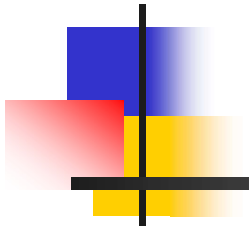
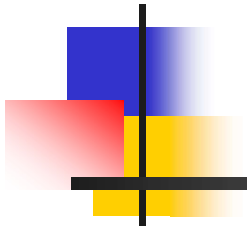
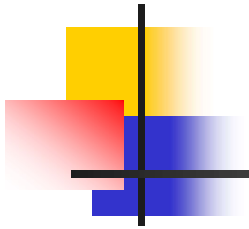


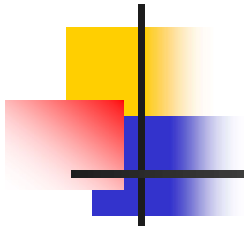
无线网络安全技术



chap1 课程概述



- 教材：PPT，以及自己感兴趣的其他教辅
- 考核：开卷卷面70%+平时30分
- 平时：课堂测试+上机
- 联系方式



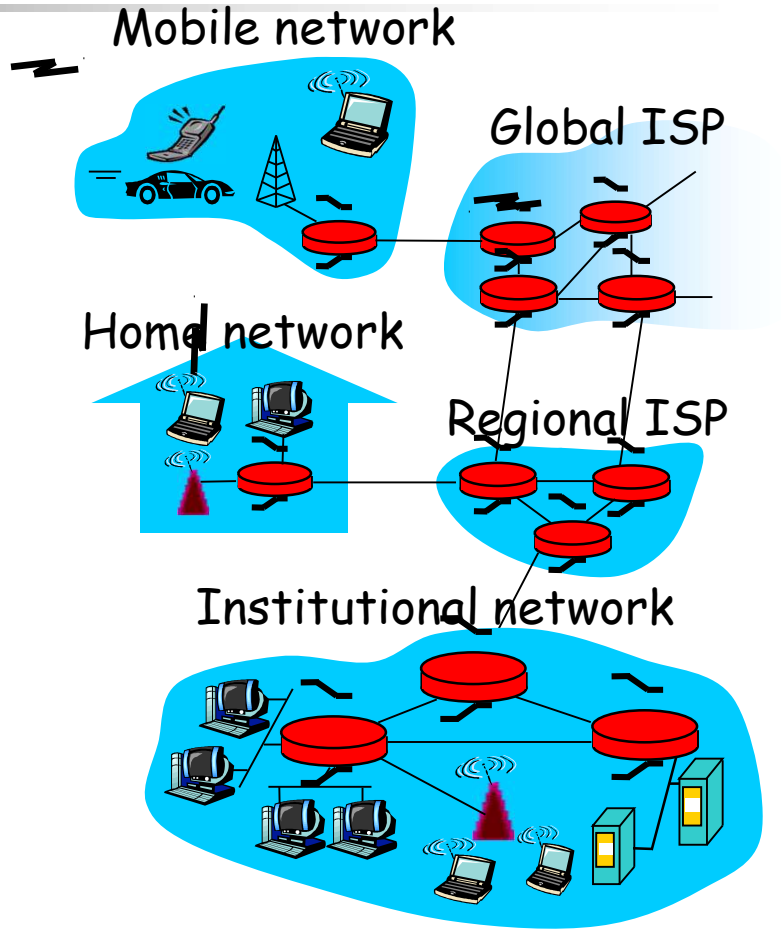
1.1 无线网络类型

- Internet
- WLAN (Wireless Local Area Network)
- Mobile Network
- WSN (Wireless Sensor Network)
- VANET (Vehicular ad-hoc Network)
- ICN (Information-Centric Networking)

