

基于有限状态机与 Petri 网的系统分析与设计

姜春英^{1,2}, 房立金¹, 赵明扬¹

(1. 中国科学院沈阳自动化研究所, 沈阳 110016; 2. 中国科学院研究生院, 北京 100039)

摘 要: 从系统组成、功能需求和体系结构方面介绍了航天器空间对接仿真系统的实时多任务控制系统, 基于有限状态机和 Petri 网方法对其进行了单任务级和多任务级的分析建模, 并以此为基础完成系统的详细设计, 其中应用分叉和资源共享模型实现了系统的同步和互斥问题。实际应用中使用工程化和模块化的方法完成系统设计, 系统运行性能良好。试验证明这种分析设计方法合理可行。

关键词: 有限状态机; Petri 网; 航天器; 实时多任务系统

System Analysis and Design Based on Methods of FSM and Petri Net

JIANG Chun-ying^{1,2}, FANG Li-jin¹, ZHAO Ming-yang¹

(1. Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang 110016;

2. Graduate School of Chinese Academy of Sciences, Beijing 100039)

【Abstract】 A real-time multitask system for the space aircraft docking simulation is presented and the system composition, the functions requirement and the system structure are introduced. Based on the methods of finite state machine (FSM) and Petri net, the single task and the multitask models are built respectively. According to these models, the system design is accomplished. By applying the fork and the resources sharing prototypes, the synchronization and the mutex functions can be realized. In actual application, the engineering and modularization methods are used and the system performances are good as a result. Experimental results show that the methods for the system analysis and design are rational and feasible.

【Key words】 finite state machine (FSM); Petri net; space aircraft; real-time multitask system

软件工程活动包括需求、设计、实现、确认以及支持等活动。需求分析是软件开发过程中至关重要的一个环节, 它的质量决定整个项目软件系统的成败^[1,2]。大量实践统计表明: 大系统软件开发中 70% 的错误是由需求和软件设计阶段引入的。为了提高软件需求和软件设计的质量, 软件工程界提出了需求分析工程技术和各种软件建模技术。针对实时多任务系统的需求分析和系统设计, 系统瞬时性和任务的并发行是最难描述的, 同时也是最重要的因素。通常基于状态转换和事件驱动模型和方法比较适合用于描述实时系统, 例如有限状态机(FSM)和Petri网模型^[3]。

有限状态机是实时系统设计中的一种数学模型, 它的优点在于简单, 能够直观看到状态间的关系。用有限状态机来分析和设计系统, 不仅有利于掌握系统的结构, 还有利于掌握系统的动态特性。但应用在实时多任务系统中的最大缺点是: 当系统部件转移较多时, 状态数随之增加, 导致复杂性显著增长; 另外, 任何时刻系统只能有一个状态, 无法表示并发性, 不能描述异步并发的系统。

为了消除这些缺点, Petri网应运而生。Petri网是一种使用图形方式对实时系统进行需求规格说明的技术, 用来定义多进程、多任务系统的数学模型, 易于描述系统的并发、竞争、同步等特性, 并可用于评价和改进系统。如今, Petri网已经大量应用于包括硬件、软件和社会领域等各种系统的模型化^[3]。为了更高效可靠地实现实时多任务系统的设计, 解决瞬时、同步和并发等问题, 本文应用软件工程化设计思想, 提出基于有限状态机和Petri网方法的模块化系统分析方法, 并将其应用于航天器空间对接仿真系统的设计应用中。

1 控制系统需求概述

1.1 航天器空间对接仿真系统介绍及其功能需求

航天器空间对接的自由度仿真系统, 主要是对我国载人航天工程正在研制的带有差动式缓冲阻尼系统的异体同构周边式对接机构进行评价鉴定试验。采用半物理仿真的方法模拟两个飞行器在设定对接初始条件下的对接动力学过程。整个系统由两个质量、惯量不等的主动和被动五自由度试验台组成。其中, 主动试验台用来模拟具有 8 000kg 质量的追踪航天器, 整个试验台长 8m。被动试验台模拟质量为 2 000kg 的目标航天器, 整个试验台的长度为 3m。这里, 航天器的质量和惯量由质量惯量模拟件来仿真。航天器的纵向 x 、横向 z 平面运动和绕 y 轴的转动 3 个自由度由气浮平台来实现, 绕 x 轴和 z 轴的转动由安装在气浮平台上的滚转与俯仰转动模拟装置来实现。主、被动试验台的主梁的端部分别装有主、被动对接机构。整个试验台示意图如图 1 所示^[4]。

