

Trust-Based Decision-Making for Energy-Aware Device Management

Stephan Hammer, Michael Wißner, and Elisabeth André

Human Centered Multimedia, Augsburg University
Universitaetsstr. 6a, 86159 Augsburg, Germany
{hammer, wissner, andre}@hcm-lab.de
<http://www.hcm-lab.de>

Abstract. Smart energy systems are able to support users in saving energy by controlling devices, such as lights or displays, depending on context information, such as the brightness in a room or the presence of users. However, proactive decisions should also match the users' preferences to maintain users' trust in the system. Wrong decisions could make them abandon the system. In this paper, a trust-based model, called User Trust Model (UTM), for automatic decision-making is proposed, which is based on Bayesian Networks. The UTM's construction, the initialization with empirical data gathered in an online survey, and its integration in an office setting are described. Furthermore, the results of a user study investigating users' experience and acceptance are presented.

1 Introduction

Reducing energy consumption has been a major concern for more than four decades, and many approaches that were aimed to support sustainability were developed during this time [1,2]. Some tried to improve people's environmental awareness by providing detailed feedback on their energy usage [3]. Others tried to persuade people to reduce their energy demand by exploiting social factors and utilizing, for example, cooperative pervasive games [4].

A number of energy management systems allow users to control devices, such as displays or lights, remotely or by setting up time tables. Furthermore, attempts have been made to adjust the energy consumption implicitly based on various context information that describes the users' and the system's surroundings [5]. For example, displays or lights, can be switched off if they are not needed. On the one hand, a system that autonomously performs energy saving actions contributes to the users' convenience. On the other hand, proactive system actions are not always understood by users and limit their control over the system. As a consequence, users might lose trust in such a system and give up using it.

For illustration, let us assume a lamp is burning in the user's office even though daylight suffices for performing the work. How should an energy management system react in such a situation? Should it trust the users are aware of their energy consumption and will take necessary actions themselves? Should it switch off the light autonomously? Or should it ask the user for permission via messages presented on the user's display or mobile phone?

In the first case, the system would leave the responsibility for energy reduction with the users, and there would be the risk that users do not see any benefit in the energy management system. The second approach bears the danger that the users do not understand the rationale behind the system's behavior and perceive it as not sufficiently self-explanatory or even randomly acting. In the last case, the system's behavior might appear transparent. However, users might nevertheless be upset because permanent and obtrusive messages interrupt their workflow. The example illustrates that a system needs to carefully balance the benefits and drawbacks of possible actions so as not to risk the users losing trust in its workings.

In this paper, a decision-theoretic approach to a trust management system for smart and proactive environments based on Bayesian Networks, the User Trust Model (UTM), is presented. It assesses users' trust in a system, monitors it over time, and applies appropriate system reactions to maintain users' trust in critical situations [6]. Section 2 discusses prior work in modelling trust considering work done in the area of agent-based modeling, social media and adaptive and personalized systems. After that, the UTM's construction, its integration in an office setting, and the initialization with empirical data are described. Section 5 presents a user study investigating the users' experience with and acceptance of the system.

2 Related Work

Since trust is a social phenomenon, it seems to be a promising 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 [7] 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 [8], Dempster-Shafer Theory [9], Hidden-Markov Models [10], Belief Models [11], Fuzzy models [12], game-theoretic approaches [13] or decision trees [14]. There is empirical evidence that the performance of agent-based societies may be improved by incorporating trust models.

In contrast to the approaches above, work in the area of social media aims to model trust between human users, see [15] or [16] 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. For example, Adali et al. [17] assess trust between two users based on the amount of conversation and the propagation of messages within Twitter. Other approaches derive trust that is given to users from community-based reputation or social feedback (e.g. [18]).

Our research focuses on trust which users experience when interacting with a software system. A system may be robust and secure, but nevertheless be perceived as little trustworthy, for example, because its behavior appears little transparent or hard to control. Following the terminology by Castelfranchi and Falcone [12], our work focuses on the affective forms of trust that are based on the user's appraisal mechanisms. That is we aim at the development of computational trust models that capture how a system - in this paper a smart environment for energy saving - is perceived by a user who is confronted with it.

