TECNICAS PARA LA DESCRIPCION FORMAL Y VERIFICACION DE PROTOCOLOS

M. GARCIA HOFFMANN

Diversos autores han propuesto técnicas para la especificación y verifica-- ción de protocolos de comunicación. En este artículo se consideran los trabajos más significativos realizados hasta la fecha en este campo.

Se presentan primeramente las técnicas que basan la especificación del protocolo en alguna forma del modelo de estados y que emplean el análisis de - la alcanzabilidad de la máquina resultante para la verificación. A continuación se discuten los métodos que utilizan lenguajes formales y de alto nivel para la descripción del protocolo y aserciones para el estudio de sus - propiedades. Por último se consideran las técnicas más recientes orientadas a la automatización parcial o total del diseño de protocolos.

La presentación en forma comparada y crítica de los diversos métodos permite perfilar las características que debería satisfacer toda técnica de diseño de protocolos de comunicación.

En un próximo artículo se desarrollarán los principios básicos de una nueva metodología de diseño de protocolos que se compara favorablemente con las - ya existentes.

1. INTRODUCCION

En los últimos tiempos viene prestándose una atención creciente al estudio de los siste-- mas informáticos distribuidos. Los multiprocesadores y las redes de computadores son -- ejemplos de este tipo de sistemas. Los microprocesadores posibilitan la concepción de -- nuevas arquitecturas multimicroprocesador -- formadas por un número elevado de microprocesadores que se comunican entre sí de forma - bien definida, sin necesidad de un control - centralizado.

Los objetivos y características de los diversos sistemas difieren notablemente, existiendo, sin embargo, ciertos aspectos comunes a todos ellos. Uno de los aspectos comunes a - todos los sistemas distribuidos es la necesidad de intercambiar información entre los -- elementos que lo integran.

El intercambio de información entre los componentes de un sistema distribuido se denomina comunicación, entendiéndose por protocolo de comunicación el conjunto de reglas que la rigen. La materialización hardware o software de estas reglas recibe asimismo la denominación de protocolo.

El diseño y estudio de protocolos de comunicación comporta varias etapas entre las que se cuentan la definición del protocolo, su - análisis cualitativo y cuantitativo y su realización práctica y documentación.

El primer aspecto, la definición del protocolo, es de suma importancia. La descripción - de gran parte de los protocolos existentes - se ha hecho en lenguaje escrito. Esta forma de descripción introduce en la especificación del protocolo las ambigüedades propias del - lenguaje humano con el consiguiente riesgo - de interpretaciones distintas por parte de - las personas encargadas de la realización -- práctica del protocolo. Diversos autores han propuesto métodos formales para la definición de protocolos que, por otra parte, se pres-- tan mejor que el lenguaje escrito al estudio de sus características.

El objeto del estudio cualitativo de protocolos es la validación de su estructura lógica y su verificación. Por validación se entiende la prueba de si en su funcionamiento el - protocolo satisface o no ciertas propiedades

- M. García-Hoffmann, de la Càtedra de Mètodes Informàtics de la E.T.S.E.I.B. Av. Diagonal, 647. Barcelona-28.
- Article rebut el Desembre del 1979.

lógicas como la ausencia de bloqueos, comportamiento cíclico, etc. La verificación consiste en demostrar que la comunicación se realiza según las pautas que el diseñador intentó imponer en la definición del protocolo. Ello exige una definición clara de los objetivos del protocolo. Practicamente todos los protocolos han de realizar dos funciones básicas denominadas función de control y función de transporte. La verificación de la función de control suele referirse a la inicialización y mantenimiento de la sincronización de las entidades que realizan el protocolo. El comportamiento correcto de la función de transporte debe tomar en cuenta la posibilidad de alteración, pérdida, duplicación y reordenación de los mensajes.

El entorno en el que está inmerso el protocolo juega también un papel importante en el estudio cualitativo. Es necesario tener en cuenta las características del medio de transmisión -desde una simple conexión punto a punto, a una red de conmutación de paquetes-, así como las características de la comunicación del protocolo con sus usuarios.

El análisis cuantitativo de protocolos aborda problemas tales como la determinación de la eficiencia de la comunicación, su banda pasante, etc.

En el resto del artículo se relacionan brevemente las técnicas propuestas por diversos autores para la especificación y estudio cualitativo de protocolos cuya bibliografía ha sido recientemente recopilada por la IFIP Working Group 6.1, Section C /16/. Un estudio más detallado de estos temas pueden encontrarse en /17/.

2. MODELOS BASADOS EN MAQUINAS DE ESTADOS FINITOS

Un primer grupo de técnicas son aquellas que basan la descripción de las entidades que realizan el protocolo en alguna forma relacionada con las máquinas de estados finitos. Pueden incluirse en él la modelación mediante redes de Petri, particularmente los trabajos de Merlin /27/, /28/, /29/, Danthine /13/, Bochmann /3/ y Symons /40/; la extensión de la teoría de coloquios realizada por Danthine y Bremer /12/, /13/, /8/, /9/, /14/, los trabajos de Mezzalira y Schreiber sobre modelación de protocolos mediante máquinas secuenciales de estructura variable /30/, /31/ y, por último, los estudios de Bochmann /2/, /39/, /6/ que ha empleado las máquinas de estados finitos para describir los subsistemas de que consta un protocolo.

