Available online at www.sciencedirect.com
ScienceDirect
Electronic Notes in Theoretical Computer Science
ELSEVIER
Electronic Notes in Theoretical Computer Science 240 (2009) 221–238
www.elsevier.com/locate/entcs

A TLA+ Formal Specification and Verification of a New Real-Time Communication Protocol

Paul Regnier [1,2] George Lima [3] Aline Andrade [4]

Distributed Systems Laboratory (LaSiD)
Department of Computer Science (DCC)
Federal University of Bahia (UFBA)
Cep 40.170-110, Salvador, Bahia, Brazil

Abstract

We describe the formal specification and verification of a new fault-tolerant real-time communication protocol, called *DoRiS*, which is designed for supporting distributed real-time systems that use a shared high-bandwidth medium. Since such a kind of protocol is reasonably complex and requires high levels of confidence on both timing and safety properties, formal methods are useful. Indeed, the design of *DoRiS* was strongly based on formal methods, where the TLA+ language and its associated model-checker TLC were the supporting design tool. The protocol conception was improved by using information provided by its formal specification and verification. In the end, a precise and highly reliable protocol description is provided.

Keywords: Formal Specification, Verification, TLA+, Real-Time Protocol

1 Introduction

New automation and control systems are characterized by the need of high levels of flexibility and service integration in addition to their usual requirements such as fault tolerance and predictability. This has motivated the development of new communication protocols based on high-bandwidth medium, such as Ethernet or Wireless. Interested readers can find good surveys on this topic [4,6,12].

Since designing is a reasonable complex task, the use of formal methods plays an important role to guarantee correct design and reliable implementation. Motivated by noticeable advances in the field [3,7], formal methods have increasingly been

[1] This work has received funding support from the Brazilian funding agencies CNPq (Grant number 475851/2006-4) and FAPESB (Grant number 7630/2006).

[2] Email: pregnier@ufba.br

[3] Email: gmlima@ufba.br

[4] Email: aline@ufba.br

doi:10.1016/j.entcs.2009.05.054

applied in the study and verification of many of these communication protocols [9,13,1,5], some of which with real-time characteristics.

Presenting the case study of the specification and verification of a new real-time communication protocol, called *DoRiS* (a Double Ring Service protocol for Real-Time Systems), we illustrate how formal methods can help the design of the protocol as well as its implementation. We have used here the Temporal Logic of Actions and its associated language TLA+ [10]. Our choice of TLA+ to specify and verify *DoRiS* was motivated by the following reasons. TLA+ provides a modular structure which allows for an incremental process of specification refinements, according to the abstraction level required. Thus, a concrete specification, close to the code level, can be achievable. Also, the TLC model-checker provides an automatic verification of the specification and its properties. Hence, the use of TLA+ has allowed us to carry out both the conception and the specification of *DoRiS* interactively and progressively as an integrated software engineering process. We present here the final specification and model-checking of *DoRiS*, which has been successfully used as a basis for the protocol implementation on a Linux-based real-time platform [14].

The remainder of this paper is structured as follows. The protocol is outlined in Section 2. Section 3 gives our modeling assumptions and some initial concepts on TLA+ before addressing the description of the specification itself. Some relevant properties of *DoRiS* are shown by formal verification. They are commented upon Section 4. In Section 5, we also comment on how the formal specification has been useful during the design of *DoRiS*. Conclusions are drawn in Section 6.

2 The DoRiS protocol

DoRiS is a deterministic protocol built on top of a shared medium communication layer. The protocol works as a logical layer, extending the MAC and LLC layer [8]. It is designed to support hybrid systems where industrial sensors, actuators and controllers share the communication network with other soft applications. In such a hybrid configuration, the processing speed and the communication characteristics of the two types of application may differ considerably [2]. Thus, we assume that a number of industrial appliances (micro-controllers, sensors etc), called hereafter *slow* nodes, have low processing times when compared to *fast* nodes such as workstations.

2.1 The model and terminology

The set of nodes (slow or fast) connected through a shared medium make up a *DoRiS* segment. Although many *DoRiS* segments can be inter-connected by switches or routers, we will restrict our specification and verification to a single *DoRiS* segment.

At each node, a server is responsible for the transmission of hard real-time and best-effort messages. Slow nodes send only hard real-time messages and fast nodes may send both hard and best-effort messages. Each server maintains a hard queue, which stores hard real-time messages to be sent. Fast servers also maintain a soft queue, which stores outgoing best-effort messages. Although there is only a single server in each node, we define $HardServ[i]$ and $SoftServ[i]$, the two server threads