Computational models that assess trust felt by a user while interacting with a system are rare. There is a large amount of work that aims to identify factors that impact user trust. For example, Glass and colleagues [19] research trust-enhancing factors for adaptive and personalized applications. However, they do not implement a model of the user's trust into an adaptive and personalized system based on these factors. Yan and colleagues' [6] model captures trust users experience when interacting with mobile applications. In order to present users with recommendations that help increase users' trust, they identified various 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 an adaptive and personalized mobile application to control the selection of system actions during an interaction with the user.

3 Modelling User Trust

We have chosen to model the users' feelings of trust by means of Bayesian Networks. A Bayesian Network (BN) is a directed, acyclic graph in which the nodes represent random variables while the links connecting nodes describe the direct influence in terms of conditional probabilities [20]. The basic idea is to derive user trust from so-called trust dimensions, such as *Comfort of Use*, *Transparency*, *Controllability*, *Privacy*, *Reliability*, *Security*, *Credibility*, and *Seriousness*. The trust dimensions are based on earlier user studies [21] which showed significant positive correlations between these trust dimensions and user trust. BNs were chosen because they meet requirements that should be accounted by models that are aimed to assess users' trust towards computer systems very well:

Trust as a Subjective Concept: Users respond individually to one and the same event. While some might find it critical if a system acts autonomously, others might not care. In a BN the system's uncertain belief about user's trust can be represented by a probability distribution over different levels of trust.

Trust as a Non-Deterministic Concept: The connection between events and trust is inherently non-deterministic. For example, we cannot always be sure

that the user notices a critical event at all. Users may also consider a critical event as rather harmless. BNs allow us to make predictions based on conditional probabilities that model how likely the value of a 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.

Trust as a Multifaceted Concept: Computational models should be able to represent the relative contribution of different trust dimensions to the assessment of trust and should help predict user's trust based on dimensions, such as the perceived transparency of a system. With BNs the modelling of relationships between trust and its dimensions is rather intuitive. For example, it is rather straightforward to model that reduced transparency leads to a decrease of trust. In the BN in Fig. 1 each trust dimension is represented by a specific node. Since exact probabilities are difficult to determine, the conditional probabilities were derived from empirical data collected in an online survey, see Section 4.1.

Trust as a Dynamic Concept: Trust depends on experience and changes over time. According to Lumsden [22], *User Trust* is affected by *Initial Trust* and *Interaction-Based Trust*. Initial 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.

In Fig. 1, a BN for modeling trust in the smart energy system is shown. To describe the determinants of *Initial Trust*, we introduce nodes for *Security*, *Seriousness* and *Credibility*. *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. Furthermore, we introduce a node for *Interaction-Based Trust*, which depends on *Quality of Interaction* and *Reliability*. The *Quality of Interaction* is characterized by *Transparency*, *Controllability* and *Comfort of Use*. Both the establishment of *Initial Trust* and *Interaction-Based Trust* are influenced by the users' *Trust Disposition* which is characterized by their *Competence* and general *Confidence* towards technical systems. The trust dimensions cannot be observed directly, but may be inferred from observable context variables that depend on the specific system. For example, the BN that decides on the reactions related to the light in an office considers the current *User* state, the *Social Context*, and the *Luminance Outside*, see Fig. 1. Knowing the contextual situation, the BN can estimate the impact of certain system reactions on the trust dimensions and thus on the user's trust. *Controllability*, for example, could be negatively affected if the system switches the light on and off autonomously.

