zigbee alliance

zigbee: 更安全的无线物联网

概述

自 2002 年以来，zigbee 联盟及其成员公司一直致力于为构建低功耗无线物联网（IoT）的可互操作产品创建标准、认证计划和测试工具。迄今应用 zigbee 标准的设备数量在全球已经超过十亿。我们完全了解安全环境在变化不断，所以为我们的成员提供了整套的安全工具应用于其产品。随着 zigbee 3.0 标准（现简称 zigbee）在 2016 年初发布，我们为产品开发者和 IoT 生态系统中的不同厂商提供了增强版的安全工具，以便构建更为牢固的网络，及在网络安全和部署便捷之间做适当的权衡取舍。 zigbee 联盟密切关注行业安全趋势，并与研究人员和 “白客”们一起不断作出更新，以确保领先于那些新兴的威胁。

zigbee 解决方案基于联盟广受赞誉的 zigbee PRO mesh 网络协议，具备多项针对当今市场和不断演化的风险环境设计的安全新功能，比如包含了最初为 zigbee Smart Energy 智慧能源标准开发的安全功能，该功能已在全球数以亿计的电表中得到应用，至今未发现存在安全漏洞。我们与领先的无线安全专家合作推出的业界领先的安全工具帮助我们成员开发了一些迄今最为安全的无线设备。这些新功能包括：

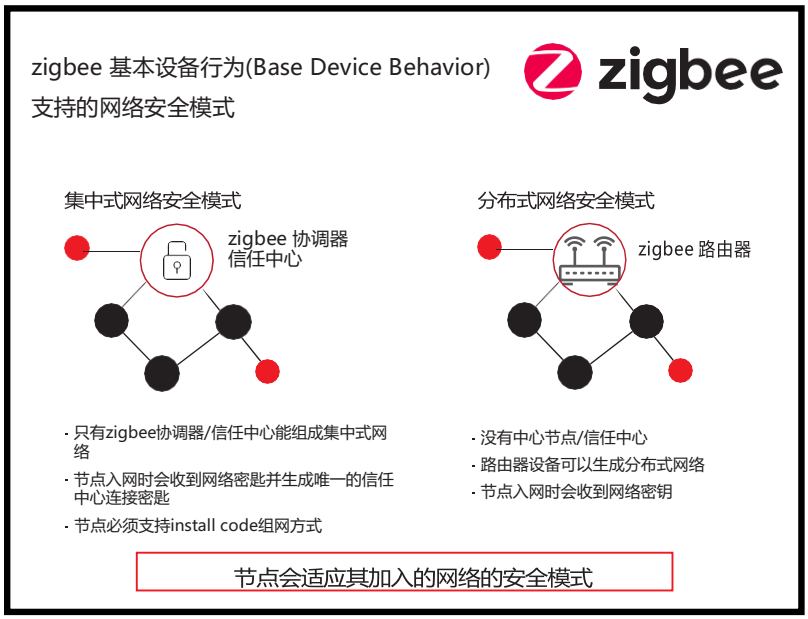
- 入网时的设备唯一身份验证
- 网络运行期间的密匙更新
- 空中固件升级（OTA）的安全措施
- 基于连接的逻辑加密

安全模式

为了适应不同的应用场景，并确保在安全性、易用性、成本效益和电池寿命之间获得最佳平衡，zigbee 提供两种网络架构和相应的安全模式：分布式网络和集中式网络，两者之间的区别在于它们解决 IoT 网络基本需求的方式不同，即：如何让新设备加入网络以及如何保护网络上传送的消息。

（1）分布式安全模式的系统较易配置，包括两种设备类型：路由器和终端设备（见下图）。如果 zigbee 路由器在启动时没有检测到已有网络，那它可以自主生成分布式安全网络。在分布式网络中，任何路由器都可以发送网络安全密钥*（network key，网络消息的加解密钥，译者注）*。随着更多的路由器和终端设备加入网络，已经存在于网络的路由器会以安全的方式发送网络密钥。网络上的所有设备都使用相同的网络密钥来加密消息。

（2）集中式系统具备更高的安全性，其包括第三种设备类型—— 信任中心（Trust Center），通常情况下实现于网络协调器（见下图）。 TC 组成集中式网络，只有路由器和终端设备拥有相关证书时才允许其加入网络。在集中式网络中，TC 是发布加密密钥的设备。在每个设备（或者一对设备）入网时，TC 还会发布唯一的 TC 连接密钥（Link Key）。



分层安全设置

最好的安全机制应使用分层设置的方法，从物理层一直到应用层。尽管物理层的安全设置超出 zigbee 标准所涉及的范围，但联盟一直在帮助我们的成员互相交流在这一领域的最佳实践方法。从协议/标准的角度来看，网络层和应用层都能提供安全方法（包括入网时的流程）。在网络层，所有设备都处于一致的安全环境之中。

