# Verification of Mascara-Control

Natalia Sidorova  Martin Steffen

*Dept. of Electrical Engineering*
*TU Eindhoven*

*Inst. für Informatik u. Prakt. Mathematik*
*CAU Kiel*

June 2000

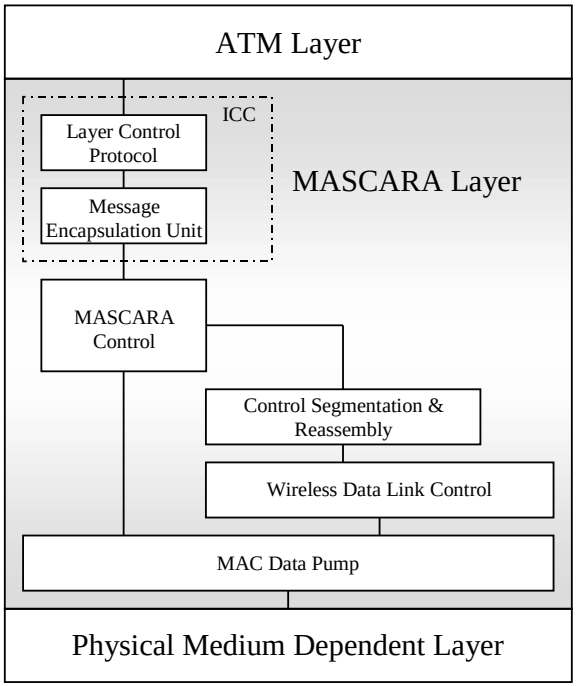
Vires-Review, Autrans

# Overview

- Mascara-control
- Approach and tools
- Results
- Conclusion

# Mascara

- medium-access for wireless ATM [1]
- Vires-Spec: $\geq 300$ pages (graphical) SDL-92 [1]
- large sub-entity: Mascara-control
  - task: signalling/control
  - interfaces will all other entities

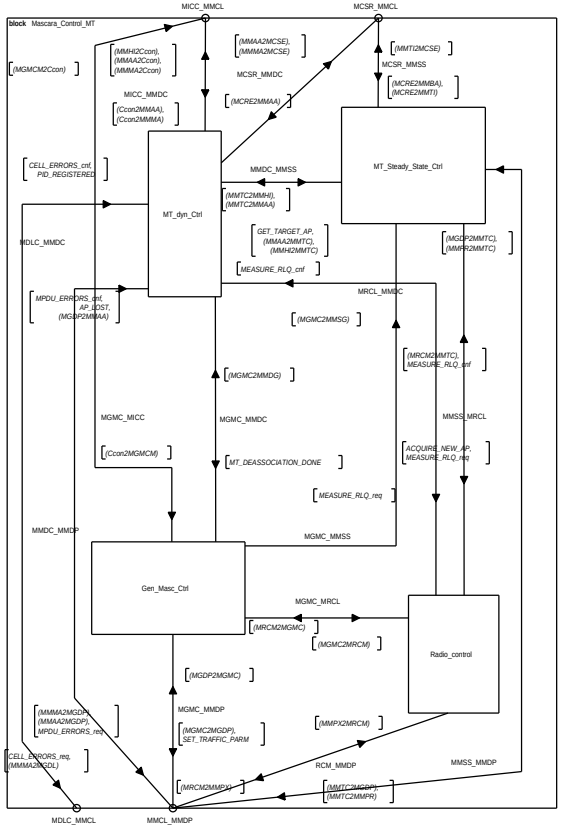



[1] "$M$obile $A$ccess $S$cheme based on $C$ontention $a$nd $R$eservation for $A$TM".

# Mascara-control

*main/largest entities:*

- dynamic control
  - set-up/tear down associations and connections[2]
  - address management (conn./assoc.)
  - process creation
- steady-state control
  - monitor current association
  - monitor radio environment
  - collect info. about alternative associations




[2] Hand-over is no MCL-service by itself, but composed of association and deassociation.