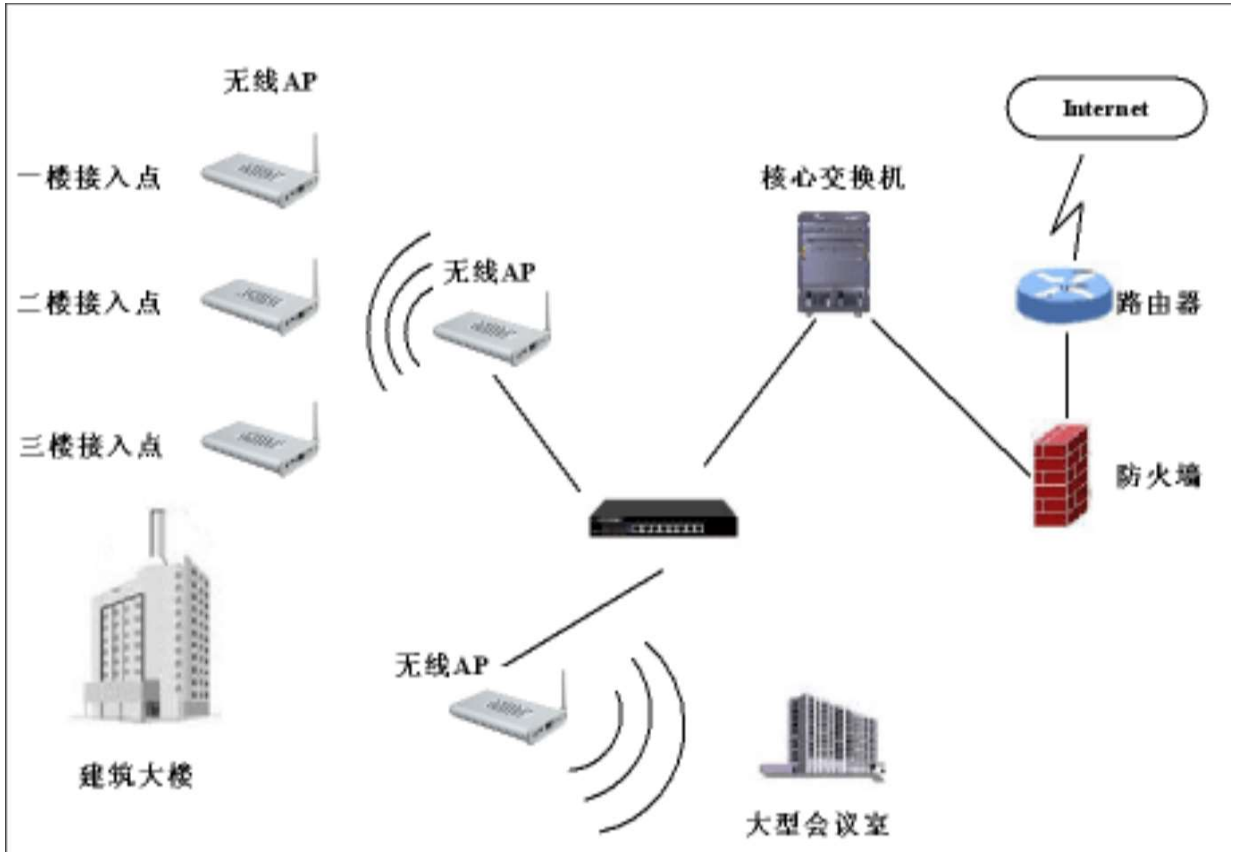
Oppnet (Opportunistic Network)
DTN (Delay Tolerant Network)

