Adv. Network 复习笔记

Part1：MANETs, VANETs, DTNs

要求掌握：

1.Routing and Forwarding Protocols（不同的路由转发协议以及其目标）

（1）Proactive, reactive, greedy/selfish, contacts, intelligent

（2）Different Aims/Objectives

2. Congestion Avoidance and Control（拥塞控制与避免，端到端的网络算法以及其目标）

（1）End to end versus in-network algorithms

（2）Different Aims/Objectives

内容：

1. MANETs（Mobile Ad hoc Networks）

a. MANET ROUTING

定义：

（1）Mobile wireless nodes in MANET create a temporary connection between them to forward data.（MANET 的无线移动节点创建临时连接进行数据转发）

（2）Because some nodes may not be cooperative or may be faulty, they may drop or compromise packets.（有节点不合作或有故障将导致数据包被放弃或者破坏）

（3） Hence routing messages successfully to the end systems is a key concern.（将路有消息成功传递给终端系统是个关键问题）

（4）Typically, routing involves two steps, a route discovery and actual data transmission（路由两个步骤：路由发现以及数据传输）

b.路由协议分类

（1）Reactive（反应式/按需路由）

（1）In reactive or on-demand routing, network nodes only store information of paths to destination nodes.（在反应式或按需路由中，网络节点只存储到目的地节点的路径信息。）

（2）Nodes delay the search for routes to new destinations in order to reduce communication overheads（节点延迟搜索到新目的地的路线，以减少通信开销。）

（2）Proactive（主动路由）

工作原理：

（1）In proactive routing, also known as table driven routing protocol, nodes in the network maintain a comprehensive routing information of the network.

（主动路由：也被称为表驱动路由驱动协议，网络中的节点维护网络的综合路由信息。）

（2）The protocol maintains routing information by spreading network status information to nodes and tracking changes in network topology.（该协议通过向节点传播网络状态信息和跟踪网络拓扑结构的变化来维护路由信息。状况信息给节点，并跟踪网络拓扑结构的变化。）

（3）Hybird Routing protocols（混合路由，结合了主动与被动）

The hybrid routing protocols combine the advantages of proactive and reactive routing protocols to reduce traffic overheads and route discovery delays（混合路由协议结合了主动和被动路由协议的优点，以减少流量开销和路由发现延迟。）

2.VANET(Vehicular Ad Hoc Networks)

1. 定义：

（1）特殊的 MANET，用于车与车（V2V）之间通信，或者车与路边设施通信（V2I）

（2）自组织和分布式网络

（3）Vehicular Ad-hoc Networks provide complementary approach for Intelligent Transport System (ITS)（为智能交通系统提供了方法），

其特点为：

a. high node mobility（高节点流动性）

b.移动模式的自由度有限（limited degree of freedom in the mobility patterns）

2.动机

（1）车辆会改变位置

（2）车辆实时需要信息

（3）提醒司机交通拥堵和事故，以及定位事故位置减少不必要的拥堵等

3.信息的类型（three categories of information）

（1）safety application information

Example: accident

（2）convenience application information

Example: (1)traffic congestion (2) parking availability

（3）pleasure information

Example: (1)games (2) videos, etc

4.VANETs 与 MANETs 的区别

(1)Large scale: all vehicles on the road are potential nodes in the VANET;

(2)Predictive mobility: the nodes in a VANET cannot follow arbitrary direction, they have to stay in the road way and cannot suddenly change their direction;

(3)High mobility: the network mobility in a VANET changes rapidly due to vehicular speeds;

(4)Partitioned Network: the range of wireless communication used in V2V networks is near 1000 meters but vehicles can get disconnected.

（1）大小不同：
VANETs 的规模很大，因为所有路上的车都是 VANET 中的节点。

（2）预测移动性（Predictive mobility）：
VANETs 节点不能跟随任意方向，必须留在道路上，不能突然改变方向（此功能允许设计高度可预测的路由协议。

MANET 假设运动的预测模式较少，并且不容易安排。

（3）高速移动性（high speed mobility）
由于车辆的速度，VANET 中的网络移动性变化很快；这一特点可能导致车辆之间的连接时间很短，在此期间可以实现低 V2V 带宽，从而导致车辆隔离。
相比之下，MANET 流动性低，连接时间长，隔离时间短，节点之间的数据传播机会多。

高速移动性导致的问题：
1. Rapid changes of network topology because the state of connectivity between nodes is dynamically changing;（网络拓扑结构的快速变化，因为节点之间的连接状态是动态变化的）

2. Occasional disconnections due to low traffic density. This keeps the nodes (vehicles) distant from each other and results to link failure that could last for a long while（由于交通密度低，偶尔会断开连接。这使得节点（车辆）之间的距离很远，并导致可能持续很长时间的链接故障。）

3. Node congestion, a high traffic situation which affects protocol performance.(节点拥堵，这是一种影响协议性能的高流量情况。)

（4）分区网络（Partitioned Network）
V2V 网络中使用的无线通信范围接近 1000 米，但车辆可能会被断开连接。
MANET 和 VANET 都可能导致分区，但 VANET 更经常遵循 Accordina 效应，其中拓扑范围在高度拥塞到高度断开之间。

5. WAVE(Wireless access for vehicular environment) IEEE 802.11p

5.1 车的交流方式
A Hop by hop

5.2 WAVE node 的沟通范围
300m- 500m

6 VDTN（Vehicle DTN）

起源：克服 VANET 的通信距离的问题

6.1 VDTN 的应用场景（面对连接问题实现通信）

场景：

（1）漫长多变的延迟
（2）稀疏和间歇性的连接
（3）高错误率
（4）高延迟
（5）高非对称数据率和端到端连接可能不存在地方

原理：

当中间节点变为正在传输的信息的保管者，在有机会时转发信息，网络的通信成为可能。

6.2 断开连接的原因

（1）电池电量
（2）拥堵
（3）连接问题
（4）导致无网络覆盖的流动模式（mobility pattern）和速度
（5）缺乏合作和协作
（6）拓扑密度

6.3 固定的 DTN 节点

（1）The stationary or relay nodes have store and forward capabilities and are located at road-side intersections (Road Side Units).(固定或中继节点具有存储和转发能力，位于路边的交叉口（路侧单元）)

（2）They allow mobile nodes that pass by them to collect and leave data on them(它们允许经过它们的移动节点收集和留下数据。).

（3）They contribute to increasing the frequency of node contacts and message getting to the destination from the source in sparse networks.(在稀疏的网络中，它们有助于提高节点接触的频率和信息从源头到达目的地。)

（4）They improve the performance of the network in terms of delivery ratio and delivery delay.(它们提高了网络在传递率和传递延迟方面的性能。)

7.VANETs 的网络结构类型

7.1 Pure cellular/WLAN(纯蜂窝或 WLAN)

VANET 可以再道路交叉口使用固定的蜂窝网关和 Wimax 接入点来收集信息以便进行路由选择（固定网关可能不可行）

车辆传感器收集到的信息在通知其他有关网络中的交通情况时将变得很有价值

7.2 Pure Ad-hoc

不依赖基础设施节点；节点之间进行车对车（V2V）通信

7.3 Hybird 混合类别

混合类别是蜂窝/无线网络和临时方法的结合。它提供了更丰富的内容，并在内容共享方面提供了极大的灵活性。

一些具有 WLAN 和蜂窝功能的车辆可以被用作网关和移动路由器，这样，只有 WLAN 功能的车辆可以通过多跳链接与它们进行有效的互动和通信，并保持连接。

7.4 应用

7.4.1 安全应用

例子：避免碰撞、事故检测、通知

VANET 中优先级最高，安全信息被高度优先对待

信标安全信息（beacon safety message）：

定义：信标安全信息由车辆定期发布，向通信范围内的其他相邻节点宣布其状态，如速度、方向等。

事件驱动的安全信息(event safety message)：

(1)当检测到迫在眉睫的危险时，就会发送事件驱动信息。

(2)当检测到时，消息会在高度优先的区域内传播。事件驱动信息应该以较高的可靠性和较短的时间传递给节点。

7.4.2 非安全应用

游戏等

8. 专用短程通信（DSRC）

构成：7 个通道（6 个为服务通道 SCH，1 个控制通道 CCH）

安全信息由控制通道提供，非安全信息由服务通道提供。

3.DTN

1. 定义：

MANET 要求源节点到目的节点间存在完整路径，因此无法满足间歇环境下的传输，

DTN 允许节点间歇性和稀疏的连接，以便在具有长延迟和高错误率特征的间歇性环境中转发（路由）信息。

2.DTN Routing Protocols：

a.路由方法：store-carry-forward

（1）messages are stored by nodes and moved in hops throughout the network until messages reach their destination.（消息由节点存储，并在整个网络中逐跳移动，直到消息到达目的地。）
（2）This approach is used by DTN routing protocols to increase the probability of message delivery（DTN 路由协议使用这种方法来增加信息传递的概率。）

b.路由类型：

1.Flooding – based(基于洪流的)

