М. В. Баклановский[1], А. С. Игумнов[2], В. С. Самунь[1]

[1]*Уральский государственный университет им. А. М. Горького,*
[2]*Институт математики и механики УрО РАН, Екатеринбург*

Верификация протокола TCP+

При разработке протоколов всегда возникает проблема проверки отсутствия ошибок. Ошибками в данном случае считаются несоответствия требований, предъявляемых к протоколу и его реализации. Для того чтобы осуществить проверку отсутствия ошибок, нужно формально описать требования, которые предъявляются к протоколу, и проверить, что протокол удовлетворяет всем требованиям.

Процесс проверки можно осуществить полным перебором всех состояний модели, но при этом возникает проблема комбинаторного взрыва и на практике такой подход неприменим. Вместо этого используют другой подход.

Рассмотрим процесс верификации подробней. Для того чтобы описать верифицируемую модель (протокол, программа), используются модели Крипке. Модель Крипке — размеченный орграф переходов: вершинами графа являются состояния модели, ребрами – возможные переходы между состояниями. Каждая вершина графа помечается множеством свойств, которые выполняются в соответствующем состоянии. При этом степень исхода каждой вершины должна быть ненулевой. Требования, предъявляемые к модели, описываются на языке темпоральных логик. Темпоральные логики позволяют описывать последовательности переходов между состояниями модели. Далее задача верификации сводится к проверке выполнимости формулы темпоральной логики на модели Крипке. Существует автоматическая система такой проверки — система SPIN. SPIN позволяет верифицировать модели, требования к которым записаны с помощью формул линейной темпоральной логики (LTL). Для того чтобы произвести верификацию, SPIN строит по формулам LTL автомат Бюхи (разновидность автомата над бесконечными словами) и проверяет, что пересечение модели Крипке и автомата Бюхи пусто. Если пересечение непусто, то это означает, что требование не выполняется на модели, и строится контрпример.

SPIN был применен для верификации протокола TCP+. TCP+ является расширением протокола TCP для синхронизации параллельных про-

© Баклановский М. В., Игумнов А. С., Самунь В. С., 2009