安全性和可靠性是工业IoT无线网络的关键

Security and reliability are key in wireless networks for industrial IoT

▶ Ross Yu 凌力尔特公司Dust Networks 产品部产品市场经理

引言

在工业物联网 (IoT) 中，从工厂和工业处理厂到建筑物能效、智能停车和商业性农业，需要在多种应用中使用无线检测和控制节点。在所有这些应用中，人们都希望工业 IoT 无线解决方案可运行很多年，且常常处于严酷的 RF 环境中和极端大气条件下。对于消费类应用而言，成本常常是最重要的系统属性，与此不同，工业应用一般视可靠性和安全性为最重要的属性。在 OnWorld 公司对全球工业无线传感器网络 (WSN) 用户进行的调查中，可靠性和安全性是参与调查者提到的两个最重要的问题 。想想看，如果一家公司的盈利能力、产品质量和生产效率及其工人的生产安全常常有赖于这些网络，那么这样的调查结果就不令人意外了。确实，工业 IoT 解决方案供应商认为，WSN 平台的选择对于其无线工业 IoT 业务的成功是至关重要的。本文将探讨数据可靠性和网络安全性对工业 IoT 应用的重要性，分析真实的案例，讨论在选择工业 IoT 无线解决方案时需要考虑的关键因素。

1 无线传感器网络的数据可靠性

在工业处理厂或工厂中，需要高可靠性是很好理解的，因为单个数据丢失点可能导致工厂停工或出现安全问题。在更广泛的工业应用中，尽管间歇性数据包丢失也许可以忍受，但是长期通信中断是不可接受的。甚至 1% 的数据误失率都太高，因为这相当于每年有 3.65 天计划外的宕机。工业 IoT 解决方案供应商也提到，半天的通信中断就会导致客户怒气冲天，而且技术人员去现场解决问题也增加了费用。如果这样的中断第二次发生，那么丢掉客户的可能性就很大。因此，工业应用需要大于99.999% 的数据可靠性，以应对在多年运行中可能遇到的多种 RF 问题。

为了让无线网络几乎无需维护地运行很多年，设计时必须采取多种方法解决问题。在设计网络时，针对可靠性的一项总体原则是提供冗余度，在此场合中，针对可能发生的问题的故障转移机制可使系统在没有数据损失的情况下从故障状态实现恢复。在无线传感器网络中，提供冗余性有两种基本方式。第一种是空间冗余概念，这时每一个无线节点都至少有两个可以通信的其他节点，并采取一种允许数据被转发到两个节点之中任意一个的路由方法，而且无论发送到哪个节点，仍然会达到原本打算到达的最终目的地。在一个恰当构成的网格网络中，每个节点都可以与两个或更多相邻节点通信，一个节点发送数据时，如果第一条通路不可用，就自动将数据发送到另一条通路上。因此，这样的网格网络比点对点网络拥有更高的可靠性。

图1 稠密的金属和混凝土环境

第二级冗余可以用 RF 频谱中多个可用通道实现。通道跳频确保一对节点每次传输数据时都可以更换通道，因此可在工业应用中典型的、严酷的且不断变化的 RF 环境中，防止由于任何给定通道出现临时问题而受到影响。在 IEEE 802.15.4 2.4GHz 标准中，有 15 个扩展频谱通道可用于跳频，从而使通道跳频系统比非跳频 (单通道) 系统的弹性大得多。有几种无线网格网络标准规定了空间和通道双冗余，称为时隙通道跳频 (TSCH)，包括 IEC62591 (WirelessHART) 和即将发布的 IETF 6TiSCH 标准。这些网

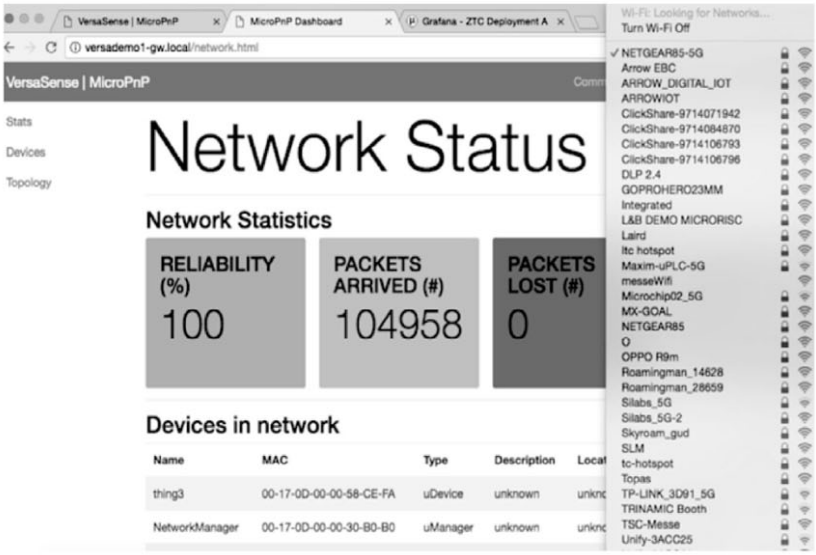

图2　在 2016 年德国慕尼黑电子展上展示网络可靠性

图3　工业 WSN 安全性

设备，还有 52个Wi-Fi网络在运行。在为期3天的展会期间，VersaSense系统在这个已经饱和的 RF 环境中，以100%的数据可靠性发送了超过 75.5Mb 数据(如图2)。

状网络标准采用全球可用和无需许可证的 2.4GHz 频谱无线信号，是以凌力特尔 Dust Networks® 的工作为基础发展而来的，2002 年 Dust Networks 通过 SmartMesh® 产品，率先在低功率、资源受限的设备中采用了 TSCH 协议。