实现仿真系统空间对接的运动和控制的仿真功能, 要求系统具有实时多任务系统的特点。分析系统的功能和性能需求如下:

- (1) 按照试验要求具有流程控制功能
- (2) 具有手动、自动运动功能, 具有较高的重复定位精度;
- (3) 具有对气缸等动作部件的控制功能;
- (4) 具有对五自由度位姿和其它相关信息的实时测量功能, 位姿

作者简介: 姜春英(1978 -), 女, 博士研究生, 主研方向: 机器人机构学, 机电测控系统, 软件系统分析; 房立金、赵明扬, 博士生导师、研究员

收稿日期: 2006-11-03 **E-mail:** jchyy@sia.cn

测量的采样周期不大于 T_1 (T_2 通常小于 10ms), 其它信息采样周期不大于 T_2 (T_2 通常取 10ms);

- (5)具有数据实时计算功能, 周期不大于 T_2 ;
- (6)具有实时通信功能, 周期不大于 T_2 ;
- (7)具有系统实时报警保护功能, 监视采样周期不大于 T_2 ;
- (8)具有记录和显示功能和人机交互功能。

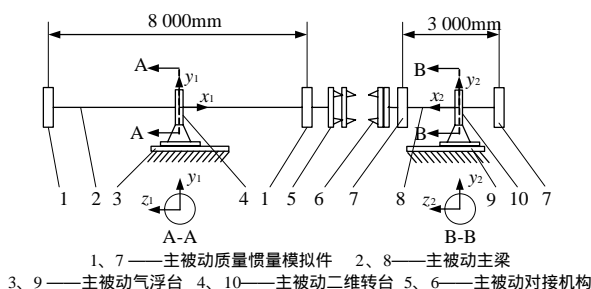


图1 航天器空间对接试验仿真系统示意图^[4]

1.2 控制系统的体系结构及任务分析

根据上述分析的系统功能和性能需求概述, 设计控制系统的体系结构。采用上下两层结构, 下位机主要完成对数据的实时采集、计算、记录功能, 对系统运动和动作的实时控制功能, 与上位机的实时通信功能; 上位机主要完成对下位机传输的数据状态信息的接收、处理功能, 发送对下位机的运动和动作控制指令功能, 状态数据显示和人机交互操作功能。上下层之间通过 CAN 总线进行网络通信。控制系统体系结构和数据流如图 2 所示。

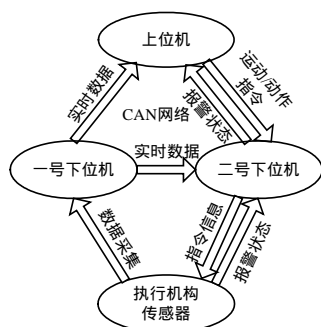


图2 控制系统体系结构和数据流示意图

根据图 2 所示, 进行如下任务分析:

一号下位机主要承担系统测量功能, 需要完成包括数据的实时测量、计算和通信传输的以 T_1 为周期的任务。由于上述任务功能具有连续性要求, 因此可以在一个时钟中断服务程序中完成, 不产生资源共享时存在的资源冲突问题。

二号下位机主要承担通信功能、数据计算功能、系统运动动作驱动功能、系统运行状态采集功能、报警保护处理功能和试验流程控制功能。由于试验流程控制只有功能要求, 执行过程没有强实时性要求, 因此单独设计为一个任务, 在主程序中执行; 其它几项功能的实现具有 T_2 执行周期的实时性要求, 设计为多个任务模块在同一时钟中断服务程序中执行。

