WirelessHART——

在实时工业过程控制中应用的无线通信技术

WirelessHART

1. WirelessHART概要
2. WirelessHART工作原理
3. Wireless HART的架构
4. Wireless HART的构建

WirelessHART概要

1.1 HART

1.1.1HART简介

1.1.2 HART的工作原理

1.1.3 HART的特点

1.2 Wireless HART

1.2.1 Wireless HART简介

1.2.1 Wireless HART技术的组成部分

WirelessHART概要

1.1.1 HART简介

HART （Highway Addressable Remote Transducer)

可寻址远程传感器高速通道的开放通讯协议,是美国罗斯蒙特公司于1985 年推出的一种用于现场智能仪表和控制设备之间的通讯协议。是智能仪器通信的全球标准,其最新版本为7.0。

HCF（HART Communication Foundation ）

HART通信基金会是一个国际性的、非盈利的会员制组织，它支持和促进HART通信协议标准和技术的广泛使用。 其成员主要包括Rosemont、ABB、Emerson、GE、Honeywell、Siemens等公司。

WirelessHART概要

- 1.1.2 HART的工作原理

HART协议利用贝尔202频移键控（FSK）标准（频率为1200Hz的正弦波表示“1”，频率为2200Hz的正弦波表示“0”）将低电平的数字通信信号叠加在4 - 20mA模拟信号之上。

HART以1200 bps的速率通信，而不影响4 - 20mA信号，并允许一个主机应用程序（主设备），从智能现场设备每秒获取两次或两次以上的数字更新。由于数字FSK信号是相位连续的，因而不会对4 - 20mA信号造成干扰。

WirelessHART概要

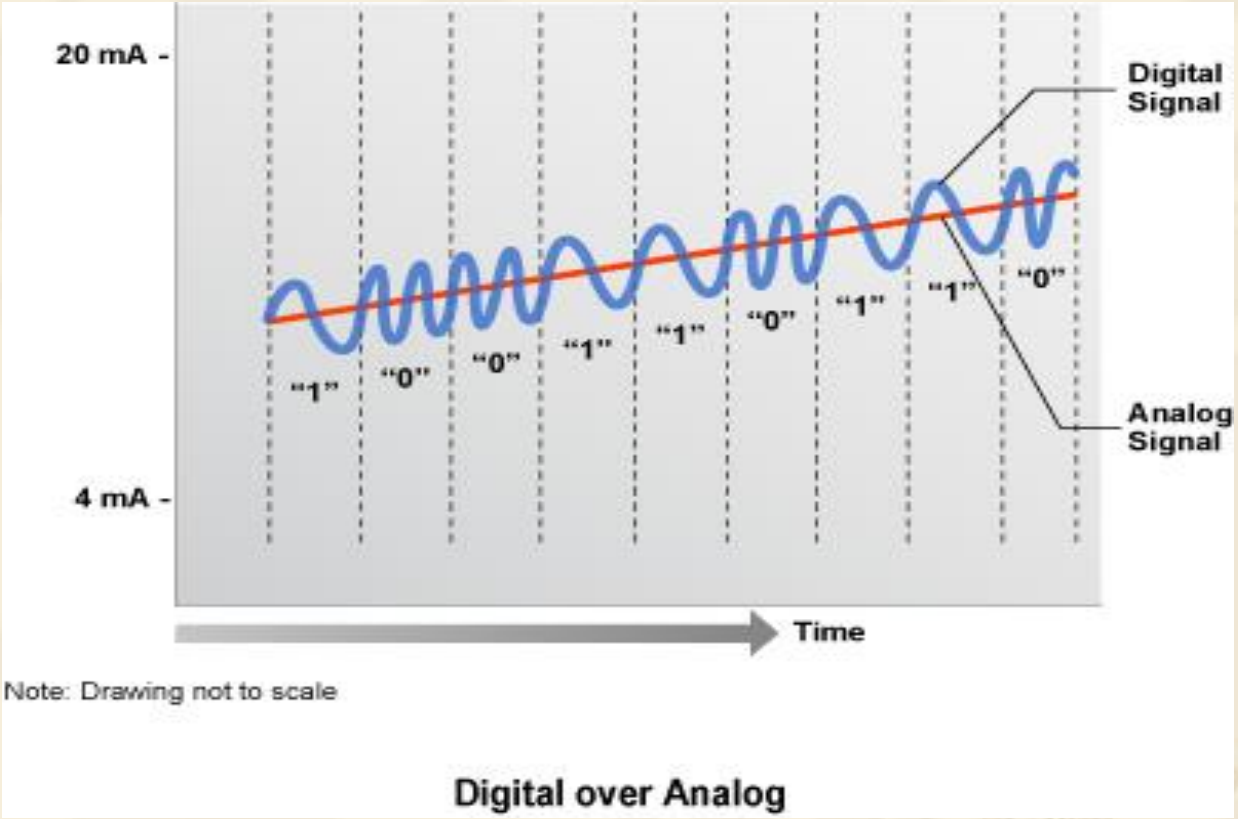

Figure1. 频移键控（FSK）

WirelessHART概要

- 1.1.3 HART的特点

1、多变量设备
2、实时调整量程
3、实时状态报告
4、在线远程故障诊断
5、通信灵活

WirelessHART概要

1.2.1Wireless HART简介

无线HART是专门为过程测量和控制应用而设计的第一个开放的无线通信标准，作为HART7规范的一部分于2007年9月正式发布。

无线HART协议是一种安全的基于TDMA（Time Division Multiple Access 时分多址）的无线网格网络技术，工作于2.4GHz的ISM（Industry Science Medicine)频段,采用直接序列扩频技术（DSSS）和信道跳频技术。