In order to use the BN for decision-making, it was extended to an influence diagram by adding the decision node *System Action*, representing all actions the system could do to react on context changes, such as "Switch the light on automatically" if the "User is arriving", and a *Utility* node that 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

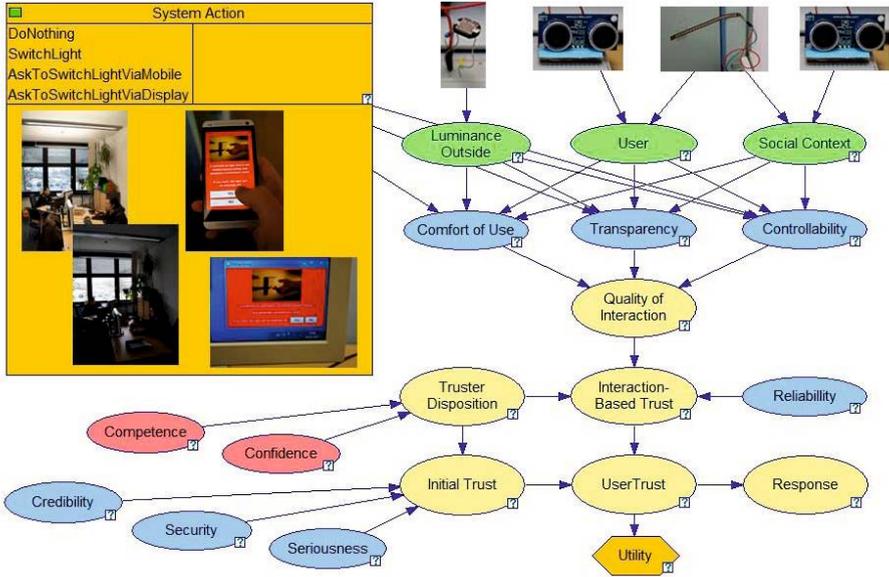


Fig. 1. User Trust Model (Light): green: Context Information (Sensors: Light, Ultrasonic, Flex-Sensor); red: User Traits; blue: Trust Dimensions; orange: Decision Nodes (System-Actions and Utility-Node)

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.

4 Building a Smart Office

In the following, we demonstrate how the User Trust Model (UTM) guides decision-making in an energy-aware device management system that controls the displays and the light in an office occupied by several people. For each type of device, a Bayesian Network (BN) was constructed and integrated using the GeNIe modeling environment and the SMILE reasoning engine¹. Fig. 1 presented the BN for operating the light. Whether and which action the system takes to control the light basically depends on environmental information, the user's presence and the social context. In case the system recognizes a situation in which the light might be adjusted, it may perform the corresponding action autonomously or ask the user for permission via the mobile phone or via the display of the user's PC. In order not to risk disturbing the user, the UTM might even decide not to do anything even if there was an action that could save energy. The BN for the display has a similar structure. However, it relies on a more fine-grained representation of the user's current activity to distinguish, for example, whether

¹ <http://genie.sis.pitt.edu/>

Table 1. Possible system reactions in different contextual combinations

Device	User	Situation		System Reaction
		Social Context	Luminance Outside	
Display	1) WorkingAtPC	-	-	a) Switch on Display
	2) IdleAtDesk	-	-	b) Ask To Switch on Display
	3) AwayFromDesk	-	-	Via Mobile Phone
	4) OutOfRoom	-	-	c) Do Nothing
Light	1) Arriving	1) Coworker	1) Dark	a) Switch off Light
	2) Present	Present	2) Bright	b) Ask Via Mobile Phone
	3) Leaving	2) Coworker Away		c) Ask Via Display d) Do Nothing

the user is sitting in front of a computer and working with it or engaged in other activities, such as reading a book. An overview on possible system actions and the utilized context information in both BNs is given in Table 1.

The data needed to recognize the context information for both BNs was gathered by Arduino-Sensors² that were distributed in the office. For example, we utilized light sensors to measure the outdoor luminance and ultrasonic sensors attached to the displays to detect the presence of persons. The control of the devices was conducted via a HomeMatic³ system and remote controlled plugs.

4.1 Gathering Empirical Data (Online Survey)

In order to be able to generate decisions, the BNs had to be initialized with data. Both for the light and the display, we collected data in a web-based survey. In both surveys, participants were confronted with textual descriptions of typical situations during daily office routines. For each situation, possible system actions were proposed for the respective device that were supposed to improve the energy consumption of the users. Table 1 summarizes the situations represented by different settings of contextual variables and the possible system reactions.

