MAXIMIZING SECURITY IN ZigBee NETWORKS

Security in the 'Internet of Things' (IoT) has been the subject of much concern and debate. ZigBee is one of the main protocols for use in home-based and office-based wireless networks that form part of the IoT, and ZigBee's security and privacy provision has therefore attracted close attention in the popular media. This document highlights the ZigBee security features and provides guidance on how to maximize the security of ZigBee wireless network products.

INTRODUCTION

The Internet of Things (IoT) is broadly accepted to mean a global IP network of everyday electrical devices (e.g. printer, washing machine, door-lock) that are able to send, collect or exchange data across the network. Since these devices are in our homes and workplaces, and in our general surroundings, there is often suspicion, fear and distrust concerning their security features and associated privacy.

Within a particular locality, such as a home, IoT devices may be interconnected in a ZigBee wireless network, which is itself connected to the Internet and the wider world via an IoT Gateway. There has been concern in the world press over how secure a ZigBee network is, fueled by the fear of the hacking of IoT devices to collect personal data from them and to possibly control them for criminal intent – for example, to release an electronic door-lock in order to gain unauthorized access to a property.

The ZigBee specification actually makes provision for highly secure wireless networks, but the security features are optional and the level of security offered by a ZigBee product depends on which of these features, if any, the product manufacturer has chosen to implement. The required or desired security features depend, of course, on the nature of the product – for example, a heating thermostat may not need any security while a door-lock will need strict security.

ZigBee SECURITY FEATURES

The ZigBee protocol has gone through a number of iterations over the years and the latest version is ZigBee 3.0. Rather than describe specific ZigBee versions, we will group them together simply as 'ZigBee'. This is possible because all the versions of ZigBee have kept backwards compatibility as an ongoing feature, although each iteration has made improvements to security and general interoperability. It is therefore possible for all ZigBee devices to interoperate and exchange messages in the same network.

The ZigBee standard includes a number of security features, including:

- Access control lists
- Frame counters
- Encryption of over-the-air communications

Relating to the last point, two devices that exchange data over an encrypted bidirectional link must share a common secret or set of parameters to encrypt and decrypt the messages that are exchanged. This secret is a symmetric security key which is used in the encryption/decryption process. ZigBee mandates the use of an Advanced Encryption Standard (AES) block cipher that employs a 128-bit key. Different levels of security are available relating to the encryption options.

CENTRALIZED TRUST CENTER

In a traditional secured ZigBee network, the security is centralized by means of a single node which can authenticate devices that attempt to join the network, allow/disallow network membership and distribute security keys. This node is called the Trust Center and is usually the network coordinator that created the network.

NETWORK KEY SECURITY

As part of the node authentication process during network joining, the Trust Center sends an encryption key to the joining device. This randomly generated key is common to all nodes of the same network and is called the network key. Nodes must use this key at the network level to encrypt/decrypt the general protocol maintenance data that they exchange. In some applications, this key is also used to encrypt/decrypt user data.

When distributed to a new node, the network key itself is encrypted with a pre-configured key that is known to the Trust Center and the node. This pre-configured key is not used again by the node but may be used by the Trust Center to authenticate other joining nodes.

LINK KEY SECURITY

It is also possible for two nodes in the same network to have a unique key shared only between these two nodes for the encryption/decryption of communications between them. This is called an application key or link key. This key provides application level security which is additional to that provided by the network key – messages between the two nodes are encrypted with both the network key and link key, providing two tiers of security.

Initially, a joining node may have a pre-configured link key for encrypted communications with the Trust Center, where this key is used to securely transport the network key from the Trust Center to the node. The Trust Center may then pass a new random key to the device. If link key security is enabled for the network, this unique link key will subsequently be used to secure communications with the Trust Center, but in any case it will be used by the device to rejoin the network later if needed.

