Reliable Model Checking for WSNs

8. GI / ITG KuVS Fachgespräch Drahtlose Sensornetze
13. – 14. August 2009

Ch. Appold
Chair of Computer Science V

Table of Contents

- *Introduction*
- *Particularities of WSNs with regard to verification*
- *Implementing a Traffic Light Synchronization Protocol*
- *Communication characteristics and verification of WSNs*
- *Conclusion and Outlook*

Introduction

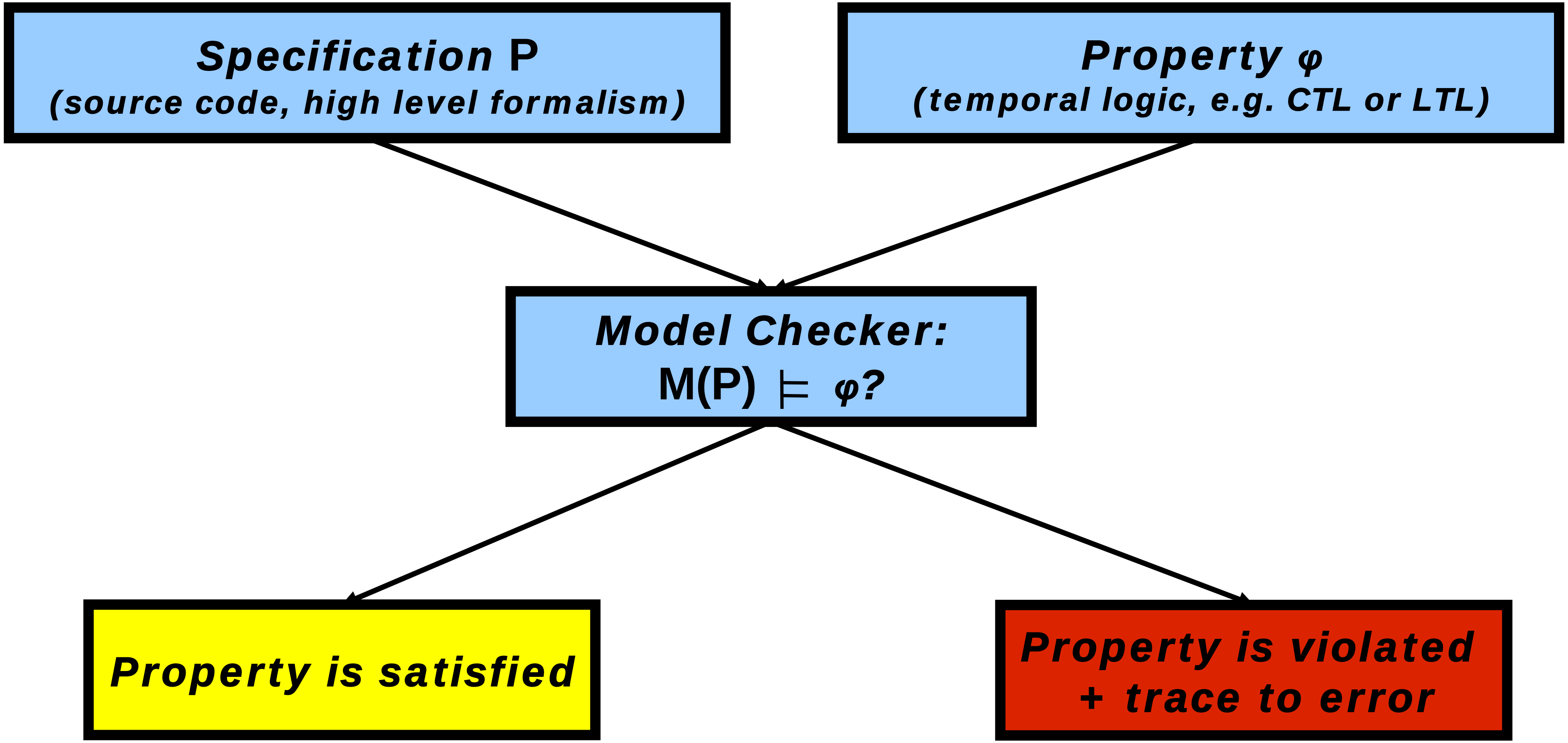
Introduction

- *Verification techniques:*
  - *Simulation:*
    - *stimulation of a system with input patterns*
    - *check if the system behaves as desired*
    - *no exhaustive analysis of system behavior*
    - *complex errors often cannot be detected*
  - *Formal Verification:*
    - *examination of all possible system behaviors*
    - *allows reliable detection of complex errors*

