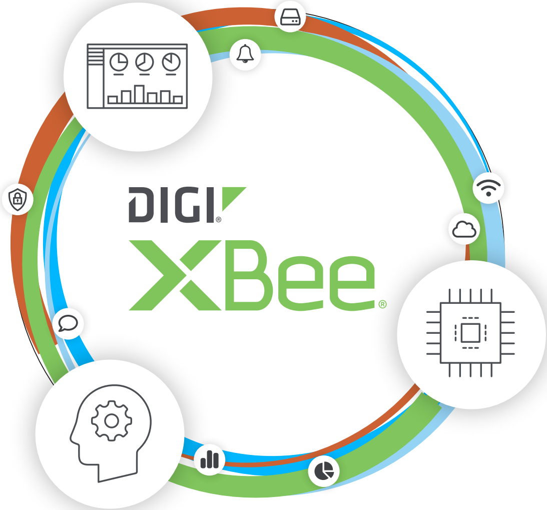
Digi XBee Device Security: A Guide to Securing XBee RF Devices

Security threats in IoT solutions are a growing concern as attacks become more sophisticated. Vulnerabilities can lead to confidentiality breaches, service theft, compromised data integrity, and reduced service availability. Implementing security measures in configuring and using your embedded devices enables you to secure your applications and protect your brand's reputation.

Digi is committed to supporting your organization's security requirements through customer education, proper documentation, and ongoing enhancements to security enablement in the design and manufacturing of our devices. But there is more to do, administratively, when configuring radio and cellular devices, and incorporating them into networks and product designs.

This technical brief provides the information you need to secure your devices, at a high level, and provides a list of resources for additional information. If you are seeking support for the security of your application, Digi offers **Professional Services**, **Wireless Design Services**, and **Technical Support plans** to meet your needs.

We will revise this technical brief over time as we continue to enhance **Digi XBee® RF** security measures and develop new products, and as industry best practices advance.



NOTE: The information in this technical brief will serve as a guideline, but in no way should be considered a guarantee that your devices are 100% secure. Device and network security require a proactive, ongoing, and multi-layered approach. For assistance, reach out to **Digi Wireless Design Services**.

For more information, visit:

www.digi.com

877-912-3444 | 952-912-3444

Introduction to Digi XBee Security

Security in Digi XBee modules is implemented differently depending on the product and protocol. Many of these capabilities are delivered as part of the **Digi TrustFence®** security framework, which provides a layered, device-level security architecture across supported Digi XBee products. XBee 802.15.4 and DigiMesh use AES-128/256 network encryption combined with Secure Sessions that use a salt/verifier pair for authentication, which you can enable through API commands to create encrypted, point-to-point sessions readable only by the two nodes involved. This gives DigiMesh strong, flexible protection at the link level. Zigbee uses a standardized, multi-layer security model with network keys, link keys, and a secure joining process that can tightly control when and how devices are allowed to join the network. Regardless of protocol, Digi RF modules ship with security disabled by default, so you must enable and configure the appropriate features for your application to ensure secure data transmission.

NOTE: Newer protocols such as LoRaWAN® and Wi-SUN® integrate more advanced security for data transmission. For this reason, this document does not cover security measures for **Digi XBee for LoRaWAN** and **Digi XBee for Wi-SUN**.

How to Think About IoT Device Security

There are several important principles to keep in mind with device security in a connected world.

1. **Shared responsibility.** The responsibility for securing IoT devices does not fall on any one individual's or entity's shoulders. It is shared by device manufacturers and those who purchase and configure the devices. A device manufacturer can establish security methods in the making of a device to enable device security, but cannot make the device secure. Securing devices requires configuration on the part of an administrative user.
2. **Multi-layer.** There is no one security method that can make a connected device 100% secure. Therefore, combining media layer security with adequate application security methods is critical.
3. **Ongoing effort.** Securing devices from the threat of hackers is not a one-time effort. As an example, setting up encryption on a network is an important security step, but that process must be repeated, as the longer any particular security method remains in place, the more likely it will be that hackers will eventually determine a way in. As another example, it is critical to generate secure passwords and to update them on a scheduled basis.

