BACnet 应用层状态机在线测试研究*

许毅平　朱振华　周曼丽
（华中科技大学电子与信息工程系　武汉 430074）

摘　要　随着 BACnet 网络技术的应用发展，对 BACnet 网络设备协议一致性测试的要求也越来越强烈，本文在比较现有的协议一致性测试方法的基础上，给出了基于在线测试的 BACnet 协议测试方法，研究了 BACnet 应用层状态机的运行模式，并采用有限状态机模型对 BACnet 应用层状态机进行了分析，给出了相应的状态机状态判定方法和在线测试的软件结构。

关键词　有限状态机，协议一致性测试，状态判定，BACnet

The Study of On-line Testing for BACnet Application Layer TSM

XU Yi-Ping　ZHOU Man-Li
(Electronics & Information Engineering Department, Huazhong University of Sci. & Tech., Wuhan 430074)

Abstract　With the development of BACnet technology, the requirements of protocol implement conformance testing become more and more intense. After comparing the methods of protocol implement conformance testing in existence, the paper presents a BACnet protocol test method based on-line. And then, the paper studies the running model of BACnet application layer TSM, and analyses the TSM using finite state machine model. Finally, this paper presents an algorithm to identify the state of TSM, and describes the software framework of On-line testing.

Keywords　FSM, Protocol implement conformance testing, State determination, BACnet

1　引言

在当今网络的时代，网络协议对网络技术和网络产品的普及和发展发挥了决定性的作用。由于网络协议通常采用非形式化的、基于自然语言的文本方式描述，这种方式可能使协议实现的不同开发者对协议标准的理解产生差异，从而使协议实现偏离协议标准，这种偏离会影响协议实现间的互操作性。因此，协议实现正确性的检测成为关注的焦点，协议一致性测试就是用来检验协议实现的正确性的有效手段，协议一致性测试方法一般分为两种：主动测试和被动测试[1]。

主动测试一般用于在协议实现出产或认证前进行，采用主动测试时，测试器（Tester）根据预先设置好的测试集主动地向被测协议实现（IUT）发送测试报文，测试器通过观察 IUT 对测试报文的响应给出判据。被动测试也叫在线测试，一般用于协议实现的在线运行测试，采用在线测试时，测试器并不主动向 IUT 发送测试报文，它主要通过观察和分析 IUT 实际运行过程中接收和发送的报文序列，推断 IUT 内部状态的变化是否符合协议的规定，以此来对 IUT 进行检测。主动测试的关键在于测试集，测试集决定了测试的覆盖范围，也决定了测试的时间费用，而产生一个高效、全面的测试集往往是很困难的，而在线测试并不需要测试集，并且在线测试具有测试环境简单，可长时间进行测试，以及在实际的工作环境下进行测试等优势，在线测试可以作为主动测试手段的有力补充，因此研究在线测试具有很现实的意义。

BACnet 协议是 A Data Communication Protocol for Building Automation and Control Networks 的缩写[2]。它是由美国供热、制冷与空调工程师学会（ASHARE）组织制定的用于楼宇设备自动化和控制的网络通信协议。该协议是美国国家标准，欧洲标准草案，并且于 2003 年 1 月 20 日被 ISO 正式采纳为国际标准（ISO 16484-5）。随着 BACnet 被接纳为 ISO 国际标准，市场对 BACnet 设备的需求也将空前增长。BACnet 作为一种网络协议，它的协议实现同样面临着协议实现一致性的问题。