The newly authenticated device may also need to communicate with another device in the network using application layer encryption requiring a unique link key to secure the messages that they exchange. Once a network node has established a secured link with the Trust Center, the latter can act as a broker to provide this unique link key for communication between the other two nodes. This is a random key generated by the Trust Center and the uniqueness of the key depends on the base random number generator on the Trust Center.

CERTIFICATE-BASED KEY ESTABLISHMENT

Some ZigBee application profiles, such as Smart Energy, employ Certificate-Based Key Establishment (CBKE) to derive a unique key to secure communication. Every device in the network is required to store a certificate issued by a trusted certification authority. From the certificate, it is possible to generate a public key and other security elements. The CBKE method provides a mechanism to safely identify a device and to allow it to start communicating. A key establishment procedure involves the following four steps:

1. Exchange static data (certificate validation) and ephemeral data
2. Generate the key
3. Derive a Message Authentication Code (MAC) key and key data
4. Confirm the key using the MAC

For the second and third steps, the key establishment procedure refers to the Elliptic Curve Menezes-Qu-Vanstone (ECMQV) key agreement scheme and a key derivation function respectively. At the end of this process, the Trust Center and the authenticating device share a new link key that will be used to protect data communications between them.

NETWORK SECURITY TYPES

Security in a ZigBee network is usually organized through a single node, the nominated Trust Center, which is often the ZigBee coordinator. The role of the Trust Center is to authenticate devices that attempt to join the network and distribute security credentials. The choice of Trust Center and the Trust Center policy is the most important decision in creating a ZigBee network.

As an alternative to the above centralized security network, ZigBee 3.0 allows de-centralized security management through a distributed security network. The two network security types are summarized below:

- **Centralized security:** Trust Center allows devices onto the network and distributes keys. It has a view of every node that has been authenticated onto the network.
- **Distributed security:** Every ZigBee router authenticates and distributes keys to devices that attempt to join the network as children of the router. In this case, there is no central node which has a view of all the authenticated nodes.

The authentication policies, the distribution and storage of authentication data, and the commissioning method all determine how secure a ZigBee network is. The ZigBee specification does not mandate any particular security policy and the choice is left to the solution providers.

SECURITY VULNERABILITIES

The vulnerability of a ZigBee node depends on the security features that are incorporated into its design and manufacture. These decisions play the level of security against cost and ease-of-use.

SECURITY RISKS

The main security risks for a ZigBee wireless network are:

- Theft of sensitive data from a node – This may be user data that can be used for criminal purposes but is more likely to be network security data, such as encryption keys, that will allow access to the node and network. It is therefore important to carefully select and protect the security keys used by the network.
- Theft of a node – A node may be stolen in the sense that it is removed from the current network and moved to another network where it can be accessed and controlled. This is a particular risk when Touchlink commissioning has been used (described later), but there are ways to prevent it.
- Unauthorized control of a node – This may result from the above thefts or from replay attacks in which genuine over-the-air command frames are captured and re-sent to the node at a later time to achieve subversive control. The frame counters incorporated in ZigBee security help to defeat this kind of breach but other measures, such as regularly changing the network key, can also help.
- Loss of network service – This may result from the jamming of the radio channel or whole radio band by interference. Applications can employ frequency agility to overcome this kind of impediment by moving the network to a quieter channel.

SECURITY KEY WEAKNESSES

The least secure element of a ZigBee network is the network key. It is used by all nodes of the network and although it is securely passed to a joining node encrypted with a pre-configured link key, this link key is likely to be of the ‘global’ type and susceptible to exposure. Therefore, depending only on the network key leaves a network vulnerable.

A ZigBee application profile (such as Home Automation) defines the level of security that is appropriate for itself. For example, Home Automation uses the well-known ZigBee 09 global pre-configured link key to authenticate devices onto the network and distribute the network key. ZigBee 3.0 has no application profiles but defines a base device behavior (BDB) that adopts and adapts the security functionality of the Home Automation profile. It permits use of the ZigBee 09 key, as this allows backward compatibility with legacy Home Automation devices. However, the use of this global key will create a hole in network security (see Figure 1). To achieve a high level of security, ZigBee 3.0 allows the use of install codes (see Figure 2).

