

5506_Note

1. 知识点总结

1.1 频段

2.4 GHz 频段 是一种无线电频率范围，指的是 **2.4 GHz（千兆赫兹）** 左右的频率。无线电频段指的是一段连续的电磁波频率区间，通常被分配给特定的用途，如通信、广播、无线传感器等。

频段的定义：

频段是指电磁波频率的一个区间。不同的频段具有不同的物理特性，这决定了它们在无线通信中的适用性。例如，低频段信号可以传播得更远，穿透障碍物能力更强；而高频段信号则能支持更高的数据传输速率，但传输距离和穿透力会相对较弱。

2.4 GHz 频段的特点：

- **全球通用**：2.4 GHz 频段是全球通用的 ISM（工业、科学和医疗）频段，意味着世界各地都可以使用该频段进行无线通信，不需要专门的许可证。
- **应用广泛**：很多常见的无线技术使用 2.4 GHz 频段进行通信，如 Wi-Fi（802.11b/g/n）、蓝牙、Zigbee 等。这是因为该频段具有较好的传输速度和中等的传输距离。
- **传输距离**：2.4 GHz 频段的无线信号在开阔环境下通常可以传输数十米到几百米，具体距离取决于功率、天线设计和环境因素（如障碍物）。
- **穿透性中等**：2.4 GHz 频段的信号比较容易被墙壁或其他障碍物削弱，但仍然具有一定的穿透能力，适合家庭和办公环境。

频段和无线通信的关系：

- 频率越高，传输速率越快**：较高的频率通常可以支持更高的数据传输速率。因此，2.4 GHz 频段在中等距离下能够提供较快的数据传输速率（如 Wi-Fi）。
- 频率越低，传输距离越远**：低频段（如 700 MHz）信号可以传播得更远，穿透障碍物的能力更强，因此更适合远距离通信。然而，低频段的带宽通常较小，支持的数据传输速率有限。
- 干扰问题**：2.4 GHz 频段是一个**非常拥挤的频段**，因为它被许多设备使用（如 Wi-Fi 路由器、蓝牙设备、微波炉等），所以设备之间可能会出现干扰，从而影响通信质量。这也是为什么有时在住宅区或办公区中，Wi-Fi 信号质量可能不稳定。

不同频段的区别：

不同的无线电频段具有不同的物理特性和适用场景。以下是一些常见的频段及其特点：

a. 700 MHz 频段：

- **特点：**低频段，信号传播距离远，穿透力强。
- **应用：**广泛用于电视广播、移动通信（如 LTE 网络）。适合覆盖大面积、障碍物多的区域。

b. 900 MHz 频段：

- **特点：**低功耗，适合长距离通信，信号穿透能力较强。
- **应用：**Z-Wave、LoRa 等低功耗广域网 (LPWAN) 技术常用该频段。适合传感器和远程监控设备。

c. 2.4 GHz 频段：

- **特点：**中等频段，传输距离适中，适合家庭、办公场景。
- **应用：**Wi-Fi、蓝牙、Zigbee 等无线设备。由于设备众多，可能存在干扰。

d. 5 GHz 频段：

- **特点：**高频段，数据传输速率高，但信号穿透力弱，传输距离较短。
- **应用：**高速 Wi-Fi（802.11ac、802.11ax）常用该频段，适合需要高带宽的应用，如高清视频流、在线游戏等。

e. 60 GHz 频段：

- **特点：**极高的频率，传输速率非常快，但穿透力极弱，通常用于短距离的高速数据传输。
- **应用：**一些高性能的无线设备如 WiGig（802.11ad）使用该频段，适合设备间的近距离高速通信。

总结：

- **2.4 GHz 频段** 是全球通用的 ISM 频段，适合中等距离、较高数据速率的无线通信，广泛用于 Wi-Fi、蓝牙和 Zigbee 等技术。
- 不同频段具有不同的传播特性和应用场景，选择合适的频段要根据应用需求来决定。较低的频段适合远距离通信和强穿透能力的场景，而较高的频段适合短距离的高速数据传输。

1.2 Zigbee 和 Z-Wave 的比较总结

Zigbee 和 Z-Wave 的比较总结

特性	Zigbee	Z-Wave
频段	2.4 GHz, 868 MHz, 915 MHz	868 MHz（欧洲）, 908 MHz（北美）
数据速率	250 kbps	100 kbps
网络架构	网状网络，支持较大规模节点	网状网络，节点数量较少
功耗	低功耗	超低功耗
覆盖范围	支持较多设备，覆盖范围广	支持的设备数量相对较少
干扰	可能受到 Wi-Fi 和蓝牙干扰	低干扰，频段不与 Wi-Fi 和蓝牙冲突
典型应用	智能家居、工业控制、环境监测	智能家居自动化（灯光、安全、温控）

结论

Zigbee 和 Z-Wave 各有优点，适用于不同的物联网和智能家居应用场景。Zigbee 在大规模、多设备场景中具有优势，而 Z-Wave 更适合小规模、对干扰敏感的家庭自动化系统。选择哪个协议取决于具体的应用需求、环境和设备兼容性

1.3 NF 公式 奈奎斯特公式 (Nyquist Formula) | 信道容量与带宽的关系

这段话介绍了 **奈奎斯特公式 (Nyquist Formula)**，它描述了在理想条件下（不考虑噪声的情况下）通信系统中 信道容量与带宽 的关系：

- 公式: $C = 2B \cdot \log_2 M$
 - C 是信道的容量，单位是每秒的比特数 (bps)。
 - B 是信号的带宽，单位是赫兹 (Hz)。
 - M 是符号可以采取的不同电平数。

这表明在理想情况下，信道容量 C 取决于带宽 B 和符号可以取的不同电平数 M 。

费曼技巧是一种通过简单易懂的方式讲解复杂概念的方法。下面我们用费曼技巧来解释**奈奎斯特公式**。

1. 什么是奈奎斯特公式？

奈奎斯特公式告诉我们，在理想条件下，一个通信信道可以传输多少数据。这公式展示了**信道容量**（也就是每秒可以传输多少比特的数据，单位是**bps**）和**带宽**（频率范围，单位是**赫兹 (Hz)**）之间的关系。

2. 如何理解公式？

公式是这样的：

$$C = 2B \cdot \log_2 M$$

- **C** 是信道容量，表示每秒可以传输多少 **比特** 数据。
- **B** 是带宽，指的是可以传输信号的频率范围，单位是 **赫兹**。
- **M** 是**符号的取值数**，表示每个符号可以代表多少种不同的状态或电平。

3. 用简单的比喻来理解公式

假设你要通过电线发送消息，消息可以通过不同的"信号"来传输。每个信号可以表示一个数据单位，我们称之为**符号**。如果你只有两种信号（例如，高电平和低电平），你只能通过每个符号传递一个比特的数据，因为两种状态只能代表 0 和 1。

- 如果你想传递更多的数据（增加**信道容量**），有两种主要的办法：
 - i. **增加带宽**：就像给你的"信号道路"加宽一样，让更多的信号可以同时传递。带宽越大，意味着你可以传递更多的符号。
- 2. **增加符号的状态数 (M)**：如果你不止有两种信号，而是有四种或更多（例如，高、低、中、极高），你就可以在每个符号中包含更多的信息。通过每个符号的不同状态，你可以传递更多比特的信息。

4. 具体例子

- 如果符号只有两种状态 (**M = 2**)，每个符号就只能传递 **1 比特** 的信息 (0 或 1)。这时公式变成： $C = 2B \cdot \log_2 2 = 2B \cdot 1 = 2B$

意思是信道容量 C 仅仅是带宽的两倍。

- 如果符号有 4 种状态 ($M = 4$)，每个符号可以传递 2 比特的信息 (00、01、10、11)。公式变成： $C = 2B \cdot \log_2 4 = 2B \cdot 2 = 4B$ 这意味着，你可以在相同的带宽下传递更多的信息，因为每个符号可以包含更多的比特。

5. 总结

奈奎斯特公式告诉我们，通信信道的容量不仅依赖于带宽，还依赖于每个符号可以代表的信息量 (M)。增加带宽或符号状态数都能提高信道的总容量。在现实中，这个公式的前提是不考虑噪声，也就是说信道是完全理想的。

1.4 能量公式 $\text{Energy} = \text{Power} \times \text{Time}$

这句话的意思是，基于能量公式 $\text{Energy} = \text{Power} \times \text{Time}$ ，在设计电子设备（尤其是低功耗设备如物联网设备）时，可以采取一种优化策略：让设备在短时间内使用较高的功率工作，然后在其余时间进入休眠状态，从而节省能量。

解释：

- $\text{Energy} = \text{Power} \times \text{Time}$ 是能量的计算公式，表示消耗的总能量等于设备在某段时间内使用的功率与时间的乘积。
- 高功率、短时间工作：**设备可以在需要执行任务时（例如，发送数据或处理信息）短时间内使用较高的功率。因为高功率工作时间较短，尽管功率大，但总能量消耗不会很高。
- 休眠：**在设备不需要工作时，它可以进入低功耗的休眠模式（或“休眠”），在这个状态下功耗非常低。

设计策略：

这个策略的核心是减少设备在高功率工作时的总持续时间，通过快速完成任务然后休眠，来最小化总能量消耗。这样可以延长设备的电池寿命或降低功耗。

具体例子：

在物联网设备中，传感器可能每隔一段时间测量数据并将其发送到云端。该设备可以：

- 在测量和传输数据的过程中使用高功率（短时间内快速完成任务）。
- 在数据传输结束后进入低功耗的休眠状态，直到下一个数据传输周期开始。

这种设计策略常用于低功耗物联网设备，如传感器、可穿戴设备等，它们的目的是在延长电池寿命的同时保持设备的功能性。

1.5 供应商锁定 (Vendor Lock-in)

这段话的意思是，如果设备和云服务之间使用的是**“专有数据协议”**（即由特定公司或厂商设计的、未公开的通信协议），那么设备的所有者或用户可能会被**“绑定”**到该特定的云服务上。这意味着用户无法自由选择其他云服务提供商来连接和管理他们的设备。这种情况通常被称为**“供应商锁定”**（vendor lock-in）。

详细解释：

- a. **专有数据协议**：这是指由特定公司开发和控制的数据通信协议，只有该公司或其授权的系统可以使用和解读这些协议。它们不公开，因此其他公司无法提供兼容的服务。
- b. **供应商锁定 (Vendor Lock-in)**：当使用专有协议时，用户和设备会被“锁定”到该供应商的服务中，无法轻易切换到其他云服务提供商。例如，如果某个智能家居设备只与一个特定的云服务兼容，用户就无法选择其他云服务平台。
- c. **影响**：这种锁定限制了用户的选择权，如果用户对现有的服务不满意，或者其他服务商提供了更好或更便宜的服务，用户可能也无法轻松切换。更换服务可能需要更换设备，增加了成本和复杂性。

总结：

如果设备使用了专有数据协议，用户可能会被“锁定”到特定的云服务商上，这样用户的选择自由受限。这种情况就是所谓的“供应商锁定”。

1.6 设备到网关模型 (Device to Gateway Model)

这张图展示了物联网 (IoT) 中的 **“设备到网关模型 (Device-to-Gateway Model)”**，描述了物联网设备如何通过本地网关与应用服务提供商（云端）进行通信。

图中元素解析：

1. 设备 (Devices):

- 图中显示了两种不同类型的设备：
 - 温度传感器设备 (Device with Temperature Sensor)**：它使用一系列协议栈（如 HTTP、TLS、TCP、IPv6）与网关通信。
 - 一氧化碳传感器设备 (Device with Carbon Monoxide Sensor)**：它使用另一种协议栈（如 CoAP、DTLS、UDP、IPv6）与网关通信。
- 这些设备使用的是不同的通信协议栈来处理数据并发送到网关。

2. 协议栈 (Protocol Stack) :

