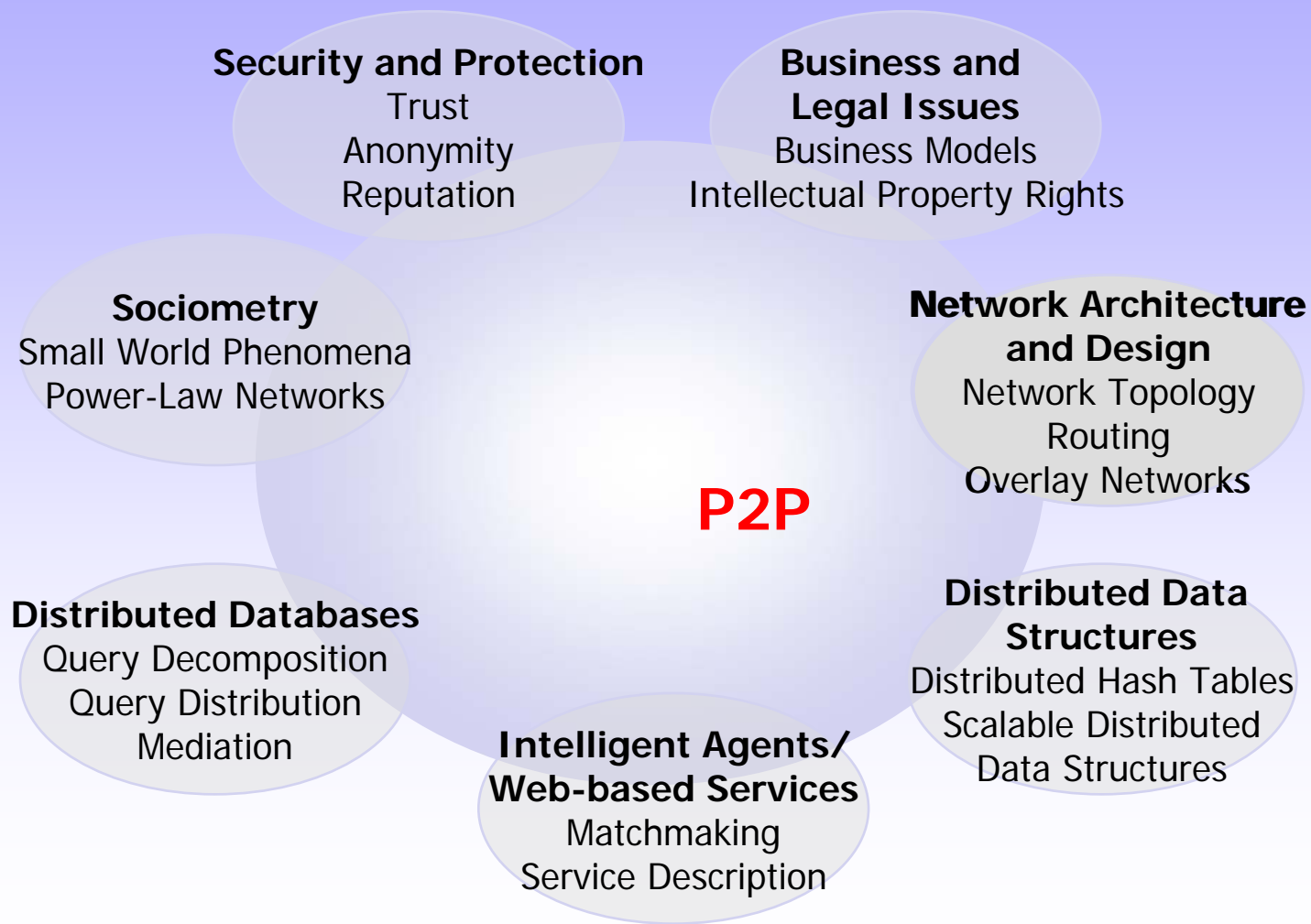


4.5 P2P网络的问题与研究



4.5.1 P2P的安全问题

◆ P2P本质是极端分布式系统

- 安全问题比一般分布式更严重
- 许多安全问题，至今仍然是开放性的（即尚未解决）
- 版权问题是非技术问题
- 安全性与方便性总是一对矛盾

◆ P2P中常规网络攻击

- 监听/截获：
 - ☞ 被动攻击，截获数据包、破坏数据机密性，难以检测、易于防止
 - ☞ 直接对称密钥方式不存在可信第三方。采用PGP电邮方式较合适，即以公开密钥机制传递对称密钥
- 中断：
 - ☞ 占据结构化网络容易暴露的下一跳路由节点
 - ☞ 主动攻击，阻断网络通信、易于检测、难于防止

◆ 篡改:

- 主动破坏数据完整性, 易于检测、难于防止
- 报文鉴别MAC、 数字签名、hash映射, 后者可取

◆ 伪造

- DOS+IP欺骗、源站文件伪造
- ID伪造, 包括Hash(IP), Hash(key)
 - ☞ Sybil: 女巫攻击: 一个节点伪装称多个ID、操纵破坏和分割网络
 - ☞ Byzantine: 拜占庭攻击: 多个恶意节点的联合欺骗
- 引入“声誉/信任”机制