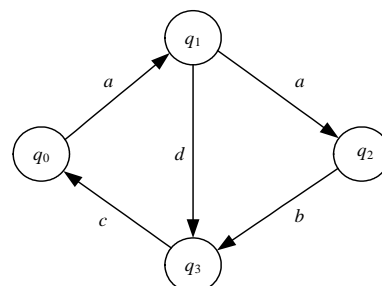
上位机的显示功能、人机交互功能和通信传输功能分属于 3 个进程。

2 有限状态机和 Petri 网建模

2.1 有限状态机方法单任务建模

有限状态机由有限个状态和相互之间的转移构成, 在任何时刻系统总是处于一个特定的状态。当接收到一个输入事

件时, 状态机产生一个输出, 同时伴随着状态的转移。有限状态机的组成包括: 一个有限的状态集合 Q , 一个有限的输入集合 I , 变迁函数 $: Q \times I \rightarrow Q$ 。有限状态机通常用图的方式表示, 其节点代表状态。若在状态 q_1 接收到某个输入事件 I 后转向 q_2 状态, 就在图中画一条从 q_1 到 q_2 的箭头线, 并在弧线上标记 I 。此时, 其变迁函数 $(q_1, I)=q_2$ 。利用FSM有限状态机方法进行任务内部逻辑的分析、设计和开发是一个理想的选择。如图 3(a)所示表示一个简单的有限状态机^[3]。



(a)简单的有限状态机

T_1 时钟中断服务程序



(b) T_1 时钟中断服务程序FSM建模

图3 有限状态机建模示意图

以一号下位机的软件设计分析为例, 使用有限状态机方法对其进行系统分析建模。图 3(b)所示为一号下位机的 T_1 时钟中断服务程序中的任务分析模型。 T_1 时钟中断服务程序不断循环执行, 当“数据采集”模块执行后, 判断采集的仿真系统数据是否完整, 正确得到后转到“计算”模块, 采集到的数据需要计算和转换完成后才能被传输, 用于控制和完成记录。这里的有限状态集合 Q 包括: 数据采集状态、计算处理状态和数据传输状态; 有限的输入集合 I 包括采集数据和计算数据; 变迁函数关系指数据处理完成的条件;

在系统中, 可以应用有限状态机方法对各个任务模块进行单任务级建模分析。上述的任务过程使用有限状态机方法表示, 过程简单, 条件和状态清晰明了。

2.2 Petri 网方法多任务系统建模

Petri 网的组成成分包括: 一个有限的库所(place)集合, 表示系统的状态; 一个有限的变迁(transition)集合, 表示系统中的事件; 一个有限的连接库所到变迁或者反向的有向箭头的集合。

任务可以有 3 种状态: 活动, 要求, 存取。任务的行为周期性地通过 3 个状态。使用 3 个库所(p_{active} , $p_{requesting}$ 和 $p_{accessing}$)描述了它的 3 个状态, 使用 3 个变迁($t_{request}$, t_{start} 和 t_{end})描述了对 3 个状态的修改。在这个模型中有一个令牌, 表示为任务实体, 初始时它被包含在库所 p_{active} 中。资源的行为可以用两个库所(p_{idle} 和 p_{busy})描述它的两个状态, 使用两个变迁(t_{start} 和 t_{end})描述对两个状态的修改。在这个模型中有一个令牌, 表示为资源实体, 初始时它被包含在位置 p_{idle} 中。通过变迁 t_{start} 和 t_{end} 的合并, 可以得到一个任务和一个资源合并的模型。图 4(a)表示一个简化的任务存取资源的Petri网模型。图 4 中的库所用圆圈表示, 变迁由短横线表示(通常由矩形表示), 在库所的圆圈中的黑点表示令牌(token)^[5]。

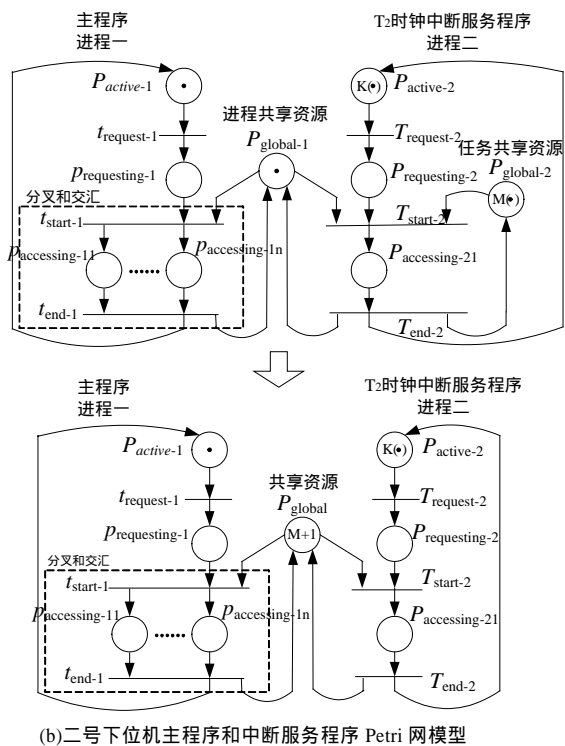
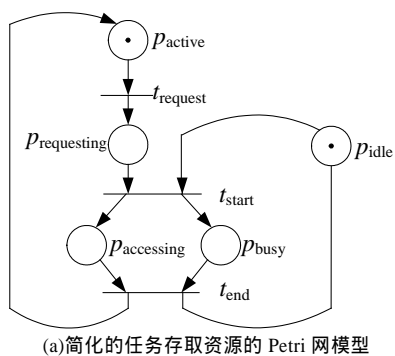


