Z-Wave Protocol

Wireless Systems and Networks
Alma Mater Studiorum - University of Bologna
Master's Degree in Computer Science (LM-18)
Academic Year 2016/2017

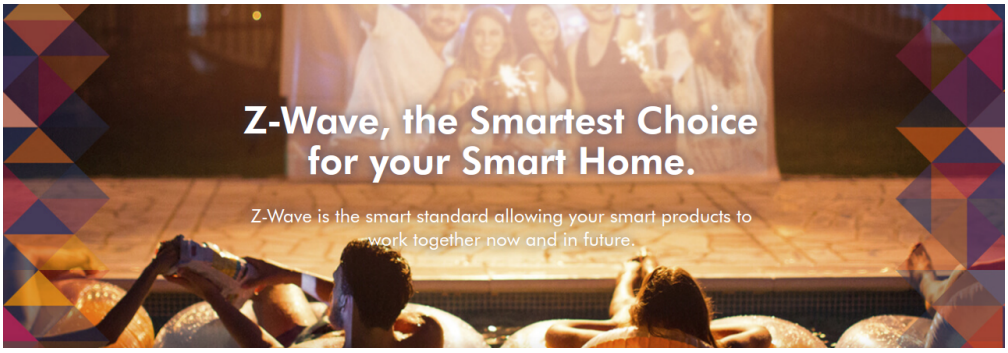
Stefano Traini
e-mail: stefano.traini5@studio.unibo.it
Student's ID: 778487

February 3, 2017

Contents

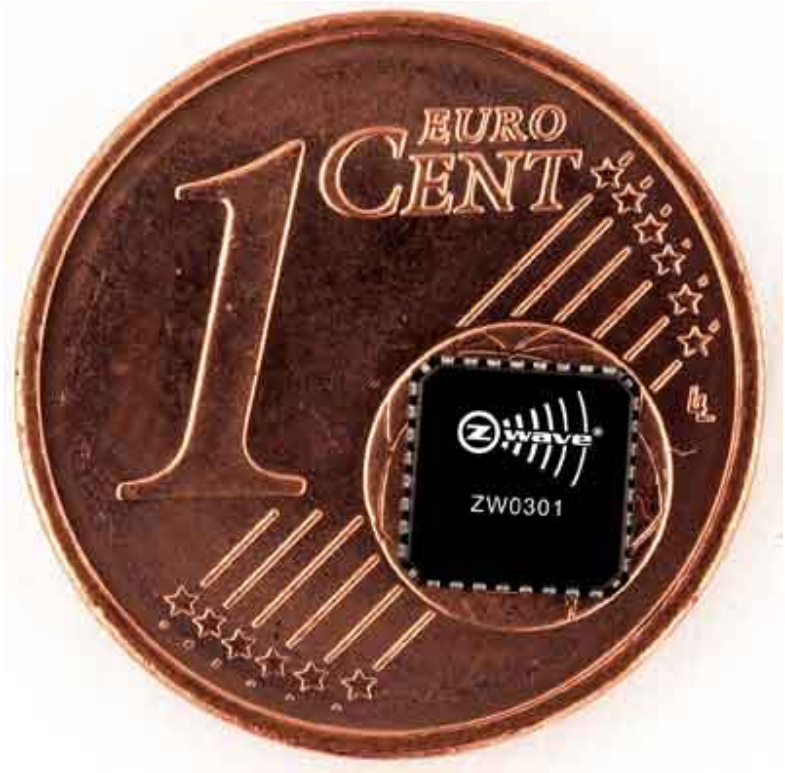
Chapter 1

Introduction: What is Z-Wave



Z-Wave is an international standard for wireless home automation (Wireless Home Area Network).
Home automation allows to interconnect all functions dealing with electricity such as light, heating, cooking, cooling, security etc with each other and to apply automation of these functions.