2.1 Extensiones de las redes de Petri

Se han empleado diversos tipos de grafos bidimensionales para representar el flujo de control y la sincronización entre procesos. Las redes de Petri /35/ constituyen uno de los métodos gráficos más potentes y adecuados para modelar ciertas estructuras de control. Algunos protocolos simples pueden modelarse con redes de Petri. Sin embargo, para la modelación de ciertas características que han de tenerse en cuenta en el estudio de protocolos mas complejos son necesarias algunas extensiones del modelo básico. Estas extensiones están destinadas a dotar a las redes de Petri de una potencia mayor de modelación y decisión.

Para poder incluir el tiempo en la descripción de protocolos Merlin asocia a las barras de transición de una red de Petri básica dos tiempos t_i^* y t_i^{**}. El tiempo t_i^* se refiere al tiempo mínimo que ha de transcurrir con todas las condiciones de entrada cumpliéndose, antes de que la barra pueda disparar. El t_i^{**} modela el tiempo que pueden estar las condiciones de entrada cumpliéndose sin que la barra se dispare.

Con este modelo Merlin ha estudiado protocolos de telefonía /28/ y algunas propiedades generales de protocolos como es la recuperabilidad, es decir, la propiedad de que ocurriendo un fallo el proceso vuelva a comportarse correctamente en un tiempo finito /29/. Un resultado interesante de su trabajo es la demostración informal de que no puede hablarse de protocolos de comunicación asíncronos recuperables si no se incluye en el modelo el tiempo de ejecución de los procesos.

A fin de modelar procesos complejos Nutt introdujo en 1972 las denominadas redes de evaluación /33/, /32/. Estas son redes de Petri en la que cada transición lleva asociada una regla propia de disparo. Cuando una barra --

dispara se quitan los puntos de un subconjunto determinado de los lugares de entrada y se colocan puntos en un subconjunto de los lugares de salida. Se incluye también un tiempo de ejecución de la transición. Danthine utiliza en /13/ un modelo híbrido que incluye redes de Petri temporales y algunos aspectos de las redes de evaluación de Nutt para crear un módulo básico mediante el cual ha descrito el protocolo de transporte de la red Cyclades.

Keller /25/ ha propuesto un modelo similar al de Nutt. El modelo es una red de Petri y un conjunto ξ de variables. Cada barra de transición lleva asociado un precicado P_t y una acción F_t. El predicado P_t es función de algunas variables de ξ; la acción F_t modifica alguna de estas variables. El estado del sistema queda definido por la situación y número de puntos y el valor de los elementos de ξ. Cuando todas las entradas de una transición t contienen al menos un punto y P_t es cierto, la transición puede disparar siguiendo las reglas normales de las redes de Petri. Bochmann /3/ ha extendido este modelo para estudiar protocolos de comunicación.

Las propiedades demostradas para algunas subclases de las redes de Petri, como son los grafos marcados o las redes de Petri de decisión libre, no son generalizables a los modelos mas complejos. Entre estas propiedades destacan la alcanzabilidad de una determinada configuración, la acotación, seguridad y vida de estas. Alguna de ellas son importantes para la verificación de propiedades de los protocolos; por ejemplo, el hecho de que la configuración inicial de una red de Petri esté viva y a salvo garantiza la ausencia de bloqueos. Desgraciadamente, el problema de decidir si una configuración está viva y a salvo es, en general, de una complejidad extraordinaria.

2.2 Extensiones de la teoría de coloquios

Se han estudiado diversas formas de describir coloquios, entre otras, gramáticas formales, autómatas y grafos. Los coloquios son un caso particular de la interacción entre procesos y pueden ser útiles para la descripción y verificación de propiedades de protocolos. Le Moli /26/ ha desarrollado una formalización de la teoría de coloquios que permite describir axiomáticamente el funcionamiento de los protocolos. Las acciones llevadas a cabo por un protocolo pueden considerarse como el intercambio de información entre dos o más interlocutores (coloquio). Un protocolo de determinado nivel se expresa mediante dos interlocutores que se comunican entre sí y que, individualmente, interaccionan con el nivel superior que utiliza el protocolo. Definida la estructura de los interlocutores y el conjunto de entradas que pueden aceptar, así como las salidas que se generan, el protocolo queda definido por un conjunto de reglas de funcionamiento que adoptan una forma matricial. Este modelo topa con el problema de la dimensionalidad si se desea estudiar un protocolo complejo que utilice variables internas.

