多维MANET可靠性建模研究

赵志峰[1,2] 赵曦滨[3,4] 陈丹宁[3,4]
(镇江船艇学院计算机教研室 镇江 212003)[1] (江苏大学控制与科学博士后流动站 镇江 212013)[2]
(清华大学软件学院 北京 100084)[3] (教育部信息系统安全重点实验室 北京 100084)[4]

摘 要 移动自组织网络(MANET,Mobile Ad hoc Network)是一种不依赖固定基础设施且不需要中心控制的动态无线网络。由于其开放自治的无线网络环境及无中心、动态拓扑等特性,导致MANET无法保障通讯的持续性,同时容易受到各种安全攻击。因此相对于传统网络,MANET在网络的可靠性上存在很大的局限性。综合考虑了影响MANET可靠性的两大因素,即节点移动性和安全攻击,提出了多维MANET可靠性模型,并对模型结果进行了实验分析,进一步指出了影响MANET系统可靠性的关键参数。

关键词 MANET,可靠性模型,移动模型,安全模型
中图法分类号 TP393 **文献标识码** A

Research of Multiple Dimensional Reliability Mobel for MANET

ZHAO Zhi-feng[1,2] ZHAO Xi-bin[3,4] CHEN Dan-ning[3,4]
(Computer Department of Zhenjiang Watercraft College, Zhenjiang 212003, China)[1]
(The Post Doctoral Station of Control Science & Engineering of Jiangsu University, Zhenjiang 212013, China)[2]
(School of Software, Tsinghua University, Beijing 100084, China)[3]
(Key Laboratory for Information System Security of Ministry of Education, Beijing 100084, China)[4]

Abstract Without infrastructure, Mobile Ad Hoc Network(MANET) is a kind of self-organized and dynamic wireless communication network that is lack of any centralized control. These characteristics make it vulnerable to communication continuity and security attack. Comparing with traditional network, MANET has great limitation in network reliability. Many researches have been focused on two main factors of reliability or reliability model, which influence the reliability of MANET. Therefore, this paper proposed a multiple dimensional reliability model, which considers both movement and security attack, for MANET. Furthermore, the experimental analysis of the model was given. According to the result of experimental analysis, the key factor of MANET reliability was presented.

Keywords MANET, Reliability model, Movement model, Security model

1 引言

移动自组织网络(MANET,Mobile Ad Hoc Network)作为一种部署方便且不依赖基础设施的通信方式,具有很高的实用价值和应用前景[1,2]。由于其自组织的特性,MANET目前主要应用于战场实时指挥、灾难应急救援以及各种需要快速反应但又无法提供基础设施的场景[2,4]。而这些应用场景对网络的可靠性有较高的要求,一旦在这些紧急情况下网络的可靠性遭受破坏,后果将不堪设想。

网络的可靠性是指网络提供稳定服务的能力不同的应用场景对网络可靠性有不同的要求,而不同网络所提供的可靠性保障也各不相同。作为临时应急环境下的通讯网络,MANET对网络可靠性要求较高。但相对于传统网络,MANET具有动态的网络拓扑、开放无中心的无线网络环境、受限的节点资源等特性,因而其可靠性极易遭受破坏。首先,拓扑结构的动态变化意味着路由的不稳定性,建立的路由随时可能因为节点位置的变化而失效,从而造成可靠性的降低。其次,开放且无中心的无线网络环境使得MANET较为容易受到各种形式的攻击[6-9]。在这些攻击手段中,最容易实现同时破坏性最大的均属于针对可靠性的攻击,如黑洞攻击、DOS攻击等[6]。最后,受限的节点能力也是影响MANET可靠性的一大因素,节点能力的限制也意味着节点的不可靠,这将直接导致网络的不可靠性。

影响MANET网络可靠性的因素可以概括为两个主要方面,即节点的移动性和网络的安全威胁。其中,节点的移动性对MANET可靠性影响的因素可以归纳为网络中节点的数量、节点的移动模型、节点的传输范围等;而网络的安全威胁对MANET可靠性影响的因素也可以具体表现为攻击节点的数量、攻击模型、防御模型等。总体上看,影响MANET网络可靠性的因素错综复杂,且很多因素存在一定程度的不确定性,所以很有必要基于关键影响因素建立MANET的可靠性度量模型,从而进一步定量地分析移动模型和攻击模型

