Verification of a Leader Election Protocol

Marco Devillers
David Griffioen
Judi Romijn
Frits Vaandrager

IEEE 1394 “Firewire”

- high-performance multi-media serial-bus protocol
- quick, reliable, cheap transfer of audio and video
- hot-pluggable
- future standard for In Home Digital Networks?

Tree Identification Phase

Second phase after initialization/reset of network

Meant to elect a leader ("root") amongst the nodes

Nodes go trough two phases:

1. Initial phase: wait until on all (but one) ports a parent request has been sent

2. Second phase: acknowledge parent requests and send parent request on remaining link (if any)

Problems:

- Contention: nodes send parent requests to each other

- Cycles: the protocol deadlocks

Tree Identification Phase (cnt)

Network Topology

Digraph $\mathbf{G} = (\mathbf{V}, \mathbf{E})$ with

- $\mathbf{V}$ finite non-empty set of *vertices*
- $\mathbf{E} \subseteq \mathbf{V} \times \mathbf{V}$ set of *edges*

We assume

1. $(v, w) \in \mathbf{E} \Leftrightarrow (w, v) \in \mathbf{E}$
2. $(v, v) \notin \mathbf{E}$
3. for each pair of vertices v, w, there is a unique sequence of distinct vertices $v_0, \ldots, v_n$ such that (1) $v_0 = v$, (2) $v_n = w$, (3) for all $0 \leq i < n$, and $(v_i, v_{i+1}) \in \mathbf{E}$.

If $e{=}(v, w)$ then source$(e) = v$, target$(e) = w$, $e^{-1} = (w, v)$.

The TIP I/O Automaton

Internal: ADD_CHILD, $CHILDREN\_KNOWN$, $RESOLVE\_CONTENTION$, ACK
Output: $ROOT$
State Variables: $init : \mathbf{V} \to \mathbf{Bool}$
$contention : \mathbf{V} \to \mathbf{Bool}$
$root : \mathbf{V} \to \mathbf{Bool}$
$child : \mathbf{E} \to \mathbf{Bool}$
$mq : \mathbf{E} \to \mathbf{Bool}^*$

Init: $\forall v, e : init[v]$
$\wedge\ \neg contention[v]$
$\wedge\ \neg root[v]$
$\wedge\ \neg child[e]$
$\wedge\ mq[e] = \mathsf{empty}$

$ADD\_CHILD(e : \mathbf{E})$
Pre: $\wedge\ init[\mathsf{target}(e)]$
$\wedge\ mq[e] \neq \mathsf{empty}$
Eff: $child[e] := 1$
$mq[e] := \mathsf{tl}(mq[e])$

$ACK(e : \mathbf{E})$
Pre: $\wedge\ \neg init[\mathsf{target}(e)]$
$\wedge\ mq[e] \neq \mathsf{empty}$
Eff: $contention[\mathsf{target}(e)] := \neg\mathsf{hd}(mq[e])$
$mq[e] := \mathsf{tl}(mq[e])$

$ROOT(v : \mathbf{V})$
Pre: $\wedge\ \neg root[v]$
$\wedge\ \forall e \in \mathsf{to}(v) : child[e]$
Eff: $root[v] := 1$

$CHILDREN\_KNOWN(v : \mathbf{V})$
Pre: $\wedge\ init[v]$
$\wedge\ \forall e, f \in \mathsf{to}(v) : child[e] \vee child[f] \vee e = f$
Eff: $init[v] := 0$
for $e \in \mathsf{from}(v)$ **do**
$mq[e] := \mathsf{append}(child[e^{-1}], mq[e])$

$RESOLVE\_CONTENTION(e : \mathbf{E})$
Pre: $\wedge\ contention[\mathsf{source}(e)]$
$\wedge\ contention[\mathsf{target}(e)]$
Eff: $child[e] := 1$
$contention[\mathsf{source}(e)] := 0$
$contention[\mathsf{target}(e)] := 0$

The SPEC I/O Automaton

Output: $ROOT$
State Variables: $done : \mathbf{Bool}$ **Init**: $\neg done$
$ROOT(v : \mathbf{V})$
Pre: $\neg done$
Eff: $done := 1$

Refinement

Claim Let $r \in states(TIP) \to states(SPEC)$ be the function defined by the state predicate:

$$SPEC.done \quad \Leftrightarrow \quad \exists_v TIP.root[v]$$

Then r is a refinement mapping from TIP to $SPEC$.
More specifically:
1) $s \in start(TIP) \to r(s) \in start(SPEC)$
2) $s \xrightarrow{a} s' \wedge s \text{ reachable} \wedge a \text{ internal} \to r(s) = r(s')$
3) $s \xrightarrow{a} s' \wedge s \text{ reachable} \wedge a \text{ external} \to r(s) \xrightarrow{a} r(s')$

How to prove it?

