文章编号:1001 - 9081(2005)02 - 0265 - 05

移动 Ad Hoc 网络中的 TCP 改进方案性能分析

程 剑,洪佩琳,李津生
(中国科学技术大学 电子工程与信息科学系,安徽 合肥 230027)
(milanmadrid@ ustc. edu)

摘 要:TCP 协议是针对固定可靠网络设计的一种传输协议,它把数据包丢失或延迟的原因都归结为网络拥塞。但在移动 Ad Hoc 网络中,其他因素如信道误码、网络分割及路由变化等也能引起数据包丢失,此时 TCP 协议的慢启动和快速重发特性将导致传输性能下降。首先讨论了 Ad Hoc 网络中影响 TCP 性能的几个主要因素,介绍几种典型的 TCP 改进方案,并对这些方法进行了性能分析与比较。

关键词:TCP;Ad Hoc;拥塞
中图分类号: TP393 **文献标识码**:A

Performance analysis on improved schemes of TCP in mobile Ad Hoc networks

CHENG Jian, HONG Pei-lin, LI Jin-sheng
(Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei Anhui 230027, China)

Abstract: The Transmission Control Protocol (TCP) was designed for reliable fixed network, it treat package loss or delayed as network congestion. But in Mobile Ad Hoc networks, other factors such as channel error, network partition and route changes also could invoke package loss, at the moment slow-start and fast recovery property of TCP will decreased the transmission performance. In this paper, we firstly discussed several main factors which infect TCP performance in Ad Hoc networks, and then presented an overall view on some representative improved schemes of TCP in Ad Hoc networks. Finally, we had an analysis and compare on these schemes.

Key words: TCP; Ad Hoc; congestion

0 引言

移动 Ad Hoc 网络[1](Mobile Ad Hoc Networks,MANET)是由多个移动节点构成的无线自组织系统,网络中的节点同时具有主机和路由器的功能,并可以随机移动与自我组织,也可以随时开机和关机,因此其网络拓扑可能快速且不可预知地变化。Ad Hoc 网络主要应用于军事、紧急营救、特殊工作环境及其他个人通讯领域。

TCP 协议是针对固定有线网络设计的,为发送方和接收方之间提供可靠、有序的传输服务。TCP 协议依靠其错误控制机制来保证连接的可靠性,它假设所有的网络丢包是由拥塞造成。但移动 AD Hoc 网络有着明显不同于固定有线网络的特点,如链路误码率高、网络分割和路由变化频繁等,这些都会导致网络丢包。而 TCP 却把一切丢包原因归结为网络拥塞,引发了不必要的拥塞控制,如减小窗口大小、加倍 RTO (Retransmission Timeout)时间等,这使得移动 Ad Hoc 网络中 TCP 的性能急剧下降。

有鉴于此,近年来提出了不少在 Ad Hoc 网络下的 TCP 改进方案,从而能够较好地区分网络丢包的错误性质,从而在很大程度上提高了 TCP 的性能。

1 Ad Hoc 网络中影响 TCP 性能的主要因素

Ad Hoc 网络是由移动节点组成的无线多跳网络,它不仅具有信道误码率高的特点,更由于节点的移动性,其网络拓扑会不时地发生变化,变化率由节点的数目、移动速度及传输范围等决定。节点移动性造成的网络拓扑变化如图 1 所示:在 T 时刻,节点 S 到 D 之间有一条经过节点 C 的路由,S 和 D 之间是连通的。而在 $T + t1$ 时刻,由于 C 节点的移动,B 和 C 之间超出了通讯范围,S 和 D 之间经过 C 的这条路由失效,S 和 D 不再连通,即发生了网络分割,此时 S 需要重新计算一条到 D 的路由。再经过一段时间 $t2$,即 $T + t1 + t2$ 时刻,S 重新发现了一条到 D 的路由(经过节点 E),S 和 D 重新连通。不幸的是,网络拓扑的这种变化对 TCP 的性能造成了灾难性的影响。下面具体分析 Ad Hoc 网络中影响 TCP 性能的各种因素。

