ISSN:2320-0790

An International Journal of Advanced Computer Technology

Development of Zigbee Based Energy Management System

Srinidhi G A[1], Dr K B ShivaKumar[2], Sagar K N[3], Dr K A Krishnamurthy[4]

[1,2] Department of TCE, Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India.
[3]Ecolibrium Energy, Ahmedabad, Gujarat, India.
[4]Principal, Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India

Abstract: The ZigBee pro was developed to provide low-power, wireless connectivity for a Wide range of network applications concerned with monitoring and control. ZigBee is a worldwide open standard controlled by the ZigBee Alliance. ZigBee PRO is an Enhancement of the original ZigBee protocol, providing a number of extra features that are particularly useful for very large networks (that may include hundreds or even thousands of nodes).
The ZigBee standard builds on the established IEEE 802.15.4 standard for packet based wireless transport. ZigBee enhances the functionality of IEEE 802.15.4 by providing flexible, extendable network topologies with integrated set-up and routing intelligence to facilitate easy installation and high resilience to failure [1]. ZigBee networks also incorporate listen-before-talk and rigorous security measures that enable them to co-exist with other wireless technologies (such as Bluetooth and Wi-Fi) in the same operating environment.
ZigBee's wireless connectivity means that it can be installed easily and cheaply, and its built-in intelligence and flexibility allow networks to be easily adapted to changing needs by adding, removing or moving network nodes. The protocol is designed such that nodes can appear in and disappear from the network, allowing some devices to be put into a power-saving mode when not active. This means that many devices in a ZigBee network can be battery-powered, making them self-contained and, again, reducing installation costs.

Keywords: Zigbee, Zigbee Pro, Wireless nodes.

I. INTRODUCTION

The JN5148-001-Myy family is a range of ultra low power, high performance surface mount modules targeted at JenNet and ZigBee PRO networking applications, enabling users to realise products with minimum time to market and at the lowest cost. They remove the need for expensive and lengthy development of custom RF board designs and test suites. The modules use Jennic's JN5148 wireless microcontroller to provide a comprehensive solution with large memory, high CPU and radio performance and all RF components included. All that is required to develop and manufacture wireless control or sensing products is to connect a power supply and peripherals such as switches, actuators and sensors, considerably simplifying product development.
Three module variants are available: JN5148-001-M00 with an integrated antenna, JN5148-001-M03[2] with an antenna connector and the JN5148-001-M04 with an antenna connector, power amplifier and LNA for extended range. The modules can implement networking stacks such as JenNet and ZigBee PRO, as well as customer applications.
ZigBee Network Nodes:
A wireless network comprises a set of nodes that can communicate with each other by means of radio transmissions, according to a set of routing rules (for passing Messages between nodes). A ZigBee wireless network includes three types of node:
Co-ordinator: This is the first node to be started and is responsible for forming the network by allowing other nodes to join the network through it. Once the Network is established, the Co-ordinator has a routing role (is able to relay Messages from one node to another) and is also able to send/receive data. Every network must have one and only one Co-ordinator.
Router: This is a node with a routing capability, and is also able to send or receive Data. It also allows other nodes to join the network through it, so plays a role in extending the network. A network may have many Routers.

End Device: This is a node which is only capable of sending and receiving Data (it has no routing capability). A network may have many End Devices.

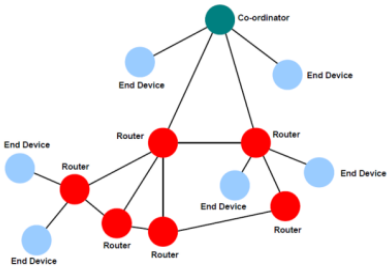

Figure1: Star Topology

II. ZIGBEE PRO NETWORK TOPOLOGY:

ZigBee facilitates a range of network topologies from the simplest Star topology, through the highly structured Tree topology to the flexible Mesh topology. ZigBee PRO is designed primarily for Mesh networks.

A Mesh network has little implicit structure. It is a collection of nodes comprising a Coordinator and a number of Routers and End Devices, where

- Each node, except the Co-ordinator, is associated with a Router or the Coordinator.
- An End Device can only communicate directly with its own parent.
- Each Router and the Co-ordinator can communicate directly with any other Router or Co-ordinator within radio range.

III. HIGHLY RELIABLE OPERATION:

IEEE 802.15.4 employs a range of techniques to ensure reliable communications between network nodes - that is, to ensure communications reach their destinations uncorrupted. Corruption could result, for example, from radio interference or poor transmission or reception conditions.