图 4 Petri 网建模示意图

在应用过程中,任何 Petri 网的扩展和应用应当考虑特定的应用环境,既要增加模型描述和理解能力,又要便于系统模型的分析 and 计算。

使用 Petri 网方法对二号下位机的软件设计进行系统分析建模,图 4(b)所示为二号下位机的主程序和 T_2 时钟中断服务程序中的任务分析模型。

活动库所表示程序的开始,令牌转移,到达请求库所和存取库所,主程序和时钟中断服务程序依此过程不断循环。主程序中的存取库所($p_{accessing-11} \dots p_{accessing-1n}$)表示试验流程控制任务的试验的不同阶段,包括状态准备阶段、手动运动及调整阶段、自动运动阶段和结束阶段,它们具有互斥性。时钟中断服务程序中包含有状态采集、指令解释、报警保护、输入输出通信传输等多个任务模块。主程序中每个试验阶段和中断服务程序中的每个任务模块都可以由有限状态机的建模方法表示其详细过程,这里不作具体阐述。

在主程序进程中使用了 Petri 网的交叉与交汇模型,在其活动库所中设置一个令牌,保证其各个分支处于互斥的状态。主程序和中断程序两个进程的总分析使用了 Petri 网的共享模型,其中进程级共享资源库所中设置一个令牌,同样保证了两个进程之间使用共享资源的互斥。两个进程中,显然中

断服务程序具有更高的优先级,保证了高优先级进程中任务的瞬时性。在 T_2 时钟中断服务程序进程中同样使用了共享模型,图中 $M(\cdot)$ 表示设置共享资源中 m 个令牌, $K(\cdot)$ 表示进程任务中设置 k 个令牌,在此进程中具有 $k(k-m)$ 个任务,对于每个任务模块有属于自己单独的令牌。由于处于同一个时钟中断中,各任务模块可以保证 T_2 时间内的同步。

时钟中断进程中的多个任务可以单独安排在不同的中断进程中,如通信任务可以用 CAN 的中断通信功能实现,系统状态监视可以在 I/O 读取的中断功能中实现,这样就形成了严格意义上的多任务系统。但是由于任务间没有较高要求的时间并发性,而只对实时性能要求严格,所以安排多个任务在同一个时钟中断服务程序进程中,同时保证区分任务的令牌标识,任务之间的资源共享。

因此,上述的系统分析建模能够基本实现系统瞬时、任务同步和进程的并发和互斥功能。

3 软件设计

根据已建立的一号下位机和二号下位机的基于有限状态机和 Petri 网的软件分析模型,可以进行软件模块化详细设计。图 5~图 7 给出了软件设计流程。图 5 为一号下位机时钟中断服务程序设计流程图;图 6 为二号下位机时钟中断服务程序设计流程图;图 7 为二号下位机主程序设计流程图。