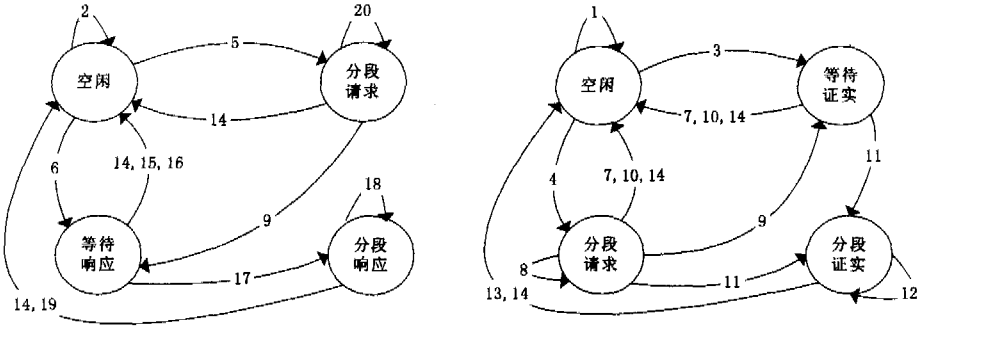
文本通过分析 BACnet 应用层协议，提出了一个 BACnet 应用层协议一致性测试方案，实现对 BACnet 协议实现的在线测试。

2　BACnet 应用层协议

BACnet 是一种开放性协议，它采用 OSI 模型的分层通信体系结构，同时鉴于楼宇控制系统的实际需要和实现成本限制等多方面因素，BACnet 并没有完全参照 OSI 采用七层结构，而是采用了一个由物理层、数据链路层、网络层和应用层组成的折叠式结构。在这四层结构中，BACnet 应用层是 BACnet 协议中地位最重要、内容最丰富的一层。BACnet 应用层定义了两大类服务：无证实应用层服务和有证实应用层服务[2]。

无证实应用层服务是一种不受保证的报文通信机制，主要用于信息广播和信息探询，发送报文的一方不要求确知发送的报文是否被期望的接收方收到，也不期待一定收到接收方的响应，因此在发送方和接收方之间不需要维持状态同步关系。

*）美国 BACnet 制造商协会（BMA）及 BACnet 测试实验室（BTL）资助。许毅平　博士。



事件：
1：发送无证实请求　2：发送无证实响应　3：发送不分段有证实请求　4：发送分段有证实请求（第一分段）
5：收到分段有证实请求（第一分段）　6：收到不分段有证实请求　7：收到简单确认
8：收到分段确认（非最后分段）　9：收到最后分段确认　10：收到不分段复杂确认
11：收到分段复杂确认（第一分段）　12：收到分段复杂确认（中间分段）　13：收到分段复杂确认（最后分段）
14：收到中止报文　15：发送简单确认　16：发送不分段复杂确认　17：发送分段复杂确认（第一分段）
18：发送分段复杂确认（中间分段）　19：发送分段复杂确认（最后分段）　20：收到分段有证实请求（中间分段）

图 1　BACnet 应用层状态机

有证实应用层服务是一种受保证的通信机制，采用客户/服务器通信模式，发起请求报文的一端为客户端（称为 BACnet Client），对请求报文进行响应的一端为服务端（称为 BACnet Server），在这种模式下，客户端和服务端采用一问一答的会话方式，客户端每发送一个有证实请求报文都要判断该报文是否被服务器端收到，以及服务器端对该请求的处理结果，在整个会话过程中，客户端和服务端之间需要进行同步，以使会话能够正常进行，为了使状态保持同步，BACnet 协议规定客户端在发送请求报文时应创建客户状态机（Client TSM），服务端在收到有证实请求报文时应创建服务器状态机（Server TSM），客户状态机和服务状态机分别依据一定的规则改变各自的会话状态，共同管理双方的会话，使通信的双方能够顺利地完成对话。BACnet 规定一个协议实现可以同时建立多个会话，在每个会话中协议实现充当不同的角色，即协议实现在一个会话中可以充当客户端，在另一个会话中充当服务端，协议实现为每一个会话创建一个状态机。因此，在某一时刻，一个协议实现可能同时存在若干个客户状态机和服务器状态机。BACnet 应用层状态机如图 1 所示，由图可知，一个客户状态机有空闲、等待证实、分段请求和分段证实 4 种状态，一个服务器状态机有空闲、分段请求、分段响应和等待响应 4 种状态。

