The SENVA Joint Team

Hubert Garavel, INRIA/VASY

Jaco van de Pol, CWI/SEN2

SENVA joint team

- CWI / SEN2, Amsterdam
  - CWI: Mathematics & Computer science
  - 210 fte, 170 scientists, 66 permanent
  - SEN2: around 15 members (3 permanent)
  - Specification and Analysis of Embedded Systems
- INRIA / VASY, Grenoble
  - INRIA Rhône-Alpes: nearly 500 persons
  - VASY: around 14 members (4 permanent)
  - Languages and Tools for Validating Asynchronous Systems

Some important changes

- SENVA leader change:
  - Wan Fokkink (until September 2004)
  - Jaco van de Pol (from September 2004)
- In 2005, NWO terminated funding for all French-Dutch collaboration projects
- SEN2 decided to pursue the SENVA collaboration from its own means, using project money and group budget

SENVA motivation

- Motivation 1: Develop new tools and integrate existing verification tools
- Motivation 2: enabling technology for new applications, “formal methods at work”
- Motivation 3: building a European consortium for distributed model checking

- So the goal of SENVA is not to do paperwork. Both groups have an excellent research output. “We do not want to duplicate papers”.

Overview

- Scientific goals of SENVA
- Software integration within SENVA
  - demo #1: Digital Rights Management (security)
  - demo #2: Asynchronous circuit for encryption (hardware)
- Case-studies tackled by SENVA
- Joint events organized by SENVA
- The future of SENVA / Consortium building

⇒ EC-MOAN European project follow-up

Scientific goals

1. High-level specification languages
2. Minimization tools for transition systems
3. Compositional verification techniques
4. Distributed algorithms for state space generation and minimization
5. Combination of verification techniques

1. High-level specification languages

- SEN2 and VASY use different specification languages (mCRL for SEN2, LOTOS for VASY)
- These languages are powerful, but too complex for a wide industrial acceptance
- SENVA achievements:
  - "SPART" initiative to design "better" languages
  - Strong influence of SPART discussions:
    - LOTOS NT at INRIA Rhône-Alpes
    - mCRL version 2 at Eindhoven Univ. of Technology

2. Minimization tools for transition systems

- The state space of industrial distributed systems is huge
- Need for minimization tools, to be applied as preprocessor for model checking
- SENVA achievements:
  - Worst-case suboptimal procedures, which have better performance on typical cases
  - Distributed algorithms to minimize astronomic state spaces on clusters of workstations
  - Techniques to avoid big state spaces (abstraction, on-the-fly, confluence, compositionality)

3. Compositional verification techniques

- Efficient means to fight "state explosion"
- SENVA achievements:
  - confluence and partial-order techniques added to mCRL and CADP toolsets
  - extension of CADP tools (Exp.Open, Projector, Open/Caesar libraries) to support mCRL labels and operators (parallel composition, cut...)
  - automatic generation of behavioural interfaces that express environment constraints on a process

4. Distributed algorithms for state space generation and minimization

- The SENVA team developed various algorithms to exploit parallel computing power/memory:
  - distributed state space generation (several variants)
  - distributed state space minimization (strong and branching bisimulation)
  - distributed cycle elimination (SCC detection)
  - distributed resolution of Boolean Equation Systems
  - distributed model checking
  - distributed equivalence checking
- SENVA achievements:
  - The SENVA team is world leader on distributed verification tools in the branching time setting.

5. Combination of verification techniques

- Both labs had developed there own tools (CADP toolbox, muCRL toolset) and had their own verification philosophy.
- Many techniques were complementary, and can now be combined
- SENVA achievements:
  In one verification project one gets the accumulated profits of (a.o.):
  - on-the-fly generation (leads to pruning)
  - confluence reduction (avoids irrelevant schedules)
  - compositional verification (reduce components first)
  - abstract interpretation (dispose irrelevant details)

Software integration within SENVA

- Software development was focused on interconnection of model checking tools
- Concrete SENVA results:
  - Compositional verification: exp.open -mcrl
  - On-the-fly connection: mcrl.open
  - Partitioned LTS formats: PBG
  - Sequential minimization algorithms: BCG_MIN vs LTSMIN
- Two demos will show interoperability

Demo #1: security protocols

- Digital Right Management (DRM)
  (M. Dashti, SEN 2)
  - a set of compliant content rendering devices,
  - operated by untrusted owners, and
  - a set of trusted entities (3rd parties)
  - Goal of the protocol: Fair exchange of digital items between devices, despite failures and malicious acts by device owners

Demo #1: security protocols

- Approach:
  - specification of the system in mCRL
    - model of each device, owner, trusted 3rd party
    - model of attacker, encoding all possible attacks!
  - specification of the security requirements in temporal logic (branching time, fairness)
- mcrl.open is the on-the-fly bridge, constructed in the SENVA project
  - the mCRL model is compiled and linked to the CADP libraries and Evaluator 3.5 tool
  - on-the-fly generation: driven by CADP’s Evaluator
  - on-the-fly confluence reduction using mCRL’s prover

