Reliable Model Checking for WSNs
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
- **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
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:

- **Specification P**
  - (source code, high level formalism)

- **Property \( \varphi \)**
  - (temporal logic, e.g. CTL or LTL)

**Model Checker:**

\[ M(P) \models \varphi? \]

- **Property is satisfied**
- **Property is violated + trace to error**
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
Case Study: Verification of a traffic light synchronization protocol at 4-way road intersections with the Model Checker NuSMV

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
Communication characteristics and verification of WSNs
Extract of the verification model for the traffic light at north:

\[
\begin{align*}
\text{init}(c\text{State}) & := \text{red}; \\
\text{next}(c\text{State}) & := \\
\text{case} & \\
\text{state} & = \text{red} \& \text{sendReqSouth} \& \neg \text{collision} : \text{recAck1}; \\
\text{state} & = \text{red} \& (\text{sendReqEast} | \text{sendReqWest}) \& \neg \text{collision} : \text{prepAck}; \\
\text{state} & = \text{red} \& \text{chanFree} \& \text{changeAllowed=yes} \& \text{boolInput} : \text{sendReq}; \\
\text{state} & = \text{sendReq} : \text{recAck1}; \\
\text{state} & = \text{recAck1} \& \text{sendAckEast} \& \neg \text{collision} : \text{ackEast}; \\
\text{state} & = \text{recAck1} \& \text{sendAckWest} \& \neg \text{collision} : \text{ackWest}; \\
\text{state} & = \text{recAck1} \& (\text{sendReqEast} | \text{sendReqWest}) \& \neg \text{collision} : \text{prepAck}; \\
\text{state} & = \text{ackEast} \& \text{sendAckWest} \& \neg \text{collision} \& \neg (\text{changeAllowed=} \text{partner}) : \text{ackPartner}; \\
\text{state} & = \text{ackWest} \& \text{sendAckEast} \& \neg \text{collision} \& \neg (\text{changeAllowed=} \text{partner}) : \text{ackPartner}; \\
\text{state} & = \text{ackPartner} \& \text{sendAckSouth} \& \neg \text{collision} : \text{yellow}; \\
\text{state} & = \text{prepAck} \& \text{boolInput} \& \text{chanFree} : \text{sendAck}; \\
\text{state} & = \text{sendAck} \& \text{changeAllowed=} \text{partner} : \text{yellow}; \\
\text{state} & = \text{sendAck} \& \neg (\text{changeAllowed=} \text{partner}) : \text{red}; \\
\text{state} & = \text{yellow} \& \text{direction=} \text{down} : \text{green}; \\
\end{align*}
\]
Communication characteristics and verification of WSNs

- Non-observance of variations of radio wave propagation

North

- red
  - send Req
  - prep Ack
  - send Ack
  - rec Ack1

- yellow
  - send Req
  - prep Ack
  - send Ack
  - rec Ack1

- green
  - change=yes
  - change=no

change=partner

South

- red
  - send Req
  - prep Ack
  - send Ack
  - rec Ack1

- yellow
  - send Req
  - prep Ack
  - send Ack
  - rec Ack1

- green

East

- red
  - send Req
  - prep Ack
  - send Ack
  - rec Ack1

- yellow
  - send Req
  - prep Ack
  - send Ack
  - rec Ack1

- green
  - ack North

West

- red
  - send Req
  - prep Ack
  - send Ack
  - rec Ack1

- yellow
  - send Req
  - prep Ack
  - send Ack
  - rec Ack1

- green
  - ack North
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
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?