The purpose of the survey was to discover for each situation which of the system reactions succeeded in maintaining user trust and which did not. To this end, the participants had to rate the system reaction in terms of transparency, controllability, comfort of use, and trust using a 5-point Likert scale:

- 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: I found the system to be trustworthy.

All in all, 16 participants (7 female, 9 male) evaluated the situations for the light; and 22 participants (9 female, 12 male) rated the situations for the display. The participants were aged between 24 and 51 years (mean: 28).

² <http://arduino.cc/>

³ <http://www.homematic.com/>

4.2 Initializing the Bayesian Network

The quantitative data obtained in the online survey enabled us to derive and model probability distributions for each trust dimension for all combinations of context and system reaction. The probability distributions for other node combinations, that were not part of the data inquired in the survey (e.g. how *Confidence* and *Competence* influence *Trust Disposition*) were modeled after the results from a previous study [23]. 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 [24] for a survey of these studies.

5 User Study

Web-based data are relatively easy to obtain. However, they might not completely reflect the experience of users interacting with the actual system. To investigate to what extent the BN is able to predict user trust and user preferences in a live setting, we conducted a study with the developed smart office environment. The purpose of this study was to evaluate the decisions taken by the UTM focusing on two criteria: (1) Would the chosen system reactions affect the users' feelings of trust and the related trust dimensions in a positive way? (2) Would the system reactions match the actions favored by the users? Apart from evaluating the BN approach, we investigated the users' experience and acceptance of our smart office environment.

5.1 Experimental Setting

During the study the participants had to run through different tasks and situations that in total simulated the daily routine in an office occupied by several people. Changes of the participant's and the colleague's state (social context) were triggered by the participants themselves and by one of the experimenters that played the role of the participant's colleague. To ensure that all participants conducted the study under the same conditions and with a most realistic experience the room was darkened and changes of the outdoor luminance were simulated by a lamp and by covering and uncovering the light sensor.

5.2 Conducting the Study

At first the participants had to provide general demographic information and information about their experience with home automation systems and their trust towards computer systems in general. Furthermore, the participants were asked whether they considered themselves confiding.

After a short introduction to the setting and the scenario, the participants had to conduct the first task, and the system showed the reactions that were selected

for both devices according to the UTM. After that, the participants had to fill in a short questionnaire for each of the reactions. Each questionnaire included the questions Q1-Q4 that were also asked in the online survey. Furthermore, the users were asked to choose their preferred system action. For instance, the statement concerning the display and the first task was: "When I enter my office and sit at my desk, I prefer..."

- P1: ...no reaction from the display."
- P2: ...to switch the display on automatically."
- P3: ...to be asked via smartphone for permission to switch on the device."

After that, the procedure continued with the next task and the respective questionnaire. All tasks, the corresponding situations and the selected system reactions triggered by context changes are summarized in Table 2. To make the experiment more realistic, the tasks were embedded in a coherent story.

Table 2. Tasks, changed context variables and system reactions of the user study

Task	Situation			System Reaction	
	User State	Social Context	Outside Luminance	Light	Display
1. Enter the room	Arriving	Coworker Away	Dark	Confirm Via Mobile	
2. Sit down at PC and	WorkingAtPC				Switch On
It is getting light.					
3. Check slides for mistakes.			Bright	Confirm Via Display	
The participant's colleague enters the room and sits down at the desk.					
4. Take book X out of the shelf.	AwayFromDesk	Coworker Present			Do Nothing
5. Come back and read chapter Y.	IdleAtPC				Switch Off
6. Add a slide about Z.	WorkingAtPC				Switch On
It is getting dark.					
			Dark	Confirm Via Mobile	
The participant's colleague leaves the room.					
7. Finish work and leave.	Leaving	Coworker Away		Confirm Via Mobile	
8. Don't forget to close the door.	OutOfRoom				Switch Off

After rating the last task, the participants had to state what they liked and disliked about the system and to rate statements related to their experience during the usage and their attitude towards the system on a 5-point Likert scale.

