容延容断网络研究及进展

郭 航 王兴伟 黄 敏 蒋定德
(东北大学信息科学与工程学院 沈阳 110004)

摘 要 容延容断网络(Delay/Disruption Tolerant Networks,DTN)是基于星际网络而提出的一种异于传统网络的抽象网络模型。从网络协议、路由算法、组播和安全机制4个方面综述DTN的研究概况及进展,分析各种协议、算法、机制的性能及特点并进行比较,指出DTN研究面对的挑战和进一步发展方向。

关键词 容延容断网络,网络协议,路由算法,组播,安全机制

中图法分类号 TP915.9 **文献标识码** A

Research on Delay/Disruption Tolerant Networks

GUO Hang WANG Xing-wei HUANG Min JIANG Ding-de
(College of Information Science and Engineering, Northeastern University, Shenyang 110004, China)

Abstract Delay/Disruption Tolerant Networks (DTN) are an abstract network model different from traditional networks, which is proposed based on interplanetary networks. This paper provided an overview on recent development in these areas of DTN, including network protocol, routing algorithm, multicast schemes, and security mechanism. It also analyzed and compared in detail kinds of protocols, algorithms, and mechanisms about DTN in performance and features, and pointed out some open research issues and the further development.

Keywords Delay/disruption tolerant networks, Network protocol, Routing algorithm, Multicast, Security mechanism

1 引言

容延容断网络(Delay/Disruption Tolerant Networks,DTN)是指能在长时延、连接频繁断开等受限网络条件下进行通信的一种新型网络体系。DTN最初主要应用于星际网络(Interplanetary Networks)和军事战地网络(Military battlefield Networks),后来随着移动自组织网络(Mobile Ad hoc Networks)等无线网络的发展而拓宽至其它领域,如乡村网络(Village Networks)、口袋交换网络(Pocket Switch Networks)、车载网络(Vehicle Networks)、野生动物监测网络(Wildlife Monitoring Networks)等。

DTN的概念于2003年由Fall[1]首先提出,随后因特网研究任务组(Internet Research Task Force,IRTF)在星际网络研究组(Interplanetary Network Research Group,IPNRG)的基础上成立了容延容断网络研究组(DTN Research Group,DTNRG)对其进行研究,并于2007年提出DTN网络体系结构[2]及Bundle协议(Bundle Protocol,BP)[3],2008年提出包括TCPCLP协议(TCP Convergence Layer Protocol)[4]、Saratoga协议[5]及Licklider协议(Licklider Transmission Protocol,LTP)[6-8]等在内的汇聚层协议,并针对BP协议的不足提出补充方案[9]。目前研究者在DTN相关领域内开展了广泛研究并进行了具体部署与试验,如英国设计的UK-DMC(United Kingdom Disaster Monitoring Constellation)灾害监测卫星网络[10]、在瑞典北部进行的SNC(Sami Network Connectivity)乡村网络试验[11]、美国进行的DieselNet车载网络试验[12]、在非洲实施的斑马监测网络[13]、鲸鱼监测网络[14]以及利用传感器节点或手机进行的一些DTN试验[15]等。这些试验表明,DTN尽管仍存在一些问题,但能够在现有网络无法覆盖的地区或特殊条件下提供有效的网络服务。

DTN涉及的网络环境多样,不满足传统网络模型中存在持续的端到端连接这一前提且网络资源受限,因此其相关技术比较复杂。本文首先从网络协议、路由算法、组播和安全机制4个方面详细介绍DTN的研究概况及进展,然后分析DTN中各种协议、算法、机制的性能及特点,最后指出DTN研究面对的挑战和进一步发展方向。

2 容延容断网络进展

2.1 DTN网络协议

IRTF设计的DTN网络体系以BP协议为主要协议,利用其协议数据单元"束"(bundle)进行信息传输,采用不同的汇聚层协议,以使BP协议适用于各种网络情况。BP协议与汇聚层协议的关系及在协议栈中的位置如图1所示[16]。

到稿日期:2009-12-02 返修日期:2010-03-01 本文受国家自然科学基金(61070162,71071028,60802023,70931001),高等学校博士学科点专项科研基金(20070145017),中央高校基本科研业务费专项资金(N090504003,N090504006)资助。

郭 航(1981-),男,博士生,主要研究方向为容延容断网络等,E-mail:guohang0001@126.com;王兴伟(1968-),男,博士,教授,博士生导师,主要研究方向为下一代互联网等;黄 敏(1968-),女,博士,教授,博士生导师,主要研究方向为智能优化算法和调度理论等;蒋定德(1974-),男,博士,主要研究方向为网络测量、网络安全、流量异常检测。

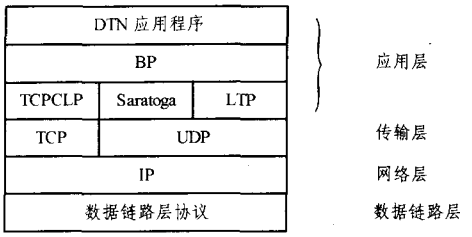

图 1　BP 协议与汇聚层协议的关系及位置

从图中可以看出，BP 协议及汇聚层协议均位于应用层，BP 协议通过不同的汇聚层协议应用于 TCP 和 UDP 之上，为 DTN 应用程序提供服务。

2.1.1　BP 协议

BP 协议将束层通过汇聚层叠加于传输层之上，形成存储转发式的重叠网络结构。该协议为 DTN 提供了一种通用解决方案，通过多种汇聚层支持异构网络互连，能够满足不同的网络情况。BP 协议定义了该层的协议数据单元束以及束的处理和记录管理过程，对束的格式、分片与重组、命名与路由、保管传输、拥塞与流量控制、可靠性与安全等方面进行了描述。