WirelessHART概要

- 1.2.2 Wireless HART技术的组成部分

1，网关（Gateway）
2，网络管理器(Network Manager)
3，安全管理器(Security Manager)
4，中继器(Repeater)
5，适配器(Adapter)
6，手持终端(Handheld)

WirelessHART工作原理

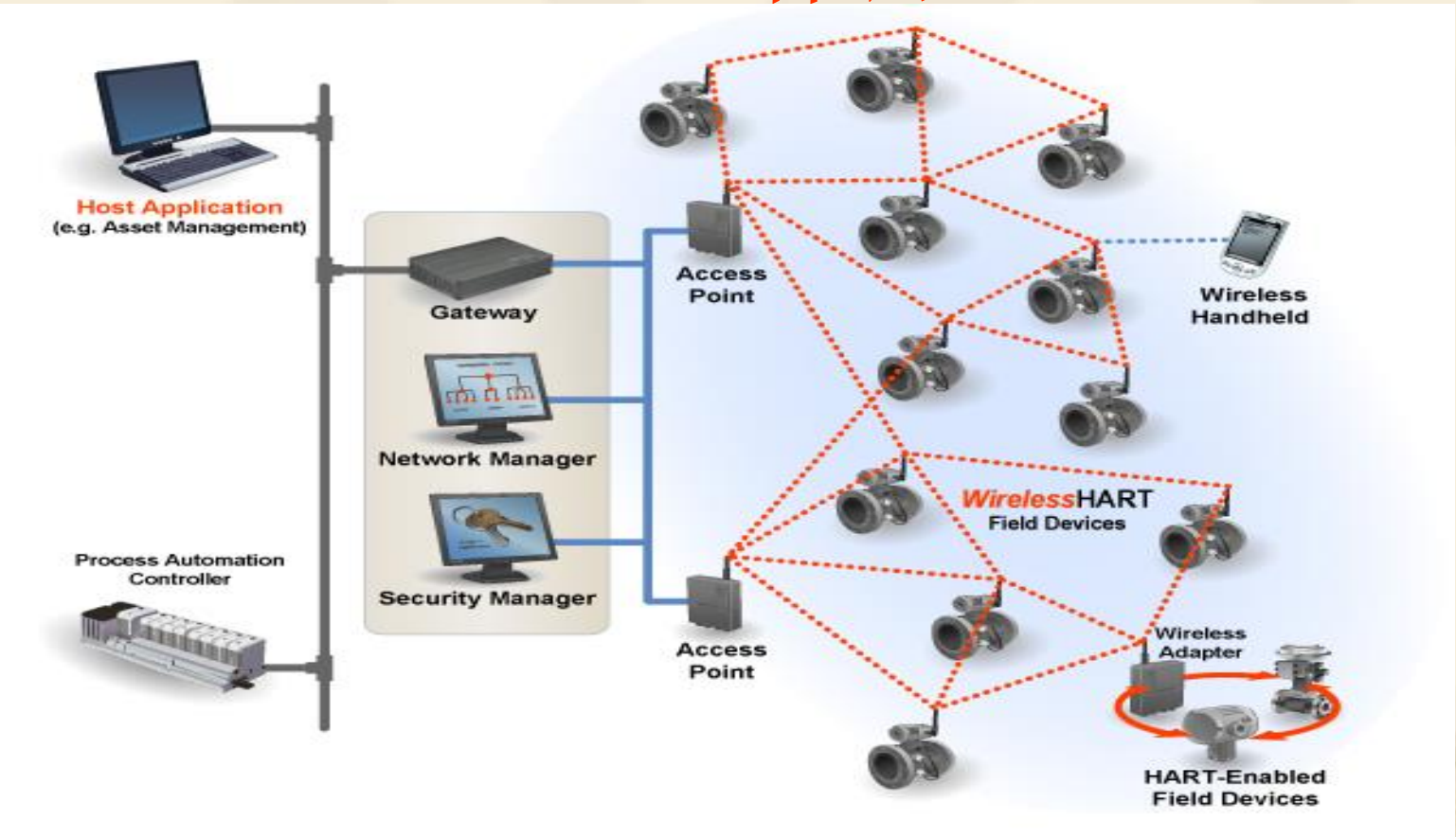

Figure .2 WirelessHART 工作原理图

Wireless HART的架构

3、 Wireless HART架构

Wireless HART协议栈包括五个层次：

1）物理层

2）数据链路层

3）网络层

4）传输层

5）应用层

