Streamlining ZigBee 3.0 Development

NXP Laboratories UK

Abstract

Low-power wireless networks are increasingly common-place in the home and the workplace as the infrastructures for 'smart' technologies relating to living and working environments. They have very stringent requirements in terms of power consumption, while security and ease-of-use are also becoming important factors for the consumer.

ZigBee® is the most well-established low-power wireless network protocol. It is built upon the IEEE802.15.4 standard to provide an easy and powerful framework for the development and operation of wireless network applications. The latest ZigBee 3.0 standard refines this protocol to facilitate the next generation of wireless networks.

NXP® has a long-term involvement in developing hardware and software platforms for ZigBee applications. Our JN516x and JN517x families of wireless microcontrollers have been designed with ZigBee in mind to provide hardware platforms optimized to form the heart of ZigBee network nodes. The JN5169 and JN5179 devices are available on ready-made modules that can be quickly and easily incorporated into prototype and final products to streamline the development of ZigBee nodes. These devices are supported by comprehensive hardware and software kits to enable rapid and simplified ZigBee application development. Example ZigBee applications are also available that can be employed as a basis for custom application development.

Table of Contents

Introduction

The advent of small, cheap, general-purpose microcontrollers has in recent years resulted in their widespread deployment in consumer and commercial products within the realm of ‘smart’ technologies, notably in the phenomenally successful smartphone. The next major conquest of the smart technologies is expected to be in the home and workplace through low-power wireless networks that will help to automate and enhance our living and working environments. The most high-profile example is the smart lighting system in which lamps can be automatically controlled from sensors or user-controlled and configured, possibly from an app on a smartphone. The potential application areas are extensive, with home heating and home security being notable areas for growth. The integration of these Wireless Personal Area Networks (WPANs) into the wider Internet allows remote access and control of the WPANs from IP-connected devices, giving rise to the ‘Internet of Things’ (IoT).

The wireless networks that form the basis of the smart home and smart building have strict requirements for low power consumption, since many of the nodes may need to be self-powered from batteries or energy harvesting (e.g. solar power). Low data-rates and infrequent transmissions are therefore necessities for these nodes, and non-routing nodes can also conserve energy through low-power sleep modes. The IEEE802.15.4 protocol standard was conceived to serve these low-power wireless networks based on a simple star network topology in which all communications are passed through a central ‘Co-ordinator’ node – therefore, communication between any other two ‘End Device’ nodes involves two hops via the Co-ordinator.

The most well-known low-power wireless networking protocol is ZigBee, which is built on top of the IEEE802.15.4 standard and therefore operates in unlicensed radio bands at 868, 915 and 2400 MHz (depending on territory). ZigBee supplements IEEE802.15.4 with high-level networking functionality, such as automated network formation and data packet routing, as well as a framework for user applications. The basic star topology of an IEEE802.15.4 network restricts the physical expanse of a wireless network, since all the network nodes must be within radio range of the Co-ordinator. This central routing node also represents a potential single point of failure. The ZigBee networking functionality allows the more elaborate tree and mesh network topologies, which may contain many ‘Router’ nodes that permit multi-hop communications between nodes and therefore achieve a large spatial coverage. The tree topology employs fixed routes between nodes, while the mesh topology allows any two Router nodes within radio range to communicate directly with each other, giving rise to alternative routes between nodes. A mesh network therefore has a highly resilient infrastructure, able to automatically circumnavigate points of failure.

ZigBee 3.0

The ZigBee 3.0 standard was recently introduced to better integrate ZigBee WPANs into the IoT and to reinforce the network-level security options for ZigBee nodes.

Traditionally, the ZigBee standard provides a number of market-specific ‘application profiles’, such as ZigBee Home Automation and ZigBee Light Link. A ZigBee WPAN adopts a particular profile and all the devices within the network come from the same profile. In the spirit of the IoT, in which devices/things of quite different functionalities are networked together, ZigBee 3.0 relaxes the market/profile requirement of a ZigBee WPAN. There are no application profiles in ZigBee 3.0 and devices from different market sectors can communicate with each other. In practice, the devices may not be able to communicate in a functional sense by exchanging useful data, but they are able to provide networking level services for each other, such as network joining and message routing - in other words, irrespective of their functional roles, the devices can participate in the same networking infrastructure.