到稿日期:2010-06-12 返修日期:2010-10-21 本文受国家863计划(2007AA040701-12009AA04Z153)资助。
赵志峰(1970—),男,博士,副教授,主要研究方向为网络信息安全,E-mail:zhaozhif@126.com。

对 MANET 可靠性的影响及防御模型的效果。

目前，针对节点移动性对 MANET 可靠性的影响，已有不少研究成果，且都基于移动模型建立了相应的可靠性度量模型。MANET 研究中比较常用的移动模型包括随机路点移动(Random Waypoint Mobility)模型、参考点组移动(Reference Point Group Mobility)模型、高速公路(Freeway)模型和曼哈顿(Manhattan)模型等[2,4]。不同的移动模型对可靠性的影响也会有所不同[2,5]。而针对安全威胁对可靠性的影响也有了一些研究，其中大部分都是在 MANET 存在典型攻击情况下及采用相应防御机制情况下对可靠性建立度量模型。但是，到目前为止，影响 MANET 可靠性的两大因素，即节点的移动性和网络的安全威胁，并没有被综合考虑：要么只考虑节点的移动性对可靠性的影响而建立度量模型，要么只针对安全威胁建立度量模型。然而，上述两大因素并不是相互独立的。首先，节点的移动性导致 MANET 易受安全威胁，在 MANET 中典型的攻击类型大都是针对路由层的不稳定性的，而路由的不稳定性正是节点移动造成的；此外，节点的移动性在一定程度上决定 MANET 所受安全威胁的影响，节点的移动可能会导致安全威胁对网络可靠性的影响扩大，局部“污染”的节点可能通过节点位置的改变进而影响全局网络的可靠性。本文针对当前 MANET 可靠性度量模型中存在的关键因素考虑不全面的问题，提出了多维 MANET 可靠性度量模型。该模型将移动性和安全威胁两大影响 MANET 可靠性的关键参数同时纳入到分析模型当中，建立了包括节点移动性参数和安全指标在内的分析模型，从而在此基础上量化评估 MANET 中不同的参数对可靠性的影响程度。

2 相关研究

当前针对影响 MANET 可靠性的两大关键参数(移动性和安全威胁)分别提出了许多不同的分析度量模型。

基于移动性方面，Cook 等[12,13]提出使用终端对的模型来对 MANET 的移动性与可用性之间的关系进行建模，他们分析节点移动所导致的不同拓扑结构的出现概率，以此分析典型拓扑下的网络终端对之间的可靠性，进一步又从终端对扩展到多个终端，最终扩展到全终端，研究节点之间的路径可用性。Trajanov 等[11]研究了两跳的 MANET 模型，他们分析中继节点移动时所处位置，使用连续时间马尔科夫方法来分析网络拓扑所处不同状态的持续时间及其转移规律，并以此提出了移动环境下的节点间连通可靠性的模型。Jiang 等[10]研究了 MANET 的链路可用性，他们是通过对链路生存周期的时间轴阶段进行细分，并且结合了节点移动的随机路点模型中定向移动时长的指数分布特征，通过理论分析给出了链路可用时间长度在统计意义下的指数分布模型，并通过模拟实验验证了这一模型。Bai Fan 等[1]使用大量模拟实验的方法，归纳出在多种移动模型之下，链路及路径的可用时间长度的分布大体呈指数分布的规律，同时分析了不同模型分布情况差异的原因，并指出节点路径可用时长满足指数分布的前提条件。

