Reconfigurable sensor networks: transforming ethical concerns?

F. Dechesne, M.J. van den Hoven, M.E. Warnier
Department of Technology, Policy and Management,
Delft University of Technology, The Netherlands
Jaffalaan 5, 26282 BX Delft
The Netherlands
Tel. +31-15-2785143
Fax. +31-15-2786439
E-mail: F.Dechesne@tudelft.nl, M.J.vandenHoven@tudelft.nl,
M.E.Warnier@tudelft.nl

Abstract

With the increasing use of sensor technology for different societal goals, like security and safety, the demand for multiple and flexible functionality of the sensors is rising. The expectation is that the development of reconfigurable sensors will lead to a continuous and affordable infrastructure. In this note, we undertake a first exploration of the ethical challenges reconfigurability raises for sensor networks, and more generally, for sociotechnical systems.

Keywords: sensor networks, reconfigurability, design for values

INTRODUCTION

The latest antenna systems for wireless telecommunication and radar show the first signs of being reconfigurable, in order to make the bundle quickly adaptable to the fluctuating information needs in varying circumstances. Also, digital technology shows a trend towards the development of chips whose functionality can be changed in a matter of seconds, even while being in use. Almost instantaneous reconfigurability is a feature that will be in high demand in the near future. In this paper we will explore some of the specific ethical problems associated with such forms of reconfigurability.

This paper is written against the background of a large scale research project in The Netherlands called STARS, aiming at the development of "necessary knowledge and technology to be able to build reconfigurable sensors and sensor networks" (STARS, 2010) By making the sensors reconfigurable, the project aims to deliver a continuous and affordable infrastructure for societal security, but it also anticipates possible use in other application areas. As an example, one may want to be able to transform a sensor network installed in a harbor for security purposes, for example to prevent theft or sabotage, into an information system for rescue workers during a fire in the same harbor.

The feature of reconfigurability will be leading in the design and development of the architecture and technologies in the project. Although the first use cases speak of the police, security- and information services fire brigade as intended users, it is expected that the technology, if successful, will cover a broader application area by a broader range of users. During the project, system concepts and application potential are to be defined and explored.

Our open and complex society is based on and motivated by values like freedom, trust, social cohesion, quality of life. Sensor networks are installed to provide security against the associated vulnerabilities. Making the sensors reconfigurable and adaptable to different application areas, should make the broad application of such networks economically and physically feasible.

A reconfigurable sensor network is developed to serve the societal goals of safety and security, but it is not just the technical features of the network that will determine the effect of the technology. The effect will be determined by the way in which the system with its features is embedded in social and societal structures: What data will be gathered and by whom? Who will handle the data? How will the data be used? Who determines the priority of functionalities, if the system is intended to serve different goals? The aspect of reconfigurability will make these questions more complex.

In this paper, we undertake a first exploration of the ethical challenges that may be raised by such reconfigurability, in terms of existing analyses of ethical aspects of surveillance technology. This is a first step in our intended contribution to the development of the architecture and methodology concerning reconfigurable sensor systems within the next few years: how can ethical challenges be addressed in the design process when the result is to be reconfigurable.

THE CONCEPT OF RECONFIGURABILITY (IN SENSOR NETWORKS)

The ultimate reconfigurable system is probably a computer, as a "universal machine". Computers have enabled many reconfigurable sensor systems already, for example the functionality of a CCTV system can be enhanced by using specific software that processes faces and compares these to a database with known subjects in order to identify them. In a sense this shift of functions could be described as “reconfigurability”, since the original functionality of the system is altered (reconfigured) for a specific purpose.

The reconfigurability in sensors and sensor networks discussed in this paper will be of a restricted form. It is mainly focused on the hardware level, and addresses analogous front-ends (infrared, radar, etc) and digital signal processing. The system concepts and architecture have yet to be developed. Reconfigurable parts of sensor networks that will be looked at are: antennas, receivers, transmitters, on-chip and off-chip communication. Methodological questions are raised by making parts of the architecture reconfigurable, such those concerning testing procedures, software-hardware partitioning and composability.