WLAN

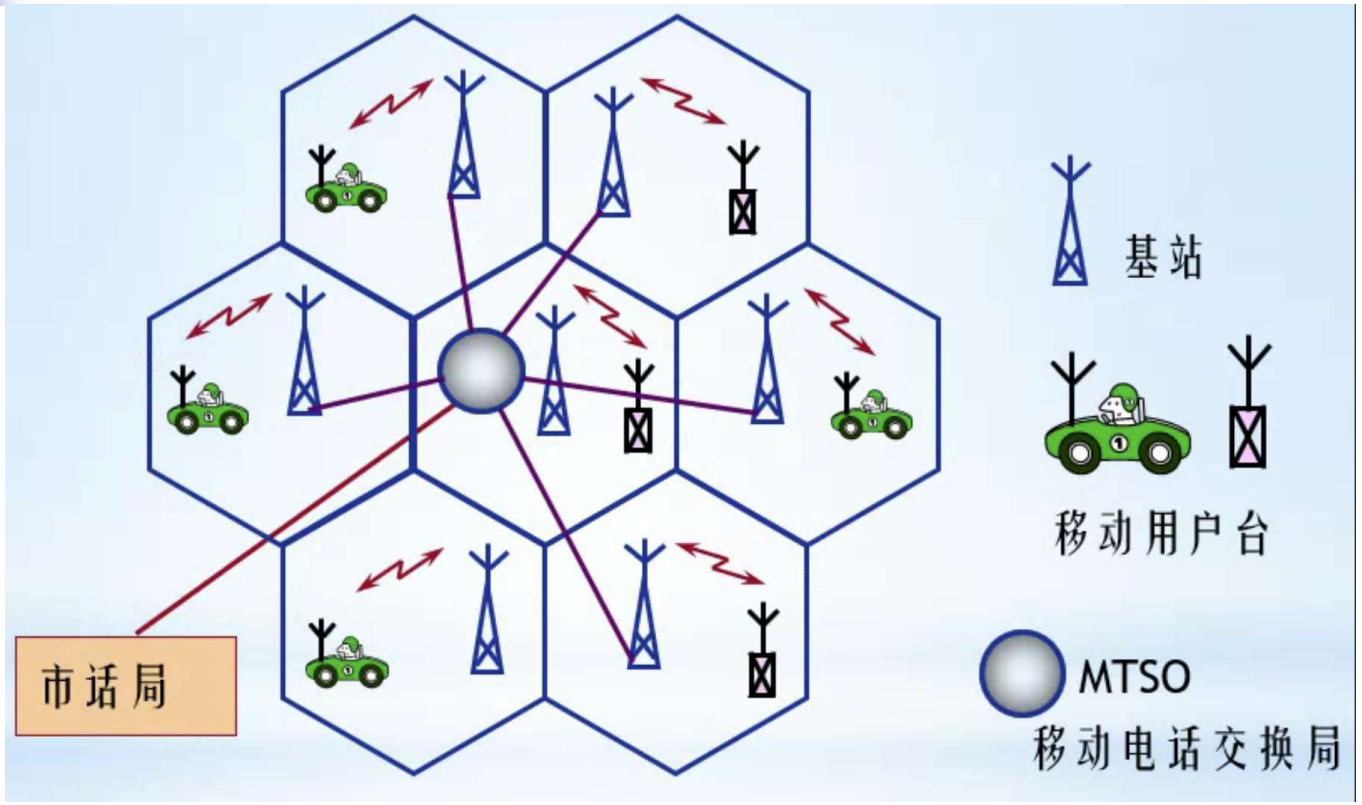
- Wired
- Wireless



WLAN

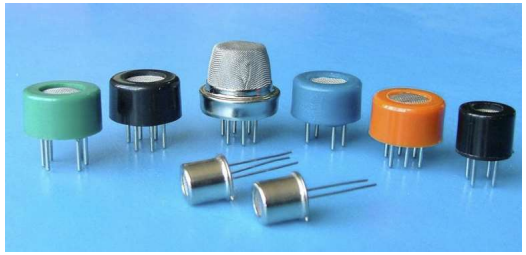

无线AP
一楼接入点
二楼接入点
三楼接入点
建筑大楼
无线AP
核心交换机
Internet
路由器
防火墙
无线AP
大型会议室

Celluar or mobile network

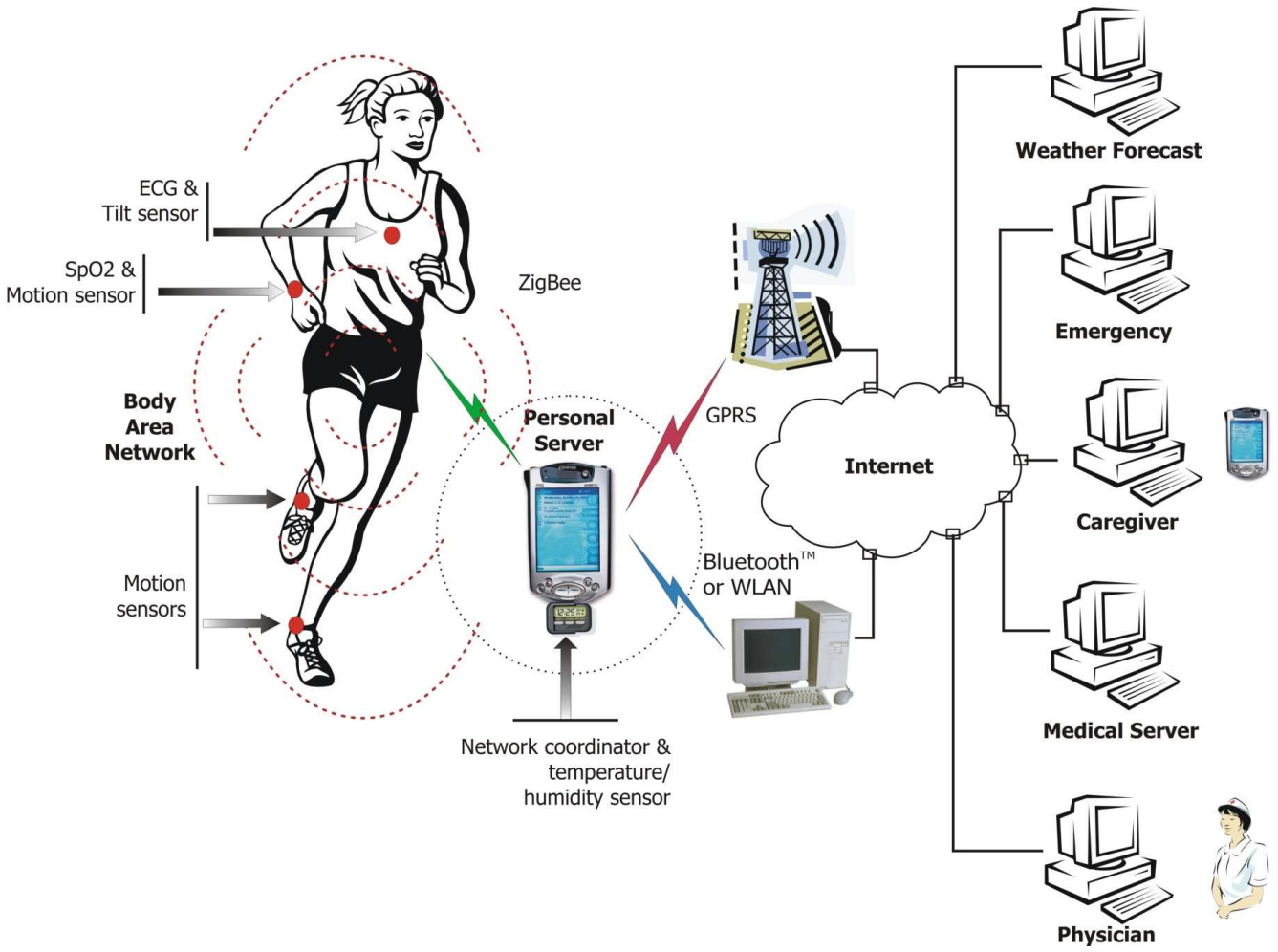


Internet of Things

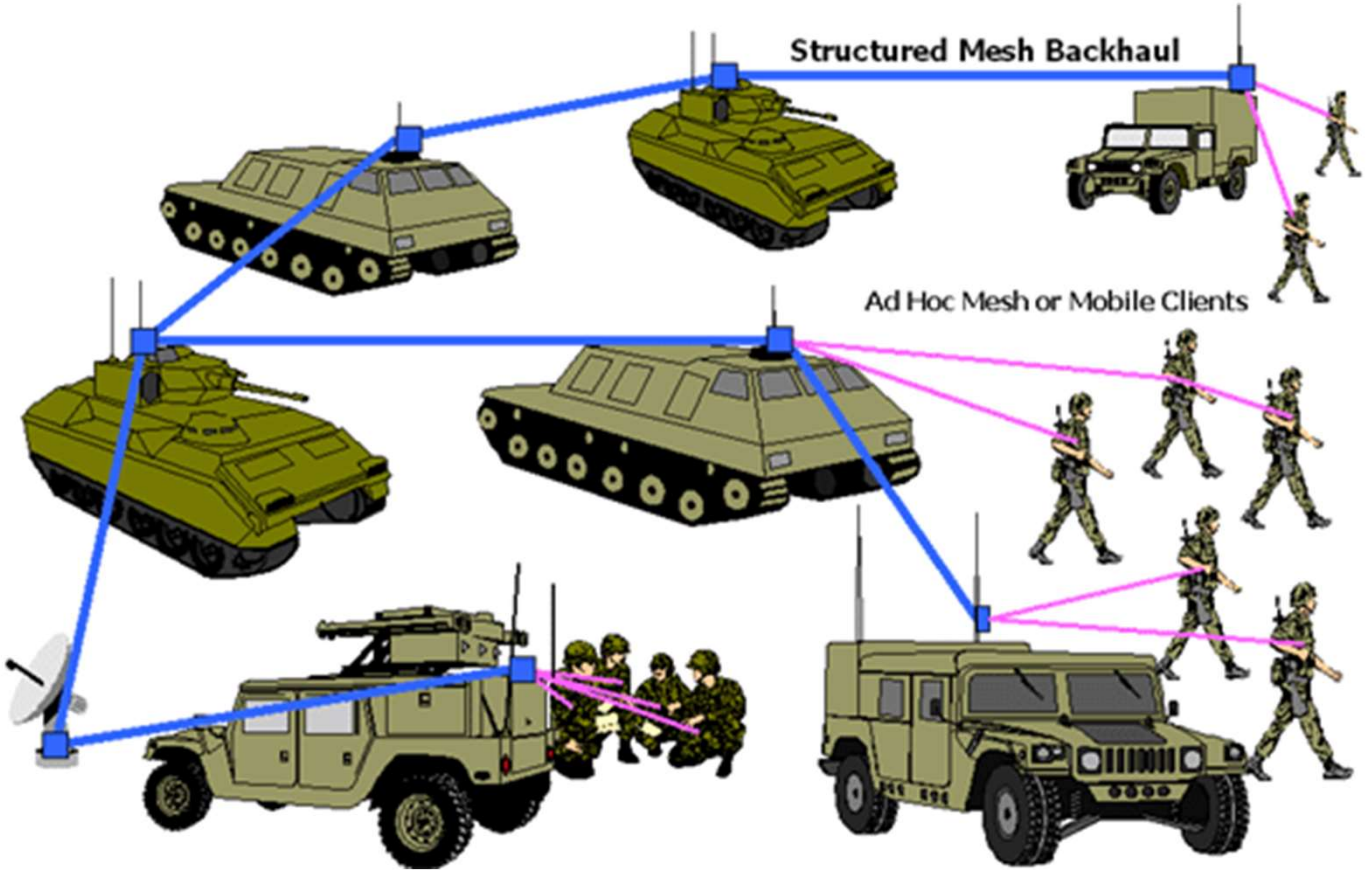
