Model Checking Networked Applications: A Comprehensive Concurrency Analysis

Cyrille Artho [1]
c.artho@aist.go.jp

Watcharin Leungwattanakit [2], Masami Hagiya [2],
Yoshinori Tanabe [3]

[1] RCIS/AIST, Tokyo, Japan
[2] University of Tokyo, Tokyo, Japan
[3] CVS/AIST, Tokyo, Japan

05/16/2008

Race conditions: A common concurrency problem

- February 2004, Japan:

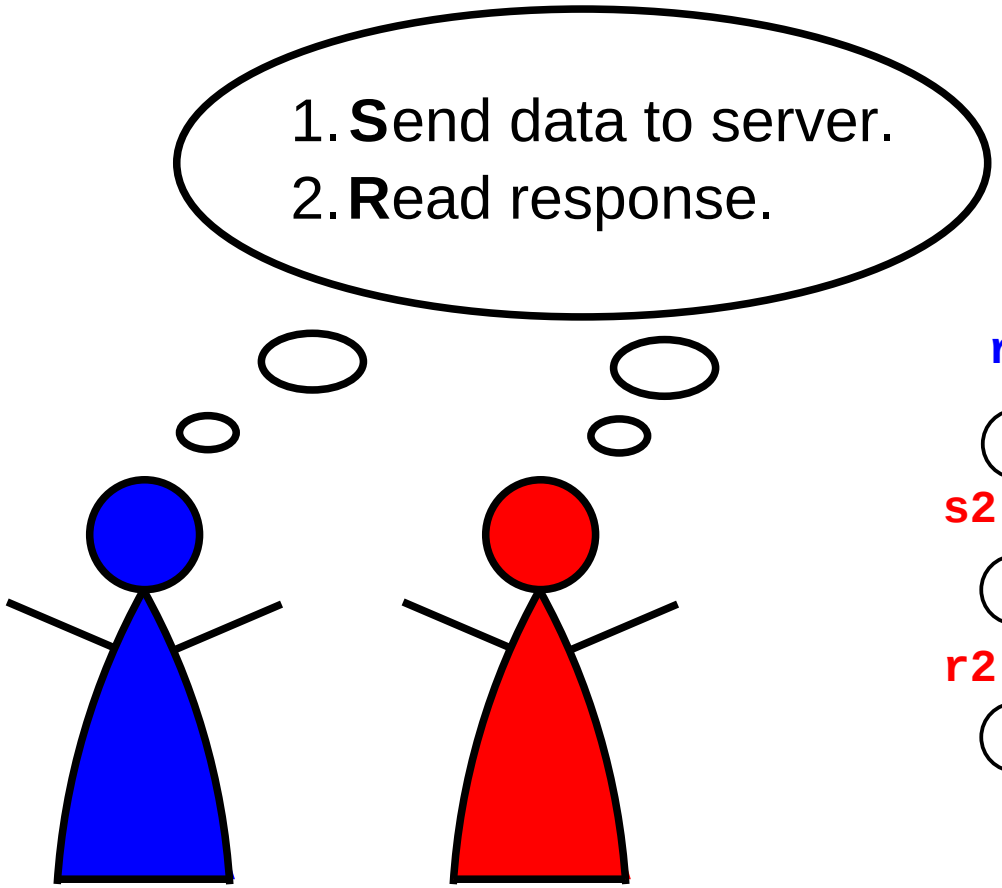
国税庁、確定申告書をPDF出力するWebサイトで個人情報流出

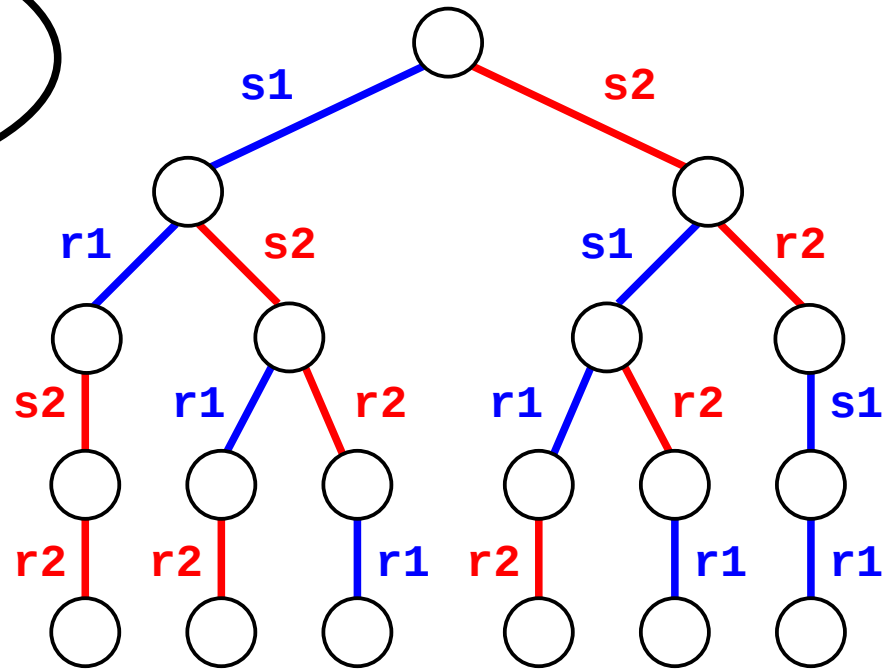