1) 信道误码率高:移动 Ad hoc 网络属于无线网络,信道误码率较高,数据包丢失较为严重。如果 TCP 发送方在 RTO 超时前没有收到 ACK 报文,就会引发 TCP 的慢启动,从而发送方的 RTO 时间加倍,并减小当前拥塞窗口为 1 个分组。频

收稿日期:2004 - 07 - 27;**修订日期**:2004 - 10 - 09

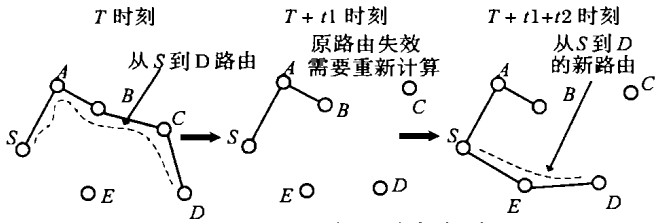
作者简介:程剑(1979 -),男,安徽安庆人,硕士研究生,主要研究方向:移动 Ad Hoc 网络; 洪佩琳(1961 -),女,浙江宁波人,教授,博士生导师,主要研究方向:网络通信与信息安全; 李津生(1937 -),男,上海人,教授,博士生导师,主要研究方向:下一代网络体系结构.

繁的错误会使拥塞窗口一直保持在很小的范围,从而导致了吞吐量的降低。

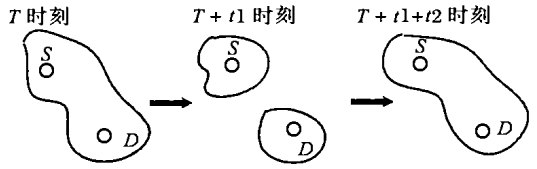
2) 路由重计算和数据包乱序:当移动 Ad Hoc 网络中原有的路由无效(如图 1(a))或过期时,需要为发送方和接收方之间重新设计一条新路由。为 Ad Hoc 网络设计的路由协议不少都是按需驱动的,如 DSR[2] 协议和 AODV[3] 协议,其优点是降低了路由维护的开销,但同时也使路由发现的时间变长,这样很可能在找到新路由之前 RTO 超时,从而引发 TCP 的慢启动,降低了传输性能。不仅如此,路由的频繁变化还会导致网络中经常突发性地产生大量乱序数据包,使 TCP 陷入不断快速重发[4] 的困境。

3) 网络分割(Network Partition):由于移动 Ad Hoc 网络的动态特性,某些时刻网络会发生网络分割(由节点的移动性等造成,如图 1(b)),发送方和接收方之间的链路断开。这种情况下,发送方不可能接收到 ACK 报文,于是 TCP 进入慢启动。

4) 多径路由:多径路由也会引起数据包乱序。某些 Ad Hoc 路由协议(如 DSR)为了保证路由的健壮性,同时在发送方和接收方之间维持多条路由。发送方发送的数据包可能会沿不同的路由传输,不同路由之间的时延不同,导致到达接收方的数据包发生乱序,从而引发 TCP 的快速重发机制(源端接收到 3 个重复的 ACK 后)。



(a)由节点移动性引起的路由重计算



(b)由节点移动性引起的网络分割及重组

图 1 节点移动性引发的问题

2 Ad Hoc 中几种典型的 TCP 性能改进方案

TCP 协议之所以在移动 Ad Hoc 网络中性能显著下降,根本原因在于缺乏有效的错误检测和错误恢复机制。因此,提高 TCP 协议的性能,其核心就是要使 TCP 具有区分网络丢包原因的能力,并针对不同情况(拥塞、信道误码或网络分割等)采用合理的策略。

