Model Checking Infinite State Machines
- Who's who in Ogawa lab -

小川瑞史（JAIST）

mizuhito@jaist.ac.jp

2008.3.3

The aim of the talk

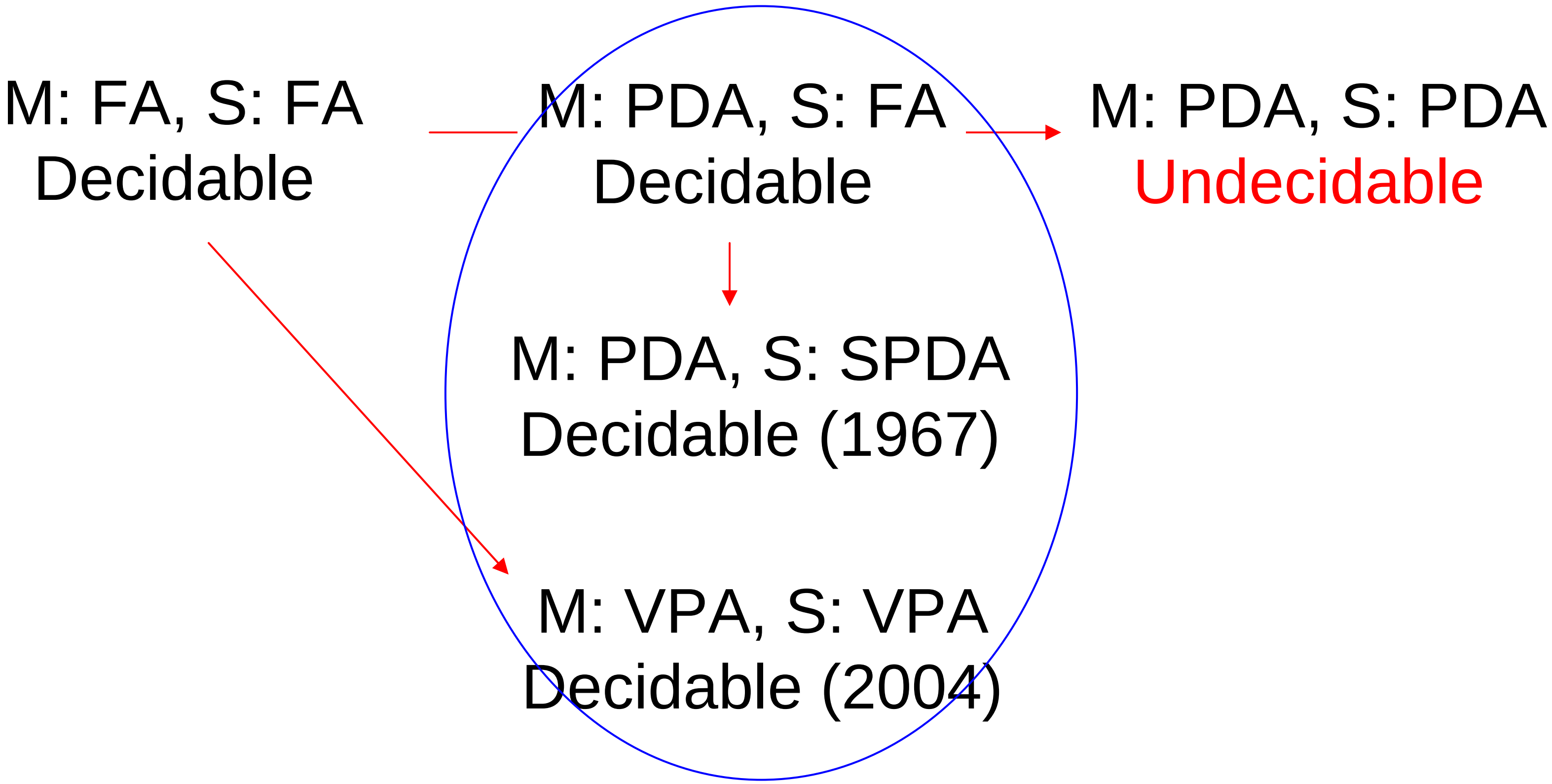
- Brief overview on model checking on infinite states, based on decidable results.

- Who’s who in Ogawa lab.; what we have done, are doing, and will do (would like to do).

Model checking : idea

- MC is the inclusion : $L(M) \subseteq L(S)$

  $\Leftrightarrow L(M) \cap L(S)^c = \phi$



M: FA, S: FA
Decidable

M: PDA, S: FA
Decidable

M: PDA, S: PDA
Undecidable

M: PDA, S: SPDA
Decidable (1967)

M: VPA, S: VPA
Decidable (2004)

What we have done/doing at a glance

Determinization fails for extensions of VPA (Nguyen Van Tang)

- Possible directions for extensions
  - Multi-stack
  - Stack automata (Ginsburg, et.al. JACM67)

- k-VPA (DLT07, LICS07) : emptiness is undecidable
  - k-MVPA (LICS07) : closure holds
  - k-ordered VPA (DLT07) : determinization claimed

- Visibly Stack Automata

Decidable emptiness; determinization fails

Collegues working on the topics

Verifying Recursive Protocol: On-the-fly MC (Li Guoqiang)

- Lazy instantiation on messages, i.e., message content that does not effect on protocol actions will be replaced with a variable and left uninstanciated.