Flooding based routing protocols spread a message and have multiple copes in a network. This is done to increase the probability of messages reaching their destination and also decrease the time of delivery (基于泛洪的路由协议在网络中传播信息并有多种应对方式。这样做是为了增加信息到达目的地的概率，同时减少传递的时间。)

2.Forwarding – based(基于转发的)

Forwarding based routing protocols gather information about the nodes in a network to select the best path to forward messages with the aim of enhancing message delivery in networks with limited resources (基于转发的路由协议收集网络中节点的信息，以选择转发信息的最佳路径，目的是在资源有限的网络中提高信息的传递。)

2.1 直接传输（Direct Transmission）

（1）直接传输是可能的最简单的单副本转发协议。

（2）一旦源生成了一条消息，它将保留并携带它，直到它遇到目的地。

（3）与目的地建立连接后，将直接转发消息。

（4）结果是一个使用最少资源的协议，但是，它也遭受无限量的延迟（延迟等于或大于节点彼此相遇所需的时间）。

（5）同样，传递消息的概率也仅与节点本身遇到目的地的概率一样。

2.2 第一次接触 First contact

(1)First Contact 是一种基于单副本的转发协议，它从所有可能的连接中随机选择一个节点，然后将尽可能多的消息转发到该特定节点。

(2)如果没有可用的连接，则将在第一次联系时进行转移。

(3)传输成功完成后，发送节点删除自己的本地消息副本，放弃对它们的保管。

(4)因此，该协议从根本上通过随机游走模式在整个网络中路由消息。这导致协议遭受与随机游走相关的问题，例如消息；被引入死胡同；在目的地方面取得负面进展；卡在多个节点之间的循环中。

3.Replication based protocols (基于复制的)

（1）基于复制的协议通过消息的复制在整个网络中传播消息。

（2）当一个节点遇到另一个节点时，它可以转发消息的副本，同时仍保留自己的（与基于转发的协议不同，转发节点删除其本地副本）。

（3）消息的多个副本的存在有助于增加消息传递的可能性，同时减少延迟——携带消息的节点越多，一个节点遇到目的地的机会就越高。

（4）与基于转发的协议相比，多副本的主要缺点是也（通常是不必要的）消耗了大量资源，尤其是在缓冲区空间方面。

（5）这通常会因许多冗余的消息副本可能继续存在于网络中这一事实而感到恼火，即使在一个已成功传递到目的地之后也是如此。

3.路由协议

3.1 Epidemic

过程：

(1)Epidemic 是用于传播消息的第一个也是最简单的基于复制的协议之一。

(2)Epidemic 利用泛洪概念，旨在通过使用消息副本泛洪网络来实现消息传递。

(3)当任何两个节点相遇时，它们会比较它们当前持有的消息。然后他们交换他们没有共同点的所有消息的副本。

(4)节点将对其遇到的任何和所有节点重复此操作。因此，消息在整个网络中传播，类似于疾病流行

作用：

这种方法可以潜在地实现最小的延迟，以及非常高的交付概率。然而，Epidemic 没有考虑到，因此深受基于复制的方案导致的资源有限问题的困扰

3.2 MaxProp

定义：

（1）MaxProp 与 Epidemic 一样，遵循泛洪的概念在整个网络中传播消息，但它也为消息缓冲区维护一个有序队列。

（2）该队列是有序的，以便通过转发到达其目的地的概率较高的消息被给予优先级并首先转发。

过程：

（1）为了确定概率，MaxProp 利用遭遇历史，维护一个向量，该向量跟踪节点遇到网络中任何其他节点的可能性。

（2）当两个节点相遇时，它们交换这些向量，然后更新它们自己的本地副本。

（3）最后，这些向量然后用于计算每条消息的最短路径，然后消息在缓冲区内按目标成本排序。

（4）MaxProp 还使用了一些额外的机制来提高性能。这包括在消息到达其目的地时的确认消息。

（5）一旦节点收到确认，该节点将删除其现在冗余消息的本地副本。

3.3 PROPHET

定义：

（1）PRoPHET（使用遭遇和传递历史的概率路由协议）是一个基于复制的协议，它维护一个向量来跟踪遇到的节点的历史，与 MaxProp 的方式非常相似。

（2）PRoPHET 使用此向量来计算消息副本通过转发到特定节点到达其目的地的概率——“训练期”以计算初始概率

过程：

（1）当源节点转发消息副本时，它会选择它可能发送到的节点子集。

（2）然后，该算法根据计算出的概率对这些节点进行排名，副本首先被转发到排名最高的节点。

（3）这种方法是有效的，但是路由表会由于计算概率预测所需的节点信息量而迅速增长。

（4）同样，为了真正有效，该算法还要求该算法还需要一个“训练期”来计算初始概率。

3.4 Spray and Wait

定义：

（1）Spray and Wait 旨在通过对消息可以复制的次数设置上限来控制复制量。

（2）这有助于减少网络内浪费的资源量，同时仍然增加由多个消息副本产生的消息传递的可能性。

两个版本：Vanilla”和“Binary

为实现这一目标而提出的协议的两个版本是“Vanilla”和“Binary”，两个版本都有两个阶段，“Spray”阶段和“Wait”阶段。这些版本的不同之处仅在于它们在喷涂阶段传播信息的方式。

当源节点创建消息时，Spray 阶段开始。一个固定的数字L与消息相关联，它表示网络中可以存在多少个消息副本的上限。

Vanilla 版本：

Vanilla 版本是可用的 Spray 和 Wait 两个版本中较简单的版本。

Spray:

（1）在 Spray 阶段，一个节点会将消息的一份副本转发给L-1 个不同的节点。

（2）每次传输后，节点将其本地副本的副本数量减 1。

（3）一旦副本数达到 1，就进入 Wait 阶段。

Binary 版本：

Spray and Wait 的 Binary 版本与 Vanilla 的不同之处在于节点可以传播的副本数量。

（1）在 Spray 阶段，节点将其消息副本的$\lfloor L/2 \rfloor$传输到接收节点，留下$\lceil L/2 \rceil$副本。

（2）同样，一旦节点剩余一份副本，它将进入等待阶段。

（3）这种行为的优点是消息以更快的速度从源节点传播出去。

Wait:

（1）如前所述，等待阶段发生在节点可能传播的副本数量 L 达到 1 时。

（2）此时，节点只会通过直接传输的方式转发消息，并且会一直携带它直到遇到目的地。

4. Congestion control（拥塞控制）

4.1 定义：

（1）速率控制通过控制网络上的流量速率来缓解网络拥塞

（2）自适应转发将流量从拥塞热点引开

4.2 协议：

a. Spray and Focus

定义：Spray and Focus 由 Spyropoulos 等人提出，旨在克服喷雾和等待中潜在的低效路由。

过程：

（1）Spray and Focus 在喷涂阶段从源复制允许数量的消息。

（2）Focus 阶段允许每个节点将其消息的副本转发到其他潜在节点，直到消息到达其目的地。

（3）该协议使用基于单副本实用程序的路由方案来进一步转发消息的副本。

（4）转发决策是基于记录节点进入彼此通信范围的时间的计时器做出的。

（5）当且仅当节点“B”具有将消息传递给节点“D”的更高潜力时，节点“A”将发往节点“D”的消息转发给另一个节点“B”。

b.SimBet

定义：Daly 等人提出了 SimBet 路由，它使用“中间中心性”和“与目的地的相似性”指标的交换来确定下一跳。

过程：
（1）不知道目的节点的源节点会将消息转发到更中心的节点，该节点有可能找到合适的中继节点。

（2）中央节点可以轻松连接网络中的其他节点。这被称为中心性；衡量网络中节点结构重要性的指标。

（3）中心节点使用相似性和中介中心性来避免整个网络中不必要的信息交换。

（4）SimBet 维护网络中每条消息的单个副本，以减少资源开销。

c. Replication Management
定义：
（1）复制管理是指通过管理复制消息的数量和频率来缓解网络拥塞。

（2）这是一个特别值得注意的问题，因为它通常是消息的复制导致 DTN 内的拥塞，多余和冗余的消息导致节点消息缓冲区内的浪费

d. Café
定义：
（1）Café（拥塞感知转发算法）是一种单副本协议，它利用自适应转发技术，旨在通过将流量从经历拥塞的节点引导到网络中拥塞较少的区域来减少网络拥塞。