根据区分丢包原因所采取的手段,可分为两大类:基于网络反馈的改进方案和"端到端"的改进方案。

2.1 基于网络反馈的改进方案

这种类型的改进方案通过网络反馈来获取网络状态信息,它要求对 Ad Hoc 网络中的各个节点配置检测机制,以使中间节点能及时反馈网络状态。例如:当 TCP 连接中的某个节点因为移动而导致链路断开时,相关节点会发送一个显式链路错误通知(Explicit Link Failure Notification,ELFN)报文给 TCP 的发送方;而当某个节点发生了拥塞,此节点则会反馈回一个显式拥塞通知[5](Explicit Congestion Notification,ECN)报文。基于网络反馈的 TCP 改进方案如下:

1) TCP-ELFN

TCP-ELFN[6] 改进方案使用 ELFN 来协助其实行错误检测,以此来区别对待网络拥塞和链路错误引起的丢包。TCP-ELFN 专为 DSR 路由协议设计,ELFN 报文的实现是通过修改 DSR 协议中的路由错误报文,使之携带一个类似于"主机不可达"ICMP 报文的载荷。当某个中间节点侦测到链路或路由错误时,反馈一个 ELFN 报文给发送方,使其 TCP 进入"stand-by"模式。在此模式下,TCP 停止发送数据包,并锁定一切变量,如 RTO 定时器和拥塞窗口(CWND)。在 stand-by 模式时,TCP 周期性地向接收方发送探测分组,若收到确认报文,则表明已经找到新的路由,此时发送方脱离 stand-by 模式,恢复正常发送功能,并重新启用在进入"stand-by"模式时冻结的各项变量。

文献[4]对 TCP-ELFN 方案进行了 ns 仿真(MAC 层协议是 802.11,路由协议是 DSR),仿真显示:改进后的 TCP 吞吐量相对传统 TCP 有很大增益。TCP-ELFN 避免了在链路断开或路由重计算时引发不必要的拥塞控制,但它对信道误码率高等其他因素的影响无能为力,仅适用于 DSR 路由协议。

2) ATCP

ATCP[7](Ad Hoc TCP)也是基于网络反馈的改进方案,但 ATCP 并不直接对 TCP 本身进行修改,而是在传输层和网络层之间嵌入一个中间层,即 ATCP 层。ATCP 层截获中间节点发来的网络状态信息,并根据不同网络状况(网络拥塞、信道误码、网络分割等)采取合适的策略,控制 TCP 的行为。ATCP 方案依靠中间节点反馈的 ICMP 报文和 ECN 报文来获取网络状态信息(网络分割和网络拥塞)。ATCP 层仅在 TCP 的发送方起作用。

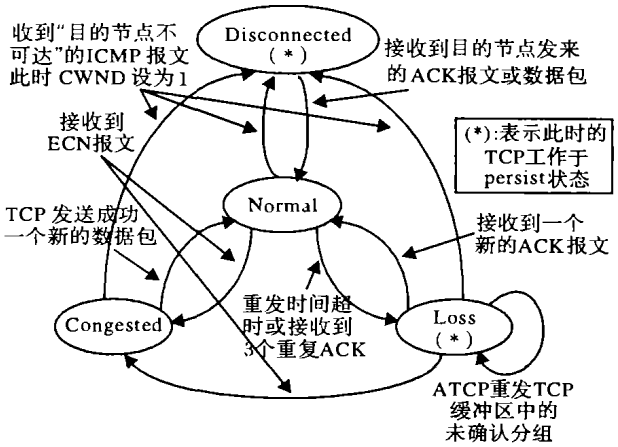


图 2 ATCP 的状态转移

如图 2 所示,ATCP 存在四种可能的状态:Normal(正常)、Congested(拥塞)、Loss(有损)和 Disconnected(分离)。相应的,TCP 也有三种工作模式:Retransmit(传输)、Persist(维持)和 Congestion Control(拥塞控制)模式。当 TCP 连接开始建立时,发送方的 ATCP 处于 Normal 状态,这种状态下,ATCP 不进行任何行为,TCP 处于正常的 Retransmit 模式。下面介绍 ATCP 各种状态间的转换及不同状态下采取的相应策略。

