Verification of Pervasive Systems*

Savas Konur and Michael Fisher*
*Department of Computer Science, University of Liverpool, Liverpool L69 3BX
{konur, mfisher}@liverpool.ac.uk

1 Introduction

Pervasive computing refers to a general class of mobile systems that can sense their physical environment, i.e., their context of use, and adapt their behaviour accordingly. Pervasive systems live around us providing services to the inhabitants of a home, the workers of an office or the drivers in a car park. We know that requirements for current and future pervasive systems involve a great diversity of types of services [6], such as multimedia, communication or automation services.

The success of pervasive computing depends crucially on verifying interoperability requirements for the interaction between the devices and their environment. These requirements introduce an important layer of abstraction because they allow modularity in the verification process: it suffices to show that each mobile device or fixed component meets the interoperability requirements, and that the interoperability requirements entail the desired high-level properties, such as "Are visitors properly prevented from accessing confidential information on our wireless network?"

Our focus is on the verification of designs; in particular we focus on the design of basic component behaviours and the protocols which dictate access to them and interaction between them. It is important to note that our intention is not to develop pervasive computing systems as such, but rather to draw motivation from, and test our ideas in, a number of planned and existing pervasive systems.

The project brings together qualitative techniques, including deductive methods, model checking, and abstraction methods, with quantitative techniques, including probabilistic and performance analysis, in order to tackle the problem of verifying pervasive systems. Working together, we aim to make a step change in verification technology by developing novel techniques and learning which techniques are most effective in different contexts. We will be investigating problems which are both new and challenging (hence new techniques and methods will be required), but are still sufficiently close to existing work that our established techniques provide a solid foundation for solving them. The outcomes will directly benefit system designers and, indirectly, end users. They will include techniques applicable to a wide range of application domains, and results and lessons learned from three specific applications including a message forwarding system, a homecare system and RFID system infrastructure.

2 Case Studies

The formal techniques are used to verify the consequent interoperability requirements, and their effectiveness is evaluated through some case studies, which include a message forwarding system - *Scatterbox* [4], a home-care application - *MATCH* [3] and underlying *RF technology* [1]. These systems are briefly described as follows:

The Scatterbox system has been designed to serve as a test bed for context-aware computing in a pervasive computing environment. It provides a content-filtering service to its users by forwarding relevant messages to their mobile phone. The user's context is derived by tracking his/her location and monitoring his/her daily schedule. As messages arrive, Scatterbox forwards them to subscribed users provided the user's available context suggests they are in a situation where they may be interrupted.

MATCH is an event driven home-care system. An event is a requirement that when a given condition is met the system takes appropriate action. Typical examples of events include: "if the front door is left open and nobody is downstairs, then send a message to a stakeholder", "if the lights are left on and nobody is in the house, then turn the lights off", "If Bill is laid down but not in bed, then contact Gill", etc. The MATCH system consists of a set of components and a set of users. The set of components can be split into 4 main categories: *sensors*, *alert triggers*, *tasks* and *outputs*.

Radio frequency (RF) technology is used in many applications for automated indentification of objects or people. A RF system consists of two main components: RF chips and RF readers. RF chips are small microchips supporting wireless data transmission. Data is stored (remotely or not) in the RF chip and can remotely be retrieved by a RF reader. RF chips can be incorporated into products, animals, or people for the purpose of identification and tracking using radio waves.

*Work is part of an ongoing project on "Verifying Interoperability Requirements in Pervasive Systems", funded by EPSRC (EP/F033567) and involving collaboration with the universities of Birmingham and Glasgow.

RF readers query these chips for some identifying information about the objects to which chips are attached. Current and emerging applications using this technology include amongst others electronic toll collection, documents such as electronic passports and visas, and RF passes for public transportation.

Our case studies will be drawn from three layers typical within pervasive systems: *individual component*, *protocols between individual components* and *information access*.

The interoperability of components depends on the components exhibiting the right behaviour as individuals. We will identify the relevant properties, and formulate them using logic-based languages (such as temporal and first-order logics and model-checking languages). We aim to develop specific approaches to describing behavioural requirements for trusted pervasive computing components. The protocols between individual components will include application-level protocols specific to the case studies (for example, protocols related to the chemotherapy sensors and mobile equipment), as well as low-level protocols of authentication and data distribution. We will formalise the expected properties of the protocols for later analysis using some process algebra languages. The case studies will identify issues and problems of access control (typically what component or group of components has the right to access a certain resource in a pervasive computing infrastructure) and privacy. We will develop and refine models of access control systems, and techniques for proving properties about them. We will also identify the deficiencies of the languages and their ability to scale up for pervasive computing.

3 Formal Verification

After specifying the requirements of the use cases with a suitable formal language, we will develop suitable technologies to verify these requirements formally. Current state of the art formal methods appear incapable of coping with the verification demand introduced by pervasive systems, because reasoning about such systems requires combinations of multiple dimensions such as quantitative, continuous and stochastic behaviour to be considered, and requires proving properties which are quite subtle to express. In order to tackle the challenge of pervasive system verification, the project aims to leverage the power of established techniques, notably

model checking, a logic-based approach to analysing properties of state-based systems. There has been work (some of which was carried out by the investigators) on extensions such as *parametrised model checking, infinite state model checking* and *probabilistic model checking*, and this will be developed further within the project.

using deduction and abstraction, two closely linked, approaches that can be used either to reduce the verification problem to a scale suitable for model checking, or to tackle the larger problem directly.

process calculi allowing high level descriptions of interaction, communication and synchronisation.

Part of our effort will involve pushing each technique further, but the majority of it will be on *pushing the combination*, i.e. bending and synthesising techniques such as [2, 5] to make them give meaningful results in our case studies.

References

[1] url=http://en.wikipedia.org/wiki/RFID.

[2] R. H. Bordini, L. A. Dennis, B. Farwer, and M. Fisher. Automated verification of multi-agent programs. In *Proc. 23rd IEEE/ACM Int. Conf. Automated Software Engineering (ASE)*, pages 69–78, 2008.

[3] J. S. Clark and M. R. McGee-Lennon. Match: Mobilising advanced technologies for care at home. Poster at *Delivering Healthcare for the 21st Century*, Glasgow, 2007.

[4] S. Knox, A. K. Clear, R. Shannon, L. Coyle, S. Dobson, A. Quigley, and Paddy Nixon. Scatterbox: Mobile message management. *Journal Revue d'Intelligence Artificielle*, 22, 2008.

[5] S. Konur. A decidable temporal logic for events and states. In *Proc. 13th International Symposium on Temporal Representation and Reasoning (TIME)*, pages 36–41. IEEE, 2006.

[6] R. Want, T. Pering, G. Borriello, and K.I. Farkas. Dissapearing hardware. *Pervasive Computing*, 1, 2002.