MODELING AND VERIFICATION OF MOBILE SYSTEMS USING CafeOBJ

Ongoing research & future directions

IAKOVOS OURANOS & PETROS STEFANEAS
National Technical University of Athens

Sinaia School on Formal Verification of Software Systems, March 2008

- New challenges from the mobile computing paradigm
- Increasing demand for reliable mobile services and software => need for effective design => Formal Methods

MOBILE COMPUTING & SYSTEMS

- Distinct characteristics of mobile systems
  - Migration
  - Resource sharing
  - Disconnected operations
  - Location awareness

MOBILE COMPUTING & SYSTEMS

- Modeling and verification of mobile systems using formal methods

<u>Some Related work</u>

1. Mobile Maude
2. Mobile UNITY
3. Mobile TLA

MOBILE COMPUTING & SYSTEMS

- Why use CafeOBJ for mobile system modeling?

1. Has been used successfully for modeling and verification of distributed systems.
2. Support for Hidden Algebra/Behavioural Specification – a research challenge to apply these techniques to mobile systems modeling

MOBILE COMPUTING & SYSTEMS

- Why use CafeOBJ for mobile system modeling?

3. Expand the application areas of CafeOBJ.
4. Based on equational specification is easier to read, understand and learn.

Modeling mobility as the change of the value of a spatial observer.

- Mobile communication systems -> objects just observe the change (location awareness)
- Mobile robots -> can manage the change

Similar kind of modeling has been also applied to Mobile UNITY and Mobile TLA

Mobile OTSs

- MOTSs are OTSs evolved with the introduction of spatial observers

  Special spatial observers: ***current_location***, ***home_location***

- Special actions:
  - Mobility action **move** that changes the value of *current_location*
  - Interactions **connect**, **disconnect** to handle disconnected operations
  - Communication actions **snd, rec** for communication through asynchronous message passing
  - **clone** action for making an exact replica of a mobile code object.

Mobile OTSs

- Operations over resources to handle resource constraints
  - A resource data type constructor:
    - » r : Rid Rval Rloc Rkind MOid -> Resource

where: **Rid** is the id of the resource

Rval is a natural number denoting the amount of the resource

Rloc is the location of the resource specified as a 4 TUPLE

Rkind is the kind of the resource such as memory, power, etc.

MOid is the id of the mobile object that is the owner of the resource

- Sharable resource: A resource that can be used simultaneously by more than one users.

  e.g. sharable?(file) = true, sharable?(printer) = false

- Hoardable resource: A resource that can be hoarded or stored.

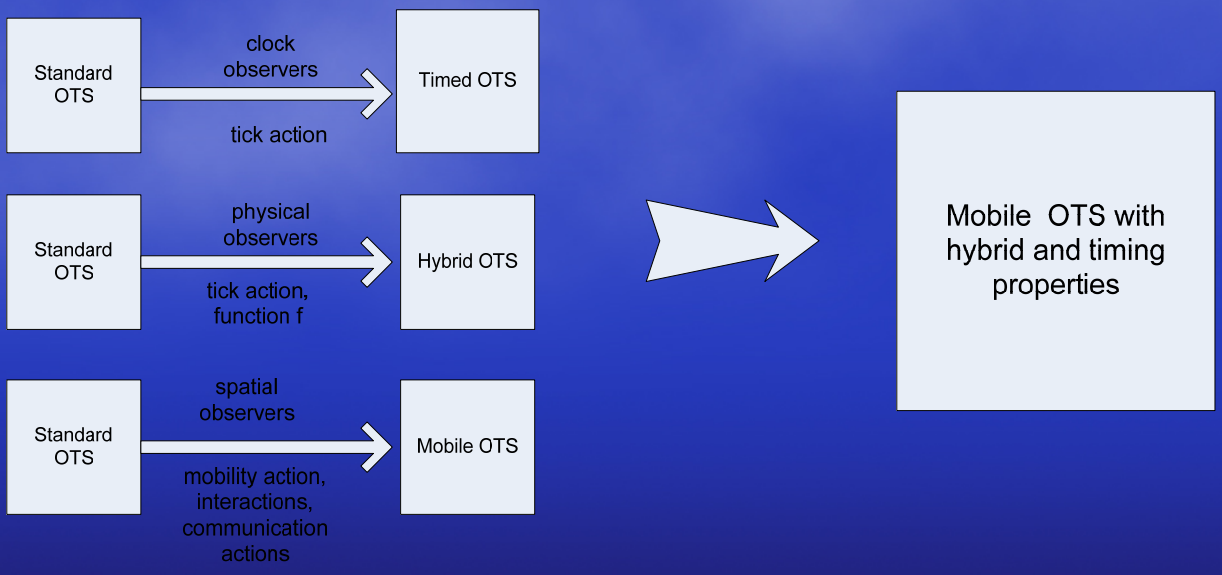
  e.g. hoardable?(file) = true, hoardable?(memory) = false

- **Communication through *asynchronous message passing:***
  - »***Queues of incoming and outgoing messages and mailboxes maintained at servers for disconnected operations***
  - ***or***
  - »***Use of network as a multiset of messages. Messages remain at network until received.***

Integration

- To model real time aspects and hybrid models of mobile systems MOTSs can be integrated with Timed OTSs and Hybrid OTSs.