另外还包括中央网络管理器和通信调度系统

Wireless HART的架构

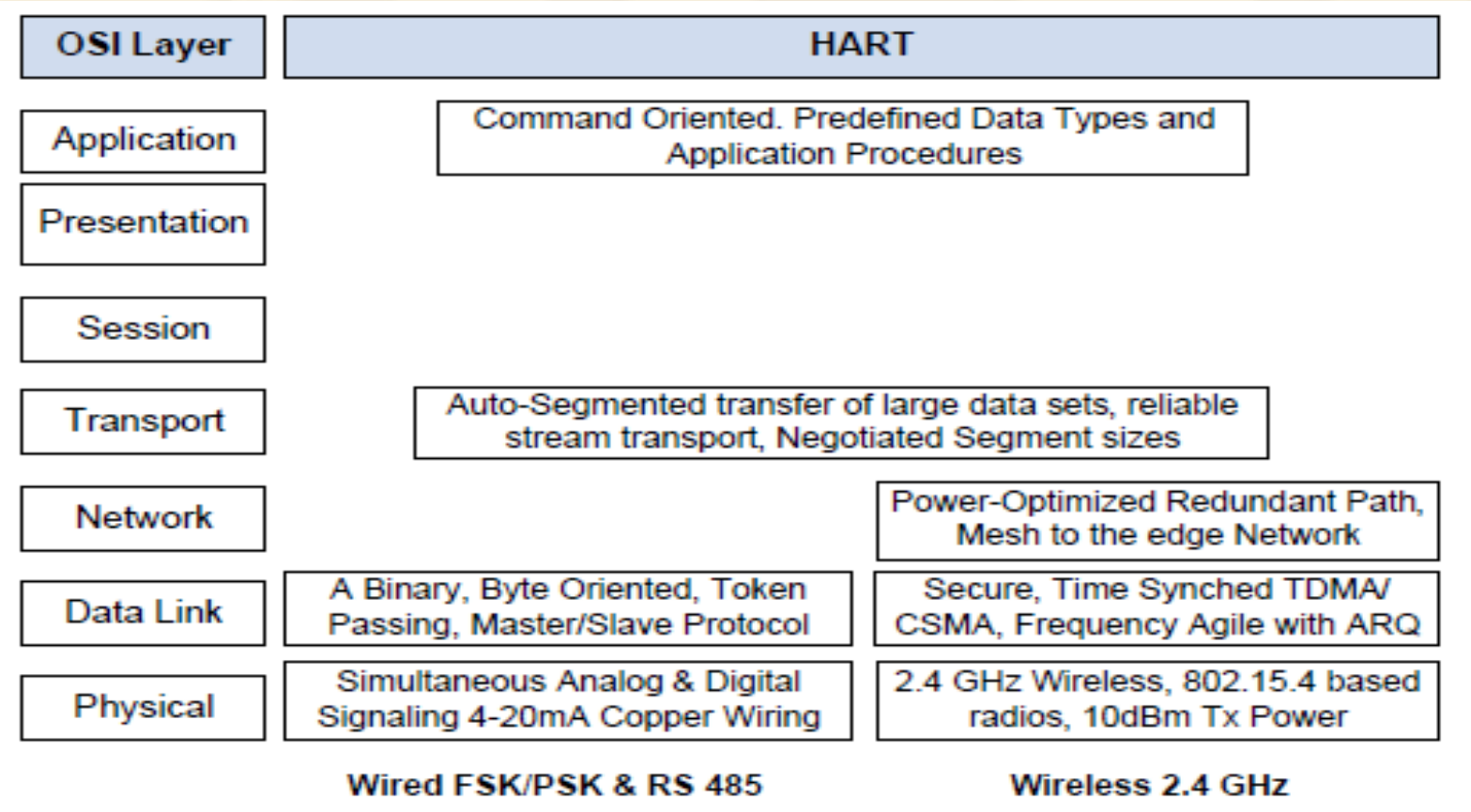

Figure .3 Architecture of HART Communication Protocol

Wireless HART的架构

- 3.1 物理层

无线HART协议物理层主要是依据IEEE STD 802.15.4-2006的2.4GHz直接序列扩频物理层。这一层定义了无线电特性，如信令方法，信号强度和设备灵敏度。

正如IEEE 802.15.4标准，无线HART工作在2400-2483.5MHz无需申请的免费ISM频段，数据传输速率高达250千比特/秒。其信道的编号从11至26，相邻信道的间隔为5MHz。

