Journal of Trust Management
a SpringerOpen Journal

RESEARCH Open Access

Trust-based Decision-making for the Adaptation of Public Displays in Changing Social Contexts

Michael Wißner*, Stephan Hammer, Ekatarina Kurdyukova and Elisabeth André

*Correspondence:
wissner@hcm-lab.de
Human Centered Mutimedia, Augsburg University, Universitätsstr. 6a 86159, Augsburg, Germany

Abstract

Public displays may adapt intelligently to the social context, tailoring information on the screen, for example, to the profiles of spectators, their gender or based on their mutual proximity. However, such adaptation decisions should on the one hand match user preferences and on the other maintain the user's trust in the system. A wrong decision can negatively influence the user's acceptance of a system, cause frustration and, as a result, make users abandon the system. In this paper, we propose a trust-based mechanism for automatic decision-making, which is based on Bayesian Networks. We present the process of network construction, initialization with empirical data, and validation. The validation demonstrates that the mechanism generates accurate decisions on adaptation which match user preferences and support user trust.

Introduction

Recent years have 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. While ubiquitous display technologies offer great benefits to users, they also raise a number of challenges. In particular, they might show a behavior that negatively affects user trust.

First, ubiquitous display environments are characterized by high dynamics. People may approach and leave a display at any time requiring the system to permanently adapt to a new situation. Due to the high complexity of the adaptation process, the user may no longer be able to comprehend the rationale behind the system's decisions which may negatively affect the formation of user trust. This echoes the view put forward by Rothrock et al. [1]. According to them, the sudden changes in an adaptive display's user interface (such as displayed content, layout or the used modality) are not always self-explanatory for the users. If they cannot recognize the reason for a system adaptation or if they do not consider the adaptation as plausible given the current situation, user trust can be impaired, which can lead to disuse of the system in the worst case.

Due to sensor technology that has become available in the recent years, interaction with ubiquitous displays is no longer exclusively based on input explicitly provided by a user,

for example, by controlling displays with a mobile phone. Instead, systems exploit information that is implicitly given by the context in which an interaction takes place. A typical form of implicit interaction with public displays is enabled by proxemics behaviors, i.e. the interpretation of human body position, orientation, and movement to proactively initiate system reactions [2]. On the one hand, the use of implicitly provided information facilitates human-computer interaction and contributes to its robustness. On the other hand, it raises trust issues with the user because proactive system actions are frequently not understood by the users and limit their control over the system. Furthermore, deficiencies of the underlying sensor technology might cause a rather obscure system behavior. Similar issues were reported by Müller et al. [3]. In interviews with the users of their adaptive digital signage system, which automatically adapts to the assumed interest of an audience, it was revealed that some users had the feeling that the system was presenting randomized information. This shows that the users were no longer able to understand the rationale behind the system's decisions.

Finally, the social setting with the possibility of viewing personalized information in the presence of other people inevitably raises privacy issues. Since public displays are typically shared by several people, personal information for a particular user has to be protected from unwanted views by others, for example, by migrating it to the user's personal device. Otherwise, there would be the risk that people lose trust in such displays and abandon using them. Röcker and colleagues [4] found that users wish to take advantage of large displays in public settings, however, they are worried about the protection of their data. The problem is aggravated by the fact that user typically interact with ubiquitous display environments on an occasional basis without having the possibility to verify the security of the underlying infrastructure.

To sum 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. In this paper, we present a decision-theoretic approach to a trust management system for ubiquitous display environments that assesses the user's trust in a system, monitors it during the interaction and applies appropriate measures to maintain trust in critical situations [5]. Such situations arise inter alia when other people enter the user's private space [4], when the system has to generate presentations based on inaccurate user or context data [6] or when the system's adaptation behavior mismatches the user's expectations [7].

While most work in the area of computational trust models aims to develop trust metrics that determine on the basis of objective criteria whether a system should be trusted or not, the focus of our work is on trust experienced by a user when interacting with a software system. A system may be robust and secure, but nevertheless be perceived as not very trustworthy by a user, for example, because its behavior appears opaque or hard to control to them. Following the terminology by Castelfranchi and Falcone [8], our work focuses on the affective forms of trust that are based on the user's appraisal mechanisms. More specifically, our objective is the development of a computational trust model that captures how a system - in this paper an ubiquitous display environment - is perceived by a user while interacting with it.

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

assisted by mobile phones. All four applications require sophisticated mechanisms to adapt to various trust-critical events. Some may disclose private information about users, and thus should be able to intelligently adapt to the surrounding social context in order to avoid possible privacy threats. Possible options include the hiding, masking or migration (to a mobile device) of the critical data. Others might allow multiple users to interact simultaneously and thus should open space for new users as they approach, rearranging the current users' content if necessary.

In the rest of the paper, we first discuss related work on increasing the user's trust in ubiquitous display environments by appropriate interface design. After that, we present our model of a trust management system and mechanism for automatic decision-making based on Bayesian Networks (BN). Relying on empirical data gathered in both an online and a live study, we initialize and validate the networks and demonstrate how they can be used to generate adaptation decisions in changing social contexts.

Background and literature review

While research on computational models of trust has become very popular in the area of agent-based society, approaches that model trust as a user experience are rare. This is unsurprising because the psychological aspects of trust are hard to measure directly. In the following, we will first review work on computational models of trust starting from approaches that have been presented for agent-based societies and social networks before we discuss how the concept of trust has been treated in the context of ubiquitous display environments.

Computational models 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 to come up with dedicated models of trust that are adapted to the specific requirements of their domains and the context they are applied to. Since trust is a social phenomenon, it seems to be a promising approach to exploit models that have been developed to characterize trust in human societies as a basis for computational models of trust.

Especially in the area of multi-agent systems, computational models for trust-based decision support have been researched thoroughly. Pioneering work in this area has been conducted by Marsh [9] who modeled trust between distributed software agents as a basis for the agents' cooperation behavior. Computational mechanisms that have been proposed for trust management in agent-based societies include Bayesian Networks [10], Dempster-Shafer Theory [11], Hidden-Markov Models [12], Belief Models [13], Fuzzy models [8], game-theoretic approaches [14] or decision trees [15]. There is empirical evidence that the performance of agent-based societies may be improved by incorporating trust models.

While the approaches above focus on trust between software agents, work in the area of social media aims to model trust between human users, see [16] or [17] for a survey investigating trust in social networks. Using algorithmic approaches or machine learning techniques, trust between users is derived from objective observations, such as behavior patterns in social networks. An example includes the work by Adali et al. [18] who

assessed trust between two users based on the amount of conversation and the propagation of messages within the Twitter social network. Other approaches derive trust that is given to users from community-based reputation or social feedback, see, for example, the work by Ivanov et al. [19].

Unlike the above-mentioned approaches, our own research focuses on trust which users experience when interacting with a software system. Most work in this area aims to identify trust dimensions that influence the user's feeling of trust. 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 [20] or Kini and Choobineh [21]. Tschannen et al. [22], who are more interested in the sociological aspects of trust, introduce willing vulnerability, benevolence, reliability, competence, honesty, and openness as the constituting facets of trust. Researchers working on adaptive user interfaces consider transparency as a major component of trust, see, for example, the work by Glass et al. [7]. Trust dimensions have formed the basis of many conceptual models of trust. However, incorporating them into a computational model of trust is not a trivial task.

Indeed, computational models that assess trust felt by a user are rare. One of the few approaches in this area includes the work by Yan et al. [23]. Their computational model captures users' trust experience when interacting with mobile applications. In order to present users with appropriate recommendations that help increase the users' trust, they identified various user behaviors that can be monitored by a mobile device in addition to external factors, such as brand impact. The benefits of this approach have been shown by means of simulations. However, the approach has not been embedded in a pervasive environment to control the selection of system actions during an interaction. Since an offline evaluation may provide different results than a more challenging online evaluation with interacting users, the approach presented in this paper has been tested within live studies as well.