如前所述，MANET 的安全威胁也是影响其可靠性的一大因素，然而当前对于安全威胁与可靠性之间的关系所做的研究并不太多。Imad Aad 等[6]分析了 MANET 中的黑洞攻击以及和它类似的水母攻击的共同点，使用概率的方法对路由发现过程中遇到恶意节点的情况进行建模，并分析了包括安全威胁在内的几种静态参数对网络可靠性的影响值。但是，文献[6]的工作并没有给出安全威胁下的网络可用性时长的分布情况，而这恰是很多上层应用对网络性能的需求所必需的参数。Jiejun Kong[3]提出了使用基于忽略(Negligibility)的网络安全模型来研究 MANET 中的安全威胁(如冲击攻击)对网络路由的破坏。在该模型当中，使用了相对安全的概念，把安全威胁程度和保护强度与 MANET 的节点数目 N 联系起来，并表示为多项式关系。基于该多项式关系进而分析出存在恶意节点情况下路由当中每一跳成功的概率的可忽略性，说明安全威胁对网络可靠性影响的严重程度。

可见，目前的研究大多仅关注节点移动性，或是仅关注安全威胁，缺乏综合考虑移动性与安全威胁对网络性能影响的研究。但移动性和安全威胁作为影响 MANET 可靠性的两大重要因素是相互影响、共同作用的。本文重点研究两大因素对网络可靠性的综合影响，并综合建立多维度的 MANET 可靠性度量模型。基于已通过实验验证的路径可用时长的指数分布模型[1]，同时加入了安全威胁下的路径可用性概率模型，综合考虑两种影响类型中可靠性的关键参数，并与网络丢包率、吞吐率以及端到端延迟的分布特征等体现网络可靠性的关键指标相关联，以实现对 MANET 网络可靠性的综合量化分析。

3 MANET 可靠性建模

本文主要基于节点的移动性和网络的安全威胁这两个方面对 MANET 可靠性进行建模。首先，为了更好地建模，引入节点间可达性的概念：在 MANET 网络中，任意选取两个互相通信的节点，它们之间的连通关系在网络中只有可达与不可达这两种瞬时状态。进一步可以定义，可达对应着存在一条可用路径将这两个节点连接起来，且这条路径当中不存在任何恶意节点；不可达则说明两节点间此时尚不存在这样的可用路径，这个时候网络的状态正处于从源节点到目的节点的路由发现过程当中。通过定义两节点之间的可达与不可达的状态，再引入两节点间路径保持时间的概念：路径保持时间是指两个节点之间的路径从建立路由开始，直到路由失效为止的时间段长度。路径保持时间是网络可靠性的关键参数[1]，因而在后续的模型分析中，将围绕着路径保持时间来展开。

在建模过程中，关键符号的定义如表 1 所列。

表 1 符号表

关键符号	定义
h	源节点到目的节点的跳数，即路径的长度
v	节点的平均移动速度
R	节点的有效传输半径
p	正常节点(非黑洞)占所有节点的比例
d_r	路由发现过程所用的平均时间
d_p	每一跳存储转发所用的时间
η	路径不可用的时间长度占总时间的比例

3.1 模型假设

针对 MANET 的实际应用场景，对模型做了如下假设：

1)所有的 MANET 节点无线传输半径相同。在实际应用中，由于所处环境的不同，相同节点的无线传输半径并不相同，甚至在有阻挡的情况下，同一节点的不同方向的传输半径

也不相同，但这对 MANET 可靠性建模并没有决定性的影响。所以为了简化模型，本文假设所有节点的无线传输半径相同。

2)节点移动速度较快。在 MANET 的几大典型应用中，比如军事指挥和应急救援中，大部分节点都处于快速运动中。尤其是一些机械设备，运动速度更高。

3.2 移动性模型

首先考察节点之间路径的保持时间长度分布。综合上面的几种因素，路径的不可用可能是由于节点移动导致链路失效，从而使整个通信路径失效，需要重新进行路由发现，这个时候两节点间原本可达的状态变成了不可达。如果节点移动频繁，路径的平均可用时间就非常短。文献[1]的研究结果已经告诉我们，当节点的移动速度大于 10m/s，而且传输的平均路径长度大于 2 跳的时候，两节点间保持连通状态的时长满足指数分布，其概率密度函数可写成如下形式

$$f_a(x)=\frac{\lambda h v}{R}e^{-\frac{\lambda h v}{R}x}$$

式中，λ 为常数。根据上面的概率密度函数，可以计算出路径连续有效时长的期望值 $E(X_a)$ 为 $\frac{R}{\lambda h v}$。这说明当 MANET 的节点移动速度增大时，路径平均有效时长会缩短。而若节点的有效传输半径增大时，路径平均有效时长会等比例增大。此外，路径包含的跳数越大，路径有效时长越短。