Wireless Sensor Network



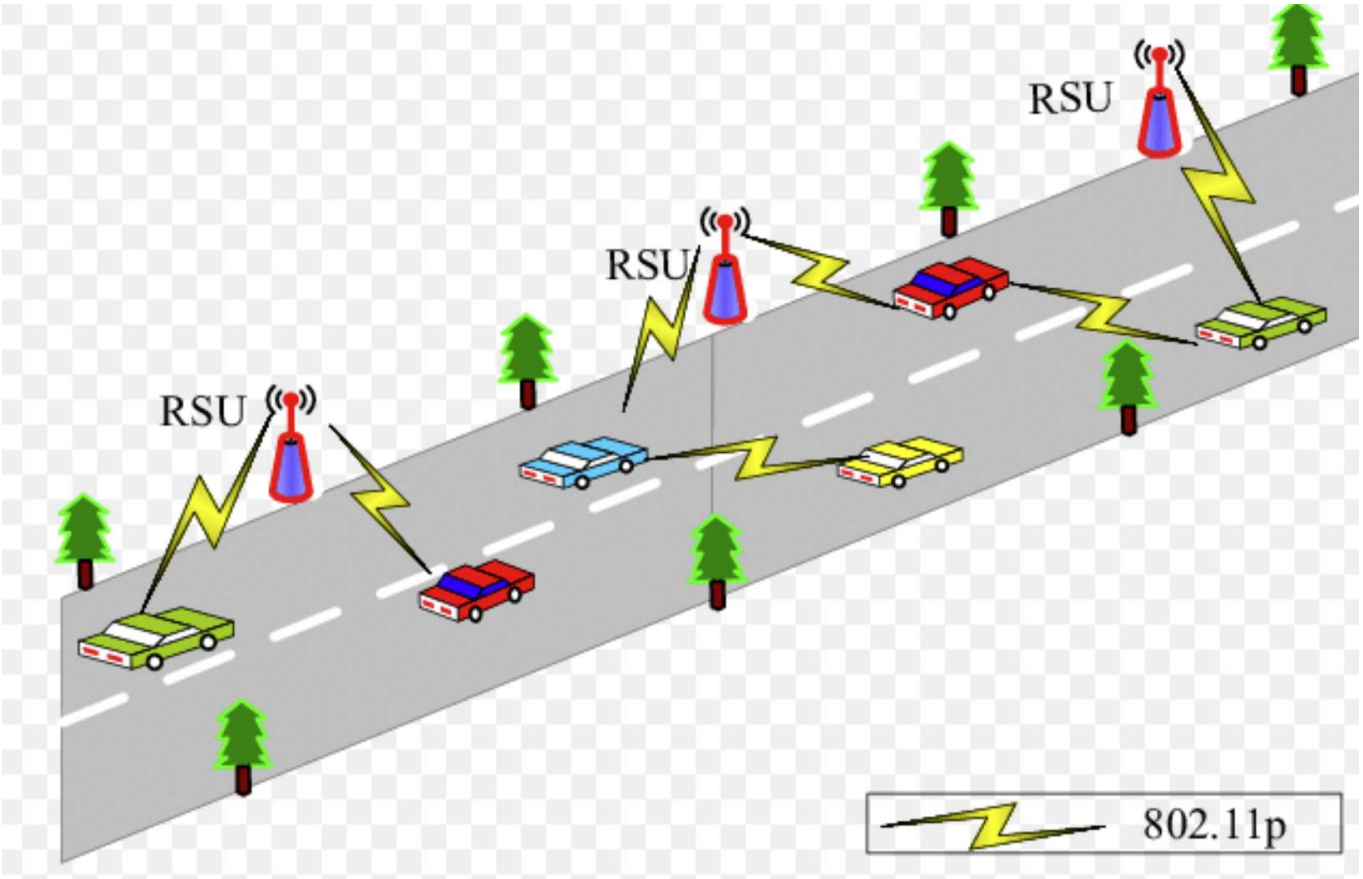
Body Area Network



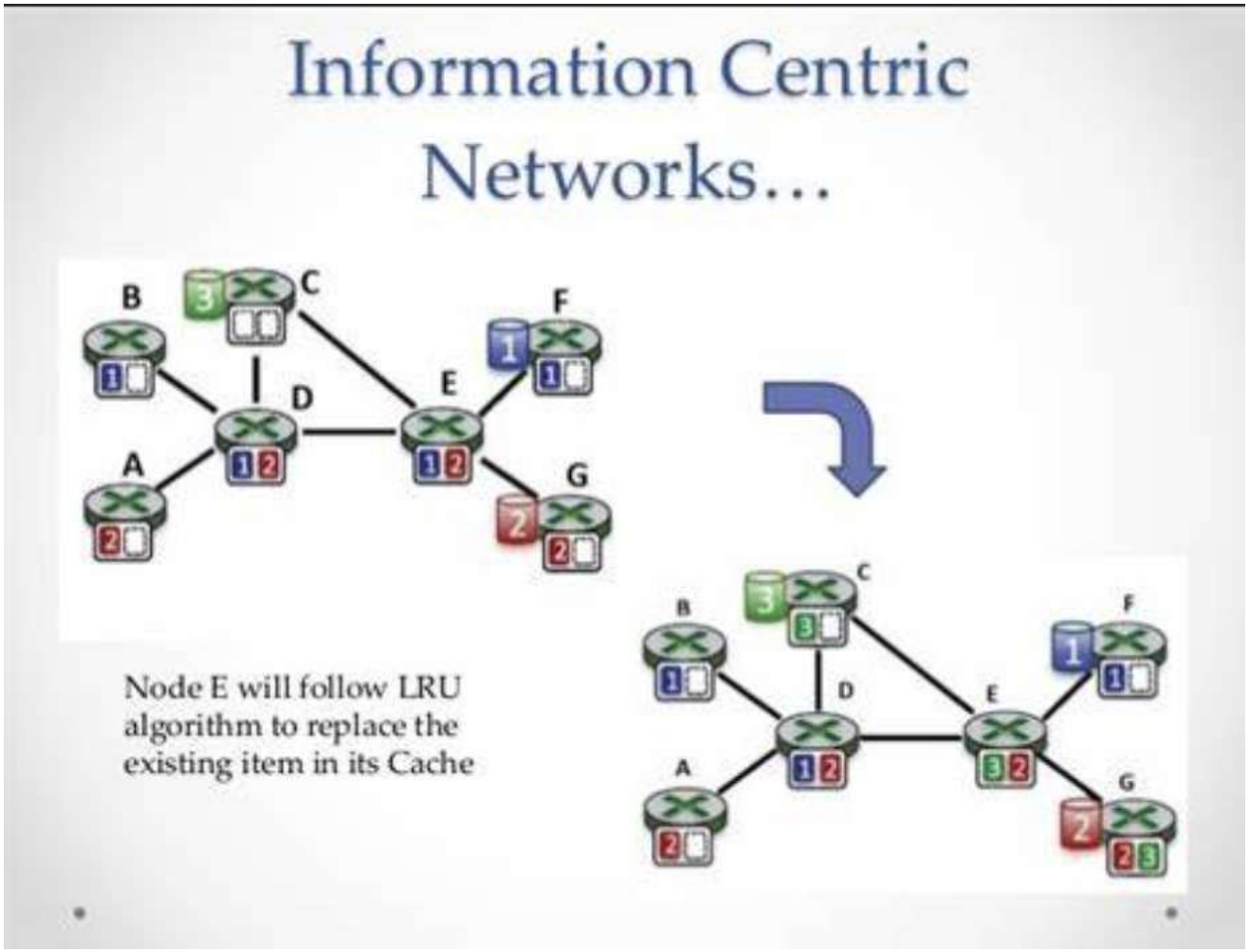
Ad Hoc 点对点

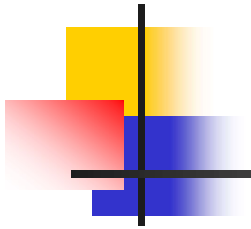


Vehicular ad-hoc network (VANET)



Information-Centric Networking



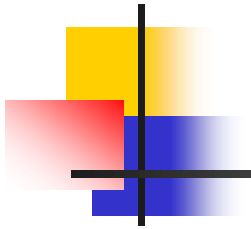


引申概念 Opportunistic network

- differ from the Internet in that disconnections are the norm instead of the exception.
- In opportunistic networks, communication devices can be carried by people, vehicles or animals, etc.
- Thus, an end-to-end connection between the source and the destination can be absent at the time the source wants to transmit, and even later.
- Delay Tolerant Network(DTN)

1.2 无线网络特点

- （1）网络连接的开放性
  - 有线网络的网络连接是相对固定的，具有确定的边界，如防火墙和网关，攻击者必须物理地接入网络或经过物理边界，才能进入到有线网络。通过对接入端口的管理可以有效地控制非法用户的接入。
  - 无线网络则没有一个明确的防御边界。无线网络的开放性带来了信息截取、未授权使用服务、恶意注入信息等一系列信息安全问题，如无线网络中普遍存在的DDoS 攻击问题。



- （2）无线信道的不稳定性
  - 无线网络随着用户的移动其信道特性是变化的，会受到干扰、衰落、多径、多普勒频移等多方面的影响，造成信号质量波动较大，甚至无法进行通信。需要ARQ