1) Normal↔Loss:Normal 状态时,若发送方的 ATCP 层检测到 RTO 即将超时(由链路丢包造成)或接收到 3 个重复的

ACK(由数据包乱序造成),此时 ATCP 不将第 3 个重复的 ACK 报文转发给 TCP(避免引发 TCP 的慢启动或快速重发),并使 TCP 进入 Persist 模式, ATCP 进入 Loss 状态。在 Loss 状态下,发送方专门重发尚未收到 ACK 确认的分组。当收到新的 ACK 报文, ATCP 恢复为 Normal 状态, TCP 也回到 Retransmit 模式。

2) Normal↔Congested: Normal 状态时,若发送方的 ATCP 层接收到带有 ECN 标记的分组或 ACK 报文(来自于处于拥塞的中间节点), ATCP 转换为 Congested 状态,此状态下 ATCP 不干涉 TCP 的拥塞控制行为, TCP 进入 Congestion Control 模式。直到成功发送了一个新的分组后, ATCP 才重新恢复为 Normal 状态, TCP 也回到 Retransmit 模式。

3) Normal↔Disconnected: Normal 状态时,若发送方的 ATCP 层接收到中间节点发来的 ICMP 目的节点不可达报文(由网络分割或路由重计算造成),则 ATCP 使 TCP 进入 Persist 模式, ATCP 本身转换为 Disconnected 状态。此时发送方不再发送数据,而只是周期性地向接收方发送探测分组。直到发送方收到 ACK 确认报文时(表明路由重新建立), ATCP 恢复为 Normal 状态, TCP 也回到 Retransmit 模式。

4) 其他状态转换:当 ATCP 处于 Loss 状态时,若收到 ECN 报文,则 ATCP 进入 Congested 状态,并使 TCP 脱离 persist 模式,进入 Congestion control 模式。当接收到 ICMP 目的节点不可达报文时,处于 Loss 或 Congested 状态的 ATCP 都会进入 Disconnected 状态,并使 TCP 进入 Persist 模式。

文献[5]中根据 ATCP 方案建立了一个实验床,在 Free BSD 系统中配置了改进后的 TCP 协议,并在不同的条件下(如信道有损、网络分割和数据包乱序)对传输性能进行了评测,改进后的 TCP 协议在这些情况下的传输时延都要小于传统 TCP。这个实验床并未基于无线信道和 Ad Hoc 的路由协议,实验中的各种条件限制是在以太网下进行人为控制的。

2.2 "端到端"的 TCP 改进方案

"端到端"的改进方案维护了 TCP 协议本身的重要特性。它不需要中间节点的支持,通过在发送方和接收方两端检验参数来获得网络状态信息。以下介绍两种典型的"端到端" TCP 改进方案。

2.2.1 TCP DOOR

TCP DOOR[8] (TCP Detection of Out-of-Order and Response)改进方案的核心在于对乱序 OOO(Out-of-Order)包的检测和处理。所谓乱序是指发送方发送的数据包没有按顺序到达接收方,这使接收方产生重复的 ACK 报文给发送方,导致发送方进行不必要的快速重发(收到 3 个重复的 ACK 后)。

移动 Ad Hoc 网络中,由于节点的移动性,路由变化频繁发生,出现 OOO 事件的原因大都因路由变化引起。如图 3 所示,节点 S 和 D 之间有一条经过 A 和 B 的路由, TCP 原先通过这条路由进行传输(如分组 1),节点 C 逐渐移动到 S 和 D 的通讯范围内,此时 S 和 D 之间重新计算了一条经过节点 C 的路由,路由发生改变,接下来的分组 2 沿新路由传输。由于新路由很可能比旧的路由传输时延小,后发的分组 2 反而先于分组 1 到达节点 D ,即发生了 OOO 事件。Ad Hoc 网络频繁的路由变化会使 TCP 陷入不断快速重发的困境。