- 每个设备根据其功能和设计，使用不同的协议栈与网关进行通信。温度传感器使用基于 TCP 的协议（如 HTTP 和 TLS），而一氧化碳传感器使用轻量级的 **UDP 协议（如 CoAP 和 DTLS）**。

3. 本地网关 (Local Gateway) :

- 所有设备的数据都会先发送到 **本地网关**，网关可以充当中介，处理来自设备的数据，并将数据转发到云端。
- 网关通过 **IPv4/IPv6** 协议与云服务提供商通信。
- 层 1 协议**：图中提到的协议（如蓝牙智能、Wi-Fi 或 IEEE 802.15.4）用于设备与网关之间的物理连接，它们属于低速率无线个人区域网络 (LR-WPAN)。

4. 应用服务提供商 (Application Service Provider) :

- 网关处理完数据后，会通过互联网（IPv4/IPv6）将数据发送到云端的应用服务提供商，服务提供商负责存储、分析和处理这些数据。

总结:

这张图解释了在 **设备到网关模型** 中，设备首先通过不同的协议栈与本地网关通信，网关起到数据中转和处理的作用，然后通过标准网络协议（如 IPv4 或 IPv6）与远程的应用服务提供商（云端）通信。这种模型使得设备不需要直接与云通信，而是通过网关进行数据汇总和转发，简化了设备的设计并提高了能效。

1.7 TLS 和 DTLS 的区别

这段话讨论了两种重要的网络安全协议：**传输层安全协议 (TLS)** 和 **数据报传输层安全协议 (DTLS)**。它们都用于为网络通信提供加密和安全保障，但应用场景和设计略有不同。以下是详细解析：

1. Transport Layer Security (TLS)

定义：

- **TLS (Transport Layer Security)** 是一种用于计算机网络中提供安全通信的加密协议。它的主要目标是确保在两个设备（通常是客户端和服务端）之间传输的数据的**保密性**、**完整性**和**身份验证**。

功能：

- **保密性**: 使用加密技术，确保数据在传输过程中不会被窃取或截获。
- **完整性**: 确保数据在传输过程中没有被篡改。如果数据被修改，接收方能够检测到这种篡改。
- **身份验证**: 确保通信的两方是合法的，防止中间人攻击（Man-in-the-Middle Attack）。

应用场景：

- **HTTPS**: TLS 在确保网页传输安全（即 HTTPS）中应用最广泛。HTTPS 是通过 HTTP 协议的加密版本，使用 TLS 来保护数据传输。
- **电子邮件**: 邮件客户端和服务端之间的通信也可以使用 TLS 来确保邮件内容和用户凭证的安全。
- **即时消息 (Instant Messaging)** 和 **VoIP**（网络语音传输）: 这些实时通信的应用也可以利用 TLS 来加密通信内容，防止窃听或篡改。

工作原理：

- **握手过程**: 当客户端与服务端之间开始通信时，会首先进行一次 "握手" 过程。在此过程中，客户端和服务端会交换加密密钥和认证证书，以便建立一个加密的通信通道。
- **对称加密和非对称加密结合**: TLS 使用非对称加密（如 RSA）进行密钥交换，然后使用对称加密（如 AES）对数据进行加密，以提高效率。

2. Datagram Transport Layer Security (DTLS)

定义:

- **DTLS (Datagram Transport Layer Security)** 是基于 TLS 协议设计的，用于**数据报 (Datagram) **传输的加密协议。它专门**为非连接、无序传输的网络通信而设计**，确保这些通信也具有与 TLS 类似的安全特性。

功能:

- **与 TLS 类似的安全性:** DTLS 提供与 TLS 相同的安全性功能，包括加密、数据完整性和身份验证。
- **支持无连接传输:** DTLS 设计用于**无连接协议**，如 **UDP (用户数据报协议) **。与 **TCP** (传输控制协议) 不同，UDP 不提供可靠的、有序的传输，因此 DTLS 必须适应这些特性，确保在这种环境下的安全性。

应用场景:

- **实时应用:** DTLS 广泛用于需要低延迟、实时通信的应用，如 **视频流**、**在线游戏** 和 **VoIP (网络语音传输) **。这些应用通常使用 UDP，因为它传输速度快，延迟低，但没有 TCP 的可靠性保障。
- **物联网 (IoT):** DTLS 在物联网设备中也有应用，**因为很多 IoT 设备使用低功耗、低带宽的通信方式 (如 UDP) ，但仍然需要加密通信。**

工作原理:

- **适应无连接性:** DTLS 保留了 TLS 的**握手和加密机制**，但增加了处理 UDP 无连接和无序传输的能力。例如，DTLS 可以处理由于 UDP 数据包丢失、重复或顺序错误而产生的问题。

TLS 和 DTLS 的区别

特性	TLS	DTLS
基础协议	TCP（连接导向，可靠传输）	UDP（无连接，非可靠传输）
数据传输模式	可靠、有序的传输	无连接、无序传输，允许丢包和乱序
应用场景	网页传输、电子邮件、即时消息、VoIP	视频流、在线游戏、实时应用、物联网
安全功能	提供加密、数据完整性和身份验证	提供类似 TLS 的安全性，适应 UDP 特性
延迟	较高，由于 TCP 的握手和确认机制	较低，适合低延迟的实时应用

总结

- **TLS** 是一种广泛使用的加密协议，主要用于 TCP 协议上，提供可靠的数据传输、安全加密和身份验证，常见于 HTTPS、邮件通信和即时消息中。
- **DTLS** 则是专门为无连接的 UDP 设计的加密协议，保留了 TLS 的安全特性，但能够适应无连接、无序传输的特性，适用于低延迟的实时应用（如视频流、VoIP）和物联网通信。

这两个协议都是网络安全的重要组成部分，确保了我们在互联网通信中的数据安全和隐私保护。

1.8 SmartThings Hub

SmartThings Hub 的工作原理及其功能：

- **SmartThings Hub** 是一个独立的网关设备，**内置 Z-Wave 和 Zigbee 无线收发器**，用于与这两类设备进行通信。
- Hub 内部包含 **Z-Wave** 和 **Zigbee** 的无线天线，能够无线连接和控制这些协议的设备。
- 作为 **Z-Wave** 和 **Zigbee** 网络的主控制器，Hub 负责管理和协调这些设备。
- 通过连接到 **SmartThings 云服务**，用户可以使用智能手机应用程序，通过互联网远程访问和控制设备。

总结来说，**SmartThings Hub** 是一种可以同时控制 **Z-Wave** 和 **Zigbee** 设备的主控制器，它通过互联网连接到云服务，使用户能够通过手机远程管理家中的智能设备。

1.9 UWA（西澳大学）Capstone 项目 & Device-to-Gateway Model : Non-invasive monitoring of Elderly

这张图片展示了**UWA（西澳大学）Capstone 项目**，主题是**非侵入性地监测老年人**的健康与安全。图中的信息描述了该项目的**目标**、**范围**和**不在范围内**的内容。下面是具体的解释：

项目目标（Objectives）：

- a. **使用当前的 SmartThings 传感器：**项目计划利用现有的 SmartThings 传感器设备来监测老年人。
- b. **自动检测风险时刻：**通过传感器自动识别可能的风险情况，例如老年人摔倒或其它危险。
- c. **构建基于 Web 的仪表盘：**开发一个基于 Web 的控制面板，用户可以通过它查看数据和设备状态。
- d. **显示实时和历史数据：**提供显示传感器采集的实时和过去数据的功能。
- e. **可配置的规则用于风险检测：**允许用户设定和配置检测风险时刻的规则。
- f. **风险时刻的警报：**当系统检测到潜在的危险时，发出警报通知。
- g. **实施访问控制：**为系统增加访问权限管理，确保只有授权用户能够访问和操作系统。

项目范围（In Scope）：

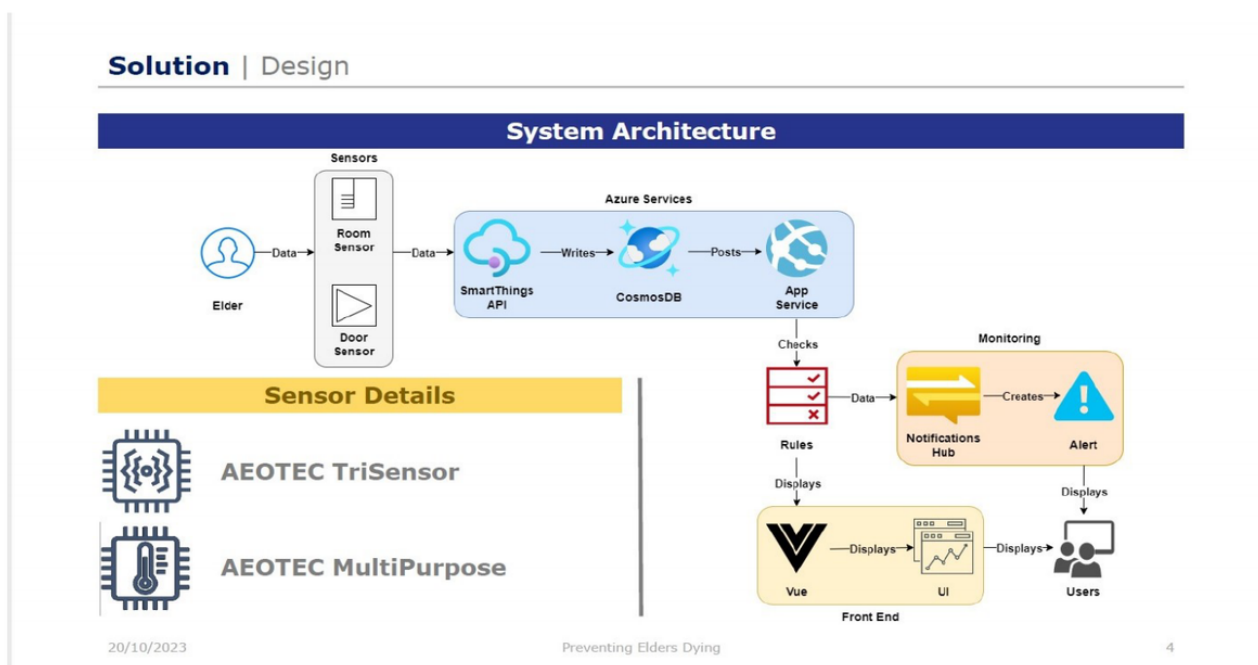
- **独立生活的老年人：**项目关注的是那些独立生活的老年人，旨在非侵入性地监测他们的健康和安全。
- **数据收集和存储：**该项目涉及到对传感器数据的收集和存储，以便后续分析和使用。

不在范围内的内容（Out of Scope）：

- **风险检测 vs 风险预防：**项目只关注**检测风险**（如摔倒），而不是预防风险（如提前防止摔倒）。
- **传感器和传感器位置的设计与配置：**项目不涉及传感器的具体设计或位置部署，使用的是现有的 SmartThings 传感器。

总结：

这个项目旨在使用现有的 SmartThings 传感器，自动监测独立生活的老年人的风险时刻（如摔倒），并通过 Web 仪表盘显示实时和历史数据。用户可以设定检测规则，并在检测到风险时收到警报。项目的重点是**风险检测**而非预防，也不涉及传感器的部署细节。



Aeotec Tri Sensor : Light Sensor. Motion Sensor. Temperature Sensor.

Aeotec Multipurpose Sensor (Works with SmartThings) enables you to receive alerts when a door or window is opened or closed. In addition, you'll be able to set connected smart devices, such as lights to power on and off as you open doors, windows or cabinets.