1.2 无线网络特点

（3）网络终端的移动性

有线网络的用户终端与接入设备间通过线缆连接，终端不能大范围移动，对用户的管理比较容易。

无线网络终端不仅可以在较大范围内移动，而且还可以跨区域漫游，这增大了对接入节点的认证难度，如移动通信网络中的接入认证问题。

1.2 无线网络特点

（4）网络的拓扑结构

动态的、变化的拓扑结构缺乏集中管理机制，使得安全技术（如密钥管理、信任管理等）更加复杂（可能是无中心控制节点、自治的）。

另一方面，无线网络环境中做出的许多决策是分散的，许多网络算法（如路由算法、定位算法等）必须依赖大量节点的共同参与和协作来完成。

1.2 无线网络特点

（5）网络终端设备具有的特点

无线网络终端设备与有线网络的终端（如 PC）相比，具有计算、通信、存储等资源受限的特点，以及对耗电量、价格、体积等的要求。

（6）网络异构性

个域网、局域网、广域网等多种网络类型，缺少统一标准，安全管理具有一定难度。

1.3 无线网络安全服务

- ITU-T(X.800)已经定义出5种服务：

  认证；访问控制；数据保密；数据完整性；不可否认。

1. 身份认证 Authentication

认证发送方和接收方的身份(对等实体身份认证);
认证信息的来源(数据源身份认证)。

2. 访问控制 Access control

保护信息免于被未经授权的实体访问。

3. 数据机密性 data confidentiality

保护数据免于非授权泄漏，并防止流量分析

4. 数据完整性 data integrity

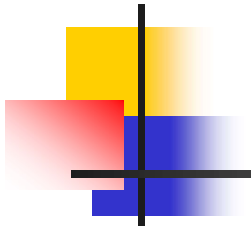
确保接收到的数据是由授权用户发出的或者是未被修改过的

5. 不可否认性 non-repudiation

防止通信方对通信行为的否认，包括源不可否认性和宿不可否认性

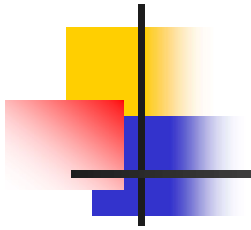
补充：Availability Service

系统或系统资源能够按照要求根据系统性能规范被授权系统的实体访问和使用



1.4 安全威胁的来源

1. 外部的各种恶意攻击
2. 系统本身的脆弱性
3. 应用软件的漏洞



恶意攻击

- 主动攻击

  以各种方式有选择地破坏信息，如添加、修改、删除、伪造、重放、冒充、乱序、病毒等，人为通过网络通信连接进行的。

- 被动攻击

  （1）不干扰网络信息系统正常工作情况下，进行侦听或监控数据传输。

  （2）计算机病毒、木马、恶意软件等。这些威胁一般是用户通过某种途径(如使用了带病毒的U盘，带病毒或木马或恶意软件的网页/图片/邮件等)感染上的。

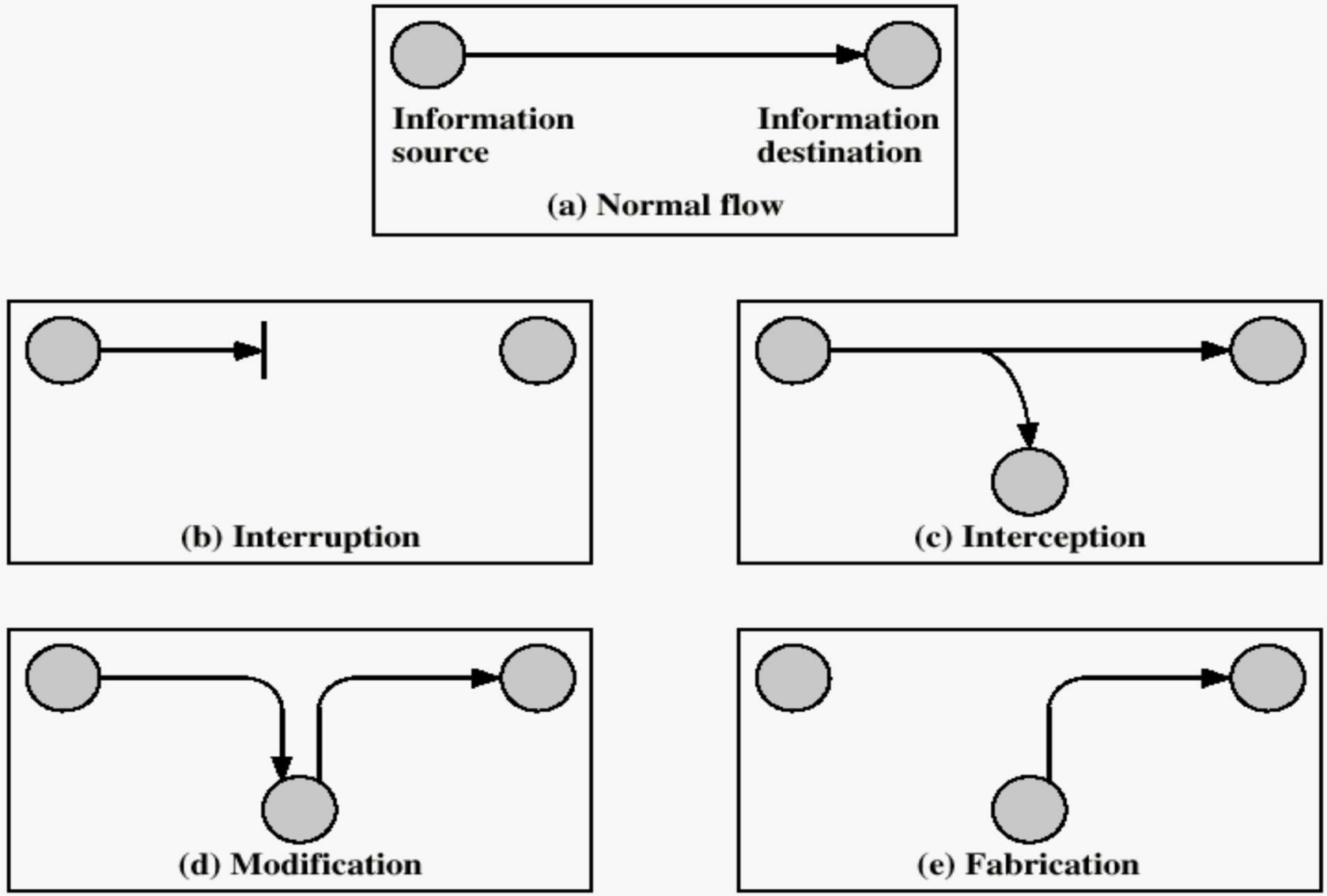


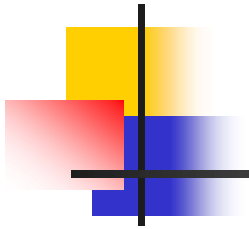
Figure 1.1 Security Threats

计算机系统本身的脆弱性

- 计算机系统本身无法抵御自然灾害的破坏，也难以避免偶然无意造成的危害。如水、火、地震的破坏及环境（温度、振动、冲击、污染）的影响以及硬件设备故障，突然断电或电源波动大及各种误操作等危害。