3.3 安全性模型

除了移动性之外，还考虑了 MANET 在安全威胁状态下的性能参考模型。接下来的部分针对 MANET 的典型攻击——黑洞攻击及相应的防御机制进行分析。针对类似的入侵机制，假设网络中已经采用了较为成熟的 Watchdog 机制来判断下一跳节点是否将数据包传递下去，从而可在数据包传递阶段发现路径中存在的黑洞节点。若存在，即重新发起一次路由发现过程，并选择一条新的路由。

假设在一个 MANET 当中共有 N 个节点，其中包含了 b 个黑洞节点，常规节点(非黑洞节点)占所有节点中的比例为 $\frac{N-b}{N}$，记为 p。那么在路由阶段，一条新发现的经过 $h(h>0)$ 步中间跳到达目的节点的路径中，包含黑洞节点的概率为 $1-p^h$。由于每一次路由发现的过程都需要消耗一定的时间，我们将该时间的平均值记为 d_r，其中包括路由发现、路由建立以及发现黑洞节点的总时间。在检测到路径当中包含了黑洞节点，需要放弃刚刚建立好的路径，重新执行路由发现过程。这样，网络中两节点之间不连通的时长等于 d_r 的概率为 p^h。相应地，不连通时长等于 $k\times d_r$ 的概率为 $p^h(1-p^h)^{k-1}$。把这种离散的概率拓展到连续时间取值，可以得到近似的两节点间持续不可达时长的概率密度函数为

$$f_u(x)=-\frac{\ln(1-p^h)}{d_r}(1-p^h)^{\frac{x}{d_r}}$$

根据上面的概率密度函数可以得到路径保持不可达的时长期望值 $E(X_u)$ 为 $d_r p^{-h}$。

3.4 多维可靠性度量模型

从网络的应用层来看，在移动性和安全威胁的共同影响下，MANET 中任意两个节点之间的连通状态是可达与不可达的交替转换。为了使模型更加通用，接下来将使用独立于协议和移动模型的几个典型的网络性能评价参数——丢包率、吞吐率和端到端延迟，来评估 MANET 在移动性和安全威胁下的模型。

(1)丢包率

丢包率是评价网络可靠性的重要指标。在吞吐率较高的网络环境中，由于路由失效导致数据包大量出现而无法转发出去，缓存队列在高吞吐率下效果很小，因此丢包率可近似等同于数据流的源节点和目的节点之间的路径不连通的时长占总时间的比例，即路径的不可用概率，记为 η。因此节点之间的丢包率可表示为

$$\eta=\frac{\lambda h v d_r}{Rp^h+\lambda h v d_r}$$

上式通过路径的不可用时长的期望占总时长的比例计算得到，即 $\frac{E(X_u)}{E(X_a)+E(X_u)}$，其中 $E(X_a)$ 和 $E(X_u)$ 的值在前面已经给出。

在 p 为 0(即所有节点均为黑洞节点)时，任意两个节点间通过中间节点的所有路径均不可达。当 h，v 或 d_r 越大时，丢包率也会随之增大。

(2)吞吐率

吞吐率是评价任何一个数据传输网络的传输能力的一个基本指标，也是网络可靠性的关键指标。在 MANET 中，吞吐率不仅受到节点上有限硬件资源的限制，还会受到源节点和目的节点之间数据传输路径的频繁失效对数据传输吞吐率的影响，在这里主要考虑后者的影响。假设路径持续有效期间两节点之间的吞吐率为 Tp，那么在引入节点移动特性和安全威胁之后的吞吐率为 $Tp'=(1-\eta)\cdot Tp$。

