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.

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 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 end point identifier. Transport session remains stable. Communication resumes with SHIM6 data packets that provide mapping information.

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

\[\text{exists}(h1: \text{HostType}) \text{ exists}(h2: \text{HostType}) \]

\[ (h1 \neq h2 \text{ and heuristics}[h1][h2]) \rightarrow \]

\[ \text{forall}(h3: \text{HostType}) \text{ forall}(h4: \text{HostType}) \]

\[ (h3 \neq h4 \text{ imply Context}(h3, h4).\text{established}) \]

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