（2）它通过使用从社会和资源启发式计算的转发启发式来实现这一点。

（3）Café 的核心架构由两个组件组成：Contact Manager 和 Congestion Manager。

Contact Manager：
联系人管理器专注于转发启发式的节点，更新每个联系人的统计信息，例如频率和持续时间。

Congestion Manager
拥塞管理器专注于计算节点的可用性，保存和更新信息记录，例如可用缓冲区的数量和每个联系节点的预期延迟。

然后，此可用性信息用于为每个消息提供转发启发式的权重，目的是向最可用的节点转发消息。

e. CafREP
定义：
（1）CafRep（拥塞感知转发和复制）是一种基于复制的协议，它建立在 Café 之上，将提出的自适应转发算法与自适应复制管理技术相结合。

（2）与 Café 类似，CafRep 使用社会驱动、资源驱动和区域驱动的启发式方法来应用自适应转发，将消息从拥塞热点传播到网络的较安静部分。

（3）它使用这些指标来计算节点自己的效用，并在接触时将其与遇到的节点的效用进行比较。

（4）基于比较，算法决定是否转发消息，以及多少副本。

f. Autonomous Congestion Control (ACC)
定义：
（1）ACC 是一种基于单副本的转发协议，它通过基于金融模型的缓冲空间建模来实现拥塞控制，将路由器的缓冲空间与银行家可用的资金相关联。

（2）空闲的缓冲空间被视为金钱，传输是金融活动。

（3）节点根据消息的 TTL 选择是否接受消息；节点缓冲占用率和预计增长；传输历史（记录以前的消息使用了多少缓冲区以及使用了多长时间）。

（4）该节点最有可能接受低风险消息，其中 TTL 较低和/或不太可能在很长一段时间内用完许多资源。

g. Density Aware Spray and Wait(DASW)
定义：
（1）DASW（Density Aware Spray and Wait）是 Spray and Wait 的变体，它利用自适应复制来选择消息允许的复制数量，而不是原始固定数量。

（2）这个动态数字是使用从之前的实验（如 RollerNet 实验）预先计算的算盘（preceding）计算出来的。

（3）算盘（preceding）是通过使用平均节点数模拟许多具有不同固定副本数的 Spray 和 Wait 算法来构建的。

（4）对于每次模拟，都会测量要传递的消息的平均延迟。

（5）这在算盘中通过测量 30 秒内的遭遇次数并将其与记录的延迟进行比较以确定最佳副本数来使用。

（6）虽然有效，但以这种方式预先计算算盘意味着它非常依赖于案例，并且可能不适用于通用方法。同样，提案中仅使用了 30 秒窗口，并未考虑使用其他测量周期可能会如何影响性能。

h. RAPID
定义：
RAPID（用于有意 DTN 的资源分配协议）[8] 将转发视为实用程序驱动的资源分配问题。

过程：
它由 4 个阶段组成：

（1）初始化——当两个节点相遇时，它们会在其缓冲区中交换元数据详细信息以及从先前交换中获得的信息；
（2）直接传递——节点将消息发送到遇到的节点。消息按其效用的递减顺序传递；

（3）复制 – 估计每条消息的边际效用，并按此效用的降序复制消息；

（4）终止——一旦连接断开或所有消息都已传递或复制，该过程将终止。

（5）消息的效用是根据预先选择的指标计算的。 RAPID 旨在改进三个选定指标之一：最小化平均延迟；尽量减少错过的最后期限；最小化最大延迟。

i. Priority Scheduling
定义：
（1）已经提出了一种通过优先级来调度消息的方法，该方法从 TCP 中存在的流控制中获得灵感。

（2）他们提出了一个动态捆绑包，它根据遭遇概率对消息进行优先级排序和调度，其中遭遇概率是通过收集和记录过去遭遇的历史来计算的。

（3）所提出的协议的设计还假设它是使用基于人的路由协议来实现和部署的，该协议将负责计算遭遇历史和概率。

j. GeOpps(Geographical Opportunistic Routing for Vehicular Networks)
定义：
GeOpps（车载网络的地理机会路由）是
（1）基于单副本的协议

（2）利用从导航系统收集的数据将数据包路由到特定的地理位置。

（3）选择消息的下一跳作为计算出能够将消息传递到离目的地最近的位置或在最短的时间内传递到目的地的车辆。

（4）每个可能下一跳到目的地的相邻车辆，计算他们将能够传递数据包的最近点。

（5）每个节点使用本地地图和效用函数来计算消息从最近的可交付点到达其目的地所需的最短估计时间。

4.3 Congestion Control in Delay Tolerant Opportunistic Networks

（1）DTN 主要侧重于提高交付到目的地的概率和最大限度地减少延误
a.使用成功但程度有限的复杂图论技术

b.表现出幂律行为，拥有有限的带宽和存储资源

c.导致负载不公平地分配到连接更好的节点和区域

d.可能导致节点和网络范围内的拥塞（RSU、AP）

（2）不清楚如何检测、测量和应对全网拥塞
DTN 中的拥塞控制是一个具有根本挑战性的问题，需要新技术

CAFREP（Congestion Aware Forwarding and Replication）

拥塞感知转发和复制 (CAFREP) 框架：利用本地化的基于相对效用的方法

设法：

（1）检测拥塞的节点和部分网络

（2）远离/减少来自热点的流量并将其传播到周围，同时保持流量的方向性，并且不会用不需要的内容压倒不感兴趣的节点并自适应地改变发送（复制）率

在决定最佳载体和最佳消息数量时，CAFREP 动态结合了三种类型的全分布式实时启发式方法：

（1）联系分析（社交），

（2）预测节点拥塞（节点存储和网络内延迟）和预测性自我网络拥塞（自我网络资源）

Node Congestion Metrics

(1) 节点保持性

旨在避免或在缓冲区可用性较低的节点上按比例减少复制

$$Ret(X) = B_c(X) - \sum_{i=1}^{N} M_{size}^{i}(X)$$

(2) 节点接受度

旨在避免或降低到具有较高网络延迟的节点的发送速率

$$Rec(X) = \sum_{i=1}^{N} (T_{now} - M_{recieved}^{i}(X))$$

(3) 节点拥塞率

旨在避免或降低以较高速率拥塞的节点的发送速率

$$CR(X) = \frac{100 \cdot T_{FullBuffer}(X)/T_{TotalTime}(X)}{1/N \cdot \sum_{i=1}^{N}(T_i end(X) - T_i start(X))}$$

（1）自我网络保持性

旨在避免或减少网络中缓冲区可用性较低的部分的复制

$$EN_{\mathrm{Re}t}(X) = \frac{1}{N}\sum_{i=1}^{N} \mathrm{Re}\,t(c_i(X))$$

（2）自我网络接受度

旨在避免或在延迟较高的网络部分复制较少

$$EN_{\mathrm{Re}c}(X) = \frac{1}{N}\sum_{i=1}^{N} \mathrm{Re}\,c(c_i(X))$$

（3）自我网络拥塞率

旨在避免或减少向拥塞率较高的网络部分发送

$$EN_{CR} = \frac{1}{N}\sum_{1=1}^{N} CR_i(X)$$

storage efficiency

（1）Availability

（2）Congestion Rates

Network Efficiency

（1）Dropped Packets

（2）Congestion Rates

（3）Forwarded Packets

4.4 DTN Security

定义：

（1）受挑战的网络类型，其中交流机会基于零星和断断续续的联系，可能经常发生长时间断开和重新连接，并且丢弃源和目的地之间存在端到端路径的假设

（2）DTN 网络功能对保护 DTN 所需的机制提出了根本性挑战，并严重限制了可用的安全解决方案

4.5 DTN Application(DTN 应用)

定义：最初是作为行星际通信，但现在用于实现通信，当基础架构难以部署、部署成本高或可用时，但 DTN 仍然可以提高性能。

应用：

（1）军事，星际（2）农村地区断开的售货亭（3）受灾地区（4）遥感应用（5）市区海量数据分布（6）共享城市地区的个性化内容（7）移动位置感知传感应用（8）社交移动应用

例子：

1.Inter-Planet Satellite Communication Network 太空互联网服务（DTN 的最初概念）

特征:

（1）高间歇性连接 （2）极长的传播 - 延迟：有限的光速（3）传输可靠性低：定位不准确，能见度有限 （4）低不对称数据速率

安全性：CCSDS 协议（1. space End to end security 2.space end to end reliability）

2. Military Battlefield Network

特征:

（1）高间歇性连接（2）移动、破坏、噪音、攻击、干扰（3）传输可靠性低：定位不准确，能见度有限（4）低数据速率

安全：

（1）主要是 MANET 安全

（2）移动自组织网络中 CA 的分布不能提供军事级别的安全性

（3）将自组织方法与离线第三方可信方 (TTP) 相结合，有希望

3. Remote Area Networks

作用：为农村/发展中地区提供互联网连接，例如电子邮件

特征：（1）间歇性连接 （2）移动性，稀疏部署（3）高传播延迟 （4）非对称数据速率：异构

安全要求：

（1）KioskNet 组件（网关、渡轮、信息亭控制器和代理）的完整性，尽管使用了不受信任的渡轮，但信息亭终端的安全性、用户数据的机密性和完整性

（2）使用的安全性：

标准加密技术，例如 PKI 和透明加密文件系统。

4. Sparse Mobile Ad Hoc Networks（间歇性自主（机会性）通信）

作用：即使基础设施可用，这也为蜂窝网络提供了更便宜的替代方案，例如从没有 3G 的公交车上谷歌

特征：

（1）间歇性连接

（2）移动性，稀疏部署

（3）端到端延迟大

安全性：DTN 或 PSN 安全性

DTN 安全目标：

由于 DTN 的资源稀缺性，DTN 安全的重点是保护 DTN 基础设施免受未经授权的访问和使用， 包含以下：

（1）防止未经授权的应用程序访问，

（2）防止未经授权的应用程序控制 DTN 基础设施，

（3）阻止授权的应用程序以它们缺乏许可的速率或服务等级发送捆绑包，

（4）及时检测并丢弃不是由授权用户发送的捆绑包（在基础设施内而不是在目的地进行早期检测），

（5）及时检测并丢弃标头已修改的捆绑包

（6）迅速检测并禁用受感染的实体

（7）次要重点是为捆绑应用程序提供可选的端到端安全服务

DTN security chanllenges

（1）安全/可靠性
（2）没有可信的基础设施
（3）没有标准 AAA，没有 PKI（公钥基础设施）
（4）没有可用的完全分布式安全算法
（5）新的和不同类别的应用程序流量
（6）支持此类应用程序的网络安全社区所面临的挑战从根本上说是深刻的。
（7）有线、无线和自组织移动网络的传统安全方法假定所有希望通信的端点之间必须（8）存在一条完全连接的路径，才能建立信任

How do DTN environments constrain available trust building mechanisms

（1）高往返时间和断开连接
不允许端到端频繁分发大量证书和加密密钥
在相邻或附近的节点上使用用户的密钥和凭证更具可扩展性。

（2）延迟或丢失与密钥或证书服务器的连接
多个证书颁发机构/密钥服务器可取但不够，证书吊销不合适

（3）长时间延误
消息可能在几天或几周内有效，因此可能无法像在其他类型的网络中那样有效地消除网络中不需要的消息。

（4）受限带宽
需要最小化报头位方面的安全成本

PKI（not applicable for DTNs）

Traditional symmetric cryptography and PKI-based approaches are not suitable for DTNs for two major reasons.

（1）In a PKI, a user authenticates another user's public key using a certificate signed by a certificate authority (CA)
In a disconnected network, without online access to an arbitrary receiver's public key or certificate, sending an encrypted message on the fly is not possible

（2）Also, PKIs implement key revocation based on frequently updated online certificate revocation lists (CRLs) posted by CAs.
In the absence of instant online access to CRLs, a receiver cannot authenticate a sender's certificate.

（3）High round-trip times and disconnections do not allow frequent distribution of a large number of certificates and encryption keys end-to-end

（4）More scaleable to use user's keys and credentials at neighboring or nearby nodes

Identity Based Cryptography（not applicable for DTNs）

基于身份的密码学 (IBC) 方案，其中每个实体的公钥被其身份替换，并且相关的公共格式策略不适合 DTN 中的安全性，原因有两个：
（1）IBC 没有解决 DTN 中的密钥管理问题

（2）它是不可扩展的，因为它假定用户必须知道所有受信任方的公共参数。

Mobile Ad hoc Key Management Proposals （not applicable for DTNs）

（1）虚拟证书颁发机构 – 阈值加密方法。

原因：由于不存在受信任的第三方 (TTP)，因此不适用

（2）基于良好隐私 (PGP) 的证书链

原因：不适用，因为证书图密度不足，受损节点未隔离

（3）基于移动性的对等密钥管理

原因：由于证书撤销机制，不适用

（4）消除所有形式的在线和离线 TTP 会降低安全性。

（5）将自组织方法与离线 TTP 相结合可以提供足够的安全性

Existing Mandatory DTN Security

（1）基于“捆绑”协议

（2）强制保护 DTN 基础设施免遭未经授权的使用 - 尽快检测非法流量并立即丢弃

a.逐跳捆绑标头完整性

b.逐跳捆绑发件人身份验证

c.访问控制（只有具有适当权限的合法应用程序/用户可以注入捆绑包）

d.通过在第一跳检测非法流量并立即丢弃它，对 DoS 提供有限的保护

Existing Optional DTN Security

（1）应用程序数据的可选保护——即使路由器可能受到威胁，目标应用程序也具有安全性

a.端到端捆绑包完整性

b.端到端捆绑源和目标身份验证

c.目的地重放检测

d.支持端到端有效载荷机密性

（2）执行更细粒度的访问控制的能力

DTN Security – Current Issues and Future Efforts

（1）当前的 DTN 安全计划基于预先共享的秘密，不涉及信任动态机制

可以很好地抵御外部威胁，但不适用于内部威胁(即，如果节点受到威胁，则没有机制来重新评估节点的凭据)

（2）DTN 社区最近的努力是针对

a.用新颖的灵活和流动的信任建立、协商和传播机制扩展 DTN 安全捆绑协议(基于行为建模，跨断开异常行为和非共识异步部分信任声明和解决)

b.与 IETF DTN-RG 和 DARPA 的愿景和目标紧密结合

Part2：ICN, CCN (Principles understanding (exam)理解原理)

要求掌握：两个的原理

ICN(Information Centric Networks)

背景：

（1）URL 和 IP 地址因定位器和标识符功能而过载

移动信息 = 更改它的名称 => 404 文件未找到

（2）没有一致的方法来跟踪相同的副本

没有一致的信息表示（与副本无关）

（3）信息传播效率低下

无法从现有副本中受益（例如客户端上的本地副本）

没有 “任播” ：例如，获取 “最近的” 副本

诸如 Flash-Crowd 效应、拒绝服务等问题……

（4）无法信任从不受信任节点收到的副本

安全性以主机为中心

主要基于保护通道（加密）和信任服务器（认证）

（5）应用程序和内容提供商的独立性

CDN 专注于主要参与者的 Web 内容分发

其他应用程序和其他播放器呢？

定义：

（1）除了使用节点直接标识符的路由协议之外，网络还可以直接基于内容进行。

（2）内容可以从网络中采集，在网络中处理，在网络中存储

（3）目标是提供能够提供更适合当今应用需求的服务的网络基础设施：

内容分发和移动性

对中断和故障更具弹性

我们回顾了基于内容的网络和数据聚合机制。

网络演化：

（1）传统网络

以主机为中心的通信寻址端点

（2）以信息为中心的网络

以数据为中心的通信寻址信息（例如，上下文中的数据）。

空间解耦——发送者和接收者都不需要知道他们的伙伴。

及时解耦—— “答案” 不一定直接由 “问题” 触发，异步通信。

（3）方法

（1）命名数据对象 (NDO)
（2）网络内缓存/存储
（3）通过复制进行多方通信
（4）将发送者与接收者分离

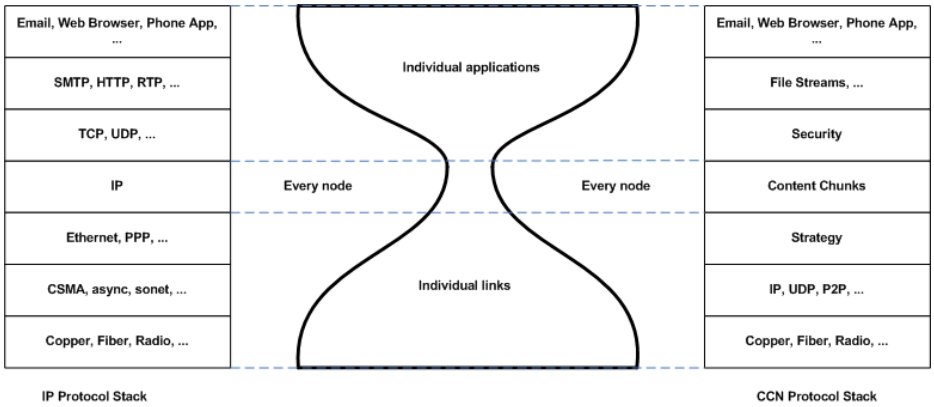
（4）架构问题

（1）我们如何处理信息？
（2）我们如何获取信息？
（3）我们如何路由信息？

（5）传播网络

（1）数据是按名称请求的，使用任何可用的方法（IP、VPN 隧道、多播、代理等）。
（2）任何听到请求并拥有有效数据副本的东西都可以响应。
（3）返回的数据经过签名，并且可以选择保护，因此可以验证其完整性和与名称的关联（以数据为中心的安全性）