OFMC (Basinm et.al. 05)

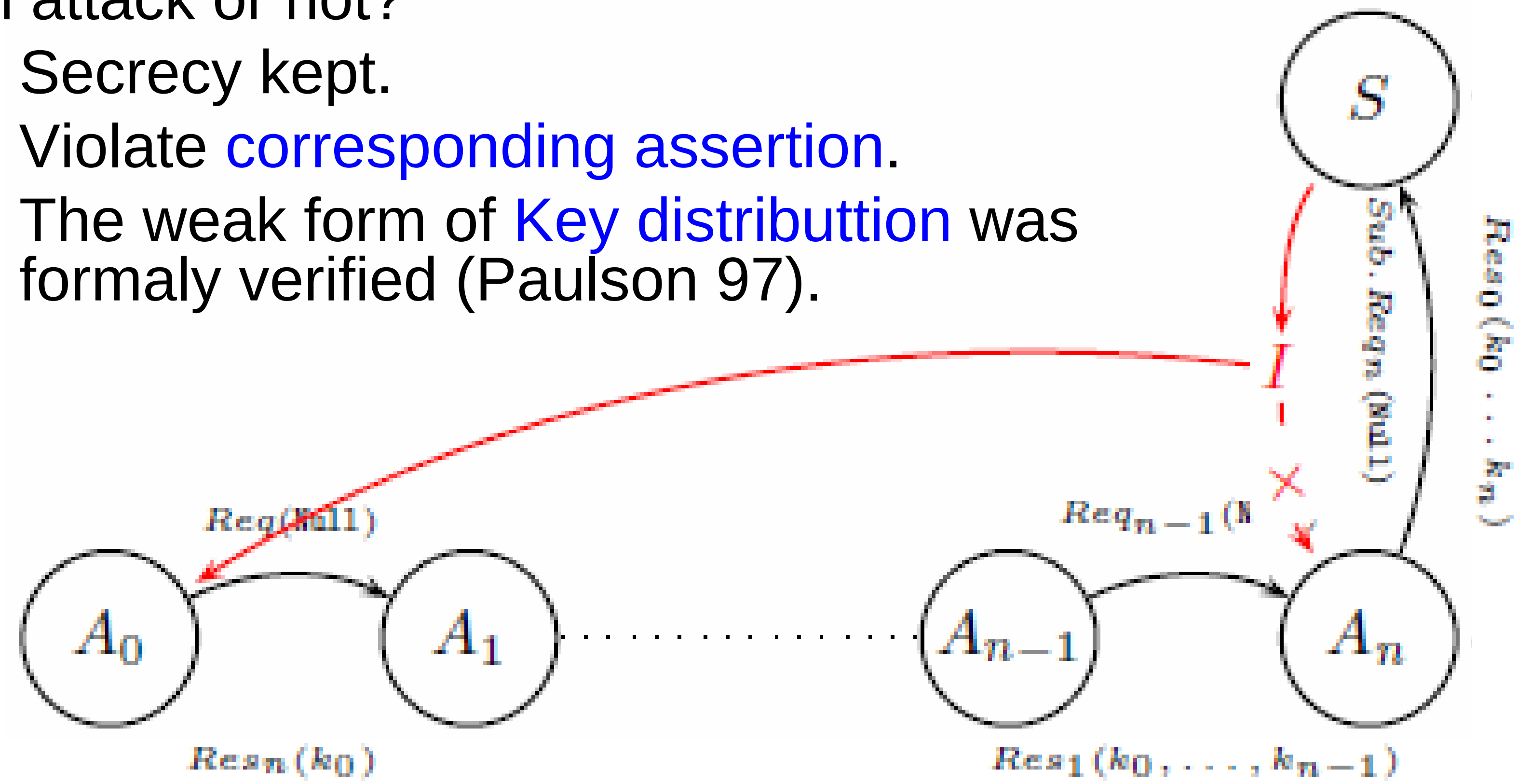
- Lazy instantiation on names, i.e., names are extended to terms, and left uninstanciated until actual principals are assigned during sessions.

- Identification of fresh messages by context, i.e., since the RA protocol does not repeat the same context, each nonce in a session is identified by the stack content.