束由至少两个数据块串联组成，前面为强制性的基本块，其后为可选的负载块及扩展块，最后一个数据块含有结束标志。基本块中不仅有类似 IP 头部的一些信息，还有 BP 协议独有的产生时间戳、寿命、服务等级标志、报告节点和保管节点、字典等。为减少传输损耗，基本块中大量采用灵活的自定界数值(Self-Delimiting Numeric Values，SDNV)，利用字典对长度可变的端点标识符进行编码并在负载块中使用以节约存储空间。为适应 DTN 网络特点，BP 协议中束采用保管传输，利用统一资源定位符为节点建立命名系统，使用后期绑定在端点指示符(Endpoint Identifier，EID)和本地网络地址之间进行映射，即不在源节点而由路由节点根据名称匹配进行绑定。束的大小没有具体要求并可以进行主动或被动分片，但分片会给加密和认证带来挑战。BP 协议不包含错误检测的检验和机制，其可靠性和安全机制由扩展协议或其它协议来实现。

2.1.2　汇聚层协议

1)TCPCLP 协议

TCPCLP 协议是基于 TCP 的汇聚层协议，通过建立 TCPCL 连接使束在 TCP 网络环境中进行双向传输，TCPCL 连接与 TCP 连接同时产生和释放并一一对应。

TCPCLP 协议中束的传输可以分为连接建立、数据传输、连接释放 3 个阶段。连接建立时，发起方初始化 TCP 连接，互相交换接触头部以确定连接的参数，并为节点建立单独的端点标识符以辅助路由并防止循环的发生。TCPCL 连接建立和配置完成后即可进行传输。束可以分片传输，但传输过程中束和分片必须依次顺序传输，每个分片只能包含一个束的数据，分片的长度取决于具体实现。束的首个分片必须包括开始标志，最后一个分片必须包括结束标志，每个分片都包含由 SDNV 定义的长度字段以指明本分片的大小。确认信息和否定确认信息均为可选部分，发送方收到拒绝信息时将终止当前束的传送，以节约传输容量，实现跨层优化。对于空闲连接，周期性地发送保活信息，并在累计一定时间后终止该连接。在传输结束前需要发出关闭信息，此时信息发送方可以继续发送确认信息或拒绝信息，但不能继续发送数据，同时节点也可以通过该信息拒绝连接的建立。

2)LTP 协议

LTP 协议作为 BP 协议的汇聚层协议，能在链路长时延和频繁中断的情况下提供基于重传的可靠通信，可以运行于数据链路层之上或 UDP 之上，其命名是为了纪念因特网的先驱者 Licklider。

LTP 协议是一种单向通信协议，通信前不需要进行协商与握手，为保证可靠传输并具有自动重传功能，必须保留会话的状态信息。该协议把数据分为红色部分与绿色部分，发送方将数据块分片时在红色部分结束后加上结束标志并设置校验点，接收端遇到该标志时必须返回接收报告，对红色部分进行确认，并在必要的时候进行重传。绿色部分则无需确认及重传，两部分的长度都可以为零。红色部分并非比绿色部分内容紧急或优先级高，而是要求确保传输。可见 LTP 在一次会话过程中能同时提供类似于 TCP 和 UDP 的传输。LTP 通信中的半双工状态使得无法通过历史统计数据来计算自动重传时间而采用估计与动态计时，重传可以稍晚几秒但不能提前，晚几秒仅稍微增加一些时延，而过早不必要的重传会给网络带来较重负担。LTP 协议可以通过在结束标志前的任意位置设置校验点并在出错时由接收端返回异步接收报告，实现加速重传。

3)Saratoga 协议

Saratoga 协议是一种轻量级的基于 UDP 的汇聚层协议，为束层或束代理提供服务。该协议最初设计用于低轨卫星所拍摄的遥感图像的文件传输，也可用于其它 DTN 环境，其命名是为了纪念美国二战时的航母 Saratoga 号。

Saratoga 协议采用简单的选择性否定确认自动重传机制，包含文件校验和机制，以检测传输错误从而提供可靠传输。校验和对小文件采用循环冗余校验(Cyclic Redundancy Check)，对大文件采用 MD5(Message-Digest Algorithm 5)或 SHA-1(Secure Hash Algorithm)算法。Saratoga 协议是一种点对点协议而不局限于客户端/服务器模式，可以在长延时或频繁中断的情况下传送文件或数据流，主要提供文件尤其是数据量巨大的文件之间的单跳传输，通过选择文件偏移量描述符来有效地传输不同大小的文件。该协议具有存储、获取、获取目录和删除 4 种操作，节点通过标志信息来发布它们的存在、容量及需求，传输通过各种操作开始。当接收端拒绝或者接收本次传送后，会产生并返回描述性的元数据包，内容包括拒绝接收或描述缺失数据边界的信息，以进行选择性重传。Saratoga 协议可以传输任意数据块，能在束交换与文件传输之间进行映射。

2.2　路由算法

路由算法是 DTN 研究中最活跃的领域之一，涌现出大量研究成果。由于 DTN 网络资源受限且网络环境差异性较大，其路由目标、路由机制等也互有差别。有些路由算法混合采用多种路由方法，本文根据算法中核心路由机制的不同将其分为传染及受控传染路由、基于概率估计的路由和基于模型的路由等三类。

2.2.1　传染路由及受控传染路由

传染路由即中间节点不进行路由决策而将消息泛洪给除发送节点外的所有邻居节点。在节点充分移动且带宽、存储

空间足够大的情况下，传染路由几乎能将所有信息都正确分发且延迟较小，但大量冗余副本的存在使得该算法对网络资源要求较高，在资源受限的情况下性能大幅下降，为此提出受控传染路由算法。