For more information on security layers and the importance of a multi-pronged approach, see our security blog posts:

- **Who Is Responsible for IoT Device Security?**
- **Risks, Challenges and Best Practices in Securing the IoT**

Implementing Security Measures for Digi XBee RF Modules

Digi XBee modules incorporate the **Digi TrustFence® IoT security framework**. This framework provides a collection of features that enable secure connections, including authenticated boot and secure physical ports. Digi XBee modules implement several key elements of the Digi TrustFence framework, including:

- **Secure Boot** — Ensures only signed software images can run on a device
- **Encrypted Storage** — Security keys are protected by an onboard security chip, and they are write-only
- **Protected Ports** — The programming interface is locked to prevent tampering
- **Secure Connections** — SSL/TLS v1.2 encryption for secure data transmissions (note that this does not apply to all modules)
- **Lifecycle Longevity** — Digi maintains a future-proof platform architecture (note that this does not apply to all modules)

Digi XBee 3 modules employ a protected boot capability and the secure element. The Digi XBee 3 binary program is encrypted to protect against tampering and reverse engineering.

As we've discussed, a multi-layer approach to security is a best practice, so that if any layer is compromised, you have another layer of protection.

Implementing Security Measures for Digi XBee RF Modules

If you are using the default settings on an XBee RF product, out of the box, the networks formed are unencrypted. Therefore, it is important to configure your XBee devices for security.

Digi's ISM band XBee modules include:

- **Sub GHz:**
  - Digi XBee SX modules running DigiMesh: Digi XBee SX 900 RF, Digi XBee SX 868
  - Digi XBee-PRO 900HP running DigiMesh
  - Digi XBee XR 900/868 running DigiMesh
  - Digi XBee-PRO XSC (not DigiMesh)
  - Digi XTend 900 MHz (not DigiMesh)
  - Digi XBee LPX 900 running DigiMesh
  - Digi XBee XR PRO running DigiMesh

NOTE: We have not listed Digi XBee LR or Digi XBee For Wi-SUN, as these modules are based on protocols that have integrated security and are not covered in this guide.

- **2.4 GHz:**
  - Digi XBee 3 modules: BLU, Zigbee 3, 802.15.4, DigiMesh 2.4
  - Digi XBee-PRO: Zigbee, DigiMesh
  - Digi XBee RR modules: Zigbee 3, 802.15.4, DigiMesh 2.4
  - Digi S2C modules: Zigbee, 802.15.4, DigiMesh 2.4

This section describes the encryption process for all Digi RF modules at a high level to help you understand how to encrypt RF data. We first cover security for non-Zigbee XBee modules, including the commands you can use to secure those modules, followed by security for Zigbee modules. As Zigbee security is a more complex process, we will describe the process overall. The stepwise procedures for encrypting Zigbee networks are provided in reference documents, which you can find in the Resources section.

Conceptual Overview

XBee modules can be configured for secure communication via encryption keys. When you enable security on a device and provide an encryption key, the information you transmit is encrypted before it is sent and must be decrypted on the receiving end to be readable. Note that this process will cause a slight increase in latency. RF packets are encrypted with either 128-bit or 256-bit AES encryption, depending on the particular XBee and protocol. As an example, XBee 802.15.4 supports 128-bit AES encryption. DigiMesh for XBee SX, XBee XR, XBee 3, and XBee RR support 256-bit encryption with an option for 128-bit encryption for backwards compatibility.

Digi XBee 3 modules use the Secure Boot feature of Digi TrustFence. In practice, this means the XBee 3 application is signed, and you therefore cannot run unauthorized code on an XBee 3 module. With prior models, it was technically possible to write a custom application and flash it (providing it referenced the correct hardware and correct region code). The XBee 3, XBee RR, and XBee XR designs require firmware images to be signed, preventing this vulnerability.

Managing Security Limitations on a Network

If you have an established network, there are limitations on the ability to secure all the network's devices. Regardless of the security you've applied, if someone hijacks one of the nodes, they can plug in a laptop and send AT commands to the network of connected devices. For example, a hacker could send a remote command to unencrypt the entire network.

To manage this vulnerability, Digi added the secure session feature. A secure session is established by using SRP (Secure Remote Password). The session exists between a local client and a remote server. In order to create a secure session, both the client and the server sides must have the password. The password itself is not sent over the air. Instead, the password is used to generate salt and verify parameters that are used to authenticate a session. By this means, a hijacker will be unable to access the network to change the configuration.

Secure remote sessions are available on Digi XBee 3, XBee RR for DigiMesh, 802.15.4, and Zigbee protocols. It is also available on XBee XR (DigiMesh).