Introduction

- *Formal Verification techniques:*
  - *Theorem Proving*
  - *Model Checking*
- *Model Checking:*
  - *fully-automated through tools called* ***Model Checkers***
  - *given a finite-state model of a system and a formal property, exhaustive investigation whether property holds for that model*
  - *counterexample generation if a property is violated*

- *Model Checking Process:*



Particularities of WSNs with regard to verification

Particularities of WSNs with regard to verification

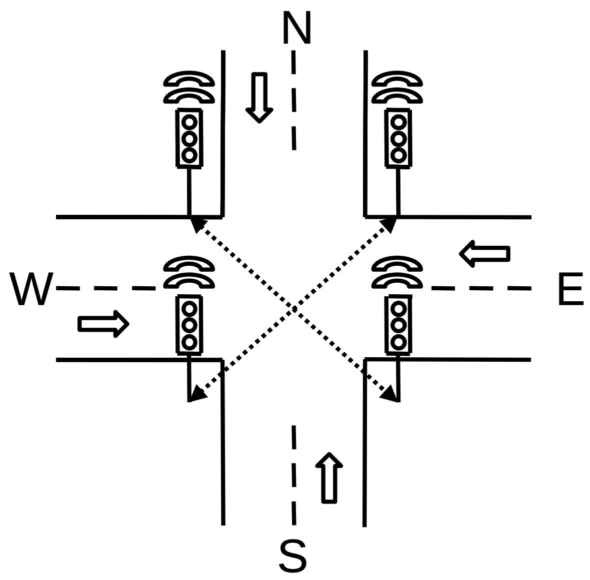
- *Verification of WSNs is a highly non-trivial task*
  - *a single sensor node (hardware+software) can be very complex*
  - *WSNs can consist of a large number of sensor nodes and verification of distributed systems is hard*
- *Additionally communication is wireless*
  - *wireless communication has some particularities, e.g. occurrence of*
    - *transmission errors and collisions*
    - *radio wave propagation variations*

Implementing a traffic light synchronization protocol

Ch. Appold
Chair of Computer Science V

Traffic Light Synchronization Protocol

- *Case Study: Verification of a traffic light synchronization protocol at 4-way road intersections with the Model Checker NuSMV*



road intersection with traffic lights

Important safety-critical property:

→ only diagonally arranged traffic lights can show green or yellow at the same time

Other desirable properties:

