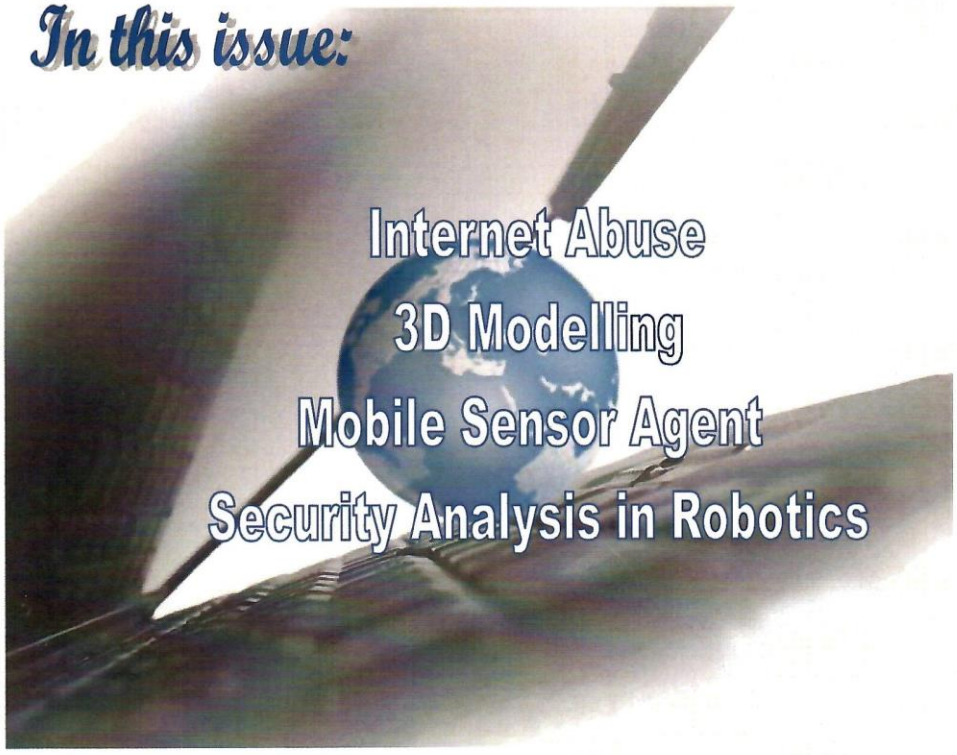
International Journal on
Information Technologies and Security

Year V № 4 / 2013

In this issue:



Internet Abuse

3D Modelling

Mobile Sensor Agent

Security Analysis in Robotics

International Journal on Information Technologies and Security

Publication of the Union of Scientists in Bulgaria
39, Madrid blvd., Sofia 1505, Bulgaria

International Editorial Board

Prof. Luís BARROSO, Ph.D.	Universidade Lusiada de Lisboa (Portugal)
Prof. Dencho BATANOV, Ph.D.	Frederick University, Nicosia (Cyprus)
Prof. Francesco BERGADANO, Ph.D.	University of Turin, Torino (Italy)
Prof. Pino CABALLERO-GIL, Ph.D.	University of La Laguna, Tenerife (Spain)
Assoc. Prof. Vassil FOURNADJIEV, Ph.D.	New Bulgarian University, Sofia (Bulgaria)
Prof. Adam GRZECH, D.Sc.	Wroclaw University of Technology (Poland)
Prof. Luis HERNÁNDEZ ENCINAS, Ph.D.	Spanish National Research Council (Spain)
Prof. Hristo HRISTOV, D.Sc.	Technical University of Sofia (Bulgaria)
Prof. Gerrit JANSSENS, Ph.D.	Hasselt University (Belgium)
Assoc. Prof. Todor KOBUROV, Ph.D.	Institute of Legal Studies – BAS (Bulgaria)
Prof. Emil KONSTANTINOV, D.Sc.	Institute of Legal Studies – BAS (Bulgaria)
Gwendal LE GRAND, Ph.D.	CNIL – Data Protection Authority (France)
Assoc. Prof. Penka MARTINCOVA, Ph.D.	University of Zilina (Slovak Republic)
Prof. Gerasimos MELETIOU, Ph.D.	Epirus Institute of Technology (Greece)
Prof. Götz NEUNECK, D.Sc.	University of Hamburg (Germany)
Assoc. Prof. Irina NONINSKA, Ph.D.	Technical University of Sofia (Bulgaria)
Coresp. Memb. Angel POPOV, D. Sc.	Sofia University "St. Kl. Ohridski" (Bulgaria)
Assoc. Prof. Goran RAFAJLOVSKI, Ph.D.	Faculty of Electronic Eng. and IT (Macedonia)
Prof. Radi ROMANSKY, D.Sc.	Technical University of Sofia (Bulgaria)
Prof. Radomir STANKOVIĆ, Ph.D.	University of Niš (Serbia)
Prof. Michael VRAHATIS, Ph.D.	University of Patras (Greece)