（6）ICN Stack



（1）网络抽象从“命名主机”到“命名内容”的变化
（2）内置安全性：保护内容而不是主机
（3）流动性是设计存在的
（4）可以处理静态和动态内容

以内容为中心的网络（Content Centric Networks）

（1）命名：分层命名，单一地址

（2）安全性：签名内容

（3）路由：最长前缀匹配

（4）缓存：基于本地或网络

（5）内容存在知识：不属于 CCN 核心

（6）生产者-消费者会议：利益传播

PSIRP（Publish Subscribe Internet Routing Paradigm）发布订阅互联网路由范式

（1）命名：多级标识符

（2）安全性：签名内容

（3）路由：（1）名称解析（2）信息传递

（4）缓存：基于网络

（5）内容存在知识：Rendezvous 系统中的注册

（6）生产者-消费者会议：集合点系统提供位置

Naming：

解决方案 1：命名数据

（1）扁平的，非人类可读的标识符

（2）分层的、有意义的结构化名称

解决方案 2：描述数据

（1）带有一组标签

（2）使用定义属性、值和属性之间关系的模式

Using Names in CCN

（1）层次结构用于进行“最长匹配”查找（类似于 IP 前缀查找），这有助于保证全局可访问数据的 log(n) 状态缩放。

（2）尽管 CCN 名称比 IP 标识符长，但它们的显式结构允许查找与 IP 一样高效。

Basic ICN forwarding

（1）消费者通过任何和所有可用的通信媒体“广播” “兴趣”

（2）兴趣标识数据的集合——所有以兴趣为前缀的数据项。

（3）任何听到兴趣并具有集合元素的东西都可以用该数据进行响应

Basic ICN transport

（1）与兴趣相匹配的数据会“消耗”它。

（2）必须重新表达兴趣才能获得新数据。（控制重新表达允许交通管理和环境适应。）

（3）可以表示同一集合中的多个（不同）兴趣（类似于 TCP 窗口）。

ICN Caching

（1）存储和缓存是 ICN 服务的组成部分。

（2）所有节点都可能有缓存；任何在缓存中保存副本的节点都可以满足对数据的请求。

（3）ICN 将网络边缘的缓存与 P2P 和其他覆盖网络中的缓存与网络内缓存（例如，透明 Web 缓存）相结合

ICN Advantages

可扩展且具有成本效益的内容分发

ICN Issue

（1）可扩展性

（2）隐私（兴趣订阅和内容描述）

（3）合法（缓存中毒）

（4）部署业务案例

CCN(Content-Centric Networks)

1 背景：

第一代：电话系统（专注于电线）
第 2 代：互联网（专注于端点）
第 3 代：传播（关注数据）

2. Structural problems with phone systems（电话系统的结构性问题）

（1）路径建设是非本地的，鼓励集中和垄断

（2）如果路径中的任何元素发生故障，调用就会失败，因此随着系统扩展，可靠性会呈指数下降

（3）在设置路径之前数据无法流动，因此当设置时间或带宽增加时效率会降低

3. packet switching（分组交换）

（1）更改点视图以关注端点而不是路径

（2）数据以独立的块发送，每个块包含最终目的地的名称

（3）（传递性）如果节点获得一个不同目的地的块，尝试使用静态配置或分布式路由计算转发它

4. ARPAnet

定义：

（1）ARPAnet 建立在现有电话系统之上

（2）它需要廉价、无处不在的电线

（3）它需要数字信号技术（但不是最先进的技术）

5. TCP/IP 的问题

（1）“已连接”是一个二元属性：您要么是互联网的一部分，可以与所有事物交谈，要么您是孤立的。

（2）成为互联网的一部分需要一个全球唯一、全球知名的 IP 地址，该地址在路由时间尺度（几分钟到几小时）上拓扑稳定。

a.连接是一项重量级的操作

b.网络不喜欢移动的东西

6. Dissemination networking（传播网络）

（1）数据是按名称请求的，使用任何可用的方法（IP、VPN 隧道、多播、代理等）。

（2）任何听到请求并拥有有效数据副本的东西都可以响应。

（3）返回的数据经过签名，并且可以选择保护，因此可以验证其完整性和与名称的关联（以数据为中心的安全性）

7. goals of CCN(Content Centric Networking (CCN))

（1）创建一个简单、通用、灵活的通信架构：

a.匹配当今的沟通问题

b.匹配当今的应用程序设计模式

c.至少与 TCP/IP 一样可扩展和高效

d.更安全

e.需要更少的配置

8.difference of IP and CCN

（1）任何在任何东西上运行的架构都是覆盖（IP 是覆盖）。

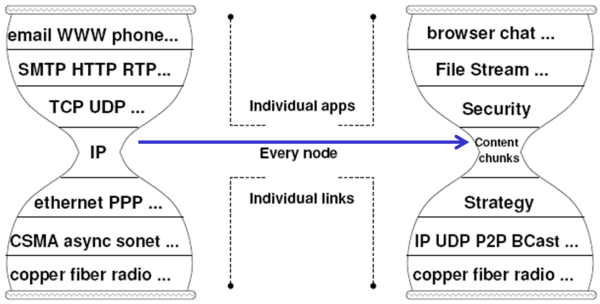
（2）IP 作为电话系统覆盖开始；今天，大部分电话系统都是 IP 覆盖。系统理论家会说“IP 是普遍的”。

（3）CCN 具有相同的特性：它可以在任何东西上运行，包括 IP，并且任何东西都可以在 CCN 上运行，包括 IP。

（4）并且 CCN 与较低层的关系比 IP 更简单、更普遍。

9. IP 到“命名内容块”（IP to “chunks of named content”）

策略：利用多个同时连接进行数据传输（例如，以太网、3G、WiFi），因为它与第 2 层的关系更简单， 左侧为 Current Internet， 右侧为 CCN



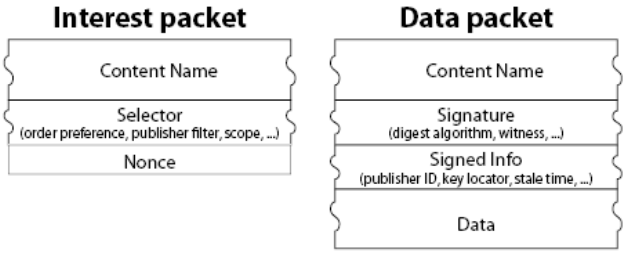
10. CCN packets

两种类型（two packet types）：

（1） Interest -- similar to http “get” and

（2）Data -- similar to http response.

Data packet is **authenticated** with **digital signature**



11. Basic CCN forwarding

（1）消费者通过任何和所有可用的通信媒体“广播” “兴趣”：

（2）兴趣标识数据的集合——所有以兴趣为前缀的数据项。

（3）任何听到兴趣并具有集合元素的内容都可以使用该数据进行响应：

12. CCN Name

在内部，CCN 名称是不透明的结构化字节字符串

表现形式：

（1）is represented as a component count

（2）for each component, a byte count followed by that many bytes:

与 IP 异同：

（1）层次结构用于进行“最长匹配”查找（类似于 IP 前缀查找），这有助于保证对全局可访问数据进行扩展。

（2）尽管 CCN 名称比 IP 标识符长，但它们的显式结构允许查找与 IP 一样高效。

（3）与 IP 一样，CCN 节点对名称没有任何语义。

（4）含义来自前缀转发规则中反映的应用程序、机构和全局约定。例如，

（5）前者是利用 DNS 全局命名结构的具有全局意义的名称。

（6）后者是本地和上下文相关的——它根据你所在的房间引用不同的对象。

13. Strategy layer(mobility management)

（1）当你不在乎与谁交谈时，你不在乎他们是否改变。

（2）当您没有对话时，没有要迁移的对话状态。

（3）多点免费为您提供多界面。

（4）当所有通信都在本地流平衡时，您的堆栈确切地知道什么在工作以及有多好。

14. Quality of Service (QoS)

（1）在当前的互联网中，QoS 问题高度局部化。

（2）大约一半的问题来自队列创建的串行依赖关系。

（3）另一半是由于缺乏基于接收器的瓶颈链路控制造成的。

（4）与 IP 不同，CCN 是本地的，没有队列，接收者具有完整的、细粒度的控制。

15. Wrap-up

（1）CCN 节点就像一个 IP 节点一样简单：

相同的内存要求

相同的计算要求（可选择提高安全性）

（2）CCN 提供简单、强大、安全的单点配置。

（3）CCN 确实接近最佳的内容分发。

（4）网络、应用程序和用户都共享相同的通信模型。

Part3: TCP/IP, DNS, BGP, Applications

要求掌握：

1. TCP/IP, DNS, BGP

2. Understanding of Non-DNS based addressing and services （基于非 DNS 的寻址与服务）

Connecting

1. Internet Quality of Service

定义：

（1）当容量<需求时你会怎么做？

如果容量 > 需求，则不需要 QoS

（2）希望尽量减少排队

由于排队直接影响延迟、抖动、丢失

至少，在稳定的网络中（参见动态路由）

（1）Elastic vs Inelastic Traffic 弹性与非弹性流量

a.资源管理

供应：路径上的可用链路容量

需求：主机传输和接收流量

b.TCP 根据观察到的丢失和延迟来管理资源使用情况

弹性：产能减少 -> 需求缩减

非弹性应用程序无法处理此问题

（2）Type of Service, ToS（服务类型，服务条款）

（1）单个 IP 头字节

（2）优先级

对于“特殊”流量

（3）服务等级

如何对待流量

（4）但他们是什么意思？！

到网络？

申请？

（3）Differentiated Services, DiffServ（差异化服务，DiffServ）

（1）对流量聚合进行操作

（1）通过 ToS 将数据包标记为所需的服务类别

（2）路由器在操作员认为合适的情况下应用排队

（2）四种服务类别或每跳行为

（1）默认值：尽力而为

（2）加速转发：低延迟、丢失、抖动

（3）保证转发：在速率范围内的低损失

（4）类选择器：使用 ToS 优先位

问题：

a.端到端语义

b.映射到服务水平协议

c.映射到应用需求

（4）Integrated Services, IntServ（综合服务，IntServ）

在许多方面与 ATM 非常相似

a.对显式信号流进行操作

b.流设置指定一些 QoS

c.路由器执行连接准入控制

问题：

a. 复杂

b. 将要求映射到参数，参见。自动柜员机

c. 每流状态

2.Network Address Translation

2.1Address Shortages

（1）IPv4 supports 32 bit addresses

（2）IPv6 supports 128 bit addresses

2.2Implementation

（1）需要 IP、TCP/UDP 报头重写

（1）地址、端口、校验和至少

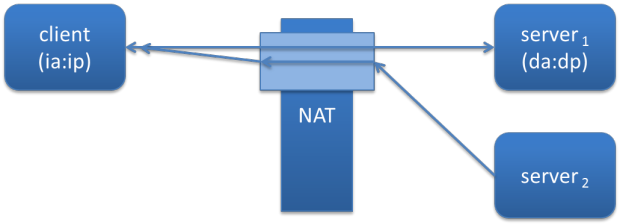
（2）行为

（1）网络地址解读

（2）网络地址和端口转换

（3）类型

（1）全锥（Full Cone）



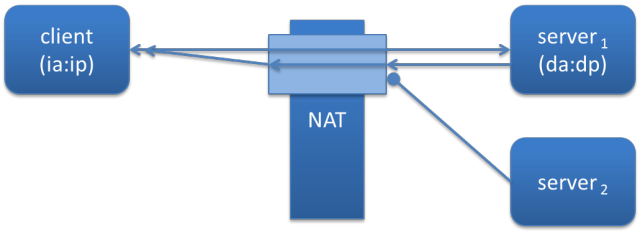
ia:ip → da:dp

(ia:ip → ea:ep) → da:dp

(da:* → ea:ep) → ia:ip

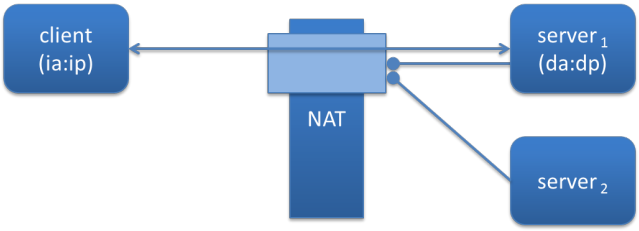
(da':* → ea:ep) → ia:ip

（2）地址/端口限制锥（Address/Port Restricted Cone）



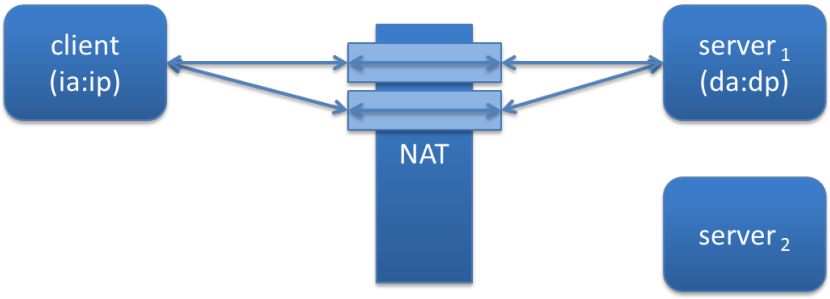
a.Address Restricted Cone
ia:ip → da:dp
(ia:ip → ea:ep) → da:dp
(da:* → ea:ep) → ia:ip
(da':* → ea:ep) → DROP

b. Port Restricted Cone



ia:ip → da:dp
(ia:ip → ea:ep) → da:dp
(da:dp → ea:ep) → ia:ip
(da:dp' → ea:ep) → DROP
(da':* → ea:ep) → DROP

（3）对称的（Symmetric）



ia:ip → da:dp
(ia:ip → ea:ep) → da:dp
(da:dp → ea:ep) → ia:ip
(ia:ip → ea':ep') → da:dp
(da:dp → ea':ep') → ia:ip

2.3 NAT Traversal

3.End-to-End

Naming

1.Naming

定义：

（1）IP 地址都很好，但是...

（2）不是特别可读（尤其是 IPv6）

（3）并不总是合适的粒度

a.地址命名一个接口

b.我们可能想要命名一个服务器、一个服务、一个站点

c.我们可能有动态地址分配

1.1HOSTS

（1）将名称映射到数字的文件

（2）导致域名服务，DNS

1.2DNS

（1）一致的命名空间

不提及地址、路线等。

（2）主要特征

a.分层、分布式、缓存

b.对于规模 [但这仍然适用吗？

c.联合 - 源控制权衡

d.灵活——多种记录类型

e.简单的客户端-服务器名称解析协议

（3）Components

a.域名空间和资源记录

树形结构的名称空间

与姓名相关的数据

b.名称服务器

包含子树的记录

可以缓存有关树的任何部分的信息

c.解析器

根据客户请求从树中提取信息

获取主机名（）

2.DNS outline

2.1 DNS 层次结构(DNS Hierarchy)

定义：

（1）根：http://root-servers.org/

美国商务部 NTIA 的最终权威，由 IANA 管理，由 ICANN 运营，由 Verisign 维护

十三个根服务器集群

（2）顶级域名、TLD

由 ICANN 授权的注册商运营

（3）将区域委托给其他注册商

...在层次结构中

（4）最终客户租用一个名字——他们的区域

a.Registrar 安装适当的资源记录

b.与区域内的名称相关联

2.2 Query(问询)

（1）解析器生成的查询

例如，调用 gethostbyname()、gethostbyaddr()

（2）在单个 UDP/53 数据包中携带

或者更罕见的是 TCP/53，以防截断

（3）标题后跟问题

a.Id、Q/R、操作码、AA/TC/RD/RA、响应码、计数

b.查询类型、查询类、查询名称

2.3 Response

响应由标题和问题后面的三个 RRsets 组成:

答案：服务器为 QNAME 拥有的 RR

Authoritatives: RRs 指向名字的权威

补充：与问题相关但未回答的 RR

2.4 DNS 名称解析：递归与迭代（DNS name resolution: Recursive vs Iterative）

1.当解析器查询一个不知道答案的服务器时会发生什么?