SECURITY DURING COMMISSIONING

Security is a concern during the commissioning of a network. It is important that only valid devices are able to join the network and also that the network key is passed to new network members in a secure manner that does not expose the key to potentially hostile parties.

The ZigBee protocol allows various mechanisms for a node to join a network.

- **Association:** Uses the standard IEEE802.15.4 management packets to exchange network parameters. This requires the network to be open for joining. The packets are exchanged insecurely.
- **Rejoin:** Uses ZigBee-defined IEEE802.15.4 data packets to exchange network parameters. The network does not need to be open for joining.
- **Join through orphaning:** Uses ZigBee-defined IEEE802.15.4 management packets to exchange network parameters. A relationship between the joiner and the potential parent must have existed before. The network does not need to be open for joining.
- **Out-of-band:** A vendor-specific method of transferring commissioning data.

Once the device has the valid network parameters to be part of the network, it can be authenticated onto the network depending on the security policy. While the ZigBee protocol facilitates a high level of security, the security features are optional and there are certain concerns that need to be addressed when choosing which features to implement in the security policy. These concerns and associated solutions are presented below.

PROTECTING THE NETWORK KEY

The basic security provided by the ZigBee network is the encryption of data using the network key. This key is transported to the joining device during the authentication process.

The network key is never sent over-the-air unencrypted. It is always encrypted with a pre-configured link key, but having knowledge of the link key makes obtaining the network key possible by capturing over-the-air packets using an IEEE802.15.4 packet sniffer application. Exposing the network key could have a very large impact on the security of the network and its vulnerability to security attacks and hacks.

Therefore, the choice and distribution of the pre-configured link key are critical. The ZigBee specification does not mandate how to distribute the link keys and it is left to each vendor to use a mechanism for securing the keys that is suitable for their products. To properly protect the network key over-the-air, the user has the choice of using an explicit 16-byte link key which is unique for each device or using install codes, described later.

The use of a pre-configured link key to protect the network key is illustrated in Figure 1. This scheme is typical in a network based on a legacy ZigBee application profile, such as Home Automation, and may result in compromised security.

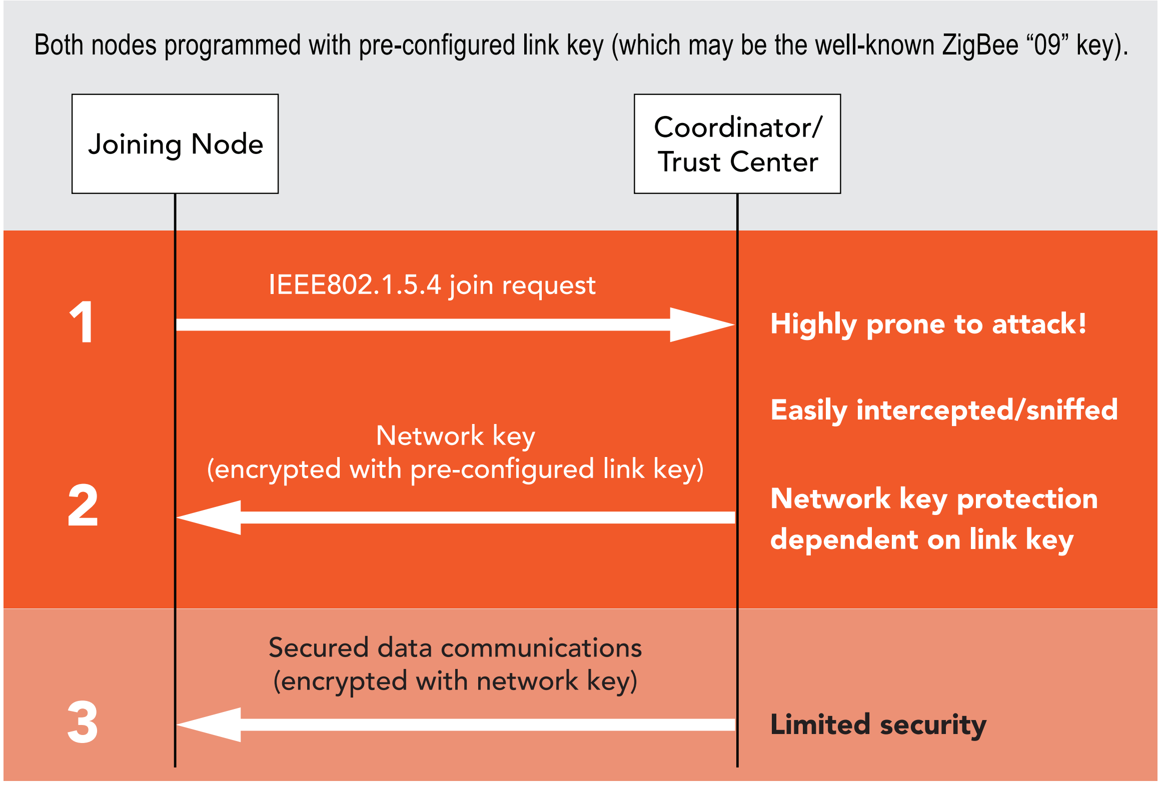
Both nodes programmed with pre-configured link key (which may be the well-known ZigBee “09” key).
Joining Node
Coordinator/ Trust Center
1
IEEE802.1.5.4 join request
Highly prone to attack!
Easily intercepted/sniffed
2
Network key (encrypted with pre-configured link key)
Network key protection dependent on link key
3
Secured data communications (encrypted with network key)
Limited security