Wireless HART的架构

- 3.2 数据链路层

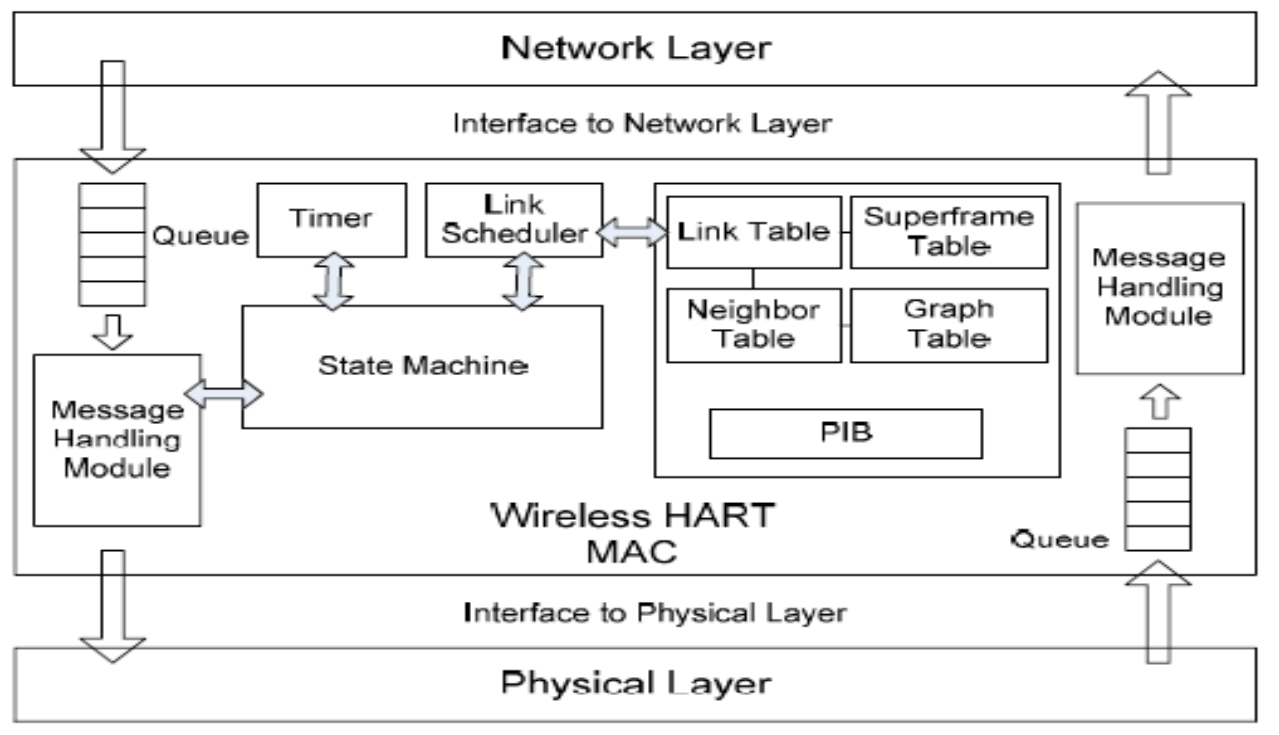

Figure .4 WirelessHART Data Link Layer Architecture

Wireless HART的架构

数据链路层主要特征：

1，时间同步数据链路层（time-synchronized DLL）；

2，用超帧（Superframe）的概念表示一组连续的时隙；

3，采用TDMA的MAC协议，每个时隙（slot）长　10ms，每秒包含100时隙，15个信道；

4，空闲信道评估（Clear Channel Assessment）；

5，信道黑名单（Channel Black Listing）；

6，按优先级别的信息传输；

7，可调整发射功率 。

Wireless HART的架构

- 3.2.1 接口(Interfaces)

MAC层和物理层之间的接口描述物理层提供的服务原语，MAC层和网络层之间的接口定义了网络层提供的服务原语。

Wireless HART的架构

- 3.2.2 定时器(Timer)