当黑洞节点的比例增加时，p 减小，从而使得路径不可用概率 η 增大，因此网络的吞吐率会随之减小，黑洞节点的数目对网络吞吐率的破坏影响比较明显。

(3)端到端延迟

端到端延迟对于上层的应用来讲是一个很重要的参数，尤其是对网络延迟非常敏感的实时系统，也是可靠性的重要指标。在 h 跳的路径中，路径有效状态下的端到端延迟为 $h\cdot d_p$，得到总的平均延迟为

$$delay=\frac{h\cdot(Rd_p p^h+\frac{1}{2}\lambda v d_r^2 p^{-h})}{Rp^h+\lambda h v d_r}$$

上式通过区分路径连通与不连通两种情况，并按概率累加两种情况下的延迟获得，即路径可用状态下的平均端到端延迟为 $h\cdot d_p$，发生概率为 $1-\eta$；而路径不可用时的平均延迟为 $\frac{1}{2}E(X_u)$，发生概率为 η，按概率加权累加即可得到上式的平均延迟。

更进一步，不仅仅要关心路径的平均延迟，路径延迟的概率密度函数也是个对于应用而言很有参考价值的考量因素。根据前面所建立的路径可用与不可用的概率密度函数，推导出 MANET 节点之间的端到端延迟的积累密度函数为

$$\Pr(delay\leqslant x)=\begin{cases}0, & x<h\cdot d_p\\ 1-\eta, & x=h\cdot d_p\\ 1-\eta+\eta\cdot\left[(1-(1-p^h)^{\frac{x-h\cdot d_p}{d_r}}+\frac{x-h\cdot d_p}{d_r}\sum\limits_{k=\lfloor\frac{x-h\cdot d_p}{d_r}\rfloor}^{\infty}\frac{(1-p^h)^k}{k+1}\right], & \text{others}\end{cases}$$

综合分析上式中的几种情况，首先，由于存储转发的机制，MANET 两个节点的最小延迟为 $h \cdot d_p$，不会有延迟更短的情况，因此延迟小于 $h \cdot d_p$ 的概率为 0，而在路径可用的时间段之内，端到端延迟则正好为 $h \cdot d_p$。此外，在路径不可用的阶段，由于不断地发起路由发现而使得延迟显著增加，直到可用的路径被重新建立，才能够成功地发送和接收数据包。由于黑洞节点的存在，路径失效后，重新进行路由发现过程并非一次就可以成功，因此恰好在第 k 次路由发现过程中成功建立路径的条件概率为

$$P_k' = \Pr(attemp = k \mid path \text{ is } unavailable) = (1-p^h)^{k-1}$$

则延迟小于 x（其中 $x > h \cdot d_p$）的时刻可能出现在路径可用时，其概率为 $1-\eta$；或出现在路径不可用时，但在路由发现尝试次数的最后 $\left\lfloor \frac{x}{d_r} \right\rfloor$ 次路由发现过程当中，延迟小于 x 的条件概率为

$$\Pr(delay \leqslant k \cdot d_r \mid path \text{ is } unavailable) = \sum_{i=1}^{k} p_i' + \sum_{i=k+1}^{\infty} \frac{k}{i} p_i'$$

将上式中的延迟时间变量 $k \cdot d_r$ 统一代换为 x，即可得到 MANET 节点之间的端到端延迟的积累密度函数。

不同的上层应用对于底层网络端到端延迟的要求有所不同。根据上式可以计算出，MANET 能够满足所需延迟要求的概率，可以此来估计网络所能提供的上层端到端延迟要求的满足程度。

4 敏感性分析

在得到多维可靠性模型之后，还需要对建模的结果进行试验分析，进而分析影响 MANET 可靠性的关键参数。由于吞吐率和丢包率的建模结果在模型参数上并没有很大的不同，因此这里只分析丢包率和端到端延迟的建模结果。

根据丢包率的实验结果，分析结果如图 1 所示。参数设置如表 2 所列。

表 2 参数设置表

参数	取值		
常数 λ	0.184	0.277	0.184
源节点到目的节点的跳数 h	2	3	2
平均移动速度 v	40m/s	40m/s	50m/s
有效传输半径 R	250m		
正常节点比例 p	0%～100%		
路由发现平均时间 d_r	5s		

