Case Studies in IoT -Smart-Home Solutions Pedagogical Perspective with Industrial Applications and some latest Developments

Hans-Petter Halvorsen, Alexander Jonsaas, Saba Mylvaganam, Josef Timmerberg, Jean-Marc Thiriet

Case Studies in IoT - Smart-Home Solutions

Pedagogical Perspective with Industrial Applications and some latest Developments

Hans-Petter Halvorsen, Alexander Jonsaas, Saba Mylvaganam

Faculty of Technology, Department of Electrical Engineering, IT and Cybernetics, University of Southeast Norway
hans.p.halvorsen@usn.no; Alexander.Jonsaas@usn.no; Saba Mylvaganam@usn.no

Josef Timmerberg
Jade University of Applied Sciences, D-26389 Wilhelmshaven,
jt@jade-hs.de ;

Jean Marc THIRIET
Université Grenoble Alpes,
jean-marc.thiriet@univ-grenoble-alpes.fr

***Abstract*— Creative common license (CCL) based microcontroller platforms boards with various processing capacities and handling of a plethora of I/O are available in the market at various levels of complexities and prices. These CCL based microcontroller platforms boards are increasingly used, predominantly in the academia, for sensor networking as well as handling complex IoT (Internet of Things) functions. This paper looks into a case study of incorporating Arduino and Raspberry Pi for sensor networking, data transmission and enabling IoT functionalities. As a practical realization, an experimental smart home is realized with an array of sensors and a system architecture consisting of a set of Arduino and Raspberry Pi modules. The paper presents necessary aspects of codes in the form of pseudo-codes and describes some aspects of I/O with respect to the sensors used. Finally, the security problems are also addressed. Depending on the time available, a real system will be operated during the presentation of the paper.**

Keywords—IoT, Smart Homes, Security, Sensor Networking, EU collaboration

I. INTRODUCTION

The basic elements of home automation were already put into use in the 1970's. Technical discoveries are made by some and taken up and further developed by others. A company in Scotland developed a smart home product X10. X10 made use of the home electrical wiring to switch on and off electrical appliances (receivers) with simple remote controls or keypads (transmitters) with a command alert to the system, using unique unit ID numbers of the receiving devices that should receive the command and the codes for the action, such as switching on/off. Such a system was prone to malfunction due to noise arising from powering of devices coupled to the electrical wiring. In recent years, some systems have been used for smart home applications. A simplified overview of the possibilities with selected systems as examples are given in Table 1.

Probably, as per today, the IT magnate Bill Gates has one of the smartest home in the world with the latest elements of IoT. According to reports, each person in Gates' household has a unique chip communicating with home entertainment systems, refrigerator, heating/air-conditioning & lighting and even the electronic still image displays matched to the taste of the person!

This paper deals with some key concepts dealing with the hardware, software including system integration addressing the DMM (Data-logging, Management and Monitoring) platform. From a pedagogical viewpoint, a simple modeling of internal temperature in a smart home is also given. A DMM is prone to problems arising from hacking like the recent global WannaCry attack experienced internationally on 12th May 2017. Hence, security issues are also addressed using a simple demo involving penetration tests.

II. IOT IN SMART HOMES

Internet of Things (IoT) has evolved out of the need to connect, communicate and interact with "things" at home, in the factory, in the car or even in space, just to name a few scenarios. IoT has different names, e.g. Web of Things (WoT), Industrial Internet of Things (IIoT), Internet of Everything (IoE) and increasingly covered by the term Industry 4.0. Intel defines IoT as "devices that are connecting to the internet, integrating greater compute capabilities, and using data analytics to extract valuable information", [1]. In March 2017, China announced a new strategic program called "Made in China 2025" addressing Industry 4.0 and promoting Industry 4.0 technologies, [2]. IoT is based on increased intelligence in things connected to each other and sharing data of mutual interest with each other and interacting to achieve predefined goals/actions and adapting to changing situations with a certain degree of autonomy. The fact that the essential component for the full-fledged IoT is the sharing of data entails mechanisms and measures to safeguard the IoT with high grade of security, which has been a growing concern, magnified after the recent global WannaCry IT-sabotage action.

IoT is already taking up the home scene with interconnected devices enabling connection to and between persons and increasing quality of services with improved security for people and property. Developmental issues related to IoT are schematically presented in Fig. 1.