国税庁は4日、同庁のWebサイト「確定申告書作成コーナー」にて、個人情報が流出したと発表した。現時点で確認されている流出件数は4件。ただし、同サイトには1日に10万件のアクセスがあり、「4件以上流出している可能性は否定できない」としている。

確定申告書作成コーナーは、画面に表示された書式に入力すると、自動的に税額などを算出し、PDF形式で出力されるというもの。今回の個人情報流出では、このPDFファイルを印刷したときに、操作したユーザーとは異なるユーザーの情報に書き換わって印刷されてしまった。国税庁では、「サーバーが、2人から同時に印刷命令を受けた時に、一方のPDFを上書きしてしまう不具合があった」と、現時点で判明している不具合を説明。詳細や今後の対策については、「調査・検討中だ」という。

Two clients print their tax sheet at same time, see same tax sheet.

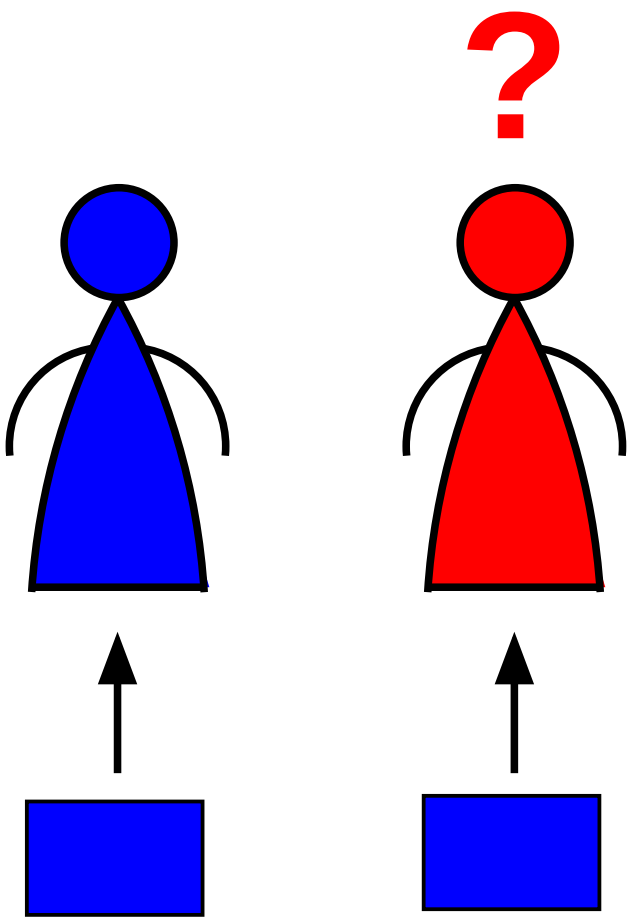
Why is concurrency difficult?