Technical Board

Section *Information Technologies*	Prof. Radi ROMANSKY, D.Sc. (***rrom@tu-sofia.bg***)
Section *Information Security*	Assoc. Prof. Irina NONINSKA, Ph.D. (***irno@tu-sofia.bg***)
Section *Security Policy*	Assoc.Prof. T. KOBUROV, Ph.D. (***todor_kobourov@yahoo.com***)
Section *Innovation Policy*	All members of the Technical Board

Proposal (manuscript) for publication in the Int'l J. IT & S should be sent to the corresponding member of the Technical Board depending on the thematic section. Instructions for authors are presented in the last pages.

ISSN 1313-8251
Copyright © 2013

International Journal on
Information Technologies and Security
№ 4 (vol. 5), 2013

ISSN 1313-8251

Contents

Information Technologies

01. Internet Abuse by University Students: a Neglected Theme in Africa 3
Almamy Touray (Finland)

02. Mobile Virtual 3D Model of a Medieval Town 13
Stanislav Kostadinov, Tzvetomir Vassilev (Bulgaria)

03. Fast and Lightweight Solution to Visualising 3D Content on the Web 19
Stanislav Kostadinov, Tzvetomir Vassilev (Bulgaria)

04. Machine Learning and Decision Making in Autonomous Mobile Sensor Agent Framework 27
Vanya Markova (Bulgaria)

Information Security

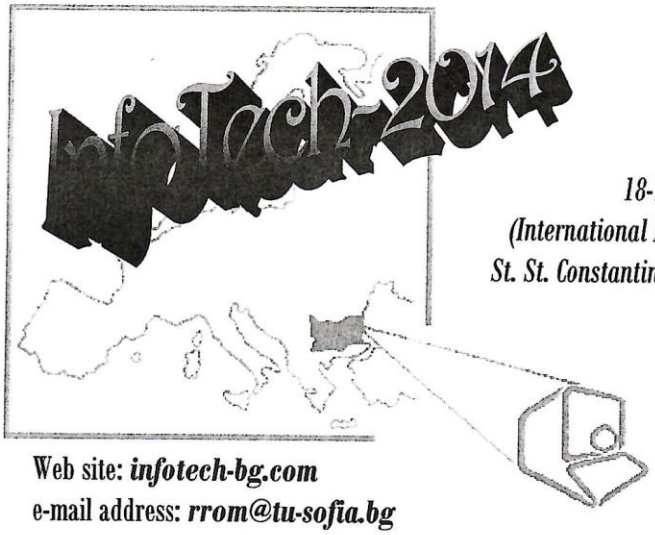
05. Security Analysis and User Acceptance of Socially Competent Robotic Systems 37
Maya Dimitrova, Anna Lekova (Bulgaria)

Innovation Policy

06. New European Thematic Network "Future Education and Training in Computing: How to support learning at anytime anywhere" (FETCH) 47
information summarized by Radi Romansky (Bulgaria)

Instruction for authors 55

28th International Conference on Information Technologies



18-19 September 2014
(International Home of Scientists)
St. St. Constantine and Elena resort
BULGARIA