1.1 History of Z-Wave



Zensys a Danish-American company founded in 1999 invented the Z-wave technology.
They are basically providers of Integrated Single chip Solutions. While trying to embed intelligence and RF communication into their products they stumbled upon the idea to come up with a new technology combining the pros of the existing technologies.
To identify a good wireless technology for house automation a list of requirements must be considered. These are:

1. Reliability of the communication: all messages will reach its destination and will be confirmed by the received device back to the transmitter

2. Security of communication: It must be guaranteed that an unauthorized third party cannot, on purpose or accidently, intercept or interfere the communication of the wireless system

3. Low radio emission: Wireless technology for home automation is used on living rooms; hence issues like electromagnetic emission need to be taken into account

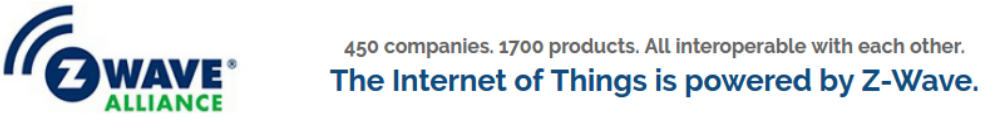
4. Simple usage: Home automation shall make the life of the user easier and not more complicated

5. Adeguate price

6. Protection of investment: It is important to make sure that the user can replace devices or extends their systems even after years and do not run into compatibility issues

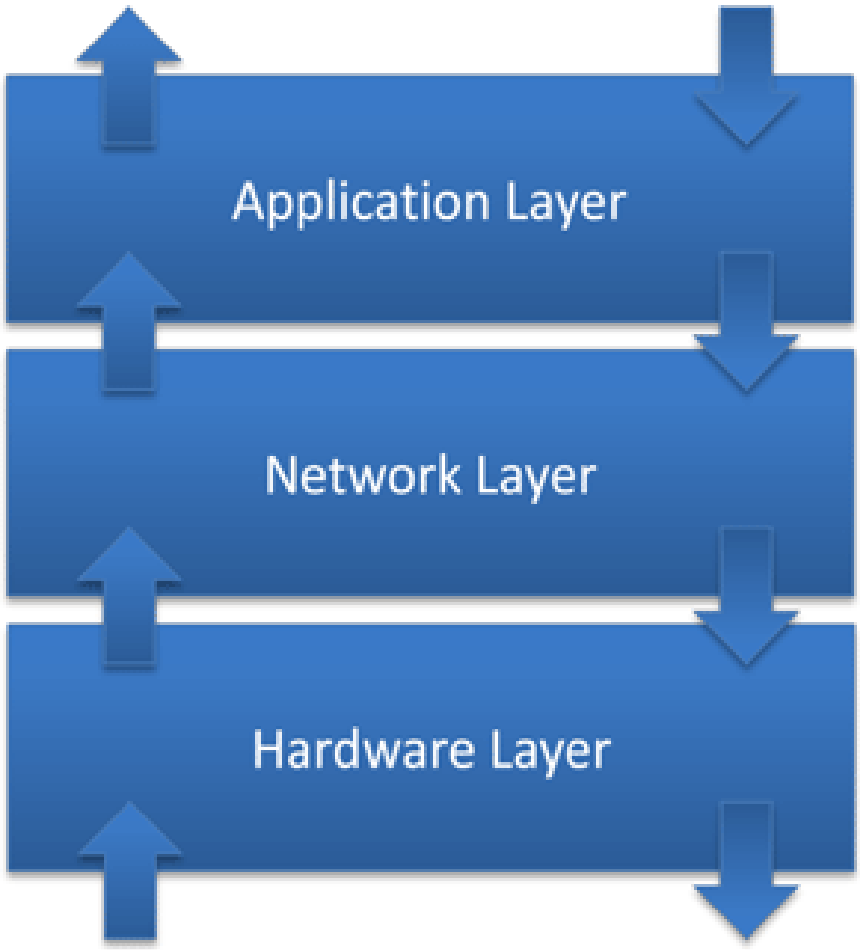
7. Interoperability: Each installed wireless technology has to be used independent from several manufacturers

1.1.1 Z-Wave Alliance



One landmark of the Z-Wave development was the foundation of the Z-Wave Alliance in 2005. In this industrial alliance the manufacturers of Z-Wave compatible products are gathered.
The Z-Wave alliance enhances the standard and takes care of central marketing events such trade shows and conferences.
The central duty of the Z-Wave alliance is the maintenance of the interoperability of the devices on the basis of the Z Wave protocol. This is guaranteed by a certification program, which results in a logo on the device guaranteeing the compliance to the Z-Wave protocol

