MODULE *crdt*

EXTENDS TLC, $FiniteSets$, $Naturals$, $Sequences$
CONSTANTS $MAX\_TIMESTAMP$, $KEYS$, $VALUES$, N_NODES
VARIABLES $timestamp$, $values$, $deliverQueues$

$vars \triangleq \langle timestamp, values, deliverQueues \rangle$
$nodeIds \triangleq 1 \,..\, N\_NODES$

$DeliverSet(n, t, k, v) \triangleq$
  LET $previous \triangleq \{\langle tp, kp, vp \rangle \in values[n] : kp = k\}$ IN
  IF $previous = \{\} \lor \forall \langle tp, kp, vp \rangle \in previous : tp < t$ THEN
    $values' = [values$ EXCEPT $![n] = (values[n] \setminus previous) \cup \{\langle t, k, v \rangle\}]$
   ELSE
    UNCHANGED $values$

$DeliverDelete(n, t) \triangleq$
  $values' = [values$ EXCEPT $![n] = \{\langle tp, k, v \rangle \in values[n] : tp \neq t\}]$

$Deliver(n, command, payload) \triangleq$
  $\lor\ command =$ "set"
    $\land\ DeliverSet(n, payload[1], payload[2], payload[3])$
  $\lor\ command =$ "delete"
    $\land\ DeliverDelete(n, payload)$

$Broadcast(n, command, payload) \triangleq$
  $\land\ Deliver(n, command, payload)$
  $\land\ deliverQueues' = [$
     $i \in nodeIds \mapsto$
      IF $i = n$ THEN
        $deliverQueues[i]$
       ELSE
        $Append(deliverQueues[i], \langle command, payload \rangle)$
    $]$

$RequestSet(n, k, v) \triangleq$
  $\land\ timestamp' = timestamp + 1$
  $\land\ Broadcast(n,$ "set", $\langle timestamp, k, v \rangle)$

$RequestDelete(n, k) \triangleq$
  $\exists \langle t, kp, v \rangle \in values[n] :$
    $\land\ kp = k$
    $\land\ Broadcast(n,$ "delete", $t)$

$RequestSetOnNode \triangleq$
  $\land\ timestamp < MAX\_TIMESTAMP$
  $\land \exists \langle n, k, v \rangle \in nodeIds \times KEYS \times VALUES : RequestSet(n, k, v)$

$RequestDeleteOnNode \triangleq$

$\land \exists \langle n,\, k\rangle \in nodeIds \times KEYS : RequestDelete(n,\, k)$
$\land$ UNCHANGED $timestamp$

$DeliverOnNode \triangleq$
$\exists\, n \in nodeIds :$
$\land\, Len(deliverQueues[n]) > 0$
$\land \exists \langle command,\, payload\rangle \in \{Head(deliverQueues[n])\} :$
$Deliver(n,\, command,\, payload)$
$\land\, deliverQueues' = [deliverQueues$ EXCEPT $![n] = Tail(deliverQueues[n])]$
$\land$ UNCHANGED $timestamp$

$DeliverQueuesIsEmpty \triangleq$
$\forall\, n \in nodeIds : Len(deliverQueues[n]) = 0$

$Terminating \triangleq$
$\land\, DeliverQueuesIsEmpty$
$\land$ UNCHANGED $vars$

$Init \triangleq$
$\land\, values = [i \in nodeIds \mapsto \{\}]$
$\land\, deliverQueues = [i \in nodeIds \mapsto \langle\rangle]$
$\land\, timestamp = 1$

$Next \triangleq$
$\lor\, RequestSetOnNode$
$\lor\, RequestDeleteOnNode$
$\lor\, DeliverOnNode$
$\lor\, Terminating$

$Spec \triangleq\, Init \land \Box[Next]_{vars} \land \mathrm{WF}_{vars}(DeliverOnNode)$

$AllValuesEqual \triangleq$
$\forall \langle n1,\, n2\rangle \in nodeIds \times nodeIds :$
$values[n1] = values[n2]$
$EventuallyConsistent \triangleq \Diamond\Box\, AllValuesEqual$