Realization of a Home Automation Network with Two Gateways Based on Open Source Hardware

Galidiya Ivanova Petrova, Grisha Valentinov Spasov and Georgi Aleksandrov Pazhev

Abstract – **The paper presents a realization of a home automation network with two wireless gateways based on open source hardware. Many of the home automation networks consist of a PC based machine (working as a gateway), a wireless network of sensors, smart systems for metering of water, electricity and gas consumption, actuators for heating, ventilation and air-conditioning (HVAC) and wireless alarm systems. The advantages of the proposed approach are the low cost, additional functionality and scalability together with better sustainability toward power supply disturbances. The described home automation network is based on microcontroller Olinuxino A13 with installed Android 4.0 operating system, used as Internet gateway, and microcontroller Olimexino 328 used as wireless sensor gateway. The communication inside the network is based on CNDEP protocol. A new adapted version of the communication protocol CNDEP, initially designed for data exchange in distributed embedded systems, is described.**

Keywords – **Smart home, Home automation network, Open source hardware, Bluetooth wireless gateway, Olimexino, Android, CNDEP protocol.**

I. INTRODUCTION

As stated in [1] the primary objectives of a smart home are to increase home automation, facilitate energy management, and reduce environmental emissions. A smart home is a residence equipped with a communications network, linking sensors, domestic appliances, and devices, that can be remotely monitored, accessed or controlled [2].

As defined in [3] the home automation is the residential extension of building automation. Home automation systems are used for monitoring and control applications for home user comfort, efficient energy management and security. These automation systems may span a variety of different networks including various sensor networks, smart systems for metering of water, electricity and gas consumption, networks for control of home environment as heating, ventilation and air-conditioning (HVAC) systems, and alarm systems networks. In general case, to handle interconnections between these networks gateways are needed.

Usually, the binding in heterogeneous networks use gateways in order to provide transparent operation of applications [4]. In this approach the gateways must implement the functionality of the protocol stacks of the networks which they connect. Traditionally, this is achieved with one of the controllers or workstations in the network. From one side, it connects a home automation network to Internet and plays the role of Internet portal, and from the other side it realizes the interfaces and protocol interactions to corresponding sensors, metering systems, actuators and alarm systems.

The alternative approach is to distribute the functionalities in two or three layers employing hierarchical structure. The first layer comprises the sensor networks with corresponding sensor gateways where the data and protocols are converted to the common format. By means of Internet gateway the second layer provides all the Internet functionalities and corresponding applications. The Internet gateway plays the role of server in the interaction with the third layer. The third layer usually is represented by Internet portals of smart grid energy control centers, security providers, central heating systems, etc.

Considering the home automation systems this approach is more perspective for future development as it allows easy integration of different types of sensor networks to the existing solutions. The advantage of such an open platform concerning the scalability of the system is obvious.

However, the implementation of a smart home system at the moment is affordable for limited group of users due to the costs associated with the purchase of smart appliances, metering systems, monitors, devices, along with installation and support services. Focusing on energy consumption and management services, high costs of the necessary technologies and difficult user interfaces are highlighted as key barriers in the literature [2] for wider spreading.

The aim of this paper is to present a realization of home area networks (HANs) and automation system for a smart home based on hierarchical structure employing low cost open source hardware and software platforms.

II. INITIAL REALIZATION OF SENSOR NETWORKS

One possible low cost solution for implementation of sensor gateway in wireless sensor networks is the employment of open source hardware platform Arduino and integrated Bluetooth module. In realization of the experimental sensor network the Arduino-compatible platform Olimexino 328 is used [5]. It consists of a 8 bites microcontroller ATmega 328 with built-in temperature sensor, 8 analog inputs, 14 programmable digital inputs (or outputs) and USB interface for connecting with a PC. The digital inputs/outputs could be programmed to realize 1-wire, I^2C and UART digital interfaces. The USB interface is used for programming the microcontroller. In addition, it

G. Petrova is with the Department of Electronics, Faculty of Electronics and Automation, Technical University of Sofia, Plovdiv branch, 25 Tzanko Djustabanov str., 4000 Plovdiv, Bulgaria, e-mail: gip@tu-plovdiv.bg

G. Spasov is with the Department of Computer systems and technologies, Faculty of Electronics and Automation, Technical University of Sofia, Plovdiv branch, 25 Tzanko Djustabanov str., 4000 Plovdiv, Bulgaria, e-mail: gvs@tu-plovdiv.bg

G. Pazhev is with the Department of Computer systems and technologies, Faculty of Electronics and Automation, Technical University of Sofia, Plovdiv branch, 25 Tzanko Djustabanov str., 4000 Plovdiv, Bulgaria, e-mail: georgpajev@gmail.com

works as a virtual RS232 interface, so it could be used for data exchange with a PC, which does not support this physical interface.