这张图展示了一个**系统架构 (System Architecture)**，用于监控老年人的非侵入性解决方案。系统使用了不同的传感器、云服务和前端应用来监控老年人的活动，并通过通知中心发送警报。以下是图中关键元素的总结：

1. 系统架构

传感器 (Sensors):

- 系统中使用了房间传感器和门传感器来采集老年人的活动数据。
- 传感器会将数据发送给 **SmartThings API**，这是一个用于连接智能家居设备和传感器的接口。

Azure 服务 (Azure Services):

- SmartThings API** 将传感器数据写入 **CosmosDB**（一个 NoSQL 数据库）用于存储。
- 数据存储后，**App Service** 会处理这些数据，并根据预设的规则进行检查。

- **监控模块 (Monitoring):**

- 当检测到某些异常情况时，**通知中心 (Notifications Hub)** 会触发警报，并通过 **警报系统 (Alert)** 向用户发送通知。
- 这些通知可以通过前端应用显示给用户。

2. 传感器详细信息 (Sensor Details):

- **AEOTEC TriSensor:**

- 该传感器能够检测**光线、运动和温度**，用于监控房间内老年人的活动。

- **AEOTEC Multipurpose Sensor:**

- 该传感器用于检测**门窗的开关状态**，并在检测到门或窗被打开或关闭时发送警报。此外，它还可以与其他智能设备（如灯光）集成。

3. 用户界面 (Front End UI):

- 前端显示通过 **Vue.js** 框架构建，用户可以在界面中查看传感器的实时数据、历史记录、风险警报等信息。
- 用户可以通过 Web 应用或其他设备来监控老年人的活动和接收通知。

总结:

这个系统架构使用 **SmartThings API** 与 **Azure 云服务** 相结合，通过房间和门传感器监控老年人的生活活动。当检测到异常情况时，系统会触发警报并通过前端应用通知用户。整个系统实现了数据的采集、存储、处理和展示，提供了对老年人安全的全面监控。

1.10 Back-End Data-Sharing Model

这段话解释了**后端数据共享模型 (Back-End Data-Sharing Model)** 的概念。主要内容如下:

- **后端数据共享模型** 扩展了传统的 **设备到云通信模型**，允许物联网 (IoT) 设备和传感器数据被授权的第三方访问。
- 在该模型下，用户可以将从云服务中导出的智能设备数据与其他来源的数据结合起来，进行分析和处理。

- 此外，数据还可以进一步发送到其他服务进行汇总和更深入的分析。

总结：

后端数据共享模型允许物联网数据被第三方访问和使用，支持数据的导出、汇总、分析和整合。这种方式扩展了设备与云的通信，提供了更多的数据共享和处理可能性。

1.11 CoAP & OAuth

这段话讨论了**受限应用协议 (CoAP)** 和其在物联网中的应用：

- **CoAP（受限应用协议）** 是一种专门为受限设备设计的互联网应用协议（定义于 **RFC 7228**）。它使这些资源受限的设备能够与更广泛的互联网进行通信，使用类似于互联网其他应用的协议。
- 随着互联网协议套件（如 IP）**越来越多地应用于小型设备**，这些设备往往受限于功耗、内存和处理能力，因此创建了所谓的**受限节点网络（Constrained-Node Networks）**。

总结：

CoAP 是为资源受限的物联网设备设计的协议，使它们能够高效地与互联网进行通信，并适应受限节点网络中的设备，解决了低功耗、内存和计算能力有限的问题。

这段话介绍了 **OAuth** 的基本概念和应用：

- **OAuth 是一种开放标准**，专用于**访问授权**。它允许互联网用户向网站或应用程序授权访问他们在其他网站上的信息，而无需分享密码。
- 这种机制被 **Google**、**Facebook**、**Microsoft** 和 **Twitter** 等公司广泛使用，用户可以通过 OAuth 授权第三方应用或网站访问其账户信息，而无需直接提供登录凭证。

总结：

OAuth 是一种安全的授权机制，使用户能够**在不透露密码的情况下**，允许第三方应用访问他们的在线账户信息。这种方式被多个大型互联网公司广泛采用。

1.12 Key Component

- a. **传感器/边缘计算 (Sensors/Edge Computing)**：传感器收集数据，边缘计算可以在靠近数据源的地方进行处理，减少数据传输的延迟和带宽需求（可能使用也可能不使用）。
- b. **连接性 (Connectivity)**：设备之间以及设备与平台之间的网络连接，确保数据能够有效传输。
- c. **平台 (Platform)**：物联网平台用于管理、存储和处理从传感器采集的数据。
- d. **分析 (Analytics)**：对收集的数据进行分析，生成有价值的见解或行动方案。
- e. **用户界面 (User Interface)**：提供给用户的交互界面，用于查看、控制和管理设备或系统的操作。

总结：

物联网系统的五个核心组成部分包括：传感器或边缘计算、网络连接、平台管理、数据分析以及用户界面，每个部分都在系统的运作中发挥重要作用。

三个关键要求：ARV

- a. **可用性 (Availability)**：系统或服务能够随时可用，确保用户需要时能够访问和使用。
- b. **可靠性 (Reliability)**：系统在运行时能持续稳定地工作，减少故障和错误的发生。
- c. **可行性 (Viability)**：系统设计和解决方案在技术上和商业上是可行的，能够长期持续运行并产生效益。

总结：

系统设计的关键要求包括可用性（随时可用）、可靠性（稳定工作）和可行性（技术和商业上的可持续性）。

1.13 Frequency Band

这张图描述了**无线通信系统中的频段 (Frequency Band)**，以及不同频段的使用情况，分为**有许可证频段 (Licensed)**和**无许可证频段 (Unlicensed)**两种。

Licensed (有许可证的频段)：

- 这些频段需要许可才能使用，通常是由政府或相关机构分配。

- 主要用于需要基础设施的传统无线网络，如：
 - **Cellular（蜂窝网络）**：如4G、5G等移动通信网络。
 - **Paging（寻呼系统）**：用于传递短信息的系统。
 - **Fixed Wireless（固定无线通信）**：在固定位置之间传输数据的无线通信，如无线电链路。
 - **Satellite（卫星通信）**：通过卫星传输数据，用于远距离通信。

Unlicensed (无许可证的频段):

- 这些频段不需要许可就可以使用，**设备可以自组织或点对点通信**，常见于短距离无线设备。
- 主要类型包括：
 - **Cordless（无绳电话）**：用于室内短距离的无线通话设备。
 - **WLAN（无线局域网）**：如 Wi-Fi 等局域网技术。
 - **Bluetooth, UWB（超宽带）**：用于短距离通信的技术，适用于设备间的数据传输。
 - **M2M（机器对机器通信）**：物联网中设备间的通信。
 - **PAN（个人区域网）**：如**蓝牙和 ZigBee** 等，适用于个人设备之间的近距离通信。

总结：

这张图对比了有许可证和无许可证的无线通信频段，分别列出了在这两种频段下常用的通信技术。有许可证的频段用于更大规模、需要基础设施支持的通信系统，而无许可证频段则适合自组织或短距离的无线通信设备。

这段话指出了**通过无线信道传输数据时可能遇到的问题**，并给出相应的教训：**EUL**

- **Error-prone（易出错）**：无线信道中的数据传输容易受到干扰，导致数据错误。
- **Unreliable（不可靠）**：无线信道的连接不如有线连接稳定，信号可能会受到阻碍或丢失，导致通信中断。
- **Latency issues（延迟问题）**：无线通信通常会遇到延迟，特别是在信号弱或干扰多的情况下，数据传输的响应时间可能变长。

结论：

- **教训**：无线信道需要****积极的管理****。也就是说，为了减少这些问题，需要采用某些管理方法或技术来优化无线通信，确保数据传输尽可能可靠和高效，例如使用错误检测与纠正、信号增强和优化延迟的技术。

总结：

通过无线信道传输数据容易遇到错误、不可靠和延迟等问题，因此必须通过积极的管理手段来优化无线通信性能。

1.14 工业、科学和医疗（ISM）

这段话介绍了**工业、科学和医疗（ISM）频段**的用途和特点：

- **ISM 频段**是国际上为非电信用途的工业、科学和医疗设备保留的无线电频段。这些频段中的无线电频率用于产生射频能量，但不是用于通信。
-
- **应用示例：**ISM 频段的典型应用包括**微波炉**和**医疗透热机**（用于物理治疗的设备），这些设备通过无线电波进行能量传输。
- **通信设备的限制：**在这些频段运行的通信设备必须能够**容忍由 ISM 设备产生的干扰**，而且使用这些频段进行通信的用户**没有法律上的干扰保护**。也就是说，ISM 设备可能会产生干扰，但通信设备的用户不能依赖法规要求免受这种干扰。

ISM 频段是为工业、科学和医疗用途保留的频段，尽管通信设备可以在这些频段中工作，但它们必须承受 ISM 设备可能带来的干扰，且无法获得干扰保护。

适合大规模部署 IoT 设备：

1. **900-928 MHz 频段：**这是 ISM 频段之一，适合低功耗、远距离的 IoT 通信。
2. **2.4 GHz 和 5.7 GHz 频段：**这些频段也属于 ISM 频段，广泛应用于 Wi-Fi、蓝牙等短距离通信技术中。
3. **低频段：**一些较低频率的频段也对 IoT 通信具有吸引力，因为它们支持更远的通信距离和较低的功耗。
4. **免许可证频段：**这些频段是**免许可证的**，允许大量的 IoT 设备无需支付频段使用费用即可部署，降低了通信成本。

1.15 802.11 工作组（负责制定 Wi-Fi 标准的组织） | 不同频段的区别

802.11 工作组（负责制定 Wi-Fi 标准的组织）当前记录了 Wi-Fi 使用的**五个不同的频段**，这些频段是：

1. **2.4 GHz 频段**：这是最常见的 Wi-Fi 频段之一，广泛应用于家庭和企业网络中，适合短距离通信。
2. **3.6 GHz 频段**：这个频段在一些地区用于专用无线网络或商业用途。
3. **4.9 GHz 频段**：主要用于公共安全无线网络等特定用途。
4. **5 GHz 频段**：这是另一个常用的 Wi-Fi 频段，支持更高的数据传输速率，通常比 2.4 GHz 的干扰更少，但信号覆盖范围较短。
5. **5.9 GHz 频段**：这个频段逐渐应用于车辆通信和其他先进的无线应用中。

总结：

802.11 工作组定义了 Wi-Fi 在 2.4 GHz 到 5.9 GHz 范围内的五个不同频段，适用于不同的通信需求和应用场景。这些频段为 Wi-Fi 技术的广泛应用提供了基础支持。

这段话解释了在**2.4 GHz 频段**变得越来越拥挤的情况下，许多用户转向使用**5 GHz ISM 频段**的原因及相关限制：

- 2.4 GHz 频段的拥挤**：由于越来越多的设备（包括 Wi-Fi、微波炉等）使用 2.4 GHz 频段，导致这个频段变得拥挤，出现干扰问题。
- 5 GHz 频段的优势**
 - **更多频谱**：5 GHz 频段提供了更多的频带空间，减少了设备间的干扰。
 - **较少干扰**：相较于 2.4 GHz，5 GHz 频段并没有被如此广泛地使用，尤其是 Wi-Fi 和家电设备，这使得其相对较少干扰。
- 限制**：尽管 5 GHz 频段有优势，但并非所有 5 GHz 频段的 Wi-Fi 信道都在**ISM 免许可证频段**内。某些频段不属于 ISM 频段，受到法律或技术上的使用限制，因此在这些频率下的操作可能会有各种限制。

总结：

由于 2.4 GHz 频段过于拥挤，许多用户选择使用 5 GHz 频段，因为它提供了更多频谱和较少的干扰。但并非所有 5 GHz 信道都在免许可证的 ISM 频段内，因此这些信道的使用受到了不同的限制。