Digi XBee SX has another method available to manage this vulnerability. The KZ command prevents anyone from sending remote AT commands if a password is set. If you set the KZ command, the results are as follows:

- The KZ command sets a password to prevent the transmission of remote AT commands
- The password is write-only, and you must know the current password to change it or disable it
- If the password is set, you cannot send or receive unsecured remote AT commands

For additional security, it is highly recommended that you set a unique password per device. That way if one node is compromised, the intruder can't get to the rest of the network.

For more information, visit:

www.digi.com

877-912-3444 | 952-912-3444

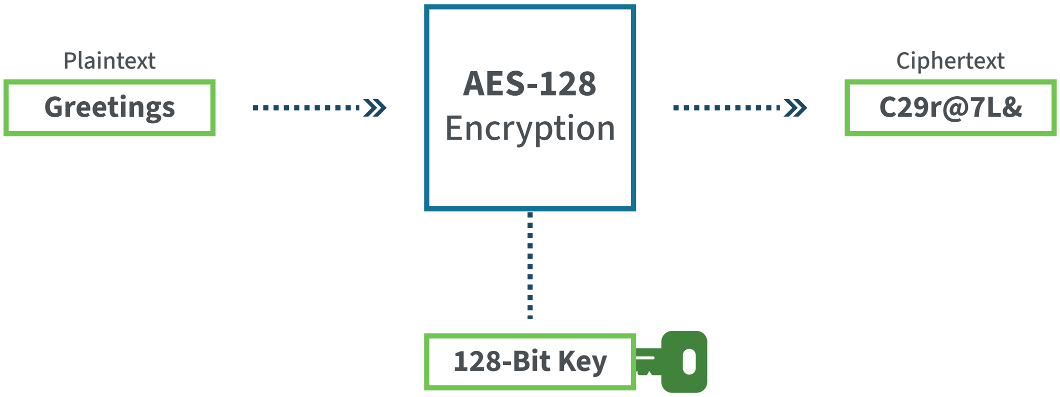
Enabling RF Encryption XBee RF Device Security for all XBee Devices Including 802.15.4 and DigiMesh

To enable secure communication, configure the following parameters with the same value in all devices in the network:

1. Set the AES Encryption Enable (EE) parameter to 1.
2. Set the AES Encryption Key (KY) parameter with up to 64 hexadecimal characters. Setting this parameter enables the encryption/decryption handshake. Once this parameter has been set, it is impossible to retrieve the actual value.

NOTE: You must use the same security settings on every device on the network. If you have a node that is unencrypted and one that is encrypted (or has mismatched keys) the data will get dropped because the devices cannot communicate.

How AES-128 Encryption Works



Enabling XBee RF Device Security for Zigbee Devices

Zigbee devices employ technology developed by the Zigbee Alliance, and employ very high levels of security. This means configuring security on these modules is more involved, but when done correctly it can provide stronger protections. This section provides a high-level overview of Zigbee device security. More in-depth information is available in the Zigbee documents listed in the Resources section.

Zigbee security protects network traffic using 128-bit AES cryptography techniques. A standard security model is defined for supporting authentication and key management. Security is a very important factor in designing a mesh network. Digi makes it easy to find the right level of security for your specific application, ranging from a completely open and unencrypted network to a high-security model with out-of-band device registration.

WARNING! The out-of-the-box default configuration is an unencrypted network with a generous join window. These defaults are meant for ease of development and should not be used on the finished product. Enabling security is highly recommended.

Enabling encryption also enables source routing with the coordinator acting as a high-RAM concentrator, by default. For smaller networks (less than 40 nodes) and low-throughput applications, this will not have a significant impact on the network, as source routing will automatically be handled by the XBee application. If you are deploying a larger network, you will likely require a full source routing implementation with the coordinator configured as a low-RAM concentrator. For more information on source routing and high/low RAM concentrator modes, see the **RF pack routing** section of the XBee/XBee-PRO S2C Zigbee RF Module User Guide.