The initial realization of experimental sensor networks is shown on Figure 1. They are based on three different physical interfaces - I^2C and 1-wire for indoors temperature measurement and UART for energy consumption measurement.

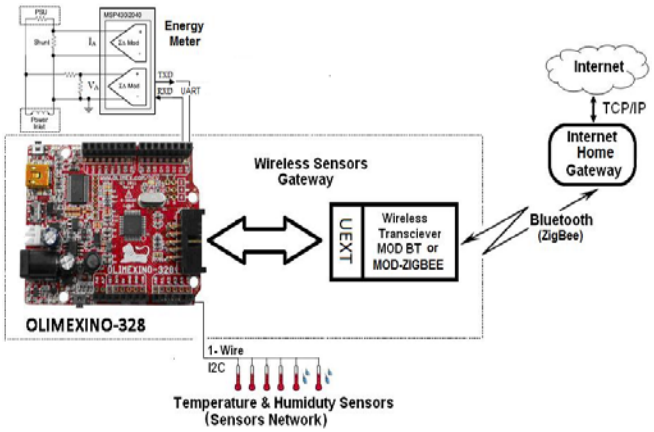

Fig. 1. Initial realizations of experimental sensor networks

For measurement of the temperature TCN75A from Microchip and DS18B20 from MAXIM sensors are used, while for energy metering the Microchip MCP39F501 Power Monitor PICtail module is connected to Olimexino 328 microcontroller. The wireless sensor gateway is realized by a Bluetooth transceiver (MOD-BT) connected to the UEXT interface of Olimexino 328. It is connected to the Internet gateway (gateway to the Internet-based network) realized with an industrial PC [6]. The applications for home monitoring and control of home environment devices are running on the Internet gateway.

III. Realization of Home Automation Network

The realization of the home automation network is based on the developed wireless sensor networks but instead of using industrial PC, the Internet gateway is realized with the open hardware platform OlinuXino – A13 WiFi, which is a low cost, very compact single board Linux computer with embedded WiFi [7]. Its features 32 bites CPU ARM9-Cortex-A8, working on 1GHz clock and very low power consumption, embedded WLAN WiFi, and easy integration of Bluetooth and Zigbee interfaces through UEXT connector and LAN ETHERNET through USB, makes it very good choice for implementation as Internet gateway. The power supply for OlinuXino – A13 WiFi is optional - with power supply adapter or autonomous with rechargeable Li-Po battery, which assures better sustainability toward power supply disturbances at low cost. The platform is working with LINUX-based Operating system Android 4.0. Although both Linux platforms Ubuntu and Android 4.0 are recommended by the producer of OlinuXino – A13 WiFi [7], Android 4.0 has been preferred due to the option to use Android SDK Tools for future Cloud applications based on Google Cloud Platforms.

The implementation of a home automation network with OlinuXino - A13 WiFi as Internet Gateway and one wireless sensor gateway is presented on Figure 2. The proposed solution allows easy integration of up to seven wireless gateways through Bluetooth interface to one Internet gateway, thus improving the scalability of the system. The different types of sensors, for example to measure humidity, to detect fire or gas leakage, additional alarm detectors for indoors presence of a human or an animal, and for notification of the presence of unwanted objects could be easily connected to the existing solution. This is an essential advantage of such an open platform.

Through WiFi WLAN a Smart phone or PDA device is connected to the Internet gateway. The Smart phone is used for local monitoring of the system parameters, the initialization of sensors' and alarms' modes, as well for the integration of new sensor types to the home automation network.

The connection of the Internet gateway to the Smart grid of energy control centers, security providers and central heating systems from the third layer of the hierarchical structure is realized through Internet by means of LAN ETHERNET or WiFi.