这段话解释了在 **2.4 GHz 频段** 变得越来越拥挤的情况下，许多用户转向使用 **5 GHz ISM 频段** 的原因及相关限制：

1. **2.4 GHz 频段的拥挤**：由于越来越多的设备（包括 Wi-Fi、微波炉等）使用 2.4 GHz 频段，导致这个频段变得拥挤，出现干扰问题。
2. **5 GHz 频段的优势**：
 - **更多频谱**：5 GHz 频段提供了更多的频带空间，减少了设备间的干扰。
 - **较少干扰**：相较于 2.4 GHz，5 GHz 频段并没有被如此广泛地使用，尤其是 Wi-Fi 和家电设备，这使得其相对较少干扰。
3. **限制**：尽管 5 GHz 频段有优势，但并非所有 5 GHz 频段的 Wi-Fi 信道都在 **ISM 免许可证频段** 内。某些频段不属于 ISM 频段，受到法律或技术上的使用限制，因此在这些频率下的操作可能会有各种限制。

总结：

由于 2.4 GHz 频段过于拥挤，许多用户选择使用 5 GHz 频段，因为它提供了更多频谱和较少的干扰。但并非所有 5 GHz 信道都在免许可证的 ISM 频段内，因此这些信道的使用受到了不同的限制。

1.16 3GPP

这段文字介绍了 **3GPP（第三代合作伙伴计划）** 的背景和目标：

- **3GPP** 是由多个电信协会组成的合作组织，称为**组织合作伙伴**。
- 其最初的目标是制定一个全球通用的**第三代 (3G) 移动通信系统规范**，基于改进后的**全球移动通信系统 (GSM)** 规范。
- 该规范属于**国际电信联盟 (ITU)** 的**国际移动通信-2000 (IMT-2000)** 项目范围内。

总结：

3GPP 是一个由电信协会组成的合作组织，旨在基于 GSM 规范制定全球适用的 3G 移动通信系统规范，属于 ITU 的 IMT-2000 项目的一部分。

这段文字解释了 **3GPP** 的作用范围随着时间的推移有所扩展，涵盖了更多的标准开发和维护工作，包括：

a. 2G 和 2.5G 标准：

- 维护 **GSM** 及相关的 2G 和 2.5G 标准，如 **GPRS**（一种面向数据包的移动数据服务）和 **EDGE**（GSM 的增强数据速率）。

b. 3G、4G 和 5G 标准：

- 开发和维护与 **3G** 相关的标准，以及 **4G** 标准（如 **LTE Advanced** 和 **LTE Advanced Pro**），并扩展到 **5G** 标准的开发。

总结：

3GPP 的职责不仅限于 3G 标准，后来还扩展到 2G、2.5G、4G 和 5G 标准的开发和维护，包括 GPRS、EDGE 和 LTE 相关的技术。

2. Lecture Quiz

Quiz Questions (MCQs)

1. What are the core components of IoT?

- A. Sensors, Connectivity, Platform, Analytics, and User Interface
- B. Sensors, Network, Platform, Analytics, and Security
- C. Devices, Connectivity, Storage, Analytics, and Security
- D. Connectivity, Devices, AI, Data, and Storage
- **Answer:** A. Sensors, Connectivity, Platform, Analytics, and User Interface

解析: IoT 主要由五个核心组件组成，分别是传感器、连接性、平台、数据分析以及用户界面 (2024_Sem02_IoT_Lecture0...)

2. What frequency bands are used by LoRa?

- A. 169 MHz, 433 MHz, 868 MHz, 915 MHz
- B. 2.4 GHz, 5 GHz
- C. 700 MHz, 1.2 GHz, 3.5 GHz
- D. 433 MHz, 915 MHz, 2.4 GHz

- **Answer:** A. 169 MHz, 433 MHz, 868 MHz, 915 MHz

解析: LoRa 是一种低功耗广域网 (LPWAN) 技术, 使用不同地区的非许可频段进行通信 (2024_Sem02_IoT_Lecture0...).

3. What does RPMA stand for in IoT communications?

- A. Random Positioning Multiple Access
- B. Reduced Power Multiple Access
- C. Random Phase Multiple Access
- D. Radio Power Management Access

- **Answer: C. Random Phase Multiple Access**

解析: RPMA 是一种为 IoT 设备设计的低功耗通信技术, 支持大量设备在高密度区域内进行通信 (2024_Sem02_IoT_Lecture0...).

4. Which wireless technology is often used for home automation and allows for low-energy communication between appliances?

- A. Wi-Fi
- B. LoRa
- C. Z-Wave
- D. Bluetooth

- **Answer: C. Z-Wave**

解析: Z-Wave 是一种专门用于家庭自动化的无线通信技术, 具有低功耗、短距离通信等特点 (IoT_Lecture02_2024_sem02).

5. What are the three key requirements for IoT connectivity?

- A. Scalability, Security, and Flexibility
- B. Availability, Reliability, and Viability
- C. Speed, Range, and Power Consumption
- D. Cost, Speed, and Security

- **Answer: B. Availability, Reliability, and Viability**

解析: IoT 设备的连接需要确保高可用性、可靠性和可行性, 特别是在大规模部署中 (IoT_Lecture04_2024_sem0...)(2024_Sem02_IoT_Lecture0...).

6. What are the technical challenges for IoT?

- A. Power, Speed, Interoperability, and Scalability
- **B. Security, Sensors, Power Consumption, Communication Technologies**
- C. Connectivity, Power, AI, and Big Data
- D. Data Analysis, Networking, Power, and AI

- **Answer:** B. Security, Sensors, Power Consumption, Communication Technologies

解析: IoT 技术面临的主要技术挑战包括传感器、功耗、安全与隐私、通信技术等 (IoT_Lecture04_2024_sem0...)(IoT_Lecture02_2024_sem02)。

7. What does **3GPP** stand for and what is its role in IoT?

- A. 3rd Generation **Partnership Project**; It develops **cellular IoT standards**
- B. 3rd Generation Platform Project; It develops LPWAN standards
- C. 3rd Generation Protocol Platform; It ensures IoT data security
- D. 3rd Generation Privacy Partnership; It works on IoT privacy standards

- **Answer:** A. 3rd Generation Partnership Project; It develops cellular IoT standards

解析: 3GPP 是一个制定移动通信标准的组织, 推动了 **NB-IoT** 等蜂窝物联网标准的发展 (IoT_Lecture04_2024_sem0...)(2024_Sem02_IoT_Lecture0...).

8. What are **LPWANs**, and name an example of LPWAN technology?

- A. Long Power Wireless Area Networks; LoRa
- **B. Low Power Wide Area Networks; Sigfox**
- C. Low Packet Wide Area Networks; Zigbee
- D. Long Packet Wireless Access Network; Wi-Fi

- **Answer:** B. Low Power Wide Area Networks; Sigfox

解析: LPWAN 是专为低功耗、长距离通信设计的网络技术, **Sigfox 和 LoRa 是其代表性技术** (2024_Sem02_IoT_Lecture0...).

9. Which communication protocol allows direct communication between devices without an intermediary?

- A. Device-to-Gateway Communication
- B. Device-to-Device Communication
- C. Device-to-Cloud Communication
- D. Device-to-Backend Communication

- **Answer:** B. Device-to-Device Communication

解析: 设备到设备 (D2D) 通信允许设备之间直接通信, 而不需要中介服务器 (IoT_Lecture02_2024_sem02)。

10. What is **Zigbee** used for, and what is its frequency range?

- A. High-speed data transmission; 5 GHz
- B. Short-range communication; 2.4 GHz ISM band
- C. Long-distance communication; 868 MHz
- D. Personal communication; 1.2 GHz

- **Answer:** B. Short-range communication; 2.4 GHz ISM band

解析: Zigbee 主要用于短距离、低功耗通信，适合智能家居等应用，运行在 2.4 GHz 频段 (IoT_Lecture02_2024_sem02)。

11. What are the **societal challenges of IoT?**

- A. Privacy concerns, AI development, Big Data growth
- B. Privacy fears, surveillance concerns, and security issues
- C. AI dominance, automation job loss, ethical debates
- D. Data storage, AI control, and political issues
- **Answer:** B. Privacy fears, surveillance concerns, and security issues

解析: IoT 带来了社会问题，尤其是关于隐私、监控和安全方面的担忧 (IoT_Lecture02_2024_sem02)。

12. What is the **primary purpose of edge computing in IoT?**

- A. To store IoT data remotely in the cloud
- **B. To perform computations closer to the data source**
- C. To provide centralized data management
- D. To increase storage capacity for IoT devices
- **Answer:** B. To perform computations closer to the data source

解析: 边缘计算的目的是减少数据传输延迟，并通过在设备附近进行计算来减少带宽使用 (2024_Sem02_IoT_Lecture0...).

13. What are some of the **legal challenges posed by IoT devices?**

- A. Ownership of data, regulations on cloud computing, government control
- B. Cross-border data flow, data misuse, and surveillance issues
- C. Device standardization, IP control, network access issues
- D. Legal device usage, proper cloud implementation, privacy settings
- **Answer:** B. Cross-border data flow, data misuse, and surveillance issues

解析: 物联网带来了许多法律挑战，如跨国数据流动、数据滥用和监控相关问题 (IoT_Lecture02_2024_sem02)。

14. What are the **key use cases for NB-IoT technology?**

- A. High-speed video streaming, real-time gaming, social media
- B. Low-cost, long-battery-life, and high-connection-density applications
- C. Large-scale AI data processing, machine learning algorithms
- D. Long-distance voice communication, high data speed, video calls

- **Answer:** B. Low-cost, long-battery-life, and high-connection-density applications
解析: NB-IoT 主要用于低功耗、长电池寿命和高密度连接的场景，如智能抄表、资产追踪 (2024_Sem02_IoT_Lecture0...).

15. Which technology is employed by smart vacuum cleaners to enable their operation in IoT?

- A. Cloud Computing
- B. Sensors and Connectivity Technology
- C. Artificial Intelligence
- D. Machine Learning Algorithms
- **Answer:** B. Sensors and Connectivity Technology
解析: 智能吸尘器依赖传感器和网络连接技术来完成其物联网

Quiz Questions:

1. What are the core components of IoT? SPAU

- Sensors, Connectivity, Platform, Analytics, and User Interface(2024_Sem02_IoT_Lecture0...).

2. What frequency bands are used by LoRa?

- 169 MHz, 433 MHz, 868 MHz (Europe), 915 MHz (North America) (2024_Sem02_IoT_Lecture0...).

3. What does RPMA stand for in IoT communications?

- Random Phase Multiple Access(2024_Sem02_IoT_Lecture0...).

4. Which wireless technology is often used for home automation and allows for low-energy communication between appliances?

- Z-Wave(IoT_Lecture02_2024_sem02).

5. What are the three key requirements for IoT connectivity?

- Availability, Reliability, and Viability(IoT_Lecture04_2024_sem0...)
(2024_Sem02_IoT_Lecture0...).

6. What are the technical challenges for IoT?

- Sensors, Power Consumption, Security & Privacy, Data Analytics, Communication Technologies, Interoperability/Standards, Development Challenges(IoT_Lecture04_2024_sem0...)(IoT_Lecture02_2024_sem02).