Web site: ***infotech-bg.com***
e-mail address: ***rrom@tu-sofia.bg***

We invite submissions of papers presenting original researches in the following topics (but not limited):

- *Information Technologies*
- *Information Security / Security Policy*
- *Networking and Communication Technologies*
- *Distributed Systems and Applications*
- *Technologies for System Design*
- *Intelligent Systems and Applications*
- *Technological Aspects of e-Governance and*
- *Technological Aspects of Personal Data Protection*

WORKING LANGUAGE: English

All accepted papers, presented at the conference, will be published in the Proceedings (ISSN 1314-1023) which will be spread over 20 libraries in the World and will be included in the scientific databases of EBSCO Publishing Inc. (USA). Selected papers could be published in special issue of this journal.

Electronic versions of the Application Form and of the **TEMPLATE** for paper preparation could be downloaded from the conference web site.

SECURITY ANALYSIS AND USER ACCEPTANCE OF SOCIALLY COMPETENT ROBOTIC SYSTEMS

Maya Dimitrova, Anna Lekova

Institute of Systems Engineering and Robotics, Bulgarian Academy of Sciences,
Akad. G. Bonchev Str., Block 2, P.O. Box 79, 1113, Sofia
e-mail(s): {dimitrova, alekova}@iser.bas.bg
Bulgaria

Abstract: The paper presents a novel account of security and acceptance of socially competent robots. The aim is to propose methodology for analysis of the newly designed assistive robotic systems in the future in order to detect even minor misperformance of the robot. A model of user acceptance of socially competent robotic systems is proposed, based on a novel framework of security analysis of human-robot interaction with socially competent robots. Several implications for future robotic systems are discussed.

Key words: security analysis, acceptance, socially competent robots

1. INTRODUCTION

Unlike the common view that robots should do "dangerous, dirty or dull jobs", public opinion favors the view that robots should perform tasks requiring *memorization*, keen *perceptual skills* and *service orientation*. People, on the other hand, are preferred for jobs requiring *artistry*, *evaluation*, *judgment* and *diplomacy* as revealed by a recent study on human-robot interaction [1]. Such functional distinction of jobs, performed in the near future, by people and robots coexisting and co-working together, will bring new concerns related to security and safety in using robots and to human acceptance of their autonomous performance.

Recent advances in robotic technology have brought to life a family of devices with compliant actuators, which make the issue of avoiding each other in a house, for example, a "softer" problem [2]. In striving to achieve social communication skills, a huggable elephant-robot Probo is designed [3]. It is being assumed that if the physical appearance of a robot is appealing, then social interaction of affection can be easily achieved. However, this is a tough engineering and technological, as well as psychological issue, because the adaptive mechanisms of the robot are much more limited than the human physical presence.

None less important in assistive robotics is the issue of designing the "social presence" of the robot [4]. The social presence theory was proposed to account for

social phenomena in the telecommunication mediated world [5, 6]. Physical presence is felt by the" just-beyond-threshold" values of the sensor systems – vision, auditory system, touch, olfaction, taste, and sense of gravitation (vertical position). With the development of telecommunications – novel indicators of the social presence emerge – in email, social web, skype and mobile technology. Either mediated or not via telecommunications – social signaling via physical means is what makes "social presence" emerge.

From a security perspective, with the wide introduction of robotic systems at work and in people's homes, new designer concerns are formulated to make them helpful to robot's full potential, overcoming barriers to better acceptance by the human. The main are – security analysis and human acceptance of the socially competent robotic systems of the future.

The paper presents a novel account of security and acceptance of socially competent robots aiming to propose methodology for analysis of the newly designed assistive robotic systems.

2. THE PROBLEM OF DESIGNING SECURE SOCIALLY COMPETENT ROBOTIC SYSTEMS

A robotic system generally consists of a robot to control or interact with and a software platform necessary to adapt and upgrade robot functionalities and behavior [7]. Therefore, all concerns addressing the problems of security of telecommunication networks apply, in addition to the design for *social presence* competence of the robot as well as flexibly controlling its *physical presence.*

In [8] **security** in telecommunication networks is defined as: "the capability of *the system to protect against (withstand, counteract) external destabilizing factors and effects as well as against internal changes, that may result in hazard* (p. 22). Therefore, the possibility of intrusions in the robotic platform and altering the social behaviour of the robot (internal change) may cause damage of unforeseen scale or effect.