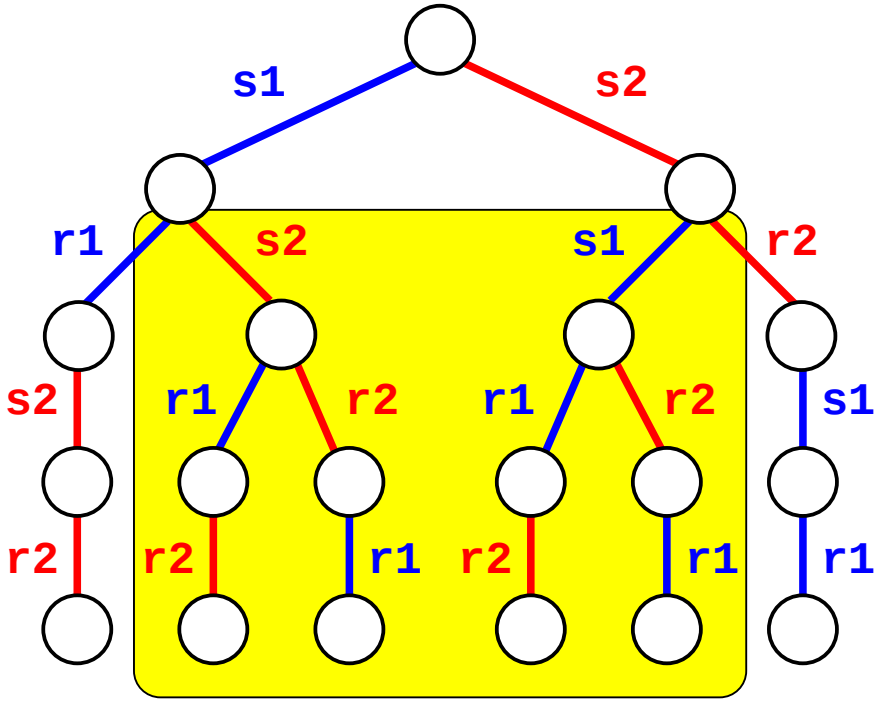




Operations of both clients can occur in any possible order!

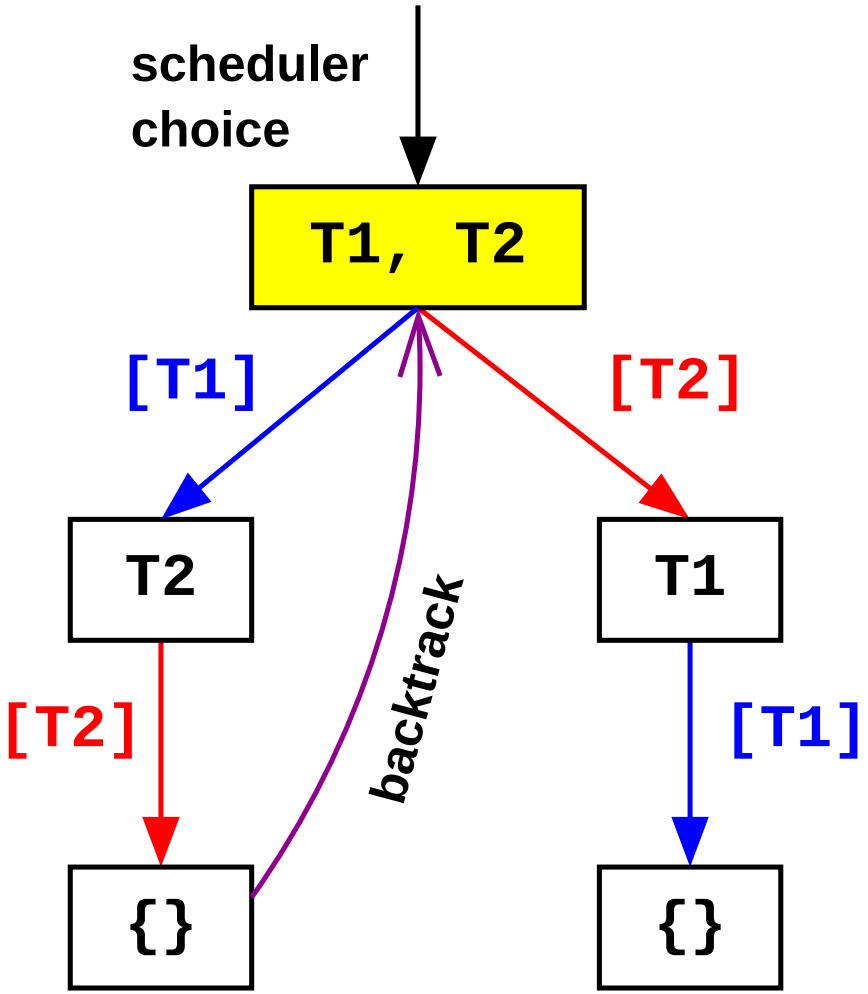
Why is concurrency difficult (2) ?