5.3 Results

Overall six women and 18 men aged between 23 and 33 (mean: 26) took part in the study. They studied and worked in all kind of professions related (88%) and not related (12%) to computer science. All statements in the questionnaires could be rated on a 5-point Likert scale. Ratings lower than 3 were interpreted as disagreement, ratings higher than 3 as agreement with a statement. Only, five persons reported a significant amount of experience with technology for controlling parts of their home environment, such as automatic timers or blind control systems. Half of the participants never used such a technology.

The participants also had to reflect on their confidence. They had to answer on two general statements and one statement related to computer systems. Concerning the statement: *I act based on the saying "Trust, but verify"*, 63% of all participants agreed. Only one participant disagreed. Concerning the statements *I am overly trusting* and *On most systems, you can be assured that they will do what they should*, one third agreed, disagreed, or rated neutrally.

The participants gave consistently high ratings for the criteria "Transparency", "Controllability", "Comfort of Use", and "Trust" when evaluating the reactions the system had chosen for the adjustment of the light. The lowest average rating was achieved for the trustworthiness of "asking to switch the light off via the user's mobile phone" when the participants left the room and closed the door (Mean (M): 3.92, Standard Deviation (SD): .86). Two participants, for example, missed feedback that the light was switched off successfully. All other average scores were between 4 and 5. Despite these high ratings, in situations in which the system sent a message to the participants' phone, other system reactions were preferred. When they (a) entered or (b) left the room, the participants preferred the system to automatically switch on or off the lamp (a: 75%; b: 67%). When it was getting dark and they sat at the desk, they preferred to be asked for confirmation via their display (58%). Correspondingly, the system' decision to ask users for confirmation via their display when it was getting bright, matched the preference of 79% of the participants. These findings were in line with several statements of the participants. For example, one participant stated that he would prefer a message on the device he is currently using. Several users mentioned that using a phone is uncomfortable in many situations - either because it is not within reach or because they have to interrupt their work to read the message on the phone. Accordingly, some users preferred autonomous system actions instead of repeated messages on their phones because this would make the system less obtrusive. Apparently, the users were not aware of these issues in the online study.

In contrast, the automatically generated reactions for the display matched the participants preferences in all situations. Most of the participants wanted the system to decide autonomously whether the display should be switched on or off (Entering the room: 54%; Idle-State: 71%; Leaving the room: 79%) as opposed to asking the user for confirmation first or to not showing any reaction. However, they did not wish any adjustment when they left their desk only for a short time (88%). The participants clearly favored autonomous reactions for the display (as in the online condition), but at the expense of "Controllability" and

"Trust". While the average trust ratings still were above 3.0 for the idle state (M: 3.63; SD: 0.95) and for "leaving the room" (M: 3.88, SD: 0.88) the average ratings for "Controllability", except for "leaving the room" (M: 3.46; SD: 1.44), were lower than 3 with the lowest average rating for automatic control in the idle-state (M: 2.50, SD: 1.29). The ratings for the trustworthiness of autonomous reactions were affected, among other things, by a lack of feedback when leaving the room and by a missing authentication mechanism when entering the room. The low ratings for "Controllability" could be explained by requests for functionality to set or disable the automatic control of the display in the idle state.

The concluding questions also showed promising results. Most participants were satisfied (83%; M:3.96; SD: .68) and agreed that the system supported them to improve their energy consumption (96%; M: 4.71; SD: .54), that it behaved adequately (88%; M: 4.38; SD: .70), and that it was transparent (100%; M: 4.96; SD: .20). The lower, but still acceptable results for unobtrusiveness (58%; M: 3.71; SD: 1.10) could be mainly explained by the fact that the users had to operate the mobile phone. Further results showed that most of the participants did not feel distracted (75%; M: 2.00; SD: 1.00), restricted (88%; M: 1.83; SD: 1.07), or observed (63%, M: 2.33; SD: 1.18).