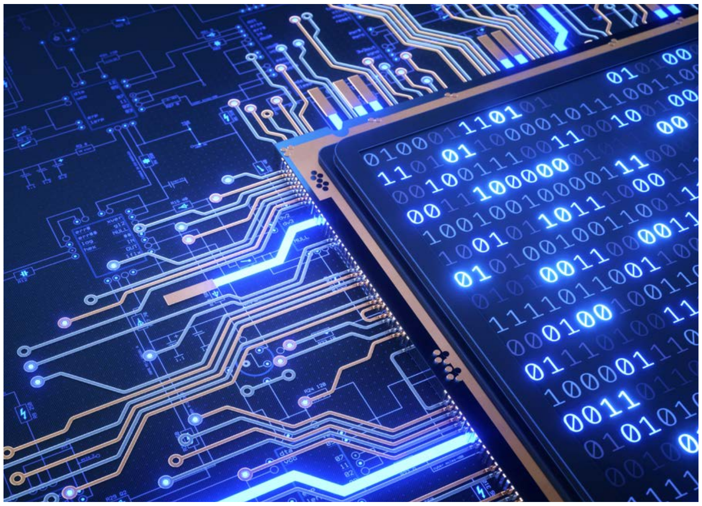
Distributed or Centralized Trust Center

Zigbee defines two security models for key management: A distributed trust center and a centralized security model (preferred).

Distributed Trust Center

A distributed security model is the simplest way to deploy a Zigbee network. Here are the fundamentals of this methodology:

- With a distributed security model, there are two device roles: Router and End Device; there is no coordinator on the network.
- Because there is no coordinator, it's more difficult to address data packets to a central aggregator, as a reserved 0 coordinator address cannot be used.
- Every router in a distributed security model has the authority to allow devices to join, assuming the joining device has a matching link key (KY parameter), and the join window is open (defined by the NJ command).
- A device that successfully joins the network securely obtains a copy of the network key. All routers share the same network key. The network key can be defined at the time the network is formed by setting the NK command on the device that initially forms the network; by default, the network key is randomly generated and cannot be read. In a distributed trust center, there is no way to change the network key after the fact without reforming the network.



Centralized Trust Center (Preferred)

A centralized trust center model uses a single device to act as the node that authorizes other devices to join and handle key exchanges with the joining devices.

- The trust center (TC) distributes network keys to joining devices if they have the proper credentials and the join window is open, allowing new devices to attempt to join.
- The network key is set on the trust center using the NK command and can be rolled after the network is established. This key feature reduces vulnerability, as a rotating key is much more secure and harder to hack than a static one.
- A variety of credentials can be used to join:
  - At the lowest level, you can use a well-known link key to authorize joining devices. By default, this method is disabled, as the key is publicly available.
  - You can use a preconfigured link key by assigning the same KY value on the trust center as well as the joining node.
  - You can use out-of-band commissioning to define a preconfigured link key for a particular joining node. In this way, unique keys can be set on joining nodes, and the key information is passed out-of-band (not using the Zigbee network) to the trust center using a registration API frame issued to the trust center through its serial interface.
  - Finally, you can assign a unique install code to every joining device and use it to create a link key. This installation code must be provided out-of-band to the trust center.
- The network join window must be opened (defined by the NJ command).

For more information, visit:

www.digi.com

877-912-3444 | 952-912-3444

Trust Center Considerations

There are pros and cons to the two methods of managing encryption. The considerations can be summarized as follows:

- If you have a distributed trust center:
  - The network key is shared amongst all the nodes, which can increase vulnerability.
  - The network key can never change. This means you do not have the option of doing a key rotation, which is best practice.
  - We only have a few options to limit the nodes joining the network. We can restrict the join window, but there are a few other options for limiting access.
- With a centralized trust center:
  - Only one node knows the network key, and that is the "trust center." That allows you to rotate your network key. If you want to regularly rotate the network key, you must use a centralized trust center.
  - By utilizing a centralized trust center, it also creates a single point of failure for the network. If the write-only network key is not known by your network administrator and the trust center needs

Zigbee Encryption Keys

Zigbee employs two keys — a network key and a link key.

The Network Key

The network key encrypts traffic hop-to-hop and is defined by the NK parameter on either the node that forms the network in a distributed trust center configuration, or the NK parameter on the centralized trust center. Every message on the network that is encrypted is encrypted with the network key.

By default, the network key is randomly generated and is typically not known by anyone. In managed networks, it's recommended to define the network key for ease of managing the secured network.

If using a user-defined network key, it is important to maintain the secrecy of this key. To ensure your system can sniff the Zigbee network traffic and decode the RF packets, you need to ensure the network key is known.