7. What does 3GPP stand for and what is its role in IoT?

- The 3rd Generation Partnership Project, which develops standards for cellular IoT including NB-IoT(IoT_Lecture04_2024_sem0...)(2024_Sem02_IoT_Lecture0...).
8. **What are LPWANs and name an example of LPWAN technology?**
- Low Power Wide Area Networks; examples include LoRa and Sigfox(2024_Sem02_IoT_Lecture0...).
9. **Which communication protocol allows direct communication between devices without an intermediary?**
- Device-to-Device Communication(IoT_Lecture02_2024_sem02).
10. **What is Zigbee used for, and what is its frequency range?**
- Zigbee is used for low-power, low-data-rate, close-proximity communications (e.g., smart homes) and operates primarily in the 2.4 GHz ISM band(IoT_Lecture02_2024_sem02).
11. **What are the societal challenges of IoT?**
- Privacy fears, surveillance concerns, and security issues(IoT_Lecture02_2024_sem02).
12. **What is the primary purpose of edge computing in IoT?**
- To process data closer to where it is generated, reducing latency and saving bandwidth(2024_Sem02_IoT_Lecture0...).
13. **What are some of the legal challenges posed by IoT devices?**
- Cross-border data flow, data misuse, and issues related to surveillance(IoT_Lecture02_2024_sem02).
14. **What are the key use cases for NB-IoT technology?**
- Low-cost, long-battery-life, and high-connection-density IoT applications(2024_Sem02_IoT_Lecture0...).
15. **What technology is employed by smart vacuum cleaners to enable their operation in IoT?**
- Sensors and connectivity technology(2024_Sem02_IoT_Lecture0...).
16. **Which wireless standard is specifically designed for personal area networks and operates in the ISM band?**
- IEEE 802.15.4 (Zigbee)(IoT_Lecture02_2024_sem02).
17. **What is the primary focus of cloud computing in IoT applications?**
- To process, manage, and store data generated by IoT devices(2024_Sem02_IoT_Lecture0...).
18. **What type of networks does the Bluetooth protocol employ and what is its typical transmission range?**

- UHF radio waves in the ISM band, with a typical range of up to 10 meters (33 feet) (IoT_Lecture02_2024_sem02).
19. What is the approximate range of Sigfox technology in urban and rural areas?
- 10 km in urban areas, 40 km in rural areas(2024_Sem02_IoT_Lecture0...).
20. Which component of IoT is responsible for presenting data to end-users in an appealing manner?
- The User Interface(2024_Sem02_IoT_Lecture0...).

3. 讲课内容字幕大纲

以下是对这五篇文档的详细总结：

第一篇文档：CITS5506 - 12 Aug 20_01.txt

- **课程信息：**
 - 课程为物联网（Internet of Things, IOT），在nal land上学习，遵循西澳大学的版权规定。
 - 授课教师为Atif，邮箱为[具体邮箱地址]，咨询时间为周一课程结束后12:00 - 13:00，地点在计算机科学楼G06a。
- **课程安排：**
 - 共八周课程，包含理论和实践部分，有实验课和项目作业。
 - 项目组由教师分配，每组会有专属的MS Teams私人频道进行交流。
 - 学生需填写技能调查表单，帮助教师平衡组队。
- **项目相关：**
 - 项目选题需具有一定影响力和实用性，包含传感、通信、计算、数据分析或行动等IOT组件。
 - 学生需提交项目提案，包括短标题、200字左右的描述，阐述项目内容和实现方式。
 - 每个小组有50美元预算用于购买不在西澳大学的传感器等物品，需在项目提案中注明传感器、网站、成本和交付时间等信息。
 - 项目评估包括项目提案（占15%）、项目报告（占35%）、项目原型和演示（占30%）以及项目展示（占20%）。
 - 教师会根据项目提案给出反馈，学生可根据反馈修改项目。
 - 项目成绩可能因小组成员的参与度和贡献不同而有所差异，通过反馈和自评进行评估。
- **实验相关：**

- 实验课使用Ardo、raspberry pi、Laura Communication等硬件进行，学生需在实验前阅读实验指导。
- 实验成绩根据实验操作和回答问题情况评定。
- 课程共有五位实验指导教师，分别为Julian Zheng、Asad、Ning Liu、Frank和F donkin，还有实验技术员Andy提供支持。
- **考试相关：**
 - 9月9日有一小时的课堂测试，占总成绩的20%，测试内容为课程讲授的理论知识。
 - 期末考试占总成绩的40%。

第二篇文档：CITS5506 - 19 Aug 20_02.txt

- **项目相关：**
 - 项目应具有一定的影响力和实用性，如解决实际问题、改进现有流程或提供新的服务等。
 - 项目应包含IOT的五个组件：传感器、通信、计算（可以是边缘计算）、平台（包括数据存储、分析和可视化）和行动（如控制设备、发送警报等）。
 - 学生需在项目提案中明确项目目标、技术方法、预期成果和时间表等。
 - 教师会根据项目提案的质量、可行性和创新性等给予反馈和建议。
 - 项目评估包括项目提案（占15%）、项目报告（占35%）、项目原型和演示（占30%）以及项目展示（占20%）。
 - 项目成绩可能会受到小组成员的贡献和参与度的影响，通过反馈和自评进行评估。
- **工具使用：**
 - 允许使用AI工具，但必须在项目中予以说明和承认。
 - 可以参考已有的IOT项目，但需要进行创新和改进，避免简单复制。
- **IOT应用架构：**
 - IOT应用架构通常包括感知层、网络层和应用层。
 - 感知层包含各种传感器，用于采集物理世界的信息。
 - 网络层负责将传感器数据传输到服务器或云端，通信技术包括Laura、Wi - Fi、蓝牙、NBIOT等。
 - 应用层对数据进行存储、分析和可视化，以支持决策和行动。
 - MQTT是一种常用的消息传输协议，适用于IOT设备的通信。
- **案例分析：**
 - 以Beehive monitoring项目为例，介绍了该项目的背景、目标、技术方案和成果。

- 该项目使用温度、湿度、压力、气体传感器、加速度计、麦克风和称重传感器等监测蜂箱状态。
- 通过机器学习算法估计蜂箱重量，替代昂贵的称重传感器。
- 项目采用Laura和NB-IoT进行通信，数据存储在云平台上，进行分析和展示。
- **其他IoT项目：**
 - 介绍了一些其他IoT项目，如Smart Pet Feeder、Smart Street Lights、Smart Surfing Weather Station、Smart Watering System、Smart Desk Occupancy、Bushfire Early Warning System等。
 - 这些项目涉及不同的应用场景和技术，展示了IoT的多样性和实用性。

第三篇文档：CITS5506 - 26 Aug 20_03.txt

- **课程信息：**
 - 课程为物联网（IoT），学习地点在nalland，遵循西澳大学版权规定。
 - 教师为Atif，通过邮箱[具体邮箱地址]联系，办公地点在计算机科学楼G06a，咨询时间为周一12:00 - 13:00。
- **课程安排：**
 - 课程包含理论和实践部分，有实验课和项目作业。
 - 项目组由教师分配，每组有专属的MS Teams私人频道进行交流。
 - 学生需填写技能调查表单，帮助教师平衡组队。
- **项目相关：**
 - 项目选题应具有一定影响力和实用性，包含传感、通信、计算、数据分析或行动等IoT组件。
 - 学生需提交项目提案，包括短标题、200字左右的描述，阐述项目内容和实现方式。
 - 每个小组有50美元预算用于购买不在西澳大学的传感器等物品，需在项目提案中注明传感器、网站、成本和交付时间等信息。
 - 项目评估包括项目提案（占15%）、项目报告（占35%）、项目原型和演示（占30%）以及项目展示（占20%）。
 - 教师会根据项目提案给出反馈，学生可根据反馈修改项目。
 - 项目成绩可能因小组成员的参与度和贡献不同而有所差异，通过反馈和自评进行评估。
- **实验相关：**
 - 实验课使用Arduo、raspberry pi、Laura Communication等硬件进行，学生需在实验前阅读实验指导。
 - 实验成绩根据实验操作和回答问题情况评定。

- 课程共有五位实验指导教师，分别为Julian Zheng、Asad、Ning Liu、Frank和F donkin，还有实验技术员Andy提供支持。
- **考试相关：**
 - 9月9日有一小时的课堂测试，占总成绩的20%，测试内容为课程讲授的理论知识。
 - 期末考试占总成绩的40%。

第四篇文档：CITS5506 - 22 Jul 20_04.txt

- **课程信息：**
 - 课程为物联网（IOT），在nal land上学习，遵循西澳大学版权规定。
 - 授课教师为Atif，邮箱为[具体邮箱地址]，咨询时间为周一课程结束后12:00 - 13:00，地点在计算机科学楼G06a。
- **课程安排：**
 - 共八周课程，包含理论和实践部分，有实验课和项目作业。
 - 项目组由教师分配，每组会有专属的MS Teams私人频道进行交流。
 - 学生需填写技能调查表单，帮助教师平衡组队。
- **项目相关：**
 - 项目选题需具有一定影响力和实用性，包含传感、通信、计算、数据分析或行动等IOT组件。
 - 学生需提交项目提案，包括短标题、200字左右的描述，阐述项目内容和实现方式。
 - 每个小组有50美元预算用于购买不在西澳大学的传感器等物品，需在项目提案中注明传感器、网站、成本和交付时间等信息。
 - 项目评估包括项目提案（占15%）、项目报告（占35%）、项目原型和演示（占30%）以及项目展示（占20%）。
 - 教师会根据项目提案给出反馈，学生可根据反馈修改项目。
 - 项目成绩可能因小组成员的参与度和贡献不同而有所差异，通过反馈和自评进行评估。
- **实验相关：**
 - 实验课使用Ardo、raspberry pi、Laura Communication等硬件进行，学生需在实验前阅读实验指导。
 - 实验成绩根据实验操作和回答问题情况评定。
 - 课程共有五位实验指导教师，分别为Julian Zheng、Asad、Ning Liu、Frank和F donkin，还有实验技术员Andy提供支持。
- **考试相关：**
 - 9月9日有一小时的课堂测试，占总成绩的20%，测试内容为课程讲授的理论知识。

- 期末考试占总成绩的40%。

第五篇文档：CITS5506 - 29 Jul 20_06.txt

• IOT挑战：

- IOT在技术、社会和经济领域具有重要意义，但也面临一些挑战，如数据隐私和安全、法律和监管问题、社会观念冲突等。
- 数据隐私和安全是主要挑战之一，包括隐私恐惧、监视担忧、安全漏洞等问题，例如智能玩具被黑客攻击、Google Glass因隐私问题停产等。
- 法律挑战包括监管和法律问题、跨境数据流动、数据误用、法律冲突和数据保留政策等，例如自动驾驶汽车事故的责任归属、数据被用于商业推销等。
- 社会观念冲突表现为对IOT的看法存在分歧，一些人认为它会带来效率和洞察力，而另一些人则担心它会侵犯隐私和自由。

• IOT历史：

- IOT的概念并不新鲜，最早由Kevin Ashton于1999年提出，当时他所在的公司叫Thing Magic，现在已改名为Jedda。
- 1977年就有了自动抄表和智能电网的概念，但当时的无线技术不成熟，通信基于专有或行业特定标准，而不是IP。
- 直到最近几十年，随着无线通信、IP网络、计算经济学、迷你化、数据分析和云计算等技术的发展，IOT才得以广泛应用。

• IOT发展：

- 目前IOT的发展得益于多种技术，如无处不在的连接、广泛采用的IP网络、计算成本降低、设备小型化、数据存储和分析能力提升以及云计算的兴起等。
- 不同机构对IOT的发展有不同的预测，例如Cisco认为到2020年将有超过500亿台设备连接到网络，而Hawaii预测到2025年将有1000亿个IOT连接。
- IOT的应用领域广泛，包括智能农业、水质量和空气质量监测、健康护理、工业自动化、环境管理等，但也面临基础设施准备、投资激励和技术技能等方面的挑战。

• IOT技术：

- IOT的技术挑战包括传感器和功率消耗、安全、隐私、数据、分析、通信技术、互操作性和标准以及开发挑战等。
- 传感器的选择需要考虑成本、适用性和准确性等因素，例如在停车场监测中，可以使用光传感器、摄像头、压力传感器或超声波传感器等，但不同传感器的效果和成本不同。
- 通信技术需要满足任何时间、任何地点和任何事物的连接需求，从高带宽连接到低功率广域网络，如Laura、NB-IOT等。
- 数据中心的能源消耗和管理也是一个问题，需要采用更高效的能源和功率管理技术。

