(n+1)sec protocol over unreliable no global order chat protocols

March 11, 2016

Contents

1 transport assumption:

1.1 the transport is unreliable in the sense that some messages might not arrive.

1.2 the transport does not have a global order in the sense that some participants see messages in different orders

2 Reliability and order during key agreement

- If only some of participants does not receive a session establishment session, they will complain by asking for the sender to be kicked out of the conversion, in response those who received the corresponding message will re-transmit the missed message.

- Message order is only important during the join process when the joiner sends its share. If two current participants have different view about which joiner has send their key first then they will go with a session with smaller hash value.

3 Reliability during a session:

- If a participant does not acknowledge a message the sender will resend it.
- When the transport is unreliable, the transport protocol build a partial order and compute the global order based on collapsing the partial order using time of arrival.
- If global order differs among participants we reshuffle messages based on their hash to reach consistent order between participants.