定时器是一个基本的Wireless HART模块。它提供精确的计时系统，以确保系统正确的操作。在无线HART时隙中对具体时序的要求如图5所示 。

Wireless HART的架构

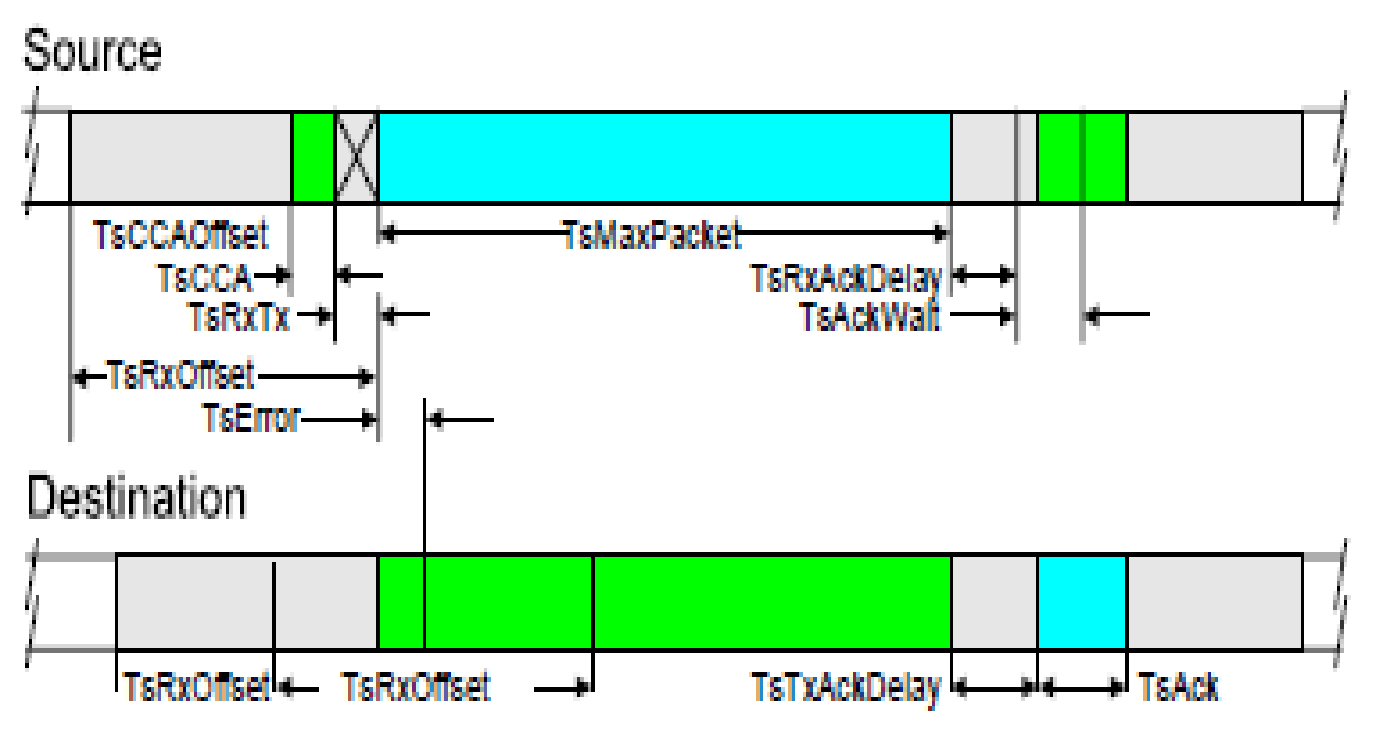

Figure 5. WirelessHART Slot Timing

Wireless HART的架构

- 3.2.3 通信表(Communication Table)

每个网络设备维护一个数据链路层中表的集合。超帧表和链接表存储网络管理器创建的通信配置；邻居表是一个该设备可以直接到达的邻居节点的列表，图表用于网络层和记录路由信息 。

Wireless HART的架构

- 3.2.4 链路调度(Link Scheduler)

链路调度的功能是基于超帧表和链接表的通信调度之上，以确定下一个被服务的时隙。这些因素，诸如事务优先级，链路变化，以及启用和禁用超帧都使调度复杂化。每一事件都可能会影响链路调度从而造成链接表重新评估。

Wireless HART的架构

- 3.2.5 消息处理模块(Message Handling Module)

消息处理模块缓冲区将来自网络层和物理层的包分开。

Wireless HART的架构

- 3.2.6 状态机(State Machine)

在数据链路层，状态机由三个主要部分组成：TDMA状态机，XMIT和RECV引擎。

TDMA状态机负责执行事务和调整定时器时钟。XMIT和RECV引擎直接与硬件接触，通过无线收发器分别发送和接受数据包。

Wireless HART的架构

- 3.3 网络层和传输层

网络层和传输层协同工作，为网络设备提供安全可靠的端到到的通信。

为了支持网格网的通信技术，每个无线HART设备需要能够作为路由为其他设备转发数据包。无线HART定义了两种路由协议：

图路由(Graph Routing)

源路由(Source Routing)

Wireless HART的架构

- 图路由：图是连接网络节点的路径的集合。每个图中的路径是由网络管理员明确的创建并下载到每个独立的网络设备中。为发送一个数据包，源设备在网络开头写入一个特殊的图号（由目的地决定）。所有的网络设备到目的地的路径都必须预先配置，它指定了包可能被转发到的邻居节点。

- 源路由：源路由是图路由的补充，针对网络诊断。为将包发送到它的目的地，源设备包含在包头，一个包必须经过的设备序列。当包被转发，每个路由设备使用列表中下一个网络设备地址，以确定下一跳，直到到达目标设备。