- 互操作性和标准的制定面临困难，因为不同公司有不同的利益，需要有监管机构来推动标准的统一。

综上所述，这些文档主要围绕物联网课程的相关内容展开，包括课程信息、项目要求、实验安排、IOT的挑战和发展历史、应用架构以及相关技术等方面的内容。

4. 讲课内容 Quiz

以下是根据文档总结的20个可能的quiz及其答案：

1. IoT的全称是什么？

- 答案：Internet of Things（物联网）。

2. IoT的主要组件有哪些？

- 答案：传感器、通信、计算（包括边缘计算）、平台（包括数据存储、分析和可视化）和行动。

3. 以下哪种技术不属于低功率广域网络技术？

- A. Laura
- **B. Wi - Fi**
- C. S Fox
- D. NBIOT
- 答案：B. Wi - Fi是短距离无线网络技术，不属于低功率广域网络技术。

4. MQTT协议的主要特点是什么？

- 答案：轻量级、低功耗、可靠性高，适用于IoT设备的通信。

5. IoT平台的主要作用是什么？

- 答案：接收和发送数据，基于云服务进行数据存储、分析和可视化。

6. 数据分析在IoT中的作用是什么？

- 答案：应用统计工具和机器学习算法对IoT数据进行分析，以获取洞察和支持决策。

7. 用户界面在IoT中的作用是什么？

- 答案：以Web或智能手机应用的形式呈现IoT数据，使用户能够直观地理解 and 操作。

8. IoT在以下哪个领域有应用？（可多选）

- A. 智能农业
- B. 智能交通
- C. 智能医疗
- D. 以上都是
- 答案：D. IoT在智能农业、智能交通、智能医疗等多个领域都有应用。

9. IoT面临的挑战包括哪些？（可多选）

- A. **数据隐私和安全**
- B. **法律和监管问题**
- C. **社会观念冲突**
- D. 以上都是
- 答案：D. IoT面临的数据隐私和安全、法律和监管问题、社会观念冲突等都是其面临的挑战。

10. 数据隐私和安全问题包括哪些？（可多选）

- A. **隐私恐惧**
- B. **监视担忧**
- C. **安全漏洞**
- D. 以上都是
- 答案：D. 数据隐私和安全问题包括隐私恐惧、监视担忧、安全漏洞等。

11. 以下哪个例子说明了IoT在智能交通中的应用？

- A. 车辆通过传感器监测道路状况，将数据发送到服务器，以优化交通流量。
- B. 智能手表监测用户的健康数据。

- C. 智能家居系统控制灯光和温度。
- D. 以上都不是
- 答案：A. 车辆通过传感器监测道路状况并优化交通流量是IoT在智能交通中的应用例子。

12. IoT的历史可以追溯到什么时候？

- 答案：IoT的概念最早由Kevin Ashton于1999年提出，但相关思想和技术在更早的时候就已经存在。

13. IP地址在IoT中有什么作用？

- 答案：IP地址是物联网设备连接到网络的基础，确保设备能够在网络中进行通信和数据交换。

14. 计算经济学对IoT的发展有什么影响？

- 答案：计算经济学的发展使得物联网设备的计算能力提高，成本降低，促进了IoT的广泛应用。

15. 迷你化对IoT的发展有什么意义？

- 答案：迷你化使得物联网设备更加小巧、便携，便于部署在各种场景中，扩大了IoT的应用范围。

16. 数据存储和分析在IoT中的重要性是什么？

- 答案：IoT 产生大量数据，数据存储和分析能够帮助提取有价值的信息，支持决策和优化系统性能。

17. 云计算在 IoT 中的作用是什么？

- 答案：云计算为物联网提供强大的计算和存储能力，支持大数据处理和分析，使 IoT 能够处理海量数据。

18. 互操作性和标准在IoT中的重要性是什么？

- 答案：互操作性和标准确保不同物联网设备和系统能够相互通信和协同工作，促进IoT的发展和应用。

19. Gardner的炒作周期包括哪些阶段？

- 答案：峰值期望、幻灭低谷、启蒙斜坡和生产力高原。

20. IoT项目评估通常包括哪些方面？

- 答案：项目提案、项目报告、项目原型和演示以及项目展示等方面。

以上quiz涵盖了IoT的基本概念、技术、应用、挑战和发展等方面的内容，通过回答这些问题，可以帮助学生巩固对课程知识的理解。

5. 知识点文档

这份笔记主要关于物联网（IoT）的相关内容，包括其面临的挑战、历史、发展、技术细节、通信模型、组件以及相关的协议和标准等。以下是详细内容总结：

一、Challenges of IoT（物联网的挑战）

1. Societal Challenges（社会挑战）：

- **privacy fears（隐私恐惧）**：人们担心物联网设备会侵犯个人隐私。
- **surveillance concerns（监视担忧）**：对物联网设备可能被用于监视的担忧。
- **Security Concern (hacking of Internet - connected devices)（安全担忧（互联网连接设备被黑客攻击））**：物联网设备的安全漏洞可能导致数据泄露和设备被入侵。

2. Legal Challenges（法律挑战）：

- **Conflict between law enforcement surveillance and civil rights（执法监视与公民权利之间的冲突）**：在物联网环境下，法律执行监视与公民权利之间可能存在冲突。
- **Data retention and destruction policies（数据保留和销毁政策）**：关于物联网数据的保留和销毁政策需要明确规定。
- **Legal liability for unintended uses（意外使用的法律责任）**：例如自动驾驶汽车事故中的责任归属问题。
- **Security breaches or privacy lapses（安全漏洞或隐私泄露）**：物联网设备的安全漏洞可能导致隐私泄露。

二、IoT History（物联网历史）

3. “Internet of Things”（IoT）一词于1999年由英国技术先驱Kevin Ashton首次使用，用于描述物理世界中的物体可以通过传感器连接到互联网的系统。

4. 1977年，开始进行商业自动抄表和电力服务负载管理的工作，从而导致了“智能电网”和“智能电表”在电话线上的应用。
5. 20世纪90年代，无线技术的进步使得“机器对机器”（M2M）企业和工业解决方案得以用于设备监测和操作。然而，许多早期的M2M解决方案基于封闭的专用网络和专有或行业特定标准，而不是基于互联网协议（IP）和互联网标准。
6. 1990年，在一次互联网会议上展示了第一个互联网“设备” - 一个可以通过互联网打开和关闭的支持IP的烤面包机。

三、IoT Evolution（物联网演进）

7. Ubiquitous Connectivity（无处不在的连接）：

- **Low cost, high - speed, pervasive network connectivity（低成本、高速、普及的网络连接）**：物联网需要低成本、高速、广泛的网络连接。
- **Widespread adoption of IP - based networking - IP has become the dominant global standard for networking.（基于IP的网络的广泛采用 - IP已成为网络的主要全球标准）**：互联网协议版本4（IPv4）具有32位地址空间，提供4,294,967,296（ 2^{32} ）个唯一地址；互联网协议版本6（IPv6）具有128位地址。

8. Computing Economics（计算经济学）：计算能力以更低的价格和更低的功耗提高。

9. Miniaturization（小型化）：制造技术的进步允许将尖端的计算和通信技术集成到非常小的物体中，以及小型且廉价的传感器设备。

10. Advances in Data Analytics（数据分析的进步）：新算法和计算能力、数据存储和云服务的快速增长使得能够分析大量数据。

11. Rise of Cloud Computing（云计算的兴起）：云计算利用远程、网络计算资源来处理、管理和存储数据，允许小型和分布式设备与强大的后端分析和控制能力进行交互。

12. Development issues（发展问题）：包括基础设施准备、市场和投资激励、技术技能要求和政策资源等方面的独特需求和挑战需要得到解决。

四、Technical Challenges（技术挑战）

13. Sensors（传感器）：应用于边缘计算和物联网、智能城市、智能制造、医院、工业、机器学习和汽车等领域。传感器是捕获模拟世界中发生的事情的数据的芯片，并将数据数字化，以便人类和机器进行处理、存储、组合、挖掘、关联和利用。能源和功率效率至关重要，量子传感器利用量子力学的特性，在传感器技术中优化了精度并突破了当前的限制。

14. How are the Network changing（网络如何变化）：

- **Extensions（扩展）**：更多的节点、更多的连接，IPv6（128位地址）与IPv4（32位地址空间）相比。

- **Any TIME, Any PLACE + Any THING（任何时间、任何地点 + 任何事物）**：M2M、IoT，数十亿互联设备，每个人都连接在一起。
- **Expansions（扩展）**：宽带和低功耗广域网（LPWAN）。
- **Enhancements（增强）**：数据中心和内容导向的网络 - 上下文感知（自主）系统（通过传感器了解周围环境）。
- **Data Centric Networking（数据中心网络）**：无线传感器网络领域的一项基本创新是数据中心网络的概念。简而言之，如果通信直接基于应用特定的数据内容而不是传统的IP式寻址，那么传感器网络的路由、存储和查询技术都可以变得更加高效。
- **Content - oriented networking（内容导向网络）**：消费者通过发送带有所需内容名称的Interest消息来请求内容。网络根据名称使用最长前缀匹配来路由兴趣。当找到匹配项（当Interest与Content Object匹配时）时，内容将在Interest的反向路径上发送回去。Interest消息可能会在途中的缓存中进行匹配，而不仅仅是在发布者处。

五、Communications Models（通信模型）

15. **Device - to - Device Communications（设备到设备通信）**：两个或多个设备直接相互连接和通信，而不是通过中间应用服务器。这些设备使用蓝牙、Z - Wave或ZigBee等协议建立直接的设备到设备通信。
 - **Bluetooth（蓝牙）**：传输功率限制为2.5毫瓦，范围非常短，高达10米（33英尺）。由蓝牙特别兴趣小组（SIG）管理。
 - **Z - Wave**：主要用于家庭自动化的无线通信协议，使用低能量无线电波在设备之间进行通信，允许对住宅设备和其他设备进行无线控制，如照明控制、安全系统、恒温器、窗户、锁、游泳池和车库门开启器。使用网状架构网络，232个节点可以连接到Z - Wave网络，桥接选项可以增加节点数量。在全球不同地区使用不同的频率，在欧洲运行在868 - 869 MHz频段，而在北美频段从908 - 916 MHz变化。
 - **Zigbee**：基于IEEE 802.15.4的规范，用于创建个人区域网络的一套高级通信协议。它与小型、低功率数字无线电一起工作，例如用于家庭自动化、医疗设备数据收集和其他低功率低带宽需求，专为小规模项目设计，需要无线连接。因此，Zigbee是一种低功率、低数据速率和近距离（即个人区域）无线网状自组织网络。传输距离视视线可达10 - 100米（30'至300'），具体取决于功率输出和环境特征。Zigbee网络通过128位对称加密密钥进行安全保护。定义的速率高达250 kbit/s，最适合传感器或输入设备的间歇性数据传输。在工业、科学和医疗（ISM）无线电频段运行，包括全球大多数司法管辖区的2.4 GHz。数据速率从20 kbit/s（868 MHz频段）到250 kbit/s（2.4 GHz频段）不等。Zigbee适用于短距离，但需要大量节点来覆盖更大范围，维护成本大幅增加。

