Technical Article

The Key to Security: Zigbee 3.0'S Security Features

Kirtana Moorthy

As a consumer, my world is built on ease of use and device interoperability; at home, I can control my connected smart lighting, heating and security system from my phone or an Amazon Echo. The wireless protocols powering these networks, such as Zigbee or Thread, offer distinct advantages and trade-offs including power consumption, network management, latency and more.

For home and building automation, Zigbee prioritizes something that cannot slip through the cracks: security. Wireless home or industrial networks can be tempting targets for hackers looking for data. Without proper security safeguards, home or building security systems are vulnerable to attackers looking to disable these systems, tamper with them or steal information.

Zigbee is an industry-proven worldwide standard for low-power, self-healing, robust mesh networks offering a complete and interoperable Internet of Things (IoT) framework for home and building automation systems. Zigbee 3.0, the latest specification from the Zigbee Alliance, incorporates improved security and robustness features such as trust center link key updates and install code enhancements to counter threats every day.

New Features

Zigbee 3.0 provides well-defined security procedures to request and change keys. In a Zigbee network, two devices must share the same keys in order to communicate.

There are two layers of encryption in Zigbee: the application support sublayer (APS) and the network layer (NWK). Previously, it was not mandatory to update the APS layer encryption key after joining the network.

The new functionality mandates that devices joining a Zigbee 3.0 centralized network must request a randomly generated trust center link key upon joining the network, which is used for all ongoing encrypted APS-layer communication.

This feature provides significant additional security to the system because a device won't compromise the NWK key if it leaves and tries to rejoin the network; there is a second layer of mandatory encryption. As Figure 1 shows, Zigbee 3.0 coordinators are configurable to accept or reject legacy devices that do not initiate the trust center link key update procedure.