3　BACnet 应用层状态机变迁规则

采用在线测试主要通过分析 IUT 接收和发送的报文序列，推断 IUT 状态机是否按协议的规定进行运行。任何一个事件都有它发生的条件，这个条件就是状态机的当前状态。因此，当一个 IUT 产生一个事件（发送一个报文），该 IUT 内部的状态机的状态肯定属于某个状态子集，该子集所包含的状态个数大于等于 1；当一个 IUT 接收到一个事件（接收到一个报文），该 IUT 内部的状态机的状态同样肯定属于某个状态子集。

由于一个事件可能在多个状态下均可能发生，因此在线测试器不能明确地确定 IUT 状态机的状态，然而，一个与某一状态机相关的连续的事件序列可以确定一个唯一的状态机状态序列，因此，当在线测试器检测足够长的事件序列时，就可以确定 IUT 状态机的状态，从而可以判断该 IUT 的状态机是否正确。

为了能够实现该目的，需要分析事件和状态机可能状态的关系，通过分析状态变迁规则，采用推理技术来判断 IUT 的状态机变迁是否正确。

表 1　客户状态机事件及状态变迁规则表

起始事件类型	起始事件编号	起始状态	变迁状态	变迁事件
发无证实请求	1	0	0	/
收无证实响应	2	0	0	/
发不分段有证实请求	3	0	2	/
发分段有证实请求（第一分段）	4	0	1	/
发分段有证实请求（其他分段）	5	1	1	/
收简单确认	6	1	0	/
		2	0	/
收分段确认	7	1	1	5
收最后分段确认	8	1	2	/
收不分段复杂确认	9	1	0	/
		2	0	/
收分段复杂确认（第一分段）	10	1	3	13
		2	3	13
收分段复杂确认（其他分段）	11	3	3	13
收分段复杂确认（最后分段）	12	3	0	14
发分段确认	13	3	3	/

BACnet 协议应用层状态机可以用有限状态机模型来进行描述，有限状态机模型是一种由若干状态、一个起始状态、一个终止状态、一组输入输出符号和状态变换函数组成的计算模型，有限状态机可以用来抽象表示一个独立进程的运行状态[4,5]。标准有限状态机可以表示为 TSM=(S, X, Y, δ, λ, Q, F)，其中，S 表示所有状态的集合；X 表示所有输入符号的集合；Y 表示所有输出符号的集合；δ 为状态迁移函数；λ 为输出函数；Q 为起始状态集；F 为终止状态集。

BACnet 应用层有客户状态机和服务器状态机两种，这两个状态机的运行是独立的，采用有限状态机模型可分别定义为：

客户状态机模型：Client-TSM=(S, X, Y, δ, λ, Q, F)，其中 S ={空闲，分段请求，等待证实，分段证实}，Q={空闲}，F={空闲}，X ={系统外部输入（所有可能接收到的报文类型），系统内部输入}，Y ={系统外部输出（所有可能发

送的报文类型)，系统内部输出}，状态迁移函数 δ 为变迁状态与输入 X 和当前状态的映射关系，状态的变迁由输入 X 和当前状态共同决定，输出函数 λ 为输出与输入和当前状态的映射关系，输出由输入 X 和当前状态共同决定。

服务器状态机模型：Server-TSM=(S, X, Y, δ, λ, Q, F)，其中 S = {空闲，分段请求，等待响应，分段响应}；Q={空闲}，F={空闲}，X = {所有可能接收到的报文类型}，系统内部输入}，Y = {系统外部输出(所有可能发送的报文类型)，系统内部输出}，状态迁移函数 δ 为变迁状态与输入 X 和当前状态的映射关系，状态的变迁由输入 X 和当前状态共同决定，输出函数 λ 为输出与输入和当前状态的映射关系，输出由输入 X 和当前状态共同决定。