16. **Device - to - Cloud Communications (设备到云通信)**：物联网设备直接连接到互联网云服务，如应用服务提供商，以交换数据和控制消息流量。一些流行的消费物联网设备，如Nest Labs Learning Thermostat和Samsung SmartTV采用这种通信模型。如果设备和云服务之间使用专有数据协议，设备所有者或用户可能会被绑定到特定的云服务，限制或阻止使用替代服务提供商，这通常被称为“供应商锁定”。
17. **Device - to - Gateway Model (设备到网关模型)**：
- **Transport Layer Security (TLS) (传输层安全)**：是一种加密协议，旨在为计算机网络上的通信提供安全保障。该协议广泛用于电子邮件、即时消息和IP语音等应用程序，但它在保护HTTPS方面的使用仍然是最公开可见的。
 - **Datagram Transport Layer Security (DTLS) (数据报传输层安全)**：是一种为数据报应用提供安全保障的通信协议。在设备到网关模型中，或者更典型的是，设备到应用层网关 (ALG) 模型中，物联网设备通过ALG服务作为管道连接到云服务。这是个人健身追踪器等流行消费产品经常采用的模型。这些设备本身没有直接连接到云服务的能力，因此它们经常依赖智能手机应用程序软件作为中间网关，将健身设备连接到云。这种设备到网关模型的另一种形式是家庭自动化应用中“集线器”设备的出现。这些设备作为单个物联网设备和云服务之间的本地网关，但它们也可以弥合设备本身之间的互操作性差距。
18. **Back - End Data - Sharing Model (后端数据共享模型)**：基本上扩展了单个设备到云的通信模型，以便授权的第三方可以访问物联网设备和传感器数据。在这种模型下，用户可以从云服务中导出和分析智能对象数据，并与其他来源的数据结合，进一步将其发送到其他服务进行聚合和分析。受限应用协议 (CoAP) 是一种用于受限设备的互联网应用协议 (在RFC 7228中定义)。它使这些受限设备能够使用类似的协议与更广泛的互联网进行通信。互联网协议套件越来越多地用于功率、内存和处理资源严重受限的小型设备，创建了受限节点网络。OAuth是一种访问授权的开放标准，通常用作互联网用户授予网站或应用程序访问其在其他网站上的信息的方式，但不向他们提供密码。这种机制被Google、Facebook、Microsoft和Twitter等公司使用，允许用户与第三方应用程序或网站共享其账户信息。

六、Components of IoT (物联网组件)

19. **Connectivity: Key Requirements (连接性：关键要求)**：
- **Availability (可用性)**：物联网设备需要随时可用。
 - **Reliability (可靠性)**：确保数据传输的稳定性。
 - **Viability (可行性)**：在实际应用中能够正常工作。
20. **Wireless System (无线系统)**：
- **Licensed (授权)**：
 - **Cellular (蜂窝)**：包括寻呼、固定无线和卫星等。
 - **Unlicensed (未授权)**：

- **Cordless (无绳)**：如WLAN、蓝牙、UWB（超宽带）、M2M、PAN等。

- **Wireless communications is highly variable. (无线通信高度可变)**：数据在这些通道上传输容易出错、不可靠，存在延迟问题。因此，无线通道需要积极管理。

21. System Requirements (系统要求)：

- **Capacity: Bits flowing reliably (bps) (容量：可靠流动的比特数 (bps))**：系统需要能够支持一定的数据传输速率。
- **Latency: Delay in delivering bits (延迟：交付比特的延迟)**：数据传输的延迟应尽可能低。
- **Coverage: Percentage of geographical locations with minimum level of service (覆盖范围：具有最低服务水平的地理位置百分比)**：确保在一定的地理范围内能够提供服务。
- **Cost of service (服务成本)**：考虑服务的成本效益。

22. Additional Requirements on Transceiver (对收发器的额外要求)：

- **Power Consumption: Battery life, Complexity (功耗：电池寿命、复杂性)**：收发器应具有低功耗，以延长电池寿命，同时结构不应过于复杂。
- **Portability: Size and weight (便携性：尺寸和重量)**：收发器应小巧轻便，便于携带和安装。
- **Cost of Transceiver (收发器成本)**：控制收发器的成本，以满足物联网设备的大规模部署需求。

23. Application Data Rate BER Latency Traffic (应用数据速率BER延迟流量)：

不同的应用具有不同的数据速率、误码率（BER）、延迟和流量特性，例如语音应用数据速率低、延迟低、流量连续；消息应用数据速率非常低、误码率非常低、延迟高、流量突发；视频应用数据速率高、误码率中等、延迟中等、流量连续等。

24. Spectrum Regulations (频谱规定)：

- **In Australia frequency spectrum is controlled by ACMA, Australian Communications and Media Authority (在澳大利亚，频谱由澳大利亚通信和媒体管理局 (ACMA) 控制)。**
- **World wide spectrum is controlled by ITU Radio communication Sector (ITU - R) (全球频谱由国际电信联盟无线电通信部门 (ITU - R) 控制)。**
- **Some spectrum for unlicensed use, which means that no one has to pay for leasing or buying that spectrum. (一些频谱用于未经许可的使用，这意味着没有人必须支付租赁或购买该频谱的费用)**：对于这些频谱，有一些基本的规则，例如特定点发射的功率谱密度，通常是天线的规则。
- **These bands may become congested. (这些频段可能会变得拥挤)**：由于许多设备都可能使用这些未经许可的频段，因此可能会出现拥塞问题。

25. Mobile phone technology is probably the best business proposition (移动电话技术可能是最好的商业主张)：

此外，一类令人兴奋的低功耗广域网络技术也正在涌现，如低功耗WiFi也是一个竞争者。

26. **ISM Band（工业、科学和医疗频段）**：工业、科学和医疗无线电频段（ISM频段）是国际上为工业、科学和医疗目的（而非电信）使用射频能量而保留的无线电频段。例如微波炉、医疗透热机等应用在此频段运行。在这些频段运行的通信设备必须容忍ISM应用产生的任何干扰，并且用户在ISM设备运行方面没有监管保护。对于物联网，一些频段特别感兴趣，例如900至928 MHz之间的频段 - ISM频段，以及2.4 GHz和5.7 GHz区域的频段，还有一些较低频率的频段也很有吸引力。这些频段基本上是免许可操作，因此可以部署大量物联网设备而无需支付频段使用费用。
27. **Low Power WiFi（低功耗WiFi）**：尽管WiFi功耗较高，但它是物联网的一个不错选择。WiFi已经取得了更大的成功，现在无处不在，并且存在更高。WiFi由于高能耗以前不太适合传感器通信，但WiFi社区开始安装IC用于占空比，当没有传感或传输发生时，它保持休眠模式，从而使其节能。随着2.4 GHz频段变得更加拥挤，许多用户选择使用5 GHz ISM频段。这不仅提供了更多的频谱，而且它不像WiFi以及许多其他设备（包括微波炉等物品）那样被广泛使用。在蜂窝技术中，我们面临电池放电的问题。在物联网中，我们希望传感器在一个小电池上运行可能长达数年。
28. **3GPP（第三代合作伙伴计划）**：3GPP是电信协会组之间的合作，称为组织合作伙伴。3GPP正在为5G的蜂窝物联网工作。
29. **Narrowband Internet of Things (NB - IoT)（窄带物联网）**：是3GPP开发的低功耗广域网（LPWAN）无线电技术标准。NB - IoT专门专注于低成本、长电池寿命和高连接密度。NB - IoT使用LTE标准的子集。由于广泛的覆盖范围、相对较低的部署成本、高水平的安全性、访问专用频谱以及管理的简单性，蜂窝网络对于支持大规模物联网安装变得越来越有吸引力。
30. **Low - Power Wide - Area Network (LPWAN) or Low - Power Network (LPN)（低功耗广域网（LPWAN）或低功耗网络（LPN））**：是一种无线电信广域网类型，旨在允许事物（连接对象）之间以低比特率进行长距离通信。
31. **MQTT（消息队列遥测传输）**：是一种在TCP/IP上运行的机器对机器连接协议。轻量级、简单，MQTT基于发布 - 订阅结构：发布者根据主题向指定的代理发送消息；代理充当总机，接受来自发布者关于指定主题的消息，并将它们发送给这些主题的订阅者；订阅者从连接的代理和指定主题接收消息。MQTT因其轻量级、高效、可靠的消息传递、双向通信、支持不可靠网络和安全启用等特点而更适合物联网。
32. **Low Power Wide Area Networks（低功耗广域网）**：
- **SIGFOX（<https://www.sigfox.com>）**：Sigfox是一家法国公司，成立于2009年，构建无线网络以连接低能量对象，如电表、智能手表和洗衣机，这些对象需要持续开启并发射少量数据。
 - **LoRa: Long Range Low Power Wireless platform（LoRa：长距离低功率无线平台）**：LoRa是一种专有的线性调频扩频（CSS）无线电调制技术，用于LPWAN，由LoRaWAN、Haystack Technologies和Symphony Link使用。LoRa是由Cycleo（法国格勒诺布尔）开发并于2012年被Semtech收购的专利技术。LoRa使用免许可的亚千兆赫无线电频段，如169 MHz、433 MHz、868 MHz（欧洲）和915 MHz（北美）。范围为5公里（城市）、20公里（农村）。

- **Weightless (Wireless Communication) (Weightless (无线通信))**：Weightless是一组LPWAN开放无线技术标准的名称，用于在基站和周围数千台机器之间交换数据。这些技术允许开发人员构建低功耗广域网（LPWAN）。Weightless由Weightless SIG或特别兴趣小组管理。目的是设备必须符合Weightless特别兴趣小组对SIG定义

以下是30个quiz及其答案：

1. IoT面临的社会挑战包括哪些？

- 答案：隐私恐惧、监视担忧、安全漏洞（黑客攻击互联网连接设备）。

2. IoT面临的法律挑战有哪些？

- 答案：执法监视与公民权利之间的冲突、数据保留和销毁政策、意外使用的法律责任、安全漏洞或隐私泄露。

3. “Internet of Things”（IoT）一词最早由谁在什么时候提出？

- 答案：由英国技术先驱Kevin Ashton于1999年提出。

4. 1977年在物联网相关领域发生了什么？

- 答案：开始进行商业自动抄表和电力服务负载管理的工作，从而导致了“智能电网”和“智能电表”在电话线上的应用。

5. 1990年出现了什么与物联网相关的事物？

- 答案：在一次互联网会议上展示了第一个互联网“设备” - 一个可以通过互联网打开和关闭的支持IP的烤面包机。

6. IoT演进中的Ubiquitous Connectivity包括哪些方面？

- 答案：低成本、高速、普及的网络连接，基于IP的网络的广泛采用（IPv6具有128位地址）。

7. 计算经济学对IoT的发展有什么影响？

- 答案：计算能力以更低的价格和更低的功耗提高，促进了IoT的发展。

8. Miniaturization对IoT的发展有什么意义？

- 答案：允许将尖端的计算和通信技术集成到非常小的物体中，以及小型且廉价的传感器设备，扩大了IoT的应用范围。

9. 数据分析的进步对IoT有什么作用？

- 答案：新算法和计算能力、数据存储和云服务的快速增长使得能够分析大量物联网数据，以获取洞察和支持决策。

10. 云计算的兴起对IoT的作用是什么？

- 答案：云计算利用远程、网络计算资源来处理、管理和存储数据，允许小型和分布式设备与强大的后端分析和控制能力进行交互，支持物联网的大数据处理和分析。

11. 技术挑战中传感器的应用领域有哪些？

- 答案：边缘计算和物联网、智能城市、智能制造、医院、工业、机器学习和汽车等领域。

12. 网络变化的扩展包括哪些方面？

- 答案：更多的节点、更多的连接，IPv6（128位地址）与IPv4（32位地址空间）相比；任何时间、任何地点 + 任何事物（M2M、IoT，数十亿互联设备，每个人都连接在一起）。

13. 数据中心网络的概念是什么？

- 答案：如果通信直接基于应用特定的数据内容而不是传统的IP式寻址，那么传感器网络的路由、存储和查询技术都可以变得更加高效。

14. 设备到设备通信中使用的协议有哪些？

- 答案：蓝牙、Z - Wave或ZigBee等。

15. 蓝牙的传输功率和范围是多少？

- 答案：传输功率限制为2.5毫瓦，范围高达10米（33英尺）。

16. Z - Wave主要用于什么？

- 答案：主要用于家庭自动化，允许对住宅设备和其他设备进行无线控制，如照明控制、安全系统、恒温器、窗户、锁、游泳池和车库门开启器等。

17. Zigbee的传输距离和数据速率范围是多少？

- 答案：传输距离视视线可达10 - 100米（30'至300'），具体取决于功率输出和环境特征；数据速率从20 kbit/s（868 MHz频段）到250 kbit/s（2.4 GHz频段）不等。