Para tratar protocolos complejos Danthine ha propuesto una extensión del modelo de coloquios que permite representar las variables y la lógica interna de los procesos integrantes del protocolo /12/, /13/, /8/, /9/. La idea central del método es dividir la unidad de proceso del modelo de coloquios en dos partes, una que tomará en cuenta el contexto y, otra, que funciona como la del modelo original. Para la descripción de la máquina de contexto se emplean lenguajes de alto nivel, lo que conduce a un método de descripción de protocolos híbrido. La inclusión del contexto en el modelo de coloquios se ha empleado para describir el protocolo de transporte de Cyclades /13/, existiendo programas destinados a conseguir una automatización parcial de la modelación /8/ y verificación /9/. En /14/ se presenta una formalización del modelo ampliado de coloquios mediante teoría de autómatas finitos.

Basándose en la teoría de coloquios Mezzalira y Schreiber /30/, /31/, han ideado un sistema para describir protocolos representando los interlocutores mediante máquinas secuenciales de estructura variable. Su estudio aborda únicamente coloquios en los que toman parte dos interlocutores que alternan el envío de mensajes. El funcionamiento de las máquinas secuenciales de estructura variable se expresa mediante grafos de transición de estados o grafos de mensajes. A partir de formas reducidas de los grafos pueden construirse unas matrices, cuyos elementos serán

funciones lógicas, que permiten definir el comportamiento de los interlocutores y del coloquio. La definición de los grafos de mensajes es un aspecto interesante que permite estudiar la interacción entre los procesos con mayor claridad que con los grafos de estados. Tal vez el aspecto más interesante del método sea la utilización de máquinas con dos tipos de entradas diferentes (mensajes y órdenes) para modelar el interlocutor. Este aspecto se encuentra de nuevo en los trabajos de Danthine y Bremer cuyo fundamento teórico tiene bastantes puntos en común con las ideas expuestas en /30/.

2.3 Máquinas de estados finitos

Bochmann ha estudiado protocolos constituidos por procesos distribuidos y medios de comunicaciones. Cada subsistema se modela mediante una máquina de estados finitos cuyas transiciones puedan ser locales o involucrar la transmisión o recepción de un mensaje /3/, /2/, /6/.

Dados dos procesos que se comunican A y B, se define el conjunto de estados adjuntos a un estado s del proceso A como el conjunto A_s de estados en que puede encontrarse B cuando A está en s. El conocimiento de los estados adjuntos, junto con el estado del medio, permite determinar los estados en que el sistema total puede encontrarse.

La búsqueda de los estados adjuntos requiere el conocimiento de como influyen en un proceso las transiciones del otro. Esta influencia depende del medio de comunicaciones que es, en definitiva, la única vía de sincronización de los procesos. En algunos protocolos simples, tal como los half-duplex o los full-duplex en modo conversacional, puede suponerse que las transiciones asociadas a la transmisión de un mensaje inducen al otro proceso a realizar una transición en la que se recibe el mensaje enviado. En estos casos no es necesario considerar mas que los instantes en que el medio no contiene mensajes, con lo que el estudio se simplifica notablemente.

El modelo del medio vacío permite calcular de un modo simple los estados adjuntos con lo que puede realizarse el análisis de la alcanzabilidad. Sin embargo, la mayoría de procesos full-duplex y los protocolos de nivel superior permiten que un número de mensajes, a veces elevado, se encuentren simultáneamente en tránsito. Bochmann propone expresar el contenido del medio mediante colas definidas por expresiones regulares, admitiendo que el modelo es insuficiente para reflejar todas las propiedades del medio.

Diversos autores han utilizado las secuencias de acciones para estudiar ciertos aspectos del cálculo paralelo /10/, /34/. Las secuencias de acciones realizables por una máquina de estados finitos pueden representarse mediante expresiones regulares. Para demostrar la corrección de un protocolo basta comprobar que la expresión regular que caracteriza la propiedad que se desea probar y la expresión regular que sigue el protocolo en su funcionamiento son compatibles /2/.

El método adolece de las faltas características de la modelación de protocolos por máquinas. Los protocolos de cierta complejidad en los que cada subsistema posee variables propias y realiza lógica interna conducen a máquinas con un número excesivo de estados.

2.4 Conclusiones

Los modelos expuestos en este apartado representan los procesos integrantes del protocolo empleando métodos relacionados con la máquina de estados finitos. Estas representaciones son adecuadas para realizar el análisis de la alcanzabilidad, que permite determinar los distintos estados a que puede llegar el sistema en su funcionamiento. El estudio se hace impracticable en los protocolos de cierta complejidad, en los que el número de estados puede ser muy grande.

Los modelos basados en la máquina de estados finitos permiten describir la estructura de control de los protocolos pero no la estructura de datos ni la lógica interna de los procesos. Para solventar estos problemas se sugiere la separación de la máquina en dos niveles; uno que atienda el contexto y otro que refleje las características del control. Esta solución, apta para la descripción de la semántica del protocolo, conduce a descripciones híbridas que hacen difícil el estudio

de sus propiedades mediante métodos formales.