TABLE I. SMART POPULAR HOME COMMUNICATION (NOT AN EXCLUSIVE LIST)

Techno logy	Features		
	Wireless/Wired	***Mesh***	***Wireless/ Wired Action***
ZWave	Wireles: With embedded code for Zwave devices[a]	Yes	Master Slave
ZigBee	Wireless: Based on IEEE wirless Personal Network	Yes	Master Slave
Insteon	Both[b]	Dual mesh	Peer
KNX[c]	Both	Mesh	Peer

[a.] Master/Slave hierarchy for communication; [b] More Insteon devices → stronger messages;

[c]Merged concept based on European Home Systems Protocol (EHS), BatiBUS, and European Installation Bus (EIB or Instabus)

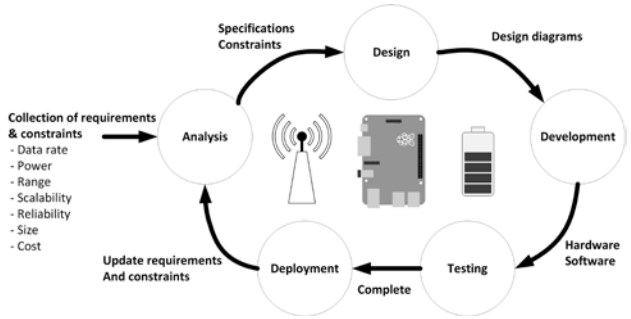


Fig. 1. Main aspects of an evolving IoT with focus on holistic design and implementation, involving transmission, reception, energy availability, reliability, security etc. From pedagogical and Interaction Design open hardware and software are common in this system integration

IoT in the context of smart homes is essentially a collection of interconnected smart and possibly autonomous things interacting with each other and authorized people encompassing home appliances, home entertainment, safety and security, vehicles belonging to the authorized people etc. The vision of technology push industries like Microsoft, Google, Intel etc. is to have a fully integrated smart home evolving into a smart city, which again leads to a smart world. This concept of smartness at all level is only possible when the security issues are foolproof, Fig. 2.

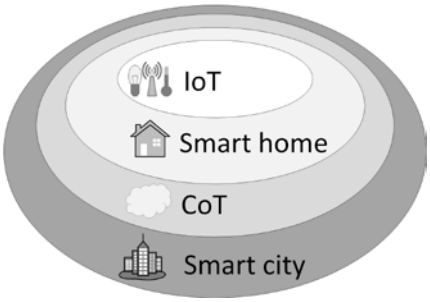


Fig. 2. Ubiquitous smart systems encompassing many stages of integration of IoT with other services and users including data from all IoTs in the Cloud of Things (CoT) available for the users

III. OVERVIEW

Home automation has gone through different stages of developments, with wired communication and control of devices in the 1970's based on X10, wireless and wired systems as shown in Table 1, inclusion of robots and humanoids with more and more applications using artificial intelligence techniques such as deep learning. This section deals with DMM and some software approaches as used in a pedagogical context.

A. Arduino

Arduino is an open-source prototyping platform consisting of several microcontroller boards, [3]. For programming these microcontroller boards, the user can download the free Arduino IDE (Integrated Development Environment). Due to the low price of different versions of Arduino boards and ease of handling and programming them, designers, members of the academia and manufacturers of popular AI items such as remote controlled vehicles and drones increasingly use them. Recently, there have been reports on various high-tech Arduino projects such as Laser Harp, Open Source GameBoy, Autonomous Robot etc. involving a plethora of sensors, shields and actuators, with a large community support and available information on the internet makes Arduino suitable for many applications. In addition to the original Arduino boards, several third party clones can be bought from a variety of vendors. In 2015 Arduino launched the Genuino as the official name for Arduinos sold outside the US. Essentially working with Arduino involves using the Arduino hardware proper in a straightforward programming environment with close interaction with the community involving a certain philosophy of design and realization of goals. With the launch of Arduino, the concepts of open hardware and software have dominated the interaction designers who participate in gatherings with their prototypes and urge the community to push the frontier even further.

B. A brief note on Raspberry Pi

Raspberry Pi is a small, low-cost single board computer (SBC) series developed by the UK based Raspberry Pi Foundation. The Raspberry Pi computers offers high performance compared with microcontroller boards like the Arduino Uno. Today, the most advanced model is the Raspberry Pi 3 Model B. This model offers a 1.2 GHz 64-bit quad-core ARM processor, 1 GB RAM and 40 GPIO pins. A microSDHC card is used for data storage. The SBC has 4 USB slots, HDMI port, Wireless LAN, Bluetooth Low Energy and an Ethernet port, [4].