2.1. Levels of design for "Overal Security", "Social Presence" and "Physical Presence" in human-robot interaction

In figure 1 we propose a new conceptual scheme of maintaining security of a robotic platform based on identifying *levels of generality* of the tasks included in the implemented safety algorithms. The least general level is the level of design for maintaining the **"physical presence"** of the robot. It consists of two types of functions – on the one hand is the performing of tasks and obeying to commands - and on the other – ensuring the overall safety of robot navigation, rotation, bending and coordination of the moving limbs. The implemented robotic platform needs to perform *model checking* all the time in order to detect even the slightest miss-performance by the robot of the constantly arriving user demands.

The next in generality level is the level of design for involving the **"social presence"** of the robot. This level is wider than the physical one because it may include "navigation, rotation, bending and coordination of the moving limbs", which functional utility is not evident in a straightforward manner. The *context* of the personalized human-robot interaction history will have to be elicited in order to understand robot behaviour and define the safety procedures to ensure the overall security of the human-robot system. One method of introducing relevant context is by *reading social signalling* in behaviour, often being performed by means of physical presence (gestures, signs, body language, mimicking and sound).

The widest generality level is the level of design for ensuring the **overall security** of the human-robot system. It includes possible unforeseen as well as predicted destabilizing factors in the environment (i.e. the flooding of Fukushima Power Plant was unexpected, so it presents a novel obstacle to the normal functioning of the robotic systems) on the one hand, and internal changes like intrusions in the software platform, damage and leaking of information, as well as creating vicious false alarms, on the other.

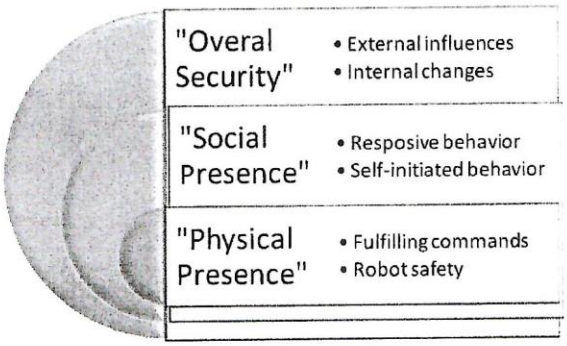


Fig.1. Levels of design for "Overall Security", "Social Presence" and "Physical Presence" in human-robot interaction

The monitoring of the internal changes becomes even more demanding and complicated task, and has to be performed in concert with maintaining the security of the other two levels. The magnitude of the task to ensure overall and long-term security of the human-robot system becomes exponential function of the amount of routines included in the basic level of behaviour of the robot.

Robots are traditionally designed to deal with dangers in the environment (external factors). None less important is the problem of being aware of its own "mental (i.e. software) health". Demanding the user to be alert on any of the peculiarities of the robot behaviour will present obstacle to, rather than enhancement of the entire human-robot interaction process. Collaboration is needed between the user (instructing users what to monitor) and the robot being

able to self-heal as a communication system [9]. Therefore, a concerted scheme of training of the user as well as adapting the behaviour of the robot to the individual preferences of the user is inevitable in order to ensure acceptable level of security of the overall human-robot system.

2.3. Acceptance of human-robot social interaction as a security factor

The model for security and acceptance analysis of socially competent robotic systems is based on the "social motivation theory" proposed by Chevalier et al. [10]. The theory provides a biological explanation to the basic social phenomena, which are guiding the individual behavior. Social motivation is understood as evolutionary adaptation to a collaborative environment where the "fittest" is performing best within this environment. Social presence is an aspect of such a collaborative environment. Without the signs of *social presence* in the communication, the collaborative environment will be simply a collection of individuals being physically present in the near vicinity. Chevalier et al. propose to account for three kinds of behavioral manifestations of social motivation:

- Social orienting;
- Seeking-liking;
- Social maintaining.