Reconfigurability of such systems can be understood at different levels, and in different degrees. In the context of system architectures for data processing, Guo (2006) makes the following distinction: "general purpose processors, application specific architectures and reconfigurable architectures. […] [R]econfigurable systems have drawn increasing attention due to their combination of flexibility and efficiency. Reconfigurable architectures limit their flexibility to a particular algorithm domain. […] High-level design entry tools are essential for reconfigurable systems, especially coarse-grained reconfigurable architectures. However, the tools for coarse-grained reconfigurable architectures are far from mature." Similarly, reconfigurable sensors and sensor networks will require new technical tools, but also a new approach towards dealing with ethical aspects.

BACKGROUND: THE STARS PROJECT

Our current society shows an increasing complexity and associated risks, under the influence of developments like globalization and the increasing use and dependence on technology. In response to this, more technology is developed and deployed in order to manage both complexity and risks.

Sensors are viewed as important sources of information that can be used to protect our society against threats on the one hand, and to help resolve crisis situations on the other. Especially, the application area of security has pushed the development of all kinds of sensor technology. The motivation of the STARS-project, as summarized in the next few paragraphs, is to develop reconfigurable sensor technology to make the vast range of possible applications of sensor technology feasible and affordable.

The security domain is characterized by the great diversity of threats and the absence of warning time. The circumstances change continuously and unpredictably so due to the creativity of the opponent. It is therefore essential to be able to anticipate and respond adequately to new situations.

The societal problem is that it takes too long, and it is too expensive, to invest over and over again in new systems to be developed to protect against the ever changing threats. Truly successful security technologies should therefore satisfy a number of characteristics: reliable and affordable, sustainable and effective, multi-domain and multi-service.

Reconfigurable sensors have these characteristics. They allow for flexible application, because the functionality enclosed in the system can be altered relatively simply and quickly. In scenarios that are expected, reconfigurability is used to instantaneously optimize for foreseen situations and the corresponding tasks. In the new, unexpected scenarios, the reconfigurability is used to respond to circumstances that were unforeseeable at the time of the system development, by adapting the functionality of the system to the new situation.

In other words, infrastructure based on reconfigurable systems diminishes the risk factor, because it allows continuously, both in development and use, to respond to human creativity and a changing environment, as created by the opponent in the security domain.

The aim of STARS is to develop, within four years, the necessary technological knowledge for the construction in the Netherlands of reconfigurable sensors and -networks, aimed at sustainable security, with expected spill-over to other domains. (STARS, 2010)

BACKGROUND: USE CASE

The intended application of the reconfigurable sensors and sensor networks is the safety and security domain. A use case for the sensor networks is for example the situation at a large port area (as for example the port of Rotterdam). Radar systems are used in large ports to 'follow' the movement of ships.. Ship sizes can also be determined by these systems. Such radar systems consist of a number of radar devices, that send their data to a central control center. Here the data is processed to provide a full overview of the whole area. Other sensor data, for example from CCTV systems or motion detectors (around security gates) is also sent here, providing even more information in case of an incident.

Numerous issues around safety and security can arise in a port environment, including fire hazards, drug trafficking, terrorism, people trafficking or transport of hazardous chemicals. During an incident all sensor data can be combined to coordinate emergency services. Reconfigurable sensors can be very useful in such environments, since they can be used for different tasks as the need arises, whereas previously multiple sensor systems were required. Consider, for example, the case where a small plane crashes into the port area. The police might be worried that this is part of an organized terrorist attack, in which case (part of) the radar system can be reconfigured to look for other (low flying) planes. Information provided by the reconfigured radar system can be very useful in this case, but it also leads to a number of problems.