答案：DNS 服务器本身不知道答案时，就会发生递归 DNS 查询，因此必须与另一台服务器进行检查。

Iterative (required)

Server responds indicating who to ask next

Recursive (optional)

Server generates a new query to the next server

2.5 Operational & Security Issues（操作和安全问题）

（1）通常需要主备服务器

独立的 IP 网络块、物理网络等。
DNS 是一种非常常见的单点故障

（2）缓存中毒

缓存和软状态意味着不良数据会传播并可以持续一段时间
即使通过一个简单的错误

（3）中间人攻击

迭代/递归查询几乎需要这个

2.6 总结

（1）DNS 是一个分布式分层数据库
（2）支持将名称解析为资源记录中表示的属性
（3）一系列技术细节/技巧
    a.递归/迭代分辨率
    b.标签压缩
    c.负载均衡

3.DNS protocol

4.DNS details

Reliability

1.Recap

（1）拥塞控制和流量控制
（2）基于定时器的自适应传输窗口
（3）TCP 通过回退来对丢失做出反应
    a.假设丢失是由网络拥塞引起的
    b.TCP 通过探测更多带宽来对成功交付做出反应

2. Achieving Reliability

（1）Retransmit lost data（重传丢失的数据）
（2）By explicit acknowledgments（明确的确认（positive or negative））

3. 可靠性和性能（Reliability and Performance）

（1）速率控制：永远不要为网络发送太快

如何估算合适的费率？

（2）滑动窗口：允许未确认的数据在飞行中

如何确定正确的窗口大小？

（3）重传超时

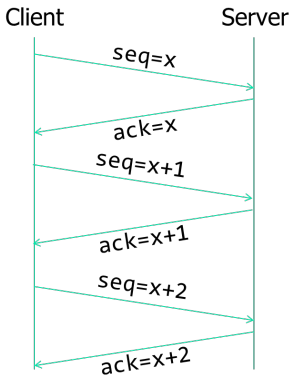
等待多长时间才能决定丢失一个段？

（4）需要估计动态量

4. Stop ‘n’ Wait

4.1 最简单的可能性

（1）发送 seq(x)
（2）等待确认 ack(x)
（3）发送 seq(x+1)

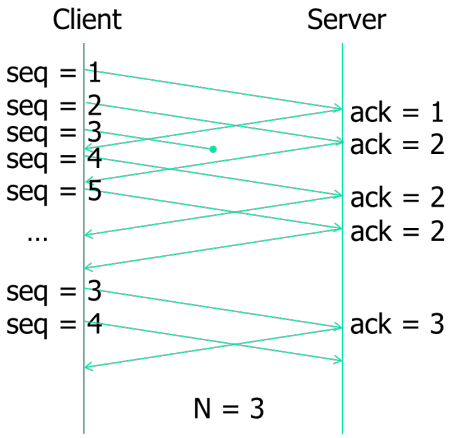


4.2 在高延迟高带宽网络中的性能真的很差

5. First Attempt

5.1 步骤：

（1）允许 N 段飞行
（2）超时意味着损失
（3）从丢失的数据包开始重新传输
（4）损失浪费吞吐量



6.拥塞崩溃（Congestion Collapse）

6.1 现象

网络负载过高导致拥塞崩溃（最初在 NSFNet 1986 年 10 月观察到）

6.2 原因

路由器缓冲区填满，流量被丢弃，主机重新传输
但是早期的 TCP (4.2BSD) 太天真了！由于数据丢失，重新传输更多……轰！

6.3 解决方案

由 Van Jacobson 在 ACM SIGCOMM'88 中解决“拥塞避免与控制”经典的计算机科学论文之一

7.网络稳定性（Stability of the Internet）

定义：互联网稳定性的一个关键点是流和协议包括某种拥塞控制和适应，以便它们调节带宽使用、限制数据包丢失以及获得大约公平的可用网络带宽份额。

（1）响应性定义为将速率降低一半所需的持续拥塞的往返次数。

（2）稳定性和平滑度定义为在稳态场景下一次往返时间内发送速率的最大降低。

（3）竞争带宽时对其他流的公平性。

（4）为多媒体拥塞控制模拟 TCP 行为会导致对 TCP 的公平性，但也会导致带宽非常显着的波动。

（5）与 TCP 相比，多媒体流应用程序需要在吞吐量方面具有低得多的变化，以产生相对平滑的发送速率，这对最终用户感知质量很重要。

（6）在争夺带宽的同时具有比 TCP 更平滑的吞吐量的代价是多媒体拥塞控制对可用带宽变化的响应比 TCP 慢。

（7）因此，如果多媒体流量想要平滑的吞吐量，就需要避免 TCP 响应单个丢包而将发送速率减半。

8.丢包（packet loss）

（1）在选择丢包检测方法时，重要的是要选择一种能够尽早、尽可能准确地检测到丢包的方法。对未能传送数据包或延迟数据包传送的错误检测会导致不正确的数据包丢失估计、较差的速率适配，从而导致无响应和不公平的行为。

（2）可以在不同长度的测量间隔上计算丢包率。一般来说，更短的间隔会导致更响应的行为，但它们更容易受到丢包信号中的噪声的影响。更长的时间间隔导致更平滑的丢包信号，但响应行为更慢。
重要的是，间隔在对噪声的弹性和对网络条件的实际变化的快速响应之间取得合理的平衡。

（3）为了保证对拥塞有足够的响应并保持平滑，必须仔细选择检测和计算丢包的方法。
问题 需要回答的包括：

a) 可以使用什么机制进行丢包检测？

类似于 TCP 的基于超时的机制来检测数据包丢失。

过程：

（1）所有发送的数据包都标有连续的序列号。

（2）当发送数据包时，会计算该数据包的超时值，并将包含序列号和超时值的条目插入到列表中并保持在那里，直到确认数据包传递或超时到期。

（3）如果在数据包被确认之前超时超时，则认为相应的数据包丢失。

b) 丢包率计算可以使用什么算法？

为了适应变化和不可预知的网络条件，超时不是固定的，而是基于 TCP 超时计算的算法之一进行计算

c) 丢包检测和计算在哪里发生？

丢包检测可以发生在接收端或发送端：

（1）发送方：

如果在发送端进行了丢包检测，发送端可以对每个数据包使用超时机制或确认数据包的序号间隔。

a. 接收方必须确认收到的每个数据包或未收到的数据包。
b. 确认每个数据包可以在发送者和接收者之间的给定链路上引入高水平的流量。
c. 这通常通过让接收器报告每个第 n 个数据包或第 n 个 RTT 的丢失或确认摘要来解决。

（2）接收方：

接收方：在接收方检测到数据包丢失并明确报告给发送方。

a. 注意到接收方接收到的数据包的序列号有间隙，可以假设发生了丢失事件。
b. 这种事件的发生直接转发给发送者。

发送方与接收方丢包检测:

（1）在选择丢包检测方法时，重要的是要选择一种能够尽早检测到丢包事件并能保证对拥塞有足够响应能力的方法。

（2）因此，接收者驱动的丢包发现可能优于发送者驱动的丢失发现。

（3）然而，在非常严重的拥塞情况下，在没有来自接收方的所有反馈（即确认和接收方报告）的情况下，纯基于接收方的丢失检测是无用的，因为发送方无法计算数据包丢失并调整发送率。在这些情况下，发送者应该进入自我限制，即假设丢包并降低甚至停止发送速率。

8.2 基于超时的方法（Timeout Based Approaches）

过程：

（1）在确认第一个数据包并进行 RTT 测量之前，发送方将 TIMEOUT 设置为某个初始值。

A.对于 TCP，此值通常为 2.5 – 3 秒。

B.对于实时交互式多媒体流量，超时值应设置为交互式会议的可容忍延迟大约为 0.5 秒（如 [Brady, P., 1971] 建议的）。

（2）当进行第一次 RTT 测量时，发送方按以下方式设置平滑 RTT (SRTT)、RTT 方差 (RTTVAR) 和 TIMEOUT：

- $SRTT = RTT$

- *RTTVAR = RTT/2*
- *TIMEOUT = Mu*SRTT + 4*RTTVAR,*

其中 Mu 是一个常数，在此实现中为 1.08（经过大量实验确定）。

（3）进行后续 RTT 测量时，发送方按以下方式设置 RTTVAR、SRTT、TIMEOUT：

- *RTTVAR = (1 – ¼) * RTTVAR + ¼ * |SRTT – RTT|*
- *SRTT = (1 – 1/8)* SRTT + 1/8 * RTT*
- *TIMEOUT =Mu*SRTT + 4*RTTVAR*

8.4 Adaptation

一旦测量给定链路的参数（数据包丢失和往返时间），在选择速率适配方案时可以遵循一系列方法。

这些方法可以分为：

（1）基于方程的控制使用一个控制方程，该方程明确给出了作为最近丢失事件率（丢失率）的函数的最大可接受发送速率。

例如。 TCP 响应函数将 TCP 的稳态发送速率表征为往返时间和稳态丢失事件率的函数

（2）响应于单个拥塞指示的加性增加乘性减少 (AIMD) 控制。

问题：处理任何适应机制时必须解决的三个问题：

（1）决策功能，

a. 决策功能的选项：

b.在拥塞（过载/丢包/丢包增加）时，立即或定期降低速率

c.在没有拥塞的情况下（欠载/无丢包，丢包减少），立即提高速率

（2）增加/减少算法

Increase Phase（增加阶段的选项：（在欠载期间））：

a.恒定的添加剂增长率，

b.直接跳转到期望值或公式计算的值

c.倍增率

Internet 的默认值是恒定线性增加。

有人可能会争辩说，丢失估计为零表明没有拥塞，因此应该以最大可能的增加因子增加发送速率，直到发生丢失事件。
然而，这种方法会导致发送速率不稳定，并且非常容易受到噪声丢包率的影响。