Several operating systems are available for the Raspberry Pi 3, with Raspbian (based on the Debian Linux distribution) as the default alternative. Raspbian comes with a variety of pre-installed tools, e.g. Python, a free version of Wolfram Mathematica and the Java development environments Greenfoot and BlueJ, [5].

C. Smart Home Example

This section gives some key concepts involved in a system with Arduino and Raspberry Pi.

Fig. 3 and Fig. 4 show the main components and concepts involved in a DMM, which is crucial for any Smart Home. Components.

- Sensor nodes acquire data from various sensors in the Smart Home (home entertainment, heating, ventilation and air conditioning, lighting control system, presence and number of people , robotics, security, home appliances such as refrigerators, washing machines, even kettles (iKettle).
- Arduino and Raspberry Pi function as sensor nodes in the configuration shown in Fig. 3 and Fig. 4
- Data Hub: Gathers data from different sensor nodes in a defined area of surveillance, in our case the Smart Home.

Once the diverse sensor data are gathered and logged in, DMM "hands over" the data to the dedicated software and services, which are typically,

- Database: Repository for the sensor data
- Data Cloud Service for acquiring data from multiple areas in the cloud. The communication can be HTTP and REST APIs, as shown in Table 1.
- Data Management Software for configuring data points, logging rates, events and actions, etc.
- Data Logging Software for acquiring and handling sensor data within a sensor node
- Data Monitoring Software for monitoring and alarm and events handling based on inputs from multiple Sensor Nodes

As shown in Fig. 3, REST API is created and used for data logging from devices like Arduino, Raspberry Pi etc.

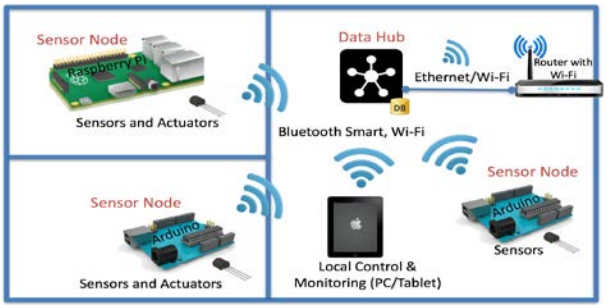


Fig. 3. Sensors, Actuators showing the DMM platform (Data-logging, Management and Monitoring)

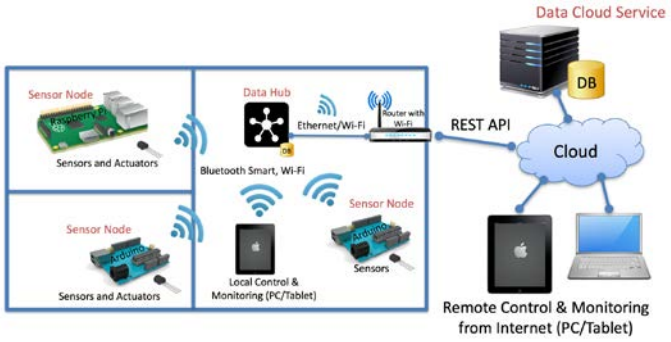


Fig. 4. DMM with remote/cloud configuration of the DMM – a general perspective Soft Sensing of parameters from existing hard sensors

Measurements such as temperature and CO_2 concentrations are affected by occupants indoors. AI Models and physical models forming soft sensors can be used to find the number of people in a room or a set of rooms. Some applications use data analytics also called big data to find useful information of the number and movement of people in buildings. An example is the innovation dedicated to the customer mobility and purchase behavior developed by emerging companies, Fig. 5.

Fig. 5. Customer count from existing cameras in a retail store, Courtesy Link An example of using soft sensing

Such soft sensing combined with other data can give valuable information when it is shared with the right authorities with secured data sharing and dedicated analytics giving more information on history, status and future developments of various parameters. An example is shown in Fig. 6.

Fig.6. Movement and purchase behavior of customers in a retail shop. SbP giving valuable information shared by authorised partners. Courtesy Link.

D. Example Program

As an example for the software based on one of the hard sensors, the temperature in a room using the configurations given in Fig. 3 and Fig. 4 are given in Fig. 7. This flow diagram illustrates the modus operandi of the software used in Arduino, for the temperature control algorithm. Fig. 8 shows the Arduino IDE (Integrated Development Environment) with the values of the measurands as displayed on the serial monitor.