1.2 Protocol Organization



The Z-Wave Protocol is dived in three main layers:

1. Radio Layer (or Hardware Layer): This layer defines the way a signal is exchanged between a transmitter and a receiver. This includes issues like frequency, encoding, hardware access, etc;

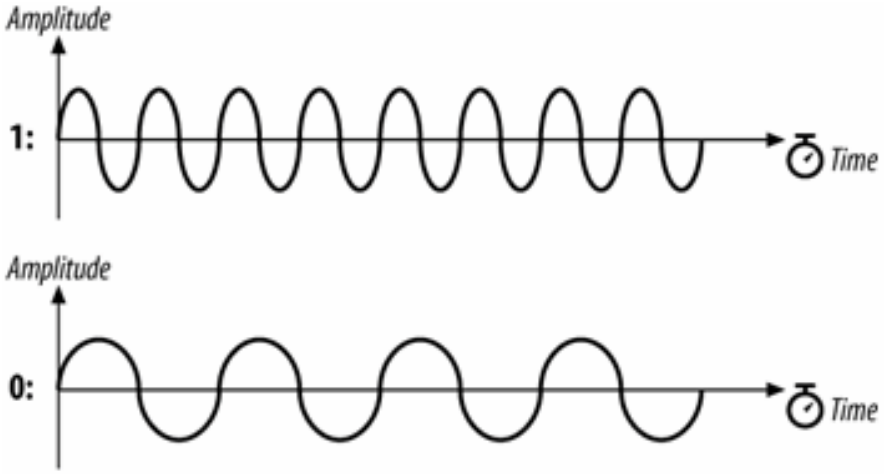
2. Network Layer: This layer defines how real control data are exchanged between two communication partners. This includes issues like addressing, network organization, routing, etc;

3. Application Layer: This layer defines which messages need to be exchanged to specific applications such as switching a light or increasing the temperature of a heating device.

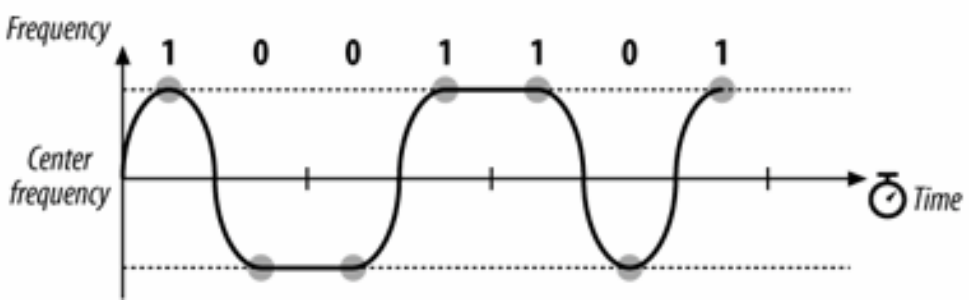
Chapter 2

Physical Layer

Z-Wave uses the ISM Band (Industrial-Scientific-Medical) in Europe. The frequency is 868.42 MHz that results in a wavelength of about 34cm. The new hardware family Z400 offers an additional radio, using the frequency of 2.4 GHz. Z-Wave uses a very robust frequency key modulation, the Gaussian Frequency Shift Keying (GFSK), which allows transmitting data with up to 40 KB/s. The most basic GFSK implementation is called 2-level GFSK, in this implementation two different frequencies are used, depending on whether the data that will be transmitted is a 1 or a 0.



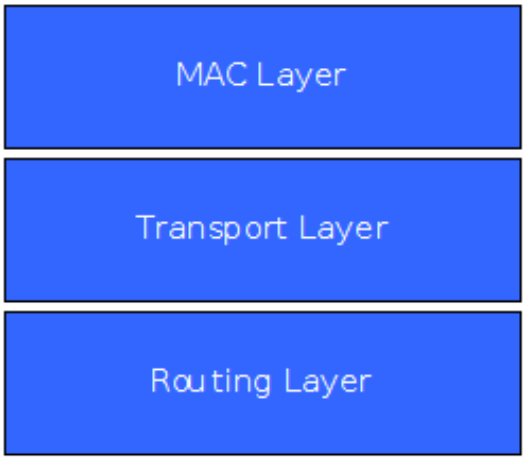
To transmit a 1 the carrier frequency is increased by a certain deviation and to transmit 0 is encoded by decreasing the frequency by the same deviation.