基于文献[1,8]的建模结果，λ 是与 h，v 相关的常数，并且文献[1,8]通过模拟实验给出了相应的结果。本文分析试验中对上述参数的取值就基于该结果。传输半径则取常用 WIFI 的正常设计传输半径，正常节点比例作为变量，路由发现平均时间则取模拟实验平均值。

从图 1 可以发现，网络中只有恶意节点时，丢包率是 100%。随着正常节点的增加，丢包率逐渐降低，并最终降至正常值。但在改变节点平均移动速度和源节点到目的节点跳数时，对丢包率的变化趋势有所影响。增加源节点到目的节点的跳数，则在同一正常节点情况下，丢包率有较大的提高。相对而言，加大节点移动速度，丢包率的升高情况有限。

端到端延迟的实验分析结果如图 2 所示。参数设置如表 3 所列。

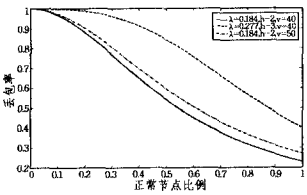

图 1 丢包率分析结果

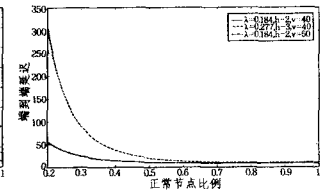

图 2 端到端延迟分析结果

表 3 参数设置表

参数	取值		
常数 λ	0.184	0.277	0.184
源节点到目的节点的跳数 h	2	3	2
平均移动速度 v	40m/s	40m/s	50m/s
有效传输半径 R	250m		
正常节点比例 p	0%～100%		
路由发现平均时间 d_r	5s		
单跳存储转发时间 d_p	5s		

参数取值基本上与丢包率分析的实验相同。端到端延迟的特有参数为 d_p，通常实验的经验值是单跳存储转发时间与路由发现平均时间在同一量级，所以这里设定单跳存储转发时间与路由发现平均时间相等。

从图 2 可以发现，端到端延迟随着正常节点数量的增加不断减少，并在正常节点比例大于 70%之后趋于稳定。但在改变节点平均移动速度和源节点到目的节点跳数时，对端到端延迟的变化趋势有所影响。增加源节点到目的节点的跳数，则在同一正常节点情况下，端到端延迟有明显的增加。相对而言，增加节点移动速度，端到端的延迟几乎没有影响。综合丢包率的实验结果，我们认为源节点到目的节点的跳数对于 MANET 可靠性更为重要。

结束语 本文针对当前 MANET 可靠性建模研究存在的只考虑节点移动性或只考虑安全攻击的问题，提出了综合考虑节点移动性和安全攻击的多维 MANET 可靠性模型，并对建模的结果进行了实验分析。发现在综合考虑节点移动性和安全攻击的情况下，源节点到目的节点的跳数是影响可靠性最为关键的因素。传统仅考虑节点移动或安全攻击的可靠性模型都未能得出这一关键结论。

基于本多维可靠性模型，可以深入研究分析影响 MANET 可靠性的关键参数，从而进一步基于分析的结果指导 MANET 网络的部署和协议的设计。

参 考 文 献

[1] Bai F, Sadagopan N, Krishnamachari B, et al. Modelling Path Duration Distributions in MANETS and Their Impact on Reactive Routing Protocols[J]. IEEE J. on Selected Areas in Communications, 2004, 22(7): 1357-1373

[2] Camp T, Boleng J, Davies V. A Survey of Mobility Models for Ad Hoc Network Research[J]. Wireless Communication & Mobile Computing(WCMC), Special issue on Mobile Ad Hoc Networking: Research, Trends and Applications, 2002, 2(5): 483-502

[3] Kong J. GVG-RP: A Net-centric Negligibility-based Security Model for Self-organizing Networks[R]. 2006/140. IACR Cryptology ePrint Archive, April 2006