Trust management in ubiquitous display environments

Most work that investigates the phenomenon of trust in the context of ubiquitous display environments focuses on privacy issues, i.e. 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 et al. [4] 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 adapts the information that is visible based on the privacy preferences of the users. An evaluation of the system revealed that privacy protection mechanisms may help increase user trust and thus improve the acceptance of public displays. While the system included mechanisms to enhance the user's privacy, it did not monitor the user's trust into the system during the interaction.

Based on the evaluation of two mobile guides, Graham and Cheverst [6] analyzed 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 included situations where the system was not able to correctly detect the user's current location or situations where the system conveyed a wrong impression about the accuracy

of its descriptions. To help users form trust, Graham and Cheverst suggested to employ 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 was supposed to be more effective in unstable situations than the chaperone or the captain. However, their guides did not include any adaptation mechanism to maintain user trust in critical situations.

Cao et al. [24] proposed an approach that enabled users to access personalized information in public places through their mobile devices while ensuring their anonymity. The basic idea was to publicly present all information on a display, but to indicate to individual users only which part of the information is relevant to them by sending personal crossmodal cues (such as vibrations) to their mobile devices. In other words, the approach tried to enhance the users' privacy by obscuring the access to personal information to the public. Initial evaluations of the approach focused on usability issues, but not on the question of whether crossmodal cues appropriately address the users' privacy concerns.

All in all, there is a vivid research interest in the design of novel user interfaces for heterogeneous display environments. However, those few approaches that do 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.

Research design and methodology

Modeling user trust through trust dimensions

Our trust management system is based on trust dimensions that allow us to derive user trust from relevant properties of a computer system. The trust dimensions are extracted from the literature (see Section 'Background and literature review') and our own user studies.

To identify a set of relevant trust dimensions, we conducted interviews with 20 students of computer science who were asked to indicate trust factors of user interfaces that they felt contributed to their assessment of trustworthiness. The choice of the study participants was motivated by the application domain, a university-wide ubiquitous display environment. The most frequent mentions fell 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"). Less frequently mentioned trust factors included the visual appeal of a user interface and the brand of its developer.

The interviews gave a first impression on which factors influence the user's trust in a user interface. However, they did not provide any concrete information regarding their relative importance. To acquire more quantitative data, we designed a follow-up study which made use of a setting that was inspired by applications developed in the area of ubiquitous display environments. The setting consisted of a mobile phone and an interactive table. The table served as the central medium for showing and editing multimedia data whereas the mobile phone was used to send data to or receive data from the table. Thereby, the transmission and the point of time of the presentation of the data on the table were trust-critical moments for the user. In order to get a sufficient variety of user

ratings, we built a number of prototypes where we manipulated the following variables: self-explainability, transparency, controllability and privacy.

We recruited 20 people of which the majority (16 people) had a background in computer science. Each participant had to perform various tasks for the single prototypes, such as transferring data between the table and the mobile phone. After completing all tasks for a single prototype, the participants had to rate the prototype according to the trust dimensions identified earlier (comfort of use, controllability, transparency, privacy, security, seriousness, credibility and trustworthiness) as well as their emotions (uneasiness, insecurity, irritation and surprise) on a five point Likert scale (from very low to very high).

The participants rated their general trust into software systems with a mean value of 3.10 (STD = 0.79) and their knowledge about secure data transmission with a mean value of 3.5 (STD = 1.05). To measure the degree of relationship between the ratings for trust and the ratings for the trust dimensions, we computed the Pearson product moment correlation coefficients. The test revealed a moderate to high positive correlation between the ratings for trust on the one hand and the ratings for seriousness ($r = 0.724$), controllability ($r = 0.70$), security ($r = 0.62$), privacy ($r = 0.61$), transparency ($r = 0.56$) and credibility ($r= 0.66$) on the other hand. For all items, the correlation was very significant ($p = 0.01$). The better the ratings for the trust dimensions, the better were also the ratings for trust.

In addition, we observed a moderate positive correlation ($r = 0.35$) between the users' ratings of their general trust into software and their reported trust into the presented system at the significance level of $p = 0.01$. We did not did not find any correlation between the user's self assessment of competence and their reported trust into the presented system. As a potential reason, we indicate that the majority of the users had a background in computer science. As a consequence, their self assessment of competence was rather high with a mean value of 4.03 (STD = 0.75).

Finally, our results revealed a moderate negative correlation between trust on the one hand and uneasiness ($r = -0.629$), insecurity ($r = -0.533$), irritation ($r = -0.484$) on the other hand. For all items the correlation was very significant ($p = 0.01$). We conclude that poor transparency, poor controllability, poor security, poor privacy and poor seriousness result into a loss of trust which in turn leads to a feeling of uneasiness.

Most of the results we obtained were in line with previous studies on the identification of trust factors even though we focused on a different application domain and target group. More information regarding the experiments described here can be found in [25] and [26].

Building the Bayesian network

As mentioned above, the identified trust dimensions form the basis of our computational trust model. Such a model should account for the following characteristics of trust:

Trust as a subjective concept: 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 the same event. While some users might find it critical if a software asks for personal information, others might not care. We aim at a computational model that is able to represent the subjective nature of trust.

Trust as a non-deterministic concept: The connection between events and trust is inherently non-deterministic. We cannot always be absolutely sure that the user notices a critical event or actually considers such an event as critical. As a consequence, it does not make sense to formulate rules that predict in a deterministic manner which level of trust a user has in a particular situation. A computational model of trust should be able to cope with trust as a non-deterministic concept.

Trust as a multifaceted concept: As shown above, trust is a multi-faceted concept. We therefore aim at a computational model that is able to explicitly represent the relative contribution of the trust dimensions to the assessment of trust. In particular, the model should help us predict the user's level of trust based on dimensions, such as the perceived transparency and controllability of a user interface. Furthermore, the model should allow us to easily add trust dimensions based on new experimental findings.

Trust as a dynamic concept: Trust depends on experience and is subject to change over time. Lumsden [27] 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. To model trust as a dynamic concept, we need to be able to represent how the user's level of trust depends on earlier levels of trust.

We have chosen to model the users' feelings of trust by means of Bayesian Networks. The structure of a Bayesian Network is a directed, acyclic graph in which the nodes represent random variables while the links or arrows connecting nodes describe the direct influence in terms of conditional probabilities (see [28]).

Bayesian Networks meet the requirements listed above very well: First of all, they allow us to cope with trust as a subjective concept. For example, we may represent the system's uncertain belief about the user's trust by a probability distribution over different levels of trust. Furthermore, the connection between critical events and trust is inherently non-deterministic. For example, we cannot always be absolutely sure that the user notices a critical event at all. It may also happen that a user considers a critical event as rather harmless. Bayesian Networks allow us to make predictions based on conditional probabilities that model how likely the value of the child variable is given the value of the parent variables. For example, we may model how likely it is that the user has a moderate level of trust if the system's behavior is moderately transparent. Furthermore, Bayesian Networks enable us to model the relationship between trust and its dimensions 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, we derived the conditional probabilities from the user data we collected both in the study mentioned above, as well as the study described later in Section 'Gathering empirical data'.

In Figure 1, a Bayesian Network (BN) for modeling trust is shown. For each trust dimension, we introduced a specific node (second layer from the top, shown in blue). Following Lumsden [27], we distinguish between initial (immediate) and interaction-based trust dimensions. The left part of the network represents the factors influencing the establishment of *Initial Trust* that arises when a user gets a first impression of a system. Initial Trust consists of the trust dimensions *Security*, *Seriousness* and *Credibility*.

