zigbee alliance

zigbee: Securing the Wireless IoT

Introduction

Since 2002, the zigbee alliance and its member companies have created standards, certification programs, and tools to develop interoperable products for the low-power wireless Internet of Things (IoT). Zigbee standards are in well over a billion devices worldwide. We are very aware of the ever-changing security landscape, and provide our members with a complete set of security tools to use in their products. With the release of the ZigBee 3.0 standard (now referred to simply as zigbee) in early 2016, we provided an enhanced toolbox for product designers and eco-system owners to implement robust networks and choose the right balance of security policies and ease of deployment. The zigbee alliance monitors security trends in the industry and works with researchers and white hats to continuously update offerings to stay ahead of emerging threats.

The zigbee solution, built on the alliance's award-winning zigbee PRO mesh-networking protocol, has several important new security capabilities designed for today's market and evolving risks. Zigbee incorporates features originally developed for zigbee Smart Energy, which hundreds of millions of revenue-grade utility meters use worldwide with no known security breaches. We have engaged with leading wireless security experts to provide several state-of-the-art security tools that allow our member companies to create some of the most secure wireless devices available today. A few of these updated features include:

- Device-unique authentication at joining
- Runtime key updates during operation
- Secure over-the-air (OTA) firmware upgrades
- Logical link-based encryption

Security models

To satisfy a wide range of applications and to ensure the optimal balance of security, ease of use, cost and battery life, zigbee offers two network architectures and corresponding security models: distributed and centralized. These differ in how they address basic requirements of IoT networks: admitting new devices into the network and protecting messages on the network.

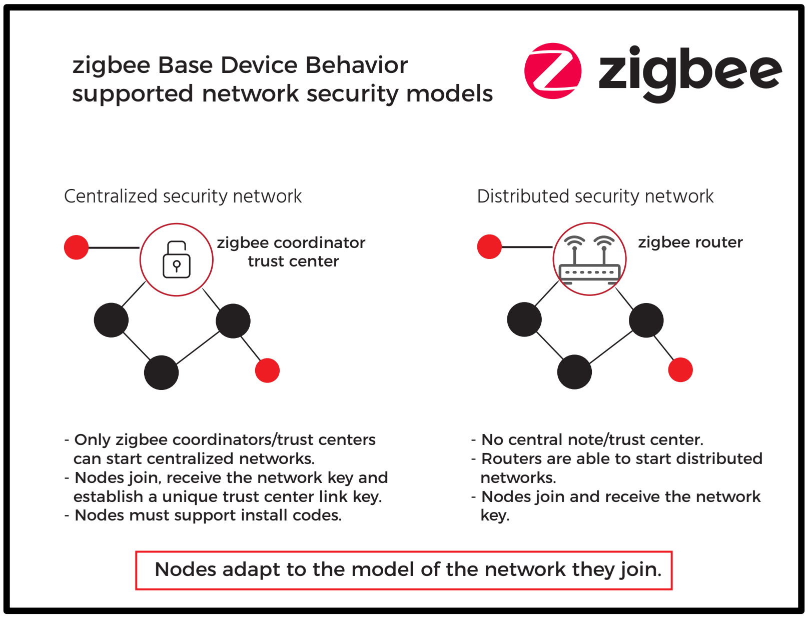
> (1) For easier-to-configure systems, a distributed security model comprises two device types: routers and end devices (see following graphic). If a zigbee router does not detect an existing network when it powers up, it can form a distributed security network. In a distributed network, any router can issue network security keys. As more routers and end devices join the network, a router that is already on the network securely sends the network key. All devices on the network use the same network key to encrypt messages.
>
> (2) For higher security, centralized systems include a third device type – the Trust Center (TC), which is typically also the Network Coordinator (see graphic). The TC forms a centralized network and allows routers and end devices to join the network if they have proper credentials. In a centralized network, only the TC can issue encryption keys. The TC also establishes a unique TC Link Key for each device on the network as they join and link keys for each pair of devices as requested.

Layered security

The best security uses a layered approach, starting with physical security and progressing all the way to the application layer. While physical security is out-of-scope for zigbee standards, the alliance does facilitate the exchange of best practices in this area between our members. From a protocol/standards perspective, both the network and application layers provide security capabilities (in addition to the procedures associated with joining a network). At a network level, all devices in the network are under the same security environment.