Excepto en las descripciones que utilizan redes de Petri, los procesos se modelan como entidades autónomas que se comunican a través de mensajes. La validación, en este caso, consiste en demostrar que durante la comunicación entre los procesos se cumplen ciertas propiedades. La validación se hace más difícil que la de los modelos que consideran los distintos procesos como elementos integrados en un sistema global. Como contrapartida, el nivel de detalle que puede alcanzarse en la descripción del funcionamiento de cada proceso es mayor, facilitando la realización práctica del protocolo. El análisis de la alcanzabilidad de un sistema modelado globalmente mediante redes de Petri es un problema sin resolver. Se conocen soluciones para ciertas restricciones de las redes de Petri, como son las redes de decisión libre y los grafos marcados. Las restricciones impuestas por estas redes son, en general, excesivas para la modelación adecuada de protocolos.

Tan solo el modelo propuesto por Merlin permite la inclusión del tiempo de ejecución en la descripción de los procesos, si bien, no se ofrece ningún método formal que permita validar las redes de Petri temporales. Sabido es que la modelación adecuada del tiempo es de suma importancia en el estudio de procesos paralelos y, en particular, de los protocolos de comunicación.

Las técnicas de modelación y estudio de protocolos reseñadas en este apartado son adecuadas para la descripción de protocolos relativamente simples, compuestos por dos procesos, y la validación de algunas de sus propiedades. La descripción y verificación de protocolos más complejos requiere técnicas más elaboradas.

3. MODELOS BASADOS EN LENGUAJES FORMALES Y DE ALTO NIVEL

Se reunen en este apartado las técnicas que emplean lenguajes formales y de alto nivel para la especificación y estudio de protocolos de comunicación: los trabajos de Harangozo /23/, /24/ que emplea gramáticas regulares, los de Bochmann /1/, /4/, /5/ y Stenning /38/, que especifican el funcionamiento de protocolos mediante lenguajes de alto nivel y emplean aserciones para demostrar propieades y, finalmente, los de Gouda /18/, /19/, /20/ que ha ideado un lenguaje gráfico de alto nivel orientado al estudio de protocolos.

3.1 Lenguajes formales

Harangozo /23/, /24/ utiliza gramáticas regulares para la descripción de protocolos. Las reglas de interacción entre procesos (protocolos) pueden considerarse generadas por una gramática regular del tipo 3, según la clasificación de Chomsky /11/.

La idea central del método es considerar que el diálogo que se establece entre dos procesos puede considerarse formado por sentencias que generan dos interlocutores. Dado que la secuencia de sentencias de un diálogo sigue unas reglas determinadas puede pensarse en la existencia de una gramática que las genere. Describir un protocolo se reduce a encontrar una gramática cuyas reglas de producción generen correctamente dichas sentencias al aplicarlas a los símbolos elementales que utilizan los interlocutores. El método aborda exclusivamente la descripción sintáctica del protocolo sin considerar los aspectos semánticos del mismo. Es esta una limitación propia de los lenguajes formales.

La descripción de protocolos mediante lenguajes formales es una alternativa interesante de la representación mediante autómatas, particularmente cuando la complejidad de éste lo hace difícilmente comprensible o irrealizable.

3.2 Lenguajes de alto nivel y aserciones

El funcionamiento de un protocolo puede especificarse describiendo las diferentes acciones en un lenguaje de alto nivel. Las propiedades del protocolo que se desea probar se expresan mediante predicados que involucran variables de los diferentes procesos y la demostración consiste en probar que entre la ejecución de los sucesos se cumplen ciertas aserciones.

Stenning /38/ ha descrito un protocolo de --

transporte de esquema de ventana en PASCAL, demostrando que si el protocolo progresa lo hace correctamente, según un criterio determinado. Bochmann /1/ emplea también un lenguaje similar al ALGOL en la descripción de protocolos utilizando aserciones para su verificación.

La demostración de propiedades mediante aserciones no permite estudiar los bloqueos ni garantizar el progreso de un programa. Sabido es que estas características se estudian más facilmente desde la perspectiva de la máquina de estados finitos. Intentando conjugar las posibilidades de ambos métodos Bochmann ha propuesto un modelo en el que el estado del sistema puede expresarse de modo equivalente mediante variables o estados /4/, /5/. Las propiedades referentes a bloqueos y progreso del protocolo se estudian desde la óptica de la máquina de estados finitos mediante el análisis de la alcanzabilidad. Por el contrario, los aspectos semánticos del protocolo pueden considerarse utilizando aserciones adecuadas. El modelo es una generalización de los trabajos de Keller mencionados en el apartado 2 para poder aplicarlo a procesos espacialmente distribuidos.

La descripción de protocolos mediante el modelo híbrido de Bochmann es bastante flexible dado que la equivalencia entre estados y variables permite diversas definiciones. Claramente, existe un compromiso entre la complejidad de la máquina de estados y la definición de acciones variables.

