LUT
Lappeenranta
University of Technology

Cognitive Living

Home Automation Code Camp 2017

Villers Geral, Ganesan Madhubala, Kugblenu Carl, Iqbal Syed Asif

(PERCCOM Cohort-4)

Table of Contents

Introduction

With the ever-increasing use of electrical and electronic devices in households, we think a step ahead with automating certain activities at home or controlling devices at home remotely. There are several home automation products out there in the market which serve specific purposes such as for comfort or security or for cost saving. There is a need for an integrated system which serves all these purposes. User's needs change from time to time so there is a need for the system to adapt and alter it functions based on the need. Our motive is to provide a sustainable solution that strengthens the pillars of sustainability: Social – Comfort & Security; Environmental – CO2 emission; Economic – Cost saving.

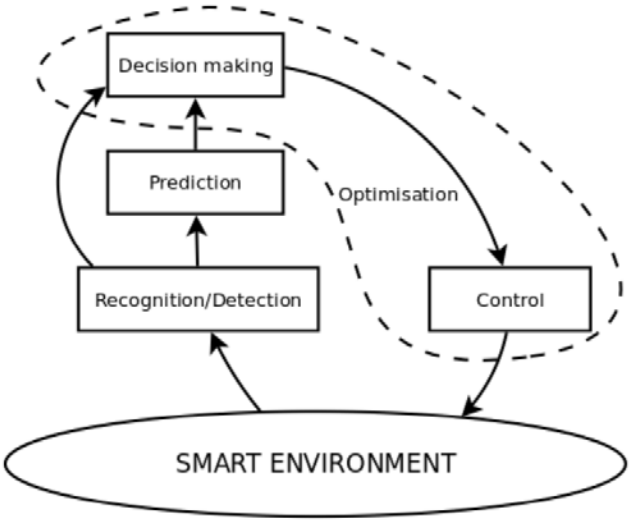
Goals of Our Project

- A comfortable environment – physiologically ambient environment for living
- Safe and Secure living
- Energy aware living & steps towards saving energy
- Cost saving by reducing power consumption
- A system that can automatically understand user's needs

Our Idea

We have implemented a system with DHS HomeManager, FHEM and HomeMatic devices which can provide comfort, security and save energy in a household. We have three operating modes namely: Normal Mode, Shield Mode and Child Mode. Normal Mode is when people are living in the house, so the focus of this mode is comfort. Shield Mode is when no one is at home, so we focus on energy saving & security. Child mode is where a child is left at home alone. So, the focus here is comfort, safety & security of the child. We control the Air Conditioner / Heating system based on room temperature and humidity values. With the help of Axis M115 camera we show the camera feed to the user at all times. We also detect motion in specific areas of the frame and alert the user in case of abnormal activities in front of the door or if there is an attempt to tamper the camera by email. The system alerts the user if doors and windows are open in Shield & Child mode for safety & security. In addition, the system should be able to predict and adapt itself based on user's behavior.

Self – Adapting System (Cognition)



The arrow starting from the environment depicts sensor readings and the arrow ending at the environment depicts the control of actuators. In the figure detection and recognition categories are presented in one box: these are two different approaches to *pre-processing* sensor data. The pre-processed information can be used to predict forthcoming events. These predictions, along with the pre-processed sensor information, is then used to make decisions about how the state of the environment should be adapted. These decisions are then used to obtain the actual commands given to the actuators.

The last two phases, decision making and device control, belong to the optimization category. As can be seen, machine learning uses form quite a clear loop structure which enables the continuous adaptation of the application. This loop is called the *control loop*. For our use case, we implemented the cognitive system using a nodejs library ‘brain’ with the inputs as temperature, humidity sensor reading and the expected output as the switch control.