Wireless HART的架构

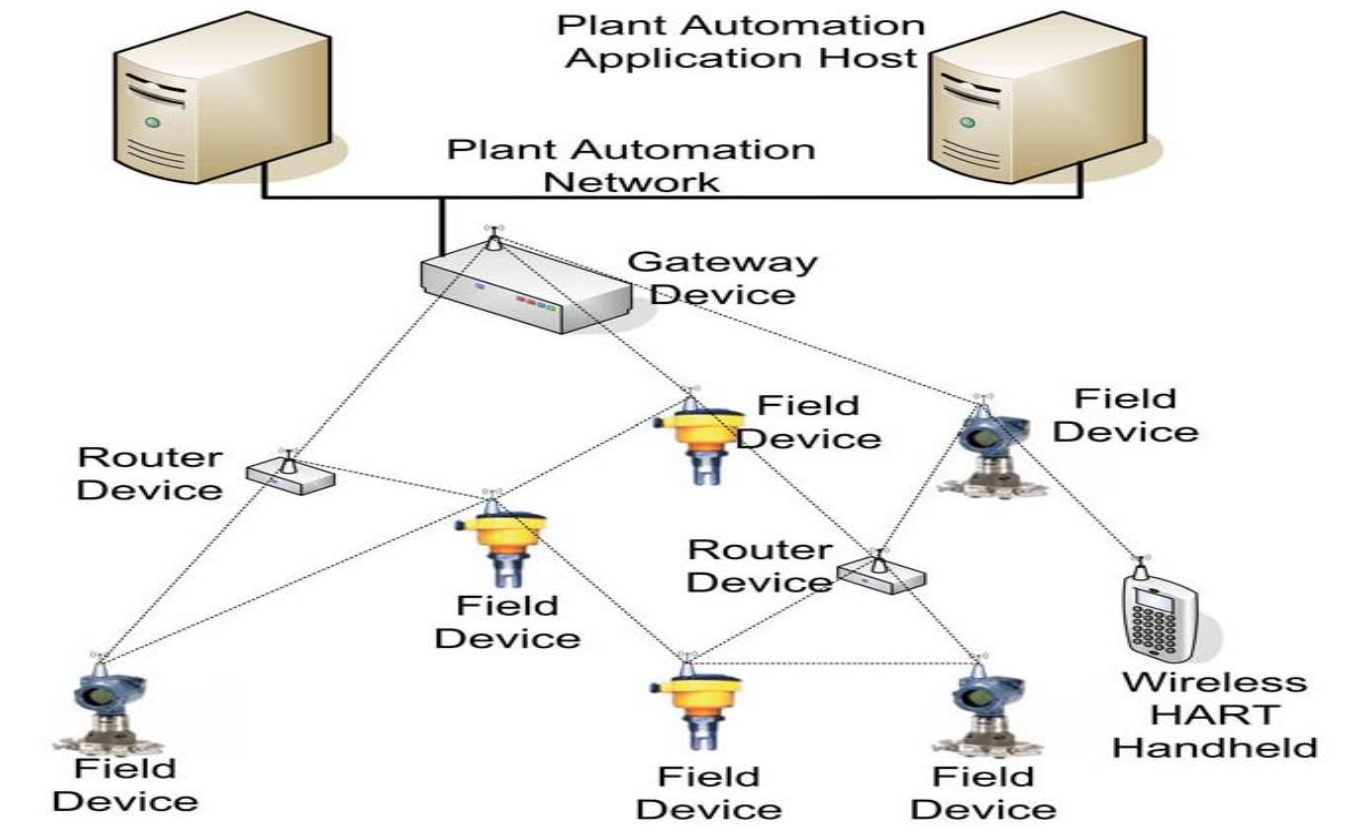

Figure 6. WirelessHART Mesh Networking

Wireless HART的架构

- 3.4 应用层

应用层是无线HART的最高层。它定义了各种设备的命令，响应，数据类型和状态报告。在无线HART中，设备和网管之间的通信是基于命令和响应。应用层负责解析消息内容，提取命令编号，执行指定的命令，并产生响应。

Wireless HART的架构

❖3.5 安全架构

无线HART是一个安全的网络系统。MAC层和网络层都提供安全服务。MAC层使用MIC（Message integrity code ）提供跳-跳的数据完整性。发送者和接受者都使用AES-128的CCM*(Counter with CBC-MAC)模式作为根本的区块加密方式以生成和比较MIC.

网络层采用不同的密钥，为端-端的通信提供保密性和完整性。在安全架构中定义了四种类型的密钥：

Wireless HART的架构

- 公共密钥：被加入设备使用生成MAC层的MIC。
- 网络密钥：被所有网络设备共享，并且被网络中现有设备使用来生成MAC层的MIC。
- 加入密钥：每个网络设备唯一，并在加入过程中由网络管理器验证加入设备。
- 会话密钥：由网络管理器生成的在两个网络设备的端—端的连接中是唯一的。提供了端-端的保密性和数据完整性。