Data Coding: At a first level, a coding mechanism is applied to radio transmissions. The coding method employed in the 2400-MHz band uses QPSK (Quadrature Phase-Shift Keying) modulation with conversion of 4-bit Data symbols to 32-bit chip sequences. Due to this coding, there is a high Probability that a message will get through to its destination intact, even if there Are conflicting transmissions (more than one device transmitting in the same Frequency channel at the same time).

Listen Before Send: The transmission scheme also avoids transmitting data when there is activity on its chosen channel - this is known as Carrier Sense, Multiple Access with Collision Avoidance (CSMA-CA). Put simply, this means that before beginning a transmission, a node will listen on the channel to check whether it is clear. If activity is detected on the channel, the node delays the transmission for a random amount of time and listens again - if the channel is now clear, the transmission can begin, otherwise the delay-and-listen cycle is repeated. *Acknowledgements:* Two systems of acknowledgements are available to ensure that messages reach their destinations.

End-to-End: When a message arrives at its final destination, the receiving device sends an acknowledgement to the source node to indicate that the message has been received. End-to-end acknowledgements are optional.

Next Hop: When a message is routed via intermediate nodes to reach its destination, the next routing node (next hop node) in the route sends an acknowledgement to the previous node to indicate that it has received the message. Next-hop acknowledgements are always implemented. In both cases, if the sending device does not receive an acknowledgement within a certain time interval, it resends the original message (it can resend the message several times until the message has been acknowledged)[3].

Frequency Agility: When a ZigBee network is initially set up, the 'best' channel in the relevant radio band is automatically chosen as the operating channel. This is normally the quietest channel detected in an energy scan across the band, but this may not always remain the quietest channel if other networks that operate in the same channel are introduced nearby. For this reason, ZigBee includes a frequency agility facility, which is a core feature of ZigBee PRO. If the operating channel becomes too noisy, this feature allows the whole network to be moved to a better channel in the radio band.

Route Repair: Networks that employ a Mesh topology have built-in intelligence to ensure that messages reach their destinations. If the default route to the destination node is down, due to a failed intermediate node or link, the network can 'discover' and implement alternative routes for message delivery. ZigBee PRO is designed for Mesh networks and therefore incorporates "route repair" as a core feature.

Co-existence: The ability of a device to operate in the same space and radio channel as devices in other wireless networks (which possibly use protocols other than ZigBee) without interfering with them.

Interoperability: The ability of a device to operate in the same ZigBee network as devices from other manufacturers - that is, to communicate and function with them

The above reliability measures allow a ZigBee network to operate even when there are other ZigBee networks nearby operating in the same frequency band. Therefore, adjacent ZigBee networks will not interfere with each other. In addition, ZigBee networks can also operate in the neighbourhood of networks based on other standards, such as Wi-Fi and Bluetooth, without any interference.

IV. SECURE OPERATING ENVIRONMENT:

Access Control Lists: An access control list allows only pre-defined 'friendly' nodes to join the network.

Key-based Encryption: A very high-security, 128-bit AES-based encryption system (built into the JN5148 device as a hardware function) is applied to network communications, preventing external agents from interpreting ZigBee network data. This encryption is key-based. Normally, the same 'network key' is used for all nodes in the network. However, it is possible to use an individual 'link key' between a given pair of network nodes, allowing communications (possibly containing sensitive data) between the two nodes to be private from other nodes in the same network. Keys can be pre-configured in nodes in the factory, commissioned during system installation or distributed around a working network from a central 'Trust Centre' node. A Trust Centre manages keys and security policies - for example, changing the network key on all network nodes, issuing link keys for node pairs and restricting the hours in which certain events or interactions can occur. Any node can be nominated as the Trust Centre, but it is by default the Co-ordinator.

Frame Counters: The use of frame counters prevents sending the same message twice, and freshness Checking rejects any such repeated messages, preventing message replay attacks on the network. An example of a replay attack would be someone recording the open command for a garage door opener, and then replaying it to gain unauthorised entry into the property.

V. NETWORK ADDRESSING:

In a ZigBee network, each node must have a unique identification. This is achieved by means of two addresses:

IEEE (MAC) address: This is a 64-bit address, allocated by the IEEE, which uniquely identifies the device, no two devices in the world can have the same IEEE address. It is often referred to as the MAC address and, in a ZigBee network, is sometimes called the extended address [4].