尽管在严酷的 RF 环境中，TSCH 是实现数据可靠性必不可少的基本构件，但是就实现连续、无问题的多年运行而言，网状网络的建立和维护是关键。在其整个生命周期中，工业无线网络将面对大量不同的 RF 挑战和数据传输要求。因此，要提供如有线网络那样的可靠性，最后一个要素是智能网络管理软件，这种软件动态优化网络拓扑，连续监视链路质量，以处于存在干扰或 RF 环境变化时，最大限度提高吞吐量。

2 案例分析 1 — 半导体晶圆制造厂的 TSCH 网络

凌力尔特已经在自己位于美国硅谷的晶圆制造厂中部署了基于TSCH 的 SmartMesh IP™，以监视数百个用于各种晶圆制造的蚀刻和清洗阶段中专业气缸的压力。以前，每天对每个气缸的压力手工检查3次，每天总共需完成4个小时的手工工作。部署 SmartMesh IP 网络后，可自动进行测量，并将读数直接发给工厂的控制中心软件。在气舱中部署了32个无线节点，每个节点测量一对气缸的压力和调节的压力。该网络每秒钟总共产生 3kb 传感器数据。该工厂中的 RF 环境属于典型的工业环境，无线节点周围到处是金属、混凝土，工作人员和设备整天穿梭其间(如图1)。该网络已经连续运行超过83天，发送了超过18.8Gb数据，提供超过7个9（>99.99999%）的可靠性。

3 案例分析 2 — 在 2016 年德国慕尼黑电子展上的 TSCH 网络

展会场地是出了名的一个高噪声 RF 环境，因此也成为衡量 WSN 可靠性的不二基准。在全球最大的 2016 年德国慕尼黑电子展上，比利时的 VersaSense展示了其基于 SmartMesh IP的无线系统。这个 RF 环境极其繁忙，除了观众携带的好几千部蜂窝和蓝牙

4 网络安全的重要性

安全性是工业无线传感器网络的另一个关键属性。WSN 的主要安全目标包括：

- 保密性：除了预定接收者，任何人不能读取网络中传送的数据；
- 完整性：任何接收到的信息都已确认完全是所发送的信息，内容没有增加、删除或修改；
- 真实性：一条声称来自给定来源的信息事实上确实是来自该来源。如果将时间作为验证方法的组成部分，那么真实性还保护信息免于被录制和重放。

不仅安全相关的应用需要保密，日常应用也需要。例如，有关生产水平或设备状态的传感器信息也许有某种竞争敏感性，比如美国国家安全局 (NSA) 不公布其数据中心的功耗，因为这种数据也许被用来估计其计算资源。

传感器数据应该加密，以便只有预定接收者才能使用该数据。检测和命令信息都需要完整且不被损坏地到达。如果传感器说“罐内液位是 72cm”或 ▶▶下转第25页

◀◀上接第17页 控制器说“将阀门旋转到 90 度”，那么这两个数据无论哪一个丢失一位数字，后果都可能非常严重。

表1　网络运行统计数据 — 凌力尔特晶圆制造厂的 SmartMesh IP 网络

无线节点数量	32 个 (每个节点有 4 个传感器产生数据)
网格网络深度	从最远的节点到网关需 4 跳
整个网络的数据产生率	3Kbps
总共发送的数据	>18.8Gb，超过 83 天
数据可靠性	>99.999996% 的数据可靠性，即 7 个 9 的可靠性

对信息来源有信心是非常关键。上面两条信息无论哪一条，如果是由恶意攻击者发送的，后果都会非常严重。一个极端的例子是“这里有一个新程序供您运行”。

必须纳入 WSN 以应对这些问题的关键安全技术包括：具坚固密钥和密钥管理的强加密 (例如 AES128)；阻止重放攻击、达到密码质量的随机数字发生器；每条信息中置入信息完整性检验 (MIC)；明确允许或拒绝对特定设备进行访问的访问控制列表 (ACL)。这些最新无线安全技术也许可以毫无困难地纳入很多 WSN 中目前使用的设备，但并不是所有 WSN 产品和协议都纳入了所有安全措施 。请注意，将安全的 WSN 连接到不安全的网关是另一个脆弱点，在系统设计中必须考虑端到端的安全性。

安全性欠佳的结果并不总是很容易预期。例如，无线温度传感器或恒温器也许看起来是一种几乎没有什么安全问题的产品。然而，试想一下报纸上报道的罪犯利用无线电信号检测恒温器上的“假期”设置、然后在业主外出时入室盗窃的事情。这对客户忠诚度的影响会是巨大的，更不用说销售了。最安全的处理方法是加密所有数据。

在工业过程自动化应用中，安全攻击的后果也许比丢失客户严重得多。通过将有问题的过程控制信息提供给控制系统，攻击者可以引起物理损坏。例如，传感器馈送给电动机或阀门控制器的数据表明，电动机速度或罐内液位太低，而如果这个数据是有问题的，那么就可能导致灾难性的故障，例如类似伊朗核强化计划的离心机受到 Stuxnet 病毒攻击时所发生的事情 。就纯粹的客观情况而言，即使一次失败的攻击或研究揭示的潜在漏洞都有可能导致销售损失、需要紧急启动工程工作以及重大的攻关挑战。

5 结论

高可靠性和网络安全性是至关重要的要求，不仅对安全相关的应用和工业过程设置而言，对所有工业 IoT 应用而言也一样。幸运的是，已有经过现场验证的 WSN 解决方案可用，这使工业 IoT 解决方案供应商能够提供在富有挑战性环境中顺利、可靠地运行很多年的系统(如图3)。