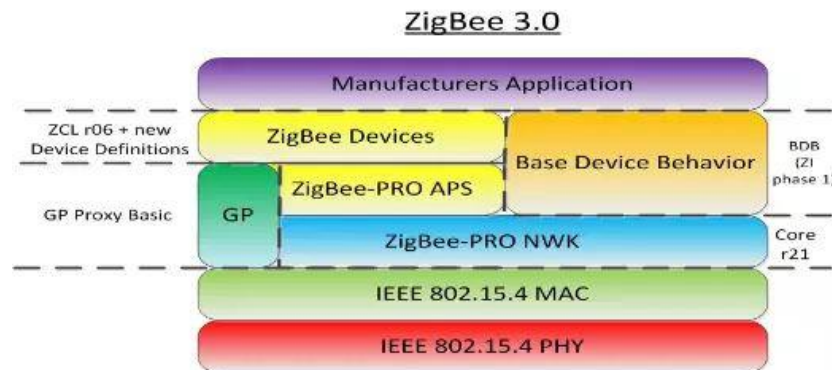


ZigBee3.0 安全探究

ZigBee 3.0

ZigBee 已经成为低功耗、低数据传输率无线网络的领先标准之一。ZigBee 3.0 在现有 ZigBee 标准的基础上构建，旨在帮助最终用户更加轻松地选择、设置和操作产品。



ZigBee Standard Security

在 ZigBee 协议栈架构中，安全是一个非常重要的关注点。Standard Security 是所有的 ZigBee 应用规范都使用的安全模型，包括 ZigBee3.0。Standard Security 分别使用 Network Key 和 Link Key 在网络层和 APS 层加密数据。APS 层安全允许 Trust Center 来安全传输 Network Key 给加入节点或拒绝节点加入，并且它允许应用来增加可选的安全加密消息。网络层安全用来保证所有的 ZigBee 网络中发送消息的安全性。Standard Security 不包括 MAC 层的通信（比如 association，数据请求 polling，MAC ACKs）。

Different Keys in Standard Security

Standard Security 定义了不同类型的 Keys，使用不同的方式来保证数据的安全。所有的 Keys 都是用 128 位对称密钥（AES-128）来解密和加密数据包。

Network Key

Network Key 用来保证网络层的安全传输。所有 Standard Security 网络中的设备都会对 Network Key 进行备份。Trust Center 可以周期性的更新 Network Key。Trust Center 通过两种方式进行更新：广播更新或单播更新。在广播更新的情况下，Trust Center 首先广播新的 Network Key，此时使用旧的 Network Key 来对广播消息进行加密。在单播更新的情况下，Trust Center 发送新的 Network Key 给每一个设备，此时使用 Trust Center Link Key 来对其进行加密。当新的 Network Key 发送给各网络节点之后，Trust Center 再发送一条转换命令告诉所有的设备转换为新的 Network Key。新 Network Key 对应一个序列码，这个序列码在旧的 Network Key 序列码基础上加 1。

- 所有的 ZigBee 相关的 Key 的长度都是 128 Bit。
- 所有加入安全网络中的设备都拥有一个对 Network Key 的备份。

Trust Center Link Key

Trust Center Link Key 用于两个节点（其中有一个节点是 Trust center）之间的端到端的安全通信。在以下情况下使用 Trust Center Link Key：

- 当节点初次加入网络时，需加密传输 Network Key 到加入节点。
- 当 Network Key 更新时，有些节点因未接收到新的 Network Key，因此需要 Rejoin。此时，Trust Center 使用 Trust Center Link Key 加密 Network Key 发送给该重新入网节点。
- 路由器向发送给 Trust Center，或从 Trust Center 接收 APS 安全消息时，需要使用 Trust Center Link Key。比如路由器发送节点加入或 Rejoin 的更新给 Trust Center 时，或由

Trust Center 发送到路由器以执行一些安全功能的命令时， 需要使用 Trust Center Link Key。

- 启用 APS 加密的应用程序单播消息， 其中发送或接收设备是 Trust Center。 由 Trust Center 决定如何管理 Trust Center Link Key 的选项。它可以为每个设备选择唯一的密钥（从设备的 IEEE 地址导出的密钥）， 或者对于所有的设备采用相同的全局密钥。

