A Nitpick Analysis of Mobile IPv6

Daniel Jackson[a] Yuchung Ng[b] Jeannette M. Wing

March 1998

CMU-CS-98-113

[a]MIT Lab. for Computer Science, 545 Technology Square, Cambridge, MA 02139
[b]Computer Science Department, Cornell University, Ithaca, NY 14853

School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213

This paper was submitted to *Formal Aspects of Computing*, September 1997, and is based on work done while the first and second authors were at Carnegie Mellon University.

This research is sponsored in part by the Defense Advanced Research Projects Agency and the Wright Laboratory, Aeronautical Systems Center, Air Force Materiel Command, USAF, F33615-93-1-1330, and Rome Laboratory, Air Force Materiel Command, USAF, F306602-97-2-0031, and in part by the National Science Foundation under Grant No. CCR-9523972. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright annotation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Defense Advanced Research Projects Agency Rome Laboratory or the U.S. Government.

Keywords: partial specifications, model checking, Nitpick/NP, mobile internetworking protocols, IPv6

Abstract

A lightweight formal method enables partial specification and automatic analysis by sacrificing breadth of coverage and expressive power. By design, NP is a specification language that is a subset of Z and Nitpick is a tool that quickly and automatically checks properties of finite models of systems specified in NP. We used NP to state two critical acyclicity properties of Mobile IPv6, a new internetworking protocol that allows mobile hosts to communicate with each other. In our Nitpick analysis of Mobile IPv6 we discovered a flaw in a 1996 version of the design: one of the acyclicity properties does not hold. It takes only two hosts to exhibit this flaw. This paper gives self-contained overviews of Mobile IPv6 and of NP and Nitpick to understand the details of our specification and analysis.