[4] Djenouri D, Khelladi L, Badache N. A survey of security issues in mobile ad hoc and sensor networks[J]. IEEE Communications Surveys & Tutorials, 2005, 7(4): 2-28

（下转第 92 页）

将式(5)和式(6)代入式(7)中可得：

$$\overline{W}^{[2]}=\left(\frac{\lambda_1+\lambda_2}{\mu-(\lambda_1+\lambda_2)}-\frac{\lambda_1}{\mu_1-\lambda_1}\right)/\lambda_2$$

$$=\left(1+\frac{\lambda_1}{\lambda_2}\right)\frac{1}{\mu-(\lambda_1+\lambda_2)}-\frac{\lambda_1}{\lambda_2}\cdot\frac{1}{\mu_1-\lambda_1} \quad (8)$$

因为信令在系统中的逗留时间等于其在系统中的等待时间加上信令的处理时间，因此有：

$$\overline{W}_q^{[2]}=\overline{W}^{[2]}-\overline{\chi}^{[2]}$$

$$=\left(1+\frac{\lambda_1}{\lambda_2}\right)\frac{1}{\mu-(\lambda_1+\lambda_2)}-\frac{\lambda_1}{\lambda_2}\cdot\frac{1}{\mu_1-\lambda_1}-\frac{1}{\mu_2} \quad (9)$$

3.2.2 TDDP-FCFS调度系统实际性能分析

对于某信令寻径式交换机的MM5并行计算应用，分析了TDDP-FCFS调度系统的实际性能。对MM5一轮并行计算的通信量进行多次统计后求平均，发现60分钟内平均调用信令的总次数约为31700万次，其中PCR信令有100万次。把这些实际数值带入上述性能指标计算公式可得：

(1)调度系统中PCR信令的平均数为：

$$\overline{N}^{[1]}=\frac{\lambda_1}{\mu_1-\lambda_1}\approx 2.224*10^{-5} \quad (10)$$

调度系统中其他信令的平均数为：

$$\overline{N}^{[2]}=\frac{\lambda_2(\mu_1^{\ 2}-\lambda_1\mu_1+\lambda_1\mu_2)}{(\mu_1-\lambda_1)(\mu_1\mu_2-\lambda_1\mu_2-\lambda_2\mu_1)}=7.003*10^{-5} \quad (11)$$

(2) 队列中PCR信令的平均等待时间为：

$$\overline{W}_q^{[1]}=\frac{\lambda_1}{\mu_1(\mu_1-\lambda_1)}=1.779*10^{-4}\text{ns} \quad (12)$$

其他信令的平均等待时间为：

$$\overline{W}_q^{[2]}=\left(1+\frac{\lambda_1}{\lambda_2}\right)\frac{1}{\mu-(\lambda_1+\lambda_2)}-\frac{\lambda_1}{\lambda_2}\cdot\frac{1}{\mu_1-\lambda_1}-\frac{1}{\mu_2}$$

$$=5.695*10^{-2}\text{ns} \quad (13)$$

(3)系统中PCR信令总的逗留时间：

$$\overline{W}^{[1]}=\frac{1}{\mu_1-\lambda_1}=80.002\text{ns} \quad (14)$$

系统中其他信令的逗留时间为：

$$\overline{W}^{[2]}=\left(1+\frac{\lambda_1}{\lambda_2}\right)\frac{1}{\mu-(\lambda_1+\lambda_2)}-\frac{\lambda_1}{\lambda_2}\cdot\frac{1}{\mu_1-\lambda_1}=80.57\text{ns} \quad (15)$$

由于信令的平均调度时间包括信令进入等待队列所用的时间以及在信令调度系统中的逗留时间，由信令寻径式交换机的实现逻辑知信令入队时间约为47.059ns，因此，PCR信令的平均调度时间为127.061ns，其他信令的平均调度时间为127.629ns。