由于客户机状态机和服务器状态机的测试方法是相同的，这里以客户状态机的例来分析事件和状态机状态间的关联，一个事件可由 5 个部分来描述：时间、发送者、接收者报文以及状态机标识，标记为 E={Time, Sender, Receiver, PDU, TSMID}。一个事件通常与起始状态、变迁状态以及变迁事件相关联，我们称这种关联为状态变迁规则。起始状态表示发生某事件的可能的条件状态，也就是一个事件一定是当状态机处于一定状态时才可能发生；变迁状态表示在起始状态下发生该事件后，状态机发生变迁后的状态，事件发生后，状态机的状态可能不变也可能变为其他状态；变迁事件表示发生变迁时状态机产生的事件(即向外发送报文)，事件发生后，状态机可能产生变迁事件，也可能不产生。由于在线测试时，在线测试器所能观察到的事件是网络上的报文，引起状态机改变的其他内部事件(如超时、上层应用软件的操作等)是没法获取的，因此，需要将客户状态机的事件和状态进行重新整理和编号。客户状态机有四种状态{空闲，分段请求，等待证实，分段证实}，分别记为{0,1,2,3}。客户状态机事件可以归纳为 15 种事件，同种事件具有相同的状态变迁规则，不同类型的事件可能具有不同的状态变迁规则，表 1 给出了各种事件的状态变迁规则。当发生某事件时，只要查找该事件对应的变迁规则，就可以得到事件的起始状态、变迁状态和变迁事件，同一个事件可能有多条变迁规则。

4 BACnet 应用层状态机状态判定

在线测试的根本方法就是通过根据前面描述的状态机模型和状态变迁规则来推断 IUT 同步的状态变迁，由于每个 IUT 可能同时存在有多个状态机，我们采用孩子-兄弟树来管理 TSM 的状态变迁推理(如图 2 所示)。图中有四种节点，Root 为根节点，用于索引状态机节点。TSM 为状态机节点，每个服务器状态机和客户状态机对应一个唯一的 TSM 节点，每个 TSM 节点都有一颗状态变迁推理子树，推理子树由事件层和状态关联层交替组成，事件层包含事件节点(即 E 节点)，每个状态变迁推理子树的事件层只包含一个事件节点，事件节点包含一个事件信息。状态关联层由状态变迁节点 S 组成，S 节点描述上一层事件层事件的状态变迁规则，包括事件的起始状态、变迁状态和变迁事件，由于一个事件可能有多个状态变迁规则，因此，状态关联层可能包含多个状态变迁节点 S，状态变迁节点作为上层 E 节点的子节点，同层的 S 节点互为兄弟。状态关联层下层的事件层包含一个事件节点，该事件节点 E 作为上层的某个状态变迁节点的子节点，条件是该事件的起始状态为上层 S 节点的变迁状态，同时生成该事件的状态关联层节点。事件层和状态关联层是一一对应的，增加一个事件层同时也会增加一个状态关联层。

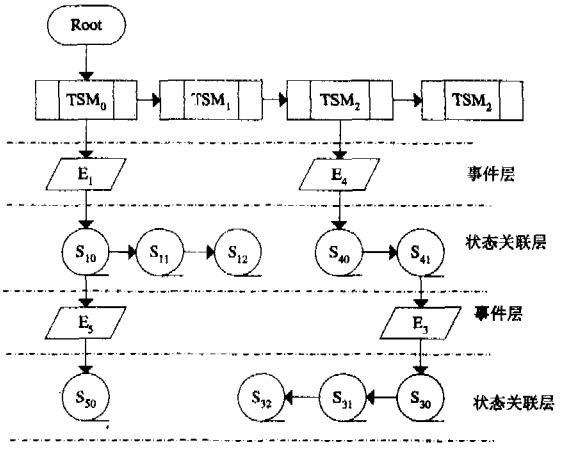


图 2 TSM 状态判定管理图

当每次事件到达时，查找 TSM 状态管理树，找到相应 TSM(如是第一次，创建新节点)，进行 TSM 推理运算，如果推理成功，则等待下一事件；如果错误返回，则将 TSM 节点从 Root 中取下，放入到错误 TSM 链表中，进行相应处理。关键的状态变迁判定算法描述如下：