Figure 1: Legacy security starting with pre-configured link key

INSTALL CODES

In ZigBee 3.0, an install code can be used to create the link key used to authenticate a node into a centralized security network and pass the network key to the node.

A random install code is assigned to the node in the factory and programmed into the node. The ZigBee stack within the node derives a link key from the install code using a Matyas-Meyer-Oseas (MMO) hash function. The install code must also be communicated (by unspecified means) for the purpose of commissioning the node into a network.

During commissioning, the install code is entered into the Trust Center and the ZigBee stack again derives the same link key from the install code. The Trust Center and node can subsequently use the link key in joining the node to the network.

An install code is made up of 6, 8, 12 or 16 bytes with a 2-byte CRC appended to the end. Therefore, from the user’s viewpoint, the install code consists of 8, 10, 14 or 18 bytes. It is recommended that install codes are 16 bytes long (18 bytes including the CRC). They should be randomly generated and not tied to any other credentials of the node, such as its IEEE/MAC address. Protecting the install code is vital and it should never be put on the outside of the product packaging or directly on the product.

ZigBee 3.0 also allows a unique link key to be negotiated between the Trust Center and node in order to enhance the security of communications between them.

The use of an install code and derived link key to protect the network key is illustrated in Figure 2, which also includes the negotiation of a unique link key. This scheme is available for networks that employ the ZigBee 3.0 standard and will result in very high-level security.