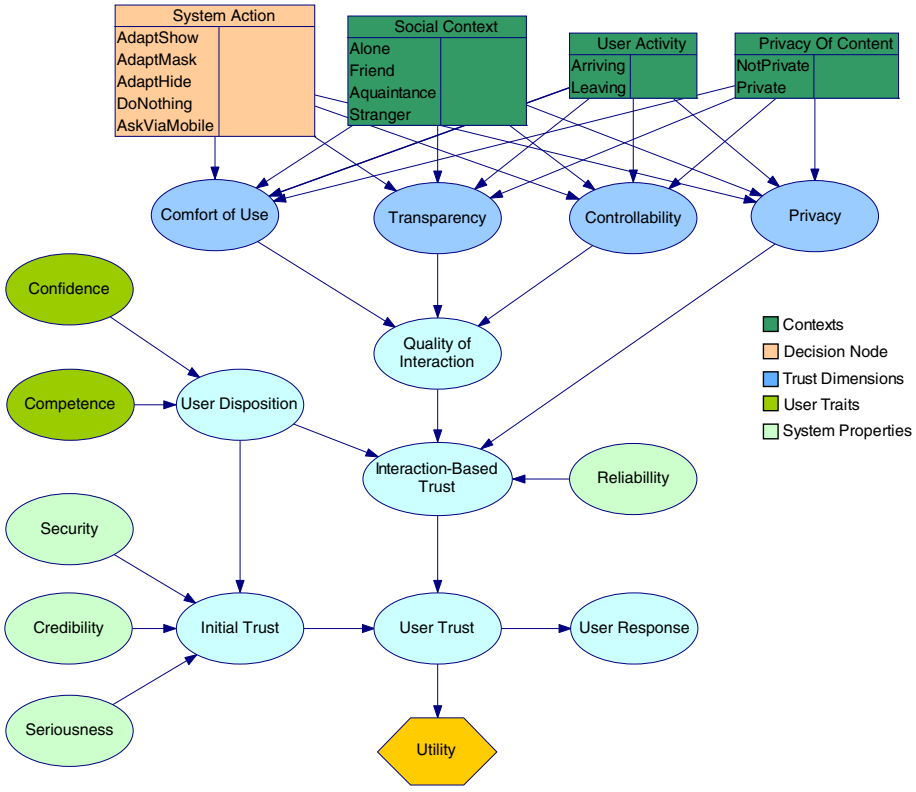

Figure 1 Bayesian network. Example of a Bayesian network for modeling trust.

Security, for example, could be conveyed by the use of certificates. A system's *Seriousness* is reflected, for example, by its look-and-feel. *Credibility* could be supported by additional information, such as a company profile. In this context, we would like to emphasize that trust dimensions may only affect the user's trust if the user is aware of them. For example, high security standards will only have an impact on user trust if the user knows that they exist. For the sake of simplicity, we assume that initial trust dimensions do not change over time. That is, we do not consider the fact that a user might notice references to security certificates only after working with a system over a longer period of time.

To describe the determinants of *Interaction-Based Trust*, we further distinguish between the *Quality of Interaction*, *Privacy* and *Reliability*. The *Quality of Interaction* is characterized by *Transparency*, *Controllability* and *Comfort of Use*. Both the establishment of *Immediate Trust* and *Interaction-Based Trust* depend on the users' *Trust Disposition* which is characterized by their *Competence* and general *Confidence* towards technical systems.

All of the single trust dimensions are treated as hidden variables that cannot be observed directly, but may be inferred from observable variables. Observable variables describe the current context: Examples include privacy level of data, presence of mobile devices, and social context. The latter reflects the social situation: whether the user is alone or not, how close the users are from the display, what the relationships between the present users are, which gender the users have, etc. Knowing the contextual situation,

the BN can be used to estimate the impact that certain actions of the display will have on trust and trust dimensions. The trust dimension *Privacy*, for example, could be negatively affected by the display of private data in the presence of other people.

In order to use the BN for decision-making, we extended it to an influence diagram. We added the decision node *System Action*, representing all actions the display could choose to react on context changes and a *Utility* node that encodes the utilities of all these actions to maintain the user's trust. As an example, let us assume a user wishes to display data on a public display while other people are present. Such a situation could be described by the values of the BN's nodes *Social Context* and *Privacy of Content*. These have been determined by sensors or application data and are thus known by the system. The system may now consider three options to cope with the user's request: (1) transferring all data to the public display no matter whether they are private or not, (2) show only the information marked as non-private or (3) asking the user for a confirmation of one of these actions. Considering the example, option (1) may result in serious privacy concerns, option (2) may confuse the users if there is no plausible explanation for the adaptation, and option (3) could be less comfortable to use in a dynamic setting, such as the prototype settings described in this paper. Furthermore, if the system decides in favor of option (1) or (2), the users might perceive the system as less controllable. The arcs between the decision node and the nodes for the five dimensions of trust represent such influences. To choose the adaptation that is most useful for the system in a specific situation, the *Utility* node computes the utility of all possible actions and their consequences and returns the action with the highest utility. Since the goal of our work is to maintain and maximize user trust, the *Utility* node is attached to a node representing the *User Trust* and measures the utility of each single decision in terms of the resulting user trust - a combination of *Initial Trust* and *Interaction-Based Trust*.

Methods

Gathering empirical data

In order to be able to generate decisions, the BN needed to be initialized with empirical data. The data was collected through experiments conducted with potential users. The users were confronted with scenarios illustrating different contextual combinations (situations) and possible adaptive reactions of the displays in these situations that differed in the degree of transparency, user control, privacy and comfort of use. To discover which of the system reactions succeeded in maintaining users' trust and which did not, the users had to reflect on their perception of the display reactions in the specific situation and had to give insights into their feelings of trust and the related trust dimensions. The estimations served as a quantitative input for the initialization of the BN.

The collection of empirical data was arranged in two steps: First, an online survey targeting as many users as possible was conducted. This study presented a collection of applications demonstrating various content types typical of modern public displays: social networks, pictures and videos, maps and travel planning, and shopping items. These content types can be frequently found in real life projects [29,30] as well as in research works [31,32]. The applications showcased different trust critical situations in which an adaptation was necessary: space conflicts, privacy issues, and migration of data from public to mobile displays. The reason to involve several applications was based on our objective

of verifying that the proposed approach works equally (or comparably) well for different kinds of content, different sources of social context, and different adaptation scenarios. If the approach indeed delivered robust results, we could generalize its applicability to a wide range of adaptive applications.

Since an online survey might not convey the experience of a real interaction and thus affect the ratings of the users, we also performed a live study. The experiments in this study involved two different applications that were also presented in the online survey. The live experiments were designed identically to the online surveys, but involved real user interactions.

All in all, the online survey was aimed to gather as much data as possible, involving online users. The live study was aimed to complement the online survey, supporting the results collected online by the evaluations of users during a real interaction. The studies were performed in compliance with the ethical guidelines set by Augsburg University. Below we describe both studies in detail and present the obtained results.

Prototypes employed for the studies

The first prototype, Friend Finder (FF), represents a public display supporting social networking [33]. Once a user comes closer, the large display shows the user's social network overlaid over a local map, depicting the status and locations of friends (see Figure 2 left). By selecting individual friends via their mobile phone users are able to display a route to the selected friend. The second prototype, Media Wall (MW), supports media exchange within a community [33]. It displays a gallery of private media items (pictures or videos) when a user approaches. Then the user, for example, can browse or rank the items via his mobile phone (see Figure 2 right). The third prototype, Travel Planner (TP), helps students arrange low-budget trips around Europe. By browsing the map on the large display map via their mobile phone, users can retrieve information on the cities and the estimated cost of a visit (see Figure 3 left). Apart from this neutral information, the application also is able to consider private budget-related data, if the user is logged in. In the budget-aware mode, the pop-up information is directly linked to the user's budget and shows whether the estimated costs are within budget. The fourth prototype, Shopping Mall display (SMD), aims at supporting customers of a shopping mall in finding products of their interests and the corresponding shops (see Figure 3 right) by displaying personalized information when a user approaches.

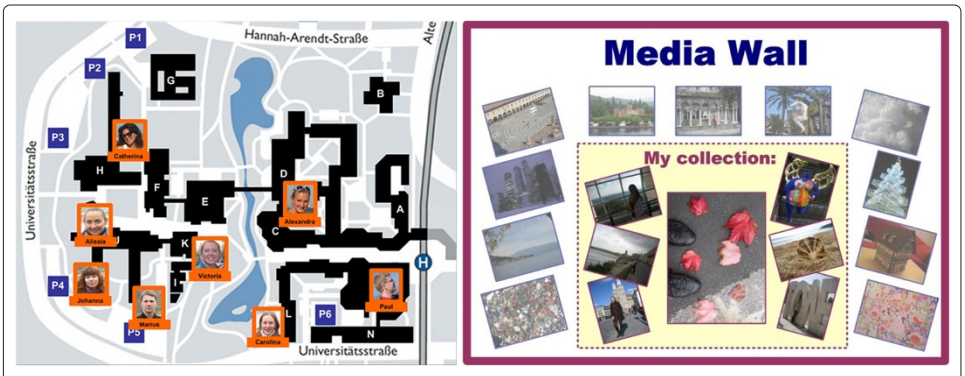

Figure 2 Online survey: applications. *Screenshots* of Friend Finder (left) and Media Wall (right).