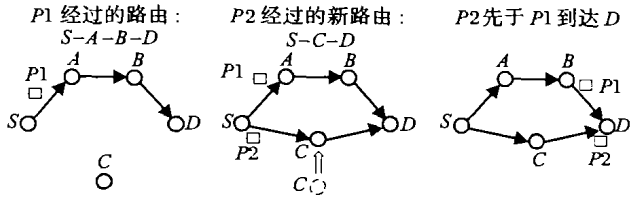


图 3　路由变化导致的 Out-of-Order 现象

TCP DOOR 就是通过在 TCP 两端对 OOO 包的检测来判断网络中是否发生了路由变化,并采取相应策略来提高 TCP 的性能。

1) 如何检测 OOO 包

对于一个 TCP 连接,接收方收到的数据包和发送方收到的 ACK 报文都可能发生乱序,因此对 OOO 包的检测在两端都可以进行。TCP 的发送方可能会重发数据包,接收方虽然不会重发 ACK,但却可能产生重复的 ACK。重发的数据包之间具有相同的序列号,重复的 ACK 报文之间也是。因此,依靠序列号不能判断是否发生了 OOO 事件。TCP DOOR 在数据包的 TCP 头标中增加一个 2 字节的选项,即 TPSN(TCP Packet Sequence Number),在 ACK 报文的 TCP 头标中增加一个 1 字节的选项, 即 ADSN (ACK Duplication Sequence Number)。每发送一个数据包或 ACK 报文、TPSN 或 ADSN 的值加 1,TCP DOOR 通过在 TCP 两端检测 TPSN 和 ADSN 来判断是否发生了 OOO 事件。

2) 对 OOO 事件的处理

由发送方处理(若是接收方检测到 OOO 时,也会通过在 ACK 报文中设置 OOO-bit 通知发送方),此时有两种处理方式:

a) 暂时禁止 TCP 拥塞控制:因为 OOO 很大可能是由路由变化而并非拥塞引起,当发送方检测到 OOO 时,TCP DOOR 在时间 T1 内禁止 TCP 的拥塞控制机制,T1 时间后 TCP 恢复为正常。

b) 拥塞避免时立即恢复:当发送方检测到 OOO 时,并不禁止 TCP 的拥塞控制,但是在时间 T2 内,一旦 TCP 进入拥塞避免,则 TCP 立即恢复到拥塞避免前的状态。

文献[6]中对 TCP DOOR 改进方案进行了 ns 仿真(MAC 层协议是 802.11,路由协议是 DSR)。仿真显示:一般只需要在发送方配置对 OOO 包的检测机制即可,和在两端同时进行检测的准确性差别不大;两种对发生 OOO 事件的处理方法中,"拥塞避免时立即恢复"要比"暂时禁止 TCP 拥塞控制"的性能增益大;TCP DOOR 比传统 TCP 的吞吐量平均要高出 50%。

2.2.2 MMJI

多参数联合检验[9] (Multi-Metric Joint Identification, MMJI)方案也保持了端到端的特性, MMJI 方案依靠对 4 个参数的联合检验,提高了判别网络状况的准确性,并且能够更详细的区分网络状况。

MMJI 方案把 Ad hoc 网络的状态分为 5 种:Normal(正常)、Congestion (拥塞)、Channel_Err (信道误码)、Route_Change(路由变化)和 Disconnection (分离)。在这些状态下 MMJI 采取的策略行为和 ATCP 方案大同小异,这里不再赘

述,不同之处在于 MMJI 方法还多了对 Route_Change 状态的检测和处理,以专门解决路由变化造成的数据包乱序问题,而 ATCP 是在 Loss 状态下统一解决信道误码和数据包乱序问题。