由以上计算结果可知，TDDP-FCFS调度系统中平均信令总数都很少，几乎趋近于0。这意味着无论是PCR信令还是其他信令进入调度系统后几乎不需等待就可马上被处理。PCR信令和其他信令的平均调度执行时间理论值分别约为127.061ns和127.629ns，其中47.059ns是信令入队时间，而信令执行时间分别为80.002ns和79.202ns，其余是信令在队列中的等待时间。也就是说，调度执行时间的三分之一左右用于信令入队，不足三分之二的时间用于信令的实际处理，信令在系统中的最大等待时间只占总时间的0.0045%。由此可见，该TDDP-FCFS调度系统的效率是非常高的。

结束语 基于先到先服务的二维动态优先级信令排队算法TDDP-FCFS，按照信令优先权和交换机的端口轮转优先权两级优先权排序对交换机接收到的信令使用先到先服务的方法进行排队调度，使得调度算法能够满足不同信令的执行特点，同时也兼顾了各个端口的服务公平性。使用强占型M/M/1/∞队列理论对TDDP-FCFS进行建模，给出了其性能指标计算方法，并计算了实际环境中的性能数值。计算结果表明，TDDP-FCFS调度系统能够满足信令寻径式交换机的调度要求，并具有较高的调度效率。

参考文献

[1] Dong Yu-guo, Wang Sheng-rong, Guo Yun-fei, et al. Exploring Load Balancing of a Parallel Switch with Input Queues[J]. Journal of Software, 2007, 18(2): 229-235

[2] Wu Jun, Luo Jun-zhou. Randomized scheduling algorithm for input-queued switches[J]. Journal of Southeast University (English Edition), 2005, 21(1): 6-10

[3] 李季，曾华鑫，许登元. CICQ交换机中一类服务可保障的调度策略研究[J]. 计算机研究与发展，2007，44(11)：1873-1880

[4] 王景存，谢馨艾，王沁，等. 基于输入队列的调度算法及其稳定性证明[J]. 计算机工程，2007，11：130-133

[5] 曾媛，龚文斌，刘会杰，等. 适合星载交换机的调度算法[J]. 计算机工程，2009，2：158-160

[6] 雷艳静. 面向MNWF的信令寻径式光纤通道先锋交换网研究[D]. 西安：西北工业大学计算机学院，2009

[7] 唐小我，唐应辉. 排队论——基础与分析技术[M]. 北京：科学出版社，2006

[8] 盛友招. 排队论及其在现代通信中的应用[M]. 北京：人民邮电出版社，2007

(上接第63页)

[5] Groenevelt R, Nain P, Koole G. The Message Delay in Mobile Ad Hoc Networks[C]//Proc. PERFORMANCE. Oct. 2005

[6] Aad I, Hubaux J P, Knightly E W. Denial of Service Resilience in Ad Hoc Networks[C]//Proc. of MobiCom. 2004: 202-215

[7] Zhou T, Choudhury R R, Ning P, et al. Privacy-Preserving Detection of Sybil Attacks in Vehicular Ad Hoc Networks[C]//Proc. of International Conference on MobiQuitous. 2007: 1-8

[8] Ramaswamy S, Fu H, Sreekantaradhya M, et al. Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks [C]//Proc. of ICWN. 2003

[9] Hu Y C, Perrig A, Johnson D B. Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols[C]//ACM Workshop, Wireless Security WiSe 2003, San Diego, CA, USA, Sept. 2003

[10] Jiang S, Hez D, Raoz J. A Prediction-based Link Availability Estimation for Mobile Ad Hoc Networks[C]//Proc. of IEEE InfoCom. 2001

[11] Trajanov D, Filiposka S, Efnuseva M, et al. Ad hoc Networks Connection Availability Modeling[C]//Proc. of the 1st ACM International Workshop on Performance Evaluation of Wireless Ad hoc, Sensor, and Ubiquitous Networks: 56-60

[12] Cook J L, Ramirez-Marquez J E. Two-terminal reliability analyses for a mobile ad hoc wireless network[J]. Reliability Engineering and System Safety, 2007, 92: 821-829

[13] Cooka J L, Ramirez-Marquezb J E. Reliability analysis of cluster-based ad-hoc networks[J]. Reliability Engineering and System Safety, 2008, 93: 1512-1522