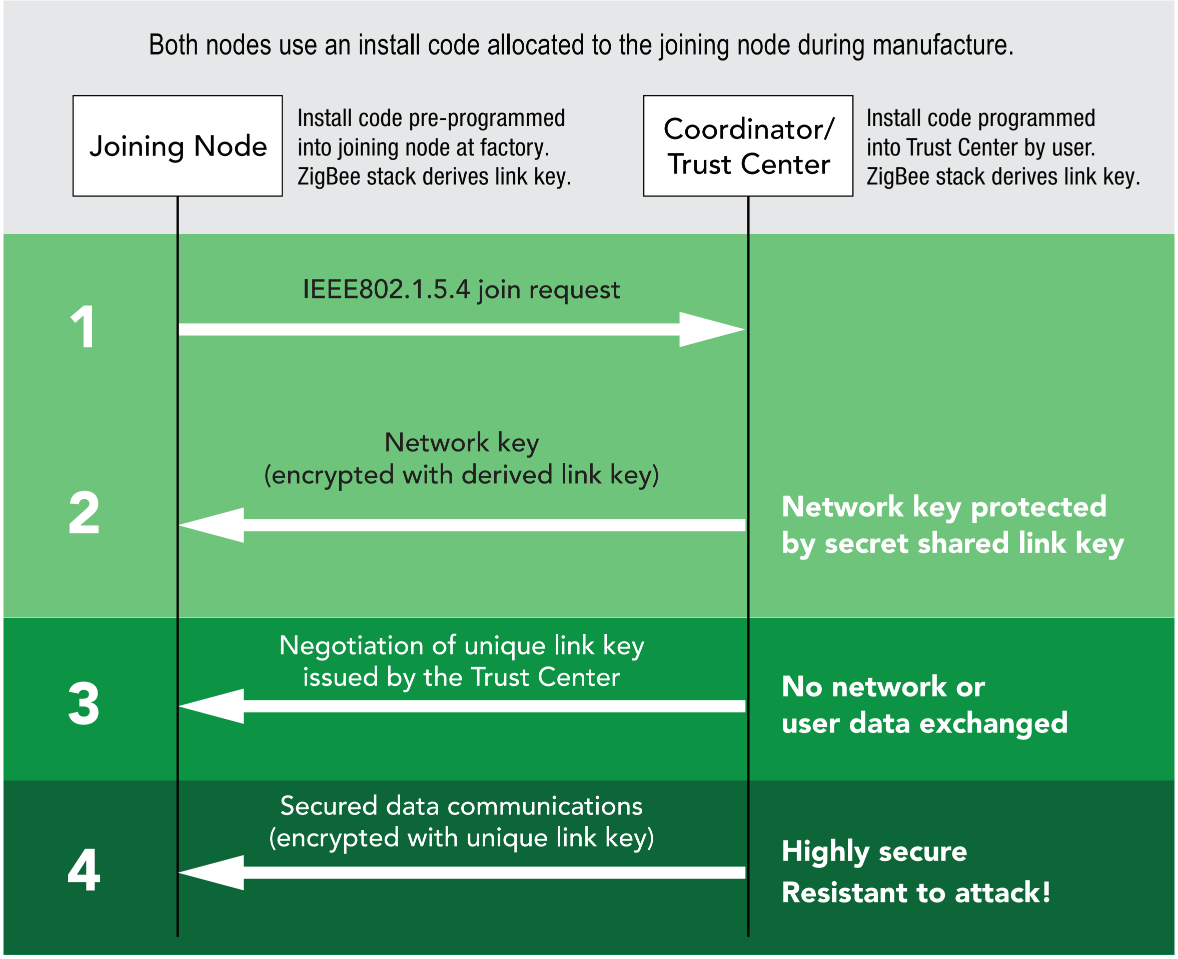
Both nodes use an install code allocated to the joining node during manufacture.
Joining Node
Install code pre-programmed into joining node at factory. ZigBee stack derives link key.
Coordinator/ Trust Center
Install code programmed into Trust Center by user. ZigBee stack derives link key.
1
IEEE802.1.5.4 join request
2
Network key (encrypted with derived link key)
Network key protected by secret shared link key
3
Negotiation of unique link key issued by the Trust Center
No network or user data exchanged
4
Secured data communications (encrypted with unique link key)
Highly secure
Resistant to attack!

Figure 2: ZigBee 3.0 security starting with install code

WHITE AND BLACK LISTS

It is recommended that a Trust Center in a centralized security network or each router in a distributed security network holds a white list (of nodes that it is allowed to authenticate onto the network) or a black list (of nodes that it is not allowed to authenticate onto the network). The nodes in each list are specified in terms of their IEEE/MAC addresses. This allows the Trust Center or router to recognize whether or not a device trying to join the network is authorized.