When using a distributed trust center, the network key can never change after the network is formed. In a centralized trust center configuration, you can rotate network keys by changing the NK parameter in the trust center. The new key will be distributed to the rest of the network devices.

The Link Key

The link key, which you manage using the KY command, encrypts data end-to-end. Link keys are used at the APS layer to add nodes to the network and send APS-encrypted transmissions. (See the Resources section for more information about Zigbee stack layers.) When joining a network with encryption enabled, the network key is securely exchanged by encrypting it with the link key.

In a centralized trust center, the link key that is used to join is exchanged with a more secure key that is randomly generated by the trust center.

Out-of-band Commissioning

The simplest method to join a secured network is to use a global link key assigned to every device on the network. This simple method can be used on both a centralized and distributed trust center model.

On a centralized trust center, a more secure means to securely allow nodes to join the network is to use out-of-band commissioning. By using a 0x24 device registration frame, you can provide the trust center with a link key and EUI64 (serial number). This will create an entry in the transient link key table. When a device with matching EUI64 attempts to join, the trust center will use the link key from the table to decrypt the join request. If successful, the necessary keys can be exchanged, and the device joins the network. The transient link key table has a timeout specified by the KT command on the trust center.

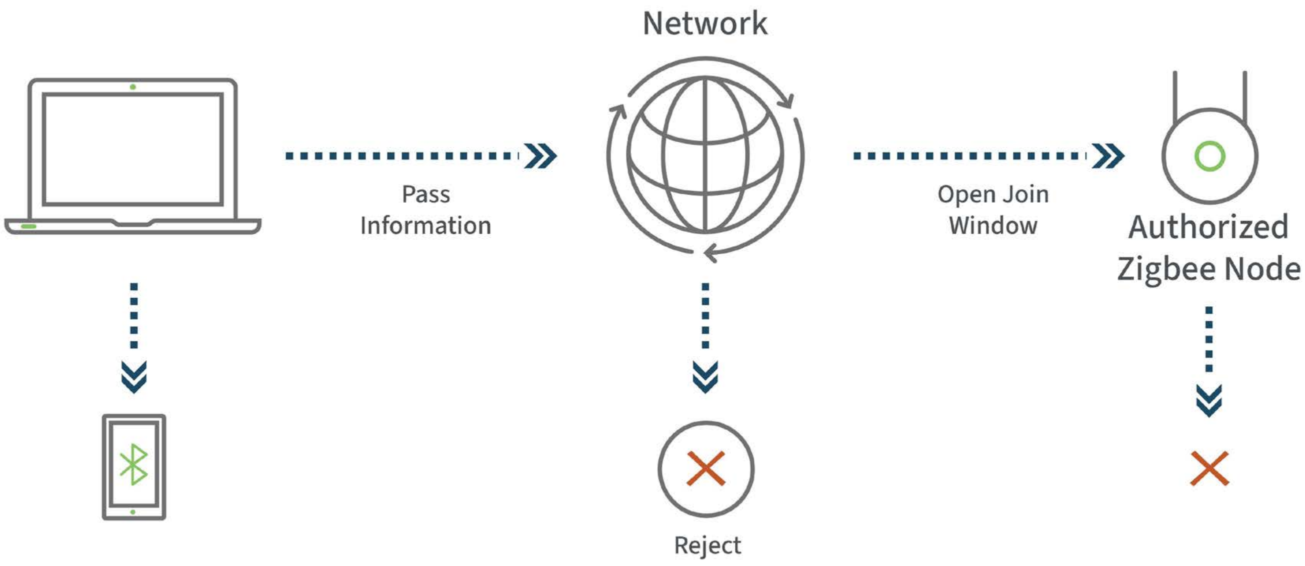
Another means of performing out-of-band commissioning is to use an install-code-derived link key for joining devices. An install code is a randomly assigned 16-byte code written to every XBee 3 radio at the factory and can be read with the I? command. The install code and joining device's EUI64 can be used to create a hashed link key in the transient link key table.

Additional Zigbee Security Methods

Another unique feature of Zigbee devices is the join window. As for Zigbee 3.0, the join window on XBee modules is closed out after 254 seconds and is configured using the NJ (network join) command. This means you form a network, and it allows joining for that period. (The joining period can be adjusted or turned off.) After the join window closes, no nodes can join the network. You can thus prevent devices from joining unless you intentionally open the join window. The join window is only opened when the physical commissioning button is pressed twice or the CB2 command is issued. The command for controlling the join window is NJ. See the security section of Digi's Zigbee documentation in the Resources section.

