COMMUNICATION PROTOCOL SPECIFICATION AND VERIFICATION

THE KLUWER INTERNATIONAL SERIES IN ENGINEERING AND COMPUTER SCIENCE

COMMUNICATION PROTOCOL SPECIFICATION AND VERIFICATION

by

Richard Lai
La Trobe University
Melbourne, Australia

Ajin Jirachiefpattana
Prince of Songkla University
Songkhla, Thailand

SPRINGER SCIENCE+BUSINESS MEDIA, LLC

ISBN 978-1-4613-7537-1 ISBN 978-1-4615-5549-0 (eBook)
DOI 10.1007/978-1-4615-5549-0

Library of Congress Cataloging-in-Publication Data

A C.I.P. Catalogue record for this book is available
from the Library of Congress.

Printed on acid-free paper.

This book is dedicated by
Richard Lai to his wife, Freda,
and three daughters: Debbie,
Jasmine and Amelia;

and by Ajin Jirachiefpattana to
his wife, Waraporn, and his
daughter, Nidjaree.

Contents

List of Figures

List of Tables

Preface

Communication protocols are rules whereby meaningful communication can be exchanged between different communicating entities. In general, they are complex and difficult to design and implement. Specifications of communication protocols written in a natural language (e.g. English) can be unclear or ambiguous, and may be subject to different interpretations. As a result, independent implementations of the same protocol may be incompatible. There is, therefore, a need for precise and unambiguous specification using some formal languages. In addition, the complexity of protocols makes it very hard to analyse in an informal way.

Many protocol implementations used in the field have almost suffered from failures, such as deadlocks. When the conditions in which the protocols work correctly have been changed, there has been no general method available for determining how they will work under the new conditions. It is necessary for protocol designers to have techniques and tools to detect errors in the early phase of design, because the later in the process that a fault is discovered, the greater is the cost of rectifying it.

Protocol verification is a process of checking whether the interactions of protocol entities, according to the protocol specification, do indeed satisfy certain properties or conditions which may be either general (e.g., absence of deadlock) or specific to the particular protocol system directly derived from the specification.

In the 80's, an ISO (International Organisation for Standardisation) working group began a programme of work to develop fromal languages which were suitable for Open Systems Interconnection (OSI). This group called such languages Formal Description Techniques (FDTs). Some of the objectives of ISO in developing FDTs were: enabling unambiguous, clear and precise descriptions of OSI protocol standards to be written, and allowing such specifications to be

verified for correctness. There are two FDTs standardised by ISO - LOTOS and Estelle.

This book is written to address the two issues discussed above: the needs to specify a protocol using an FDT and to verify its correctness in order to uncover specification errors in the early stage of a protocol development process. The readership primarily consists of advanced undergraduate students, postgraduate students, communication software developers, telecommunication engineers, EDP managers, researchers and software engineerers. It is intended as an advanced undergraduate or postgraduate text book, and a reference for communication protocol professionals.

Contents

Part I: Protocol Specification

Chapter 1 gives an introduction to communication protocols, the ISO reference model, layering concepts, and protocol specification. Then the specification of the Sliding Window and the ISO ACSE protocols are described.
Chapter 2 describes the need for formally specifying communication protocols, gives an introduction to Formal Description Techniques and outlines the different types of FDTs.
Chapter 3 gives a detailed description of Estelle and the uses of Estelle in specifying the Sliding Window and the ACSE protocols.
Chapter 4 presents LOTOS and the uses of LOTOS in specifying the Sliding Window and the ACSE protocols.
Chapter 5 describes SDL and the uses of SDL in specifying the Sliding Window and the ACSE protocols.

Part II: Protocol Verification

Chapter 6 gives an introduction to protocol verification, the most commonly used techniques and the major difficulty - the state space explosion problem.
Chapter 7 presents the principles of Estelle verification. This is followed by a survey of some of the Estelle verification methods.
Chapter 8 describes an approach based on Numerical Petri Nets (NPNs) for modelling Estelle.
Chapter 9 describes a software environment, EVEN (Estelle Verification Environment using NPNs), which facilitates the automatic verification of communication protocols specified in Estelle.
Chapter 10 presents a method to address the well-known state space explosion problem and its algorithm which is implemented in EVEN.

Chapter 11 describes the results of using EVEN for the verifications of the Estelle specifications of the Sliding Window and the ISO ACSE protocols.

RICHARD LAI

AJIN JIRACHIEFPATTANA

Acknowledgments

We would like to thank NIST of the US Department of Commerce for making Pet and Dingo and Telecom Australia for making PROTEAN available to us for the work on protocol verification, and the Australian Research Council for the financial support under the grant A49601203 for a part of the work on specification and implementation described in this book.