# Main protocols involved

- association handling (set-up, tear-down)
- connection handling (set-up, tear-down)
- incommunicado: scanning the radio environment regularly
- I'm alive: sending invitations to overdue MTs
- alarm handling: fast reaction, if association breaks down

# Approach

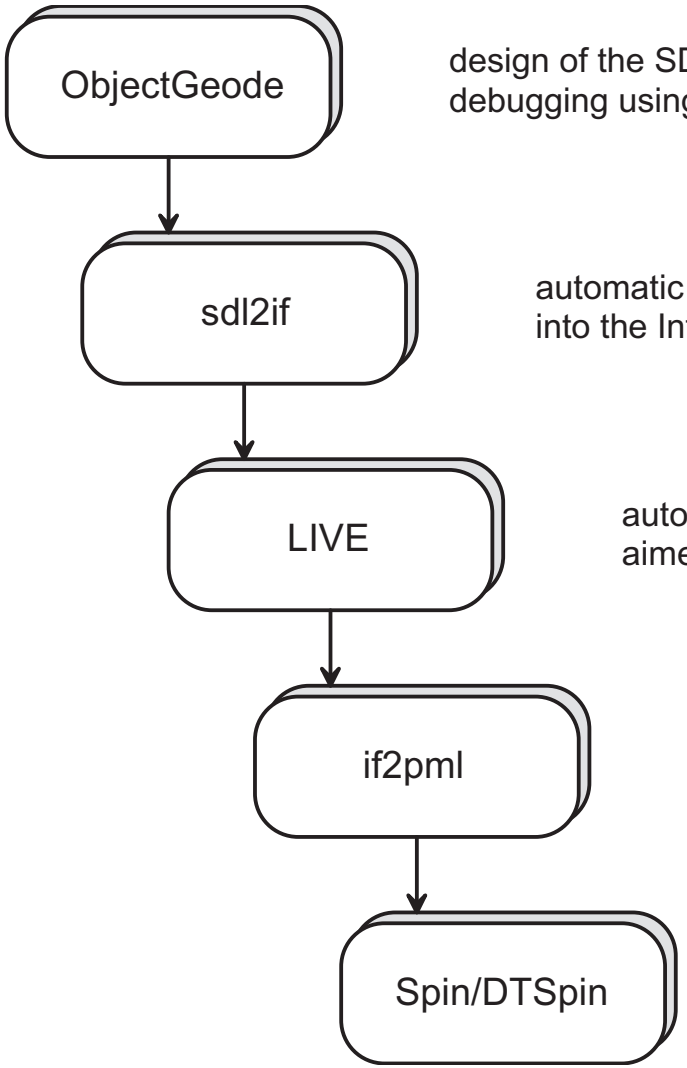
- bottom-up approach:
  1. MTC/steady-state control
  2. dynamic-control
  3. one-sided configuration for MCL
  4. 2-sided configuration for MCL
- closing manuall each configuration by enviroment
- debugging entities step-by-step

# Abstractions

- underlying physical layer + data pump + WDLCs + CSR: lossy buffer[3]
- abstracting away from generic Mascara control (= global initialization)
- abstracting largely radio control: non-determinism to represent decisions depending on physical environment
- general types of abstractions:
  - data-abstractions:
    - keeping the control-structure + reducing/removing the data-part
    - e.g.: two addresses
  - simple control-abstractions

[3] for 2-sided configurations.

# Model checking environment




design of the SDL-specification, syntax checking,
debugging using the ObjectGeode simulator facilities

automatic translation of the SDL-specification
into the Intermediate format (IF)

automatic transformation of the IF specification
aimed at the reducing of the state space of the model

automatic translation of the obtained IF-specification
into DT Promela/Promela

model cheking the model

# Reachability checks

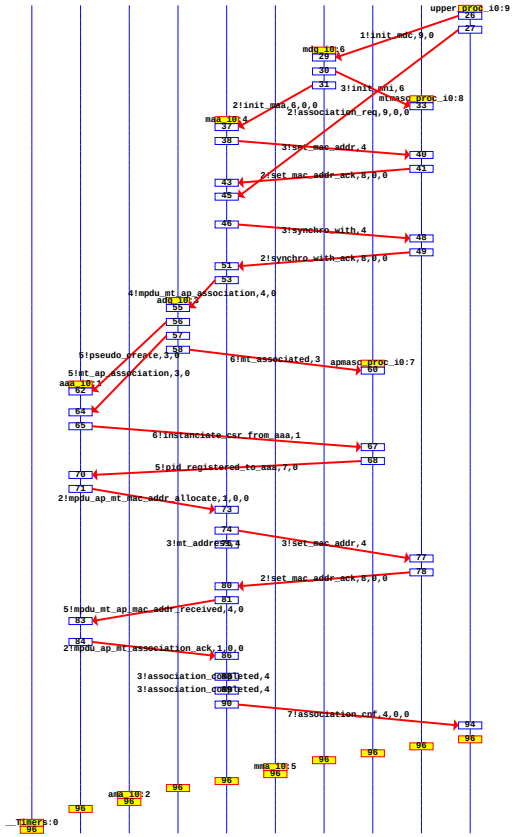
- easily done, by assertion violations

$\Rightarrow$ routine check-pointing crucial steps

- additional value: asserting desiredly reachable points as $false$

$\Rightarrow$ illustration of desired behaviour

$\Rightarrow$ comparison with Wand-MSCs [4]