下面重点介绍 MMJI 方案是如何通过端到端的检测机制来区分上述网络状态的。此方案所提议的 4 个检验参数分别为 IDD、STT、POR 和 PLR,如表 1 所示。其中 IDD 和 STT 联合判断是否发生网络拥塞,POR 和 PLR 则可以进一步区分非拥塞情况中的各种状态。

表 1 MMJI 方案的 4 个提议参数

参数	定义	解释
IDD	$(A^{i+1}-A^i)-(S^{i+1}-S^i)$	A^i 是第 i 个包到达的时间,S^i 是第 i 个包发送的时间,IDD 即接收方的包间延迟减去发送方的包间延迟
STT	$Np(T)/T$	$Np(T)$ 是在时间 T 内收到的数据包数目
POR	$Npo(T)/Np(T)$	$Npo(T)$ 是在时间 T 内收到的乱序数据包数目
PLR	$N_l(T)/Np(T)$	$N_l(T)$ 是在时间 T 内丢失的数据包数目

1) 包间延迟差异(Inter-packet Delay Difference,IDD):网络拥塞程度越高,IDD 的值越大;但如果网络中发生路由变化,数据包出现乱序时,也会使 IDD 的值增大。

2) 短时吞吐量(Short Term Throughput,STT):网络拥塞程度越高,STT 的值越小;但如果网络中发生了网络分割或突发性信道误码,也会使 STT 的值减小,特别是当发生了网络分割时,STT 的值接近于 0。

3) 数据包乱序比率(Packet Out-of-order delivery Ratio,POR):网络中路由发生变化时,POR 的值会增大。

4) 数据包丢失率(Packet Loss Ratio,PLR):网络中发生突发性信道误码时,PLR 的值会增大。

MMJI 方案通过检验上述 4 个参数获取网络状态信息。如表 2 所示,检验判别过程可分为以下两个步骤:

1) 判断是否拥塞:由于 IDD 的值对路由变化很敏感,而 STT 的值对网络分割和信道误码敏感。因此,为提高判别准确性,仅当 IDD 值比较高,同时 STT 值比较低时,才判定网络处于 Congestion 状态,其他情况都属于非拥塞状态。

2) 判别非拥塞时的各种状态:通过 1)判定网络非拥塞后,若发现 POR 值比较高,则判定网络处于 Route_change 状态;若发现 PLR 值比较高,则判定网络处于 Channel_Err 状态;若发现 STT 值接近于 0,即收不到数据包,则表明网络处于 Disconnection 状态。

表 2 通过 MMJI 判断网络状态的规则

	IDD 和 STT	POR	PLR
Congestion	(高,低)	任意	任意
Route_Change	非(高,低)	高	任意
Channel_Err	非(高,低)	任意	高
Disconnection	STT 0	任意	任意
正常	不属于以上的其他情况		

文献[7]中对 MMJI 方案进行了 ns 仿真(MAC 层协议是 802.11,路由协议是 DSR)。仿真显示:使用 IDD 和 STT 联合判别是否拥塞的准确性要远高于只使用一个检验参数;在不同的信道误码率和节点移动率下,用此方案改进后的 TCP 吞吐量大约是 TCP New Reno 的 1 ~ 8 倍,基本接近于 TCP-ELFN。

文献[7]中还在 Linux 主机上实现了改进后的 TCP:普通情况下,其吞吐量大约比 TCP Reno 下降了 5%(因增加了一些算法代码);而在有信道误码和节点移动时,其吞吐量要远大于 TCP Reno,并随着信道误码率和节点移动率的增加,增益更加明显(超过 100%)。

3 性能分析和比较

基于网络反馈的改进方案优点在于能准确地获取网络状态信息,因为信息直接来自于中间节点的反馈。但它需要对移动 Ad Hoc 网络中的每个节点配置检测功能,从而增加了网络开销,也加大了网络的安全隐患。同时,由于需要中间节点的支持,网络反馈的方案也不利于 Ad hoc 网络和其他固定有线网络之间的协作。