Installation Code Keys

ZigBee 3.0 支持 Installation Code Key， 在之前只用于 Smart Energy Network（智能能源网络）， Smart Energy Network 必须使用 install code。现在所有 ZigBee 3.0 认证设备都需要支持 install code， 但是由 Trust center 决定是否在网络中使用。

Install code 用来预配置 Trust Center Link Key， 其用于加入 ZigBee 网络时对 Network Key 的传输进行加密。在进入网络时， 加入设备和 Trust Center 都必须知道这个唯一的密钥， 所以 install code 用于在两端导出密钥。Install code 可以是 6, 8, 12 或 16 字节的任意值， 再末尾加上这些字节的 16 位 CRC（最低有效字节优先）。Install code 用作 Matyas-Meyer-Oseas (MMO) Hash 散列函数的输入， 其散列长度等于 128 位。该 AES-MMO 哈希函数的 128 位（16 字节）结果就是用作该设备的预配置 Trust Center Link Key 的值， 并且 Trust Center 可以安装密钥表条目（该密钥和加入设备的 EUI64）， 其然后允许在加入网络期间成功地进行认证， 加入设备可以成功地接收和解密 Network Key。作为此过程的一部分， Install code 和加入设备的 EUI64 必须在带外传送（目标 ZigBee 之外网络， 因为新节点尚未加入）到网络的 Trust Center。

Joining a Network

设备加入 ZigBee Standard Security 网络时， 首先向父节点发送 MAC 关联请求。 如果关联成功， 则设备处于已加入但未认证状态， 此时它不具有 Network Key。父节点给设备发送 MAC 关联成功的响应之后， 再向 Trust Center 发送更新设备消息， 指示新节点希望加入 ZigBee 网络。 然后由 Trust Center 决定是否允许设备加入。如果不允许设备加入， 则向父节点发送移除设备（Remove device）请求。 如果允许该设备加入， Trust Center 则向父节点发送 Network Key， Trust Center 的行为取决于设备是否具有预配置的 Trust Center Link Key。