Integration



- Hybrid models for mobile systems may include:
  - Time
  - Velocity
  - Distance
  - Resources
  - Space?

Case Studies (1)

- Mobile computing environment (to introduce Mobile OTSs)
  - Specification of an abstract mobile computing environment as an OTS
  - Verification of invariant properties of the system

No	Informal definition
1	At any reachable state, if a mobile is connected then its mailbox is empty.
2	At any reachable state, a mobile can have only one home location.
3	At any reachable state, a mobile can have only one current location.
4	At any reachable state, a mobile has one and only installed mailbox at a support station.
5	At any reachable state, a mobile has one and only queue of inbound messages.
6	At any reachable state, a mobile has one and only queue of outbound messages.
7	At any reachable state, a support station has one and only queue of inbound messages.

Case Studies (2)

- Mobile IP registration procedure (to include the timing constraints)

  Invariant At any reachable state of the registration procedure, if a reply message that was sent in response to a request message of a mobile, exists in the network, and its status flag is set to OK, then the address of the requested mobile has been added to the set of mobiles away from home and its forwarding address to the home agent has been set to the care of address requested.

```
op inv2 : Sys Address Address Address Status Id -> Bool
eq inv2(S, A1, A2, A3, ST, I) = RepMsg(A1, A2, A3, ST, I) \in
   nw(S) and ST = OK implies A3 \in ha-mobiles(S, subnet(A1))
   and fwd-addr(S, subnet(A1), A3) = A2 .
```

Case Studies (3)

- GSM simple handoff (to show hybrid modeling)

  Invariant At any reachable state of the system, the handoff procedure will have finished before the mobile reaches the boundary of the cell.

```
inv3(S, M, MS) = MS \in nw(S) and switch?(MS) and dst-
   sw(MS) = M implies distance(S, M, BS1) <= Rmax .
```

Verification

- Using verification techniques applied to standard OTSs
  - OTS/CafeOBJ method-simultaneous induction-case analysis-lemmas
  - Invariant properties of mobile systems
  - Infinite state space
  - Can be thought as complementary to Mobile Maude where model checking is used for finite state space (BOTS/Maude method)

Publications on Mobile OTSs

- **Journal**
  1. An algebraic framework for modeling of mobile systems, (IEICE Trans. Fund.)
  2. Formal analysis of real time and hybrid models of mobile systems in MobileOBJ framework, (submitted).
- **Int. Conf.**
  1. A formal specification framework for ad hoc mobile communication networks, SOFSEM 07, SRF.
  2. MobileOBJ: A Mobility Approach Using CafeOBJ Algebraic Specification Language, ICNAAM 2004.
  3. An Algebraic Specification of Mobile IPv6 Protocol, PRISE 2004.

Security aspects of mobile systems

To model security protocols applied to mobile systems we need standard OTSs

Case Studies

- Secure Network Encryption Protocol (SNEP) for wireless sensor networks, and
- TESLA protocol (a source authentication protocol in multicast settings) specified as a Timed OTS!

Publications

1. Modelling Real Time Authentication Protocols using Algebraic Specification Techniques-the case of TESLA protocol
   IFIP TC7 Conference.
2. Verifying Security Protocols for Sensor Networks using Algebraic Specification Techniques *CAI 2007*, LNCS 4728, Springer.

Ongoing research

- Case studies
- A license language for Mobile DRMs based on OMA REL.

Ideas

- Combine formalisms based on process algebra such as π-calculus with CafeOBJ and look for connections with hidden algebras,
- Build new protocols using the method during the requirement/domain analysis to show the benefits.
- Semantics of mobile systems as Kripke structures and institutions.

Protocol Algebra based on Behavioural Specification

- Protocol Specifications as behavioural objects
- Definitions:

1. Protocol run/execution as a sequence of states
2. Equivalence of protocols as behavioural equivalence
3. Subsumption of protocol runs
4. Similarity of protocol runs
5. Sub-protocol relation

Protocol composition

- Three different approaches to protocol composition
  - Composing protocols as composing systems (parallel protocol composition with hierarchical object composition technique)

  e.g. composing two simple communication protocols in parallel to take the same protocol with more participants. The invariant properties are preserved in the compound protocol.

Protocol composition

- Composing sequences of messages (sequential approach) - behavioural inheritance can be used

e.g. security protocols

- When a protocol uses services offered by other protocols – protocol specification import

e.g. protocol stacks

Protocol Algebra

- Inspired by module algebra

1. Protocol sum
2. Protocol import
3. Parallel composition
4. Synchronized composition
5. Subsumption
6. Sub-protocol
7. Renaming

Advantages

- Reusability of verified protocols
- Build complex protocols from simpler ones
- Reasoning about protocols
- All these based on CafeOBJ/Behavioural specification

Future research

- Case studies
- Composition of security protocols under the conditions of Strand Space Theory encoding in CafeOBJ
- Build libraries of verified protocol specifications to reuse them.

Thank you !

Questions?

iouranos@central.ntua.gr

http://users.ntua.gr/iouranos