Secure commissioning for ZigBee home automation using NFC

Colin Faulkner - January 23, 2015

Wireless sensor networks such as ZigBee can provide many benefits when installed in buildings, including improved comfort, cost, and convenience.

The low power wireless network ensures that devices can be deployed quickly and easily without the need for many meters of extra cabling which is costly to install whether in new build or refurbishment. By deploying more sensors, thermostats for example, it is easier to regulate the temperature across the building on a room by room basis, leading to improved comfort. At the same time, cost can be reduced by managing the use of energy more efficiently. Improved convenience results by adding functional links between different types of devices, such as automatically switching on lights if a door is opened or unlocked.

All of these functions can be handled by a network such as ZigBee, but one of the issues of installation is the time taken to securely join all of these devices to the network and to establish the control relationships. This paper describes the implementation of a home temperature control system using ZigBee Home Automation. In particular, it describes techniques for secure installation and commissioning of devices using low cost NFC tags that are connected to the ZigBee wireless microcontroller, enabling exchange of information about the network such as security keys and device bindings.

Introduction

Home automation is a hot topic right now, with numerous standards being proposed to provide connectivity to devices within the home. The standards proposed generally fall into two camps; the connectivity standard used to provide a data link in the home to individual devices, and the application layer standard that dictates which commands have what effect. With these two capabilities in place, it becomes possible to monitor and control many of the functions within a home or building. Examples of functions that may be controlled include lighting, heating/cooling, and security. Interesting usage models arise by combining these in various ways, for example arming the security system at the same time as putting the lighting into night mode.

At the current time, several new developments are available which ensure that meaningful automation of the home is on the cusp of dramatic market growth. The ZigBee wireless technology needed in the home is available as a globally acceptable standard and at low cost, ensuring that devices can be installed with no disruption to the home and that connectivity can be added cost effectively to almost any type of device.

As home automation can be a complex system to manage, the almost universal availability of an
intuitive graphical interface in the form of the smartphone or tablet provides a ready-made way to interact with all the devices in the home. This is in addition to the more simple functionality available from switches or sensors which will still be required for basic on/off/dimming control, or for sensing.

The technology required to implement secure connectivity and control from outside the home is also available in the form of various cloud services products, connected through the home broadband facility. These enable control and monitoring to happen away from the home, and also facilitate interactions between a smartphone and the home, for example switching on heating at a preset time before you arrive home, based on your location and traffic information. ZigBee Home Automation is a key element of these systems by providing standardised, secure connectivity and application functionality within the home.

Figure 1 shows the potential for connecting devices to the internet in the residential market.

**ZigBee Home Automation**

The ZigBee Home Automation profile is constructed using the ZigBee PRO mesh networking stack. This ensures that dozens or hundreds of devices can connect together reliably using the ZigBee mesh networking stack that has been described extensively elsewhere. The Home Automation profile provides the functionality that allows everyday home devices to be connected and controlled or monitored. This functionality can be broken down into three basic areas; securely commissioning devices into the network, providing data connectivity between devices, and providing a common language for communication between different devices. In this paper, we focus on the issues involved in commissioning.

Security within the ZigBee network is handled by encrypting the data using the AES algorithm, seeded by a network security key. The network key itself is chosen randomly by the coordinator of the network and is therefore unique for every installation, protecting against casual interception of data or malicious attempts to control the network. New devices joining the network are not aware of the key, so need a secure mechanism to acquire it.

There is a default commissioning key defined within the ZigBee specification which can be used to
encrypt the chosen network key as it is transferred to the joining device. This is very similar to the push button commissioning method used to add WiFi devices to a router in that the key could in principle be detected by a determined listener monitoring the network at the exact time of commissioning. However, for most domestic applications, this is a perfectly acceptable balance between risk and ease of use. Once the device has received the network key, it can fully participate in the network and can be bound to other devices to set up control relationships as required by the user.

Figure 2 shows some examples of control relationships that could be set up in a home automation system.

To avoid the potential for the security of the network becoming compromised, a fully protected method is required to transfer security information between devices and the network. This could take one of several forms. A bar code or QR code could be printed on the packaging or the product, containing a unique commissioning key which could be transferred to the coordinator via a mobile phone or similar tool. The packaging would typically get lost or confused with other devices of the same type and there is often insufficient room on the device to print a readable code. Alternatively, the device could be supplied with the key printed out, but this would require the user to enter a long string of numbers which is not user friendly and is also prone to error. What is needed is a robust and secure method of transferring information between a new device and the network itself, such as the use of NFC. **NFC commissioning**