6 Conclusion

We presented an approach for trust-based decision-making for smart and proactive environments based on Bayesian Networks, the User Trust Model (UTM). It assesses users' trust experienced while interacting with a system and applies appropriate system reactions to maintain users' trust in critical situations. We described the UTM's construction, its integration in an office setting, and its initialization with empirical data. The results of a user study revealed that the system succeeded in maintaining the users' trust in the investigated situations. Even though the approach has been developed and evaluated for an energy management system, the basic mechanism is applicable to other applications of adaptation and personalization as well. While the basic structure of the BN representing the dependencies between trust and its dimensions could be reused, the nodes representing the context and possible system actions would have to be adapted to the corresponding applications.

Future work should investigate which factors in addition to trust impact the user's ultimate choice of a system action. Although, the participants provided high ratings for the chosen system actions, their preferences were not always in line with the system's decisions. Furthermore, we will investigate how to improve the accuracy of the UTM by incorporating knowledge about user-specific attitudes. Depending on their trust disposition, users might favor different system reactions. 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. A promising approach might be to distinguish between different categories of users based on multiple dimensions [25]. Another important aspect is the decision making for more than one user. For example, some participants wondered

whether they were the only person in control of the light. Therefore, the UTM should be extended to be able to consider the trust of all affected users. Finally, 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.

Acknowledgments. This research is co-funded by OC-Trust (FOR 1085) of the DFG and IT4SE of BMBF.

References

1. Hazas, M., Friday, A., Scott, J.: Look back before leaping forward: Four decades of domestic energy inquiry. *IEEE Pervasive Computing* 10(1), 13–19 (2011)
2. DiSalvo, C., Sengers, P., Brynjarsdóttir, H.: Mapping the landscape of sustainable hci. In: *Proc. of the SIGCHI Conf. on Human Factors in Computing Systems, CHI 2010*, pp. 1975–1984. ACM, New York (2010)
3. Gamberini, L., Spagnoli, A., Corradi, N., Jacucci, G., Tusa, G., Mikkola, T., Zamboni, L., Hoggan, E.: Tailoring feedback to users' actions in a persuasive game for household electricity conservation. In: Bang, M., Ragnemalm, E.L. (eds.) *PER-SUASIVE 2012. LNCS*, vol. 7284, pp. 100–111. Springer, Heidelberg (2012)
4. Simon, J., Jahn, M., Al-Akkad, A.: Saving energy at work: the design of a pervasive game for office spaces. In: *Proc. of the 11th Int. Conf. on Mobile and Ubiquitous Multimedia, MUM 2012*, pp. 9:1–9:4. ACM, New York (2012)
5. Cheverst, K., Byun, H., Fitton, D., Sas, C., Kray, C., Villar, N.: Exploring issues of user model transparency and proactive behaviour in an office environment control system. *User Modeling and User-Adapted Interaction* 15(3-4), 235–273 (2005)
6. Yan, Z., Holtmanns, S.: *Trust Modeling and Management: From Social Trust to Digital Trust*. IGI Global (2008)
7. Marsh, S.: Trust in distributed artificial intelligence. In: Castelfranchi, C., Werner, E. (eds.) *MAAMAW 1992. LNCS*, vol. 830, pp. 94–112. Springer, Heidelberg (1994)
8. Wang, Y., Vassileva, J.: Bayesian network trust model in peer-to-peer networks. In: Moro, G., Sartori, C., Singh, M.P. (eds.) *AP2PC 2003. LNCS (LNAI)*, vol. 2872, pp. 23–34. Springer, Heidelberg (2004)
9. Yu, B., Singh, M.P.: An evidential model of distributed reputation management. In: *Proc. of the 1st Int. Joint Conf. on Autonomous Agents and Multiagent Systems: Part 1, AAMAS 2002*, pp. 294–301. ACM, New York (2002)
10. Vogiatzis, G., MacGillivray, I., Chli, M.: A probabilistic model for trust and reputation. In: van der Hoek, W., Kaminka, G.A., Lespérance, Y., Luck, M., Sen, S. (eds.) *9th Int. Conf. on Autonomous Agents and Multiagent Systems (AAMAS 2010)*, Toronto, Canada, May 10-14, vol. 1-3, pp. 225–232. IFAAMAS, Richland (2010)
11. Jøsang, A., Hayward, R., Pope, S.: Trust network analysis with subjective logic. In: Estivill-Castro, V., Dobbie, G. (eds.) *29th Australasian Computer Science Conf (ACSC2006)*, January 16-19. *CRPIT*, vol. 48, pp. 85–94. Australian Computer Society, Darlinghurst (2006)
12. Castelfranchi, C., Falcone, R.: *Trust Theory: A Socio-Cognitive and Computational Model*. Wiley (2010)