First of all, by reconfiguring the radar system, the 'normal' radar view of the ships in the harbor is compromised: the spatial resolution will go down, making it harder to distinguish different ship sizes. Part of the harbor may not be visible at all. This might be acceptable in a crisis situation, but it does lead to another issue: Who decides if the radar system may be reconfigured, and under which circumstances? Is the fire brigade in charge or the police? Or perhaps the port authorities or the government? Clear policies need to be defined for this, policies that can become more complex as the sensor systems' reconfigurable functionality increases. Although the aim is to be almost instantaneously reconfigurable, initial versions of the technology will be likely to need some processing time for each reconfiguration. This can be crucial in crisis situations: during reconfiguration sensors cannot be used, leaving the control center in essence blind to the current situation. This may be acceptable if reconfiguration time is in the range of fractions of seconds, but longer delays may compromise the functionality of the technology.

All these issues stem from the same core problem: reconfigurable systems have more functionality than normal systems, but they cannot use the added functionality concurrently: One can either search for ships or for low flying planes, not both (at the same time).

CHALLENGES RAISED BY RECONFIGURABILITY

An important aspect of reconfigurability is that it challenges the type of stable, knowable, unambiguous function ascriptions to artifacts and systems. In that sense, it may ask for an extension of existing theories of technical functions. (Houkes & Vermaas, 2010)

This bears on the principle of informed consent. A prerequisite of that principle is a knowable impression of what the system will do under which circumstances. One can argue that this prerequisite is hard to fulfill for many of today's (socio-technological) systems, as they are developed for a certain goal, but once in place, easily combined with other functionalities, e.g. in the sense of *function creep*. But the issue is even more prominent if the system is intended to be reconfigurable to changing circumstances, and maybe even fit for yet unthought of functionalities. At which level can the system's behaviour be specified for people subject to it, and is that enough of a basis for them to be able to consent or as a basis to justifiedly assume their consent.

The specification of the behaviour of the system requires a sophisticated and complex balancing of the different goals the different functionalities of the technology serves. Combining technology for multiple-functionality into one sensor, adds the restriction that only one functionality at a time can be actually used: as mentioned above, the functionality may not be usable concurrently. This means that more crucially than usual, priorities of the different functionalities must be assigned. This adds an extra dimension to the design process: the specification of priorities.

The observations above show that the reconfigurability leads to an increased range of choices that need to be made. These choices address not only practical aspects, but more essentially higher order choices: who will be in control of such (practical) choices? who will bear responsibility for the different functionalities, or for the system as a whole? This indicates that the development of policies around reconfigurable systems will bring in new complexities. Such complexity may compromise the expected efficiency of reconfigurability.

Although the initial use case for the reconfigurable sensor networks is not primarily related to the observation of persons and their behaviour, we deem it useful to look at the ethical issue related to sensor networks like camera surveillance and RFID access control systems. There is extensive literature discussing how sensor networks for observation of individuals and their environment bring up issues concerning privacy and the protection of personal data, e.g. (Chan & Perrig, 2003) (Shi & Perrig, 2004) (Hoven J. v., 2008) (Solove, 2008). Despite the fact that the described use case for the reconfigurable sensor networks does not center around privacy, we expect that the technology may in the future be applied in privacy sensitive ways. But besides that, we argue that central notions from the discussion of privacy may be helpful in the analysis of reconfigurability.

Reconfigurability puts the context of use and control of information, captured in notions like ‘spheres of justice’/‘spheres of access’ (Hoven M. J., 1999) (Nagenborg, 2009) and ‘contextual integrity’ (Nissenbaum, 2010), even more crucially at the heart of the challenge put forward by privacy. For example, Nissenbaum understands privacy in terms of context-relative information norms, and distinguishes norms of appropriateness, and norms of distribution. She defines contexts as “structured social settings, characterized by canonical activities, roles, relationships, power structures, norms (or rules), and internal values (goals, ends, purposes).” Most relevant to the framework of Contextual Integrity are the roles, activities, norms and values. (Nissenbaum, 2010, p.132-134). For reconfigurable systems there may be different roles, activities, norms and values that need to be combined in the design of one system. How to deal with the composition of these different contexts for one system is a particular challenge.