The two signals pass through a Gaussian filter that has the advantage of reducing sideband power and reducing interference with neighboring channels.

Chapter 3

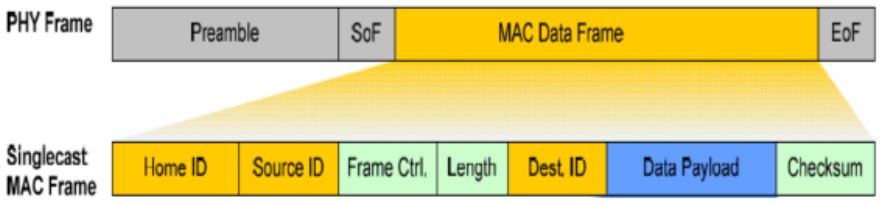
Network Layer



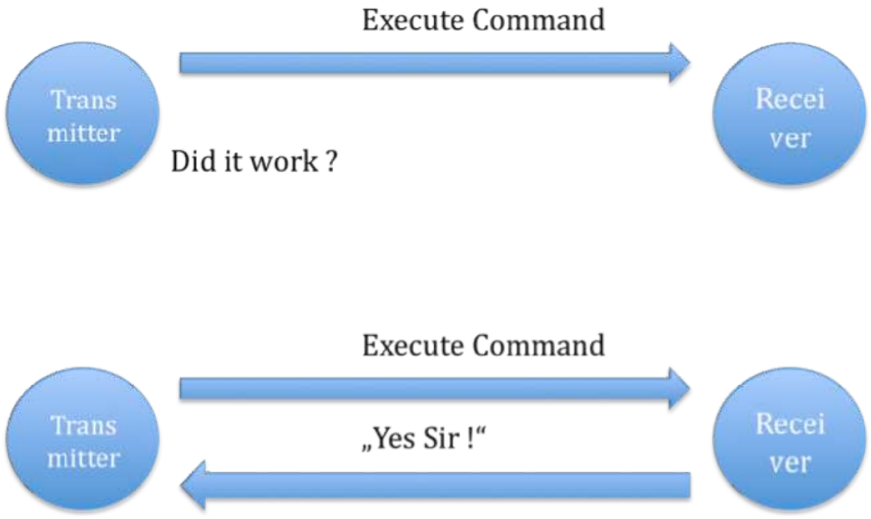
The Z-Wave network layer is divided into three sub layers:

- Media Access Layer: The MAC layer controls the usage of the wireless hardware;
- Transport Layer: This function makes sure that a message can be exchanged free of error between two wireless nodes;
- Routing Layer: This layer makes sure that a message is passed between the original sender and the desired receiver.

3.1 MAC and Transport Layers



The MAC layer controls the radio frequency medium which in turn is controlled by wireless hardware and it is independent of the RF medium. When the payload frame received to the node the MAC layer wants access to it or access to the full binary signal as a decoded bit stream.
The MAC layer of Z-Wave contains collision avoidance technique that allows the transmission of a frame when the channel is available and if there is no other nodes are transmitting.



The transport layer administers the connection between two sequential devices, including re-transition, checksum screening and the ACK.
After three unsuccessful attempts the Z-Wave transceiver will give up and report a failure message to the user.

3.2 The Z-Wave Network

A network consists of at least two nodes that communicate with each other. To be able to communicate with each other these nodes need to have access to a common media (Radio Frequency).
The communication protocol needs to define an identification that allows the different nodes of one network to identify each other and to exclude received messages from unknown or other radio sources.
The Z-Wave protocol defines two identifications for the organisation of the network:

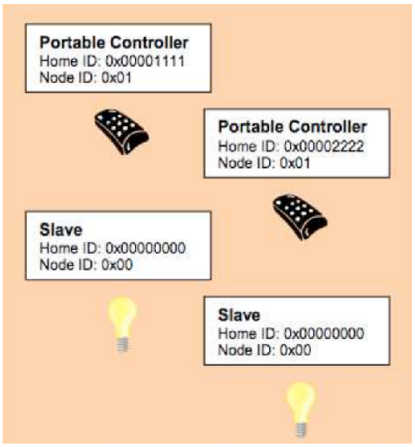
- Home ID: is the common identification of all nodes belonging to one logical Z-Wave network (length of 4 bytes = 32 bits);
- Node ID: is the address of the single node in the network (length of 1 byte = 8 bits).

