UNDERSTANDING SIP THROUGH MODEL-CHECKING

Pamela Zave

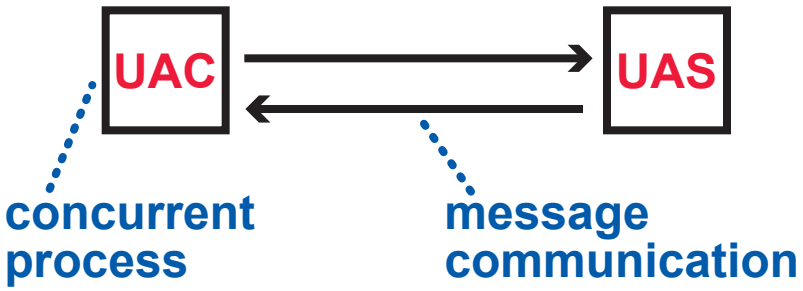
AT&T Laboratories—Research

Florham Park, New Jersey USA

OVERVIEW

MODELING

- wrote formal models of SIP INVITE dialogs in Promela



- the models have a special emphasis on media control (offer/answer exchange)
- limitations and simplifications are documented carefully
- all versions of the model are available on my Web site

ANALYSIS

- analyzed the models using the model-checker Spin

  verification of embedded assertions, completeness in the sense of being responsive to all inputs, etc.

- discovered a few problems in the SIP RFCs
- collected data on the analysis of several model versions
- made some recommendations

WHY?

Because there are thousands of pages of RFCs, scattered with rules such as:

"The UAS MUST NOT send a second reliable provisional response until the first is acknowledged."

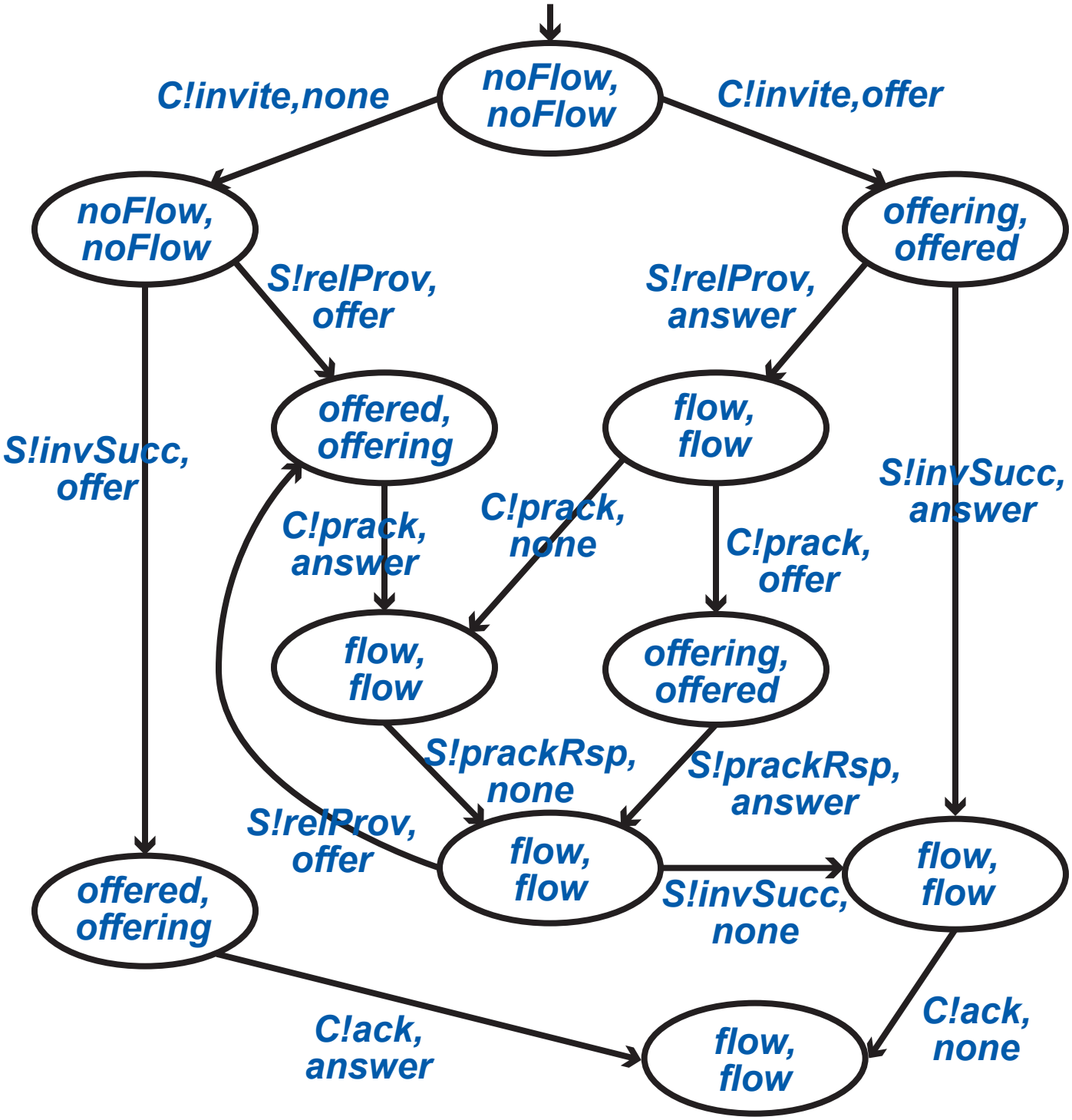
A state-oriented model pulls many of these rules together in this form:

WHY?

Because there are thousands of pages of RFCs, scattered with rules such as:

"The UAS MUST NOT send a second reliable provisional response until the first is acknowledged."

A state-oriented model pulls many of these rules together in this form:



Reliable provisional responses must be handled in exactly this way.

This state-oriented view has many advantages as supplementary documentation of SIP:

- centralized, rather than distributed over RFCs
- formal, and therefore unambiguous
- can be checked automatically
- shows the state information that user agents must maintain
- can be used for other purposes such as testing