"端到端"的改进方案不需要中间节点的支持,而是通过在 TCP 连接的两端进行参数检验来判断网络状态。这类方案维持了 TCP 协议"端到端"的特性,能更好的和传统 TCP 兼容。但由于它是通过参数检验间接获取网络状态信息,因此判断准确性不如网络反馈的方案。

TCP-ELFN 考虑了路由重计算和网络分割对 TCP 性能的影响,通过区别对待网络拥塞和链路错误丢包,很大程度上提高了 TCP 的性能。相比 TCP-ELFN,ATCP 方案对影响 TCP 性能的因素考虑得更为全面,如信道误码和数据包乱序。

TCP DOOR 通过对 OOO 包的检测来判断网络是处于拥塞还是发生了路由变化,但它不能处理信道误码和网络分割等情况,而且其检验准确性不是很高。MMJI 方案通过 4 个参数的联合检验在一定程度上提高了判别网络状态的准确度,同时也能够区分更多的网络状态。

表 3 给出了这几种方案的性能比较。

表 3 几种 TCP 改进方案的性能比较

	信道误码	路由重计算	网络分割	数据包乱序	检验准确性	吞吐量增益	网络开销和网络安全性	和传统网络的协作
TCP-ELFN		*	*		高	大	网络开销大,安全性较低	差
ATCP	*	*	*	*	高	未仿真	网络开销大,安全性较低	差
TCP DOOR		*		*	一般	一般	网络开销小,安全性较高	好
MMJI	*	*	*	*	较高	较大	网络开销小,安全性较高	好

其中:"*"表示可以区分并处理这种网络状况,空格表示不能区分。

4 结语

TCP 协议是针对固定有线网络设计的,在移动 Ad Hoc 网络中,经常发生信道误码或网络分割等情况。TCP 协议不能正确区分和处理这些情况造成的丢包,因此传输性能急剧下降。为提高 TCP 的传输性能,近年来提出了一些 Ad Hoc 网络中 TCP 的改进方案,主要分为两类:基于网络反馈的方案和"端到端"的方案。

Ad Hoc 网络未来将广泛应用于个人通信领域,需要使一台普通电脑(如笔记本)能够随心所欲的加入到 Ad Hoc 网络中。"端到端"的改进方案不需要中间节点的支持,将更有利于实现这一点。

从另一个角度考虑,在军事领域或其他特殊领域,Ad Hoc 网络是作为边缘网络存在,网络中的主机要面临能源和带宽受限等诸多问题。此时更准确的获取网络状况,提高 TCP 协议的传输性能更为关键,因此网络反馈的方案更适合这些领域。

需要指出的是,在移动 Ad Hoc 网络中,TCP 传输性能的提高还不仅仅依赖于对 TCP 协议本身的改进。例如,在 MAC 层的机制中,隐终端和暴露终端问题,以及带宽不对称问题,都在很大程度上影响了 TCP 协议的性能;路由层中,研究设计出稳定且健壮的 Ad Hoc 网络路由协议,也对 TCP 的性能起着至关重要的作用。

参考文献:

[1] CORSON S, MACKER J. Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations [S]. RFC2501, 1999.

[2] JOHNSON DB, MALTZ DA. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks [EB/OL]. Internet-Draft, draft-ietf-manet-dsr-10.txt, 2004.

[3] PERKINS C, BELDING-ROYER E, DAS S. Ad hoc On-Demand Distance Vector (AODV) Routing[S]. RFC3561, 2003.

[4] SEMERIA C. Supporting Differentiated Service Classes: TCP congestion Control Mechanisms [Z]. Sunnyvale: Juniper Networks Inc, 2002.

[5] LEINEN S. ECN (Explicit Congestion Notification) in TCP / IP [EB/OL]. http://www.icir.org/floyd/ecn.html, 2004.