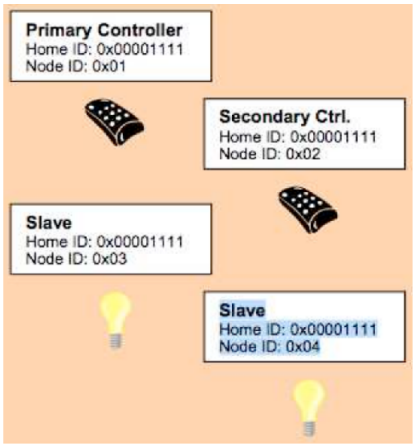
Z-Wave distinguishes two basic types from devices:

- Controllers: Z-Wave devices that can control other Z-Wave devices (already have their own individual Home ID at factory default)
- Slaves: Z-Wave devices that are controlled by other Z-Wave devices (do not have a Home ID)

3.2.1 Inclusion of the nodes

During the inclusion the controller who begins to build up a network transfers its Home ID to other devices becomes the designated primary controller of this network. In a bigger network several controllers can work together but there is always only one controller with the privilege to include other controllers. During the inclusion process the primary controller assigning not only the Home ID but also assigns an individual Node ID to the new device.



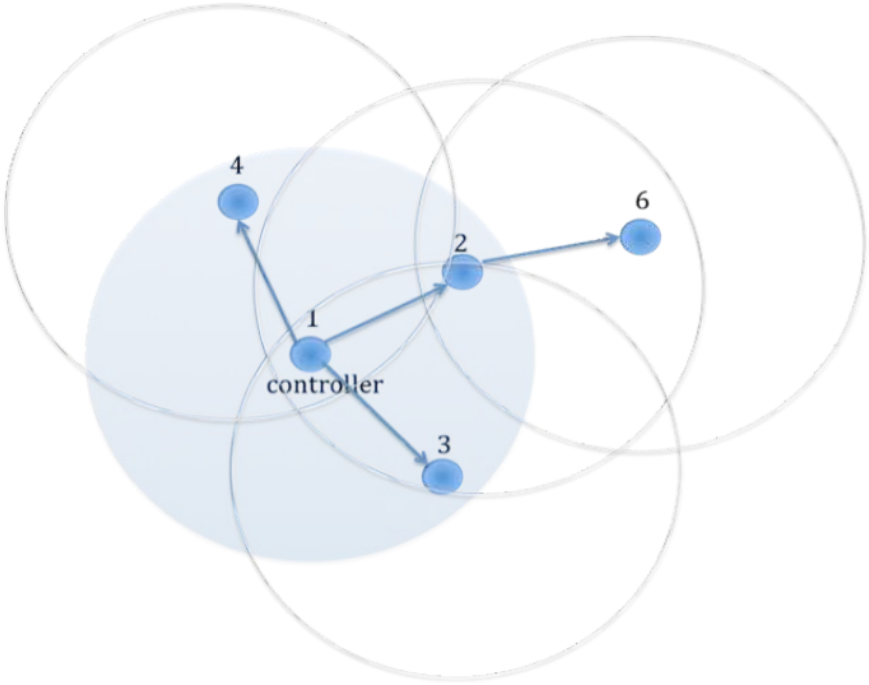


The 32 bit long Home ID allows to distinguish up to 4 billion different Z-Wave to networks with a maximum number of 256 different nodes. Because some addresses of the network are allocated for the internal communication and special functions, maximum 232 different nodes can communicate in a network.

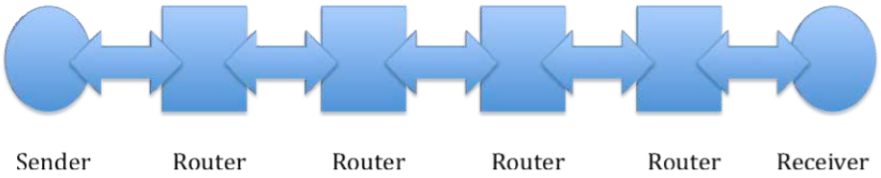
3.2.2 Exclusion of the nodes

If Z-Wave nodes are deleted from a network, this is called Exclusion in the Z-Wave terminology. During the Exclusion process the Home ID and the Node ID are deleted in the device. The device is moved back in the factory default state (controllers have their own Home ID and laves do not have any Home ID).

