Validation Of A Distributed ‘SmartSpace’ Architecture Through Simulation

Ian Oliver
Nokia Research Center
Itämerenkatu 11-13
Helsinki
Finland

Summary. The use of formal methods in software and systems development has advantages but often suffers from difficulty in applying such methods and the visualisation of the results. We show here that the use of a light-weight formal specification language - Alloy - and the use of simulation traces similar to that of scenario explorations with object-diagrams in UML can be effective in understanding the behaviour of such systems at analysis and design-times.

Keywords: Simulation, Validation, Formal Specification, Alloy

1 Introduction

The abundance of personal, mobile devices such as mobile phones or laptop computer with significant computational power, large memories - both temporary and persistent, multi-tasking operating system and with high-speed wireless communication facilities such as UMTS, WLAN and Bluetooth provides the potential for a sophisticated, distributed computation environment which we term a ‘SmartSpace’ [24]. Based loosely upon the original Linda communication model, blackboard architectures and now Tuple-spaces based computation environments [27] have been researched and developed for an extensive period of time. Indeed some of the principles can be found in communication models such as Linda and also in some sophisticated AI work. Later blackboard architectures have been proposed as models for agent systems and suggested as bases for Semantic Web [4] architectures [18]. While there exist a number of blackboard and tuple-space based architecture implementations it is only now with the advent of high-speed data transfer mobile communications and the ubiquity of mobile [25] and embedded devices with the addition of semantic web capabilities (cf: semantic gadgets and infrastructure [19]) that these types of system can start to be fully exploited.
We have developed [24] an architecture based upon an augmented blackboard system for the linking together of processes running upon various mobile devices though the notion of a ‘knowledge space’ (cf: [14]) in a dynamic semantic web context. The blackboard model is augmented to provide a publish-subscribe mechanism with the notion of passing facts (items of knowledge) rather than messages. This provides us with an implicit communication method. The motivation for this work was to investigate the provision of information sharing between heterogeneous clusters of devices (including mobiles).

We chose to use as the development method for this particular system a pragmatic formal approach using the Alloy specification language [23]. Alloy was chosen for the ease of use, its ability to specify dynamic systems and its suitability for producing execution traces and analyses which are more akin to how many engineers visualise a system. In addition the Alloy language has a closer semantic correspondence with defacto standard languages such as the ubiquitous UML [9,2,11]. In some previous projects have used languages such as B in isolation for the development of such systems with varying results [22] due to the strictness of the B-Method approach.

In this paper we describe our ‘Smart Space’ system concepts through the use of a domain modelling approach and formalisation in Alloy along with various simulations of the operations of that system. We then make discussion on the validation of the demarcation or policy structure used in that system and following this describe how these models are integrated and simulated.

2 Smart Space Domain Model

The SmartSpace System provides a method for concurrently running agent-like processes known as Nodes to interact with SmartSpaces which provide publish-subscribe mechanisms across a space-based communication environment in which are contained facts represented using the Resource Description Framework (RDF). Figure 1 shows the structure of this described using the UML class diagram notation. Applications are constructed from dynamic combinations of Nodes at design and run-times across multiple, heterogeneous devices. Nodes interact with the SmartSpace through Sessions which provide facilities for the Node to add and remove facts and also subscribe and query for patterns of facts. Sessions can also provide additional pre/post-processing of the information as well as other functionalities relates to encryption and security. They also are used to hide the underlying communication mechanisms and technologies. The SmartSpace itself manages the facts and input and requested for by the Nodes. These facts however are pieces of information which means that the normal rules of message passing as one normally sees in a Linda-type system do not apply - communication here is through implicit communication as a form of publish/subscribe. Typically in a Linda system the messages are either unordered (set based) or ordered (queue based) with duplication