算法：TSM 推理运算

```
Input：事件 Event
Output：返回成功；返回错误
Function；
MatchCount = 0(初始化，表明此次查找匹配规则数目)
在 Root 中查找对应 TSM 节点
If 没找到
Then 创建新的 TSM 节点添加到 Root，深度 Depth = 0，Match-
     Count = 0
   Else 找到相应的 TSM，在当前 TSM 节点下查找深度为 depth 的
   状态关联层节点(广度遍历)
      For 该层每一个状态变迁节点
      For 事件的每个变迁规则
        If 规则匹配
          Then
              {
                将事件节点添加当前状态变迁节点的子节点，同
                时增加该事件节点的子节点(关联层子节点)，
                MatchCount++，Depth++。
              }
   If MatchCount 为 0
   Then 返回错误(所有规则不匹配)
   Else 返回成功
```

5 BACnet 协议在线测试系统软件结构

图 3 为系统的软件结构图，各模块的主要功能如下。

包捕捉模块：包捕捉模块根据包过滤器的设置对网络上传输的报文进行监听，将符合包过滤器规则的报文上传给包处理模块，同时也将包传递给数据存储模块。

包处理模块：包处理模块的主要目的是提取事件信息，事件信息包括时间、发送者、接受者、报文类型以及状态机标识，这些信息需要根据报文内的信息加工获得。因此，包处理模块需要对报文进行解码，为了正确解码，包处理模块需要调用编解码模块的解码处理函数。如果解码正确，则包处理模块将事件信息传递给事件匹配模块，如果解码失败，则将错误信息传递给异常处理模块处理。

编解码模块：该模块是 BACnet 编解码函数接口模块，提供了 BACnet 协议定义的报文、数据的编解码实现。

事件匹配模块：该模块根据包处理模块提供的事件信息查询状态变迁规则库，查找出与该事件相关的状态变迁规则，并将事件及其状态变迁规则传给状态树管理模块。

(下转第 82 页)

对型的访问权限；访问限制描述在整个访问控制框架中用到的限制关系，例如对访问时间的限制。

```
#Domain Definitions                  #Access Control Materix
/bin/phone=trusted_d                 (trusted_d,system_t,all)
/usr/bin/mplayer=certified_d         (certified_d,sensitive_t,rw)
#Type Definitions                    #Constraints
/ect/network=system_t                (certified_d,sensitivie_t,
/usr/local/abc. mpe=sensitive_t      Timeinterval! 9:00! 22:00)

#Reservation Definitions
CPU_P1=20ms,*
Memory_P1=30
Power_P1=strict
Set1={CPU_P1,Memory_P1,}
Set2={Power_P1}
/bin/phone 90
```

图 3　策略语言示例

进一步的工作和结论　在预留执行中，系统对主体使用超过预留资源的情况进行了处理。另一方面，用户对主体运行所需要的资源无法准确判断，定义的预留资源可能大于实际用到的资源，造成系统资源浪费，降低系统性能。对于这种情况，需要进一步改进资源预留模型，以便用户可以根据资源的实际使用情况进行调整。另外，在系统运行过程中，一些非周期性进程需要动态修改其预留资源，需要在模型定义以及框架方面做进一步的改进。

本文设计了一种应用于移动终端系统的访问控制框架，不但能够保证数据的机密性和完整性要求，而且满足系统对关键应用及时响应的要求，提高移动终端的可用性。在该访问控制框架中，移动终端客体被分为两类：静态客体和动态客体。主体提出的访问请求通过访问代理转交给访问监控器和预留监控器，前者负责对静态客体的访问进行控制，后者负责对主体提出的动态客体预留请求进行裁决并对系统预留资源进行管理。通过预留资源的实施，系统避免了关键应用与其它程序之间产生的资源使用冲突。在访问控制框架中，我们使用一种扩充 DTE 策略的描述性语言来定义访问控制策略，方便用户的配置和管理。