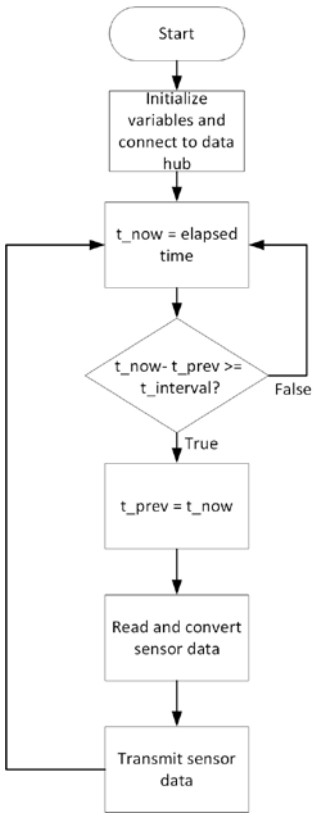


Fig. 7. Temperature Control with Arduino – an example of the flowchart for one measurand in Smart Home Application. Software example as applied for the temperature control problem shown in Fig. 4

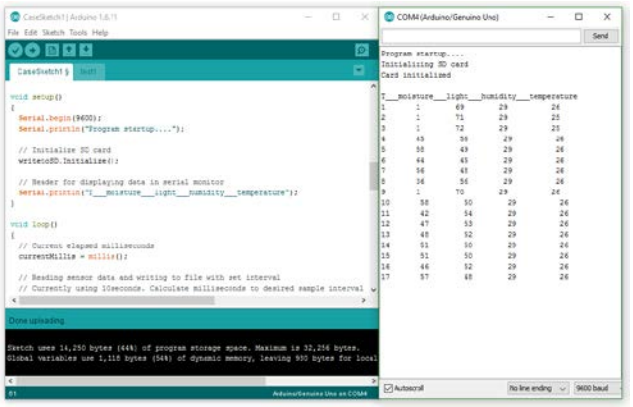


Fig. 8. : Arduino IDE with measurements displayed on the serial monitor

IV. Security Aspects using Arduino and Raspberry Pi

Low level programming should cater to computer security considerations with close scrutiny of the operating system design with embedded systems. Raspberry Pi comes in handy in enabling embedded systems in conjunction with Arduino. System security is often compromised in cases of unexpected software behavior. Malicious code running besides user code is sometimes visible. Very often, hackers exploit weaknesses at system-level to hide their attacks. Rootkits dive into the operating system, taking full control of the system.

A. Sensor data broadcasting using Plotly

There are various ways of accessing sensor data and processing them. To address security aspects with transmission and reception of sensor data, the application called Plotly is used. Plotly, (URL address: plot.ly) is a tool for online data analytics and visualization capable of handling programming languages like MATLAB, Arduino, Python, R etc.

The main steps are the following:

JavaScript is coupled to a web application called plotly. Raspberry Pi sends the sensor data via TCP to the servers of plot.ly. Data is transformed into real time trend graphs using plotly analytics tool. Accessing web browser after uploading a firmata library (available in the Arduino IDE in the examples). This library implements the firmata protocol. A URL address is displayed in the console. Then the trend plots are displayed as shown in Fig. 9. The necessary details are shown in the flow diagram given in Fig. 10.

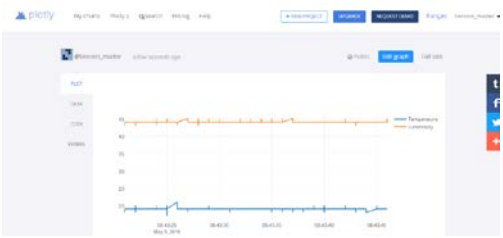


Fig. 9. Screenshot of the web page displaying the trend of the sensor data as observed using the plotly web application showing real time values

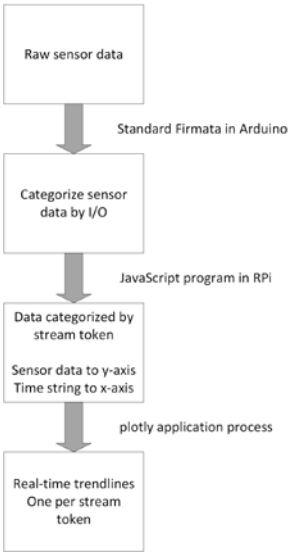


Fig. 10. Real time data as trend plot delivered using a program like plotly.adapted from [6].