Invariants

$I_1(v) \triangleq init[v] \;\rightarrow\; \neg contention[v]$

$I_2(e) \triangleq init[\mathsf{source}(e)] \;\rightarrow\; mq[e] = \mathsf{empty}$

$I_3(e) \triangleq init[\mathsf{source}(e)] \;\rightarrow\; \neg child[e]$

$I_4(e, f, v) \triangleq \begin{array}{l} \mathsf{target}(e) = \mathsf{target}(f) = v \wedge e \neq f \\ \quad \rightarrow\; init[v] \vee child[e] \vee child[f] \end{array}$

$I_5(e) \triangleq \mathsf{length}(mq[e]) \leq 1$

$I_6(e) \triangleq init[source(e)] \;\rightarrow\; \neg contention[\mathsf{target}(e)]$

$I_7(e) \triangleq child[e] \;\rightarrow\; mq[e] = \mathsf{empty}$

$I_8(e) \triangleq contention[\mathsf{target}(e)] \;\rightarrow\; mq[e] = \mathsf{empty}$

$I_9(e) \triangleq mq[e] \neq \mathsf{empty} \wedge \mathsf{hd}(mq[e]) \;\rightarrow\; child[e^{-1}]$

$I_{10}(e) \triangleq mq[e] \neq \mathsf{empty} \wedge \neg\mathsf{hd}(mq[e]) \;\rightarrow\; \neg child[e^{-1}]$

$I_{11}(e) \triangleq child[e] \;\rightarrow\; \neg child[e^{-1}]$

$I_{12}(e) \triangleq contention[\mathsf{source}(e)] \;\rightarrow\; \neg child[e]$

$I_{13}(e) \triangleq root[\mathsf{target}(e)] \;\rightarrow\; child[e]$

$I_{14}(e, f) \triangleq child[e] \wedge \mathsf{source}(e) = \mathsf{target}(f) \wedge e \neq f^{-1} \;\rightarrow\; child[f]$

Key Invariant in Refinement Proof

I_{14} and I_{11} together with the fact that $\mathbf{G}$ is a tree imply that there is always at most one node for which all incoming links are child links:

$$I_{15}(v) \triangleq (\exists_v \forall_{e \in \mathsf{to}(v)} child[e]) \rightarrow (\exists!_v \forall_{e \in \mathsf{to}(v)} child[e])$$

Termination

Theorem All executions of TIP are finite

Proof We define a norm function of the states of TIP.

Let s be a state of TIP. Then:

$$\begin{aligned} I(s) &= |\{v \in V \mid s \models init[v]\}| \\ U(s) &= |\{e \in E \mid s \models \neg child[e] \wedge \neg child[e^{-1}]\}| \\ M(s) &= |\{e \in E \mid s \models mq[e] \neq \mathsf{empty}\}| \\ R(s) &= |\{v \in V \mid s \models \neg root[v]\}| \end{aligned}$$

Define $norm(s) = (I(s), U(s), M(s), R(s))$.

Let $\prec$ denote usual lexicographical ordering on tuples.

Then we can prove, using invariants I_3, I_5, I_7 and I_{12}, that for each transition $s \xrightarrow{a} t$ of TIP with s reachable, $norm(t) \prec norm(s)$.

Fair Trace Inclusion

In order to prove that TIP implements $SPEC$, i.e., fair trace inclusion, it suffices to prove that the refinement function r maps quiescent states of TIP to quiescent states of $SPEC$.

This amounts to proving that if a state of TIP has no outgoing transitions, a leader had been elected.

In order to prove this, two additional invariants are required:

$$I_{16}(e) \stackrel{\Delta}{=} init[\mathsf{target}(e)] \wedge \neg child[e] \wedge mq[e] = \mathsf{empty} \;\rightarrow\; init[\mathsf{source}(e)]$$

$$I_{17}(e) \stackrel{\Delta}{=} \neg init[\mathsf{source}(e)] \wedge mq[e] = \mathsf{empty} \wedge \neg child[e] \wedge \neg child[e^{-1}] \;\rightarrow\; contention[\mathsf{target}(e)]$$

Concluding Remarks

- Invariant and refinement proofs mechanically verified using PVS
- Other features of the protocol (root contention, cycle detection,..) treated as refinements of TIP automaton
- Current IEEE 1394 standard ambiguous and incomplete