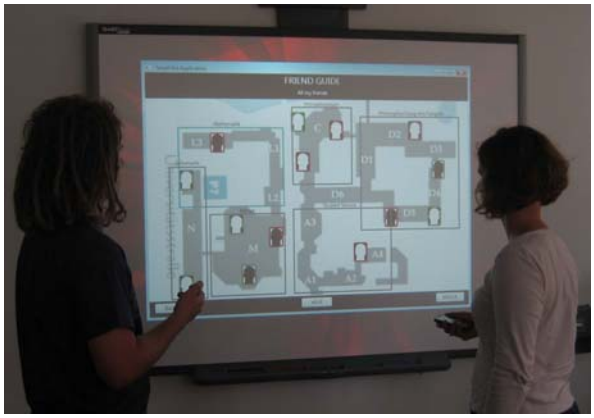

Fig. 8 - Friend Finder: System masks the private data for both interacting users

Table 2 summarizes the analysis above. It lists the consequences of system actions on relevant trust dimension. In particular, we indicate how likely it is that the system actions will change the ratings of the trust dimensions if private context is displayed in the presence of others. Based on this table, conditional probabilities may be derived that represent the dependencies between system actions and trust dimensions. For example, the likelihood that privacy is low is high if private content is displayed in the presence of other people and the system takes no action while it is low if the system masks private content. Please note that the table refers to a particular situation that is described by values of the variables *Social Context* and *Privacy of Content*. For other situations, additional tables describing the impact of possible system actions on trust dimensions need to be built up.

7. EVALUATION OF THE APPROACH

In the following, we present a first evaluation of the decision-theoretic approach.

In an earlier experiment [8], we evaluated to what extent the system is able to predict the user's ratings of trust based on her ratings of relevant trust factors (transparency, controllability, comfort of use, seriousness, credibility and security). In particular, we created a model based on the ratings given by the users using the Genie built-in algorithm for learning Bayesian Networks (see http://genie.sis.pitt.edu/). When evaluating this model in 10-fold cross validation, we achieved an accuracy rate of 73 % for five classes(very low trust, low trust, medium trust, high trust, very high trust).

In this paper, we briefly discuss first steps towards the evaluation of the decision-making approach. In a small experiment, we aimed to test to what extent our approach leads to an increase of user trust. To this end, we presented six users in Friend Finder and Media Wall with a situation in which the user is viewing private information as other users pass by. We furthermore showed them how the system would respond in such a situation (Options 1 – 4) and ask them to rate their trust into the system. The results of this test are shown in Fig. 9.Since there was no clear preference for a particular system action, it was not possible to assess the system's ability to decide on an appropriate action to take. Despite the small number of users, the test shows, however, that the users clearly preferred the system to take initiative and either adapt automatically to the social context or ask the user to confirm the adaptation.

Another interesting finding is the fact that the user trust was higher in situation where the system automatically adapted to a trust-critical situation than in situations where no problem occurred. Furthermore, the differences in the case of the Media Wall were less extreme than in the case of the Friend Finder. We hypothesize that the information displayed with Media Wall (ratings of photos) was considered as less sensitive than the information displayed with Friend Finder (location of people).

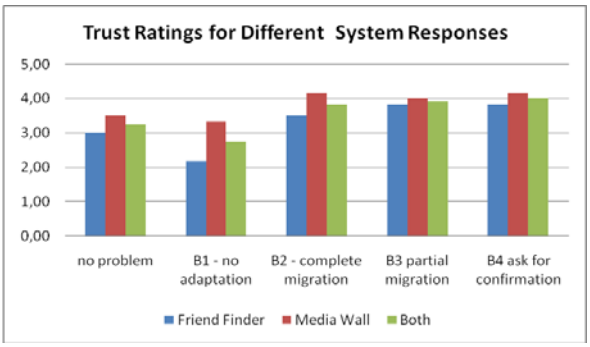

Fig. 9 - Trust ratings for different responses

Table 2. Relationship between system actions and trust dimensions

	Transparency	Controllability	Comfort of Use	Privacy	Reliability
No Adaptation Option 1	**0**	**0**	**0**	--	- -
Complete Migration Option 2	-	-	--	++	**0**
Partial Migration Option 3	-	-	-	+	**0**
Offer Options and Ask for Confirmation Option 4	+	++	--	++	**0**

-: Somewhat likely to decrease, --: likely to decrease, 0: not likely to change,

+: Somewhat likely to increase, ++: likely to increase

8. CONCLUSIONS

Ubiquitous displays environments require a high degree of flexibility due to the changing social context and probably incomplete or inaccurate information a system has to base its presentations on. In order to maintain user trust in such environments, a system needs to be able to carefully evaluate the consequences of its actions and the trade-offs between them. In this paper, we presented a decision-theoretic approach to trust management. The approach has been informed by guidelines on user interface design in order to assess the impact of system actions on trust dimensions, such as comfort or use, transparency, controllability and privacy. A first evaluation of the approach within two applications that have been developed as part of a university-wide public displays environment revealed that users preferred the adaptive system over the non-adaptive system.