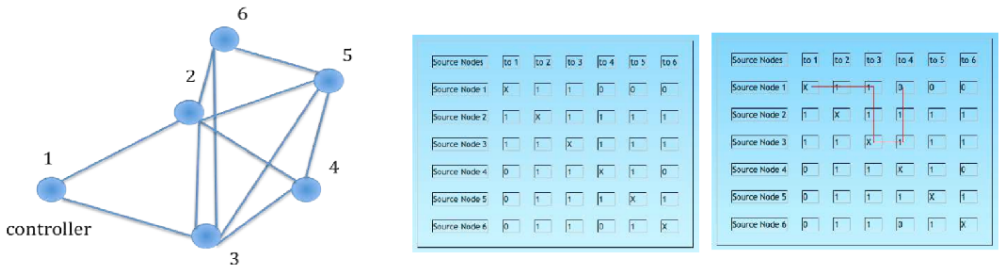
3.3 Routing Layer



Z-Wave nodes can forward and repeat messages that are not in direct range of the controller.



Z-Wave is able to route messages via up to four repeating nodes, this is a compromise between the network size, stability and the maximum time a message is allowed to travel in the network.



Every node is able to determine which nodes are in its direct wireless range (neighbours). During inclusion and later on request, the node is able to inform the controller about its list of neighbours.
The controller is able to build a table that has all information about possible communication routes in a network. The tools that allow to visualize the routing table are called Installer Tools.

3.3.1 The role of the devices

In the Z-Wave network devices can play two roles:

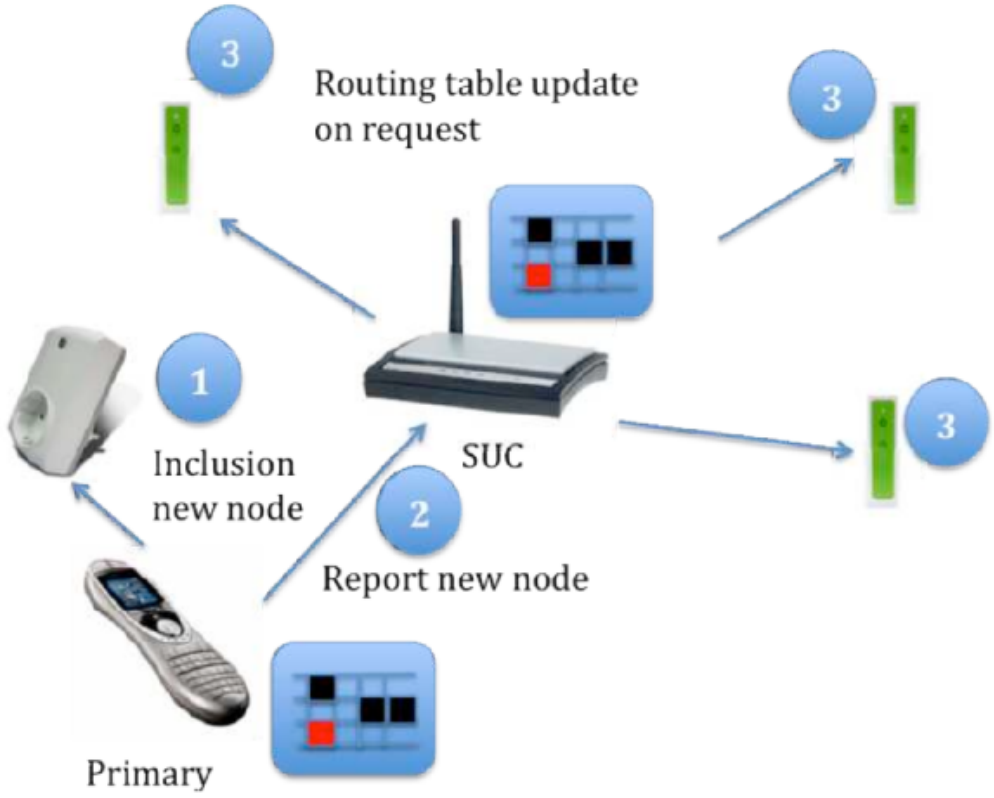
- Controller: Has access to the complite routing table and can communicate with every device in the network if a route exist;
- Slaves are categorized into standard slaves and routing slaves:
  - Standard Slave: Has no information about routing table, can only reply to the node that has received the message from and can not send unsolicited messages;
  - Has partial knowledge about routing table, can reply to the node that has received the message from and can send unsolicited messages to a number of predefined nodes.