Fhem Implementation

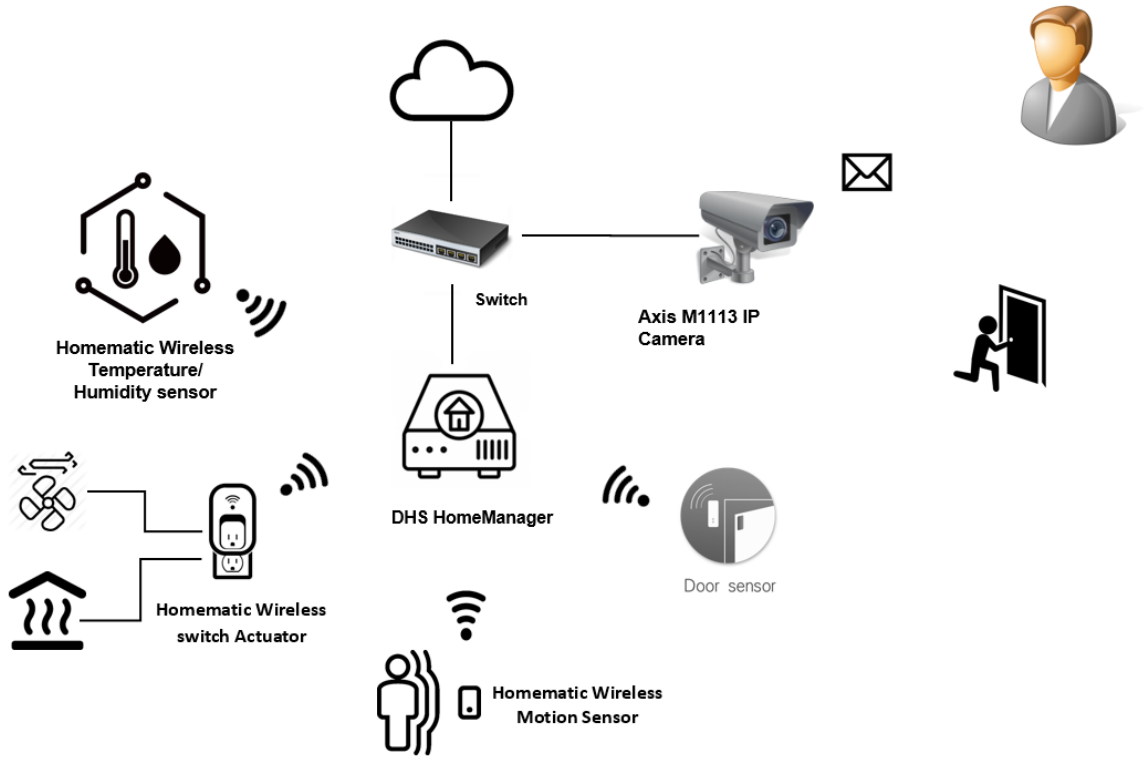
For our setup, we used the FHEM home automation system developed in Perl. Our host for the FHEM server is a Cubieboard, a Linux based embedded computer which interfaces with the sensors and receivers (HomeMatic Devices). Fhem as a platform is extensible with the use of modules and supports a wide variety of protocols and devices like FS20, HomeMatic among others.

We utilize Fhem.js, a node.js server which works as a websocket gateway to the Fhem server. Clients can use socket.io in Javascript to establish a websocket connection to Fhem.
It is possible to subscribe for updates of Fhem resource state like on/off or temperature. The websocket connection will deliver this values just in time. Furthermore, Fhem commands could be send other this connection.