3.3 Lenguajes gráficos de alto nivel

Gouda /18/, /19/, /29/ ha introducido un lenguaje básico de alto nivel que, basándose en cuatro operaciones básicas, permite definir el comportamiento de las denominadas máquinas de protocolos. En sentido amplio, las operaciones corresponden a las sentencias de lectura, escritura, asignación y selección de los lenguajes usuales de alto nivel. Las máquinas están formadas por una estructura de datos y una estructura de control. Para su realización en hardware un sencillo algoritmo permite transformar la máquina de protocolo a otra forma lógicamente equivalente, la máquina digital síncrona, más próxima a la electrónica digital. Para obtener realizaciones en software Gouda sugiere la construcción de un traductor del lenguaje gráfico al lenguaje de alto nivel que se desee.

A fin de estudiar propiedades tales como la ausencia o presencia de bloqueos o la acotación de la comunicación se utiliza una simplificación de la máquina de protocolos denominada máquina SR (send-receive). La máquina SR es una máquina de protocolos sin estados internos y con ciertas restricciones estructurales que refleja exclusivamente el comportamiento externo de esta. La simplificación es de gran interés por dos razones; por una parte muchas de las propiedades sintácticas de los protocolos pueden probarse tomando únicamente en cuenta el comportamiento externo de los procesos que realizan el protocolo. Por otra parte, toda máquina de protocolos que satisfaga un cierto número de propiedades estructurales puede transformarse en una máquina SR equivalente /20/.

Gouda utiliza máquinas de costo probabilístico /18/ para estudiar aspectos de la eficiencia del protocolo. En estas máquinas cada camino de ejecución posible lleva asociado una probabilidad (de que se pase por él) y un costo (por pasar por él).

Las máquinas de protocolos son una herramienta potente para describir el funcionamiento de un protocolo. Sin embargo, el nivel de detalle al que se alcanza impide el estudio del comportamiento lógico del sistema. La máquina SR equivalente de una máquina de protocolos permite, de existir, estudiar la ausencia o presencia de bloqueos y la acotación de la comunicación. Hay que señalar, sin embargo, que las restricciones impuestas en la estructura de las máquinas de protocolos para que exista su máquina SR equivalente y las restricciones impuestas a éstas para que la comunicación sea acotada y carezca de bloqueos son excesivamente severas, haciendo que el método sea dificilmente aplicable a la mayor parte de los protocolos útiles de cierta complejidad.

3.4 Conclusiones

Los lenguajes formales permiten describir en detalle los aspectos sintácticos del funcionamiento de los procesos que forman un proto

colo pero no los aspectos semánticos. La descripción mediante gramáticas compite con las basadas en la máquina de estados finitos, aventajando a estas cuando el número de estados de la máquina hace difícil su representación. Este tipo de descripciones no es adecuado para realizar el estudio de propiedades del protocolo.

La modelación de los procesos mediante lenguajes de alto nivel (gráficos o no) es, probablemente, el mejor método para especificar de forma clara y detallada el funcionamiento de los protocolos de comunicación. Dos son fundamentalmente las limitaciones del estudio de protocolos mediante aserciones. De una parte, la generación y demostración de aserciones es una tarea notablemente compleja, de otra, la prueba de programas mediante aserciones tan solo permite afirmar que si el programa progresa se cumple determinada propiedad. El progreso del programa no queda garantizado.

Gouda ha estudiado las características lógicas de protocolos bajo fuertes restricciones estructurales. En general, estas restricciones son inaceptables cuando se trata de protocolos de cierta complejidad, particularmente cuando el protocolo está compuesto por más de dos procesos.

4. MODELOS ORIENTADOS A LA AUTOMATIZACION DEL ESTUDIO DE PROTOCOLOS

En los últimos tres años se han conseguido avances notables en el estudio de protocolos reales (X.25, HDLC ...) gracias al desarrollo de métodos que permiten la automatización parcial del proceso de diseño y verificación. En este apartado se consideran los trabajos llevados a cabo por el Data Networks Group de IBM, Zurich, /37/, /44/, /41/, /42/, así como los resultados de otro grupo de investigadores del IBM Thomas J. Watson Research Center, que han desarrollado un método para la verificación automática de protocolos descritos en lenguaje de alto nivel /7/. Otros trabajos relacionados con la automatización del estudio y diseño de protocolos pueden encontrarse en /6/, /14/, /22/, /36/, /17/.

4.1 Duólogos y perturbaciones

Zafiropulo /44/ modela protocolos destinados a controlar la interacción entre dos procesos mediante un par de grafos que interaccionan entre sí. Define una matriz de duólogos cuyos elementos son los pares de secuencias de sucesos posibles que los dos procesos pueden seguir en su funcionamiento. El estudio de la corrección de los duólogos es la base de la validación de la estructura lógica de los protocolos.

En el modelo de duólogos la validación se realiza empleando predicados lógicos y su aplicación no es, por tanto, facilmente automatizable. West /43/ ha desarrollado un método gráfico para representar la interacción entre los procesos que, utilizando los mismos principios que el método anterior, conduce a la realización práctica de un programa de validación.

En cualquier caso, las limitaciones del método son dos. Por un lado, solo puede ser aplicada a protocolos que comunican dos procesos y que vuelven a su estado inicial tras un número finito de interacciones. Por otra parte, no pueden validarse protocolos conteniendo bucles que incluyan el estado inicial.