为降低传输时延并增加传输率，Small[17]等提出了共享信息基站模型(Shared Wireless Infostation Model，SWIM)。SWIM与传统传染路由的区别是报文可以将任一基站作为目标节点，节点相遇时相互交换所存储的信息，当处于基站的通信范围内时把存储的所有信息传输至基站，信息的任意一个副本传输到任意基站即可完成传输。SWIM通过增加存储需求来降低传输时延，通过对基站分布的优化和网络节点过时信息的删除，能够以增加计算复杂度为代价降低存储需求并提高传输率。

为减少对网络资源的需求，Nain[18]提出了移动中继路由(Mobile Relay Protocol，MRP)。MRP将路由与存储相结合，当目的节点不可达时向附近节点发出受控本地广播。收到广播的节点存储信息并进入中继模式。在中继模式下首先检查是否有少于d跳的路由存在，有则进行转发，否则进入存储阶段：如果该信息已在节点缓存内，则丢弃旧的副本；若节点缓存未满，则存储信息并将生存时间参数减1；若存储空间已满，则将最近收到的生存时间大于零的信息取出并随机中继到附近的某个节点。MRP通过增加复杂度降低了网络资源消耗，可以通过参数改变路由性能。

为限制广播数量并适应节点高速移动的网络环境，Tchakountio[19]等提出喷射(Spraying)路由协议。该算法假设节点具有位置管理器并可获得任意节点的最近位置。传输时信息首先单播至目的节点附近的某节点，然后由其向附近节点进行多播，多播的数量由节点的移动性决定。这种算法将位置跟踪与转发相结合，避免了过多冗余副本的存在。为在不增加副本数量的基础上提高传输效率和降低传输时延，Spyropoulos等[20,21]提出喷射聚焦(Spray&Focus)路由协议，在聚焦阶段采用基于效用的路由协议，将数据转发给具有更高效用的节点。这类算法需要独立的位置管理器，在节点较多的大规模网络中难以实现。

2.2.2 基于概率估计的路由

基于概率估计的路由算法，中间节点不再盲目地向全部或部分邻居节点转发信息，而是估计邻居节点到达目的节点的概率或对链路状态进行估计，并据此进行路由选择，以计算量为代价降低对网络资源的需求。

Lindgren等[22]提出了PROPHET路由(Probabilistic Routing Protocol using History of Encounters and Transitivity)。该算法按式(1)在每个节点a上为每个已知节点b计算一个预测转发概率值$P(a,b)$，以表示从a到b成功转发的概率。

$$P(a,b)=\begin{cases}P(a,b)_{old}+(1-P(a,b)_{old})P_{init}, & a,b\text{相遇}\\ P(a,b)_{old}\times\gamma^{k}, & \text{其他}\end{cases} \quad (1)$$

式中，P_{init}表示概率初始化值，γ表示衰减因子，k表示节点上一次接触后所经过的时间。节点接触时交换已知的摘要向量和到目的节点的成功转发概率向量，并根据式(1)更新其分发概率。节点之间预测转发概率值也具有传递性，如果a、b及b、c间经常接触，则a能够将信息传送至c，$P(a,c)$按照式(2)进行更新。

$$P(a,c)=P(a,c)_{old}\times P(a,b)\times P(a,c)\times\beta \quad (2)$$

式中，β表示影响因子。该算法性能依赖于节点的移动模型，在组移动模型中性能较好。Li[23]等同时考虑节点相遇的频率和接触的持续时间，提出了E-PROPHET(Enhanced PROPHET)路由，仿真表明该算法具有更低的传输时延及开销。

为使路由算法自适应网络环境，Musolesi等[24]提出CAR(Context-Aware Routing)路由算法。该算法结合同步和异步的报文分发机制。同步机制指存在到达目的节点的端到端路径时，使用原有路由协议转发报文。在不存在端到端路径的异步机制下，报文被存储在具有最大概率到达目的节点的主机，这一过程利用时间序列分析方法中的卡尔曼滤波。传输概率的计算在网络发生断开时进行初始化，并持续至传输概率足够高为止。CAR是一种单副本路由算法，节点缓存较小时仍具有良好性能。

端到端性能的预测和估计也可以用来优化路由算法，Burns[25]提出了MV(Meets and Visits)路由。该算法统计节点间相遇及访问某区域的频率，按照历史信息对节点经特定路径成功转发的概率进行排序，把节点k经过n跳将信息转发到区域i的概率记作$P_n^k(i)$并按式(3)进行计算。

$$P_n^k(i)=1-\prod_{j=1}^{N}[1-m_{j,k}P_{n-1}^j(i)] \quad (3)$$

式中，$P_0^k(i)=t_i^{(k)}/t$，$t_i^{(k)}$表示节点j和k在同一区域相遇的次数。Burgess[26]在车载网络中对该算法进行扩展并提出MaxProp算法，它采用优化信息传输路径和缓存管理的方法并在网络内洪泛确认信息以消除网内过时信息。Tan[27]提出了SEPR(Shortest Expected Path Routing)算法，该算法按照式(4)基于历史数据计算链路估计转发概率。

$$P_{i,j}=\frac{Time_{connection}}{Time_{window}} \quad (4)$$

式中，$Time_{connection}$表示节点i，j连接的时间，$Time_{window}$是时间窗口长度的抽样值。根据$P_{i,j}$可以计算出最短期望路径，每个进入节点缓存的信息都被赋予一个有效路径长度，值越小意味着传输的概率越高，节点相遇时按有效路径长度从小到大顺序传输，若另一个节点到目标节点的期望路径长度较小，则更新有效路径长度值。SEPR算法不需要位置信息，可以向多个节点转发同一信息以提高传输率并降低时延。

