基于分组和差错恢复组的可靠多点广播协议研究

Research of Reliable Multicast Protocols Based on Grouping and Error-Recovery Group

符云清　张　伟　吴李瀚　吴中福

（重庆大学计算机科学与工程学院　重庆400044）

Abstract　This paper proposes a reliable multicast protocol which is appropriate for real-time and interactive collaborative environment. The grouping and error-recovery group mechanism are introduced to make error recovery localized, which can efficiently decrease the amount of packet stream on the backbone and the workload of host. Analysis and practice show that the protocol has perfect performance and can be extended to very wide and large scale applications.

Keywords　Protocol, Multicast, Reliable multicast

1　引言

在多用户实时协同应用环境中，发送方要将报文信息以较小的端到端延迟传送给远程的多个接收者，以保证协作的实时性和交互性[1]。传统点对点通信方式和广播通信方式都难以满足大规模协作应用的要求。多点广播协议(multicast)综合了点对点通信和广播通信的优点，发送方一次便可将报文高效地传送给指定的多个接收者，且多点广播路由协议保证任何给定的链路仅使用一次。因此，多点广播协议能充分利用通信网的传输能力，降低报文传输延迟。

要求实时传输和处理的音频和视频等连续媒体适合采用多点广播方式传送。参与协作用户的状态变化、交互协作中的共享信息及控制信息等既需要以较小的端到端延迟实时传输，又要保证传输的可靠性，传输过程中的任何差错必须及时纠正，以保证协作的一致性和有效性[2]。这便要求在多点广播协议的基础上提供可靠报文传输服务，即需要可靠多点广播协议。

传统点对点通信方式中的可靠传送机制并不适合一个发送节点和多个接收节点的应用场合。首先，多个接收节点在短时内几乎同时发送 ACK/NAK 报文，这些大量突发的应答报文将导致“应答爆炸”[3]，容易导致网络拥塞。其次，发送节点要负责处理所有节点的应答报文，管理和维护大量接收者的状态信息，并负责报文重传，将导致主机性能瓶颈。可靠多点广播协议大多采用 NAK 抑制技术[4]，即未正确接收报文的节点采用随机延迟和多点广播应答报文方法，保证发送方在最好情形下最多只收到一个 NAK 报文，达到抑制 NAK 报文的目的，避免了上述网络拥塞和性能瓶颈问题。

目前，世界上许多研究小组致力于可靠多点广播协议的研究，提出了多种适合不同应用场合的可靠多点广播协议，如基于登记服务器的可靠多点广播协议[5]和基于 ACK 树的可靠多点广播协议[6]等。但是，大多数协议中，小部分接收节点因链路拥塞、本地缓冲容量或接收速度限制等原因造成报文丢失或出错时，其应答和重传报文都涉及整个网络或大量已正确接收报文的节点，且大多由固定节点(通常是发送节点)来处理请求和进行报文重传。因此，协议的吞吐性能、扩展性、端到端传输延迟都很难满足大规模实时交互协作的要求。

2　基于分组和差错恢复多点广播组的可靠多点广播协议

当协作用户分布的网络范围很大时(大型广域网、甚至 Internet)，各协作用户分散在网络的各个部分。高效的可靠多点广播协议必须将差错恢复尽可能控制在网络的局部，而不应涉及整个网络或大量已经正确接收报文的节点，且应在节点间均衡处理负担，而不应由某个固定节点来集中处理请求和重传报文。

基于上述要求，作者提出了基于分组和差错多点广播组的可靠多点广播协议(Group and Recovery Multicast Group Based Reliable Multicast Protocol，GRRMP)。GRRMP 协议对参与协作的用户按一定的原则进行分组，并将未能正确接收报文的节点加入到差错恢复多点广播组，利用该多点广播组进行报文重传，从而使差错恢复完全局部化，保证协议具有良好的吞吐性能、扩展性和较小的传输延迟。

2.1　分组思想

大型网络通常是由许多局域网通过接入网与骨干网连接而形成的互连网(internet)，协作用户分布在局域网中。众所周知，局域网具有较高的传输带宽和可靠性，而接入网部分的传输速率和可靠性相对要低得多，如 DDN 传输速率通常为 64kbps～2Mbps。差错恢复时，如利用所有参与协作的用户组成的多点广播组进行请求和重传，短时内大量的重传请求将集中传送给发送节点，这些请求报文会蔓延到低速的接入网链路上，容易造成网链路饱和，导致拥塞；且发送节点因处理负担过重而造成性能瓶颈。上述情况如图1所示。