A fin de reducir las limitaciones del método de duólogos West propone una generalización /42/. El sistema se modela globalmente, especificándose el estado mediante una matriz que contiene en su diagonal principal el estado de cada proceso y en sus elementos extradiagonales el estado del medio de comunicaciones que liga los procesos. Se denomina perturbación de un estado a otro al cual se llega ejecutando una transición en un único proceso. Perturbando el estado inicial puede generarse un árbol de ejecuciones que indica los posibles caminos que puede seguir el sistema en su funcionamiento. En cada estado del árbol de ejecuciones deben cumplirse un conjunto de reglas cuya violación conduce a la detección de errores de recepción, bloqueos y saturación de los canales.

La generación del árbol de ejecución está intimamente relacionada con el análisis de la alcanzabilidad de la máquina de estados finitos asociada. La realización automática de los algoritmos puede encontrar limitaciones

en la capacidad de memoria y en el tiempo de cálculo si el número de estados del sistema es muy grande. La complejidad de los protocolos que pueden validarse es difícil de determinar a priori puesto que el número de estados del sistema depende en mayor medida del número de sucesos que eventualmente puedan encontrarse en los canales y del grado de acoplamiento de los procesos, que del número y complejidad de estos. En /42/ se consideran estos aspectos del método concluyéndose que protocolos bastante más complejos que el X.21 pueden validarse sin tomar en cuenta estos problemas.

La modelación mediante grafos de procesos que contienen variables propias es en general inadecuada, por lo que el método encuentra dificultades en la validación de protocolos de transmisión de datos de cierta complejidad.

4.2 Verificación automática de protocolos

Brand y Joyner /7/ han desarrollado un método semiautomático de verificación de protocolos. Las especificaciones del protocolo son programas escritos en lenguajes de alto nivel. El método se basa en la ejecución simbólica de programas /21/ y está relacionado con el método de las perturbaciones /42/. La demostración de propiedades requiere el empleo de aserciones.

El lenguaje empleado en /7/ es similar a un ALGOL extendido para describir procesos paralelos. El método allí expuesto para modelar el paralelismo permite describir cierto tipo de protocolos. Su verificador utiliza como datos de entrada los programas correspondientes a cada proceso y una relación de simulación consistente en una lista de puntos de paro de cada proceso y de una lista de aserciones que han de cumplirse en los puntos de paro. El verificador construye para cada punto de paso un árbol de ejecución, comprobando si la aserción asociada se cumple o no.

El verificador prueba las propiedades reflejadas por las aserciones para todas las combinaciones posibles de acciones. En la búsqueda de caminos de ejecución no se toma en cuenta el tiempo de ejecución de las distintas acciones, lo que en protocolos de cierta complejidad puede conducir a un problema de dimensionalidad al tener que considerar muchos casos que en la realidad no puedan darse. En /42/ se sugiere un método para incluir limitaciones temporales en el texto de los programas que resulta un tanto artificioso.

4.3 Conclusiones

La complejidad de la validación y verificación de protocolos sugiere buscar la ayuda del ordenador para crear métodos de estudio total o parcialmente automáticos. West modela los procesos componentes de un protocolo mediante máquinas de estados finitos que se comunican entre sí. El análisis de la alcanzabilidad se realiza automáticamente, probando todos los posibles caminos de ejecución. Como ya se ha dicho, la modelación mediante máquinas presenta el inconveniente de no permitir la representación de estructuras de datos sin provocar un crecimiento tan grande en el número de estados que haga intratable el problema.

La verificación semiautomática propuesta por Brand y Joyner es, probablemente, el método más potente de los descritos en este trabajo. En contra del método pueden aducirse algunas razones. Por una parte, el modelo de comunicación y sincronización entre procesos escogido está condicionado por el objetivo de la modelación -el estudio de los protocolos de comunicación entre un computador microprogramado y su interfase de entrada/salida-. La utilización de variables comunes para la comunicación y las primitivas de sincronización escogidas parece adecuada para modelar el hardware. Sin embargo, la modelación de protocolos de comunicación puede realizarse mejor con primitivas expresamente diseñadas para modelar el paralelismo.

La ejecución simbólica, como el método de West, considera todas las combinaciones de acciones, al no existir la noción de tiempo de ejecución de los procesos. Se generan por tanto caminos que los procesos no pueden ejecutar en una realización práctica. La reducción del número de estados del árbol es importante por ser el factor que más limita la complejidad de los protocolos que pueden estudiarse.

Mencionemos para concluir la limitación que supone el hecho de que el cálculo de predicados de primer orden -en el que se basa la -- prueba de aserciones- no es decidible. El método puede por tanto fallar en la determinación de si un protocolo es o no correcto respecto a una relación de simulación determinada.

5. CONCLUSION

Del estudio de los diferentes trabajos presentados puede concluirse, como en /39/, que existen fundamentalmente tres formas de abordar el estudio cualitativo de protocolos. La primera se basa en la modelación del protocolo mediante algún método relacionado con el modelo de estados y en el análisis de la alcanzabilidad. La segunda forma se fundamenta en la descripción algorítmica de los elementos constituyentes del protocolo y en la -- prueba de propiedades mediante aserciones. - La tercera es la sintetización de las dos anteriores.

