Verification of the FDDI protocol with Kronos *

C. Daws
daws@imag.fr

A. Olivero
alfredo@dc.uba.ar †

S. Tripakis
tripakis@imag.fr

S. Yovine
yovine@imag.fr

VERIMAG
Centre Equation, 2 Ave. Vignate, 38610 Gières, France
http://www-verimag.imag.fr

The FDDI communication protocol

FDDI (Fiber Distributed Data Interface) [1] is a high performance fiber optic token ring Local Area Network. In this section we show the verification of the temporal mechanism that limits the possession time of the token by each station.

Specification

We consider a network composed by N identical stations $S_1, \ldots, S_N$ and a ring, where the stations can communicate by *synchronous* messages with high priority and *asynchronous* messages with low priority.

Station. Each station S_i can be either waiting for the token ($\texttt{Idle}_i$), in possession of the token and executing the synchronous transmission ($\texttt{T}_i$, $\texttt{ST}_i$) or in possession of the token and executing the asynchronous transmission ($\texttt{T}_i$, $\texttt{AT}_i$). The two clocks a station uses to control the possession time of the token are called TRT_i (Token Rotation Timer) and THT_i (Token Holding Timer).

- TRT_i counts the time since the last reception of the token by the station. This clock is reset to zero each time the station S_i takes the token.
- THT_i counts the time since the last reception of the token, added to the time elapsed since the precedent one, given by the value of the clock TRT_i just before it is re-initialized.

*In "The tool Kronos", DIMACS Workshop on Verification and Control of Hybrid Systems, October 1995. Lecture Notes in Computer Science 1066, Springer-Verlag.

†Depto. de Computación, FCEyN, Universidad de Buenos Aires, Argentina.

When the station S_i receives the token (action $\texttt{TT}_i$), the clock THT_i takes the value of the clock TRT_i, TRT_i is reset to zero, and the station S_i starts sending synchronous messages ($\texttt{BS}_i$). The duration of the synchronous transmission ($\texttt{ST}_i$) is given, for each station S_i, by a constant SA_i (Synchronous Allocation).

When the synchronous transmission ends (action $\texttt{ES}_i$), the station has the possibility of starting the transmission of asynchronous messages (action $\texttt{BA}_i$) if the current value of THT_i minus the time of synchronous transmission SA_i is greater than a global constant of the system called $TTRT$ (Target Token Rotation Timer). Before $THT_i - SA_i$ reaches the value $TTRT$, the station must release the token ($\texttt{RT}_i$), ending the asynchronous transmission ($\texttt{EA}_i$) if this one has began. The behavior of the station S_i is described by the timed automaton $\mathbf{Station}_i$ of the Figure 1(a).

Ring. The ring controls the transmission of the token between two consecutive stations S_i and S_{i+1}. There is a delay of td (Token Delay) time units, measured by the clock T, in this transmission. The Figure 1(b) shows the timed automaton **Ring** that models the ring for two stations.

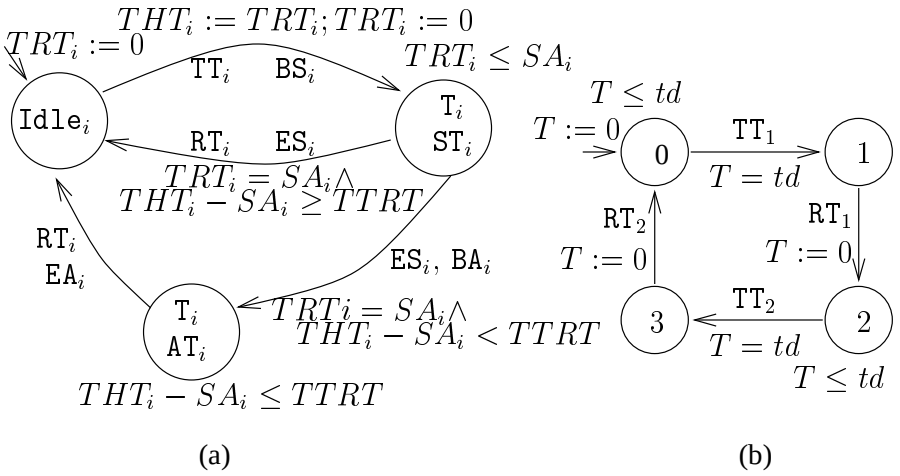

Figure 1: Station_i (a) ; Ring (b)

System. The timed automaton that models the protocol is obtained as the parallel composition $\mathbf{FDDI}_N = \mathbf{Ring} \parallel \mathbf{Station}_1 \parallel \ldots \parallel \mathbf{Station}_N$ where the automata synchronize through the actions $\texttt{TT}_i$ and $\texttt{RT}_i$.

Verification

We verify here two properties of the FDDI protocol.

Bounded time for accessing the ring. The time elapsed within two consecutives receptions of the token by any station is bounded by a constant c_1. We can express this property in TCTL with the following formula:

$$(\mathtt{ST}_i \wedge T = 0) \Rightarrow \forall\Diamond_{\leq c_1} \mathtt{enable(TT}_i\mathtt{)} \tag{1}$$

where c_1 is equal to $TTRT + 2N.SA_i$, and $\mathtt{enable(TT}_i\mathtt{)}$ characterizes the symbolic states where the edge labeled $\mathtt{TT}_i$ is enabled.

Bounded time for sending asynchronous messages. Each idle station will send asynchronous messages before a time c_2. The formula of TCTL that describe this property is:

$$\mathtt{Idle}_i \Rightarrow \forall\Diamond_{\leq c_2} \mathtt{AT}_i \tag{2}$$

where c_2 is equal to $(N-1).TTRT + 2N.SA_i$.

References

[1] R. Jain. *FDDI handbook: high-speed networking using fiber and other media.* Addison-Wesley, 1994.