2.2.3 基于模型的路由

实际应用中节点多具有一定的运动模式。例如通信卫星具有一定的轨道，由人或其它动物所携带的无线设备的运动方式也具有规律性并能反映出携带者的社会关系和社会网络状况。如能够精确地描述节点运动模式或利用节点间社会关系就可以更好地进行路由选择。

针对节点移动的循环性，Liu[28]提出了RCM(Routing in a Cyclic MobiSpace)路由算法。该算法认为，若两个节点在上一循环中某时间段接触，则下一循环中相同时间段再次接触的概率较高。在处理过程中，将移动模型化为概率时间-空间图，再将时间离散化以消除时间维度，转换为概率状态-空间图，利用马尔科夫决策过程计算节点间的期望最小延迟。仿真结果表明，在同样的场景下，其传输速率和时延优于MaxProp及喷射路由算法，但适用范围有限。

为提高关键节点在路由中的作用，Li[29]等提出了ANBR

(Articulation Node Based Routing)算法。该算法把全局意义上中断的网络看作若干个聚集的移动节点组成的互连的子网,节点的移动性使得子网之间具有通信的可能,但需要选择合适的节点来存储和传递信息。所谓关节节点指若移去该节点就会导致图无法连通的节点,因此关节节点将信息从聚集节点中传递出去的概率较大。当节点相遇时,相互交换相邻节点信息,以构建局部子图并计算关节节点,把需发送的信息传送至关节节点,由其进行存储并转发到其它关节节点,直至到达目的节点。ANBR 算法有较高的传输速率和较低的网络开销,但时延和计算复杂度较高。

将社会网络分析应用于 DTN 路由也是一个热点问题。Daly[30]等提出了 SimBet(Similarity and Betweenness)路由,利用社会网络中的小世界原理将具有较高中心性的节点作为桥节点以加快信息传递。由于大规模网络中中心性度量的复杂度,提出了自我网络(Ego Networks)的概念。节点通过构建局部网络拓扑结构图计算"介度"和"相似度"并据此计算节点的效用值,相遇时把信息传至效用值较高的节点。该算法不需要节点的先验知识或移动轨迹,并采用单副本方式,缺陷是若两个节点效用值相等,则信息会无法继续传输。Pan[31]等人在此基础上提出了 BUBBLE 路由,利用社会关系变化比较缓慢的特点研究网络的群体性和中心性,采用文献[32]中采用的方法进行群体检测,采用加权网络分析分布式计算个体中心性。传输时,首先将信息按照分层排序树向上传递,直至到达与目标节点同属一个群体的节点。然后利用局部排名树继续传递该信息,直至到达目的节点或超时。BUBBLE 算法解决了 SimBet 路由中信息在中间节点因效用值相同而无法继续转发的问题,采用分布式计算易于具体实施。这类算法主要基于小规模网络或短期数据。如何在一般网络中发现和寻找短链路尚需解决。

2.3 组播

许多潜在的 DTN 应用都是基于组播方式。但传统的组播方法不适用于 DTN 网络环境,需要开发新的组播语义模型和组播路由算法。

Abdulla[33]等采用受控传染路由实现 DTN 中的组播,提出 CERM(Controlled Epidemic Routing for Multicasting)算法。该算法不需要网络先验知识,而通过一系列控制机制实现资源消耗与传输速率之间的折中。采用的控制机制包括信息传输的最大跳数、信息超时时间、概率路由和副本数量等。与单播传染路由类似,CERM 算法复杂度低,但对网络资源要求较高。调整参数可以使其在各类网络环境下均获得高的传输率。

组播中也可基于概率估计进行路由。Xi[34]提出了 EBMR (Encountered Based Multicast Routing)组播路由。EBMR 仅基于节点间的接触进行路由,每个节点在一跳内广播其标志,并据此建立到任意已知节点的传输概率值,该值包含于标识信息中并在接收到其它节点的标识信息时进行更新。该算法能够经过较少的跳数进行高效率的组播。Yang[35]提出了 CAMR(Context Aware Multicast Routing)组播路由,该算法能够处理 DTN 中的机会连接和稀疏连接,分 5 个阶段进行多播:本地节点密度估计、两跳内邻居接触概率估计、路由发现、路由修复和信息传递。当源节点无法到达任何接收节点时,进入路由发现阶段,同时支持保管传输。当组播树断开时,进入路由修复阶段,以适用于不同的节点密度和节点移动模型。该算法能够适应节点稀疏或者移动性较强的场景,但依赖于路由发现机制和控制节点移动的能力。

Greifenberg[36]等提出了基于发布/订阅模式的组播路由,以有效地把信息分发到感兴趣节点。该算法通过向邻居节点复制束并经多跳的存储转发进行多播;在发布/订阅通信过程中节点在时间、空间、同步方面均为了适应 DTN 的特性而分离;把订阅管理与分发作为分布式网络功能;节点对资源利用及束的传输进行局部优化决策;根据本地资源情况独立地控制束处理过程,从而提供更好的全局网络性能。该算法的核心是节点相遇时如何交换订阅及束,步骤包括交换订阅列表;从本地缓存中建立待转发束队列并通过过滤器滤除传递至邻居节点不能增加传输概率的束;基于复制的效用计算优先级并根据优先级对束进行排序;对束进行传递直至队列空或者接触断开。过滤器包括已知订阅过滤器、跳数计算过滤器和副本过滤器 3 种类型,可以组合使用并结合优先级计算方法以适应不同的应用场景。