Components Used

1. DHS HomeManager
2. Homematic Wireless switch Actuator 1-channel
3. Homematic Wireless Door/Window Sensor, optical
4. Homematic Wireless Temperature/ Humidity sensor indoor
5. AXIS M1113 Network Camera

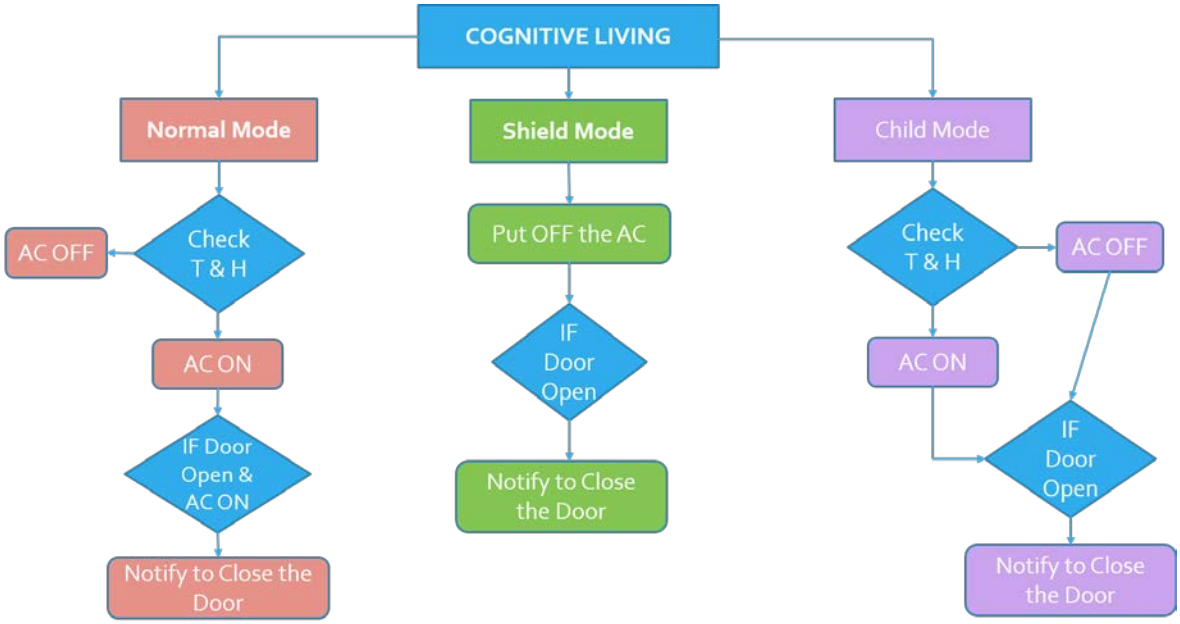
System Architecture



The heart of our prototype is the DHS Homemanager, which is a small computer based on CubieBoard 2. It has built-in wireless antenna which supports Homematic Wireless devices. Homematic Wireless switch Actuator 1-channel, Homematic Wireless Door/Window Sensor, Homematic Wireless Temperature/ Humidity indoor sensors are connected to the DHS Homemanager via Wireless médium. The door/window sensor is used to detect if the door or window is open or not. The temperature and humidity sensor sends temperature and a humidity readings to the Homemanager. The Wireless switch Actuator is used to control the connected electrical load (Heating/Cooling system) to control the comfortability of the living space. In the ideal system we will also use wireless motion sensors to detect human presence in the room and optimize the energy consumption when there is no one in the room. The Axis M1113 network camera is connected to the network and used for surveillance and sending email notification to the user in case of unwanted movement detected in the monitored area.

Proof of concept

To prove our idea, we implemented the following scenario using FHEM. As we discussed earlier, Cognitive Living has three operating modes: Normal mode, Shield mode and Child mode. The flow chart below depicts the function of the three modes.