13. Sankaranarayanan, V., Chandrasekaran, M., Upadhyaya, S.: Towards modeling trust based decisions: A game theoretic approach. In: Biskup, J., López, J. (eds.) ESORICS 2007. LNCS, vol. 4734, pp. 485–500. Springer, Heidelberg (2007)
14. Burnett, C., Norman, T.J., Sycara, K.P.: Trust decision-making in multi-agent systems. In: Walsh, T. (ed.) IJCAI 2011, Proc. of the 22nd Int. Joint Conf. on Artificial Intelligence, IJCAI/AAAI, pp. 115–120 (2011)
15. Sherchan, W., Nepal, S., Paris, C.: A survey of trust in social networks. *ACM Comput. Surv.* 45(4), 47:1–47:33 (2013)
16. Bhuiyan, T., Xu, Y., Jøsang, A.: A review of trust in online social networks to explore new research agenda. In: Arabnia, H.R., Clincy, V.A., Lu, J., Marsh, A., Solo, A.M.G. (eds.) Proc. of the 2010 Int. Conf. on Internet Computing, ICOMP 2010, July 12–15, pp. 123–128. CSREA Press, Las Vegas (2010)
17. Adali, S., Escriva, R., Goldberg, M.K., Hayvanovych, M., Magdon-Ismail, M., Szymanski, B.K., Wallace, W.A., Williams, G.T.: Measuring behavioral trust in social networks. In: Yang, C.C., Zeng, D., Wang, K., Sanfilippo, A., Tsang, H.H., Day, M.Y., Glässer, U., Brantingham, P.L., Chen, H. (eds.) IEEE Int. Conf. on Intelligence and Security Informatics, ISI 2010, Proc., pp. 150–152. IEEE, Vancouver (2010)
18. Ivanov, I., Vajda, P., Korshunov, P., Ebrahimi, T.: Comparative study of trust modeling for automatic landmark tagging. *IEEE Transactions on Information Forensics and Security* 8(6), 911–923 (2013)
19. Glass, A., McGuinness, D.L., Wolverton, M.: Toward establishing trust in adaptive agents. In: Proc. of the 13th Int. Conf. on Intelligent User Interfaces (IUI 2008), pp. 227–236. ACM (2008)
20. Russell, S.J., Norvig, P.: *Artificial Intelligence: A modern approach*, 2nd edn. Prentice Hall, Upper Saddle River (2003)
21. Kurdyukova, E., André, E., Leichtenstern, K.: Trust management of ubiquitous multi-display environments. In: Krueger, A., Kuflik, T. (eds.) *Ubiquitous Display Environments*, pp. 177–193. Springer (2012)
22. Lumsden, J.: Triggering trust: To what extent does the question influence the answer when evaluating the perceived importance of trust triggers? In: Proc. of the 2009 British Computer Society Conf. on Human-Computer Interaction (BCS HCI 2009), pp. 214–223. British Computer Society (2009)
23. Bee, K., Hammer, S., Pratsch, C., Andre, E.: The Automatic Trust Management of Self-Adaptive Multi-Display Environments. In: *Trustworthy Ubiquitous Computing. Atlantis Ambient and Pervasive Intelligence*, vol. 6, pp. 3–20. Atlantis Press (2012)
24. Kumaraguru, P., Cranor, L.F.: Privacy indexes: A survey of westin’s studies. Technical Report CMU-ISRI-5-138, Technical Report, Institute for Software Research Int (ISRI), Carnegie Mellon University (2005)
25. Knijnenburg, B.P., Kobsa, A., Jin, H.: Dimensionality of information disclosure behavior. *Int. J. Hum.-Comput. Stud.* 71(12), 1144–1162 (2013)