Figure 3 Online survey: applications. *Screenshots* of Travel Planner (left) and Shopping Mall (right).

All four applications require mechanisms for deciding how to respond to trust-critical events, such as a passer-by approaching the display. Since all applications may disclose private information, such as a user's social network (FF) (see Figure 4 left), personal preferences (MW and SMD) or budget limitations (TP), they should be able to appropriately adapt to the surrounding social context in order to avoid potential privacy threats. Potential protection mechanisms include the migration of personal data from the public display to the user's mobile device, the hiding or masking of personal information (see Figure 4 middle) as well as offering these actions to the users via their mobile phones (see Figure 4 right). The corresponding scenarios in which users interact with a display while others pass or join will be in the following summarized under the common term "Spectator Scenario".

Besides people quickly passing the public display without taking notice of its content and people that may stop and watch, people may even engage in an interaction as well. In this case, the system does not only have to protect private information against unwanted disclosure, it should also account for strategies to accommodate the data and input originating from multiple users [2]. For example, several users may interact with the Shopping Mall display in parallel to exploring product information ("Space Scenario"). To accommodate the needs of multiple users, the size of the space allocated to particular users may be dynamically adapted. Alternatively, data may migrate to the user's mobile device. On the one hand, these strategies enable the simultaneous exploitation of a public display by

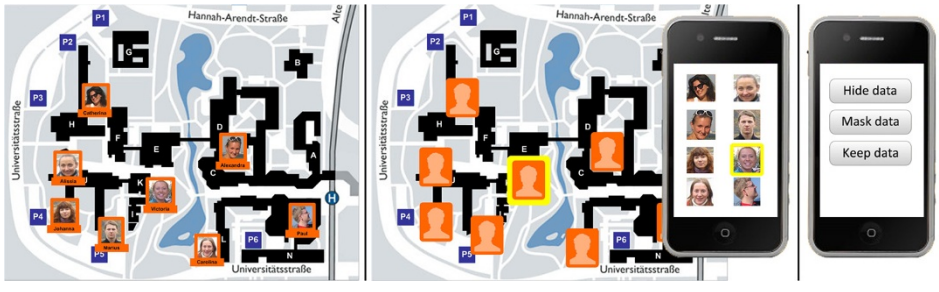

Figure 4 Possible display reactions (example). Examples of display reactions for Friend Finder (caused by privacy issues): Left: No reaction needed; Middle: Display Reaction: Mask private data on display and migrate data to the user's mobile phone; Right: Display Reaction: Present possible actions on the user's mobile phone.

multiple users. On the other hand, users might get irritated by the unsolicited customization. As a consequence, the system has to carefully balance the benefits and drawbacks of each action in order to come up with an optimized solution.

In addition, three of the applications (FF, MW and SMD) utilize additional sensors, such as cameras, to also offer proxemic interaction [2]. The corresponding scenarios for these applications will in the following be summarized under the term "Proximity Scenario". Whenever a user approaches the display, information relevant to him or her could be proactively presented on the screen. As soon as the user leaves the display, this information could be immediately removed again. On the one hand this feature offers great comfort. On the other hand, it limits the user's control over the system and might also be considered as opaque. Therefore, whenever a user approaches or leaves, the system could ask the user for confirmation via the user's mobile phone. Again this is a situation in which a system has to find a tradeoff between comfort of use, transparency and controllability to maximize the user's trust. The high dynamics in public places make this task even more difficult.

Online survey

The online survey was aimed at capturing the users' subjective assessment of display reactions in situations with changing social context. To this end, participants were shown videos clips of the four prototypes.

For each prototype, we recorded several short videos demonstrating scenarios in which a specific situation was given, the social context changed, and the display conducted a possible reaction. For example, the "Spectator Scenario" of the Friend Finder showed a single user interacting with the display in a public area (see Figure 5 left). The display recognized the arrival of an unknown person (change in social context) and masked the user's social network automatically (reaction) (see Figure 5 middle). Another video illustrated the same situation and context change, but a different display reaction: Instead of masking the data automatically, the data were blurred and the user was presented with various options on his mobile phone (see Figure 5 right).

Table 1 summarizes the recorded scenarios including possible situations which were represented by different settings of contextual variables, such as the social context and the privacy of the displayed content, and possible display reactions. Some scenarios were illustrated by different applications, in order to compare how people perceive the same

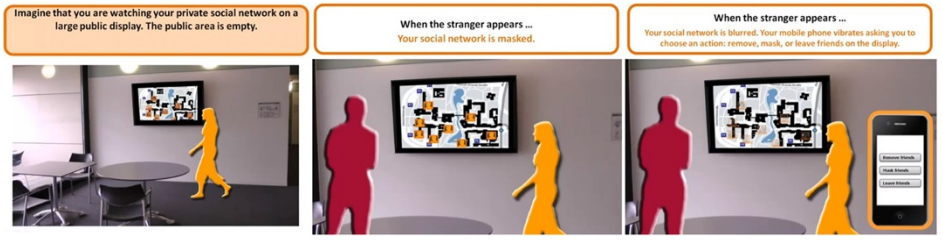

Figure 5 Online survey: screenshots of video (example). Screenshots of Video (Example) Screenshots of Video "Friend Finder - Approaching Stranger": Left: Single user interacting with private data on public display; Middle: Display Reaction: Mask private data; Right: Display Reaction: Blur private data and present possible actions on the user's mobile phone.

Table 1 Scenarios illustrated by videos: possible display reactions in different contextual combinations (situations)

Proximity scenario (privacy issues)			
User context	**Data context**	**Social context**	**Display reaction**
User approaching (FF, MW, SMD)	a) Private data b) Neutral data	a) User alone b) User not alone	a) Show user data automatically b) Ask via mobile device c) Do nothing
User leaving (FF, MW)	a) Private data b) Neutral data	a) User alone b) User not alone	a) Remove user data automatically b) Ask via mobile device c) Do nothing
Spectator scenario (privacy issues)			
User context	**Data context**	**Social context**	**Display reaction**
User interacts alone. (FF, MW)	a) Private data b) Neutral data	A person comes: a) Friend b) Acquaintance c) Stranger	a) Hide private data b) Mask private data c) Ask via mobile device d) Do nothing
User logged in (TP)	a) Private Data b) Neutral data	a) User alone b) User not alone	a) Show data on public display b) Show data on mobile device
Space scenario (space conflicts)			
User context	**Devices context**	**Social context**	**Display reaction**
User A interacts with the display. (SMD)	a) Mobile available b) not available	User B approaches the display: a) B is female b) B is male	a) Provide space for B, shrink data of A b) Provide space for B, move data of A to mobile c) Do nothing. B will wait

adaptations applied to different content. The applications illustrating the scenarios are indicated by the capital letters in the Scenario column.

All in all, four to six situations for each scenario (see Table 1 (Column 1–3)) and 22 situations in total were investigated. Considering two to four possible display reactions per situation (see Table 1 (Column 4)) this resulted in a total number of 68 recorded short videos. In order to reduce the time of the survey completion to about 10 minutes, we grouped the videos into six online surveys. Each survey contained about 8–12 videos. After an introductory page, the surveys provided a description of the used applications. Then, the user was confronted with the first scenario. The corresponding video illustrated the first situation and the first display reaction to the context change. After watching a video the user had to fill in a questionnaire. The questions aimed at capturing the participant's perception of the shown display reaction in terms of transparency, controllability, comfort of use, privacy, reliability, and trust. The questions represented statements which had to be ranked on a Likert scale from 1 ("absolutely disagree") to 5 ("absolutely agree"):

- Q1: I understood why the system was reacting in this way.
- Q2: I had control over the system.
- Q3: I found the system comfortable to use.
- Q4: The system protected my privacy in an appropriate way.
- Q5: I found the system reliable.
- Q6: I found the system trustworthy.