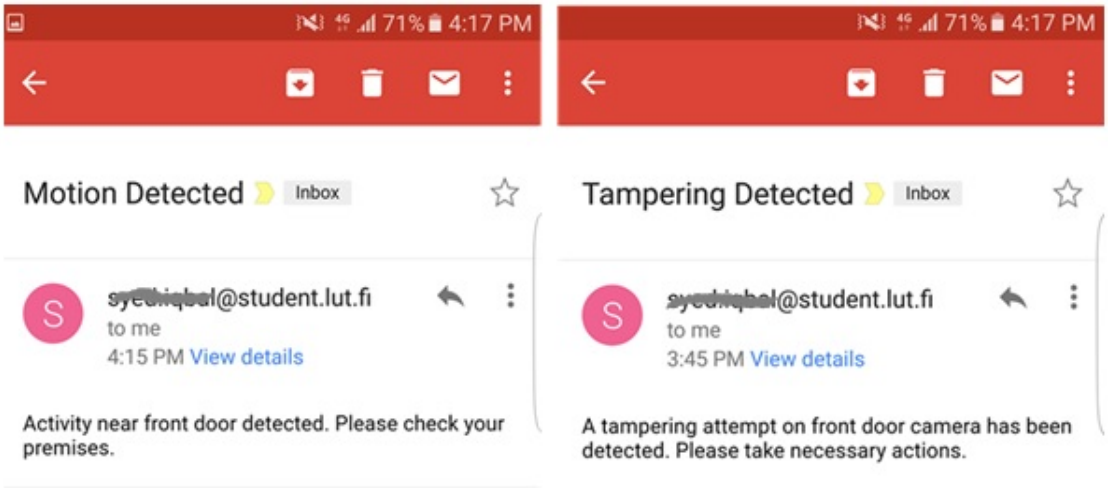


Normal mode is when people are at home. The main purpose of normal mode is to provide comfort and save energy in possible ways. In our scenario we check the temperature and humidity inside the house on a regular basis and decide if we should put on the air conditioner or not (comfort). If the air conditioner is ON, we check if any of the doors or windows are open. If it is found to be open, we notify the user to close the door / window to save energy (as the air conditioner is ON).
Shield mode is when no one is at home. The main purpose of shield mode is to save energy by putting OFF all the electric and electronic devices and security by detecting motion in the house and notifying users in case of motion or tampering attempt by using AXIS IP Camera. When shield mode is activated, it automatically puts OFF the devices (Air conditioner in our implementation) and checks if doors and windows are open (Security) and notifies.
Child mode is when a child / children above the age of 5 are left alone at home. The main purpose of this mode is comfort and security of the child. Similar to normal mode, we decide to put ON or OFF the air conditioner based on room conditions. The system also notifies to close the doors / windows if they are open for the safety and security of the child.

Motion Detection IP Surveillance Camera

For surveillance, in our prototype we have used Axis M1113 Network camera. The camera features advanced motion detection and manual focus lens. We have used the latest firmware to use Axis Motion Detection 3 application for our purpose.

This application allows us to select one or multiple spots/area which is our area of interest in its capture frame to define as ‘Include Area’. We can define the monitored object size, sensitivity and also compare the change of activity to historical data to detect a motion. We can also define area in the capture frame as ‘Exclude Area’, which will not be counted as motion detection zone.



This feature helps us to get precise and accurate motion detection notification. The camera can also detect tampering attempts if the view is blocked, spayed upon or even the lens is out of focus. The camera uses SMTP to send notification via e-mail to the predefined users in case of tampering attempt or motion detection. This way we can get immediate notification in case of burglar attacks or any unwanted movements in the zone under surveillance.

Energy Analysis

Our average houses features electronic equipment like TV, washing machine, microwave oven etc. They are usually connected to the power outlet, even when we are not using them. These electronic equipments keep drawing power while they are in standby. We can consider these electronic equipment as leeching devices.

Equipment	Energy consumption per hour(Watt)
LED TV	0.3
Mobile Phone charger	1
Computer Display, LCD	1.13
Computer, desktop	2.84
Computer, notebook	4.42
Printer, laser	4.5
Speakers, computer	4.12
Washing machine	3.2
Induction cooker	7
Coffee maker	1
Microwave oven	3
Audio System	10
Air Conditioner	50
Total per hour usage	92.51

Total Energy Consumption per year (kW)
485.86252

Total Energy Savings (0.155 euro/kw)
74.33696556

Carbon footprint reduction (kg CO2)
106.8897544

Considering 9 hours work and 8 hours during night on weekdays and 8 hours during night during weekend, we get on average 5,252 hours of standby time in a year. This standby energy consumption results in 485.86 kW of energy consumption per year. If we are able to save this standby power consumption, we will be able to save 74.33 € per year and reduce CO2 footprint up to 107 kg. Our proposed Cognitive Living approach can save a lot more than this when implemented by optimizing the energy consumption while people are in the house and cutting the standby consumption when they are not in use.