Yang[37]等提出了一种整合型域间组播算法,它采用基于摆渡的域间组播路由和包含冗余机制的域内组播路由 EBMR。假设网络包括多个域且各域均有一个领导节点和一个或多个摆渡节点。领导节点和摆渡节点装有定位系统和长距离无线电进行通信。领导节点与摆渡节点构成上层网络而其余节点构成下层网络。组播时,源节点把信息传输至本域领导节点并由其将信息转发至本地组成员及到访的摆渡节点。同时领导节点通过 EBMR 将它从到访摆渡节点处接收到的信息传送给本地多播组成员。增加摆渡节点个数或移动速度,能够提高网络性能,复制机制使得在节点稀疏的情况下算法仍然可行。

2.4 安全机制

DTN 网络资源受限,BP 协议必须确保只有经过认证的节点才能在网络中发送束,还要保证其通过网络时的完整性与保密性。尽管 BP 协议采用保管传输方案但并不包含检验和机制。为此在束安全协议中[38]定义了 3 种安全模块:束认证模块(Bundle Authentication Block)、负载完整模块(Payload Integrity Block)和保密模块(Payload Confidentiality Block),分别负责传输时逐跳的真实性与完整性、端到端的数据真实性与完整性、数据的保密性,模块可以同时或有选择地部分使用。束格式中缺少对头部和负载完整性的检查,文献[39]对此提出了可靠的加密算法,它可检查传输错误但对蓄意的篡改攻击无效。

TCPCLP 协议没有单独的安全机制,依靠下层 TCP 协议进行可靠性检测,依靠 BP 协议中的安全模块进行认证。Saratoga 协议采用可选的 MD5 码对传输部分进行完整性校验,这个校验和弥补了 UDP 较弱的传输层检验,覆盖了接收信息的重新组装。LTP 协议本身不包含保护头部、扩展数据部分和负载完整性的机制,因此需要底层校验和进行错误检测。但 LTP 协议中绿色部分允许差错而低层的校验和会影响绿色部分的效用,致使包含错误的绿色部分无法到达应用程序。文献[9]中提出了可选认证头部的解决方案,该头部独立于低层的校验和,能够保护红色部分而不影响容忍错误的绿色部分。

DTN 中的认证和加密由于网络状况的特殊性而难以实

现。Shi[40]等提出了基于信用的认证方法。该方法在处理高时延、高错误率的链路时，采用可更新的认证信用和多点本地认证机制，将未知网络部分隔离以减少等待时间。节点在签名认证时需要一定的计算量并引起额外的时延，DTN 中洪泛或多副本路由协议的使用使这种情况更加严重。为此 Zhu[41]等提出了批处理认证方法(Batch Bundle Authentication，BBA)，由离线安全管理器选择公钥/私钥对，并为每个节点产生一个密钥。节点发送束时用自己的私钥进行签名，然后中间和目的节点对签名采用批处理方法进行认证以确保完整性，处理时按源节点分情况处理并采用递归方法来检查签名的有效性。该方法能够快速有效地对束进行认证，并能抵御伪造签名类攻击。Asokan[42]提出了基于身份的加密方法，对密钥管理进行了改进，使得认证过程对服务器的需求减少而将大部分工作转移到发送端。接收到信息时不需要向服务器查询，在网络连接性较差时认证过程依然得以进行。

3 性能分析

下面分别从网络协议、路由算法、组播和安全机制 4 个方面对 DTN 研究中提出的协议、算法、机制进行性能分析，比较它们的优缺点并指出适用范围。

3.1 各种协议性能分析

BP 协议是 DTN 网络协议的核心内容，是 DTN 网络互联的通用解决方案，设计比较复杂且部分内容尚未明确定义，仍存在许多缺陷。BP 协议主要集中在束格式的逻辑设计而不是对协议实体即束代理间的操作和相互作用进行说明，因此更像是一种复杂的文件格式规范。协议中 EID 的格式及如何按照 EID 进行转发仍未定义，且缺少类似 DNS(Domain Name Service)和 SIP 协议(Session Initiation Protocol)的定位及解析服务，其全部依赖于后期绑定。地址映射的本地化增加了安全更新的难度，需要为束代理建立合法、安全和有效的注册管理机制。同时缺少对数据流 QoS(Quality of Service)的识别、标记、监管等功能。由于 DTN 大量使用网内存储和更加复杂的路由协议，后期绑定与 QoS 资源预留方面的协作也比较复杂。BP 协议在可靠性和错误检测、时间同步机制、密钥交换、网络管理和监控等方面仍需要改进。

TCPCLP 协议、LTP 协议和 Saratoga 协议为 BP 协议适应各类具体下层网络提供服务。TCPCLP 是基于 TCP 的汇聚层协议，在 DTN 节点间提供面向连接的通信，在该层主要实现了 TCPCL 连接的建立、管理和释放以及束的分片传输。该协议使 BP 协议能够适应大量存在的 TCP/IP 网络。Saratoga 协议与 LTP 协议都是从深空通信的实践中发展而来，在专用链路中效率很高，在使用公共网时有所下降，两者都可以为束层提供可靠传输并支持束分片。区别在于 LTP 协议相对复杂且可运行于 UDP 及其它协议之上，提供的服务比较灵活多样，但需要高层处理命名问题。Saratoga 协议比较简单，可以把数据作为含有文件元数据的命名文件进行传输，仅支持 UDP 或者 UDP 协议的精简版。