3.4 Network configuration

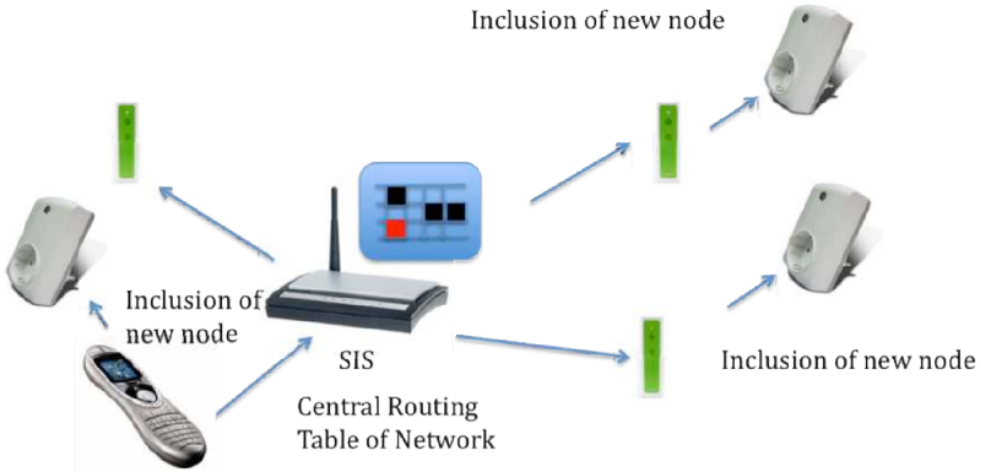
During the inclusion the controller requests an updated list of neighbouring nodes from these nodes and updates his routing table, in case a secondary controller

is included into the network primary controller hands over an actual snapshot of his routing table to the new controller. If more nodes are included later the routing table of the primary controller gets updated while the routing table of any secondary controller may still show the old status and needs to be updated manually (or by a user request).
If nodes are excluded from the network the corresponding entries in the routing table are deleted.
In both cases the routing table is not longer valid and communication to the moved or damaged node may fail. Any failed communication to a node results in an error message and the controller will mark this node as failed by putting him into a failed node list. To find a moved node in the network the controller can scan the whole network and ask every known node to update its neighbouring list. If the moved node is still in range of at least one node the controller is able to update its routing table and remove the moved node from the failed-node-list.
If no successful communication happens the node will stay in the failed node list and can be removed from the network by an user request.
Controllers are distinguished into static or portable controllers.
A static controller is supposed to be located on a fixed position in the network and shall not be moved and if a static controller is moved a network reorganisation or network scan is required.
A portable controller is supposed to be moved around and is therefore typically battery powered. A portable controller will always try to reach nodes in wireless range, if this fails the controller will try to generate a temporary routing table to find a routed way to the destination device.

3.4.1 Synchronization of the routing tables of the different controllers



To make sure that there is at least one updated and valid routing table only, the primary controller shall have the privilege to include/exclude devices. For a secondary controller it is always possible to request an update of his routing table. Static Update Controller (SUC) is a special function of a static controller, it receives the updated routing table from the primary controller and offers this routing table to all other controllers in the network. Any other controller can request an updated routing table from the SUC. If the original primary controller is lost or damaged, the SUC can assign the primary privilege to a new controller.



SUC ID Server (SID) is a special function of a SUC. Having an SIS pre sent in the network allows every controller in the network to include a further device. The controller will just request a new node ID from the SIS and assign this new Node ID to the server.