Benefits

Cognitive Living is an example of using ICT for Greening. Energy saving is one of the chief motives of the system and in turn plays a role in reducing carbon footprint and cost saving. Cognitive Living being an integrated system acts as a solution with enhanced safety and security

capabilities. By maintaining room conditions, it creates an ambient environment for living. Cognitive Living makes Home a Haven!

Home Automation Protocols

LONWorks

This technology was developed by Echelon Corporation for implementing control system networks. The root term LON, is an acronym for: Local Operating Network.

LONWorks is a complete solution for implementing distributed control networks. These networks consist of nodes that communicate with one another over a variety of communications media using a common message-based communications protocol.

Users can access all the elements required to design, install, and support control networks. The major elements include Neuron Chips, LONWorks transceivers, LONTalk protocol and LNS (LONWorks Network Service). LONTalk is a Control Network Protocol. Is a complete seven-layer communications protocol, with each layer optimized to the needs of control applications.

Features of LONWorks

- Efficient delivery of small messages.
- Reliable delivery of messages.
- Duplicate message detection.
- Multiple communications media.
- Low installation and maintenance cost
- Efficient use of channel bandwidth.
- Prevent tampering.

It implements the seven OSI layers.

Layer	Purpose	Services provided
Physical	Electrical Interconnect	Media-Specific Interfaces and Modulation Schemes (twisted pair, power line, radio frequency, coaxial cable, fiber optic)
Link	Media Access and Framing	Framing; Data Encoding; CRC Error Checking; Predictive CSMA; Collision Avoidance; Priority & Collision Detection
Network	Message Delivery	Unicast & Multicast Addressing; Routers
Transport	End-to-End Reliability	Acknowledged & Unacknowledged Message Delivery; Common Ordering; Duplicate Detection
Session	Control	Request-Response; Authentication
Presentation	Data Interpretation	Network Variables; Application Messages; Foreign Frame Transmission
Application	Application Compatibility	Network Configuration; Network Diagnostics; File Transfer; Application Configuration; Application Specification; Alarming; Data Logging; Scheduling

The physical layer defines the transmission of bits over a medium channel. Depending on the LONWorks transceivers characteristics, there are different channels that this technology supports. For instance, it can support twisted pair, radio frequency, power line and fiber optic. Depending on that, the channel network bit rate will vary. For example, the twisted pair channel has a typical rate of 78.1kbps.

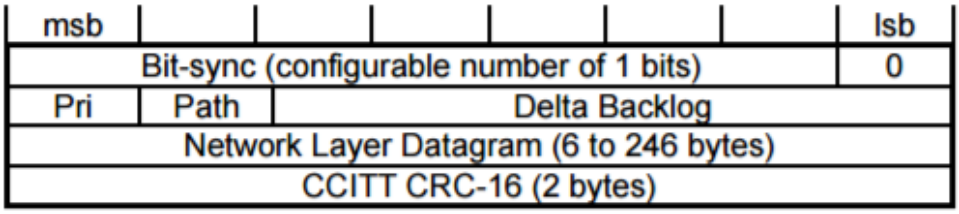
In the link layer is where the data encoding and media access method occur and the transmission of data frames its defined. LONTalk protocol uses a variant of the Carrier Sense Multiple Access (CSMA) algorithm for avoiding collisions in the transmission process the one used for this protocol is called Predictive p-persistent CSMA. It is known that on CSMA all the devices randomize their access to the medium to not interfere with the transmission of the other, they randomize different levels of delay (beta 2 slots). In this variant, a device will send a message in a

random slot with a certain probability p. This probability p is dynamically adjusted depending on the load of the network.