3.2 各种路由算法性能分析

路由算法中传染路由设计最为简单且性能优良，但对网络资源要求较高。由于 DTN 中缺乏成熟的拥塞和流量控制机制，过多冗余副本会导致网络性能恶化，需进一步研究受控传染算法，扩大应用范围并使之能适应网络环境的变化。基于概率估计的路由能在不降低路由性能的情况下降低网络资源需求，但部分预测估计方法或先验知识在实际应用中难以实施，需要寻找计算复杂度低且贴近实际的算法。基于模型的路由一般只适用于特定网络环境，在复杂度和性能上居中，应在模型的普适性方面进一步改进。另外，可以通过增加基础设施或编码的方法来改进路由性能。

DTN 路由算法的实现具有较大差异性，不同网络条件下算法性能差别很大，很难简单地评判其优劣性。文献[43,44]对各种路由算法性能做了比较详细的论述。表 1 对本文提到的路由协议在网络资源需求和性能方面进行了比较。由于参数的调整及场景的变化会导致需求及性能有所改变，比较时采用了各协议的典型参数和场景。

表 1 路由协议资源需求及性能比较

网络协议	知识	存储	时延	传输率	复杂度	性能
Epidemic	+	+++	+	+++	+	+++
SWIM	+	+++	+	+++	++	+++
MRP	+	++	++	++	+	++
Spraying	+++	++	++	++	++	++
PROPHET	++	+	++	++	++	+++
CAR	+++	+	++	++	+++	++
MV	++	+	++	++	++	++
SEPR	+++	++	++	+++	++	++
RCM	+++	+	++	+++	+++	+++
ANBR	+++	+	+	+++	+++	+++
SimBet	++	+	++	++	++	++
BUBBLE	++	+	++	+++	+++	++

3.3 组播算法性能分析

DTN 连接频繁断开和长时延特性导致组成员关系在一次会话尚未结束时就会发生变化，难以获得整体网络拓扑知识，组播树不易维持。同时组管理和链路状态信息更新由于缺乏反馈回路而难以进行。现有 DTN 组播算法多采用动态多播树以应对网络的变化，尽量减少对组成员关系及其它网络先验知识的依赖性。

组播算法中，CERM 不需要网络先验知识，复杂度低且性能较好，但对网络资源要求较高，需要进一步研究不同网络环境下控制机制的组合和参数设定，多副本的存在要求大规模应用时网络具备完善的拥塞和流量控制机制。基于概率估计的 EBMR 和 CAMR 组播算法仅需要本地网络知识，对网络资源要求低但复杂度较 CERM 有所增加。EBMR 算法传输时延较小但不适用于节点稀疏的情况。CAMR 算法对节点的密度和移动模式不敏感，但依赖于路由发现机制和对节点的控制，而在 DTN 中由于资源受限和控制回路缺乏而难以实现。基于发布/订阅模式的组播路由能够对本地网络资源进行最优选择并基于内容进行传输，对网络拓扑变化具有鲁棒性；不足之处是传输时延较高，且束格式中缺乏对传输内容的描述，使其适用范围受到局限。所介绍的整合型域间组播算法通过增加基础设施提高多播的效率和范围，具有可扩展性和层次性，但其性能依赖于基础设施；网络规模增加时，大量摆渡节点运动路径难以规划，传输效率和网络性能难以保证。

3.4 安全机制性能分析

安全机制是所有网络协议中的重要部分。但由于网络环境的特殊性，DTN 中安全机制仍处于研究和完善之中。DTN 网络无法把检验工作全部交由接收端和应用层去处理，缺少端到端的控制回路，可靠性实现比较复杂。由于 DTN 网络

资源受限，恶意路由发送伪造束并经其它未知路由节点对其进行复制和传播，对网络造成很大威胁。BP 协议定义的安全模块仅仅是一个框架，其具体实施细则有待研究。汇聚层协议、传输层协议等下层协议也存在不同的可靠性与安全机制，应对这些机制进行优化组合，使其互相协作，以提供安全的网络环境。现有认证及加密方法均假设共享密钥，但密钥的分发和管理仍处于研究阶段。由于 BP 协议中 EID 和地址之间采用后期绑定，为防火墙或准入控制列表的建立带来困难，需要设计适应不同 EID 格式的新的过滤准则。

基于信用的认证方法主要解决认证的长时延问题。通过历史信息和预认证，将认证过程作后台处理，以较小的风险博取更大的收益，在网络状况不佳时大大降低认证时延。BBA 认证方法将多个认证同时处理并加入对伪造签名的检测，减少认证过程的计算量并降低资源消耗和时延。基于身份的加密方法以用户的身份信息作为公钥，私钥由可信的第三方生成，用户间不用交换公私钥，简化了密钥和公共证书的管理，适用于连接频繁断开的网络情况。

结束语 DTN 作为新概念提出以来，其相关领域涌现出大量研究成果，形成了以 BP 协议为基础，采用多种汇聚层协议来适应不同网络和应用的需求，以存储携带转发和保管传输的方式进行通信的网络体系，其路由和组播算法多种多样。本文进行了分析和对比，并讨论了可靠性和安全机制。DTN 尽管已有些成功的应用，但大多为临时性短期试验，仍处于其初期研究阶段并面临许多挑战。

首先是网络协议的复杂度及多样性问题。BP 协议本身比较复杂，部分设计细节仍待完善，且具有多种汇聚层协议并有将汇聚层适配器直接运行于链路层之上等替代方案，导致协议间功能重叠，需要对 DTN 网络协议的功能进行明确界定，对关键实施细则如安全模块、EID 后期绑定及网络管理等进行精确定义，增加协议的适用范围并减少数量，提高其传输效率并有效地实现与因特网的互联互通。

其次是 DTN 路由算法的标准化和实用化问题。尽管已有大量针对 DTN 的单播和组播路由算法，但多数仅适用于特定场景或设施，其路由机制、路由目标差别很大，缺少统一的性能评价体系，仿真环境与具体应用差别较大，应在多种路由算法的基础上提高路由的标准化水平，使路由协议与具体网络环境相分离，增加其适用范围和实用性。