Los modelos de estados son adecuados para estudiar los aspectos de control. Sin embargo, al intentar representar la estructura de datos de los distintos elementos o modelar medios de comunicación complejos se genera un número de estados excesivo. Dentro de este - grupo, algunos autores han propuesto considerar tan solo un número pequeño de estados básicos del sistema, incluyendo en ellos información del contexto. Se consigue así limitar el número de estados totales. Sin embargo, - la aplicación de las técnicas de análisis aptas para los modelos de estados encuentran - aquí grandes dificultades.

La descripción algorítmica de protocolos permite, en general, representar adecuadamente la estructura de datos de los procesos que - forman el protocolo. En el campo de las redes de computadores los métodos de verificación mediante aserciones han permitido verificar la función de transporte de ciertos -- protocolos. Sin embargo, se encuentran serias dificultades en la verificación de la función de control, estrechamente vinculada al modelo de estados.

Los trabajos más recientes intentan aprovechar las ventajas y eludir las limitaciones de los grupos de métodos anteriores. Las descripciones son algorítmicas, pero es necesario modelar de alguna forma los estados a -- que puede llegar el protocolo en su funcionamiento. Los aspectos de control se estudian sobre este modelo mediante el análisis de la alcanzabilidad. Para la verificación se in-- cluyen aserciones sobre el estado y la estructura lógica del protocolo. La demostración - de las aserciones combina el análisis de la alcanzabilidad con las pruebas lógicas sobre las aserciones que hacen referencia a la estructura de datos. Buena parte del éxito de estos métodos en el estudio de protocolos -- reales se debe a la incorporación del computador como ayuda a la verificación. En un -- próximo trabajo se presentará un nuevo método de definición y verificación de protocolos que por sus características puede considerarse incluido en este último grupo.

6. REFERENCIAS

/1/ BOCHMANN, G.V. "Logical verification -- and implementation of protocols". Proc. of the 4th Data Communication Symposium, Québec, 1975.

/2/ BOCHMANN, G.V. "Communication Protocols and Error Recovery Procedures". Proc. - of the ACM Sigcomm/Sigops Interprocess Communications Workshop, Santa Mónica, Ca., 1975.

/3/ BOCHMANN, G.V. "Finite State Description of Communication Protocols". Departement d'Informatique, Univ. de Montreal Pu. #236, Julio 1976.

/4/ BOCHMANN, G.V., CHUNG, R.J. "A Formalized Specification of HDLC Classes of -- Procedures". University of Montreal, Tr n° 265, 1977.

/5/ BOCHMANN, G.V., GECSEI, J. "A Unified - Method for the Specification and Verification of Protocols". Proc. of IFIP'77, Toronto, 1977.

/6/ BOCHMANN, G.V. "Finite State Description of Communication Protocols" Proc. Symposium on Computer Communication Protocols, Liège, 1978.

/7/ BRAND, D., JOYNER, W.H. "Verification of Protocols Using Symbolic Executions" Proc. Symposium on Computer Communication Protocols, Liège, 1978.

/8/ BREMER, J. "Representation Axiomatique d'un Protocol. Description du Programme Reduction". S.A.R.T. 76/19/10, Univ. de Liège, Setiembre 1976,

/9/ BREMER, J. "Verification de la Logique d'un Protocol. Description du Programme Verify". S.A.R.T. 77/03/10, Univ. de Liège, Enero 1977.

/10/ CAMPBELL, R.H., HABERMANN, A.N. "Specification of Process Synchronization by Path Expressions" Proc. of the International Symposium on Operating Systems, Rocquencourt, 1974.

/11/ CLEVELAND, J.C., UZGALIS, R.C. "Grammars for Programming Languages". Elsevier North-Holland, Amsterdam, 1977.

/12/ DANTHINE, A.S., BREMER, J. "Communication Protocols in a Network Context". Proc. of the ACM Sigcom/Sigops Interprocess Communications Workshop, Santa Mónica, Ca., 1975.

/13/ DANTHINE, A., BREMER, J. "An Axiomatic Description of the Transport Protocol of Cyclades". Professional Conference on Computer Networks and Teleprocessing, Aachen, 1976.

/14/ DANTHINE, A.S. "Petri Nets for Protocol Modelling and Verification". Proc. of the Computer Networks and Teleprocessing Symposium, Budapest, Octubre, 1977.

/15/ DANTHINE, A.S., BREMER, J. "Modelling and verification of End-to-End Transport Protocols". Proc. Symposium on Computer Network Protocols, Liège, 1978.

/16/ DAYTON, J.D. "A Bibliography on the Formal Specification and Verification of Computer Network Protocols". Proc. Symposium on Computer Networks Protocols, Liège, 1978.