Works for recursive protocols without parallel compositions

An attack in Recursive Authentication Protocol - Found by experiments on Maude -

- An attack or not?
  - Secrecy kept.
  - Violate corresponding assertion.
  - The weak form of Key distributtion was formaly verified (Paulson 97).



protocols	protocol spec.	states	times(s)	flaws
recursive authentication protocol	32	416	0.82	detected
fixed recursive authentication protocol	32	416	1.07	secure

Collegues working on the topics

Implementing Java context-sensitive analyses by weighted pushdown MC (Li Xin)

- Weighted Pushdown Model Checking (Reps 05)
  - Control flow : pushdown model
  - Dataflow : bounded idempotent semiring
    - Product = composition of flows
    - Summation = meeting of flows

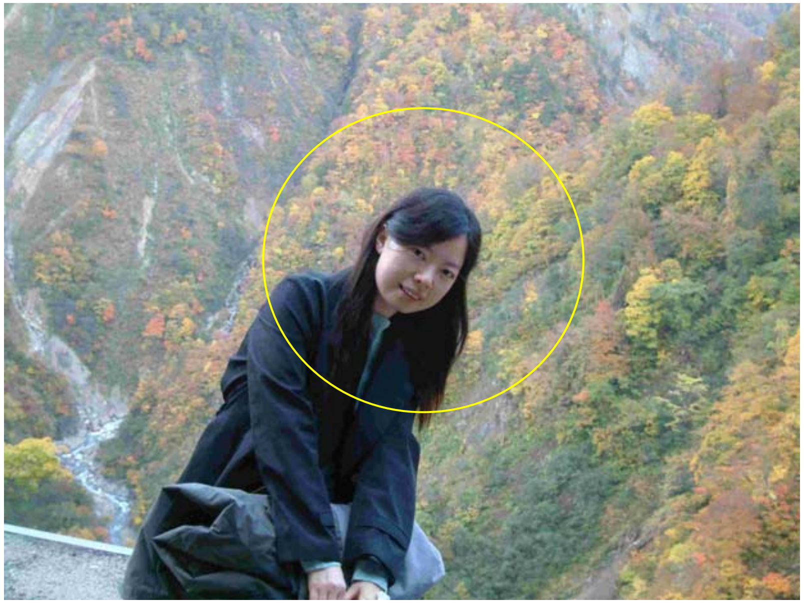
- Java context-sensitive analysis by weighted PMC
  - Integrate existing tools (SOOT, Weighted PDS)
  - Interprocedural control flow graph is mutually dependent to points-to information.

Java Relevance Analysis for Symbolic Execution

- Symbolic execution: Java PathFinder extension
  - Old technique (from early 70s)
  - Constraints (Presburger Arithmetic, 1st order logic) are computed for dynamically decided variables.
  - Test data with full coverage will be generated.

- Relevance analysis:
  - Reduce variables that require symbolic execution.
  - Based PTA (we developed), weighted PDS is applied with PER-based abstraction.
  - Collaboration with FLA (2007.10~)

Collegues working on the topics



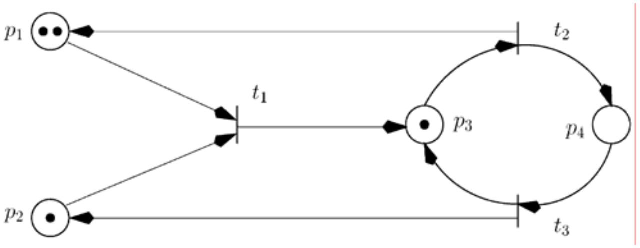
What we would like to do

Yet another infinite state transition systems

- A well-structured transition system (WSTS) has:
  - S : *finite* set of *control states*
  - D : WQO (D,≦) (*infinite* set of *data on cont. states)*

$$\begin{tikzcd}
\forall & s_1 \arrow[r, no head, bend left, "\leq"] \arrow[d] & t_1 \arrow[d, dashed] & \\
 & s_2 \arrow[r, no head, dashed, bend left, "\leq"] & t_2 & \exists
\end{tikzcd}$$

- Safeness of monotonic WSTS: decidable
  - Inclusion problem of timed automata on finite words where specification has a single clock
  - Coverability of Petri net.



Yet another infinite state transition systems

- Liveness of WSTS: undecidable
  - Inclusion problem of timed automata on infinite words where specification has a single clock.

- Restricted Liveness of WSTS: decidable?
  - Non-Zeno inclusion problem of timed automata on infinite words where specification has a single clock?
  - Reachability of Petri net? (Coming phd candidate?)

Developing deduction engines

- Diophantine Constraint Solver (DCS):
  - Needs from automatic termination prover.
  - SMT : decidable imported theories/engines
  - DCS : specialized to bounded Diophantine constraints (Nao Hirokawa)
- VPA model checker:
  - Only preliminary one known in France.
  - "Complete-pre" approach (backward on-the-fly algorithm, Nguyen Van Tang)
- Enhance Weighted PDS library (?) :
  - Needs for efficient integration of tools.

Collegues working on the topics

SMT-like approach for Weighted PDS (Li Xin, Do Thi Binh Ngoc)

- SMT = SAT (efficient search) + theory (outer oracle)
  - Theory : typically, Presburger Arithmetic, equations with uninterpreted function symbols.

- Weighted PDS = pushdown model + weight
  - Pushdown model : trace control flows
  - Weight : outer oracle
    - 1st order prover to compute product / sum.
    - Widening by Craig interpolation to guarantee the finite ascending chain condition ?
  - Array bound check / round off error analysis on C

Collegues working on the topics