B. *Security aspects and penetration tests*

When the sensors are connected to the Arduino with wires, remote attack is not possible, as the Arduino transfers the sensor data via wires to the Raspberry Pi. When the web server is on the Raspberry Pi, the transmission and reception of data are done locally. When the sensor data is sent to a plot.ly server using TCP, without any encryption, this data can be captured with a "sniffer" like Wireshark placed between the Raspberry Pi and plot.ly. When the transmission of sensor data and the data processed by plot.ly are sent with https, we have some security. Higher security is achieved in plot.ly with so called "behind-the-firewall" security, which is subscription based facility.

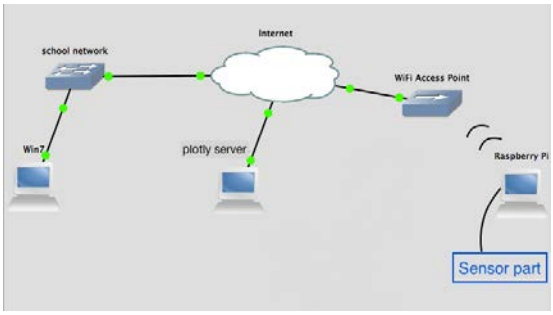


Fig.11. The system with sensors and data feed to plotly, [6].

C. *Man in the middle attack*

This case involves sensor data transmission between Raspberry Pi and a web server. A scenario of a "Man in the middle attack" between the Raspberry Pi and the plot.ly receiving the sensor data was realized and tested. The Raspberry Pi is connected using the WiFi via the Internet to the plot.ly server. Man in the middle attack was realized using a laptop with Kali Linux operating system. Laptop with Wi-Fi and Kali Linux is has several software packages for performing penetration tests and suitable for performing penetration tests.

The Raspberry Pi is connected to a guest network provided by USN, called HSN-guest, to which the Kali laptop was connected. This network has the IP address 158.36.239.0 (USN uses public addresses for the Wi-Fi network). IP and MAC addresses of the Raspberry Pi, which represent the victim, with the IP address 158.36.239.35; the laptop, which represents the hacker, with the IP address 158.36.239.28; and the gateway, with the IP address 158.36.239.1 are now in the penetration test. The type of attack ARP spoofing (also called ARP poisoning), is done using the ARP tables. Raspberry Pi send packets to the gateway for transmitting data to plot.ly server using the Internet.

Kali laptop can play the role of gateway for the Raspberry Pi with ARP packets, and the role of the Raspberry Pi to the gateway. Through this arrangement, data packets flowing between the Raspberry Pi and the gateway, will be forced to go through the Kali laptop. When sensor data are sent by the Raspberry Pi, the Kali Linus Laptop will receive the data and then transmit the data to the gateway and vice versa as shown in Fig. 12. During the attack, Kali Laptop with a dedicated program called Ettercap can access data flowing between the Raspberry Pi and the gateway.

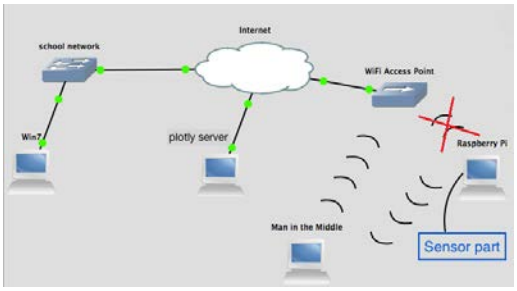


Figure 12. Overview of the networking scenario with the data transmission and penetration tests using Man in the Middle attack performed with Kali Linux OS installed in the PC. Raspberry Pi, which represent the victim, with the IP address 158.36.239.35; the Kalin Linux laptop, which represents the hacker, with the IP address 158.36.239.28; and the gateway, with the IP address 158.36.239.1. From [6]

The details of the programming involved is presented in [6]. Targeted IP is shown in Fig. 13 using the program Ettercap.

