The Pandora System: An Interactive System for the Design of Data Communication Protocols

Gerard J. Holzmann
Delft University of Technology, P.O. Box 5, 2600 AA Delft, The Netherlands

PANDORA is an interactive system for the analysis, synthesis, and real-time assessment of data communication protocols. The Pandora system is being developed at the Delft University of Technology in cooperation with the Dr. Neher Laboratories of the Netherlands PTT. This paper gives an overview of the structure of the system and discusses the main design goals.

Keywords: automated protocol validation, deadlock detection, validation algebra, protocol synthesis, protocol assessment.

Gerard J. Holzmann was born in Amsterdam, The Netherlands, in 1951. He received the B.S. (1973) and M.S. (1976) degree in electrical engineering, and the Ph.D. (1979) degree in technical sciences from the Delft University of Technology in The Netherlands. He obtained a Fulbright Fellowship in 1979. From September 1979 to June 1980 he was with the University of Southern California in Los Angeles. From June 1980 to June 1981 he worked at the Computing Science Research Center of Bell Laboratories in Murray Hill. Dr. Holzmann is now an assistant professor at the Delft University of Technology. In Oct. 1981 he was awarded the Prof. Bähler prize by the Royal Dutch Institute of Engineers (KIVI) for his research on telecommunication systems.

North-Holland
Computer Networks 8 (1984) 71–79

1. Introduction

Data communication protocols are used to formalize the interactions in distributed computer systems [10,11]. The protocols take care of such issues as routing, flow control, error recovery, and connection establishment. A badly designed protocol can degrade a system's performance significantly, it can introduce errors, and it may even surprise its users by bringing their system to a complete standstill at the occurrence of certain unexpected combinations of events. Such occurrences are almost always time-dependent and thus very hard to trace.

So, protocols are an important part of distributed systems. But, "good" protocols, that is: protocols with provable properties and with measurable real-time characteristics, turn out to be extremely hard to design.

The Pandora system, an acronym for "interactive system for Protocol ANalysis, Design and OpeRation Assessment," aims to provide the protocol designer with a set of tools that can facilitate this task.

The Pandora system consists of three major parts: analysis, synthesis, and real-time assessment.

(1) In protocol analysis we form an algebraic model of a protocol and prove its consistency, completeness, and freedom from deadlocks.

(2) In protocol synthesis we try to guide a protocol designer to a description that is succinct, complete, and correct.

(3) In protocol assessment we measure the real-time characteristics of protocols.

Each of the following sections will describe a small part of this Pandora system.

In section 2 we give a general overview of the hardware and software configuration. Section 3 describes the protocol validation method. In section 4 we discuss protocol synthesis guidance. Section 5 describes the design of the network simula-