Demo #1: security protocols

- Compilation:
  - mcrl -nocluster -regular drm.mcrl
- Static analysis/reduction:
  - constelm drm | stategraph | constelm > drm1.tbf
- Confluence analysis with theorem prover:
  - confcheck -mark drm1.tbf > drm2.tbf
- On-the-fly generation and model check:
  - mcrl_open -confluent ctau drm2.tbf evaluator fair.mcl
  - mcrl_open -alt rw drm2.tbf evaluator –diag safe.mcl
- Inspection of diagnostics:
  - bcg_draw evaluator.bcg

Demo #2 : hardware circuits

- Data Encryption Standard (DES)
- Asynchronous circuit (= no clock) designed at TIMA and CEA/Leti labs
- Described first in M. Boubekeur's thesis
- Modelled in LOTOS by Gwen Salaün and Wendelin Serwe (VASY)
- Goals:
  - verification of correctness for control aspects
  - generation of a prototype software implementation

Demo #2 : hardware circuits

Approach:

1. specification of the DES circuit in LOTOS
   → (simplified version used for the demo)

2. state space generation using CADP tools
   → distributed generation using DISTRIBUTOR

3. state space minimization using LTSMIN

Case-studies tackled by SENVA

- SEN2
  - Several security protocols (evaluator tool)
    - Fair Payment protocol (E-commerce)
    - DRM protocol (demo #1) (digital rights management)
    - Authentication protocols (Needham Schroeder style)
  - for Weidmüller : truck lift system
  - for Thales : SPLICE shared data space architecture
  - for Philips : several IEEE1394 Firewire subprotocols
  - CEPS (common electronic purse system) (TGV tool)
    - intially modeled by INRIA (Vertecs and Vasy)
    - combination of abstraction/graph algos/constraint solving
    - symbolic test case generation

Case-studies tackled by SENVA

- VASY
  - Fame Scalability Switch in Bull's NovaScale servers
  - Asynchronous circuit implementing DES cypher (demo #2)
  - Turntable handled first by SEN2 (Anton Weis, Wan Fokkink et al), then by VASY (Radu Mateescu)
- Others used SENVA tools in combination
  - Clara Benac (Madrid) : Ericsson resource locker
  - Juan Jose Sanchez Penas (La Coruhna) : video on demand systems (Vodka)
  - Jan Friso Groote (Tech. Univ of Eindoven) : Philips medical systems, OCE copiers, …

SENVA workshops and meetings

- Jun. 2004: SENVA 1st workshop (4 days)
- May 2005: SENVA 2nd workshop (3 days)
- Nov. 2005: SENVA meeting on distributed verification (2 days)
- Apr. 2006: SENVA meeting on verification grids (2 days)
- Jun. 2006: SENVA 3rd workshop (4 days)

+ *many working meetings joint with conferences*

SENVA research visits

- 2004:
  - J. van de Pol, S. Blom → Grenoble
  - H. Garavel, F. Lang, W. Serwe → Amsterdam
- 2005:
  - F. Lang, W. Serwe → Amsterdam
- 2006:
  - J. van de Pol → Grenoble
  - H. Garavel, R. Mateescu → Amsterdam

Additional dissemination

- ERCIM news: kickoff SENVA joint team
- Web site: http://www.inrialpes.fr/vasy/senva
- Handbook of Formal Methods: 2 SENVA chapters
  - Temporal logic for asynchronous systems
  - Some trends in formal methods applications to railway signaling

Consortium building by SENVA

- We organized various joint meetings with EU experts

⇒ European project EC-MOAN (STREP in FP6 – NEST):
scaling MOdelling and ANalysis techniques
to study Emergent Cell behaviour:
understanding *E. Coli* stress response

- Participants:
  - CWI /SEN 2 (leader) + CWI / MAS 2 (Amsterdam, The Netherlands)
  - INRIA / VASY + INRIA / HELIX (Grenoble, France)
  - Free University (Amsterdam, The Netherlands)
  - Université Joseph Fourier (Grenoble, France)
  - Masaryk University, Brno (Czech Republic)
  - University of Edinburgh (Great Britain)

The future of SENVA

- Further integration of tools: the next generation
  - cross-translation with other formalisms
  - release of distributed tools for generation and minimization
  - serialization/deserialization interfaces to enable on-the-fly connections with distributed tools

- Strategic application domains:
  - hardware circuits and multiprocessor architectures
  - security protocols (intruder models / intelligent data enumeration)

- Bio informatics: new application domain
  - real biologists involved for modeling and experimentation
  - bio-models combine modules: metabolic, signalling, gene expression
  - mathematicians transform/reduce/discretise differential equations
  - currently: analysis tools for these huge models are missing!
  - challenge: study “reachable equilibriums” with distributed model checking algorithms