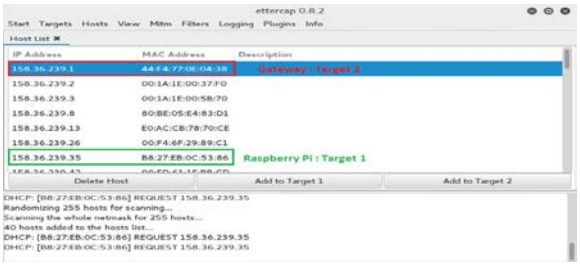


Fig. 13. Host list of the network 158.36.239.0 obtained by sniffing with Ettercap, where the Raspberry Pi is connected to Internet showing Man in the Middle attack is performed, from [6].

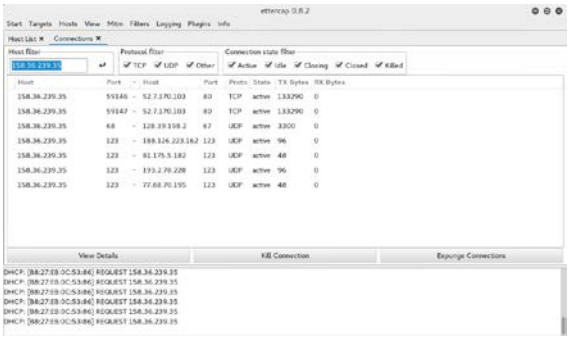


Figure 14. Connections to the IP address 158.36.239.35 (Raspberry Pi). Two ports used for transmission of sensor data plot.ly server (port 59146 and 59147),
[6].

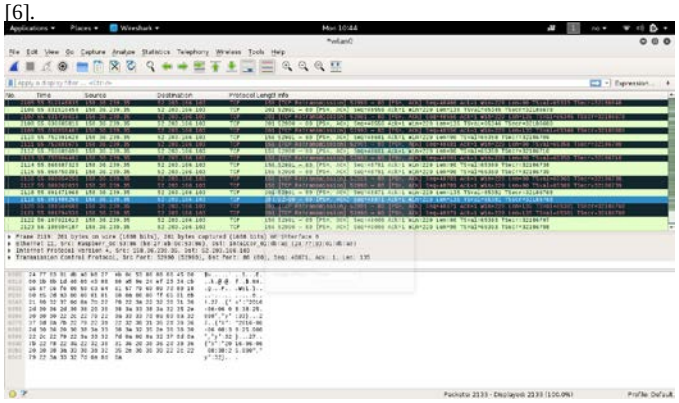


Fig. 16. Data transfer between the Raspberry Pi and the plot.ly server captured by Wireshark. Highlighted data are sensor values with time stamp. Captured with Kali Linux laptop with Man in the Middle attack using Ettercap, from [6].

Fig. 15 shows the IP address of the Raspberry Pi and the two ports used for “spoofing”. Figure 16 shows the captured sensor data strings in the successful Man in the Middle attack performed.

V. SMART HOME MODELING AND CONTROL

As a final stage in the pedagogical effort following the trend of Intel Smart Tiny House, used in experimenting with various smart appliances meant for a smart home [7], miniature homes were built for a collaborative course between Jade University of Applied Sciences and Texas Tech University. The goal is to model systems in smart homes and control certain parameters, such as temperature and humidity. A typical house is made to the scale 1:10. An example is shown in Fig. 17. About 30 students were divided into five groups, to work with selected engineering problems associated with the smart house. The tasks are defined for seven groups as follows: Group A - Heating Pool (4 students); Group B - Heating Room (4 students) ; Group C - Light regulation (4 students);Group D – Photovoltaics; (4 students), Group E - Communication Arduino – Mobile Phone (4 students); Group F - Optical Movement Recognition (4 students). In the modeling and control problem, the heating of swimming pool and the floor were addressed using the miniature house shown in Fig. 17. The size of the house used in this project based learning program can be seen in Fig. 18.

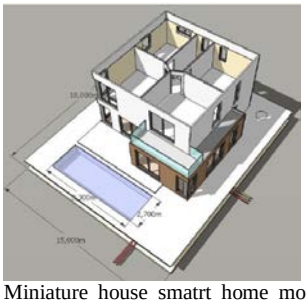


Fig. 17 Miniature house smatrt home modeling with temperature, illumination, optical moement detection etc.

Fig. 18 . Windows used in the miniature houses of the PBL projects at Jade University of Applied Sciences

In addition to the communication issues discussed in earlier sections of this paper, a simple model was also devloped to estimate the temperature due to floor heating. The model and the control loop for the heating are shown in Fig. 19 and Fig. 20. These sub-tasks were assigned to different groups of students.