最后是实际应用问题。DTN 技术仍不成熟且应用匮乏，缺少相关设备的支持。许多问题只有在长期大规模的应用和实践中才能发现和解决，因此需要针对 DTN 的潜在应用，增加实用性试验的规模，开发相应的网络设备，在实践中对 DTN 进行逐步完善。

参 考 文 献

[1] Fall K. A Delay-Tolerant Network Architecture for Challenged Internets[C]// Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications. Karlsruhe, Germany: ACM, 2003: 27-34

[2] Cerf V, Burleigh S, Hooke A, et al. Delay-Tolerant Network Architecture[S]. IETF RFC4838. informational, 2007

[3] Scott K, Burleigh S. Bundle Protocol Specification [S]. IETF RFC5050. experimental, 2007

[4] Demmer M. Delay Tolerant Networking TCP Convergence Layer Protocol[Z]. draft-irtf-dtnrg-tcp-clayer-02, 2008

[5] Wood L. Using Saratoga with a Bundle Agent as a Convergence Layer for Delay-Tolerant Networking[Z]. draft-wood-dtnrg-saratoga-05, 2009

[6] Burleigh S, Ramadas M, Farrell S. Licklider Transmission Protocol- Motivation[S]. RFC5325. informational, 2008

[7] Ramadas M, Burleigh S, Farrell S. Licklider Transmission Protocol - Specification[S]. RFC5326. informational, 2008

[8] Farrell S, Ramadas M, Burleigh S. Licklider Transmission Protocol - Security Extensions[S]. RFC5327. informational, 2008

[9] Wood L. Using HTTP for delivery in Delay/Disruption-Tolerant Networks[Z]. draft-wood- dtnrg-http-dtn-delivery-04, 2009

[10] Wood L, Ivancicl W. Use of the delay-tolerant networking bundle protocol from space[C]// 59th International Astronautical Congress. Glasgow, Britain, 2008: 1-11

[11] Lindgren A, Doria A. Networking in the Land of Northern Lights-Two Years of Experiences from DTN System Deployments [C]// Proceedings of the 2008 ACM Workshop on Wireless Networks and Systems for Developing Regions. San Francisco, California, USA: ACM, 2008: 1-7

[12] Balasubramanian A, Mahajan R. Interactive WiFi Connectivity for Moving Vehicles[C]// Proceedings of SIGCOMM'08. Seattle, Washington, USA: ACM, 2008: 427-438

[13] Liu Ting, Christopher M S, Zhang Pei. Implementing software on resource-constrained mobile sensors: experiences with Impala and ZebraNet[C]// Proceedings of the 2nd International Conference on Mobile Systems, Applications, and Services. Boston, USA: ACM, 2004: 256-269

[14] Haas Z J, Small T. A New Networking Model for Biological Applications of Ad Hoc Sensor Networks[J]. IEEE Transactions on Networking, 2006, 14(1): 27-40

[15] Pietilainen A K, Diot C. Experimenting with Real-life Opportunistic Communications using Windows Mobile Devices[C]// International Conference on Emerging Networking Experiments and Technologies. New York, USA: ACM, 2007: 1-2

[16] Wood L, Eddy M, Holidy P. A bundle of problems[C]// IEEE Aerospace Conference. Big Sky, Montana, USA: IEEE, 2009: 1-16

[17] Small T, Haas Z J. Resource and Performace Tradeoffs in Delay-Tolerant Wireless Networks[C]// Proceedings of ACM SIGCOMM'05 Workshop on DTN. Philadelphia, USA: ACM, 2005: 260-267

[18] Nain D, Petigar N, Balakrishnan H. Integrated for messageing application in mobile ad hoc networks[J]. Mobile Networks and Applications, 2004, 9(6): 595-604

[19] Tchakountio F, Ramanathan R. Tracking Highly Mobile Endpoints[C]// Proceedings of the 4th ACM International Workshop on Wireless Mobile Multimedia. Rome, Italy: ACM, 2001: 83-94

[20] Spyropoulos T, Psounis K, Cauligi S, et al. Efficient Routing in Intermittently Connected Mobile Networks: The Single-copy Case[J]. IEEE Transactions on Networking, 2008, 16(1): 63-76

[21] Spyropoulos T, Psounis K, Cauligi S, et al. Efficient Routing in Intermittently Connected Mobile Networks: The Multiple-copy Case [J]. IEEE Transactions on Networking, 2008, 16(1): 77-90

[22] Lindgren A, Doria A, Schelen O. Probabilistic routing in intermittently connected networks[J]. ACM SIGMOBILE Mobile

Computing and Communications Review, 2003, 7(3): 19-20

[23] Li Yun, Li Xin, Liu Qilie, et al. E-PROPHET: A Novel Routing Protocol for Intermittently Connected Wireless Networks[C]// Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing. Leipzig, Germany: ACM, 2009: 452-456

[24] Musolesi M, Mascolo C. CAR: Context-aware Adaptive Routing for Delay-Tolerant Mobile Networks[J]. IEEE Transactions on Mobile Computing, 2009, 8(2): 246-260

[25] Burns B, Brock O, Levine B N. MV Routing and Capacity Building in Disruption Tolerant Networks[C]// 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Miami, Florida, USA: IEEE, 2005: 398-408

[26] Burgess J, Gallagher B, Jensen D, et al. MaxProp: Routing for Vehicle-based Disruption-Tolerant Networks[C]// 25th IEEE International Conference on Computer Communications. Barcelona, Spain: IEEE, 2006: 1-11