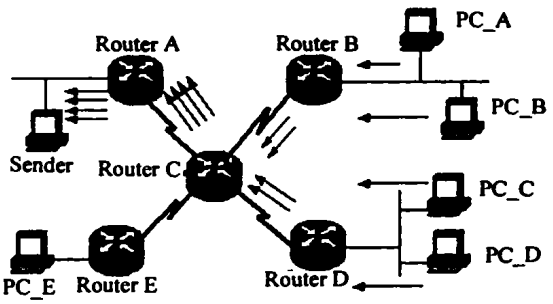

图1　接收节点直接向发送节点传送应答过程

为此，我们按照一定的原则对参与协作的节点进行分组，

每个分组包含若干成员节点，用唯一的D类IP地址进行标识。每个分组中指定一个管理节点，由管理节点负责处理该分组内的成员节点的请求报文和进行组内报文重传。这样，应答和重传报文都限制在网络的局部（即分组内），只有当管理节点未正确接收报文时，才通过接入网向外发送重传请求，重传报文也只传送给分组管理节点，再由分组管理节点重传给组内成员节点。这样既分散了差错处理负担，又大大减少了接入网和骨干网上的差错处理负担，还大大减少了接入网和骨干网上的通信流量，如图2所示。

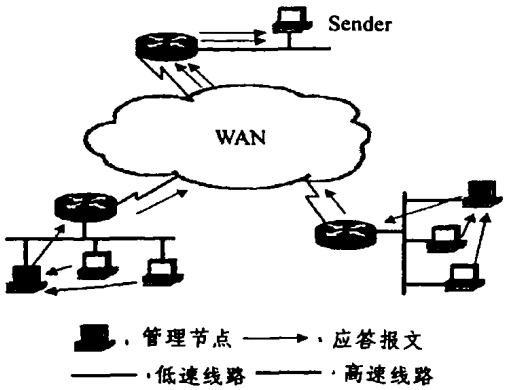

图2　接收节点通过管理节点向发送节点传送应答过程

2.2　差错多点广播组思想

通常，可靠多点广播协议正常传输的报文和因差错恢复而重传的报文都是使用同一个多点广播组地址。这样，已经正确接收报文的节点也将收到重传报文，增加这些节点不必要的处理开销和造成网络带宽浪费。

为此，我们提出差错多点广播组的思想：发送方正常广播报文时使用一个多点广播分组，而差错恢复时，使用另外一个多点广播组，即差错多点广播组。未正确接收报文的节点加入到该差错多点广播组，一旦正确接收报文，则退出该差错多点广播组。这样，保证已经正确接收报文的节点不会再收到该报文的重传报文，减少不必要的处理负担和网络带宽浪费。

为便于理解，下面以发送节点一次发送一个报文为例，阐述其工作原理。

假设发送方与所有接收方同时加入多点广播组G_0和G_1

2.2.1　*采用基于发送方的可靠多点广播方法（简称协议P0）*　假设发送节点要传送的报文序号为$i(i>=1)$，则

$j=i \bmod 2-1$，$k=1-j$

1）发送节点利用G_j向所有管理节点多点广播报文i，并启动发送定时器；

2）分组管理节点正确接收到报文i后，立即以点对点可靠传输方式向发送节点回送报文i的ACK应答，并退出多点广播组G_j，加入多点广播组G_k；

3）发送定时器超时前，若发送节点收到所有管理节点的ACK应答，若发送节点还有报文需要发送，则$i=i+1$，$j=i \bmod 2-1$，$k=1-j$，转1）继续；若发送节点无报文继续发送，则终止发送；

4）发送定时器超时后，若发送节点未收到所有管理节点的ACK应答，则转1）继续，直到收到全部应答或超过最大重传次数为止。

2.2.2　*采用基于接收方的可靠多点广播方法（简称协议P1）*

1）发送方将报文P多点广播给多点广播组G_0；

2）接收方r一旦发现报文P丢失或错误，则立即加入到多点广播组G_1，并随机延迟一段时间ΔT；

3）接收方r在ΔT时间内若未收到其它接收节点对报文P的NAK报文，则向多点广播组G_0广播对报文P的NAK报文，并启动定时器；若接收方在ΔT时间内若收到其它接收节点对报文P的NAK报文，则不再广播对报文P的NAK报文，只是启动定时器；

4）发送节点收到对报文P的NAK报文后，立即向多点广播组G_1广播报文P；

5）接收方r在定时器超时前，若正确收到发送方的重传报文P，则立即退出多点广播组G_1；若定时器timer超时后，r尚未正确收到发送方的重传报文P，则转2）继续，直到正确接收到报文P或超过规定的最大次数为止。

2.3　基于分组和差错多点广播组的可靠多点广播协议

在可靠多点广播协议GRRMP中，同时引入上述分组和差错多点广播组机制。首先，对所有参与协作的用户进行分组，每个分组指定多点广播地址G_0和G_1（一个用于正常的报文传送，一个用于差错恢复重传），所有分组管理节点与发送节点组成一个多点广播分组，并指定多点广播地址GM_1和GM_2。报文传输过程，实际上是分两步进行，首先发送节点将报文可靠地传送给所有的分组管理节点，然后各分组管理节点将接收的报文可靠地传输给其组内成员节点。在这两个过程中，既可采用基于发送方的可靠多点广播协议，也可采用基于接收方的可靠多点广播协议。报文重传时，采用上述差错多点广播组思想，即采用与正常报文传送不同的多点广播组。