**NFC commissioning**

The NFC wireless standard operates at 13.56MHz, with an on-air datarate of 106kbps. It provides a method to transfer data from a powered device (such as a mobile phone) to an unpowered, disconnected one (such as a light switch) at very short range, in the order of a few cm. The NFC signal power radiated from the powered device, is used to provide the miniscule amount of energy required to power up an NFC receiver and memory in the unpowered device, enabling information to be transferred into local memory on any kind of product. This is particularly useful for devices like light bulbs before they have been installed, or for energy harvesting light switches where there is no energy available for anything other than the transmission of a few packets of data. The very short range ensures full protection from third parties trying to access network keys and the operation to transfer data is as simple as putting a smartphone close to the device and starting an app to transfer data. There are a couple of options to use NFC for the transfer of security credentials.
The simplest option is to use a purely passive NFC tag that can be programmed with a unique commissioning key. During manufacture, the single chip ZigBee device would be given a unique key to be used for the exchange of commissioning information. This unique key would then be copied into the tag, together with the MAC address during the manufacturing process and the tag would be attached to the end product, or embedded within it. In its simplest form, the tag could comprise a simple self adhesive label which includes the NFC chip and the coil antenna required. Alternatively, the chip and antenna could be incorporated into the structure of the device itself. The end user would read the unique key in the tag using the built in NFC reader in their mobile phone. The phone is connected by WiFi to the gateway of the ZigBee network, so the key can be transferred securely.

This unique key is then used by the ZigBee coordinator to encrypt the network key which can be sent to the MAC address of the new device. Once the new device is aware of the network key, it can commence secure membership of the ZigBee network. This method gives us a secure technique for joining devices to the network, but is limited in functionality and still requires significant interaction to set up the ZigBee device, join it to groups and scenes etc. It also raises production difficulties as each tag needs to be matched to the specific ZigBee device address for best security.

The full value of NFC can be realised when the tag is electrically connected to the ZigBee device. Effectively, the tag then behaves as a dual port memory. One port is connected to the NFC interface and the other to an I2C port. In this case, data can be transferred from the phone into the tag memory. The I2C port can then be used to transfer that information into the wireless microcontroller that manages the ZigBee network. It is also possible to use the NFC tag to supply a small amount of power (up to 5mA) if it is desired to power up the microcontroller during the data transfer. A typical connected tag, such as the NXP NTAG devices shown in Figure 3 can store 1 or 2 kbyte of data.

![Figure 3](image.png)

Figure 3 shows a connected tag architecture.

This capability opens up many possibilities for the commissioning of devices into a ZigBee network. Firstly, it provides a simple method to securely add network keys to devices by using an NFC equipped smartphone. The phone can acquire the necessary key either over its own secured WiFi connection to a system gateway, or it can be transferred using NFC by touching the phone onto the gateway or remote control device. When the phone is placed close to the device being commissioned, the key can be transferred.

Because a significant amount of data can be transferred, the system can be made much more powerful. Running an application on the phone can allow the user to see all of the devices that have been commissioned. This enables the control relationships to be set up on the phone and programmed into the device at the same time as the network key is installed. Likewise, a text name can be added to the device to allow it to be easily identified, and perhaps associated with a
photograph of its location. All of these approaches become possible with the connected NFC tag, and doubtless many new techniques will be adopted using the capabilities offered by the technology.

**Home control system**

To demonstrate the operation of NFC commissioning within the context of a ZigBee network, a home control demonstration system was designed and built (Figure 4). This is based around a smart thermostat that can monitor temperature and humidity and is connected using the ZigBee Home Automation profile running on the JN5168 wireless microcontroller and NFC implemented on the NTAG connected tag. A smartphone application was written to enable the commissioning and assignation of control relationships. Individual rooms are represented by separate Perspex boxes, each fitted with a heater element and thermostat, connected with ZigBee Home Automation. Separately, lamps and smart plugs can be added to the system.

*Figure 4 is a home climate control demo.*

In this example, the network coordinator is a gateway device running the OpenWRT Linux operating system. The gateway is also equipped with a NFC reader device. This enables the phone to be “touched” to the gateway to receive a security key unique to the gateway. The phone is then “touched” to the device. The phone receives a unique commissioning key from the device. This can then be transferred back to the gateway encrypted with the unique gateway key.

The gateway can then send the network parameters to the device encrypted by the device’s unique
key which is unknown to anyone else. In this way, the network security credentials are never sent unencrypted by any mechanism. Once the device has the network parameters, it can securely join the network. The same procedure can be used for all the other devices in the system such as lamps, smart plugs, switches etc. This is explained graphically in Figure 5.

Figure 5 demonstrates the network key exchange process.

Summary

As the demand for home automation functionality grows, the need for secure systems becomes more important. ZigBee Home Automation is a powerful and robust open standard that can fulfil the connectivity and application requirements for automation in the home. However, the standard methods of security of joining and key exchange can be enhanced by the use of out of band techniques to transfer network credentials. Using an NFC tag connected to the ZigBee device enables secure information to be transferred without any possibility of detection by malicious listeners to the network traffic. This has been demonstrated by the development of a home climate control system using ZigBee Home Automation and NFC-based commissioning.

Also see:

- The future of home automation - ZigBee or Z-Wave?
- ZigBee 3.0 radio chips and modules can add Smart Home/IoT capabilities to lighting applications
- GreenPeak CEO discusses Smart Home at CES 2015
- NFC tags enable simple Wi-Fi and Bluetooth pairing
- Tips for home automation IoT design