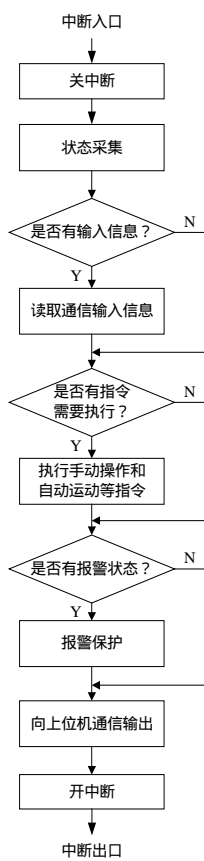


图 5 一号下位机中断服务程序流程

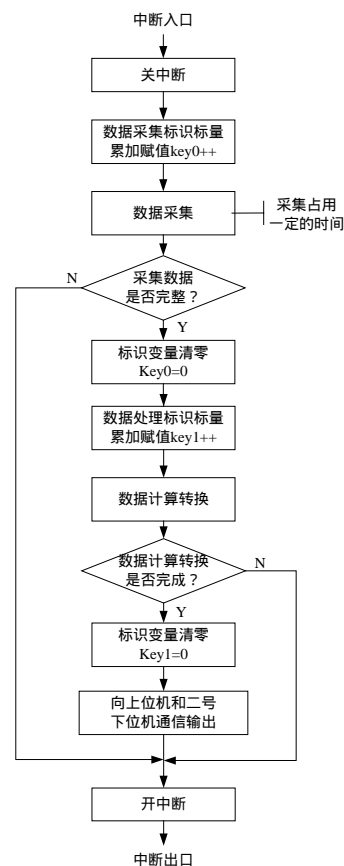


图 6 二号下位机中断服务程序流程

图 7 中的试验结束标识变量 Pro_Finish 的判断过程表示主程序执行事件的变迁,各试验阶段标识变量 Pro_Mode 代表任务级的令牌,实现各试验阶段的互斥。图 6 中的开、关中断过程即为进程间的令牌转移过程,在主程序的初始化和反初始化模块中同样具有开、关中断的过程,即允许令牌由主程序向中断程序转移。共享资源中的表示各任务开始条件

的全局变量标识，代表各任务的执行令牌。

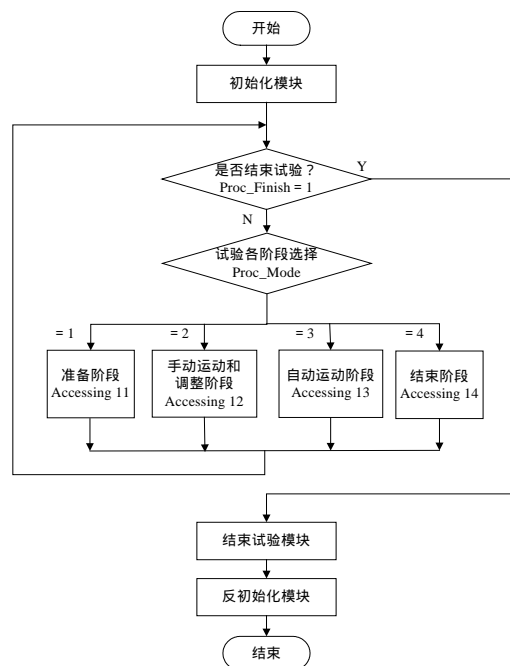


图 7 二号下位机主程序流程

系统中多进程和进程中多任务都能够使用有限状态机和 Petri 网的方法进行分析建模，如上位机的显示进程、通信进程和人机交互进程及二号下位机时钟中断进程中的各个任务，并以模型分析为基础，可完成各任务的模块化设计编程。

4 实验与应用

在实际应用中，两台下位机分系统基于 IPC 机，采用 DOS 操作系统应用 Borland C 语言进行开发，上位机基于 PC 机，采用 LabVIEW 软件进行程序设计。实际应用中采用工程化

和模块化的方法完成系统设计，应用本文所述的分析设计方法，实现了系统的功能要求和性能指标，系统运行性能良好，提高了系统的安全性、可靠性和可维护性。图 8(a)所示为软件中的位姿数据显示界面，图 8(b)为试验现场的控制系统硬件组成图。

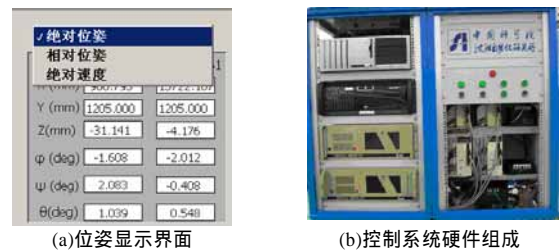


图 8 试验系统实际应用

5 结论

本文从系统组成、功能需求和体系结构方面详细介绍了航天器空间对接仿真系统的实时多任务控制系统，应用软件工程的思想，基于有限状态机和 Petri 网方法完成了其任务级内部和多任务系统的分析建模，并给出了一号、二号下位机程序分析的具体实例。分析了应用分叉和资源共享模型实现同步和互斥问题的具体方法。最后以分析建模为基础完成系统的详细设计。