The ZigBee standard has always included security measures to protect communications between nodes but has never insisted on their use for the purpose of ZigBee certification – the security choices for a product are left to the manufacturer. ZigBee network-level security is provided by a randomly generated encryption key called the 'network key', which is distributed to every node in the network and used by the nodes to encrypt/decrypt communications between them. The network key is itself encrypted when it is transported to new nodes, but the vulnerability of the network is dependent on how well the network key is protected. In ZigBee application profiles, such as Home Automation, the network key is distributed by a 'Trust Center', which is often the Co-ordinator, and it is normally encrypted with a pre-configured key that is known to both the Trust Center and joining node. If the pre-configured key is well-known (quite possibly the same for all nodes in the network) then there is a significant risk of the network key being exposed. ZigBee 3.0 provides enhanced protection for the network key by allowing the pre-configured key to be derived from an 'install code'. An individual install code is randomly generated for a node and programmed into the node during manufacture. The ZigBee protocol stack in the node derives an encryption key from this code. The install code is also communicated by unspecified means to the installer of the node, who enters it into the network Trust Center node, which derives the same encryption key from it. This key is then used to secure the network key when it is transported from the Trust Center to the joining node. Therefore, the network key is secured with a different pre-configured key for every joining node and this key is never exposed outside of the participating nodes.

For networks with less tight security requirements, ZigBee 3.0 introduces the option of 'distributed security'. In a distributed security network, there is no Co-ordinator and no centralised security management through a Trust Center. The network consists only of Routers and End Devices, and any Router can authenticate another device onto the network. Operational security is based on the network key and, when passed to a joining node, this key is encrypted with a pre-configured key. The same pre-configured key must be pre-programmed into all nodes of the network. One commissioning option in a distributed security network is to use Touchlink commissioning, which has its own pre-configured key.

ZigBee's Over-The-Air (OTA) Upgrade feature for software updates during device operation ensures that applications on devices already deployed in the field can be seamlessly migrated to ZigBee 3.0. OTA Upgrade is optional functionality that manufacturers are encouraged to support in their ZigBee products.

ZigBee 3.0 also continues support of ZigBee Green Power (GP). The Green Power specification provides a simplified protocol to minimize the power consumption of devices that are self-powered through energy harvesting. GP devices can only transmit and they employ a specific set of commands that allow short data packets and minimal transmission times. Since they do not need to receive, these devices can remain unpowered when not transmitting. They are usually devices that only become active through a user interaction (e.g. a light switch).

The integration of a ZigBee WPAN into the 'Internet of Things' requires an IoT Gateway. Data messages exist as over-the-air IEEE802.15.4 packets within the WPAN but as IP packets outside of the WPAN. The IoT Gateway is needed to transform the messages between the two packet types, in both directions. This unit includes a device called a ZigBee Control Bridge which handles the ZigBee side of the interface. The Control Bridge may also act as the ZigBee Co-ordinator and/or Trust Center for the WPAN. An IP-connected device, such as a tablet, may run an application providing a graphical user interface which interacts with the ZigBee Control Bridge to allow the monitoring and control of nodes in the WPAN.

NXP ZigBee Platforms

The NXP JN516x and JN517x families of wireless microcontrollers are broadly deployed in Smart Home and Smart Lighting systems around the world. They are extremely low-power, high-performance hardware platforms with integrated IEEE802.15.4-compliant 2.4GHz transceivers targeted at ZigBee WPANs and other IEEE802.15.4-based wireless networks.