我们知道，在基于接收方的可靠多点广播协议中，发送方若在某个固定的时间片MaxInterval无报文发送，则必须多点广播一个“心跳”（keep-alive或Heartbeat）报文，报文序号为已经传送的最大报文序号。接收方利用该“心跳”报文和自己的定时器来检查是否报文丢失（报文序号不连续或在MaxInterval时间内未收到报文）。这样各接收方都设置一个定时器，记录从上一次从发送方接收报文到目前已经过去的时间。另外，每个接收方还要维持一个“接收报文序号”计数器。

在有n个用户的多对多实时交互协同应用中，每个节点都要定时向其它n－1节点多点广播这种“心跳”信息，每个节点都要维持一个具有n－1项的“心跳”信息表，每收到一个报文，节点便更新该表中的相关记录项。同时，每个节点还有n－1个定时器在工作。这样，增加了处理器负担，影响了实时交互协同效果，在时间和效率上都是不经济的。

因此，在GRRMP协议中，我们使用基于发送方的可靠多点广播协议，即在发送方和各管理节点，以及管理节点和各成员节点间都采用类似2.2.1节中基于发送方和差错多点广播组的可靠多点广播方法，协议工作原理简单阐述如下：

（1）发送节点利用“点对点”可靠传输方式将报文传送给其所在分组管理节点。

Sender $\xrightarrow{\text{reliable unicast}}$ Sender所在分组的管理节点

（2）发送节点所在的分组管理节点将报文多点广播给所有分组管理节点组成的多点广播分组，采用基于发送方和差错恢复组的可靠多点广播协议。

Sender所在的分组管理节点 $\xrightarrow{\text{协议P0}}$ 所有其它分组管理节点

（3）各分组管理节点将报文多点广播给所有分组成员节点，采用基于发送方和差错恢复组的可靠多点广播协议。

（下转第66页）

击。

在这一领域的下一步研究中，以下方向是值得注意的：移动代理防恶意复制，基于参考状态的恶意主机攻击检测，基于移动代理复制的一般化攻击检测方法，基于智能卡的防恶意主机攻击系统的研究，基于加密函数计算的防恶意主机攻击方法研究，时限黑箱有效构建方法，等。

参 考 文 献

1 Farmer W M, Guttman J D, et al. Security for mobile agents: Issues and requirements. In: Proc. of the 19th National Information Systems Security Conf. Baltimore, Md., October 1996. 591～597. http://csrc. nist. gov/nissc/1996/papers/NISSC96/paper033/SWARUP96. PDF

2 Ng S K. Protecting Mobile Agents against Malicious Hosts. Master Thesis. Division of Information Engineering, The Chinese University of Hong Kong, June 2000. http://mole. informatik. uni-stuttgart. de/security/ngthesis. pdf

3 Yee B S. A Sanctuary for Mobile Agents. DARPA Workshop on Foundations for Secure Mobile Code, Feb. 1997. http://www. cs. ucsd. edu/～bsy/pub/sanctuary. ps

4 Westhoff D, Schneider M, et al. Protecting a Mobile Agent's Route against Collusions. In: Proc. of SAC'99, Springer LNCS 1758, 1999. http://www. informatik. fernuni-hagen. de/import/pi2/agents/Papers/ontario99-env. ps

5 Baek J. A design of a protocol for detecting a mobile agent clone and its correctness proof using Coloured Petri Nets: [Technical Report TR-DIC-CSL － 1998-002]. Info. &Comm., K-JIST, 1998. http://atom. kjist. ac. kr/～jsbaek/pub/tr-dic－1998-02. ps

6 Vigna G. Protecting Mobile Agents through Tracing. Mobile Object Systems ECOOP Workshop'97. http://arthur. cs. ucdavis. edu/～barnes/seminar/papers/vigna97. ps

7 Hohl F. A Protocol to Detect Malicious Hosts Attacks by Using Reference States. Universitat Stuttgart, Fakultat Informatik, Bericht Nr. 1999. ftp://ftp. informatik. uni-stuttgart. de/pub/library/ncstrl. ustuttgart_fi/TR－1999-09/TR－1999-09. ps. gz

8 Farmer W, Guttman J, et al. Security for Mobile Agents: Authentification and State Appraisal. Fourth European Symposium on Research in Computer Security (ESORICS 96), P. 118－130. http://imps. mcmaster. ca/doc/esorics96. ps