We also employ a device registration method in Zigbee modules, which is called out-of-band commissioning. This method is a means to allow one or more specific devices to join the network. You achieve this by authorizing specific devices with specific serial numbers to join the network. This process does not happen over the air. You must enable the commissioning process via the serial interface.

Secure Join Process with Out-of-Band Comissioning



Example

Here is an example of how the secure join process works with out-of-band commissioning. The installer establishes a network and needs to add an additional Zigbee node. Using a laptop (not connected to a wireless network) or a Bluetooth-connected phone, the installer passes in information about a node that will join. The installer opens the join window, and the authorized node can join the network because it is commissioned. If anyone else tries to join, the trust center will see that the information doesn't match and reject it.

While it does require an intensive effort on the part of the installer, the combination of out-of-band commissioning and the join window is an effective strategy for establishing highly secure networks.

For more information, visit:

www.digi.com

877-912-3444 | 952-912-3444

Managing Physical Security with Embedded Devices

Physical security is the most difficult problem to solve in many ways because anyone who has physical access to a device often has privileged capabilities. As a result, it is possible to exploit weak links in the security of the system. For example, you could potentially attach a logic analyzer and analyze the electrical signals of the process. If you have advanced tools, such as an X-ray machine or other laboratory tools, you could potentially examine devices.

One of the best ways to solve the problems associated with physical security is to restrict access to the device. For example, here are some methods of establishing physical security:

- You can use a physical lock and place the device in a sealed enclosure that prevents or discourages access.
- You can add tamper-proofing by erasing sensitive data such as private keys when a breach is detected. If a seal is broken, and the seal is what keeps the electrical charge going, the keys are erased.
- Or the device can erase itself. For instance, if you have highly sensitive information such as financial transaction data or patient data, you can program higher security into the end device application.

Another method is to make sure that your embedded device does not draw attention to itself, so that attackers would not be drawn to it. More conspicuous devices are typically more vulnerable to vandalism, theft, and other security risks.

Digi's **Professional Services** and **Wireless Design Services** teams can help. **Contact Digi** to learn about the services available to support your security requirements.

For more information, visit:

www.digi.com

877-912-3444 | 952-912-3444

Conclusion: Additional Thoughts on Device Security

IoT device security is more important as the sophistication of hacking methods increases. Employing security requires planning and ongoing strategy. It is all too common, even today, for organizations to believe they are protected by the measures put in place by their device manufacturer, or to take missteps in the application of security practices.

Here are some of the most important steps you can take in securing your devices:

- Make sure you are using the right security measures correctly, and for what they were designed to do.
- Follow all best practices, including the practice of employing multiple layers of security to thwart attackers at multiple points.
- Evaluate security measures to ensure they are providing the level of security you expect, and the level of security needed for your application. For example, using a password randomizer is an excellent approach. However, if the randomizer uses a predictable sequence, it is not actually random.
- Ensure that you are using a complete security solution, not just making a token effort. As an analogy, if you lock all your windows, your home still isn't secure if you haven't locked your door.

For more information, visit:

www.digi.com

877-912-3444 | 952-912-3444

Resources

Digi XBee 3 User Guides

Digi XBee 3 DigiMesh 2.4 RF Module User Guide

- See the **Encryption** and **Security commands** sections

Digi XBee 3 802.15.4 RF Module User Guide

- See the **Encryption** and **Security commands** sections

Digi XBee 3 Zigbee RF Module User Guide

- See the **Zigbee security** and **Configure security keys** sections

Digi XBee User Guides

Digi XBee/XBee-PRO SX RF Module User Guide

- See the **Security protections**, **Secure a network**, and **Security commands** sections

Digi XBee/XBee-PRO S2C 802.15.4 RF Module User Guide

- See the **Networking and security commands** section

Digi XBee Wi-Fi RF Module User Guide

Zigbee Guides

Security Analysis of Zigbee from MIT

Zigbee Security AN1233 from Silicon Labs is very helpful in understanding Zigbee security implemented on our XBee devices

Digi XBee/XBee-PRO S2C Zigbee RF Module User Guide

- **See the security section**

Digi XBee 3 Zigbee RF Module User Guide

- See the **security**, **key management** and **Zigbee stack layers** sections

For more information, visit:

www.digi.com

877-912-3444 | 952-912-3444