◆ 重放

- 制造网络混乱、破坏一致性
- 给消息附加时间戳

◆ 抵赖

- 抵赖已经收、发的消息
- 策略: 数字签名

◆ 应用层安全

- ♣ 恶意节点: 不给回应、错误回应
带宽搭便车
- ♣ 文件共享: 传播伪造文件、填充垃圾/流氓文件、网络置毒...
- ♣ 备份服务: 敏感数据可见、备份性能、协定违反
- ♣ 文件存储: 恶意删除文件...

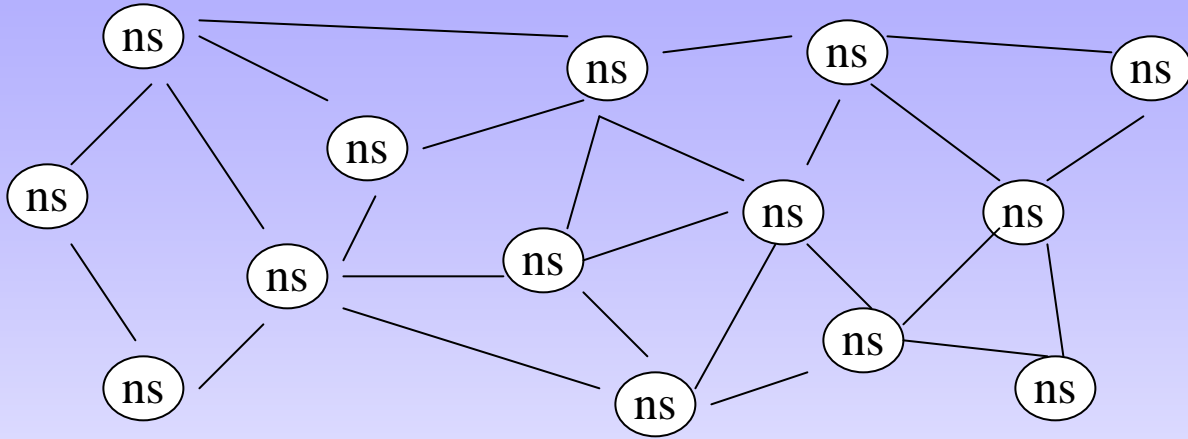
◆ 联网层安全

- ♣ 错误网络状态信息误导对等端
- ♣ 无效查找: 转发给一个无效节点
- ♣ 无效路由更新: 破坏它点路由表
- ♣ 嗅探: 观察节点行为、嗅探内容
- ♣ Sybil攻击: 削弱冗余性
- ♣ Byzantine攻击
- ♣ Dos攻击
- ♣

源于P2P网络的安全问题

- ◆P2P蠕虫传播
- ◆P2P僵尸网络
- ◆P2P信誉危机
- ◆P2P网络路由安全

Peer to Peer对象定位机制



◆ 特征

- 节点与节点是平等关系（相对于层次结构）
- 负载相同（性能）
- 重要性相同（功能）
- 两两能通讯（通过节点转发）

◆ 优势

- 无瓶颈 – 可扩展性好、可用性高

◆ p2p的对象定位

- 将对象的定位信息 $\langle oid, p \rangle$ 分散到各节点上, 分配方案: $nid = \text{hash}(oid)$

Peer to Peer网络基本问题

◆ p2p网络概念

- 连接(hop)：两个节点互知对方的IP地址
- 路由表：每个节点上都保存着一个邻居节点IP列表
- 通讯：消息通过连接在p2p网络中的传递
- 消息延迟：消息传递经过的连接数

◆ P2P网络基本问题

- Peer to Peer网络路由（支持任意两个节点之间通讯）

◆ 挑战

- 高可扩展性：每个节点的邻居节点IP列表要小
- 高效：消息传递平均延迟要小
- 高可用性：每两个节点之间的不同通讯路径要多

◆ 路由方法→路由表→网络拓扑结构

P2P路由问题形式化描述

◆路由问题

- 针对 N 个节点，设计一个包含这 N 个节点的连通图 G ，使得节点之间度的最大差值(b)尽量小，每个节点的度(d)尽量小， G 的直径(r)尽量小，使得边连通度(e)尽量大。

◆作用

- 指导研究新算法
- 评价现有算法性能

现有的P2P路由算法

◆ 直接手段1：完全图

- $b: 0$ --- P2P
- $d: O(N)$ --- 可扩展性差
- $r: 1$ --- 高效
- $e: O(N)$ --- 高可用
- 实例: Afs, xFS, Farsite, ethernet

◆ 直接手段2：环

- $b: 0$ --- P2P
- $d: 2$ --- 可扩展性好
- $r: O(N)$ --- 效率低
- $e: 2$ --- 低可用
- 实例: Token Ring