When this load increases, devices randomize over a larger number of beta 2 slots. The number of slots increases by a factor of n, which is the estimated channel backlog, meaning, the number of devices with a packet to send during the next packet cycle.

Additionally, to what is being described before, this protocol also offers a priority level when transmitting the frames, it gives a fixed number of 2 beta slots per channel as priority for the devices that need that. The limitations on this is that only 126 devices per channel can have priority assigned the pre-allocation of the bandwidth caused by reserving time slots.

The data frame in this protocol is the following:



- The preamble is for synchronization purposes. The Bit-sync are fields of the preamble, which implements Differential Manchester encoding.
- The Pri field is for the frame´s priority.
- Path, specifies the channel to use for special purpose mode transceivers.
- Delta Backlog: receivers add this value to the backlog estimated for transmission of the frame.
- CRC field is just for cyclic redundancy check, to compare if the data sent has been correctly received.

The packet size depends on the type of channel of your choice, for example on the twisted pair channel of 78.1kbps the average packet size is 112 bits.

An average packet is in the range of 10 to 16 bytes long, depending on the length of the domain identifier, the addressing mode, and size of the data field. The maximum packet size is 249 bytes including data, addressing, and protocol overhead

This technology has been used in the USA and it's been applied in different sectors:

- Municipal and highway/tunnel/street lighting.
- Heating and air conditioning systems.
- Subway train control.
- Stadium lighting and speaker control.
- Security systems, fire detection and suppression, and newborn location monitoring and alarming.
- Smart electricity metering.

DASH7 Alliance Protocol

Is an open source Wireless Sensor and Actuator Network protocol; built on top of an asynchronous Wireless Sensor Network Media Access Control (for 433 MHz wireless sensor communication). Due to its frequency, it has better propagation characteristics also, this standard was mainly used for military logistics.

It uses Generally Radio Frequency Identification technology, which is used for locating and tracking objects in a variety of applications. This technology consists of a tag and a reader. There are two types of tags, active and passive. Passive tags receive their energy from the readers, when readers emit electromagnetic radiations to detect the tag.

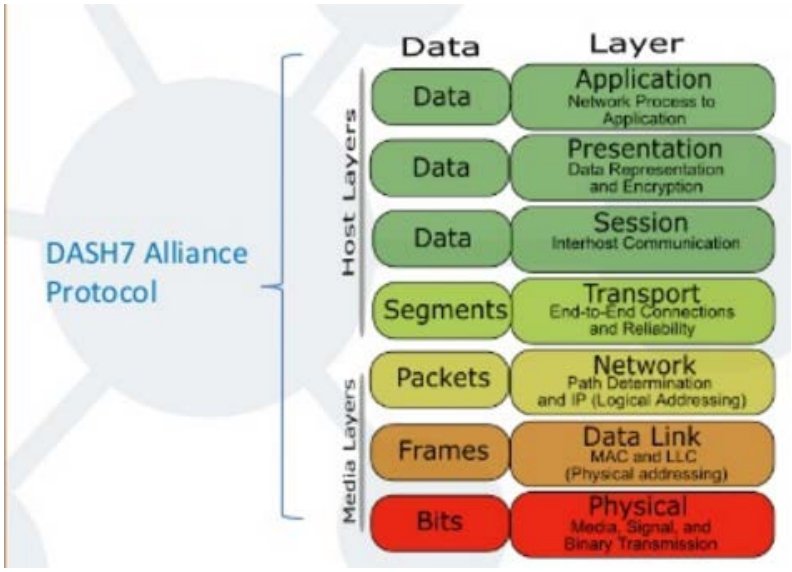
DASH7 protocol features:

- Provides multi-year battery life.
- Long range, of up to 2 km.
- Low power (about 10 times less consumption than Zigbee)
- Low latency for connecting with moving things.
- AES 128-bit shared key encryption support.
- Data transfer of up to 167 kbit/s.
- Good for indoor use where is much concrete and walls.