参 考 文 献

1　Trusted Computing Group. TCG Specification Architecture Overview. V1. 2, Apr. 2004. https://www. trustedcomputinggroup. org/

2　Trusted Mobile Platform. Software Architecture Description, 2004. http://www. trusted-mobile. org/

3　Consumer Electronics Linux Forum. CELF Specification v1. 0, Jun 2004. http://www. celinuxforum. org/

4　Badger L, Sterne D F, Sherman D L, et al. Practical Domain and Type Enforcement for UNIX. In: IEEE Symposium on Security and Privacy, Oakland, California, May 1995. 66～77

5　Rajkumar R, Juvva K, Molano A, et al. Resource Kernels: A Resource-Centric Approach to Real-Time and Multimedia Systems. In: Proceedings of the SPIE/ACM Conference on Multimedia Computing and Networking, January 1998

6　Mercer C W. Operating System Resource Reservation for Real-Time and Multimedia Applications. Carnegie Mellon University, 1997

7　Scordino C, Lipari G. Using Resource Reservation Techniques for Power-Aware Scheduling. In: Proc. of the 4th ACM Intl. Conf. on Embedded Software, Pisa, Italy, Sept. 2004

（上接第 78 页）

状态变迁规则库：用于存放事件和事件状态变迁规则。每个状态变迁规则包括事件类型、起始状态、变迁状态和变迁事件，一种事件可能具有多条状态变迁规则。

状态树管理模块：该模块主要根据事件匹配模块匹配的结果对状态树进行管理，该模块对每一个事务状态机维持一个 TSM 节点，每个 TSM 节点下有一个对应的状态变迁树，每次事件到达时，以事件的状态机标识信息为索引找到相应的状态变迁树。然后，根据变迁规则，通过推理，使状态树向每一个可能的方向进行生长。当状态变迁树不能生长时，通知异常处理模块进行异常判断，并对已无生长可能的分支进行剪枝处理。

异常处理模块：对包处理模块、状态树管理模块中产生的异常信息进行格式化处理，并且能对出错原因进行一定的推理分析，然后将分析结果发送给数据存储模块。

数据存储模块：对收到的报文信息、正在维护的 TSM 树信息以及异常信息进行存储管理，以便用户查看。

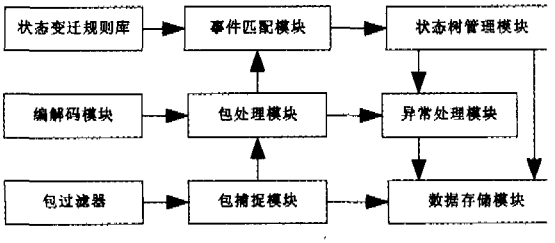


图 3　软件结构图

总结　通信协议一致性测试是一个十分活跃的研究领域，在线测试作为一种协议一致性测试方法具有其独特的优势，由于这种测试本身不对被测系统的正常运行带来干扰，因此可以实现对被测系统长时间的测试。本文对在线测试在 BACnet 通信协议的应用进行了讨论，给出了基于有限状态机模型的 BACnet 协议状态机测试方法和软件框架。

参 考 文 献

1　吴建平，尹霞. 基于形式化方法的协议测试理论[J]. 清华大学学报(自然科学版)，2001，41(4/5)

2　ASHRAE. BACnet: A Data Communication Protocol for Building Automation and Control Networks 135-2001

3　Spitsyna N, Trenkaev V. FSM Based Interoperability Testing of Communication Protocols. Control and Communications, the 2003 IEEE-Siberian Conference on, 2003. 20 ～ 23

4　Zhao Yixin , Yin Xia , Han Bo, et al. Online Test System Applied in Routing Protocol Test Modeling. Analysis and Simulation of Computer and Telecommunication Systems. In: Proceedings of Ninth International Symposium on, Aug. 2001. 331～338

5　赵邑新，吴建平. 应用于在线测试的状态判定算法. 电子学报，2000，28(11)：83～87