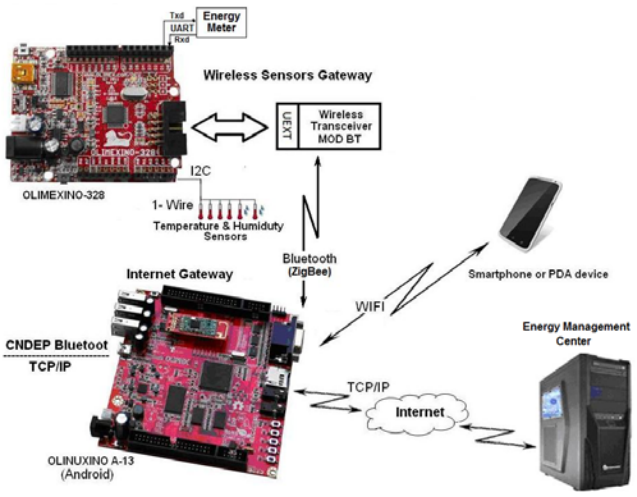

Fig. 2. The implementation of a home automation network with OlinuXino - A13 WiFi as Internet Gateway and wireless sensors gateway.

Although the Internet gateway could be realized using Olimexino 328 with added Ethernet and WiFi shields, and Bluetooth module (MOD-BT), the realization with OlinuXino – A13 WiFi has been preferred due to the easier integration to the third layer. With Olimexino 328 the integration to the third layer is possible by means of simple Web server [8], which makes more difficult the employment of SOA or RESTful web service technology. The prices for both platforms are comparable but the additional advantage of OlinuXino – A13 WiFi working with Android OS concerning the possibility to use multi-treat applications is also taken into consideration.

IV. Description of CNDEP Protocol

The communication protocol CNDEP is initially designed for data exchange in Internet-based distributed embedded systems [9]. There are three available versions

of this protocol at the moment: CNDEP – TCP/IP, CNDEP – 485 and CNDEP - Bluetooth. The basic version is CNDEP – TCP/IP. The other two versions are implemented in particular applications as sensor networks based on interface RS-485 or physical layer RS-Bluetooth [6]. Since CNDEP is intended for use in networks of controllers connected to a LAN (Ethernet, WiFi) and applications based on the TCP/IP protocol stack, the utilization of Bluetooth interface requires several changes in the basic protocol. The CNDEP-Bluetooth protocol version is adapted for applications where the data have to be exchanged between wireless sensor gateways and the Internet gateway. First, the Internet gateway sets the initial configuration parameters (default settings) of the sensors in the sensor networks. Then, in the monitoring mode the exchange of data generated in the sensor nodes is initiated by the sensor gateway (Olimexino-328). When it is necessary the default settings of sensor parameters could be changed by the Internet gateway submitting commands across the network. The communication protocol CNDEP is adapted for implementation in the home automation network and several extensions are added. For example, there are one extension for configuration of new sensors connected to the sensor gateway and another extension for self-identification from the client part.

The message formats are presented in Figure 3. There are two types of packets: packet for sending commands (request) and packet for sending a reply (response). Both begin with ASCII character STX (Start of Text) and end with character ETX (End of Text).

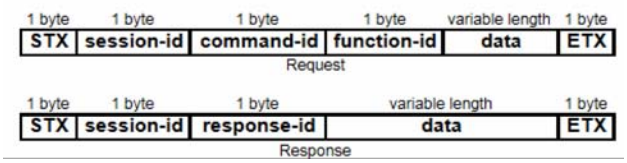

Fig. 3. Message formats

After the start symbol a field session-id follows, which is used to identify a session in case of re-transmission. The field command-id is used to represent the command to the corresponding sensor note. There are 5 types of commands used: TEST, GET, SET, CONFIG and SSID.

- TEST command is used for testing the connection between the Internet gateway and the corresponding sensor nodes through the sensor gateway;
- GET command is used when the Internet gateway requests data through the sensor gateway from a particular sensor node;
- SET command is used for sending the settings of parameters for sensors and actuator nodes;
- CONFIG command is used for sending meta-data which describe new sensors attached to the sensor networks, and definitions of their corresponding functions for execution of the commands SET and GET;
- SSID command is used for setting up the session identifier from the client-side.