■ 改进型：树

- $b: C$ --- P2P
- $d: O(C)$ --- 可扩展性好
- $r: O(\log N)$ --- 高效
- $e: O(1)$ --- 低可用
- 实例: INS(99mit), Arrow(98brown), Gnutella(98)

■ 经典算法

- $b: C$ --- P2P
- $d: O(\log N)$ --- 可扩展性好
- $m: O(\log N)$ --- 效率高
- $r: O(\log N)$ --- 高可用
- 实例: CAN, Pastry, Chord, Tapstry

P2P的未来

◆ P2P将变得更成熟

- 增加交互性
- 更多连接到因特网
- 健壮的应软件

◆ P2P是一重要的方法

- 可扩展性对网络、系统和应用始终都是一个待解决的问题（全球、无线）
- 世界总有不被连入的部分，需要Ad-hoc和非集中组
- 系统组成和应用固有是P2P而须借助该解

非技术挑战

◆ 接受和使用

- 每个Peer端依赖另一端提供服务，故必须存在大量可用的Peers提供服务
- Gnutella下载者多，上载者少

◆ 用户群分裂的危险

- 个体一般只加入一个或少数几个P2P系统，因无更多资源同时支持多个系统
- 每个新系统引入，必然分裂用户群，并危害所有其它P2P系统，Napster和即时消息都有这个问题

◆ 规模

- 很多算法依赖用户的规模；需要知道每个本地Peer，但有很少的全局信息和知识

◆ 发布控制：版权，威胁传统服务

◆ 思想方式

- 根本原因是**用对等互助**模式替代目前服务和被服务模式
- 在互助中提供规模性服务似乎矛盾，但实际生活中的确存在，如资助餐厅、自驾车旅游团，网络
- 似乎不应该限制，而是在寻找其中的商机
- 取系统边界的资源的优点
- 支持用户间的直接交互

◆ 一种模式

- P2P并不是所有未来问题的解，有其强势和弱势
- 一个实现的选择，应依据系统或环境的特性

对网络管理的影响


◆ P2P流量对网络带宽的影响

- P2P音视频文件共享占50-60%流量(白天),晚上占90%

◆ P2P成组连接方式对网管的影响

- 网管如何识别和控制P2P流
- 如何防止违反数字知识版权法规
- 如何提供基于P2P的服务
- 商业模式?

◆ P2P与IPV6的充分结合



◆ 至少存在3个方面对未来有影响

- P2P算法：可能有很大的机会；世界变得越来越非集中化和连接化；需要P2P算法来克服可扩展、匿名和连接问题
- P2P应用：最有可能成功，如Napster
- P2P平台：可能广泛采用JXTA

◆ 自动计算8法则（类生物）

- 知道自我
- 构成自我
- 优化自我
- 治愈自我
- 保护自我
- 生长自我
- 知道邻居
- 帮助用户

下一代互联网上的P2P应用

P2P应用

通信协作

- 通信 – 聊天, 消息
- Co-共同-评论/编辑/创作/创立
- 游戏
- 发明

分布计算

- 互联网分布计算
- 内部网分布计算
- 网格计算

内容共享

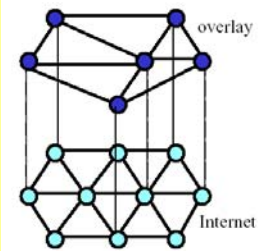
- 文件分发
- 内容分配
- 分布存储
- 缓存, 边缘服务
- 信息管理 – 发现
集中, 滤波, 组织, ...

分布式管理（分布自治）

QoS和安全性

路由探测、选择
病毒发现、消灭
数据分类、管理

智能结点 重叠网



网络存储：如Oceanstore

◆ 背景

- 无处不在的计算：台式机、笔记本电脑、PDA、移动电话
- 无所不在的连接：宽带加速发展、宽带无线电接入
- 对瘦客户机的需求：超小型的瘦客户机
 - ☞ MEMs设备-传感器+CPU+无线网络的体积约 1mm^3

◆ 网络存储是基础设施

- 如水、电一样。用户付月租就可以在网上存储数据。

◆ 规模越大效果越好

- 网络存储加密的文件被分解成为互相重叠的片断存储在全球各地
- 即使本地的节点损坏，也可以通过一组片断恢复原始的文件。
- 系统为每一个片断分配ID码，当用户需要取回其文件时，他的计算机告诉节点寻找最近的所需要片断，将其组装恢复文件



◆P2P网络没有考虑物理网络距离?

主要参考文献

- ◆ Peer-to-Peer Computing
Dejan S. Milojevic, Vana
Kalogeraki, Rajan Lu
Kiran Nagaraja, Jim
Pruyne, Bruno
Richard, Sami
Rollions, Zhichen Xu,
HP Laboratories Palo
Alto HPL-2002-57 March
8th, 2002
- ◆ 对等网络：结构、应用与设计；陈贵海等，清华大学出版社，2007. 9