BLAST Network Technology.

- Bursty: abrupt data transfer unlike streaming video or audio.
- Light: Limited packet size of 256 bytes.
- Asynchronous: communication is command response based (no need of periodic synchronization).
- Stealth: no need of periodic address broadcasting.
- Transitive: mobile transitional behavior of devices and tags.

Same as LONTalk, this protocol also implements the 7 layers of the OSI Model.



On the physical layer, this protocol defines the channels that will be used, the modulation, encoding and packet structure.

There are different classes for the channel:

- High rate class, which consist of a 432kHz bandwidth and a bit rate of 200kbps.
- The normal class, consist of 216kHz bandwidth and a bit rate of 55.55kbps
- The blink class with 648kHz bandwidth and bit rate of also 200kbps.

The packets consist of a preamble of 32 bits on the normal channels and 48 bits on the high rate and blink channel.

The modulation technique used in this protocol is the Gaussian frequency shift keying, which uses a Gaussian filter to makes the transitions smoother and then continue to the FSK modulator that

transmits the digital data through discrete frequency changes of the carrier signal. The data link layer is where the filtering, addressing and MAC process happen.

The incoming frames from the physical layer are filtered by three processes:

- Cyclic Redundancy Check for validation.
- Subnet matching (4-bit specifier and 4-bit mask).
- Link quality assessment, link budget should be higher than a predefined link threshold.

For addressing, the protocol provides the device ID in a fixed Unique ID, which contains 24 or 36 bits Organizational Unique Identifier based on a 40 / 28 bits serial number. It also provides a dynamic network- unique Virtual ID of 16-bit ID (unique).

DASH7 has two types of frames:

- Foreground, for regular data or data requests, with variable length up to 255 bytes.

Length	Headers	Payload	Footer	CRC16
1 byte	3-38 bytes	0-249 bytes	0-20 bytes	2 bytes

- Background, for short broadcast messages and with a fixed length of 6 bytes per frame.

Subnet	Payload	CRC16
1 byte	3 bytes	2 bytes

The headers contain information related to data link layer security, address control (source and destination id), subnet, and estimated radiated power of the transmission.

CSMA/CA is implemented in this protocol as avoidance collision mechanism for data transmission of the devices by checking if the medium is idle or free for sending their information and then randomizing the turn of transmission for each device.

This technology has been applied in:

- Building automation. (HVAC, humidity, lights, etcetera.)
- Location-based services
- Smart Energy (metering).
- Logistics area for tracking shipments, trucks, rail cars (supply chain).

References

1. Using machine learning in the adaptive control of a smart environment ISBN 978-951-38-7420-9. URL: http://www.vtt.fi/publications/index.jsp)
2. https://github.com/winne27/Fhem.js
3. ECHELON Corporation. Introduction to the LonWorks Platform. Revision 2. Revised 1st of March 2017. URL: http://www.echelon.com/assets/blt893a8b319e8ec8c7/078-0183-01B_Intro_to_LonWorks_Rev_2.pdf
4. ECHELON Corporation. LonTalk Protocol Specification. Version 3. Revised 1st of March 2017. URL: http://www.enerlon.com/JobAids/Lontalk%20Protocol%20Spec.pdf
5. Weyn, M. Ergeerts, G. Wante, L. Vercauteren, C. Hellinckx, P. (2013). Survey of the DASH7 Alliance Protocol for 433 MHz Wireless Sensor Communication. Revised 1st of March 2017. International Journal of Distributed Sensor Networks. URL: http://journals.sagepub.com/doi/full/10.1155/2013/870430
6. Weyn, M. Dash7 Alliance Protocol Technical Presentation. (2013). Revised 1st of March 2017. URL:https://www.slideshare.net/MaartenWeyn1/dash7-alliance-protocol-technical-presentation