参考文献

- 1 杨芙清. 软件工程技术发展思索[J]. 软件学报, 2005, 16(1): 1-7.
- 2 Lauesen S. 软件需求[M]. 北京: 电子工业出版社, 2002.
- 3 张友生. 系统分析与设计技术[M]. 北京: 清华大学出版社, 2005.
- 4 赖一楠, 张广玉, 陈志刚. 基于虚拟样机的航天器对接转动模拟装置仿真研究[J]. 系统仿真学报, 2005, 17(3): 639-642.
- 5 Peterson J L. Petri Theory and the Modeling of Systems[M]. [S.l.]: Prentice Hall, 1981.
- 6 Eberhart R C, Kennedy Y J. A New Optimizer Using Particle Swarm Theory[C]//Proc. of the 6th International Symposium on Micro Machine and Human Science, Nagoya, Japan. 1995.
- 7 Kassabalidis I, Sharkawi E I, Marks M A, et al. Adaptive-SDR: Adaptive Swarm-based Distributed Routing[C]//Proc. of the 2002 International Joint Conference on Neural Networks. 2002.
- 8 段晓东, 王楠楠, 王存睿, 等. 一种基于粒子群算法的分类器设计[J]. 计算机工程, 2005, 31(20): 107-109.
- 9 Robinson J, Sinton S, Rahmat S. Particle Swarm, Genetic Algorithm and Their Hybrids: Optimization of a Profiled Corrugated Horn Antenna[C]//Proc. of 2002 IEEE Antennas and Propagation Society International Symposium and URSI National Radio Science Meeting, San Antonio, TX, USA. 2002-06.
- 10 张丽平, 俞欢军, 陈德钊, 等. 粒子群优化算法的分析与改进[J]. 信息与控制, 2004, 33(5): 513-514.
- 11 Shi Y, Eberhart R C. Empirical Study of Particle Swarm Optimization [C]//Proc. of the IEEE Congress on Evolutionary Computation. 1999.
- 12 Shi Y, Eberhart R C. A Modified Particle Swarm Optimizer[C]//Proc. of the IEEE Congress on Evolutionary Computation. 1998.
- 13 Zhang Liping, Yu Huanjun, Hu Shangxu. A New Approach to Improve Particle Swarm Optimization[C]//Proc. of GECCO'03. 2003.
- 14 Alba E, Donrsonoro B. The Exploration/Exploitation Tradeoff in Dynamic Cellular Genetic Algorithms[J]. IEEE Transactions on Evolutionary Computation, 2005, 9(2): 126-142.

(上接第 223 页)

表 2 不同维数时两算法的比较结果

维数	BPSO		NPSO	
	平均最优值及标准差	达优率/%	平均最优值及标准差	达优率/%
n=30	0.192 0±0.482 2	88	0.011 2±0.002 9	100
n=50	0.342 9±0.568 1	79	0.082 5±0.019 2	100
n=60	0.478 2±0.593 2	78	0.137 9±0.026 9	100
n=80	0.722 9±0.559 3	67	0.263 4±0.034 8	100
n=100	1.092 9±0.502 7	40	0.402 6±0.052 5	100

由表 2 可知，随着问题复杂度的增加，基本粒子群算法的优化结果和达优率明显下降，而新算法不仅在优化结果、稳定性方面显著优于基本粒子群算法，每次搜索也均能达优。

4 结论

本文采用种群熵这一种群多样性指标，对种群的多样性进行了定量描述，并把二维元胞引入到粒子群算法中，在粒子群优化算法的基本框架上给出了基于种群熵的自适应粒子群算法。测试结果表明，本算法不仅保持了粒子群优化算法简单、易实现的特点，而且有效增强了算法跳出局部最优的能力；在处理复杂多峰函数优化问题时，其全局搜索性能显著优于基本的粒子群算法。

参考文献

- 1 Kennedy J, Eberhart R C. Particle Swarm Optimization[C]//Proc. of IEEE International Conference on Neural Networks. 1995.