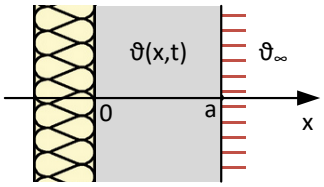


Fig. 19. Floor materials with heater and temperature distribution. Modeling with Fourier equations and series. $\vartheta(x,t)$ is the temperature as a function of distance and time

Fig. 20 Control loop for ground floor heating . Regler: Controller; Reglerstrecke – Controlled system; Stellglied-Actuator.

The model can be studied further to estimate and control the temperature to adjust the room temperature in different rooms. The main goals are controlling and holding the temperatures in the room and swimming pool at desired temperatures. One group of students worked with the following tasks:

- measuring the step function response of the control process
- building the mathematical model from the step function response
- simulating (Scilab, Xcos) the control process with the mathematical model value

Another group had the following tasks:

- create a pulse packages controlled modulator for the power converter
- simulate the circuit with LT-Spice
- build (hardware) and test the above unit
- measure the step function response of the control unit
- build (hardware) PWM (Pulse Width Modulation) controlled unit for the room heating

All groups in the category of temperature control had in addition the following tasks:

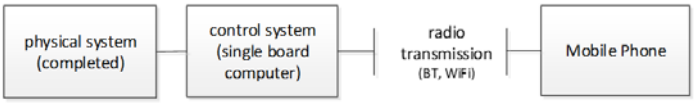
- creating the mathematical model with physical knowledge
- comparing the mathematical model with that of measurement
- calculating the frequency response characteristic from the step function response
- simulating (Scilab, Xcos) the control process with the mathematical model and the frequency response characteristic

The following tasks were also assigned:

- programming the controller with Arduino
- measuring the step function response of the overall system and giving the presentation with a movie

Simple modeling with heat transfer modeling using ansatz with Fourier series gave the temperature distribution shown in Fig. 21.

A module suitable for students following courses in communication, control and sensorics may use the model shown in Fig. 22 to cover different topics needed for such interdisciplinary course.



1. Development of a mathematical system
2. Planning of sensors and actuators for the system
3. Selection and analysis of single board computer
4. Programming of the SBC
5. Testing the current system
6. Programming the Mobile Phone
7. Testing the complete system

Fig. 22. Summer school project at Jade University of Applied Sciences in collaboration with Texas Tech University; SBC – Single Board Computer, BT – Bluetooth.

For this purpose, a mathematical model is necessary. As the starting point, layered floor structure shown in Figure 23 is used. :

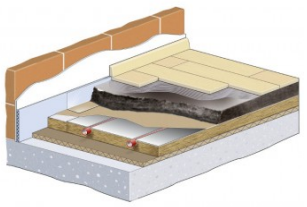


Fig. 23. Layered floor structure used in the mathematical modeling of temperature distribution $\theta(x,t)$

As the floor consists of different layers of materials, a simplified model consisting of the layers shown Fig. 24 is considered. The cross-section of the sections shown in Fig. 24 is a series of parallel layers with the grey layer in the middle.

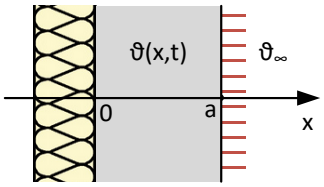


Fig. 24 Parallel layers of materials considered for heat transmission modeling for determining the temperature distributin $\theta(x,t)$

The temperature distribution $\theta(x,t)$ in the sections satisfies the following equation in temporal and space domains:

$$\frac{\delta\vartheta}{\delta t} = \alpha \frac{\delta^2\vartheta}{\delta x^2} \quad (1)$$

Using the product ansatz for $\theta(x,t)$, the general solution is given by:.

$$\vartheta(x,t) = A_0 + B_0 x + \sum_n \left(A_n cos(s_n x) + B_n sin(s_n x)\right) e^{-s_n{}^2 t} \quad (2)$$

By using the boundary values and initial state of the system, the distribution can be determined.

In a simplified scenario, a solution can be found for the distribution of temperature at any given point x of Fig. 24, as a function of time t. At x= 1 heat is transferred into the layer. The heat insulation is at x=0 (yellow part in Fig. 24). At t=0, the temperature is everywhere 20 °C (red line). With the heating on, at t=15s, the temperature is 80 °C everywhere in the material (blue line).