Install codes *（无合适翻译，译者注）*

TC 可以要求每个新设备通过唯一的 Install Code 来加入集中式安全网络。Install Code 必须与以带外方式（out-of-band，即不通过 zigbee 网络）预先输入 TC 的密码匹配。例如，Install Code 可以用数字或二维码的形式打印在加入设备的包装中；用户或安装者可以将密码键入或扫描到连接 TC 的智能手机或平板电脑中。所有 zigbee 设备都必须包含唯一的 Install Code，这是一个由 16 位 CRC 保护的随机 128 位数字。加入设备和 TC 根据其共同的 Install Code 使用 Matyas-Meyer-Oseas（MMO）哈希算法生成唯一的 128 位信任中心连接密钥（Trust Center Link Key）。

滚动密匙（Rolling keys）

在集中式安全网络中，TC 定期地创建、分发、然后切换到新的网络密钥。因此，即便攻击者获取了网络密钥，它也将很快到期失效。TC 生成的更新的密钥会使用 TC 连接密钥加密后发送。

应用层加密

另一个关键的安全工具是能够在网络中的一对设备之间创建应用层安全连接。通过在一对设备之间创建唯一的 AES-128 加密密钥可以在网络中的任何两个设备之间建立逻辑安全连接，从而在网络的许多设备中某对设备能够形成“虚拟专用连接”。以家庭局域网为例，所有设备（例如，灯，恒温器，存在传感器，门

锁，门窗传感器和车库门开启设备）形成的网络由网络层的一组密钥进行防护 ，而对控制家庭出入户的设备（例如门锁和车库门开启设备）设定附加的一对安全密匙。这样万一攻击者获取网络密钥后能通过拦截或注入网络消息影响其他设备的操作，门户仍然固若金汤。

OTA 升级

空中升级（Over-the-air）能够帮助制造商为其产品添加新功能，修复缺陷，并在识别到新威胁时使用安全补丁。然而，如果使用的机制未能提供充分保护，或者制造商没有应用所有可用的安全措施，OTA 更新也会带来潜在的安全漏洞。 zigbee 设备和相关兼容平台为现场更新提供多层安全设置，并确保更新的代码镜像（code image）未被恶意篡改。首先，zigbee 标准用唯一密钥加密所有空中传输的镜像文件；其次，另一唯一密匙对 OTA 镜像进行签注；另外，还可以在制造期间对镜像进行加密，而只有最终产品包含相应的解密密钥。最后，镜像文件可以存储在调试读取功能设置为禁用的片上存储器中 —— 以防止使用标准调试工具进行反向工程，这是其它解决方案经常忽视的漏洞。

一旦设备接收到加密的镜像文件，其安全引导程序将在解密镜像、验证签注后再更新设备。此外，引导程序在每次设备启动时会检查当前镜像的有效性。如果镜像文件无效，引导程序将阻止它进行更新并返回最近一次有效更新后的状态。因此，镜像损坏将被快速检测到以便系统操作者可以采取行动。

其它安全技术

为防止中继攻击（即攻击者截取命令消息后进行重放，例如打灯或关灯），每个 zigbee 命令都包括一个帧计数器，接收设备检查会帧计数器并忽略重复的消息。

zigbee 还支持动态频率切换。如果当前信道受损，例如遭受阻塞攻击，则网络可以迁移至不同的信道（频率）上。

结论

zigbee 联盟及其成员公司非常重视 IoT 的安全。我们提供多种技术和安全解决方案，以满足广泛的市场需求。一些技术已经通过 zigbee 智能能源标准得到证明，zigbee 智能能源被认为是遍布全球的先进计量基础设施（AMI）的黄金标准。许多联盟成员公司本身就是安全领域的专家，作为领先的无线标准制定组织，我们也经常与研究机构和商业安全专家沟通交流来完善我们的解决方案和审核已经完成的标准和技术指标。

要了解有关 zigbee 联盟的更多信息以及我们如何努力使 IoT 更加安全，请访问 www.zigbee.org。要了解更多加入联盟参与解决方案制定的信息，请访问 www.zigbee.org/zigbeealliance/join/。

附录：zigbee 的安全算法

zigbee 标准（以前称为 zigbee 3.0）使用的经过验证的算法包括：

•128 位 AES - CCM *用于消息加密、验证和完整性（根据 NIST FIPS Publication 197）

•Hash Message Authentication Code 哈希消息验证码（根据 NIST FIPS Publication 198）

•Matyas-Meyer–Oseas hash function MMO 哈希函数，用于从 Install Code 中导出预配置的连接密钥（根据 Handbook of Applied Cryptography 应用密码学手册）