In addition, having a set of permissions for authorized devices helps control what the devices can and cannot do on the network. Examples of permission settings are:

- Whether the device is allowed to send 'request key' messages to obtain a unique link key for communications between itself and another network device
- Whether the device is allowed to rejoin the network—this helps to prevent some well-known security attacks on the device

TOUCHLINK COMMISSIONING

The ZigBee protocol provides an optional commissioning method called Touchlink, which is an easy-to-use proximity mechanism for commissioning a device into a network. This method works by the Touchlink 'initiator' determining the proximity of the target device (to be commissioned) and negotiating/transferring network parameters.

It is legitimate for a Touchlink initiator to send a factory-reset command to a target node already in the network, allowing the target node to be moved to another network. The process is aptly known as stealing. However, it provides a window of opportunity for an unauthorized person to move a device into another network for malicious intent.

To prevent such attacks on a distributed network and prevent nodes from being stolen, it is recommended that once a device is in the network:

- The device stops responding to inter-PAN Touchlink messages
- Touchlink is disabled on the device and only re-enabled via a manual interaction by authorized personnel

OUT-OF-BAND COMMISSIONING

During the commissioning of a node into a network, it is possible to exchange all the relevant network parameters outside of the IEEE802.15.4 domain. These parameters include the network identifiers, radio channel and even the network key. This allows the device to be authenticated and commissioned without having to exchange any over-the-air ZigBee or IEEE802.15.4 messages that can be intercepted. Since the network key is not sent out over the wireless network, it is not visible outside the device.

Some mechanisms for doing this out-of-band commissioning are as follows.

- **Pre-configuring the devices at production:** Each device is configured with the network key at production time. The device never joins a network unsecured and will only ever do a secured rejoin onto the network. This method is difficult to manage and any mistakes in configuration will render the device unusable. Also, if a whole batch of devices is hacked, all the devices in the batch will be compromised.
- **Near Field Communication (NFC):** Commissioning data is provided in an NFC tag and read out by an NFC reader. This is a highly flexible mechanism to exchange commissioning data. However, once the data is in the NFC tag, it can be easily read using any NFC reader. This makes the data vulnerable.
- **Bar codes/QR codes:** Commissioning data is encoded in a bar code or QR code. Large amounts of data can be encoded in this way. The data can easily be read using bar code/QR code readers. Again, this makes the data vulnerable.
- **Encrypted IEEE802.15.4 data exchange:** This method uses a dedicated commissioning device and proprietary network parameters to provide commissioning data to the joining device via IEEE802.15.4 messages. Again, this requires pre-configured network credentials and has the same issues as pre-configuring the devices at production.
- **Web sites:** The web hosting of security credentials is another possibility. This involves registering the device with the web site and obtaining keys/install codes online. This requires a huge database of products and needs a high level of security and management of the web sites.

Each of the above methods has its advantages and flaws. The commissioning process should be given considerable thought.

SECURITY AFTER COMMISSIONING

Once a joining device has obtained the network key, it becomes a part of the ZigBee network. This gives it access to other nodes on the network. The device should now be able to access the network parameters of other devices as well as obtain information on the services that they can provide and access these services.

PREVENTING REJOIN SECURITY ATTACKS

When a device joins the network, a pre-configured link key is used to join the network and decrypt the network key received from the Trust Center. If the same link key is used for every join attempt, it opens up the system to rejoin security attacks. Therefore, the same link key should not be used for any subsequent rejoins.

In more detail, if the same link key is allowed to be used for rejoins, it is possible to copy a device's addressing credentials and spoof a network layer insecure rejoin using a separate device. This would result in the Trust Center passing the network key encrypted with the previously used link key to the cloned device. If the network key finds its way into the wrong hands, it compromises the entire network.

To prevent this type of attack, the ZigBee 3.0 mechanism of Trust Center link key negotiation should be used. In this scheme, once the device has joined the network, it is issued with a new Trust Center link key which is randomly generated by the Trust Center and replaces the original link key. Thus, the new link key (instead of the original link key) is subsequently used for transporting the network key during future rejoins.