After presenting all possible display reactions for a particular situation, the users were asked to rank their preferences for it. The preferences also had to be estimated as statements of a 5-Likert scale. The statements emphasized the context of the given scenario, such as the presence of others or the privacy of data. For instance, a statement for the scenario of Friend Finder where the user was interacting with the display in a public area looked liked this:
"When I am watching my social network alone and a stranger approaches the display..."

- P1: I prefer to hide my data.
- P2: I prefer to mask my data.
- P3: I prefer no reaction from the display.
- P4: I prefer to be asked by my mobile phone.

Questions Q1-Q5 were aimed to collect empirical data to initialize the BN. Question Q6 was required to validate the network by checking whether the generated decisions matched the system action that created the highest user trust. Questions P1-P4 reflected subjective user preferences. In particular, we wanted to find out whether user preferences were in accord with the highest trust ratings and decisions generated by the BN. All in all, we collected evaluations of 85 online users and each video was seen by at least seven participants (Mean: 14). Supplying gender and age was not mandatory. The 73 users that provided demographic data included 24 women and 49 men. They were aged between 23 and 62 years, with an average age of 33.3 years.

Before using the data collected in these online studies for the initialization of the BN, we investigated whether the results of the online study were in line with the perception of users actually interacting with an adaptive system.

Live experiments

For the live experiments we picked two prototypes from the online studies that could be easily installed and tested in a university public area and that covered all scenarios related to privacy issues: Friend Finder and Travel Planner. The experiments were conducted individually in front of large displays that were installed in a university public area with a moderate circulation of researchers, students, and visitors. That is, the study participants were not just watching a video, but actively experiencing an application by interacting with it (see Figure 6). In each application, the users were confronted with a variety of trust-critical situations, such as the approach of another person, while they were viewing private information. As in the online survey, the users had to assess potential system reactions to these events. Hence, the procedure and the questions used in the live study reproduced the web-based study as closely as possible to control for any unintended side effects. Both prototypes were tested between groups: Every participant evaluated either Friend Finder or Travel Planner. Altogether, 36 people took part in the live experiments (FF: 16; TP: 20). Among them there were 16 female and 20 male persons, aged from 20 to 36 (mean 28.3).

The results of the live experiment generally matched the results obtained in the online study. Both experiments yielded similar distributions of user rankings of transparency, controllability, comfort of use, privacy and reliability. Moreover, we found similar distributions of trust and user preferences. Figure 7 shows the distributions of the user ratings for one particular situation in Friend Finder, namely the automated removal of data from a public display as soon as the user leaves. Most distributions are skewed to the right

Figure 6 Life study: applications. Prototypes of Friend Finder (left) and Travel Planner (right).

reflecting positive user ratings both for the online and the live condition. Overall, the ratings in the online and in the live experiments show a similar trend. Similar observations could be made for the Travel Finder application.

Interestingly, the participants gave higher trust ratings in the live condition than in the online condition. For Friend Finder, a two-tailed t-test showed that the differences were significant with mean values of 3.66 (STD = 1.50) and 3.08 (STD = 1.27) in Friend Finder ($t(238) = -2.46$, $p < 0.02$) and mean values of 3.98 (STD = 0.84) and 3.14 (STD = 1.40) in Travel Planner ($t(248) = 5.86$, $p < 0.001$). Apparently, the fact that the participants had the chance to interact with the system had influenced their ratings positively.

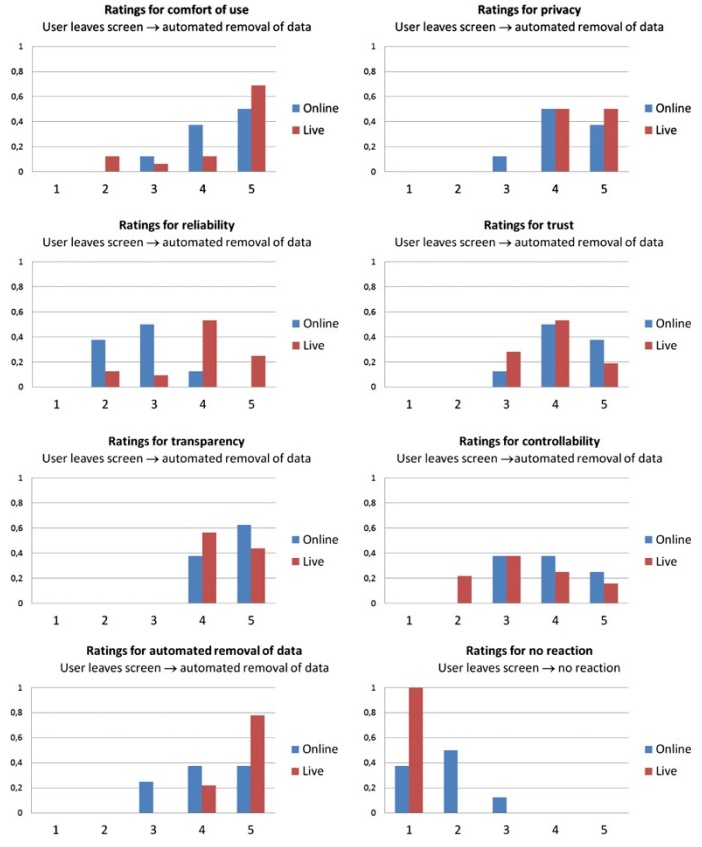

Figure 7 Distributions of ratings. Distributions of ratings in the live and online setting of Friend Finder.

However, the important result for us was to see that apart from a few exceptions the ranking of system reactions in the online experiments was in line with that obtained in the live experiments. Independently of whether users had to evaluate the online or the live setting, participants preferred the same system reaction. In the case of Travel Planner, this system reaction got significantly higher rankings than any other system reaction in all four situations for the live condition and in three out of four situations in the online condition. For example, people preferred private information to be displayed on a mobile phone in the presence of other people. Accordingly, performing a two-tailed paired t-test, we found that "Show on Mobile Device" got significantly higher ratings than "Show on Display" with mean values of 3.44 and 1.44 in the online scenario ($t(8) = -4.24, p < 0.01$) and mean values of 4.75 and 1.95 in the live scenario ($t(19) = -7.10, p < 0.001$). This system reaction also got the highest trust value in both conditions (albeit not significant). Similar observations could be made for Friend Finder even though less distinct. Again participants preferred the same system reaction in both conditions. Apart from two cases, the system reactions the users trusted most in the live setting matched the system reactions the users trusted most in the online setting. Overall, the results indicate that the online study provides realistic input for the initialization of the BN despite a few discrepancies.

Results and discussion

Initialization and validation of the Bayesian network

As the next step, the BN was populated with the empirically obtained data. For the creation of conditional probability tables, we employed the GeNIe (see http://genie.sis.pitt.edu) built-in algorithm for learning Bayesian Networks.

Overall, we constructed four different networks from the data received in the online studies, one for each row in Table 1, with the first two rows being combined into one network. While the basic structure was shared by all networks and was similar to the example network shown in Figure 1, each had different context nodes and possible adaptations, based on the respective scenario. For example, the first of the Spectator scenarios required one context node with two contexts and another one with three, as well as four different system reactions in the decision node. On the other hand, the second Spectator scenario required two context nodes with two contexts each and only two system reactions.

The quantitative data obtained in the evaluations enabled us to derive distributions for each trust dimension related to each contextual combination. For each trust dimension, we modeled the probability distribution for all combinations of context and display reaction in the BN after the data taken from both studies. The probability distributions for other node combinations were derived from the study described in Section 'Modeling user trust through trust dimensions'. In particular, dependency information from the earlier study was used to model (1) the relationship between the trust dimensions and user trust and (2) the relationship between the user's trust disposition and user trust.