Operations of both clients can be interleaved!

What can model checking do?

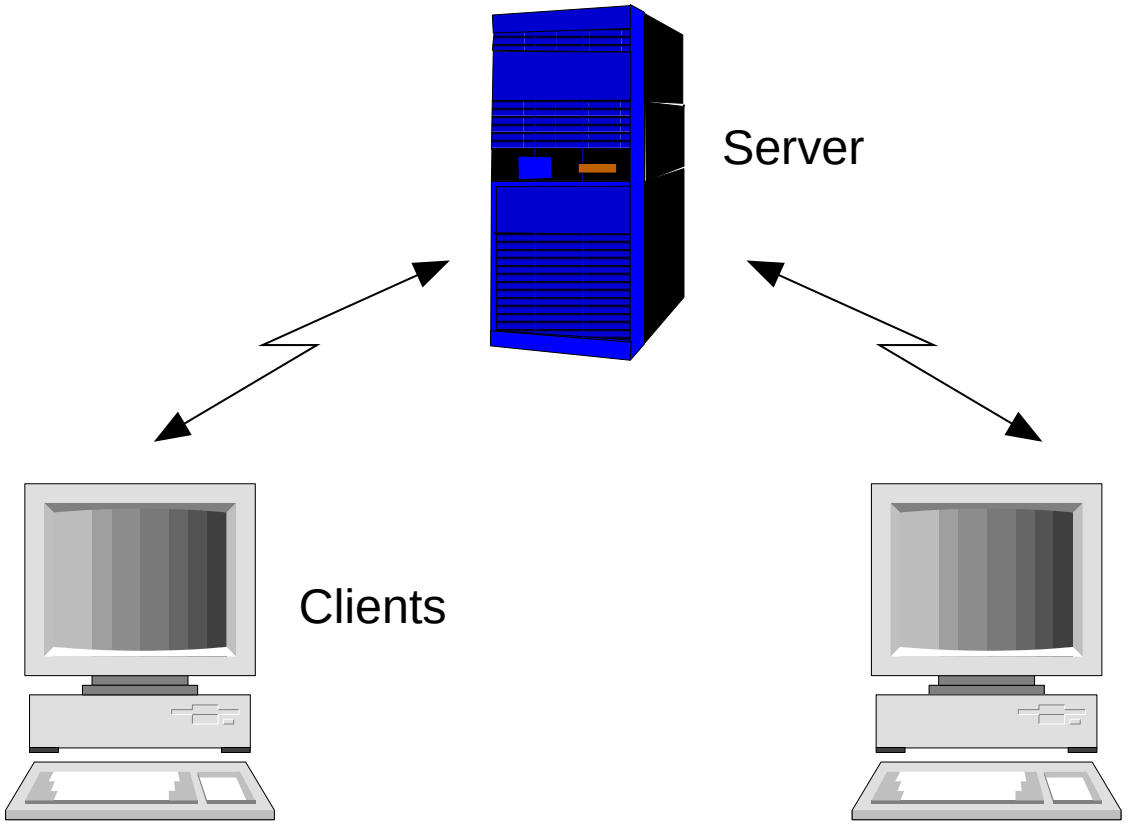


- MC can **backtrack** program execution.
- Explores all possible thread schedules!
- Finds all possible program failures.