These manifestations are underlined by the biological circuit of the brain "orbitofrontal – striatal – amygdala", influenced by specific neuropeptides (oxitocin, dopamine, opoids), participating in understanding social signaling and responding to socially reinforcing stimuli [10]. Robotic systems, in the general case, use software platforms instead of biological circuits, in particular when *conscious* functions are being modeled.

Table 1 presents a comparison between perceiving social motivation signals performed by humans and by present-day robots. Performance by robots is "symbolic" in its manifestation (based on propositional logic), whereas human communication of social signals is natural and spontaneous. The left column of the table contains the proposed in [10] behavioral manifestations of social motivation, presented as hierarchical levels in human development. The right column presents parallel phenomena, revealed in research on human-robot interaction, that are useful for a novel framework of user acceptance of socially competent robotic systems.

The most general is the level of "Social orienting". This level is characterized by innate attention to faces, automatic attention capture by social signals and by "eye contact effect". Babies learn at very early stages to read these signals of social, rather than physical presence of the people around them. Studies of user perception of robots show diverse effects, like people not assuming the main feature of the robot being its face [11], robot gaze not cueing human attention automatically as faces and symbols do [12, 13], as well as eye contact being used only by platforms aiming to model how users interpret the robot's "attitude" [14].

The next level, presented in table 1, called "Seeking – liking" represents the evolutionary value of socializing for the people, i.e. the rewarding nature of the social contact. In humans this is manifested by the incentive value of the social reward stimuli, the experienced pleasure in collaboration as well as in the so called "over-justification effect". This effect denotes cases when people exaggerate the social value of material possessions and thus justify the striving for material things. This particular level, in fact, is the main focus of social and assistive robotics research. Because it directly relates to emotions, research efforts are being focused on making robots likable and responding to emotion [15, 16]. Whenever social contact is not indirect, but tactile, physical interaction imposes different security demands. For example, safety of the designed huggable robots becomes a sensitive issue, especially if the platform is intrusion prone.

Technological and software platforms, proposed for socially assistive robots, tend to be open source and of higher availability. Therefore they may contain threats that are not obvious at first sight. In [7] cases are discussed with malicious applications that can unnoticeably change robot behavior to violate user privacy. It has been established in [16] and [17] that people prefer robots of similar personality – introvert or extravert. If an introverted robot suddenly becomes cheerful – this may be malicious intrusion rather than change in robot emotionality.

Unlike in science fiction films, present-day **robots are inherently altruistic**. The reason is not just because it is a difficult task to build a harmful, but intelligent robot. Robots are being built to reinstate or replicate the best of the human performance, including as "social presence". They do not understand "overjustification" of material things – cars, houses, personal belongings, valuable pieces of art, luxury items. A robot finds it difficult to distinguish "its own owner" – i.e. one human form another [7]. Therefore, for the present-day robots functionality is the highest quality of an item, not the aspect of an object being someone's possession.

The above comparison of the manifestations of the "social motivation" in humans and robots reveals that they are much more complementary than in competition. Together people and robots perform better than alone and help each other in a much unprecedented and unpredicted way. In order to become more widespread as well as more accepted in performing tasks requiring *memorization*, keen *perceptual skills* and *service orientation*, novel designs focusing on "social maintaining" can be proposed.

The level of "Social maintaining" in table 1 includes behavioral strategies that people employ in order to increase their status in society. These strategies include orientation to self and/or other enhancement, management of one's own reputation as well as the so called "chameleon effect", when people imitate the most desired role models. Socially competent robotic systems can contribute enormously to the improved functioning of the society in general.

Robots employ various self-learning algorithms in order to better adapt to the user. These can be focused on implementing diagnostic capabilities – i.e. for

dementia [18]. With adequate detection of symptom worsening – alarm can be used to inform the relatives or the medical staff on the user's current condition.

In relation to reputation management – the robot can assist the user in making socially appropriate choices. The robot can become a competent companion of the user; therefore it can be also competent not only of safety precautions, but also on security maintaining strategies to be provided to the user.