Since knowledge about the user's trust disposition is hard to acquire in an ubiquitous display environment, it does not make sense to assume detailed knowledge about the trust disposition of a particular user. Rather, we created user trust profiles from empirical data acquired in the population that was of relevance to our application domain. That is the reasoning process of the BN did not start from "hard" evidence, but from distributions for user trust disposition. These distributions reflect the trust disposition of our users. However, data for other user groups can be easily integrated into the BN by replacing the

corresponding distributions in the BN. An interesting resource to explore is the work by Westin who conducted a large number of studies to determine the percentage of people with certain levels of distrust or privacy concerns, see the paper by Kumaraguru and Cranor [34] for a survey of these studies.

Figure 8 shows an example of probability distributions for *Initial*, *Interaction-Based* and *User Trust* for a selected system reaction, assuming a very low *Trust Disposition* (blue) in one case and a very high one (red) in the other. As can be seen, we chose to model the distributions with a (skewed) bell curve, with a bias towards the lower end of trust scale. The utility function from *User Trust* to *Utility* maps "very low" to 1, "low" to 2 and so on, resulting into an overall trust value of 2.03 for the very low *Trust Disposition* and 3.34 for the very high one.

Although we also asked for the users' preferred display reaction for each context combination as well as their trust in the display reaction presented for each such combination, it should be noted that this information was not used to model the networks. As mentioned above, we only used the users' rankings of the different trust dimensions for each combination of context and display reaction. Instead, the data on user trust ratings and user preferences was used to validate the decisions generated by the BN. In this vein, we were able to check to what extent the relationship between trust and trust dimensions (see Section 'Modeling user trust through trust dimensions') was application-independent. For the validation of each created network, we generated decisions for all contextual combinations. These decisions were compared to the results from the user studies. In particular, we compared the decision obtained from the BN with the user's ratings of system actions and their own trust.

The contextual combinations were set by entering appropriate evidence into the matching context nodes. For example, for a specific situation in the Proximity scenario, the evidence would be set to "Privacy of Data → Private", "Movement → Arriving" and "Others Present → Yes". We only used "hard" evidence at this point, i.e. the corresponding values were set to 100%. For each of these combinations, the display reaction with the highest utility rating (which was directly based on the computed value of User Trust) was chosen as the system's decision.

First, we compared these generated reactions with those preferred by the participants in the studies. For each context combination, we selected the display reaction that received the highest average score in the surveys. When comparing the display reactions preferred by the users with those generated by the respective network, we found that they matched in 21 out of the 22 situations (95.45%). Second, we compared the generated

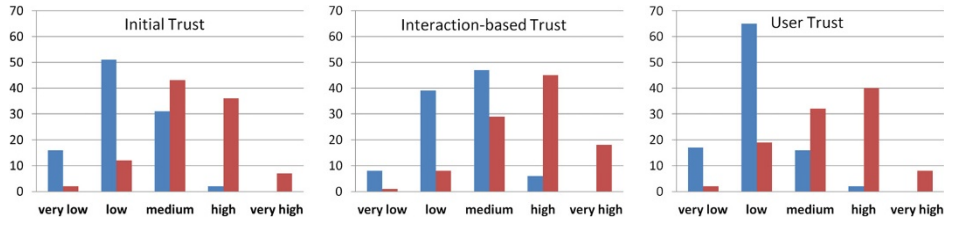

Figure 8 Impact of trust disposition on initial trust, interaction-based trust and overall user trust. Probability distributions for very low (blue) and very high (red) Trust Disposition.

reactions with those that received the highest trust in the studies. They matched in all 22 situations.

These results show that the BN delivers good accuracy in the generated decisions. As an example from the results, let us take a look at the BN for the first Spectator scenario (the third row in Table 1) and its eight context combinations. Table 2 shows the different situations along with the respective display reactions which received the highest trust from the study participants. As mentioned above, these reactions matched those generated by the BN. For the preferred reactions, there was one mismatch. For the first situation (Data is private, Spectator is Friend), the study participants indicated a preference for "Hide private data" (even though they gave "Ask via mobile device" the highest trust value). Thus, the participants' trust ratings were in line with those determined by the BN while the favored reactions of the participants and the most appropriate reactions determined by the BN differed. It is worth mentioning that only two out of four possible system reactions for this scenario were among those favored (both preference- and trust-wise) by the study participants. As another, more diverse example, Table 3 shows the results for the Proximity scenario (the first two rows in Table 1).

However, this form of validation only validated our model within the same population and also the generated decisions were compared to average and not individual preferences. Thus we were also interested in how its generated decisions matched with the preferences of "new" and individual users. Therefore we also performed a leave-one-person-out cross-validation of our networks: For each network, we performed n validations, where n is the number of users that participated in the respective study for the scenario(s) in that network. In each of the n validations, the network was initialized with the data from (n - 1) users and then validated with the missing user. The final result for each network was the average of all n validations. The comparison of user preferences with the adaptations generated by the networks now resulted in 15.84 out of 22 matching situations (72.00%). The comparison with the highest-trust adaptations now matched in 17.26 out of 22 (78.45%). These results are in line with the percentages of study participants who individually preferred the system reaction which received the highest average score, 78.80% for preference and 82.58% for trust.

Finally, we were also interested in how the approach would perform in non-ideal situations, thus leveraging the BN's strength of decision-making under uncertainty. To test whether it still would be able to generate appropriate decisions in such situations, we simulated the following two problems (again using the leave-one-person-out cross-validation for all networks, as described above):

Table 2 Study results for display reactions in the first Spectator scenario

Context	Reaction with highest user ratings for trust
Data is private, Spectator is Friend	Ask via mobile device
Data is private, Spectator is Acquaintance	Hide private data
Data is private, Spectator is Stranger	Hide private data
Data is not private, Spectator is Friend	Ask via mobile device
Data is not private, Spectator is Acquaintance	Ask via mobile device
Data is not private, Spectator is Stranger	Ask via mobile device

Table 3 Study results for display reactions in the proximity scenarios

Context	Reaction with highest user ratings for trust
User is arriving, Data is private, User is alone	Ask via mobile device
User is arriving, Data is private, User is not alone	Ask via mobile device
User is arriving, Data is not private, User is alone	Do nothing
User is arriving, Data is not private, User is not alone	Do nothing
User is leaving, Data is private, User is alone	Remove user data automatically
User is leaving, Data is private, User is not alone	Remove user data automatically
User is leaving, Data is not private, User is alone	Remove user data automatically
User is leaving, Data is not private, User is not alone	Remove user data automatically

- No empirical data for certain context combinations: Especially for complex applications with many different contexts and system reactions, performing studies to obtain empirical data for each single situation might not be feasible. If a certain context combination (such as the transparency of a system action in a given situation) can not be initialized with empirical data, another solution, such as a uniform distribution, has to be chosen. Figure 9 shows the matching rates for trust and preference for an increasing number of uninitialized context combinations, using a uniform distribution when necessary.
- No context data for certain situations: If it is not possible to determine the context for a certain situation (e.g. the face-tracking sensor is not providing any data and thus the system cannot determine whether the user is alone or not) then only insufficient evidence can be entered into the network which will of course impact on the decision-making process. Figure 10 shows the matching rates for trust and preference for an increasing number of context nodes without evidence, using a uniform distribution instead of concrete evidence when necessary.

It is important to emphasize that a solution that results into the highest user trust is not necessarily the solution that the user actually prefers the most. The results of our online and live study support this fact: distributions of user preferences did not always reflect distributions of trust. From the comments of the live study participants, we found that the

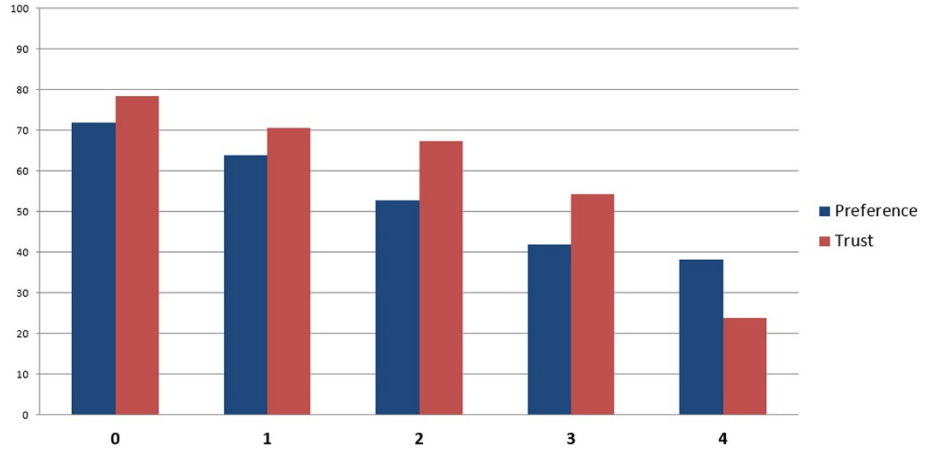

Figure 9 Matching rates for preference and trust. Increasing number of uninitialized context combinations.