18. 设备到云通信模型的特点是什么？

- 答案：物联网设备直接连接到互联网云服务，如应用服务提供商，以交换数据和控制消息流量。一些设备可能存在“供应商锁定”问题。

19. 设备到网关模型中TLS的作用是什么？

- 答案：是一种加密协议，旨在为计算机网络上的通信提供安全保障。

20. 后端数据共享模型的作用是什么？

- 答案：扩展单个设备到云的通信模型，以便授权的第三方可以访问物联网设备和传感器数据，用户可以从云服务中导出和分析智能对象数据，并与其他来源的数据结合，进一步将其发送到其他服务进行聚合和分析。

21. 物联网组件中连接性的关键要求有哪些？

- 答案：可用性、可靠性、可行性。

22. 无线系统中的未授权频段包括哪些？

- 答案：Cordless、WLAN、蓝牙、UWB（超宽带）、M2M、PAN等。

23. 系统要求中的容量指的是什么？

- 答案：系统需要能够支持一定的数据传输速率，即可靠流动的比特数（bps）。

24. 对收发器的额外要求包括哪些？

- 答案：功耗（电池寿命、复杂性）、便携性（尺寸和重量）、成本。

25. 语音应用的数据速率、误码率、延迟和流量特性是什么？

- 答案：数据速率低、误码率中等、延迟低、流量连续。

26. 频谱规定中澳大利亚的频谱由谁控制？

- 答案：由澳大利亚通信和媒体管理局（ACMA）控制。

27. ISM频段是用于什么的？

- 答案：ISM频段是国际上为工业、科学和医疗目的（而非电信）使用射频能量而保留的无线电频段。

28. 低功耗WiFi的特点是什么？

- 答案：尽管WiFi功耗较高，但它是物联网的一个不错选择。WiFi已经取得了更大的成功，现在无处不在，并且存在更高。WiFi由于高能耗以前不太适合传感器通信，但WiFi社区开始安装IC用于占空比，当没有传感或传输发生时，它保持休眠模式，从而使其节能。随着2.4 GHz频段变得更加拥挤，许多用户选择使用5 GHz ISM频段。

29. 3GPP在物联网中的作用是什么？

- 答案：3GPP是电信协会组之间的合作，正在为5G的蜂窝物联网工作。

30. MQTT基于什么结构？

- 答案：基于发布 - 订阅结构，发布者根据主题向指定的代理发送消息；代理充当总机，接受来自发布者关于指定主题的消息，并将它们发送给这些主题的订阅者；订阅者从连接的代理和指定主题接收消息。

以下是对这两份文档的总结：

《2024_Sem02_IoT_Lecture05(1).pdf》

1. 项目与项目展示

- **项目：**
 - 思考一个物联网产品或服务，确保其有价值，例如解决问题、改进现有流程、降低成本或提供新服务等。
 - 考虑项目的可行性，包括技术专长、基础设施、资金、组件可用性和时间要求等。
 - 使用自下而上的方法，从简单功能开始，逐步增加复杂性。
 - 准备框架，包括概念设计、框图、子系统，并确定如何检查子系统的功能（相互依赖或独立）。

- 制定时间表，考虑子系统的相互依赖性，为意外情况预留额外时间。
- 尽早编写项目报告，可使用协作工具如Slack、Github（软件开发）和Overleaf（报告写作）。
- 解决团队成员之间的问题，否则尽早与单元协调员讨论。
- 学生将评估自己和团队成员对团队有效运作的贡献，评估标准包括尊重他人、守时、自我激励、贡献、团队沟通和协作等。
- 项目提案文档需在2024年8月25日晚上11:59之前提交，示例文档已上传至LMS的“Example/Support Material”，单元协调员将在9月2日之前给出反馈。

◦ 项目展示：

- 总时长15分钟，包括5 - 6分钟演讲、5 - 6分钟演示和3 - 5分钟问答。
- 每个团队成员都要展示，展示时间和日期将由团队在MS Teams上传的Excel表格中按先到先得的原则选择，展示将在第12周进行。
- 展示应组织清晰，重点关注“Why”“What”“How”。
- “What”部分包括项目标题，标题应吸引人且传达项目的意义、工作领域和目标。
- “How”部分包括设计，呈现实现方式（可从初始设计开始讨论变化及原因，或先展示最终设计再介绍中间步骤），还应包括实验部分，如项目功能检查的细节、评估时间、数据收集和分析情况、功能实现情况、与市场产品的成本比较等。
- 结论部分应包括项目的优势和局限性，以及与现有产品的比较。
- 未来工作部分应简要提及优化方向，如消除弱点、降低成本、增加功能等。
- 项目展示的必选幻灯片列表已上传至LMS的“Example/Support material”作为单独文件。

2. 创业之旅

- 介绍了精益画布（Lean Canvas），它是由Ash Maurya创建的一页商业计划模板，有助于解构想法的关键假设，源自Alex Osterwalder的商业模型画布并针对精益创业进行了优化。

3. 物联网应用架构和示例

◦ 物联网架构层：

- **应用层：**负责通过用户界面（包括仪表板、远程控制面板和相关业务计算）为用户提供应用服务。
- **网络层：**负责连接其他设备或服务器，包括传输和处理来自传感器的数据，如LoRa和MQTT。LoRa是一种无线调制技术，LoRaWAN是基于LoRa调制的媒体访问控制层协议。MQTT是一种运行在TCP/IP上的机器对机器连接协议，基于发布 - 订阅结构。
- **感知层：**物理层包含收集数据的传感器。

◦ 应用层：

- 数据对用户变得可操作和有意义，将技术数据转化为用户友好的格式，以支持决策、监控和控制物联网设备和系统。
- 基本应用架构包括前端和后端，如Web客户端、API网关、数据库等。
- 组件包括用户界面（如仪表盘、移动应用、语音界面等）、API、应用逻辑、数据存储和分析等。
- 用户界面示例包括图形用户界面、语音控制界面和手势界面等。
- 数据分析工具包括R、Python、Excel、Splunk等。
- 有用的云平台包括The Things Network、Amazon IoT Core、Azure IoT Hub、Home Assistant、Blynk等。
- 自开发应用工具包括HTML 5、JS、PHP、JAVA、CSS、React、Vue.js等。
- **之前的物联网项目及工具：**
 - **智能宠物喂食器：**利用前端Web界面连接到NoSQL数据库（MongoDB）进行后端存储，使用Constrained Application Protocol (CoAP)与通过Wi - Fi连接到互联网的硬件宠物喂食器通信，使用Python Flask框架开发网站逻辑，使用Chart.js库显示宠物食物消耗，通过Google Dialogflow的Intent和Fulfillment组件实现Google Assistant功能，还使用了Blynk和Eclipse Paho Android Service等。
 - **智能路灯：**操作员仪表盘的第一层与TN通信并依赖TTN应用SDK，将信息插入本地机器上的数据库；第二层是使用Express框架开发的Web应用，用于向系统操作员显示从TTN收集的信息。
 - **智能气象站：**使用Microsoft Azure、Django和React开发网站以图形方式显示实时数据，服务器使用Ubuntu 18.04 LTS和静态IP，应用包含接收数据和显示数据两部分，数据存储存储在SQLite数据库中并由Django连接。
 - **智能浇水系统：**土壤传感器连接到ESP8266，软件组件包括数据库（PostgreSQL）、后端（Phoenix框架）和前端（Vue.js框架），使用JWT验证数据所有者。
 - **智能办公桌占用率监测：**传感器连接到ESP8266 Node MCU，通过HTTPS Post请求将信息发送到Azure IoT Hub，再转发到Azure Service Bus，后端Python文件处理信息并更新显示实时UI数据的仪表盘，前端使用Python Flask服务器，通过Pusher库进行实时通信。
 - **其他项目：**使用Node Red MQTT在Things Network、Twilio的API、Tago IO创建仪表盘、Flutter UI开发移动应用、D3.js可视化数据、Cryptojs生成随机令牌和加密会话等。

《2024_Sem02_IoT_Lecture06(1).pdf》

4. 物联网组件（续）

- **连接性：**

- **低功耗广域网 (LPWAN)：**包括Sigfox（范围10公里（城市），40公里（农村），使用868MHz或902MHz频率）、LoRa（范围5公里（城市），20公里（农村））、Weightless（范围10公里）、RPMA（覆盖范围大，如农村Texas油田每座塔覆盖450平方英里）、NB-IoT（范围1公里（城市），10公里（农村））等。
- **新兴5G网络：**蜂窝网络对物联网的支持越来越有吸引力，因其具有广泛覆盖、相对低的部署成本、高安全性、专用频谱访问和简单管理等优点，但LTE网络需要改进以适应物联网设备的事件驱动特性。
- **平台：**物联网平台通常是基于云的基础设施，用于存储和处理数据，许多商业平台如Amazon Web Services (AWS)、Microsoft Azure、IBM Watson、Google Cloud Platform、Oracle、Bosch、CISCO IoT cloud Connect、SAP等可供选择，推荐使用软件即服务（SaaS）模型的可扩展云解决方案，PaaS用于应用程序开发，IaaS提供基础设施的自助服务模型。
- **中间件：**是为软件应用提供操作系统之外服务的计算机软件程序，如ODBC是一种数据库访问服务中间件。
- **运行时：**指程序运行的时间，某些编程语言有可链接和使用的运行时库。
- **分析：**需要对数据进行分析以获取洞察，大数据分析工具包括从简单统计工具到更复杂的机器学习方法（如深度学习）。
- **用户界面：**物联网产品需要有吸引人的用户界面，包括基于Web和智能手机或平板电脑的界面，如OpenRemote是一个开源项目，可用于智能建筑和城市自动化的可视化工具。

5. 智能产品

- **智能网球传感器：**未提及具体内容。
- **研究项目：桥梁健康监测：**使用物联网开发管道，以实现成本效益高、易于安装且及时收集、传输和可视化振动响应数据，从而预测桥梁健康状况。测试了三个不同的平台（Libelium Waspote、RAKwireless WisTrio RAK5010、Arduino MKR NB1500），在2022年9月对Fremantle的Stirling Bridge进行了为期3天的数据收集（包括视觉、有线传感器和物联网原型数据），数据通过MQTT经纪商发送到AWS IoT核心并存储在S3存储桶中，开发了使用Dash/Plotly库的仪表盘进行数据显示，但需要进一步研究以减少数据传输，未来工作包括改进数据传输、与桥梁健康监测参数对齐以及比较数字和模拟加速度计等。

6. 智能城市：提及TEDXSingapore的相关内容，但未具体阐述与智能城市的关系。

7. 智能产品 - 改变业务：

- 传统产品过去仅由机械和电气部件组成，现在的产品已成为结合硬件、传感器、数据存储、计算实体、软件和连接性的复杂系统。
- 智能连接产品提供了新功能、更高可靠性、更高产品利用率以及跨越传统产品边界的能力。
- 这些产品改变了价值链，迫使公司重新思考和调整内部几乎所有的事情，包括如何创造和获取价值、如何利用和管理大量新数据、如何重新定义与传统业务伙伴的关系以及在行业边界扩展时公司应扮演的角色等。

- 信息技术的发展经历了从自动化价值链中的单个活动到通过互联网实现协调和集成的过程，现在信息技术成为产品的一部分，导致产品和生产过程发生改变，包括产品设计、营销、制造、售后服务以及产生对产品数据分析和安全等新活动的需求。

综上所述，这两份文档主要围绕物联网的项目、组件、应用架构、智能产品以及相关研究等方面进行了阐述。