In the function-id field the type of parameter to be measured is specified, which determines the corresponding sensors for data extraction. Also some additional options concerning the measurement procedure could be set. In the packets for sending commands (request) the data field contains the arguments of the commands, while in the packets for sending reply (response) this field contains the data extracted from the sensors. In the response-id field the type of response, sent from the sensor gateway is determined. The possible types of responses are: error, OK and data transfer.

The CNDEP is asymmetric protocol from the type client-server. The server scenario in the home automation network is realized from the sensor gateway in the request/response interactions. The server side decodes the received request from the client (Internet gateway in this case), performs the command, generates and sends the corresponding response. The working state diagram on the server side is presented on Figure 4. A new state (Save) in the execution of the commands CONFIG and SSID is added. This was done with the aim to add the security policy with interaction type 'Resurrecting Duckling'[10], which provides additional mechnisms for defence against external intrusion through wiress interfaces in the home automation network.

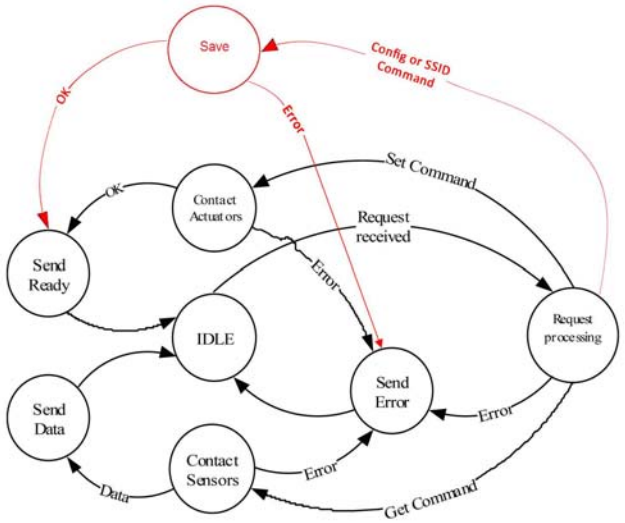

Fig. 4. Working state diagram on the server side

The sensor gateways are configured by the end user of the home automation network depending on the sensors attached to them. The Internet gateway sends configuration message (message with CONFIG command) to the corresponding sensor gateway to set the description of SET and GET functions. The function description consists of basic microinstructions that are supported by each gateway - commands for reading and sending data through interfaces 1-wire, I^2C, UART; commands for reading data from analog sensors and commands for control of the actuators via GPIO (General Purpose Input / Output) interface.

The functional diagram of the application for interaction of the Internet gateway (OlinuXino - A13 WiFi platform) with the sensor gateways is presented on Figure 5. The application comprises three processes (activities), one

service, one integrated database and two broadcast receivers. The 'Configure Gateways' activity is used for adding the definitions of the functions to the corresponding sensor gateway. These definitions are stored in the database and they are sent as CONFIG messages to the sensor gateway. The 'Configure Internet Gateway' activity is used for constructing and adding rules for data extraction (rules type GET) and rules for setting up the behavior of the sensor gateway (rules type SET). The data extracting rules are unconditional. Command GET is sent to set the function to be performed. The rules for setting the behavior are executed based on the user pre-defined condition. All these rules are also stored in the database. The 'View All Gateways' activity is used to display the status of each sensor gateway. The values obtained from the sensors in result of performance the assigned GET rules are visualized.

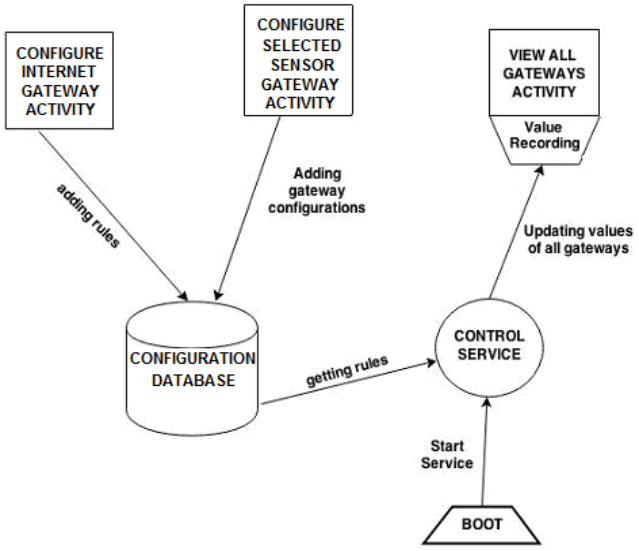

Fig. 5. Functional diagram of the application for OlinuXino A13.