Key limitation: Scalability.

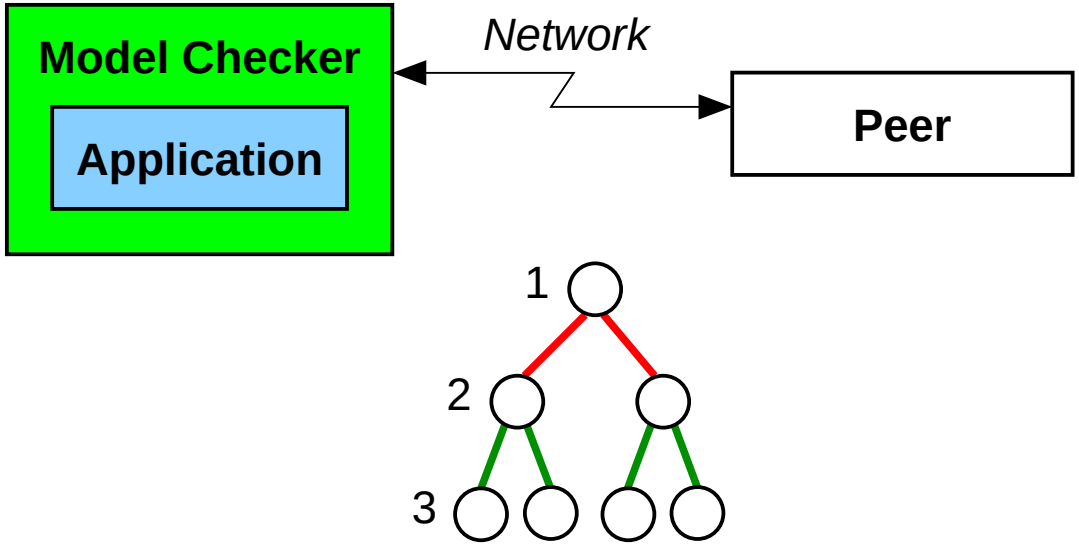
Another limitation: Networking!

Networked programs



- Multiple separate processes.
- Most software model checkers can only handle a **single** process!

