MODULE *Broadcast*

The specification caputers the *DAG* base reliable broadcast to disseminate shares over a peer to peer network.

The broadcast enables nodes to know which nodes have revceived the message by using implicit acknowledgements. The broadcast is not a *BFT* broadcast. We depend on the higher layers to provide that.

Does this open this broadcast to a *DDoS* attack? Yes, and our argument remains that $p2p$ network can resist *DDoS* attacks by other means.

First pass - We assume no processes failures or messages lost.

EXTENDS *Naturals*, *Sequences*

CONSTANT

Proc, Set of processes
Data,
Nbrs

VARIABLES

sent_by, Set of messages sent by processes to their neighbours
recv_by Set of messages received by processes

$Message \triangleq [from : Proc,\ data : Data]$

$Init \triangleq$
$\quad \land\ sent\_by = [m \in Message \mapsto \{\}]$
$\quad \land\ recv\_by = [m \in Message \mapsto \{\}]$

$TypeInvariant \triangleq$
$\quad \land\ sent\_by \in [Message \to Proc]$
$\quad \land\ recv\_by \in [Message \to Proc]$

SendTo(m, p) - send message m to neighbour p

$SendTo(m,\ p) \triangleq$
$\quad \land\ m.from \neq p$ Don't send to self
$\quad \land\ m.from \notin sent\_by[m]$ Don't send again - we can add decay here
$\quad \land\ \langle m.from,\ p\rangle \in Nbrs$ Send only to neighbours
$\quad \land\ sent\_by' = [sent\_by \text{ EXCEPT } ![m] = @ \cup \{p\}]$
$\quad \land$ UNCHANGED $\langle recv\_by\rangle$

RecvAt(m, q) - receive message m at q. This can be received from forwards

$RecvAt(m,\ q) \triangleq$
$\quad \land\ \exists\, p \in Proc : p \in sent\_by[m]$ Some process has sent the message
$\quad \land\ q \notin recv\_by[m]$ Not already received by q
$\quad \land\ recv\_by' = [recv\_by \text{ EXCEPT } ![m] = @ \cup \{q\}]$
$\quad \land$ UNCHANGED $\langle sent\_by\rangle$

Forward$(m,\ p,\ q)$ - forward message m from p to q
- enabling condition - m has been sent by some process, q has received the message, q is not the sender
- effect - p forwards the message m to its nbrs

$$
\begin{aligned}
&\mathit{Forward}(m,\ p,\ q) \triangleq \\
&\qquad \land \exists\, r \in \mathit{Proc} : r \in \mathit{sent\_by}[m] \quad \text{Some process has sent the message} \\
&\qquad \land p \neq q \quad \text{Don't forward to self} \\
&\qquad \land \langle p,\ q \rangle \in \mathit{Nbrs} \quad \text{Forward only to neighbour} \\
&\qquad \land p \in \mathit{recv\_by}[m] \quad p \text{ has received } m \\
&\qquad \land \mathit{sent\_by}' = [\mathit{sent\_by} \ \text{EXCEPT}\ ![m] = @ \cup \{q\}] \\
&\qquad \land \text{UNCHANGED}\ \langle \mathit{recv\_by} \rangle
\end{aligned}
$$

$$
\begin{aligned}
&\mathit{Next} \triangleq \exists\, p \in \mathit{Proc},\ q \in \mathit{Proc},\ m \in \mathit{Message} : \\
&\qquad \lor \mathit{SendTo}(m,\ p) \\
&\qquad \lor \mathit{RecvAt}(m,\ p) \\
&\qquad \lor \mathit{Forward}(m,\ p,\ q)
\end{aligned}
$$

$$\mathit{Spec} \triangleq \mathit{Init} \land \Box[\mathit{Next}]_{\langle \mathit{sent\_by},\, \mathit{recv\_by} \rangle}$$

THEOREM $\mathit{Spec} \Rightarrow \Box\, \mathit{TypeInvariant}$

* Modification History
* Last modified *Tue Mar* 07 19:55:10 *CET* 2023 by *kulpreet*
* Created Sun *Mar* 05 15:04:04 *CET* 2023 by *kulpreet*