MODULE *skeenAlgorithm*

EXTENDS TLC, $Naturals$, $FiniteSets$, $Sequences$

CONSTANTS $NPROCESS$, $MESSAGES$

VARIABLES pc, $sent$, $pending$, $received$, lc, $messages$

ASSUME $(NPROCESS \in Nat) \land (MESSAGES \neq \{\})$
ASSUME $(NPROCESS > 1)$

$vars \triangleq \langle pc, sent, pending, received, lc, messages \rangle$

$Processes \triangleq 1 \,..\, NPROCESS$

$Init \triangleq$
$\land\ messages = [i \in Processes \mapsto MESSAGES]$
$\land\ pending = [i \in Processes \mapsto \{\}]$
$\land\ received = [i \in Processes \mapsto \{\}]$
$\land\ sent = [i \in Processes \mapsto [bcast \mapsto \{\},\ ts \mapsto \{\},\ sn \mapsto \{\}]]$
$\land\ pc \in [Processes \to \{\text{“BCAST”},\ \text{“”}\}]$
$\land\ lc\ = [i \in Processes \mapsto 0]$

$UpponBCAST(self) \triangleq$
$\land\ (pc[self] = \text{“BCAST”}) \land (messages[self] \neq \{\})$
$\land$ LET $currentMessage \triangleq$ CHOOSE $x \in messages[self] :$ TRUE
IN $\land\ sent' = [i \in Processes \mapsto [sent[self]$ EXCEPT $!.bcast = sent[self].bcast \cup \{[source \mapsto self,\ m$
$\land\ messages' = [messages$ EXCEPT $![self] = messages[self] \setminus \{currentMessage\}]$
$\land$ UNCHANGED $\langle lc, pending, pc, received \rangle$

$ReceivedBCAST(self) \triangleq$
$\land\ pc[self] \neq \text{“SN”}$
$\land\ \exists\, m \in sent[self].bcast :$
$\land\ m \notin pending[self]$
$\land\ pending' = [pending$ EXCEPT $![self] = pending[self] \cup \{m\}]$
$\land\ sent' = [sent$ EXCEPT $![m.source].ts = sent[m.source].ts \cup \{[source \mapsto self,\ message \mapsto m.messag$
$\land\ lc' = [lc$ EXCEPT $![self] = lc[self] + 1]$
$\land$ UNCHANGED $\langle received, pc, messages \rangle$

$MaxTSAllProcess(S) \triangleq$ CHOOSE $t \in S : \forall\, s \in S : s.ts \leq t.ts$

$ReceivedTS(self) \triangleq$
$\land\ pc[self] \neq \text{“SN”}$
$\land$ LET $msgs \triangleq sent[self].ts$
IN $\land\ Cardinality(msgs) = NPROCESS$
$\land$ LET $maxTS \triangleq MaxTSAllProcess(msgs).ts$
IN $\land\ \exists\, m \in msgs :$
$\land\ [source \mapsto self,\ message \mapsto m.message,\ ts \mapsto maxTS] \notin sent[self].sn$

$\land\ sent' = [i \in Processes \mapsto [sent[self] \text{ EXCEPT } !.sn = sent[self].sn \cup \{[source \mapsto$
$\land\ pc' = [pc \text{ EXCEPT } ![self] = \text{“SN”}]$
$\land$ UNCHANGED $\langle pending, received, lc, messages\rangle$

FIX RECEIVED

$Accept(self) \triangleq$
$\land\ (Cardinality(MESSAGES) = Cardinality(sent[self].sn))$
$\land\ pc' = [pc \text{ EXCEPT } ![self] = \text{“AC”}]$
$\land\ received' = [received \text{ EXCEPT } ![self] = sent[self].sn]$
$\land$ UNCHANGED $\langle sent, pending, lc, messages\rangle$

$Steps(self) \triangleq$
$\lor\ UponBCAST(self)$
$\lor\ ReceivedBCAST(self)$
$\lor\ ReceivedTS(self)$
$\lor\ Accept(self)$
$\lor$ UNCHANGED $vars$

$Next \triangleq (\exists\, self \in Processes : Steps(self))$

$Fairness \triangleq \text{WF}_{vars}(Next)$

$Spec \triangleq Init \land \Box[Next]_{vars}$

$TypeOK \triangleq$
$\land\quad pc \in [Processes \to \{\text{“BCAST”}, \text{“SN”}, \text{“AC”}, \text{“”}\}]$

Properties

$Agreement \triangleq \Box((\forall\, self \in Processes : pc[self] = \text{“AC”}) \Rightarrow \Diamond(\exists\, self \in Processes : pc[self] = \text{“AC”}))$

$GetMessage \triangleq$ CHOOSE $m \in MESSAGES$: TRUE

Validity $\triangleq \text{WF}_{\_\langle\rangle}(\forall\, p \in Processes : \langle p, GetMessage\rangle \in deliveryBuffer[p])$

Integrity $\triangleq$ ()

$TotalOrder \triangleq$ ()