Network address: This 16-bit address identifies the node in the network and is local to that network (thus, two nodes in separate networks may have the same network address). It is sometimes called the short address. In ZigBee PRO, the network address of a node is dynamically assigned as a random 16-bit value by the parent when the node first joins the network. Due to the randomness of the address allocation, this is known as stochastic addressing. Although random, the parent ensures that the chosen address has not already been assigned to one of its neighbours. In the unlikely event of the address already existing in the network beyond the immediate neighbourhood, a mechanism exists to automatically detect and resolve the conflict. The allocated network address can be retained by the joining node, even if it later loses its parent and acquires a new parent. The Co-ordinator always has the network address 0x0000. While an application on a node may use IEEE/MAC addresses or network addresses to identify remote nodes, the ZigBee PRO stack always uses network addresses for this purpose.

Network Creation:

1. Starting a Network (Co-ordinator): The Co-ordinator is responsible for starting a network. It must be the first node to be started and, once powered on, goes through the following network initialisation steps

a)Set EPID and Co-ordinator address: The Co-ordinator first sets the Extended PAN ID (EPID) for the network and the device's own network address: Sets the EPID to the 64-bit value specified in the Co-ordinator's application (if this value is zero, the EPID will be set to the 64-bit IEEE/MAC address of the Co-ordinator device) Sets the 16-bit network address of the Co-ordinator to 0x0000.

Select radio channel: The Co-ordinator then selects the radio channel in which the network will operate, within the chosen RF band. The Co-ordinator performs an Energy Detection Scan in which it scans the RF band to find a quiet channel[5]. The channel with the least detected activity is chosen.

Set the PAN ID of the network: Once the radio channel has been selected, the Co-ordinator chooses a 16-bit PAN ID for the network. To do this, it listens in the channel for traffic from other networks and identifies the PAN IDs of these networks (if any). To avoid conflicts, the Co-ordinator assigns its own network a random PAN ID that is not in use by another network.

Receive join requests from other devices: The Co-ordinator is now ready to receive requests from other devices (Routers and End Devices) to wirelessly connect to the network through it.

2 Joining a Network (Routers and End Devices): Routers and End Devices can join an existing network already created by a Coordinator. The Co-ordinator and Routers have the capability to allow other nodes to join the network through them. The join process is as follows:

Search for network: The new node first scans the channels of the relevant RF band to find a network. Multiple networks may operate, even in the same channel, and the selection of a network is the responsibility of the application (for example, this decision could be based on a pre-defined Extended PAN ID).

Select parent: The node now selects a parent node within the chosen network by listening to network activity. The node may be able to 'hear' multiple Routers and the Coordinator from the network. Given a choice of parents, the node chooses the parent with the smallest depth in the network - that is, the parent closest to the Co-ordinator (which is at depth zero).

Request joining: The node sends a message to the desired parent, asking to join the network.

Receive response: The node now waits for a response from the potential parent, which determines whether the node is a permitted device and whether the parent is currently allowing devices to join. To determine whether the joining node is a permitted device, the parent consults the Trust Centre (if it is not the Trust Centre itseIf). If these criteria are satisfied, the parent will then allow the node to join the network as its child. In its acceptance response to its new child, the parent will include the 16-bit network address that it has randomly allocated to the child.If the potential parent is unable to accept the node as a child, a rejection response

will be sent to the node, which must then try another potential parent (or another network).

Learn network Ids: The new node learns the PAN ID and Extended PAN ID of the network, as well as the network address that it has been assigned. It will need the PAN ID for communications with the network and will need the Extended PAN ID if, at some point in the future, it needs to rejoin the network (it will also be able to reuse its network address if it later rejoins the network). A Router or Co-ordinator can be configured to have a time-period during which joins are allowed, controlled by its 'permit joining' status. The join period may be initiated by a user action, such as pressing a button. An infinite join period can also be set, so that child nodes can join the parent node at any time.

VI. DESCRIPTORS

An application may need to obtain information about the nodes of the network in which it runs, There are three mandatory descriptors and two optional descriptors stored in a node. The mandatory descriptors are the Node, Node Power and Simple descriptors, while the optional descriptors are called the Complex and User descriptors For each node, there is only one Node and Node Power descriptor, but there is a Simple descriptor for each endpoint. There may also be Complex and User descriptors in the device.

Node Descriptor: The Node descriptor contains information on the capabilities of the node, including: Type (End Device, Router or Co-ordinator), Frequency band in use (868 MHz, 902 MHz or 2400 MHz), IEEE 802.15.4 MAC capabilities - that is, whether: The device can be a PAN Co-ordinator, The node implements a Full-Function or Reduced-Function IEEE 802.15.4 device, The device is mains powered,The device is capable of using MAC security, The receiver stays on during idle periods, Manufacturer code.

