Model Checking the EAP-NOOB Protocol

Aleksi Peltonen, Mohit Sethi, Tuomas Aura

**EAP-NOOB protocol background**
- New IoT appliance has **no owner or domain, no credentials** for cloud or Wi-Fi
- EAP-NOOB:
  - Connects the device to access network
  - Registers the device to AAA server/cloud
- Security from a **single user-assisted out-of-band** message between peer device and AAA server

**Modelling EAP-NOOB**
- Modelled with mCRL2 (micro Common Representation Language 2)
- Goals of model checking:
  - Protocol simulation and visualisation
  - Debugging the specification, liveness and safety properties
    - Reachability of good and bad states
    - **Deadlock freedom**
    - **Recovery from errors and timeouts**
    - Handling persistent vs. ephemeral data
  - **Detecting persistent denial of service**
    - Recovery after message loss and manipulation

**Results and changes**
In the **protocol**:
- Recovering from rejected nonces caused by attackers or unreliable channels
- Recovering from expired out-of-band messages caused by timeouts
- Handling of redundant out-of-band messages caused by delays or replays

In the **implementation**:
- Recovering from message type mismatches

In the **modelling language**:
- Detected and reported a bug in the linearisation of user-defined type aliases