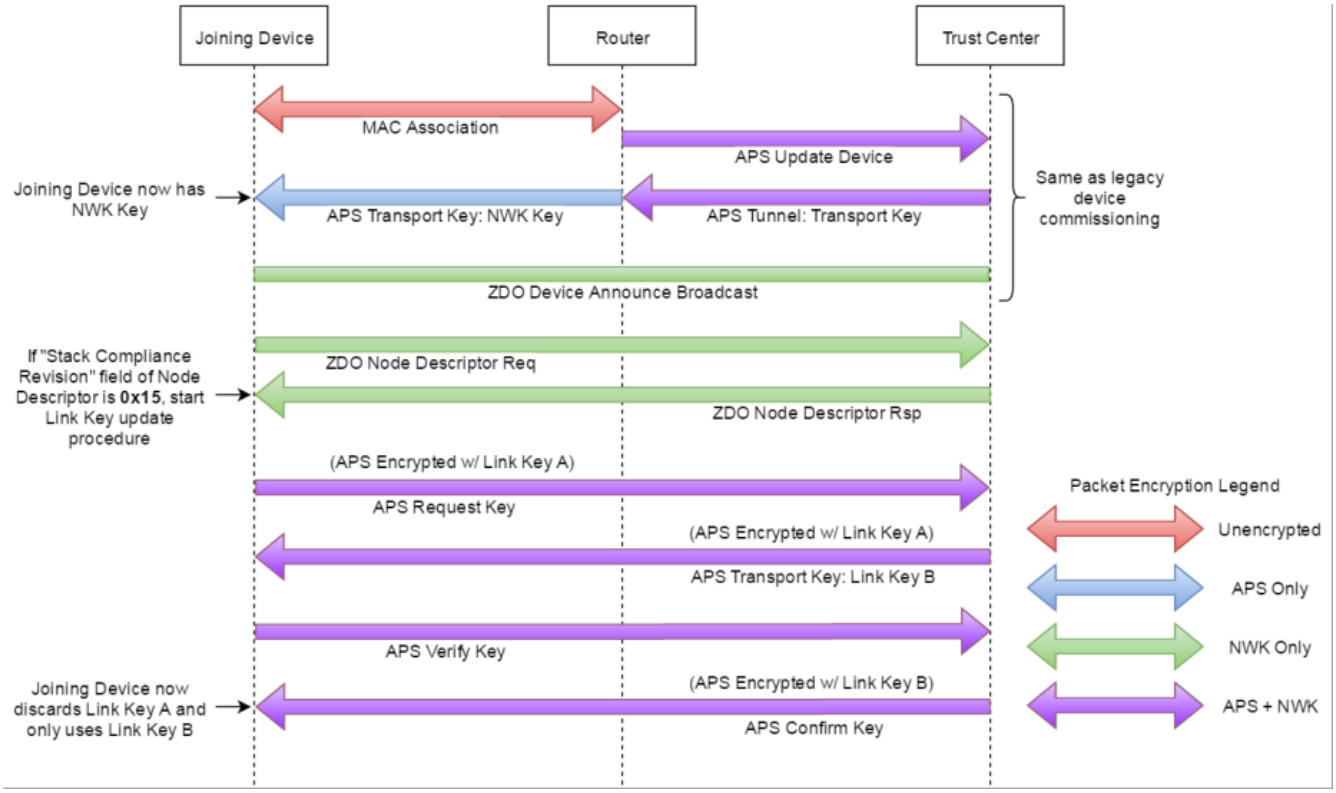

Figure 1. Diagram of a Zigbee 3.0 Network Allowing a Device to Join

To enhance security even further, Zigbee 3.0 now offers the option to use pre-configured keys and install codes. Install codes are 128 bits of random data and a 16-bit cyclic redundancy check (CRC) that pass through a hash function to generate a trust center link key. Instead of using the global trust center link key to obtain the NWK key, Zigbee 3.0 enables developers to generate these keys with install codes.

Trust center link keys eliminate the use of well-known keys such that no well-known key is ever used to encrypt data over the air, making the system significantly more secure. Generally, install code-derived trust center link keys are hard-coded into devices during manufacturing, and the corresponding install code is included with the device and programmed into the network leader through an out-of-band method such as a user interface.