/17/ GARCIA HOFFMANN, M. "Aportación al estudio de la descripción, validación y verificación de protocolos de comunicación". Tesis Doctoral, E.T.S.Eng. Industrials de Barcelona, 1979.

/18/ GOUDA, M.G., MANNING, E.G. "On the Modelling, Analysis and Design of Protocols. A Special Class of Software Structures". Proc. of the 2nd International Conference on Software Engineering, 1976.

/19/ GOUDA, M.G., MANNING, E.G. "Protocol Machines: a Concise Formal Model and its Automatic Implementation", Proc. of the 3rd Int. Conf. on Comp. Communication, Toronto, 1976.

/20/ GOUDA, M.C. "Protocol Machines: towards a Logical Theory of Communication Protocols". Honeywell Systems' Research Center, 2600 Ridgway Parkway Minneapolis, Minnesota 55413, Nov. 1977.

/21/ HANTLER, S.L., KING, J.C. "An Introduction to Proving the Correctness of Programs". ACM Computing Surveys, v.8, n.3, 1976.

/22/ HAJEK, J. "Automatically Verified Data Transfer Protocols". Proc. of the 1978 Int. Conf. on Comp. Communications, 1978.

/23/ HARANGOZO, U. "An Aproach to Describing a Data Link Level Protocol with a Formal Language". Proc. of the 5th Data Communications Symposium, Snowbird, 1977.

/24/ HARANGOZO, J. "Protocol Definition with Formal Grammars". Proc. Symposium on Computer Communication Protocols, Liège, 1978.

/25/ KELLER, R.M. "Formal Verification of Parallel Programs". Comm. of the ACM, v.19, n.7, 1976, pp. 371-384.

/26/ LE MOLI, G. "A Theory of Colloquies". 1st European Workshop on Computer Networks, Arles, 1973.

/27/ MERLIN, P., FARBER, D.J. "Recoverability of Communication Protocols". IBM Research Report RC 5415 (23664), 1975.

/28/ MERLIN, P.M. "A Methodology for the Design and Implementation of Communication

Protocols". IEEE Trans. on Communica-- tions, v. COM-24, n.6, 1976, pp. 614-621.

/29/ MERLIN, P.M., FARBER, D.J. "Recoverability of Communication Protocols-Implications of a Theoretical Study". IEEE -- Trans. on Communications, v. COM-24, -- n.9, 1976, pp. 1036-1043.

/30/ MEZZALIRA, L., SCHREIBER, F.A. "Designing Colloquies". 1st European Workshop on Computer Networks, Arles, 1973.

/31/ MEZZALIRA, L., SCHREIBER, F. "A Proposal for a Formal Description of Collo-- quies as a Form of Interaction of Se-- quential Machines". Instituto di Electrotecnica e d'Electronica del Politécnico di Milano, Abril, 1973.

/32/ NOE, J.D., NUTT, G.J. "Macro E-Nets for Representation of Parallel Systems", -- IEEE Trans. on Computers, v. C-22, n.8, 1973, pp. 715-727.

/33/ NUTT, G.J. "Evaluation Nets for Compu-- ter System Performance Analysis", AFIPS Conf. Proc. Vol. 41, Part I, 1972, pp. 275-286.

/34/ PETERSON, J.L., BREDT, T.H. "A Comparision of Models of Parallel Computation" Proc. IFIP Congress 74, 1974.

/35/ PETERSON, J.L. "Petri Nets". ACM Computing Surveys, v.9, n.3, 1977, pp. 223-252.

/36/ POSTEL, J.B. "A Graph Theory Analysis - of Computer Communications Protocol". - UCLA-ENG 7410, Univ. California, Los Angeles, 1974.

/37/ RUDIN, H. et Al. "Automated Protocol Validation: One Chain of Development". -- Proc. Symposium on Computer Communica-- tion Protocols, Liège, 1978.

/38/ STENNING, N.V. "A Data Transfer Proto-- col", Computer Networks, v.1, n.2, 1976, pp. 99-110.

/39/ SUNSHINE, S.A. "Survey of Protocol Definition and Verification Techniques". -- Proc. Symposium on Computer Network Protocols, Liège, 1978.

/40/ SYMONS, F.J.W. "Modelling and Analysis of Communication Protocols Using Numerical Petri Nets". Ph.D. Thesis, Dep. of Electrical Engineering Science, Univ. - of Essex, G.B., 1978.

/41/ WEST, C.H., Zafiropulo, P. "Automated - Validation of a Communication Protocol: The CCITT x.21 Recommendation". IBM J. Res. Develop., v.22, n.1, 1978, pp. 59-71.

/42/ WEST, C.H. "General Technique for Communications Protocol Validation". IBM Journal of Research and Development, v.22, n.4, 1978, pp. 392-404.

/43/ WEST, C.H. "An Automated Technique of - Communications Protocol Validation". -- IBM Journal of Research and Development, v. 26, n.8, 1978, pp. 1271-1275.

/44/ ZAFIROPULO, P. "Protocol Validation by Duologue-Matrix", IEEE Trans. on Communications, v. COM-26, n.8, 1978, pp. -- 1187-1194.