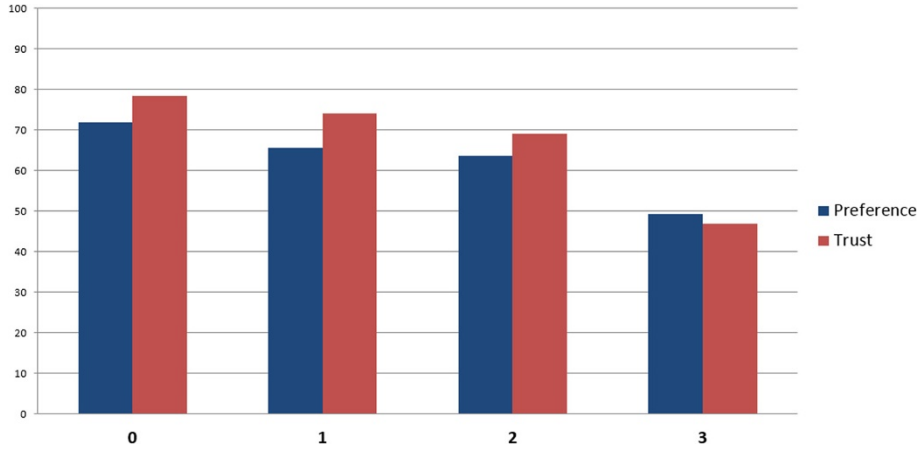

Figure 10 Matching rates for preference and trust. Increasing number of context nodes without evidence.

feeling of trust often depends on the person's ability to explain the system reaction and agree with it. For example, when a person comes closer to the display, it seems logical and expected that the display does not show any reaction. We learn this behavior from everyday life: Fixtures, even electronic ones, usually do not react. Apparently, the option "Do nothing" therefore received highest trust rankings. However, the most understandable reaction might not be the most preferred or the most convenient one. Here, the more creative (but less predictable) reactions were favored. For example, the users found it smart and convenient that the display noticed them and proposed via a mobile device to show their data on the large screen. Thus, the "Ask via mobile device" option was chosen as a preference.

Conclusion

The ability of ubiquitous display environments to dynamically adapt to changing social contexts comes with a lot of benefits. At the same time, it raises issues with user trust. In this paper we delineated a decision-theoretic mechanism to trust management based on Bayesian Networks that assesses user trust through trust dimensions, monitors it during the interaction and chooses appropriate measures to ensure user trust in critical situations. Using empirical data collected in online and live experiments, we demonstrated how the network was initialized and cross-validated. The evaluation revealed that the approach succeeded in determining system actions that obtained the highest value for trustworthiness from users. An interesting result obtained by the empirical validation of the Bayesian Network was the mismatch between the system reactions users *preferred* most and the system reactions resulting in the highest amount of user *trust*. A creative solution is more likely to impress users. At the same time, a surprising system response may have a negative impact on user trust. Future work should aim at gaining a deeper insight into this question, investigating which factor - trust or subjective preference - drives the user's ultimate choice of a system reaction. One limitation of our live studies is the homogeneity of the participants, since most of them were rather young students from the engineering sciences. Also, all interactive prototypes were deployed in a university setting. While we already reached a larger demographic variety with our online

studies, future work should also extend the live studies in a similar fashion. So far, we do not exploit any knowledge about user-specific attitudes during the selection of system actions. Depending on their trust disposition, users might, however, favor different system responses. For example, users that tend to distrust technical systems might give more importance to a high level of control than to a high level of comfort. In our future work, we will investigate how to improve the accuracy of the user trust model by incorporating knowledge about user-specific attitudes. A promising approach might be to distinguish between different categories of users, such as privacy fundamentalists, pragmatics and unconcerned users, following Westin's privacy indices [34].

Unlike most earlier work, we focused on the challenge of modeling experience-based user trust. Since experience-based user trust refers to a psychological user state, it is hard to measure directly. The approach presented in the paper was based on the assumption that user trust may be assessed through trust dimensions that refer to trust-enhancing system properties. While the estimation based on trust dimensions gave promising results, more complex scenarios might require the consideration of additional trust indicators. For our future work, we plan two extensions. First of all, we aim to derive user trust not only from its causes, i.e. system properties, but also from its effects, i.e. observable user behaviors. In our earlier work [35], we investigated various physiological patterns as an indicator of trust felt by a user when viewing web pages. As a next step, we will concentrate on the identification of behavioral factors from which experience-based user trust might be derived in ubiquitous display environments, such as the time spent in front of a public display or the number of downloads. Secondly, we intend to extend the Bayesian Network to a Dynamic Bayesian Network in order to consider how user trust felt at a particular point in time depends on user trust experienced at an earlier point in time. While we presented the topology of such a network in [26], it has not yet been grounded and evaluated by user data.

Competing interests

The authors declare that they have no competing interests.

Authors' contributions

MW took over the lead of the design and the implementation of the trust management system based on Bayesian Networks. He also performed the statistical analysis for the online survey and the live studies. SH provided support in the implementation and the evaluation of the trust management approach. EK designed and implemented the scenarios which formed the basis of the evaluation. She was also involved in the conduction of the user studies. EA supervised the research. Also the concept of the decision-theoretic approach to trust management goes back to ideas from her. Finally, she acquired the funding from the German Science Foundation (DFG) for conducting the research. All authors collaborated in drafting and revising the manuscript and all authors read and approved the final manuscript.

Acknowledgments

This research is co-funded by OC-Trust (FOR 1085) of the German Research Foundation (DFG). The core of our implementation is based on the SMILE reasoning engine and the network shown in this paper was created using the GeNIe modeling environment. Both SMILE and GeNIe are developed and contributed to the community by the Decision Systems Laboratory, University of Pittsburgh and available at http://genie.sis.pitt.edu/.

Received: 7 October 2013 Accepted: 14 January 2014
Published: 20 May 2014

References

1. Rothrock L, Koubek R, Fuchs F, Haas M, Salvendy G (2002) Review and reappraisal of adaptive interfaces: toward biologically inspired paradigms. Theor Issues Ergon Sci 3: 47–84
2. Greenberg S, Marquardt N, Ballendat T, Diaz-Marino R, Wang M (2011) Proxemic interactions: the new ubicomp? ACM Interact 18(1): 42–50
3. Müller J, Exeler J, Buzeck M, Krüger A (2009) ReflectiveSigns: digital signs that adapt to audience attention In: Proceedings of 7th International Conference on Pervasive Computing. Springer, Berlin, Heidelberg, pp 17–24