The Control service is the core of this Android application. First, it retrieves the user defined GET and SET rules from the database. Then performs these rules and updates the information for the status of each sensor gateway, which is displayed on the 'View All Gateways' activity. The 'Configuration Database' allows better and easier configuration and re-configuration of the home automation network according to the user requirements.

V. Conclusion and Future Work

A low cost realization of a home automation network with two gateways based on open source hardware is presented in this paper. The communication between the sensor gateways and the Internet gateway is realized through Bluetooth wireless interface. The communication within the network is based on CNDEP protocol initially designed for data exchange in distributed embedded systems. A new adapted version of the CNDEP- Bluetooth protocol with several extensions is described. The advantages of the proposed solution are low cost, additional functionality and scalability of the system together with better sustainability toward power supply disturbances.

Employing this platform specific algorithms for energy efficiency of smart homes could be investigated experimentally. For profesional realization headboards as AVR-T-3244 and A13-SOM-512 could be used. Moreover, asymmetric encryption in the CNDEP protocol could be added and possibility for transfer of public keys using the Near Field Communication interfaces. While, the private keys for each gateway can be stored on their internal read-only memories.

The future research is directed toward adaptation of the home automation system to the Internet of Things (IoT) technology and integration to the Smart Grid and Smart Sity systems.

Acknowledgments

The paper preparation is supported by Project ДФНИ E02/12 "Investigation of methods and tools for application of cloud technologies in the measurement and control in the power system".

References

[1] Ameena Saad Al-Sumaiti, Mohammed Hassan Ahmed, and Magdy M. A. Salama, *Smart Home Activities: A Literature Review*, Taylor & Francis Group, Electric Power Components and Systems, 42(3–4), 2014, ISSN: 1532-5008, pp. 294–305.

[2] Nazmiye Balta-Ozkana, Benjamin Boteler, Oscar Amerighi, *European smart home market development: Public views on technical and economic aspects across the United Kingdom, Germany and Italy*, Energy Research & Social Science No 3, 2014, Elsevier, ISSN: 2214-6296, pp. 65-77.

[3] Matthias Kovatsch, Markus Weiss, Dominique Guinard, *Embedding internet technology for home automation*, IEEE Conference on Emerging Technologies and Factory Automation (ETFA), 2010, ISBN: 978-1-4244-6848-5, pp. 1-8.

[4] Kastner W., Neugschwandtner G., Soucek St., Newman H., *Communication Systems for Building Automation and Control*, Proceedings of the IEEE, 2005, vol. 93, no. 6, ISSN: 0018-9219, pp. 1178–1203.

[5] http://www.olimex.com, *OLIMEXINO – 328 development board users manual*, Olimex Ltd.

[6] Пъжев Г., Спасов Г., *Приложение на протокол CNDEP-BLUETOOTH при мрежа от сензори за измерване на температура*, Национална младежка школа и борса за научни идеи в областта на информационните и комуникационните технологии, 2013, ISSN: 1314-9024, pp. 41-45.

[7] http://www.olimex.com, *OLINUXINO - A13, development board users manual,* Olimex Ltd.

[8] Kim Baraka, Marc Ghobril, Sami Malek, Rouwaida Kanj, Ayman Kayssi, *Low cost Arduino/Android-based Energy-Efficient Home Automation System with Smart Task Scheduling*, 2013 Fifth International Conference on Computational Intelligence, Communication Systems and Networks, ISBN: 978-0-7695-5042-8, pp. 296-301.

[9] Kakanakov N., Stankov I., Shopov M., Spasov G., *Controller Network Data Extracting Protocol – design and implementation*, Proceedings of the CompSysTech, 2006, ISBN: 978-954-9641-46-2, pp. III-A.14-1-6.

[10] Frank Stajano, *The Resurrecting Duckling - what next*, Security Protocols, 8th International Workshop, LNCS 2133, Springer 2000, pp. 204–214.