Table 1. Social motivation theory account of levels of human-robot interaction

Signals	***Human***	***Robot***
Social orienting	*1. Innate attention to faces* *2. Automatic attention capture by social signals* *3. Eye contact effect*	*1. Robots are not stereotypically defined by their face [11]* *2. Robot gaze is not automatically processed [12], [13]* *3. Eye contact depends on context [14]*
Seeking – liking	*1. Incentive value of social reward stimuli* *2. Pleasure in collaboration* *3. Over-justification effect*	*1. Safety of huggable robots [2]* *2. Prefer robots with similar personality [16], [17]* ***3. Robots are inherently altruistic***
Social maintaining	*1. Integration strategies – self and other enhancement* *2. Reputation management* *3. Chameleon effect*	*1. Self-learning algorithms to adapt to the user; diagnostic capabilities (i.e. for dementia)[18]* *2. Assisting the user in making socially appropriate choices; being a competent companion* *3. Robots can make good psychotherapists (listening and mirroring the other); calm and patient tutors; do not get bored, do not display negative attitude.*

Assisting the natural inclination of people to follow desired behavioral models and to imitate favored examples, robots can make good psychotherapists, because they can skillfully listen and mirror the others. Robots can make calm and patient tutors; they do not get bored and do not display involuntarily nervousness or negative attitude. If following these design guidelines, future assistive robots will help people reveal their advantages in performing jobs requiring *artistry*, *evaluation*, *judgment* and *diplomacy*. Security of human-robot interaction can be

maintained by informing the user on these aspects of the proposed job allocation to robots and to people.

3. A MODEL OF USER ACCEPTANCE OF SOCIALLY COMPETENT ROBOTIC SYSTEMS

A model of user acceptance of socially competent robotic systems is proposed based on the above security analysis of human-robot interaction (figure 2).

