The following full text is a publisher’s version.

For additional information about this publication click this link.
http://hdl.handle.net/2066/34748

Please be advised that this information was generated on 2018-02-12 and may be subject to change.
Revealed incorrectness upon receiving payload in I2-SENT or I2BIS-SENT.

- Revealed possible deadlock with optional retransmitting I2 / I2bis messages.
- Clarified confusion about responder nonce.

Revealed several other ambiguities, omissions and inconsistencies. Acknowledged by SHIM6 draft authors. Will be incorporated in new IETF proposal.

FORMALIZING SHIM6
AN IETF PROPOSED INTERNET STANDARD IN UPPAAL
Matthijs Mekking\textsuperscript{1,2}, Wouter Wijngaards\textsuperscript{1}, Frits Vaandrager\textsuperscript{2}, Theo Schouwen\textsuperscript{2}
\textsuperscript{1}Foundation NLnet Labs
\textsuperscript{2}Institute for Computing and Information Sciences, Radboud University Nijmegen

matthijs@nlnetlabs.nl
wmekking@science.ru.nl

Background

Multihoming
- A technique to increase the reliability of a network connection.
- Features redundancy, load sharing, performance and policy.
- Current multihorning practices (IPv4) impose a threat on address and routing scalability.
- SHIM6 is a proposal by the IETF to provide multihorning that solve those issues.
- No formal methods have been applied to the draft specification.

Aim: improve the quality of the specification by applying formal methods.

How SHIM6 works
- IP roles: SHIM6 splits the two semantics of an IP address (end point identifier and locator role).
- Initial contact: Normal data communication between end point identifiers, no SHIM6 needed.
- Context Establishment: Communication to exchange multihorning information. Data communication remains normal.
- Failure detection: Messages are transmitted to detect a link failure.
- Locator pair exploration: In case of a link failure, a new locator needs to be selected. Locators are mapped back at the host to the end point identifier. Transport session remains stable. Communication resumes with SHIM6 data packets that provide mapping information.

Formalization and Verification

UPPAAL
An integrated tool environment for modelling, validation and verification of real-time systems modelled as networks of timed automata, extended with data types.

Properties:
- \(A[] \) not deadlock
- \(\exists (h_1: \text{HostType}) \exists (h_2: \text{HostType}) (h_1 \neq h_2 \land \text{heuristics}[h_1][h_2]) \rightarrow \exists (h_3: \text{HostType}) \exists (h_4: \text{HostType}) (h_3 \neq h_4 \land \text{established}(h_3, h_4))\)

Results

- Revealed incorrectness upon receiving payload in I2-SENT or I2BIS-SENT.
- Revealed possible deadlock with optional retransmitting I2 / I2bis messages.
- Clarified confusion about responder nonce.

Revealed several other ambiguities, omissions and inconsistencies. Acknowledged by SHIM6 draft authors. Will be incorporated in new IETF proposal.

Future Work

UPPAAL: Improve model to verify on scale. Add failure detection and exploration. Extend UPPAAL verifier language. Indicate model state space.


Further Information

SHIM6: http://www.shim6.org
http://tools.ietf.org/wg/shim6/
http://www.ietf.org/html.charters/shim6-charter.html

UPPAAL: http://www.uppaal.com