It is also recommended that rejoins are disabled by setting the Trust Center policy to disallow automatic rejoins with the pre-configured link key. Then if a device needs to rejoin the network, it will perform a fresh join with the pre-configured link key but, in this case, it is advised that the applications implement a mechanism for manual intervention at the Trust Center by the user in order to authorize the join.

PRIVATE NODE-TO-NODE COMMUNICATIONS

The network key is possibly the most vulnerable security feature of a ZigBee network. Therefore, wherever possible, over-the-air transactions between devices should also be secured with link keys, particularly for sensitive data. In addition, broadcasts should not be used for any sensitive traffic—only unicast data packets should be used.

After joining the network, a node should request the Trust Center to broker a unique link key between itself and the node with which it needs to communicate, as follows:

1. The node sends a request to the Trust Center to issue a unique link key for itself and its partner node.
2. On receiving the request, the Trust Center checks the requestor node's address against a list of devices that are allowed to request a link key.
3. On validating the node, the Trust Center randomly generates a unique link key and securely transports it (encrypted with the network key and pre-configured unique link key, if it exists) to the requestor and the partner.

ROLLING THE NETWORK KEY

Once a device has left a network, it is possible to obtain the network credentials from the device, including the network key and any link keys that it had for peers in the network. To prevent this from compromising the network, it is recommended that when a device leaves the network, the Trust Center rolls the network key to a new key, as follows:

1. The Trust Center broadcasts a new network key (with a new key sequence number) to all the nodes of the network.
2. The Trust Center then broadcasts a Switch Key command (with the new key sequence number) to all the nodes of the network.
3. Each device in the network switches to the new network key.

Any devices that do not receive the new network key will try to find the network again and will receive the new network key encrypted with the last negotiated Trust Center link key.

It is possible to prevent replay attacks on devices on the network by simply rolling the network key at regular intervals. However, this would be a huge overhead if done every time a device joins the network and it is more feasible to do it when network commissioning is opened and/or when the network is closed for any further joins. During normal network operation, rolling the key every fourth night would be a reasonable time-frame.

PREVENTING SPOOF LEAVE NOTIFICATIONS KEY

It is possible to repeatedly issue a spoof Leave request from a non-network device for a device in the network. This would result in the Trust Center and/or the parent of the victim device losing all network information for the device, including its keys. This renders the device stranded, outside the network.

This situation can be prevented by the Trust Center or parent not clearing network data for the device on receiving a Leave request that supposedly originates from the device, but only when a Leave request has been issued by the parent of the device. If a device does attempt a (genuine) self-leave then it is prudent for the removal of the network credentials to require manual interaction by an authorized person.

In order to avoid the unnecessary or accidental removal of a device from the network:

- The management leave server should be disabled, since the Management Leave command is only network key encrypted.
- Leaves should be disabled on routing devices so that a network layer Leave command is ignored, since this command is only network key encrypted.

To cause a device to leave the network, it is safest to allow this action only through Remove commands issued by the Trust Center, as this requires link key encryption.

KEY ESTABLISHMENT CLUSTER AND SECURITY CERTIFICATES

The ZigBee Smart Energy profile includes a Key Establishment cluster which provides the functionality to authenticate devices using very strong Elliptic Curve Cryptography (ECC) based security. This security scheme generates and employs unique link keys for communications between pairs of nodes. It does, however, require digital security certificates for the joining nodes and Trust Center, and is reliant on the availability of these certificates.

There are a number of certification authorities that can issue these certificates and this brings its own complications. Certificates issued by different authorities are likely to be different and a device may need to hold certificates and root keys from multiple certification authorities. This has huge memory implications for the devices, which have small memory footprints.

The only practical ways of managing the use of security certificates on devices with very limited memory are to either use only devices that have certificates issued from the same authority or rely on installing the certificates into the devices using a custom validation and certification method.