Wireless HART的架构

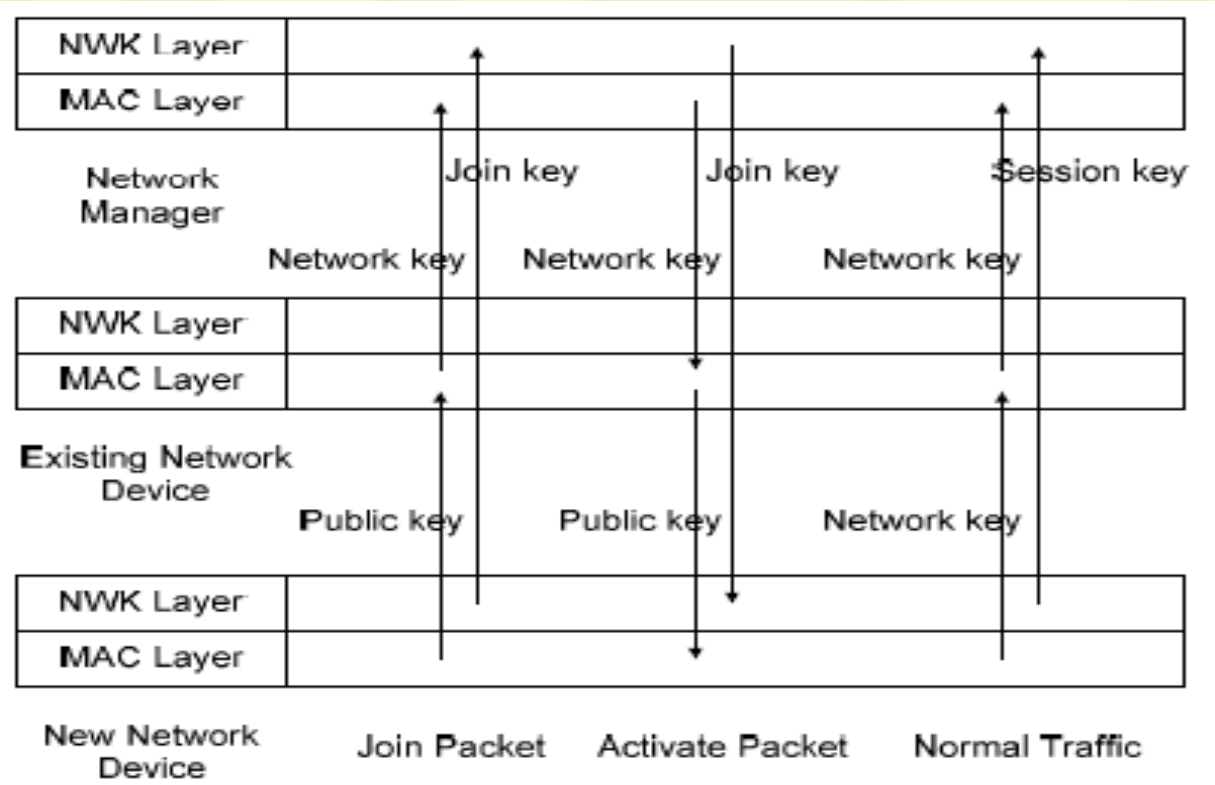

Figure 7. Keying Model

Wireless HART的构建

4、 WirelessHART的构建

- 4.1 硬件平台
- 4.2计时器和定时器中断
- 4.3 同步
- 4.4 状态机的设计
- 4.5 网络数据模型设计
- 4.6 安全

Wireless HART的构建

4.1 硬件平台

freescale MC1321X评估套件。

- 40MHz 8-bit HCS08 MCU
- 2.4GHz无线收发器，兼容IEEE802.15.4标准
- 可编程的60 KB的闪存和4KB RAM内存
- 多个16位定时器
- USB端口
- 3轴加速度传感器和温度传感器
- 4个LED和开关用于显示，监测和控制开关

Wireless HART的构建

- 4.2 计时器和定时器中断

无线HART对每个网络设备都有非常严格的时序要求。一个10ms的时隙又进一步被划分成几个时间间隔。每个长度从100us到4.5ms不等。

我们使用一个单独的16位TPM（定时器/脉宽调制模块）模块来实现计时器。TPM模块的输入时钟被设置到总线时钟（16MHz）。TPM模块包含一个自由运行计数器和一个比较计数器。每当自由运行计数器等于比较计数器，一个定时器中断就被触发 。

Wireless HART的构建

通过改变TPM模块的内部分频器，我们可以改变定时器的时钟频率
如下面公式：

$$ftimerclock = fbusclock / prescaler$$

预分频器设置为16。因此，每个定时器的精度是1us，已经足够精确满足无线HART的MAC层的需求 。

Wireless HART的构建

- 4.3 同步

对于每个进入的（DLPDU）数据链路协议数据单元，节点都记录了DLPDU的第一位到达的时间。由于严格的时隙结构，一个节点可以根据接收到的数据链路协议数据单元推导出下一时隙的起始。

依据如下公式：

$$T\text{next slot} = \text{arrival time} + 10ms - \text{TsTxOffset}$$

Wireless HART的构建

- 4.4 状态机的设计

无线HART的MAC层最主要的部分是一个复杂的状态机。每个运行的状态机包括以下三个步骤：

1，呼叫链路调度服务，以确定下一个被服务的时隙。

2，从定时器接收到“时隙开始”事件，使ASN增加1。

3，当轮到服务步骤1中的给定的时隙时，执行相关的事务。

Wireless HART的构建

大部分状态机中的代码与一个执行的事务相关联。我们在状态机中定义了六种状态：

- 加入：在这种状态下，设备尚未得到网络管理器的授权。当成功加入网络后，它便进入空闲状态。
- 空闲：当设备成功加入网络，或者结束传递/接收数据包时，它进入这种状态。
- 会话：当准备好发送数据包时，状态机进入此状态，并调用XMIT（发送）引擎。
- 等待应答：当一个非广播的数据链路协议数据单元成功地传输，状态机进入这种模式。
- 监听：此状态下，状态机调用RECV（接受）引擎等待即将传入的数据链路协议数据单元。
- 应答：在此状态，状态机构造并发送一个与与之前监听状态接收到的DLPDU相应的DLPDU。

Wireless HART的构建

- 4.5 网络数据模型设计

类似MAC层，网络层维护包括会话表，传输表和路由表的一组表。

会话在设备和它相关的设备之间建立了一个安全的数据管道。

传输表被用来支持端-端具有自动重连可信通信。它使用主机标示位，以确定该设备是否是主机或者从机。依据相应的序列号，此表也缓冲最后一个请求（在主机模式）或响应（从机模式）的有效载荷。因此，当重置定时器溢出时它允许设备重新发送请求或响应。

Wireless HART的构建

对于每个目标设备，使用图编号在路由表中可以有多个不同的条目。当生成一个网络层数据包，无线HART查阅路由表，超帧表和图表协同确定要使用的路由信息。对确定的目的地，也存在一个源路由，它主要用于网络诊断。

Wireless HART的构建

4.6 安全

在MAC层，无线HART提供数据认证服务。身份验证服务使用CCM*模式（Counter with CBC-MAC (corrected)）使用AES-128作为根本区块加密。CCM*需要4个字节的字符串作为参数（a，m，N和K）。

a: DLPDU头和有效载荷；

m:值为空（DLPDU不加密）；

N:长度为13字节，是ASN与源地址的联结；

K:长度为16字节，其值取决于节点的当前状态。

Wireless HART的构建

- 4.7 网络管理器

  无线HART中网络管理器的两个最重要功能是：

  生成路由

  通信调度

Wireless HART的构建

- 4.7.1 建立路由

基于链路上的每个节点提供的信息，网络管理器需要建立整体网络图。在这个过程中，管理器依据如下几个规则：

Wireless HART的构建

1，最少的跳数。
2，路由可通过的在线的可用设备。
3，使用信号强度来选择到邻居节点的最佳路径。
4，使用加权信号强度的组合在替代路线之间选择。
5，缩减邻居的数量为4个或更少。