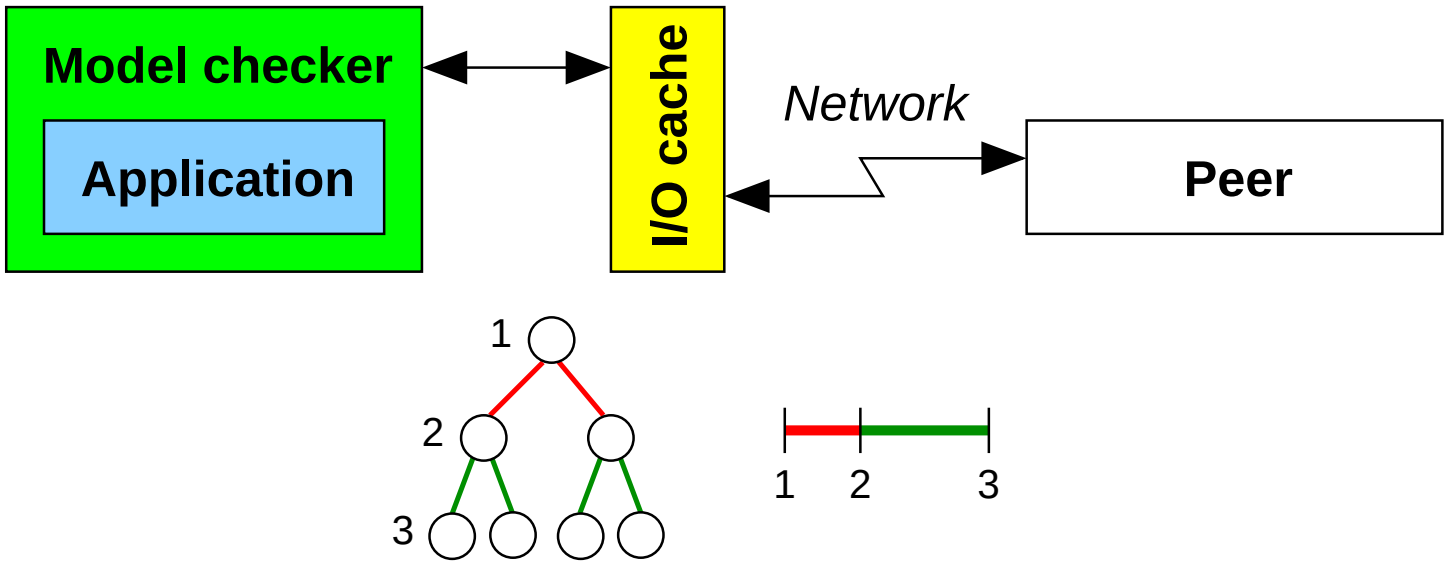
Network communication



Model checker repeats I/O operations during state space exploration!

- Output of local application is sent several times.
- Input is expected several times.
- Communication with external applications won't quite work this way. . .

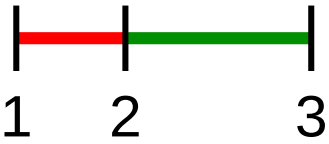
New approach: MC-aware I/O caching



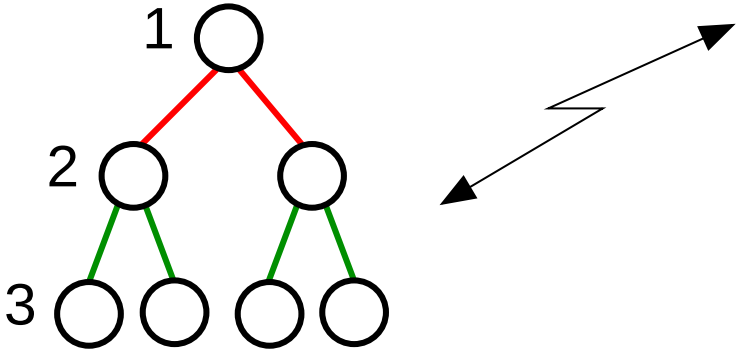
- Each I/O operation is captured by (MC-aware) cache layer.
- Duplicate send operations: „ignored” (not relayed to server).
- Duplicate read operations: previous output from server is replayed.
- Implemented on top of **Java PathFinder** model checker (from NASA).

Conclusion

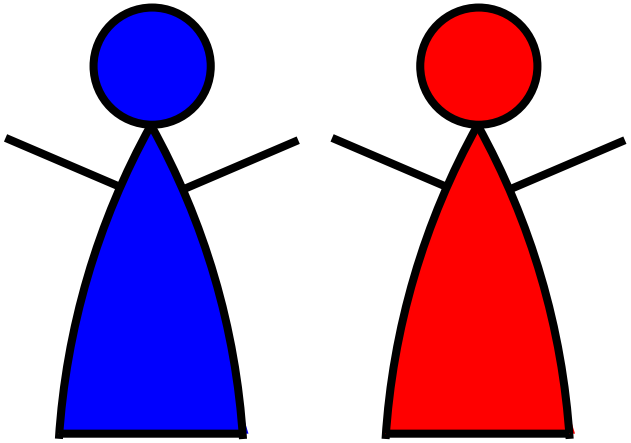
Cache input/output



Use model checking!



Concurrency is difficult



My e-mail: **c.artho@aist.go.jp**
JPF: **http://javapathfinder.sourceforge.net/**

I/O cache will be released as extension to JPF model checker.