[27] Tan Kun, Zhang Qian, Zhu Wenwu. Shortest Path Routing in Partially Connected Ad Hoc Networks[C]// Global Telecommunications Conference, 2003. San Francisco, California, USA: IEEE, 2003: 1038-1042

[28] Liu Cong, Wu Jie. Routing in a cyclic MobiSpace [C]// Proceedings of the 9th ACM International Symposium on Mobile Ad hoc Networking and Computing. Hong Kong, China: ACM, 2008: 351-360

[29] Ding Li, Gu Bo, Hong Xiaoyan, et al. Articulation Node Based Routing in Delay Tolerant Networks[C]// Proceedings of the 2009 IEEE International Conference on Pervasive Computing and Communications. Galveston, Texas, USA: IEEE, 2009: 1-6

[30] Daly E, Haahr M. Social Network Analysis for Routing in Disconnected Delay-Tolerant MANETs[C]// Proceedings of the 8th ACM International Symposium on Mobile Ad hoc Networking and Computing. Montréal, Québec, Canada: ACM, 2007: 32-40

[31] Pan Hui, Crowcroft J, Yoneki E. BUBBLE Rap: Social-based Forwarding in Delay Tolerant Networks[C]// Proceedings of the 9th ACM International Symposium on Mobile Ad hoc Networking and Computing. Hong Kong, China: ACM, 2008: 241-250

[32] Pan Hui, Yoneki E, Shu Y, et al. Distributed community detection in delay tolerant networks[C]// Proceedings of 2nd ACM/IEEE International Workshop on Mobility in the Evolving Internet Architecture. Kyoto, Japan: ACM, 2007: 1-8

[33] Abdulla M, Simon R. Controlled Epidemic Routing for Multicasting in Delay Tolerant Networks[C]// IEEE International Symposium on Modeling, Analysis and Simulation of Computers and Telecommunication Systems. Baltimore, USA: IEEE, 2008: 1-10

[34] Xi Y, Chuah M. Performance Evaluation of an Encountered Based Multicast Scheme for Disruption Tolerant Networks[C]// IEEE International Conference on Mobile Ad Hoc and Sensor Systems. Atlanta, USA: IEEE, 2008: 353-358

[35] Chuah M, Peng Yang. Context-aware Multicast Routing Scheme for Disruption Tolerant Networks[J]. International Journal of Ad Hoc and Ubiquitous Computing, 2009, 4(5): 269-281

[36] Greifenberg J, Kutscher D. Efficient Publish/Subscribe-based Multicast for Opportunistic Networking with Self-organized Resource Utilization[C]// Proceedings of the 22nd International Conference on Advanced Information Networking and Application. Okinawa, Japan: IEEE, 2008: 1708-1714

[37] Peng Yang, Chuah M. Efficient Interdomain Multicast Delivery in Disruption Tolerant Networks[C]// The 4th International Conference on Mobile Ad-hoc and Sensor Networks. Wuhan, China: IEEE, 2008: 81-88

[38] Farrell S, Symington S, Weiss S, et al. Delay-Tolerant Networking Security Overview[Z]. draft-irtf-dtnrg-sec-overview-06, 2009

[39] Wesley M, Eddy M, Wood L, et al. Reliability-only Ciphersuites for the Bundle Protocol[Z]. draft-irtf-dtnrg-bundle- checksum-05, 2009

[40] Shi Minghui, Almotairi K, Shen Xuemin, et al. Credit-based User Authentication for Delay Tolerant Mobile Wireless Networks [C]// International Conference on Communications. Beijing, China: IEEE, 2008: 2752-2756

[41] Zhu Haojin, Lin Xiaodong, Lu Rongxing. BBA: An Efficient Batch Bundle Authentication Scheme for Delay Tolerant Networks [C]// Global Telecommunications Conference. New Orleans, USA: IEEE, 2008: 1-5

[42] Asokan N, Kostiainen K, Ginzboorg P. Applicability of Identity-based Cryptography for Disruption-Tolerant Networking[C]// Proceedings of the 1st International MobiSys Workshop on Mobile Opportunistic Networking. San Juan, Puerto Rico: ACM, 2007: 52-56

[43] Zhang Zhensheng. Routing in intermittently connected mobile AD Hoc networks and delay tolerant networks: overview and challenges[J]. IEEE Communications Surveys & Tutorials, 2006, 8(1): 24-37

[44] Islam A, Waldvogel M. Reality-Check for DTN Routing Algorithms[C] //The 28th International Conference on Distributed Computing Systems Workshops. Washington, USA: IEEE, 2008: 204-209

(上接第 11 页)

[21] Kearns M, Camerer C. Behavior, Computation and Networks in Human Subject Experimentation (WBCN) [C]// Workshop of the GENI Engineering Conference. Del Mar, CA, July 31, August 1, 2008: 31-35

[22] Li Yung-ming, Kao Chien-pang. TREPPS: A Trust-based Recommender System for Peer Production Services[J]. Expert Systems with Applications, 2009, 36: 3263-3277

[23] Tapscott D, Williams A D. Wikinomics: How Mass Collaboration Changes Everything. Expanded edition [M]. Portfolio Hardcover, 2008: 10-13

[24] Flanagan M, Howe D, Nissenbaum H. Values in Design: Theory and Practice[M]// van den Hoven J, Weckert J, eds. Information Technology and Moral Philosophy. Cambridge: Cambridge University Press, 2008: 1-31

[25] Nissenbaum H. Where Computer Security Meets National Security[J]. Ethics and Information Technology, 2005, 7(2): 61-73

[26] Introna L, Nissenbaum H. Shaping the Web: Why the Politics of Search Engines Matters[J]. The Information Society, 2000, 16(3): 1-17