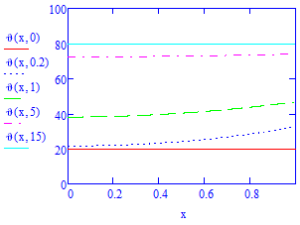


Fig. 25. Temperature distribution $\theta(x,t)$ in different layers with heating as a function of x and t for the case shown Fig. 24

The temperature in the insulated wall as a function of time is given in Fig. 26 (red Line). The saturation function is also shown in Fig. 26.

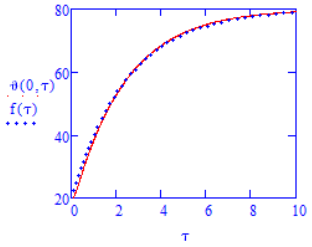


Fig. 26. Temperature distribution as a function of time in the wall.

Based on the exponential function involved in the saturation effect shown in Fig. 26, a series of different layers of materials can be represented by a series . RC-components as shown in Fig. 27. The RC-network shown in Fig. 27 forms the well known Cauer circuit and can be analysed using many tools such as SPICE.

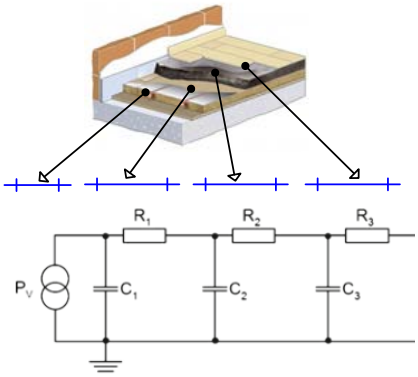


Fig. 27 Temperature modeling for the floor heating in the miniature model. x =0 using Cauer circuit – RC lumped components in tandem. Each layer characterised by a pair of parameters $R_i$and C_i

Each layer is modelled using a circuit consisting of R_i and C_i, lumped components, characteristic to the layer i= 1,2, 3… As early as 1958, in conjunction with research studies in fire-resistance of building materials, electrical equivalent circuits have been used for simulations of transient phenomena related outbreak of fire in buildings, [8]. Recently, a similar model has been used for circuit level simulations of heat transmission studies in layered structures, [9]. This method of simulations opens up a scenario (recently called “digital twin”) which is often found in many IoT applications, where the virtual world helps to improve performance in the real world with very much less financial cost and frequently also in much shorter time

ACKNOWLEDGMENT

The results presented here are based on different project based learning sessions with students and staff at University College of Southeast Norway, Jade University of Applied Sciences and Université Grenoble Alpes. Collaboration between these institutions were facilitated by ERASMUS + funding. Colleagues, Mr. Nordli and Mr. Varholm of Vestfold in the Campus Vestfold of USN helped us with guidance and advice in performing penetration tests discussed in this paper. Louis le Gac, a student from Université Grenoble Alpes, had his internship in USN during June 2016.

References

[1] https://newsroom.intel.com/press-kits/intel-and-the-internet-of-things-2/, accessed on 22.05.2017

[2] http://www.chinadaily.com.cn/business/tech/2015-04/02/content_19980929.htm, accessed on 22.05.2017

[3] https://www.arduino.cc/en/Guide/Introduction , accessed on 22.05.2017

[4] https://www.raspberrypi.org/products/raspberry-pi-3-model-b/, accessed on 22.05.2017

[5] https://www.raspberrypi.org/files/about/RaspberryPiFoundationReview2016.pdf, accessed on 22.05.2017

[6] L. le Gac, The Connected Ship – Sensors and Data Security, Internship Report, in partial fulfilment of the requirements of the " Licence Professionnelle Réseaux Sans Fil et Sécurité" program Institut Universitaire de Technologie – Université Grenoble 1 & University of Southeastern Norway & , June 2016

[7] Intel, Introducing the Intel Smart ‘Tiny House’: Exploring Smart Home Technology in 210 Square Feet, Nov. 2, 2015

[8] A. F. Robertson and D. Gross, “An Electrical-Analog Method for Transient Heat-Flow”, Journal of Research of the National Bureau of Standards Vol. 61, No.2, August 1958 Research Paper 2892

[9] R. Wu, H. Wang, K. Ma, P. Ghimire, F. Iannuzzo, and F. Blaabjerg, “A temperature-dependent thermal model of IGBT modules suitable for circuit-level simulations," in Proc. IEEE Energy Convers. Congr. and Expo., 2014, pp. 2901-2908.