Node Power Descriptor: The Node Power descriptor contains information on how the node is powered: Power mode - whether the device receiver is on all the time, or wakes up periodically as determined by the network or only when an application requires (e.g. button press). Available power sources indicates whether the mains supply, or rechargeable or disposable batteries can be used to power the device, Current power sources - indicates which power source (mains supply, or rechargeable or disposable batteries) is currently being used to power the device, Current power source level - indicates the level of charge of the current power source.

Simple Descriptor: The Simple descriptor for an application includes: The endpoint on which the application communicates, The Application Profile that it implements, The Application Profile device identifier and version, Whether there are corresponding Complex and User descriptors.

VII. MESSAGE ADDRESSING AND PROPAGATION:

If a message sent from one node to another needs to pass through one or more intermediate nodes to reach its final destination[6][7] (up to 30 such hops are allowed), the message carries two destination addresses: Address of the final destination, Address of the node which is the next hop ZigBee PRO is designed for Mesh networks in which the message propagation path (the route) depends on whether the target node is in radio range:

- If the target node is in range, only the "final destination" address is used.
- If the target node is not in range, the "next hop" address is that of the first node in the route to the final destination.

The next hop address is determined using information stored in a Routing table on the routing node (Router or Co-ordinator). An entry of this table contains information for a remote node, including the network addresses of the remote node and of the next routing node in the route to the remote node. Thus, when a message is received by a routing node, it looks for the destination address in its Routing table and extracts "next hop" address from this table to insert into the message. The message is then passed on and propagation continues in this way until the target node is reached.

Route Discovery: The ZigBee stack network layer supports a 'route discovery' facility which finds the best available route to the destination, when sending a message. A message is normally routed along an already discovered mesh route, if one exists, otherwise the routing node (Router or the Co-ordinator) involved in sending the message initiates a route discovery. Once complete, the message will be sent along the calculated route.

The mechanism for route discovery between two End Devices has the following steps:

- A route discovery broadcast is sent by the parent of the source End Device, and contains the destination End Device's network address.
- All routing nodes will eventually receive the broadcast, one of which is the parent of the destination End Device.
- The parent of the destination node sends back a reply addressed to the parent of the source node.
- As the reply travels back through the network, the hop count and a signal quality measure for each hop are recorded. Each routing node in the path can build a Routing table entry containing the best path to the destination End Device. The choice of best path is usually the one with the least number of hops, although if a hop on the most direct route has a poor signal quality (and hence a greater chance that retries will be needed), a route with more hops may be chosen.
- Eventually each routing node in the path will have a Routing table entry and the route from source to destination End Device is established. Note that the corresponding route from destination to source is not known - the route discovered is unidirectional. A source Router implements route discovery in a

similar way to the above except the Router broadcasts its own route discovery message (without needing its parent to do this). Similarly, the Co-ordinator broadcasts its own route discovery messages.

VIII. CONCLUSION:

The ZigBee standard builds on the established IEEE 802.15.4 standard for packet based wireless transport. ZigBee networks also incorporate listen-before-talk and rigorous security measures that enable them to co-exist with other wireless technologies (such as Bluetooth and Wi-Fi) in the same operating environment. ZigBee enhances the functionality of IEEE 802.15.4 by providing flexible, extendable network topologies with integrated set-up and routing intelligence to facilitate easy installation and high resilience to failure.

ZigBee's wireless connectivity can be installed easily and cheaply, and its built-in intelligence and flexibility allow networks to be easily adapted to changing needs by adding, removing or moving network nodes. The protocol is designed such that nodes can appear in and disappear from the network, allowing some devices to be put into a power-saving mode when not active. This means that many devices in a ZigBee network can be battery-powered, making them self-contained and reducing installation costs.

References:

[1] Yuan-Yao Shih, Wei-Ho Chung, Pi-Cheng Hsiu and Ai-Chun Pan, "A Mobility-Aware Node Deployment and Tree Construction Framework for ZigBee WirelessNetworks," IEEE Transactions of Vehicular Technology, Volume 62, Issue 6, pp. 2763-2779, (2013).

[2] Hirakata Y, Nakamura A, Ohno K and Itami M, "Navigation system using ZigBee wireless sensornetwork for parking," 12th International Conference on ITS Telecommunications (ITST), pp. 605-609,(2012).

[3] Bunyai D, Krammer L,and Kastner W, "Limiting constraints for ZigBee networks," 38th Annual Conference on IEEE Industrial Electronics Society , pp. 4840-4846,(2012).

[4]http://www.jennic.com/products/wireless_microcontrollers/.

[5] http://www.jennic.com/support/software/

[6] http://www.jennic.com/support/user_guides/jn-ug-3075_jenos_user_guide

[7] http://www.jennic.com/support/user_guides/jn-ug-3048_zigbee_pro_user_guide