MISCELLANEOUS CASE STUDIES — First Year Report

UT, all CRs

May 25, 2003

AMETIST DELIVERABLE 3.5.1

Project acronym: AMETIST
Project full title: Advanced Methods for Timed Systems
Project no.: IST-2001-35304

1 Introduction

This is the AMETIST first year's deliverable of Task 3.5 on Miscelleneous Case Studies. This Task has been created to collect and publish internal case studies of the CRs pertinent to the AMETIST project.

At the AMETISTplenary meeting of September 2002 it was decided that priority should be given to work on the project case studies linked to the AMETIST associate partners reported under Tasks 3.1–3.4. Although most of the project's resources have consequently been directed to these Tasks, a number of internal case studies have been carried out in addition to the prioritized case studies in the past year. They are reported in this deliverable.

A substantial part of the reported work has been funded from other sources than the AMETIST project, but all of the reported work is strongly related to AMETIST in terms of application area or techniques and tools used, as well as the involved researchers. It is expected that the work on these internal case studies will be relevant for the remaining two years of AMETIST.

2 Internal Case Studies

2.1 A Broadcast Communication Protocol

There are many situations in which one would like to use the Internet Protocol for local communication, for instance in the setting of in home digital networks or to establish communication between laptops. For these type of applications one would like to have a plug-and-play network in which new hosts automatically configure an IPv4 address. In [ZV03] a protocol is studied that has been proposed by the IETF to achieve this. Within this protocol a host needs 8 or 10 seconds to get an IP address, which is too long for users in the real world. And even after such a long waiting time it may occur that two hosts configure the same IP address. So how to improve the performance is a meaningful work. This protocol is formally specified as a network of timed automata, and the Uppaal toolset is used to verify some properties. From a modelling perspective our case study is interesting since it involves the modelling of broadcast communication. The goal of the analysis focuses on two points: (1) no two hosts can have the same IP address (2) a host spends less time to acquire a new IP address. Some parametric constraints are given to achieve this goal. Even though full analysis of this protocol clearly requires a model in which probabilistic information can be incorporated, some interesting correctness properties can be established, even in a setting with more than 2 hosts. Due to state space explosion, Uppaal cannot explore the complete state space of the unrestricted model for more than two hosts. Thus this case study presents a clear challenge for the timed model checking community.

2.2 IPv4 Zeroconf Protocol

In [BSHV03] the trade-off is investigated between reliability and effectiveness for the IPv4 Zeroconf protocol, proposed by Cheshire/Adoba/Guttman in 2002, dedicated to the self-configuration of IP network interfaces. Although this protocol in its original setting does not have (soft) real-time features, the problem can be addressed fruitfully using techniques that fit the AMETIST paradigm. A simple stochastic cost model of the protocol is constructed, where reliability is measured in terms of the probability to avoid an address collision after configuration, while effectiveness is viewed as the average penalty perceived by a user. An analytical expression for the user penalty is derived, which is used to obtain optimal configuration parameters of the network, restricting to those parameters which are under the control of a consumer electronics manufacturer. In particular it is show that minimal cost and maximal reliability are qualities that cannot be achieved at the same time.

2.3 Asynchronous Circuit Verification

In [BJMY02] the timing verification tool OpenKronos, which is based on timed automata, is used to verify correctness of numerous asynchronous circuits. The desired behavior of these circuits is specified in terms of signal transition graphs (STG) and it is checked whether the synthesized circuits behave correctly under the assumption that the inputs satisfy the STG conventions and that the gate delays are bounded between two given numbers. The results demonstrate the viability of the timed automaton approach for timing analysis of certain classes of circuits.

References

[BJMY02] M. Bozga, H. Jianmin, O. Maler, and S. Yovine. Verification of asynchronous circuits using timed automata. In *Proceedings of TPTS'02 Workshop*. Elsevier, April 2002.

[BSHV03] H. Bohnenkamp, P. van der Stok, H. Hermanss, and F.W. Vaandrager. Cost-optimisation of the IPv4 zeroconf protocol. In *Proceedings International Performance and Dependability Symposium (IPDS),* San Fransisco. IEEE CS Press, June 2003. To appear.

[ZV03] M. Zhang and F.W. Vaandrager. Analysis of a protocol for dynamic configuration of IPv4 link local addresses using Uppaal. Report NIII-R03XX, Nijmeegs Instituut voor Informatica en Informatiekunde, University of Nijmegen, 2003. To appear.