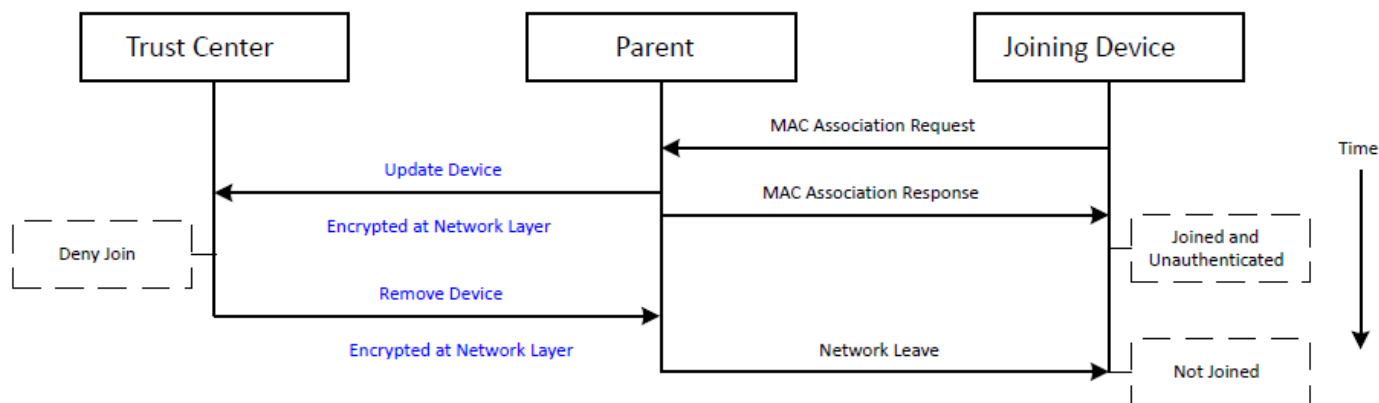


Figure 3.2. A Device that is Denied Access to Join the Network

Preconfigured Link Keys

Trust Center 规定了如何处理新设备和确定设备是否应该具有 Preconfigured Link Key。 如果新设备没有 Preconfigured Link Key， 它将无法加入网络。Trust Center 可以选择该密钥是 Default global Link Key (ZigBeeAlliance09) 还是 installation code。 下图说明了使用 Preconfigured Link Key 的加入网络的过程。 为了允许设备加入到网络， Trust Center 发送 Network Key（使用 Preconfigured Link Key 加密）给父节点。 ZigBee 3.0 和所有 ZigBee 应用程序配置文件需要 Preconfigured Link Key 才能加入。