Install codes

The TC may require that each new device use a unique Install Code to join a centralized security network. The install code must match a code previously entered into the TC out-of-band (i.e., not using a zigbee message). For example, the install code may be printed as a number or QR code in the packaging of the joining device; the user or installer may type or scan the code into a smartphone or tablet that is connected to the TC. All zigbee devices must contain a unique install code, which is a random 128-bit number protected by a 16-bit CRC. The joining device and the TC derive a unique 128-bit Trust Center Link Key from the install code using the Matyas-Meyer-Oseas (MMO) hash function.



zigbee Base Device Behavior
supported network security models

- Only zigbee coordinators/trust centers can start centralized networks.
- Nodes join, receive the network key and establish a unique trust center link key.
- Nodes must support install codes.

- No central note/trust center.
- Routers are able to start distributed networks.
- Nodes join and receive the network key.

Nodes adapt to the model of the network they join.

Rolling keys

In centralized security networks, the Trust Center periodically creates, distributes, and then switches to a new network key. Thus, if an attacker acquires a network key, it will have a limited lifetime before expiring. Updated keys are sent encrypted with the TC-generated TC Link Key.

Application-layer encryption

Another key security tool is the ability to create an application-level secured link between a pair of devices in the network. This is managed by establishing a unique set of AES-128 encryption keys between a pair of devices. This allows logical, secured links between any two devices in the network; thus supporting “virtual private links” between a pair of devices in a network with many others. An example is a home area network where all devices (e.g., lights, thermostats, occupancy sensors, door locks, window sensors, and garage door openers) are in one functional network (properly secured at the network level with a common set of credentials), while an additional set of security credentials is established for devices that provide physical access to the home such as door locks and garage door openers. This limits the ability of an attacker that acquires the network key from intercepting or injecting messages that other devices would act upon.

OTA upgrades

Over-the-air (OTA) updates allow a manufacturer to add new features, fix defects in its product, and apply security patches as new threats are identified. However, OTA updates also represent a potential security vulnerability if the protocol does not provide ample protections, or the device manufacturer does not use all available safeguards. Zigbee devices and associated silicon platforms provide multi-layered security to update devices in the field and assure that updated code images have not been modified maliciously. First, the zigbee standard provides a method to encrypt all image transfers over the air with a unique key. Second, the standard provides a method to sign the OTA image with another unique key. Third, the image may be encrypted during manufacturing so that only the end product contains the key to decrypt it. Finally, the image may be stored in on-chip memory that is configured with the debug read-back feature disabled – preventing reverse engineering with standard debug tools, which is a common vulnerability of other solutions.

Once a device receives an encrypted image, its secure bootloader decrypts the image, validates the signature, and then updates the device. Further, the bootloader checks the validity of the active image each time the device boots. If the image is invalid, the bootloader prevents it from updating and returns to using the previous known good image. Thus, image corruption will be quickly detected, and the system operator can take action.

Additional techniques

To stop replay attacks (in which an attacker could record and replay a command message to, for example turn lights on or off), every zigbee command includes a frame counter. The receiving device checks the frame counter and ignores duplicate messages.

Zigbee supports frequency agility. The network may be relocated on a different channel (frequency) if the current channel is impaired, for example, by a jamming attack.

Conclusion

The ZigBee Alliance and its member companies take IoT security very seriously. We provide several technology and security solutions to meet a broad set of market requirements. Some of the technologies are proven in ZigBee Smart Energy, which is considered the gold standard for advanced metering infrastructure (AMI) around the world. Many alliance member companies are specialists in security, and as a leading wireless standards organization we engage often with research and commercial security experts to contribute to our solutions and to audit our finished standards and specifications.

To learn more about the ZigBee Alliance and how we are working to make the IoT more secure, please visit www.zigbee.org. To learn more about joining the alliance and becoming part of the solution, visit www.zigbee.org/zigbeealliance/join/.

Appendix: Zigbee's security algorithms

The zigbee standard (formerly referred to as ZigBee 3.0) uses these proven algorithms, among others:

- 128-bit AES-CCM* for message encryption, authentication and integrity (per NIST FIPS Publication 197)
- Hash Message Authentication Code (per NIST FIPS Publication 198)
- Matyas-Meyer-Oseas hash function to derive pre-configured link keys from install codes (per Handbook of Applied Cryptography)