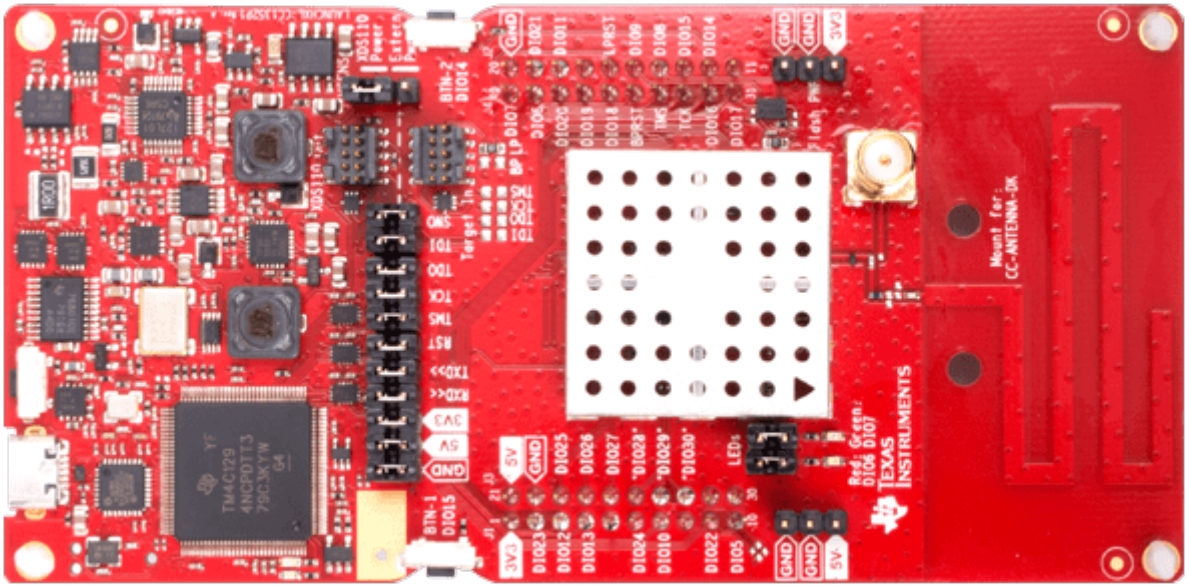

Figure 2. LAUNCHXL-CC1352P Front View Horizontal

For IoT home and building automation systems, Texas Instruments (TI) SimpleLink™ CC1352P (shown in Fig. 2) and CC2652R devices integrate features such as:

- Advanced Encryption Standard 128-/256-bit crypto accelerators for more efficient encryption, yielding lower-power operation.
- A 20-dBm integrated power amplifier for long-range applications.
- A low-power sensor interface to sense while the device sleeps.

TI's royalty-free Zigbee software development kit (SDK) offers:

- Z-Stack™ software, a Zigbee 3.0-compliant stack.
- Software examples for common applications (including electronic door locks, light switches and temperature sensors).
- Comprehensive documentation and training to jump-start development.

The Zigbee software architecture is shown below in Figure 3.

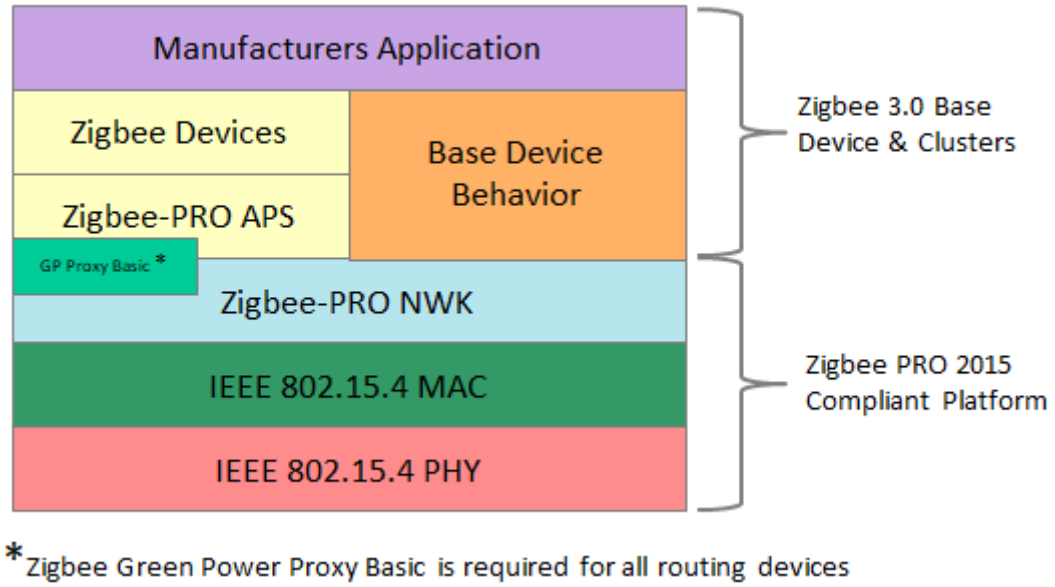

Figure 3. Zigbee Software Architecture

Conclusion

It is possible to build connected IoT home and building automation systems without the fear of malicious hackers or cybersecurity threats; Zigbee 3.0 is the key to a secure home and building network.

Additional Resources

- Learn more about other Zigbee 3.0 security updates in the white paper, "What's New in Zigbee 3.0."
- Check out the "Zigbee Selection Guide for SimpleLink MCUs."
- Order the CC26x2R wireless microcontroller (MCU) LaunchPad™ development kit.
- Learn more about SimpleLink MCUs and the SimpleLink CC26x2 SDK.
- Read the application report, "Z-Stack 3.1.0 End Device Power Consumption Measurement with the SimpleLink Wireless MCU Family."

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265