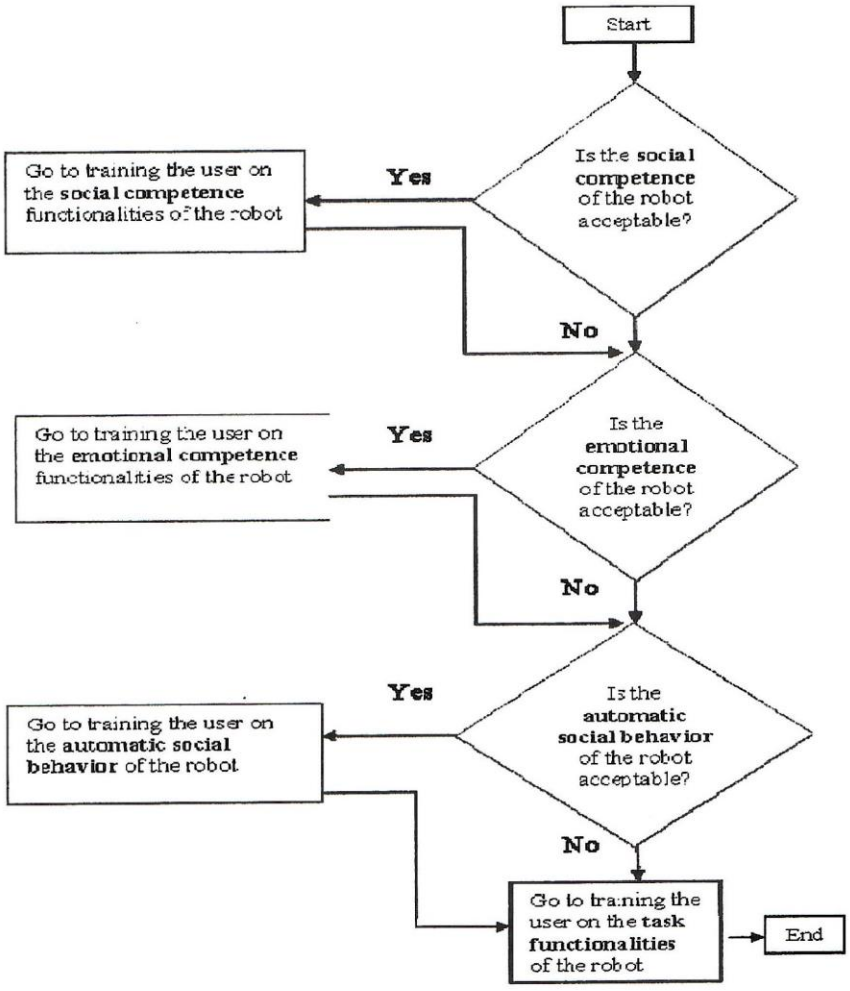


Fig. 2. A model of user acceptance of socially competent robotic systems

It is proposed to start the analysis of user acceptance of socially assistive robots from the top level of the social motivation signals down to the basic task-defined robot behaviors. The presented in the left column of table 1 social motivation levels are related in figure 2 to the respective levels of social behavior of the robot as follows: The level of "social maintaining" corresponds to the level of *social competence* of the robot; the level of "seeking – liking" corresponds to the level of *emotional competence* of the robot and the level of "social orienting" corresponds to the level of *automatic social behavior* of the robot.

The set of observed robot behaviors are divided in four groups of increasing behavioral complexity. The baseline is the set of task-defined behaviors, which are the basic skills of the robot – cleaning, cooking, lifting, transporting, playing musical instruments, etc. One step above the basic task dependent functionalities are the preprogrammed automatic social behaviors – responding to its name, smiling, gazing, gesturing, body language, etc. [19, 20]. Next are the behaviors, displaying the range of emotional competence of the robot – interaction styles, personality type, etc. The top level is the social competence of the robot – not only performing behaviors like giving advice or imitation of the user, but providing coherent explanation of its own intentions. Ability for complex dialogue (spoken, written or gestural) is a necessary element of this level of user-robot interaction. Users are being interviewed on the desired set of robot behaviors starting top down. If complex social behaviors are not acceptable, then the interview proceeds to the emotional level and so on. Finally a decision is made if the set of basic functions are all necessary and acceptable for the current user.

Reshaping and retraining is always possible to increase the social competence of the robot. This approach will provide clear and understandable view to the user of possible and implausible behaviors of the robot, which can inform the overall security of the interaction and diminish the false alarm rate, which is the most important aspect of making the robotic help efficient and natural to the user.

4. CONCLUSION

The paper presented a novel framework for security analysis of socially competent robotic systems. The social motivation theory was employed to draw parallels of user social behaviors and existing robot competencies at the present moment. A model of user acceptance of socially competent robotic systems is proposed where the user is being interviewed on the desired robot functionalities starting from the most complex behaviors top down to the basic task-related functionalities of the robot. It is proposed that this approach can provide more salient understanding to the user of the most important security issues related to using novel socially competent robotic technologies. Future work will include tests of the proposed framework in realistic human-robot interaction scenarios.

REFERENCES

[1] Takayama, L. et al. Beyond dirty, dangerous and dull: What everyday people think robots should do. *Proc. of the Human-Robot Interaction Conference HRI 2008*, Amsterdam, NL, 2008, pp. 25-32.

[2] van Ham, R. et al. Compliant actuator designs. Review of actuators with passive adjustable compliance/controllable stiffness for robotic applications. *IEEE Robotics & Automation Magazine,* September 2009, pp. 81-94.

[3] Goris, K. et al. How to achieve the huggable behavior of the social robot Probo? A reflection on the actuators. *Mechatronics*, **21**, 2011, 490-500.

[4] Short, J. A. et al. *The Social Psychology of Telecommunications*. New York: John Wiley & Sons, USA, 1976.

[5] Biocca, F. et al. The Networked Minds measure of social presence: Pilot test of the factor structure and concurrent validity. *Proc. of the 4th Int'l. Workshop on Presence*, Philadelphia, USA, May 2001 (accessed October 2013). http://www.temple.edu/ispr/prev_conferences/proceedings/2001/Biocca2.pdf

[6] Young, J.E. et al. Evaluating human-robot interaction. Focusing on the holistic interaction experience. *Int'l. Journal of Social Robotics*, **3**, 2011, pp. 53-67.