Wireless HART的构建

生成整体网络图后，网络管理器开始创建以下三种图：

1，描述每个网络节点到网关的路径图；
2，网关到每个下游设备的广播图；
3，网关到每个设备的图。

Wireless HART的构建

- 4.7.2 建立通信调度

网络管理器为每个绘制的图中的设备分配时隙。所采取的策略如下：

Wireless HART的构建

- 网络管理器超帧的优先级高于数据超帧；
- 以广度优先算法搜索（breath-first search）遍历图，从网关开始，用N0，N1，…,Nn给设备标号；
- 对于持续通信的消息，每个设备都需要有一个时隙，持续通信定时器时间是60s；
- 对于最远端设备的加入请求，为每个中途网络设备到网关分配一个链接（无冗余提供）；
- 对于加入响应，通过广度优先搜索遍历图，为每个从网关到终端网络设备的中间设备分配一个链接；
- 对于数据请求，分配类似于加入请求。为每个中间设备分配一个额外的时隙；
- 如果有替代路径，则为其分配时隙。

Wireless HART的构建

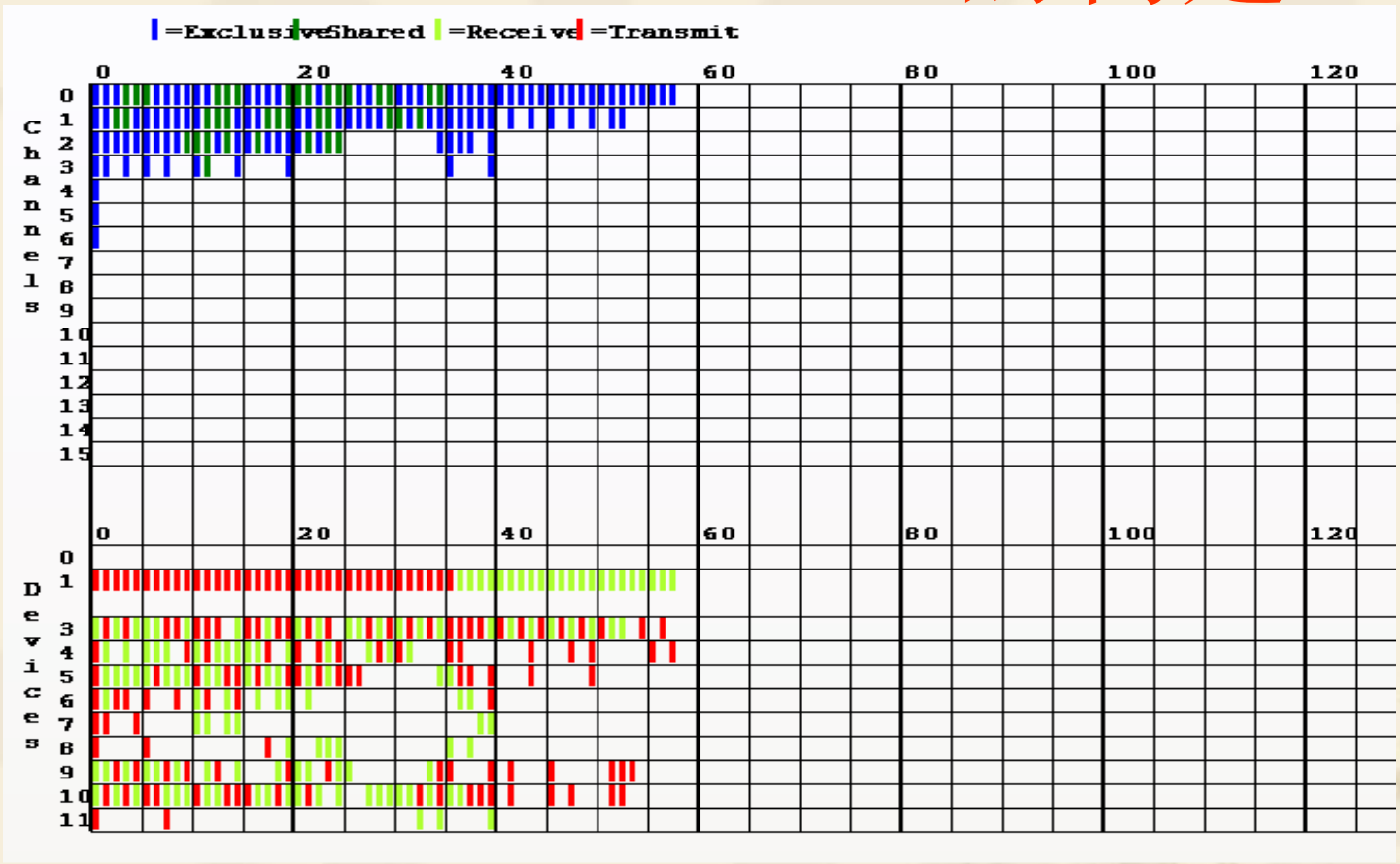

Figure 8. The Overall Schedule for the Sample Network