FORMALIZING SHIM6
AN IETF PROPOSED INTERNET STANDARD IN UPPAAL
Matthijs Mekking1, Wouter Wijngaards1, Frits Vaandrager1, Theo Schouten1
1 Foundation NLnet Labs
2 Institute for Computing and Information Sciences, Radboud University Nijmegen

Revealed incorrectness upon receiving pay-load in I2-SENT or I2BIS-SENT.
Revealed possible deadlock with optional re-transmitting I2 / I2bis messages.
Clarified confusion about responder nonce.

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 loca-tor role).
Initial contact Normal data communication between end point identifiers, no SHIM6 needed.
Context Establishment Communication to exchange multihoming 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

UPPAAL
An integrated tool environment for modelling, validation and verifica-tion of real-time systems modelled as networks of timed automata, extended with data types.
Properties:
A[] not deadlock
exists(h1:HostType) exists(h2:HostType)
    (h1 != h2 and heuristics[h1][h2]) -->
forall(h3:HostType) forall(h4:HostType)
    (h3 != h4 imply Context(h3, h4).established)

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.htm
UPPAAL: http://www.uppaal.com

References
[2] Foundation NLnet Labs
[3] Institute for Computing and Information Sciences, Radboud University Nijmegen

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

http://www.ietf.org/html.charters/shim6-charter.htm
http://tools.ietf.org/wg/shim6/
http://www.ietf.org/html.charters/shim6-charter.html
http://www.shim6.org
http://www.uppaal.com

Results
• Revealed incorrectness upon receiving pay-load in I2-SENT or I2BIS-SENT.
• Revealed possible deadlock with optional re-transmitting I2 / I2bis messages.
• Clarified confusion about responder nonce.

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