[7] Finnicum, M., S.T. King. Building secure robot applications. *Proc. of the 6th USENIX Conf. on Hot Topics in Security*, 2011, pp. 1-6.

[8] Hristov, H., V. Trifonov. Security of telecommunication networks: A dominant feature within current safety problems. *Int'l Journal on Information Technologies & Security*, **2**, 2009, pp. 19-28.

[9] Ghosh, D. et al. Self-healing systems — survey and synthesis. *Decision Support Systems*, **42**, 2007, pp. 2164–2185.

[10] Chevallier, C. et al. The social motivation theory of autism. *Trends in Cognitive Sciences*, **16** (4), April 2012, pp. 231-239.

[11] Ramey, C.H. An inventory of reported characteristics for home computers, robots, and human beings: Applications for android science and the uncanny valley, *Proc. of the ICCS/CogSci-2006 Long Symposium: Toward Social Mechanisms of Android Science*, Vancouver, Canada, July 2006, pp. 21-25.

[12] Admoni, H. et al. Robot gaze does not reflexively cue human attention. *Proc. of the 33rd Annual Conf. of the Cognitive Science Society CogSci 2011*, Austin TX USA, 2011, pp. 1983-1988.

[13] Admoni, H. et al. Are you looking at me? Perception of robot attention is mediated by gaze type and group size. *Proc. of the 8th ACM/IEEE Int. Conference on HRI,* Tokyo, Japan, March, 2013, pp. 389-396.

[14] Choi, J.J. et al. The less you look the more you get: Designing gaze avoidance in human-robot interaction. *Archives of Design Research*, **26** (2), 2013, pp.71-83.

[15] Poel, M. et al. Gaze behavior, believability, likeability and the iCat. *Proc. of the 6th Workshop on Social Intelligence Design*, Trento, Italy, 2007, pp.109-124.

[16] van Breemen et al. iCat: an animated user-interface robot with personality. *Proc. of the 4th Int'l. Joint Conf. on Autonomous Agents and Multiagent Systems AAMAS '05*, Utrecht, Netherlands, July 2005, pp. 143-144.

[17] Merel, B. *Effect of robot-user personality matching on the acceptance of domestic assistant robots for elderly*. University of Twente, http://essay.utwente.nl/61971/1/EffectPersonalityMatchingOnRobotAcceptance_1482012.pdf (accessed October 2014).

[18] *An Interactive Pet Companion with Emotion Recognition*, http://www.ipi-singapore.org/skin/wbn/pdf/tmp/techbrochure_1148.pdf?4638284 (accessed October 2013).

[19] Lekova A, M. Dimitrova. Hand gestures recognition based on lightweight evolving fuzzy clustering method. *Proc. of the 2nd IEEE Int'l. Conf. on Image Information Processing – ICIIP*, India, December 2013 (in print).

[20] Barakova E., T. Lourens. Expressing and interpreting emotional movements in social games with robots. *Personal and Ubiquitous Computing*, **14**, 2010, pp. 457-467.

Information about the authors:

Maya Dimitrova is Associate Professor at the Institute of Systems Engineering and Robotics of the Bulgarian Academy of Sciences. She received her PhD degree in Application of Principles and Methods of Cybernetics in Different Areas of Science from the Institute of Control and Systems Research in 2002. Her research interests are in user-robot interaction, cognitive modeling, neural networks and interface technologies for medical information systems.

Anna Lekova is Associate Professor at the Institute of Systems Engineering and Robotics of the Bulgarian Academy of Sciences. She is Head of Department Hybrid Systems. She received her PhD degree in CAD/CAE/CAM systems from the Technical University - Sofia in 1995. Her research interests are in fuzzy logic, fuzzy clustering, robot vision, gesture recognition, visual grammar, communication technologies, mobile computing, multi-hop wireless networks.

Received: 15 October 2013
Revised: 21 November 2013