Decrease Phase（在拥塞期间，减少因子可以是：）：

a.常数乘法减小因子，类似 TCP 或类似 TCP。

b.线性减少

c.直接跳转到期望值（通过公式计算）

Internet 的默认值是乘法减少，即减半。
减少是乘法的，因为拥塞恢复应该是指数的而不是线性的。

（3）决策频率 Decision Frequency
a.决策频率指定更改速率的频率。基于系统控制理论，最优调整频率取决于反馈延迟。反馈延迟是从改变速率到检测到网络对该变化的反应之间的时间。

b.建议基于方程的方案在每个 RTT 中调整其速率不超过一次。过于频繁地改变速率会导致振荡，而不频繁地改变速率会导致反应迟钝。

c.由于 RTT 信号的随机性，使用最后测量的样本 RTT 可能会导致不良行为。
我们需要一个表示 RTT 低频变化并滤除瞬态（即高频）变化的 RTT 平滑版本。

8.5 Congestion Control
过程：
（1）需要确定当前参数
大多数 TCP 的窗口大小

（2）加法增加，乘法减少

8.5.1 TCP Tahoe
目标：遵守数据包守恒
（1）在平衡状态（运输中的全窗口），流量是保守的
（2）新数据包在旧数据包离开之前不会进入

失败的三种方式
（1）连接未达到平衡
（2）发件人发送太快
（3）资源限制阻止达到平衡

通过多种技术修复：
（1）RTT 方差估计；
（2）慢启动；拥塞避免和恢复

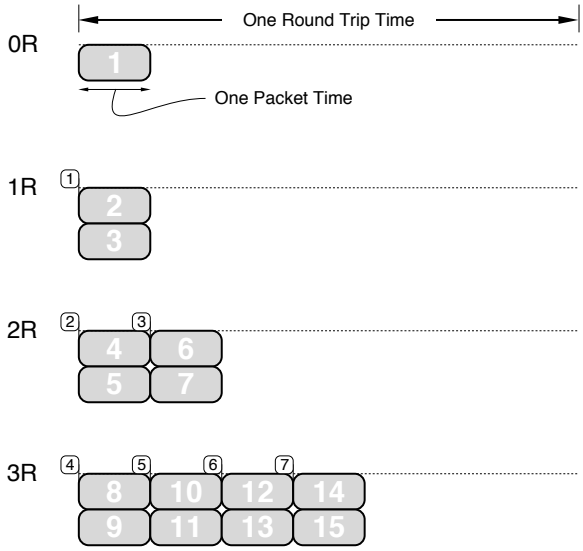
8.6 Self-Clocking
（1）目标是传输间隔匹配瓶颈率
a. 避免瓶颈处的一致排队
b. 排队以消除短期变化

8.7 Slow-Start
（1）每个 ACK 打开拥塞窗口 1 个数据包
a.每个 ACK，cwnd = 1, cwnd *= 2 每个 RTT

（2）停止

a.当损失发生时，或 cwnd == ssthresh

b.乘法增加



8.8 Congestion Avoidance（拥堵避免）

两个组件：

（1）网络信号发生拥塞

检测丢失

（2）主机通过降低发送速率来响应

ssthresh := cwnd/2 /* 乘法递减 */

cwnd := 1 /* 启动慢启动 */

（3）通过缓慢增加避免拥堵

cwnd = 1/cwnd /* 窗口每个窗口增加 1 */

8.9 Multimedia

（1）TCP 并不总是有用的

可靠性可能导致交货不及时

（2）音频/视频编解码器通常会产生帧

不是连续的字节流

（3）丢失一帧可能比延迟所有后续数据更好（考虑图形和视频与交互式音频）

9 Real Time Protocol

（1）RFC 1889 / RFC 3550

（2）通过 UDP 封装媒体

排序，时间戳，交付监控

没有可靠性，没有 QoS

（3）添加控制通道 (RTCP)
用于报告统计数据、参与者等的反向渠道

（4）仅运输
将编码、楼层控制等留给应用程序

（5）可扩展

10. TCP 友好性（TCP Friendliness）

（1）以给定速率发送的实时媒体
可能导致 TCP 经历丢失和退避
媒体终将获胜

（2）需要适应实时媒体
a.基于方程的单流拥塞控制
b.基于方程和 AIMD 的多流拥塞控制（分布式部分混合（DPM））

Internetworking

1.Routing and Forwarding

（1）路由器收到 IP 包：怎么办？
通过接口丢弃或转发

（2）决定转发哪个接口
IP 仅根据目标 IP 地址做出此决定（几乎）

（3）为此建立信息是路由
目前所有的地址在哪里？

2.路由

2.1 域间路由

a. 路由协议

（1）分发数据以构建转发表

（2）我们看到的例子：OSPF
链接状态，距离向量

（3）这些是域内路由协议
或内部网关协议
同一网络内的源和目标

（4）网络之间会发生什么？

b. Inter-domain Routing

（1）一个重要的区别：本地与全球
内部与外部网关协议（IGP、EGP）
为什么这很重要？两个原因：

（2）动力学
需要确定信息传播范围（为什么？）

（3）保护
需要隐藏信息（为什么？）

2.2 BGPv4（Border Gateway Protocol, BGPv4）

（1）Internet 域间路由协议

RFC 4271，更新 RFC 1771
最初源自 GGP、EGP (1982)
随时间更新（RFC 1105、1163、1267）

（2）处理 IP 前缀和自治系统

ASs 纯粹的行政管理
目的是使政策得以应用
只有前缀在数据平面中很重要

2.3 自治系统（Autonomous Systems, ASs）

3.协议 Sessions；Updates；Path Attributes

3.1simple protocol

（1）交换前缀

a.使用 TCP/179 作为传输
b.开放、更新、保持活动、通知

（2）对等体之间的会话

a.简单的能力协商
b.管理同时打开
c.在会话失败时丢失所有内容（为什么？）

3.2 Sessions & Routing Information Base (RIBs)（会话和路由信息库 (RIB)）

（1）BGP 对等体通常有很多会话
10？ 20？ 100 s？

（2）从逻辑上讲，每个会话的 Adj-RIB-In & -Out
收到和发送的广告

（3）从 Adj-RIB-In 生成 Loc-RIB
a.使用和可能分发的路线
b.解析为每个端口的转发表

（4）从 Loc-RIB 和策略生成 Adj-RIB-Out

3.3 Updates

（1）增量 - 指示状态更改
a.撤回的路线
b.路径属性，所有通告的路由共有
c.广告路线，称为 NLRI

（2）定义了约 27 个路径属性
a.也许有十几个是常用的
b.传达有关前缀的信息
c.用于在 BGP 决策过程中应用策略

4.决策过程

4.1 Path Vectors – AS_PATH（路径向量）

（1）距离向量——首选成本最低的路径
需要以某种方式打破循环（如何？）

（2）路径向量
我们怎么知道我们以前是否看过这个广告？
存储它通过它到达我们的 AS 列表
AS_PATH

（3）循环可以被打破：
如果我们的 ASN 出现在收到的 AS_PATH 中，则删除广告

4.2 在以下情况下删除前缀：

（1）NEXT_HOP 无法通过本地路由表访问
（2）本地 AS 出现在 AS_PATH

5.操作

5.1 Consistency（一致性）

（1）了解 EBGP 会话的外部路由
EBGP 定义为具有不同 ASN 的对等体
必须确保每个路由器都知道所有外部路由（为什么？）

（2）在网络内重新分配外部路由
通过 IGP——仅在小型网络中（为什么？）
通过 IBGP – 完全控制路由分配

（3）IBGP 有什么问题？

5.2 Scaling（缩放）

（1）无法在 IBGP 会话上分发 IBGP 路由

为什么？

（2）必须维护 N.(N-1)/2 个 IBGP 会话
每个携带多达 49 万条路线 x 2 Table

（3）两种标准方法
路由反射器：
a.超级节点
b.读取 IBGP 路由

AS Confederations：
a.将 AS 拆分为 mini-AS
b.两者都在一定程度上调整了决策过程

5.3 Operation

（1）处理链路故障
a.绑定到环回
b.襟翼阻尼（但会使事情变得更糟！）

（2）进程失败
由于路由过多导致内存不足错误

（3）劫持，有意无意

（4）任播（1:1-of-N）
在许多地方宣传相同的前缀。小心。

5.4 Network Interconnection（网络互联）

（1）网络通过 EBGP 会话互连
持久性有机污染物，存在点；或 IX，互联网交换

（2）多宿主
这都是合乎逻辑的——物理多样性呢？

（3）这一切如何结合在一起？
a.公共/私有对等互连与传输
b.大致分层（尽管这种情况正在改变）
c.第 1 层/核心/骨干与其他(Tier-1/core/backbone vs the rest)

（4）一如既往，商业和政治
例如，Level3 vs Cogent depeering