# Most common errors

- plain programming bugs
- values out of range
- race conditions (especially in the initialisation phases)
- ambiguous receiver
- unspecified reception

# Time-dependent property: unique MAC addresses

- AP dynamic control: administers MT-addresses

Requirement:

*"never the access point relinquishes an association before the mobile terminal does"*

$$\Box(\varphi_{mt-lost} \rightarrow \varphi_{ap-lost}) \quad (1)$$

- satisfaction depends on 4 timers + 4 program constants

| side | timer | program constant | process entity |
|---|---|---|---|
| AP-side | $T_{iaa\_poll}$ | $Max\_Time\_Periods$ | AIA |
| | $T_{frame\_start}$ | $IAA\_Max$ | AIA |
| MT-side | $T_{GDP\_period}$ | $Max\_Cellerrors$ | GDP |
| | $T_{rcm}$ | $Max\_AP\_Index$ | MTC |

# Unique MAC addresses (2)

*"minimal time for AP to give up must exceed maximal time for MT to give up"*

$$\min(\tau_{AP}) > \max(\tau_{MT}),$$

- Bounds of times

$$\begin{aligned} \tau_{AP} &\geq (Max\_Time\_Periods + 1) * T_{iaa\_poll} + (IAA\_Max - 1) * T_{frame\_start} \\ \tau_{MT} &\leq (Max\_Cellerrors) * T_{GDP\_period} + (Max\_AP\_Index + 1) * T_{rcm} \end{aligned}$$

- extremal case (for $\tau_{AP}$): 1 MT

$\Rightarrow$ configuration 1 AP, 1 MT

# Results (overview)

| | Reachability |
|---|---|
| 1. | MT can go incommunicado |
| 2. | forward hand-over possible |
| 3. | incommunicado scenario |
| 4. | backward hand-over at MT |
| ... | |

| | Errors found |
|---|---|
| 1. | negative number of associated MT's |
| 2. | twice "*start-of-tip*" without end-of-tip in between |
| 3. | twice "*end-of-tip*" without start-of-tip in between $\rightarrow$ illegal termination |
| 4. | incommunicado becomes impossible |
| 5. | illegal termination |
| 6. | infinite undetected loop in backward hand-over |
| ... | |

| | Verified properties |
|---|---|
| 1. | no illegal termination |
| 2. | toggle-array chooses correct branches in ATI (start-tip) |
| 3. | toggle-array chooses correct branches in ATI (end-of-tip) |

| | Timed properties (positive and negative results) |
|---|---|
| 1. | permanent backward hand-over (im)possible |
| 2. | unique/ambiguous MAC-addresses |

# Conclusions

- Debugging of one large part of Mascara using model-checking
- good touch-stone of the Vires tool-set
- experiments provided valuable feed-back to the tool-development
- simple abstractions already get you far

# Lessons learned

- more effort on specification
- tool integration
- make easy things easy

$\Rightarrow$ support for routine task, like

  - diagnostics
  - automatic closing of the model
  - whole-sale chaotic abstraction of complete entities + necessery (small, but many) interface adaptations

# Literatur

[1] Dennis Dams, Susanne Graf, Guoping Jia, Natalia Sidorova, Martin Steffen, and Diana Tourko. SDL-specification of the Mascara protocol. Available electronically at `www.informatik.uni-kiel.de/~seriv/Deliv/Spec/`, November 1999.

[2] Natalia Sidova and Martin Steffen. Verification of a wireless ATM medium-access protocol. Technical Report TR-ST-00-3, Lehrstuhl für Software-Technologie, Institut für Informatik und praktische Mathematik, Christian-Albrechts-Universität Kiel, May 2000. Submitted for publication.

[3] A wireless ATM network demonstrator (WAND), ACTS project AC085. `http://www.tik.ee.ethz.ch/~wand/`, 1998.

[4] Working groups at Intracom Ascom, UoA and Eurecom. Message sequence charts for the Mascara-protocol. distributed electronically for internal use, 1998.