9 Tschudin C. Environmental Security: Apoptotic Functions and a Way to Protect Them. 4th WORKSHOP ON MOBILE OBJECT SYSTEMS: Secure Internet Mobile Computations. In association with the 12th European Conference on Object-Oriented Programming (ECOOP'98), 21 July 1998, Brussels, Belgium. http://cuiwww. unige. ch/～ecoopws/ws98/slides/tschudin. ps

10 Guan Xudong, Yang Yiling, et al. POM - A Mobile Agent Security Model Against Malicious Hosts. In: Proc. HPC-Asia 2000, pp. 1165～1166, Beijing, China, May. 15～18, 2000. http://202. 120. 7. 27/member/～gxd/pom(hpcasia2000_2_pages). zip

11 Minsky Y, van Renesse R, et al. Cryptographic Support for Fault-Tolerant Distributed Computing. In: Proc. of the Seventh ACM SIGOPS European Workshop. Connemara, Ireland, September 1996. 109～114. http://www. tacoma. cs. uit. no/papers/SIGOPS. ft-agents. ps

12 Wilhelm U G. A Technical Approach to Privacy based on Mobile Agents Protected by Tamper-resistant Hardware. PH. D. dissertation. 1999. http://lsewww. epfl. ch/～ wilhelm/Papers/thesis. pdf

13 Funfrocken S. Protecting Mobile Web-Commerce Agents with Smartcards. In: Proc. of the First International Symp. on Agent Systems and App. s / 3rd International Symp. on Mobile Agents (ASA/MA'99), IEEE Computer Society, 1999. 92～102. http://www. informatik. th-darmstadt. de/VS/Publikationen/papers/ma99/secure-webagents. pdf

14 Hohl F. Time Limited Blackbox Security: Protecting Mobile Agents From Malicious Hosts. In: Vigna G, ed. Mobile Agents and Security. Springer-Verlag, 1998. 92～113. http://www. informatik. uni-stuttgart. de/ipvr/vs/projekte/mole/vignabuch. ps. gz

15 Sander T, Tschudin C. Towards Mobile Cryptography. IEEE Symposium on Security and Privacy, 1998. 215～224. ftp://ftp. icsi. berkeley. edu/pub/techreports/1997/tr-97-049. ps. gz

16 Loureiro S, Molva R. Function Hiding Based on Error Correcting Codes. In: Blum M, Lee C H, eds. Cryptographic Techniques and E-Commerce. Proc. of the 1999 Intl. Workshop on Cryptographic Techniques and E-Commerce (CrypTEC '99), City University of Hong Kong Press. ftp://ftp. eurecom. fr/pub/loureiro/cryptec99. ps. gz

17 Feigenbaum J, Merritt M. Open questions, talk abstracts, and summary of discussions. DIMACS Series in Discrete Mathematics and Theoretical Computer Science, 1991, 2: 1～45,

18 Lipton R, Sander T. An additively homomorphic encryption scheme or how to introduce a partial trapdoor in the discrete log. Nov. 1997

（上接第58页）

分组管理节点 —协议 P0→ 分组成员节点

协议 GRRMP 具有这样一些特点：(1)采用分组和差错恢复组思想，实现差错恢复本地化，减少骨干网上报文流量。(2)已经正确接收报文的节点不会接收到重传报文，能避少不必要的处理开销及网络资源浪费。(3)支持“点对多”和“多对多”可靠报文传输服务。

结论 作者采用 B. N. Levine 和 J. J Garcia-Luna-Aceves 在文[3]中提出的模型，对协议 GRRMP 的吞吐性能、骨干网上的报文流量、传输延迟等进行了分析，并在校园网环境下，利用该协议实现了远程教学中的共享白板应用。分析和实验表明，该协议具有良好的吞吐性能、较小的传输延迟，能有效减少骨干网上的通信负荷。由于使用了分组和差错恢复多点广播组策略，使差错恢复局部化，同时均衡了主机的处理负担，克服了集中处理的性能瓶颈问题，因此协议 GRRMP 能适合大规模分布式实时协同应用环境。

参 考 文 献

1 龙晓苑，吴良芝. 多媒体通信协议与应用. 清华大学出版社，1998

2 郑庆华. CSCW 的理论、实现方法与应用. 计算机科学，1996，23(5)：18～25

3 Towsley D. A Comparison of Sender-Initiated and Receiver-Initiated Reliable Multicast Protocol. Proceeding of ACM Multimedia，1996，11(2)：282～291

4 Holbrook H W. Log-based Reliable Multicast for DIS. Proceeding of SIGCOMM'95，1995，25(4)：328～341

5 Levine B. The Case for Concurrent Multicast Using Shared ACK Trees. Proceeding of ACM Multimedia，1996，11(2)：365～376

6 Yavatkar R. A Reliable Dissemination Protocol for Interactive Collaborative Application. University of Kentucky，1995(10)：36～47