9. ACKNOWLEDGEMENTS

This research is partly sponsored by OC-Trust (FOR 1085) of the German research foundation (DFG).

10. REFERENCES

[1] Cao H., Olivier P. & Jackson D. Enhancing privacy in public spaces through crossmodal displays. *Soc. Sci. Comput. Rev.*, 26 (1), 2008, pp. 87-102.

[2] Castelfranchi C. & Falcone R. *Trust Theory: A Socio-Cognitive and Computational Model.* Wiley, 2010.

[3] Cheverst K., Dix A., Fitton D., Kray C., Rouncefield M., Sas C. et al. Exploring bluetooth based mobile phone interaction with the hermes photo display. *MobileHCI '05: Proceedings of the 7th international conference on Human computer interaction with mobile devices & services*. New York, NY, USA: ACM, 2005, pp. 47-54.

[4] Glass A., McGuinness D. L., & Wolverton M. Toward establishing trust in adaptive agents. *IUI '08: Proceedings of the 13th international conference on Intelligent user interfaces,* New York, NY, USA: ACM, 2008, pp. 227-236.

[5] Graham C., & Cheverst K. Guides, locals, chaperones, buddies and captains: managing trust through interaction paradigms. *3rd Workshop 'HCI on Mobile Guides' at the Sixth International Symposium on Human Computer Interaction with Mobile Devices and Services,* New York, NY, USA: ACM, 2004, pp. 227-236.

[6] Grandison T., & Sloman M. A survey of trust in internet applications. *IEEE Communications Surveys and Tutorials, 3* (4), 2000, pp. 2-16.

[7] Kini A., & Choobineh J. Trust in electronic commerce: definition and theoretical considerations. *Proc. of the Hawaii International Conference on System Sciences, 31,* 1998, pp. 51-61.

[8] Leichtenstern K., André E., & Kurdyukova K. Managing user trust for self-adaptive ubiquitous computing systems. *MoMM'10: Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia.* New York, NY, USA: ACM, 2010.

[9] Lumsden J. Triggering trust: to what extent does the question influence the answer when evaluating the perceived importance of trust triggers? *BCS HCI'09: Proceedings of the 2009 British Computer Society Conference on Human-Computer Interaction*. Swinton, UK, UK: British Computer Society, 2009, pp. 214-

223.
[10] Müller J., Exeler J., Buzeck M., & Krüger A. ReflectiveSigns: digital signs that adapt to audience attention. In H. Tokuda, M. Beigl, A. Friday, A. J. Brush, & Y. Tobe (Hrsg.), *Pervasive Computing, 7th International Conference, Pervasive 2009, Nara, Japan, May 11-14, 2009. Proceedings 5538*, pp. 17-24. Springer.
[11] Röcker C., Hinske S., & Magerkurth C. Intelligent privacy support for large public displays. *Proceedings of Human-Computer Interaction International 2007 (HCII'07)*. Beijing, China.
[12] Rukzio E., Leichtenstern K., Callaghan V., Holleis P., Schmidt A., & Chin J. S.-Y. An experimental comparison of physical mobile interaction techniques: touching, pointing and scanning. In P. Dourish, & A. Friday (Hrsg.), *UbiComp 2006: Ubiquitous Computing, 8th International Conference, UbiComp 2006, Orange County, CA, USA, September 17-21, 2006. 4206*, pp. 87-104. Springer.
[13] Russell S. J., & Norvig P. *Artificial Intelligence a modern approach* (2nd international edition Ausg.). Upper Saddle River, N.J.: Prentice Hall, 2003.
[14] Tschannen-Moran M., & Hoy W. K. A multidisciplinary analysis of the nature, meaning, and measurement of trust. *Review of Educational Research*, 70 (4), (2000), 547.
[15] Yan Z., & Holtmanns S. Trust modeling and management: from social trust to digital trust. *Book chapter of Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions, 2008*.

Katja Kurdyukova *is a PhD student at Augsburg University. Before that, she got her Bachelor's degree at the Moscow Technical University and studied for her Master's at the Technical University of Aachen, Germany. Her research interests comprise interaction design, persuasive computing, and ubiquitous computing.*

Elisabeth André *is a full professor of computer science at Augsburg University and Chair of Human-Centered Multimedia. Before that, she worked as a principal researcher at DFKI GmbH where she has been leading various academic and industrial projects in the area of intelligent user interfaces. Her main research interests include multimodal interfaces, affective computing and embodied conversational agents.*

Karin Leichtenstern *is a PhD student at Augsburg University. Before that, she graduated in Media Informatics at the University of Munich and stayed a half of a year at the Intelligent Inhabited Environments Group at the University of Essex, UK. Her main research interests include pervasive and mobile computing as well as mobile context-awareness.*