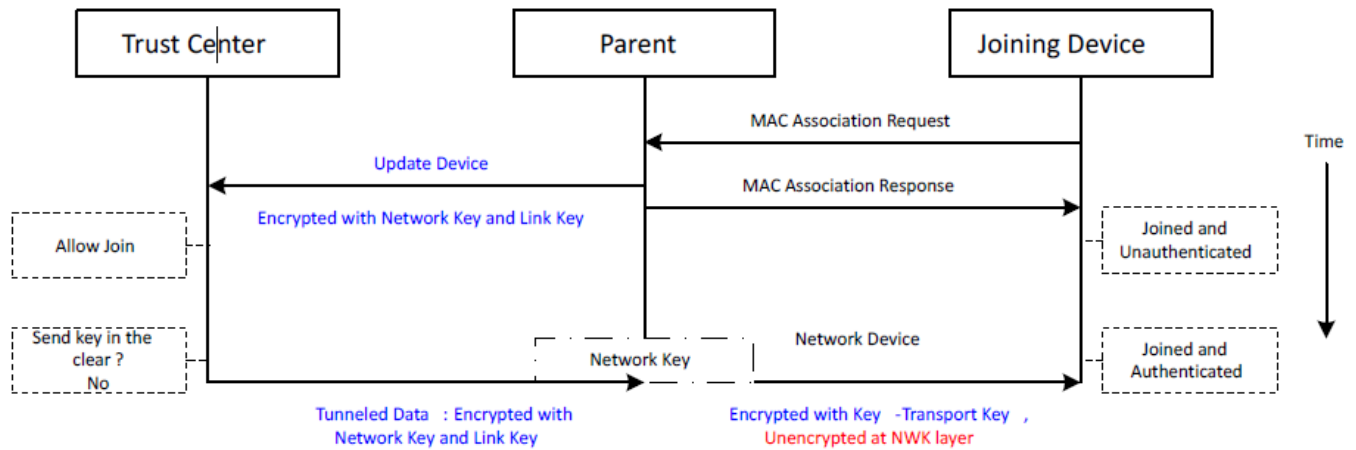


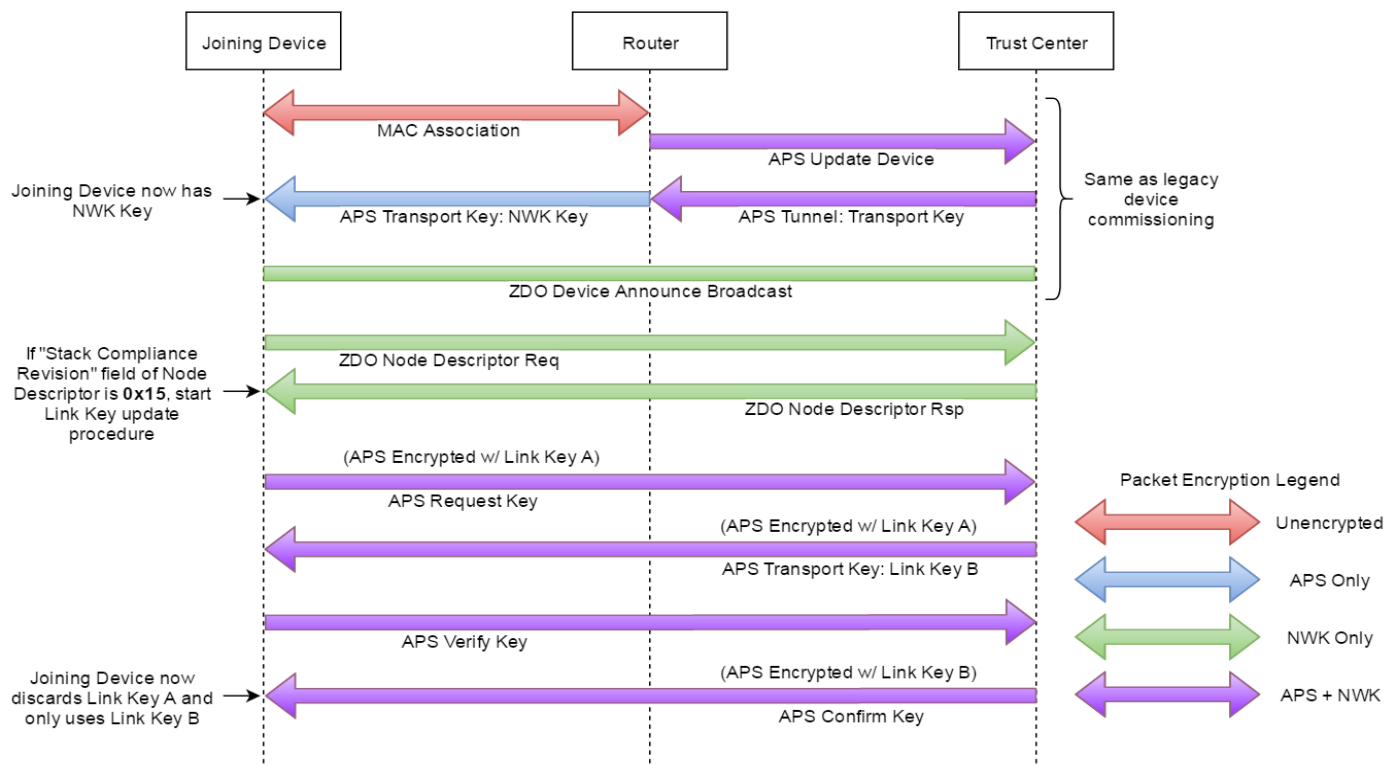
Figure 3.3. Joining Using a Preconfigured Trust Center Link Key

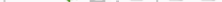

Preconfigured Link Keys or Installation Code

Trust Center 是使用 Well-Known Key (例如 ZigBeeAlliance09) 还是 Installation Code, 取决于易用性和安全性之间的平衡。使用 Well-Known Key 使设备能够更容易地加入网络, 而无需大量的用户交互。然而, Well-Known Key 加密 Network Key 提供了一个脆弱的时刻, 直到该 Well-Known Key 被替换为新的密钥。使用 Installation Code 为 Network Key 到设备的初始交换提供了安全性, 代价是用户和 Trust Center 之间增加了交互。用户必须以某种方式将密钥从设备传输到 Trust Center。这是通过 ZigBee 网络之外的机制来完成, 例如从列出加入设备上的代码的标签将代码输入到 Trust Center GUI 中; 在加入设备上运行的主应用程序。在网络上运行的主要应用程序将帮助决定是否易于使用与更好的安全性谁更重要。

Joining a ZigBee 3.0 Network

ZigBee 3.0 设备成功加入网络后, 设备需要请求更新的 Trust Center Link Key 以替换它们现有的 Preconfigured Link Key。即使使用 Installation code 的设备, 也将替换成新的 Trust Center Link Key。下图说明了 ZigBee 3.0 设备如何更新 Trust Center Link Key。




No Filters


如果是一个 ZigBee3.0 网络，将会更新替换默认的 Trust Center Link Key

Update a new Link Key

Navigation icons: Home, Back, Forward, Search, and a dropdown menu labeled "No Filters".

Network Key不变

ZigBee3.0 设备在加入网络后，需要在 EEPROM 中保存更新后的 Link KeyB，用于后续重新入网。如果在开发、测试过程中擦除了整个 EEPROM 内容，将会导致设备无法重新入网。