→ no deadlock

→ fair allocation of green phases

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

Communication characteristics and verification of WSNs

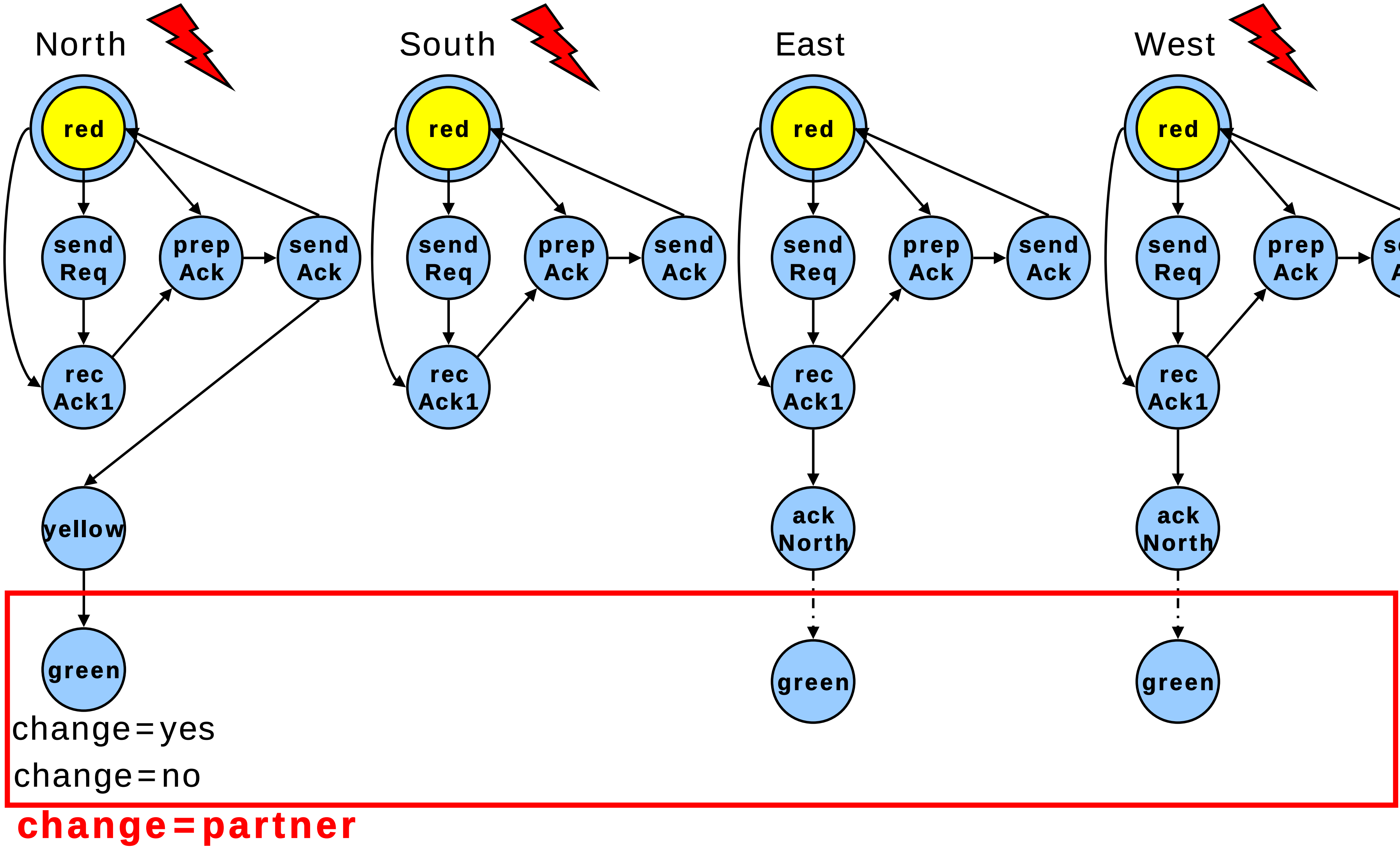
8. GI / ITG KuVS Fachgespräch Drahtlose Sensornetze
13. – 14. August 2009

Ch. Appold
Chair of Computer Science V

- *Extract of the verification model for the traffic light at north:*

```
init(cState) := red;
next(cState) :=
        case
                state = red & sendReqSouth & !collision : recAck1;
                state = red & (sendReqEast | sendReqWest) & !collision : prepAck;
                state = red & chanFree & changeAllowed=yes & boolInput : sendReq;

                state = sendReq : recAck1;

                state = recAck1 & sendAckEast & !collision : ackEast;
                state = recAck1 & sendAckWest & !collision : ackWest;
                state = recAck1 & (sendReqEast | sendReqWest) & !collision : prepAck;

                state = ackEast & sendAckWest & !collision & !(changeAllowed=partner) :
ackPartner;

                state = ackWest & sendAckEast & !collision & !(changeAllowed=partner) :
ackPartner;

                state = ackPartner & sendAckSouth &!collision : yellow;

                state = prepAck & boolInput & chanFree : sendAck;

                state = sendAck & changeAllowed=partner : yellow;
                state = sendAck & !(changeAllowed=partner) : red;

                state = yellow & direction=down : green;
                ...
        esac;
```

- *Non-observance of variations of radio wave propagation*



- *Non-observance of variations of radio wave propagation can circumvent the detection of safety-critical errors*
- *For reliable verification of WSNs it's necessary to include them in the verification model*
- *Because of the state space explosion problem abstract models which contain at least all relevant behaviors are necessary*
- *In our work we have developed some suitable abstractions, e.g. for*
  - *variations of radio wave propagation*
  - *a MAC protocol with carrier sense and a randomized backoff procedure*

Conclusion and Outlook

Conclusion and Outlook

- *Often system components of WSNs cannot be verified isolated*
- *A model of the communication characteristics can be necessary for reliable verification*
- *Even models of other system components, like e.g. timers or parts of operating systems, could be necessary*
- *Especially for non-verification experts, suitable and faultless abstractions should be available*
- *Future work:*
  - *Development of suitable abstractions for several other WSN components*
  - *Improvement and examination of verifiability of dynamic topologies*

Questions?