PERSISTING ESSENTIAL DATA WHEN USING CLOUD SERVICES

The storage of network parameters in a remote location or in the Cloud provides huge benefits in terms of security, memory management and remote access.

The weakness of this approach is that access to the network parameters is lost when the connection to the Cloud or remote location goes down. It is recommended that only non-essential data is stored away from the network nodes. Essential data should be persisted on the nodes themselves, so that they continue to operate through the loss of backhaul links or network issues. This essential data includes:

- Network key and link key
- PAN and channel information
- Authentication and commissioning data
- Factory-default settings

FREQUENCY AGILITY TO COMBAT INTERFERENCE

Since ZigBee is a wireless protocol, it is possible to create interference and loss of service in the radio channel of operation or across the whole frequency band. It is worthwhile implementing a network manager application on the network coordinator, where this application is responsible for periodically assessing the operating channel and traffic by means of various ZigBee messages, such as Management Network Update notifications. If interference is present in the operating channel, the network manager can initiate a channel scan to find a safe channel and move the network to this channel (frequency agility). If no suitable channel is found, the network manager node may declare a loss of service.

DEALING WITH LOSS OF SERVICE

If a network is jammed by radio interference, this can result in a loss of service which may apply to the whole network or individual nodes – an example of the latter case is an electronic door-lock which is swamped with interference to prevent it from locking.

The assumption of the network manager node (e.g. coordinator) should be that an individual node will not be able to signal an error and it is the responsibility of the network manager to make decisions about the states of individual nodes or the whole network. There should be regular pings between the nodes to confirm that the nodes and network are active. If there is a problem, the network manager may be able to raise audible or visible alarms.

If the network is connected to the outside world (e.g. via the Internet) then the node or gateway with the backhaul connection should make loss-of-service decisions and take appropriate actions, such as raising the alarm and reporting the situation via this connection.

CONCLUSION

The ZigBee protocol defines a highly secure operating environment but does not mandate the level of security that a product needs to provide. This is a choice for the product manufacturer, depending on how sensitive the handled data is, as well as how easily and securely the product should interoperate with products from other manufacturers.

If data security is important then care must be taken to avoid eavesdropping as well as rejoin and replay attacks, and it is absolutely critical to protect the network key that is used to secure all network communications. If backwards compatibility and ease-of-use are requirements then there is a possible vulnerability introduced by using well-known keys to securely distribute the network key. The use of install codes and Trust Center link keys is highly advisable to ensure that the network key is secured when passing it to joining nodes.

If the intention is to produce highly-secured network applications, as a minimum they should be designed to employ link key security and not just network key security. In addition, use of the Key Establishment cluster should be given due consideration, with its support of ECC-based key establishment, digital certificate management and choice of certification authority.

If Cloud services are used by low-power wireless network products, these devices will also be vulnerable if the connection to the Internet and Cloud is not properly secured. So the end-to-end security of the system should also be considered. The ZigBee network should also not be fully reliant on such backhaul connections, otherwise the loss of a connection could render the ZigBee network unusable. There should be some autonomy for network recovery and maintenance in the event of the loss of backhaul links.

The wireless medium can be contaminated with interference and it is possible to cause sufficient interference for two devices not to be able to communicate effectively. It may be possible to overcome such interferers by building frequency agility into the network and it is strongly recommended that this is considered for the final implementation of the system.

Outside the scope of the ZigBee protocol itself, the encryption of program memories and firmware as well as read/write protection on devices should be considered. Erasing the security credentials of any device that is no longer in use is also advisable.

The level of security that is realistically required depends on the nature of the product but manufacturers should not overlook security for the sake of cost. The security measures implemented in a product should form part of the product specifications and features list in the advertising, marketing, documentation and packaging.

Prepared by NXP Laboratories UK

Visit www.nxp.com/ZigBee for additional product information and design resources.

Date of release: January 2017
Document order number: MAXSECZBNETART REV 0