Chapter 4

Application Layer

The application layer of the Z-Wave product defines and specifies what and why two nodes communicate with each other.
All Z-Wave devices on the market can be categorized into one of the following function groups:

1. Electrical switches
2. Electrical dimmers
3. Motor control
4. Electrical display or other kind of signal emission
5. Sensors
6. Thermostat sensors controls
7. Thermostat radiator valves
8. Remote controls
9. USB sticks and IP gateways

The Z-Wave devices are devided in three different classes:

- Basic Device Class: The Basic device class makes a distinction merely whether the device is a controller, a Slave or a Routing-Slave;

- Generic Device Class: The generic device class defines the basic function as device is supposed to offer as a controller or slave (General Controller, Binary Switch, Binary Sensor, Multi-livel Sensor, etc.);
- Specific Device Class: Assigning a specific device class to a Z-Wave device allows it to specify the functionality of the device further. Assigning a specific device class is voluntary and only makes sense if the device really supports all specific functions of a specific device class.

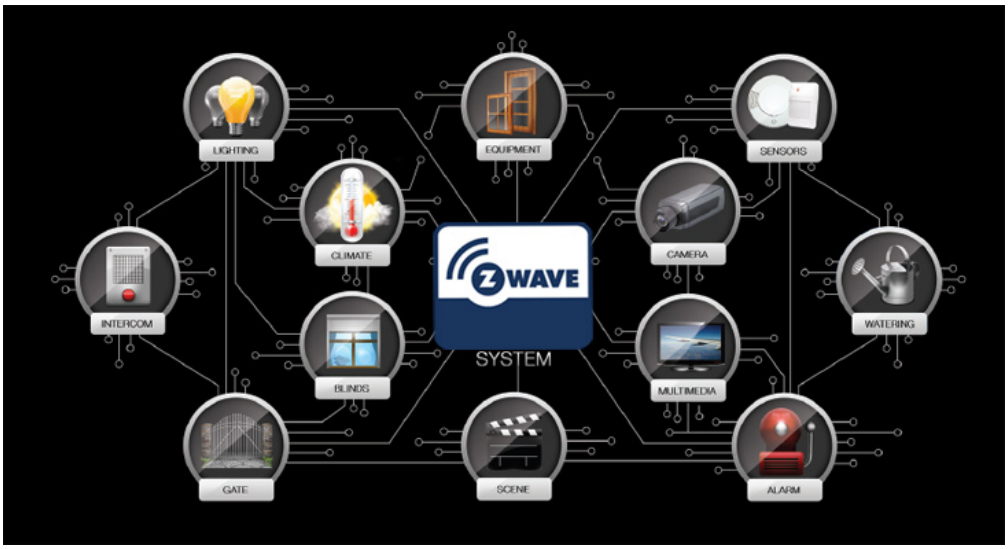
All communication within the Z-Wave network is organised in Command Classes.The basic commands are:

- SET: set a value between 0 and 255;
- GET: ask the device to report a value;
- REPORT: response to the Get command. Reports a value between 0 and 255.

In case the Z-Wave device is assigned to a specific or a generic device class it is required to support a set of command classes as functions of this specific device class (mandatory command classes):

- Mandatory commands: to enable compatibility to other manufacturers;
- Reccomended commands: to enhance compatibility to other manufacturers;
- Optional commands: to differentiare from other manufacturers.

4.1 Scenes and Events



With Z-Wave you can also create “Scenes” like “Leave for Work” and select what you want to happen in your home when you leave for the day, also you can create “Events” which react when something happens, for example when a motion detector is tripped a light can come on for 5 minutes. There is also a “Timer” setting where you can set the lights or the thermostat to go on or off at a certain time.

Bibliography

[1] Z-wave alliance official site". http://z-wavealliance.org/.

[2] Z-wave beginner guide. https://www.domotiga.nl/attachments/download/1075/Z-Wave%20Technical%20Basics-small.pdf.

[3] Z-wave official blog. http://blog.z-wave.com/.

[4] Z-wave official site". http://www.z-wave.com/.

[5] Muneer Bani Yassein, Wail Mardini, and Ashwaq Khalil. Smart homes automation using z-wave protocol. In *Engineering & MIS (ICEMIS), International Conference on*, pages 1–6. IEEE, 2016.