4. Röcker C, Hinske S, Magerkurth C (2007) Intelligent privacy support for large public displays In: Proceedings of Human-Computer Interaction International 2007 (HCII'07). Springer, Berlin, Heidelberg, Germany
5. Yan Z, Holtmanns S (2008) Trust modeling and management: from social trust to digital trust. IGI Global, Hershey
6. Graham C, Cheverst K (2004) Guides, locals, chaperones, buddies and captains: managing trust through interaction paradigms In: 3rd Workshop 'HCI on Mobile Guides' at the sixth international symposium on human computer interaction with mobile devices and services. ACM, New York, pp 227–236
7. Glass A, McGuinness DL, Wolverton M (2008) Toward establishing trust in adaptive agents In: Proceedings of the 13th international conference on Intelligent User Interfaces (IUI '08). ACM, New York, pp 227–236
8. Castelfranchi C, Falcone R (2010) Trust theory: a socio-cognitive and computational model. Wiley, Hoboken
9. Marsh S (1992) Trust in distributed artificial intelligence. In: Castelfranchi C, Werner E (eds) Artificial social systems, 4th European workshop on Modelling Autonomous Agents in a Multi-Agent World, MAAMAW '92, S. Martino al Cimino, Italy, July 29–31, 1992, selected papers. Lecture notes in computer science, vol. 830. Springer, Berlin, Heidelberg, pp 94–112
10. Wang Y, Vassileva J (2003) Bayesian network trust model in peer-to-peer networks. In: Moro G, Sartori C, Singh MP (eds) Agents and peer-to-peer computing, second international workshop, AP2PC 2003, Melbourne, Australia, July 14, 2003, Revised and invited papers. Lecture notes in computer science, vol. 2872. Springer, Berlin, Heidelberg, pp 23–34
11. Yu B, Singh MP (2002) An evidential model of distributed reputation management In: Proceedings of the first international joint conference on Autonomous Agents and Multiagent Systems: Part 1. AAMAS '02. ACM, New York, pp 294–301
12. Vogiatzis G, MacGillivray I, Chli M (2010) A probabilistic model for trust and reputation. In: van der Hoek W, Kaminka GA, Lespérance Y, Luck M, Sen S (eds) 9th international conference on Autonomous Agents and Multiagent Systems (AAMAS 2010), Toronto, Canada, May 10–14, 2010, Volume 1–3. IFAAMAS, Richland, pp 225–232
13. Jøsang A, Hayward R, Pope S (2006) Trust network analysis with subjective logic. In: Estivill-Castro V, Dobbie G (eds) Computer science 2006, Twenty-nineth Australasian Computer Science Conference (ACSC2006), Hobart, Tasmania, Australia, January 16–19 2006. CRPIT, vol. 48. Australian Computer Society, Darlinghurst, pp 85–94
14. Sankaranarayanan V, Chandrasekaran M, Upadhyaya SJ (2007) Towards modeling trust based decisions: a game theoretic approach. In: Biskup J, Lopez J (eds) Computer Security - ESORICS 2007, 12th European Symposium On Research In Computer Security, Dresden, Germany, September 24–26, 2007, Proceedings. Lecture Notes in Computer Science, vol. 4734. Springer, Berlin, Heidelberg, pp 485–500
15. Burnett C, Norman TJ, Sycara KP (2011) Trust decision-making in multi-agent systems. In: Walsh T (ed) IJCAI 2011, Proceedings of the 22nd International Joint Conference on Artificial Intelligence, Barcelona, Catalonia, Spain, July 16–22, 2011. IJCAI/AAAI, Palo Alto, California, USA, pp 115–120
16. Sherchan W, Nepal S, Paris C (2013) A survey of trust in social networks. ACM Comput Surv 45(4): 47:1-47:33
17. Bhuiyan T, Xu Y, Jøsang A (2010) A review of trust in online social networks to explore new research agenda. In: Arabnia HR, Clincy VA, Lu J, Marsh A, Solo AMG (eds) Proceedings of the 2010 International Conference on Internet Computing, ICOMP 2010, July 12–15, 2010, Las Vegas Nevada, USA. CSREA Press, Las Vegas, pp 123–128
18. Adali S, Escriva R, Goldberg MK, Hayvanovych M, Magdon-Ismail M, Szymanski BK, Wallace WA, Williams GT (2010) Measuring behavioral trust in social networks. In: Yang CC, Zeng D, Wang K, Sanfilippo A, Tsang HH, Day M-Y, Glässer U, Brantingham PL, Chen H (eds) IEEE international conference on Intelligence and Security Informatics, ISI 2010, Vancouver, BC, Canada, May 23–26, 2010, Proceedings. IEEE, s.l., Washington, DC, USA, pp 150–152
19. Ivanov I, Vajda P, Korshunov P, Ebrahimi T (2013) Comparative study of trust modeling for automatic landmark tagging. IEEE Trans Inf Forensics Secur 8(6): 911–923
20. Grandison T, Sloman M (2000) A survey of trust in internet applications. IEEE Commun Surv Tutorials 3(4): 2–16
21. Kini A, Choobineh J (1998) Trust in electronic commerce: definition and theoretical considerations In: Proc. of the Hawaii international conference on system sciences, vol. 31. IEEE Computer Society, Washington, DC, USA, pp 51–61
22. Tschannen-Moran M, Hoy WK (2000) A multidisciplinary analysis of the nature, meaning, and measurement of trust. Rev Educ Res 70(4): 547
23. Yan Z, Zhang P, Deng RH (2012) Truberepec: a trust-behavior-based reputation and recommender system for mobile applications. Pers Ubiquitous Comput 16(5): 485–506
24. Cao H, Olivier P, Jackson D (2008) Enhancing privacy in public spaces through crossmodal displays. Soc Sci Comput Rev 26(1): 87–102
25. Bee K, Hammer S, Pratsch C, Andre E (2012) The automatic trust management of self-adaptive multi-display environments In: Trustworthy ubiquitous computing. Atlantis ambient and pervasive intelligence, vol. 6. Atlantis Press, s.l., Paris, France, pp 3–20
26. Kurdyukova E, André E, Leichtenstern K (2012) Trust management of ubiquitous multi-display environments. In: Krueger A, Kuflik T (eds) Ubiquitous display environments. Cognitive technologies. Springer, Berlin, Heidelberg, pp 177–193
27. Lumsden J (2009) Triggering Trust: to what extent does the question influence the answer when evaluating the perceived importance of trust triggers? In: Proceedings of the 2009 British Computer Society Conference on Human-Computer Interaction (BCS HCI '09). British Computer Society, Swinton, pp 214–223
28. Russell SJ, Norvig P (2003) Artificial intelligence: a modern approach, 2nd international edn.. Prentice Hall, Upper Saddle River
29. Müller J, Krüger A, Kuflik T (2007) Maximizing the utility of situated public displays In: Proceedings of the 11th international conference on User Modeling (UM '07). Springer, Berlin, Heidelberg, pp 395–399
30. Peltonen P, Salovaara A, Jacucci G, Ilmonen T, Ardito C, Saarikko P, Batra V (2007) Extending large-scale event participation with user-created mobile media on a public display In: Proceedings of the 6th international conference on mobile and ubiquitous multimedia. ACM, New York, pp 131–138
31. Alt F, Balz M, Kristes S, Shirazi AS, Mennenöh J, Schmidt A, Schröder H, Goedicke M (2009) Adaptive user profiles in pervasive advertising environments In: Proceedings of the European conference on Ambient Intelligence (Aml '09). Springer, Berlin, Heidelberg, pp 276–286

32. Churchill EF, Nelson L, Denoue L, Girgensohn A (2003) The plasma poster network: posting multimedia content in public places In: In Proceedings of the IFIP International Conference on Human-Computer Interaction (INTERACT 2003). IOS Press, Amsterdam, The Netherlands, pp 599–606
33. Kurdyukova E, Bee K, André E (2011) Friend or foe? Relationship-based adaptation on public displays In: Proceedings of the second international conference on Ambient Intelligence (Aml'11). Springer, Berlin, Heidelberg, pp 228–237
34. Kumaraguru P, Cranor LF (2005) Privacy indexes: a survey of westin's studies. Technical Report CMU-ISRI-5-138, Technical Report, Institute for Software Research International (ISRI), Carnegie Mellon University
35. Leichtenstern K, Bee N, André E, Berkmüller U, Wagner J (2011) Physiological measurement of trust-related behavior in trust-neutral and trust-critical situations. In: Wakeman I, Gudes E, Jensen CD, Crampton J (eds) Trust Management V, 5th IFIP WG 11.11 international conference, IFIPTM 2011, Copenhagen, Denmark, June 29-July 1, 2011, proceedings. IFIP advances in information and communication technology, vol. 358. Springer, Berlin, Heidelberg, pp 165–172

doi:10.1186/2196-064X-1-6
Cite this article as: Wißner *et al.*: Trust-based Decision-making for the Adaptation of Public Displays in Changing Social Contexts. *Journal of Trust Management* 2014 **1**:6.