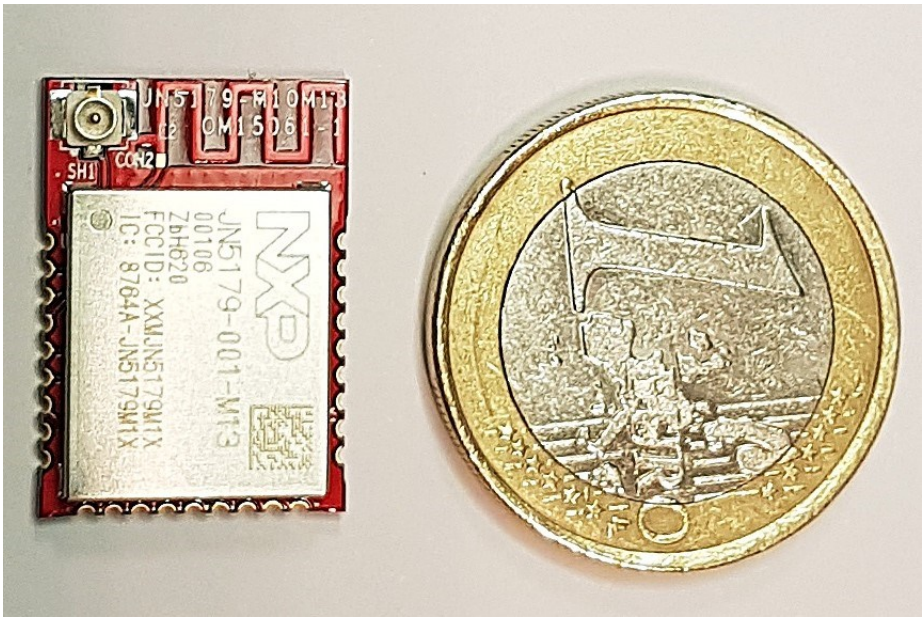
The low power consumption and sleep modes of these devices make them ideal for deployment in wireless nodes powered by batteries or energy harvesting – for example, the sleep mode current is as low as 0.6µA. The JN517x devices are among the best in their class in terms of low power consumption.

All the JN516x and JN517x devices have an AES 128-bit encryption engine built into the hardware for high-speed, secure communications. They also support encrypted external Flash memory that can be connected to the device's SPI bus. Security is an important feature of these devices and to prevent malicious access via JTAG, this interface can be locked down.

The devices provide a wide range of on-chip digital and analog peripherals that allow them to interface with the sensors and displays typically incorporated in the nodes of smart networks. Their embedded Flash memory ensures that they can be kept current by receiving over-the-air firmware upgrades while still performing their functional roles in the network.

The flagship chips from the two ranges are the JN5169 and JN5179 devices, which provide the most generous amounts of on-chip memory (512KB Flash, 32KB RAM and 4KB EEPROM). These chips are available pre-mounted on modules that incorporate integral and external antenna options, and can easily be deployed on proprietary mother-boards. The modules provide ready platforms for the rapid development of ZigBee 3.0 solutions, allowing fast product introduction with minimal investment in hardware. They are FCC/CE pre-certified for use in North America and the European Union, and therefore no RF design and testing are required.

JN5179 Module and a One Euro Coin



As a single supplier of microcontrollers and modules, NXP provides an easy path for the migration from modules for development to microcontrollers for high-volume production environments.

NXP ZigBee Support Software

NXP is a leader in the provision of ZigBee 3.0 certified solutions. The JN516x and JN517x wireless microcontrollers are supported by comprehensive software resources to simplify and aid the development of complete ZigBee 3.0 network solutions. A Software Developer's Kit (SDK) provides all the required ZigBee 3.0 software resources and acts as a framework for custom application development within Eclipse-based Integrated Development Environments (IDEs). As a starting point for custom application coding, application templates are also available for key devices from the ZigBee Lighting and Occupancy set, including a ZigBee Control Bridge for IoT access. All of these resources are available free-of-charge and can be deployed on the components of our JN516x-EK004 and JN517x-DK005 hardware kits.

The NXP ZigBee solutions have been thoroughly tested and are fully interoperable with other ZigBee solutions already deployed in the market. Our solutions have also been through Large Network Tests (LNTs) which have demonstrated the robustness of our ZigBee stack. Our LNTs are continually evolving to take into account customer requests.

For more information on the NXP ZigBee solutions, please visit www.nxp.com/zigbee.

Document Number: JN-WP-7005 REV 1