DESIGN FOR VALUES IN RECONFIGURABLE SENSOR NETWORKS

Reconfigurability involves applicability of one system with multiple functionality in possibly distinct contexts. In the case of reconfigurable sensor networks, the challenge will be to formulate requirements that are both general and specific enough to cover each possible use. For example, how to balance privacy issues if the sensor system monitors individuals only in very few of its configurations? And how to go about changes in this configuration?

Nissenbaum's framework for Contextual Integrity provides explanation, evaluation and prescription, and thereby contributes to the design process. However, it does not “support substantive descriptions for general families of technologies”, and “the most fruitful assessments take place within particular contexts”. (Nissenbaum, 2010, p.190) In the case of reconfigurable systems, the particular context may be underspecified, or only one of a vast number of possible contexts. Therefore, a specific challenge for design for values of reconfigurable technology, like the sensor networks, requires an analysis of the composition and interaction of different contexts.

CONCLUSION

Reconfigurability of sensors in networks seems to be an attractive answer to the increasing and unvariably changing demands in the security and crisis management domain, both in terms of economy and of effectivity. In this paper, we have presented an initial exploration of the challenges reconfigurability may add in the ethical analysis of technology. In the coming years, we will develop a more thorough analysis of the concept. It will be interesting to see how reconfigurability can be analyzed from the perspective of the literature on function ascriptions. We believe that a proper analysis and definition of context and spheres will be crucial in the ‘design for values’ of such technology, and essential for understanding its effect.

BIBLIOGRAPHY

Ackerman, M., Darrell, T., & Weitzner, D. (2001). Privacy in context. *Human-Computer Interaction, 16*, 167-176.

Chan, H., & Perrig, A. (2003). Security and privacy in sensor networks. *IEEE Computer, 36* (10), 103-105.

Guo, Yuanqing (2006). *Mapping applications to a coarse-grained reconfigurable architecture*. PhD-thesis, University of Twente.

Houkes, W., and P.E. Vermaas (2010) Technical Functions: On the Use and Design of Artefacts, vol. 1 of *Philosophy of Engineering and Technology* (Dordrecht: Springer).

Hoven, J. v. (2008). Information Technology, Privacy, and the Protection of Personal Data. In J. v. Hoven, & J. Weckert (Eds.), *Information Technology and Moral Philosophy* (pp. 301-321). Cambridge University Press.

Hoven, M. J. (1999). Privacy or informational injustice? In L. Pourcia (Ed.), *Ethics and information in the twenty-first century* (pp. 140-150). Purdue University Press.

Nagenborg, M. (2009). Designing spheres of informational justice. *Ethics and Information Technology , 11* (3), 175-179.

Nissenbaum, H. (2010). *Privacy in Context.* Stanford University Press.

Shi, E., & Perrig, A. (2004). Designing Secure Sensor Networks. *Wireless Communications, 11* (6), 38-43.

Solove, D. J. (2008). *Understanding Privacy.* Harvard University Press.

STARS. (2010, July). Project Information. Retrieved from STARS-Project website: http://starsproject.nl/

BIOGRAPHY

Francien Dechesne studied foundations of mathematics, with a minor in philosophy, and wrote her PhD-thesis in the field of mathematical logic. She then continued to do research in the field of computer science, on the topic of proving with computer assistance, and verification of computer security using modal logic. Since 2009, she is affiliated to the 3TU Centre for Ethics and Technology, with a special interest in specification and verification of non-functional requirements for information technology, and more generally, *design for values* in socio-technical systems.

Jeroen van den Hoven is professor of Moral Philosophy at Delft University of Technology. He is Scientific Director of the Centre for Ethics and Technology of the Three Technical Universities in The Netherlands and Editor in Chief of Ethics and Information Technology (Springer). He has published numerous articles, books on Ethics and ICT and has been advisor to the Dutch Government in various roles.

Martijn Warnier is an Assistant professor in the Systems Engineering Section within the Faculty of Technology, Policy and Management, Delft University of Technology. He holds a PhD in Computer Science from the Radboud University Nijmegen. After focusing on security of embedded systems, his current research is on self-management of dynamic distributed systems, in particular on security aspects involved. He has studied security in many areas with a specific interest for robust systems in highly dynamic distributed environments.