安全漏洞

- 漏洞：漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。是受限制的计算机、组件、应用程序或其他联机资源的无意中留下的不受保护的入口点。
- 2021年7月12日，工业和信息化部、国家互联网信息办公室、公安部联合印发通知，公布《网络产品安全漏洞管理规定》（工信部联网安〔2021〕66号），自2021年9月1日起施行。



例：协议本身的漏洞

A.考虑网络互连缺乏对安全方面的考虑。

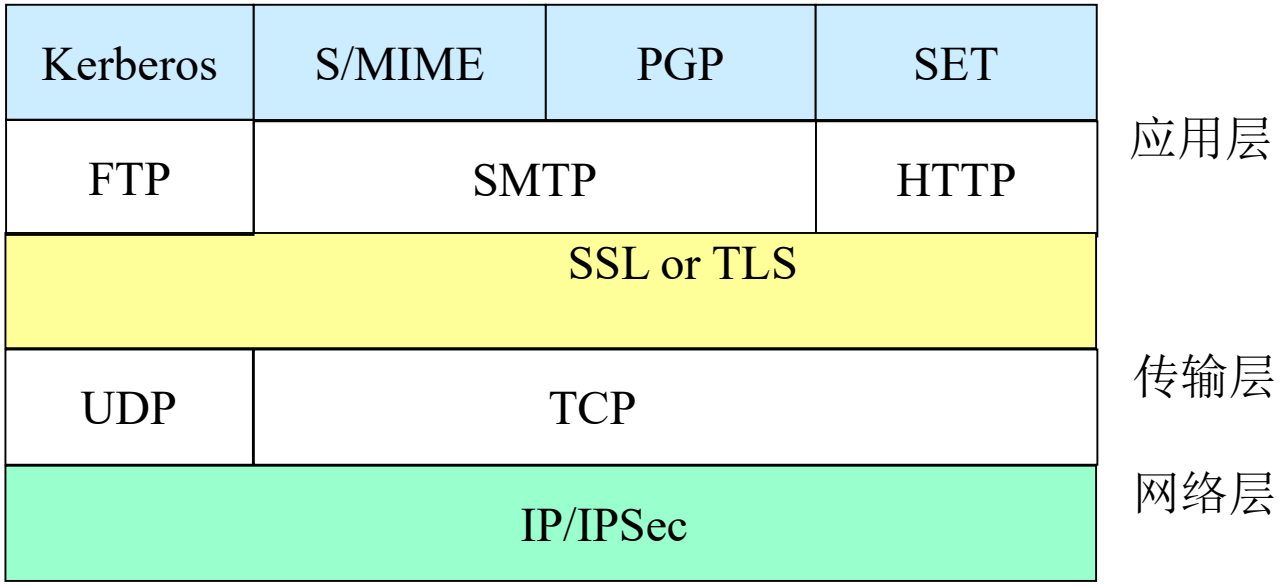
B.TCP/IP是建立在三次握手协议基础之上，本身就存在一定不安全的因素，握手协议的过程当中有一定局限性。例：SYN洪泛攻击；IP伪装攻击。

C.网络的开放性，TCP/IP协议完全公开，远程访问使许多攻击者无须到现场就能够得手，连接的主机基于互相信任的原则等等性质使网络更加不安全。

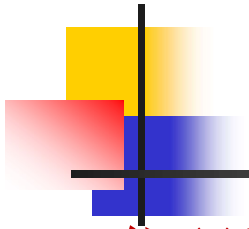
电子邮件安全协议（PEM、S/MIME、PGP）；

远程登陆的安全协议（SSH）；

Web安全协议（S-HTTP）；



基于TCP/IP协议的网络安全体系结构基础框架



例：常见漏洞

代码注入，包括SQL注入在内的广义攻击，它取决于插入代码并由应用程序执行。

会话固定，这是一种会话攻击，通过该漏洞攻击者可以劫持一个有效的用户会话。会话固定攻击可以在受害者的浏览器上修改一个已经建立好的会话，因此，在用户登录前可以进行恶意攻击。

路径访问，或者“目录访问”。该漏洞旨在访问储存在Web根文件外的文件或者目录。

弱密码，字符少、数字长度短以及缺少特殊符号。

硬编码加密密钥，提供一种虚假的安全感。硬编码是将数据直接嵌入到程序或其他可执行对象的 源代码 中的软件开发实践，与从外部获取 数据 或在运行时生成数据不同。硬编码密码是指在程序中采用硬编码方式处理密码。

Thank You!!