[6] HOLLAND G, VAIDYA N. Analysis of TCP Performance over Mobile Ad Hoc Networks [Z]. MOBICOM'99, 1999.

[7] LIU J, SINGH S. ATCP: TCP for Mobile Ad Hoc Networks [J]. IEEE Journal, 2001, 19(7): 1300-1315.

[8] WANG F, ZHANG YG. Improving TCP Performance over Mobile Ad Hoc Networks with Out-of-Order Detection and Response [Z]. Mobihoc'02, 2002.

[9] ZHENG HF, GREENSTEIN B, MENG XQ. Design and Implementation of a TCP-Friendly Transport Protocol for Ad Hoc Wireless Networks [Z]. ICNP'02, 2002.

(上接第 247 页)

PBR²S 的优点还体现在其灵活性方面。一方面,基于策略管理的特点就是灵活性;另外,其分布 DNS 服务器具有可重用性,可以被其他 CDN 重复使用,从技术角度来看,这样有利于灵活地组建更大规模的 CDI。

最后,PBR²S 还具有可扩展性。这里的可扩展性体现在三个方面:1)规模的可扩展性,采取 PBR²S 的 CDN 系统之间可以很方便地建立互联关系,通过共用的分布 DNS 服务器群,简化了将多个孤立的 CDN 扩展成 CDI 的过程。2)策略框架中层次结构的可扩展性,上述内容所提及的只有一个全局的 PDP,在实际的操作中可以设计多个 PDP,从而增强系统的层次感和规模。3)性能的可扩展性,若是将各边缘服务器进行集群化,并且在前端放置第 4/7 层交换机,则系统的稳定性、安全性以及服务的粒度将会得到显著的改善。

4 结语

我们对现有 CDN 路由请求机制进行分析的同时,提出了 PBR²S 架构。PBR²S 是一个基于 DNS 机制并包含策略框架的路由请求系统,该系统架构采取分布式的结构,标准化的协议,具有良好的安全性、灵活性和可扩展性,能够对 CDN 的路由请求进行合理有效的规划,最大限度地满足用户对内容的需求。

参考文献:

[1] JOHNSON KL, CARR JF, DAY M, *et al.* The measured performance of content distribution networks[J]. Computer Communications, 2001, 24: 202-206.

[2] DAY M, CAIN B, TOMLINSON G, *et al.* RFC 3466, A Model for Content Internetworking (CDI)[S], February 2003.

[3] BARBIR A, CAIN B, DOUGLIS F, *et al.* RFC 3568, Known CN Request-Routing Mechanisms[S], July 2003.

[4] BILIRIS A, CRANOR C, DOUGLIS F, *et al.* CDN Brokering[A]. AT&T, In Proceedings of the 6th International Workshop on Web Caching and Content Distribution[C]. Boston, MA, June, 2001.

[5] WESTERINEN A. RFC 3198, Terminology for Policy-Based Management[S], November 2001.

[6] KANGASHARJU J, ROSS KW, ROBERTS JW. Performance Evaluation of Redirection Schemes in Content Distribution Networks[A]. 5th Web Caching Workshop[C]. Lisbon, Portugal, May 2000.

[7] KANADA Y. Dynamically Extensible Policy Server and Agent[A]. 3rd International Workshop on Policies for Distributed Systems and Networks (Policy 2002)[C], June 2002.

[8] VIXIE P, THOMSON S, REKHTER Y, *et al.* RFC 2136, Dynamic Updates in the Domain Name System (DNS UPDATE)[S], April 1997.

[9] WELLINGTON B. RFC 3007, Secure Domain Name System (DNS) Dynamic Update[S], November 2000.

[10] JUNG J, KRISHNAMURTHY B, RABINOVICH M, *et al.* Flash Crowds and Denial of Service Attacks: Characterization and Implications for CDNs and Web Sites[A]. In Proceedings of the International World Wide Web Conference[C], May 2002.