Internet Controlled Embedded System for Intelligent Sensors and Actuators operation

Ondrej Perešíni, Tibor Krajčovič
Institute of Computer Systems and Networks
Faculty of Informatics and Information Technologies, Slovak University of Technology in Bratislava
Bratislava, Slovakia
ondrej.peresini@stuba.sk, tibor.krajcovic@stuba.sk

Abstract – **Devices compliant with Internet of Things concept are currently getting increased interest amongst users and numerous manufacturers. Our idea is to introduce intelligent household control system respecting this trend. Primary focus of this work is to propose a new solution of intelligent house actuators realization, which is less expensive, more robust and more secure against intrusion. The hearth of the system consists of the intelligent modules which are modular, autonomous, decentralized, cheap and easily extensible with support for encrypted network communication. The proposed solution is opened and therefore ready for the future improvements and application in the field of the Internet of Things.**

Keywords - Internet of Things; decentralized network; embedded hardware; intelligent household; actuators

I. INTRODUCTION

The worldwide industry is currently experiencing intelligent smart homes boom. Besides the recently built modern houses new projects arise to modernize existing and older buildings. This creates a demanding potential for new smart homes and increases the demands for advanced features that are easier to control and more suitable for home environment.

Currently there is no exact definition of intelligent smart home capabilities, however there are many common aspects shared between various implementations. Some smart homes are focused on HVAC (*heating, ventilating, and air conditioning*) thermal control and others may control household lighting. The most common problem with these models are lack of interoperability and compatibility amongst them. Our approach is focused on proposal and implementation of new communication protocol and smart home model which will allow flawless interoperability between various types of actuators and sensors. This ecosystem should be a decent baseline for future improvements and application in field of the *Internet of Things*.

II. LIMITATIONS OF CURRENT APPROACHES

During analysis stage we have analyzed many academic approaches as well as some commercially available systems. As a result we were not able to discover system which will be sufficiently modular, safe and will meet all system specifications. However we have found two interesting yet differently specified academic publications related to our topic by *P. Jombík* [1] and *S. Kišák* [2].

Numerous examined commercially available systems for intelligent household control (*Sensaphone FGD-W600* [3]; *LockState Connect LS-90i* [4] and *Ecobee EB-EMS-02* [5]) are linked with several disadvantages:

- Extremely high price – which is a result of this lucrative market and limited offer.
- Proprietary and closed implementations – as producers tend to guard their know-how and the majority of systems are closed and do not allow modification or extension.
- Complex configuration and installation – a common problem of commercially available systems that require professionally trained and expensive assembling staff.
- Low level of security – where most of the equipment is protected only by access password, but does not have the additional security validations that may avoid system hacking.
- Various functional limitations – devices often do not provide any type of software or hardware update and are locked to existing functionality without ability for extension.
- Centralized control – in case of one module failure the whole system is completely disabled and users are forced to perform expensive repairs or change the entire system.

A. Existing standards

Since most of the intelligent household systems are proprietary and closed, it is virtually impossible to operate devices from different vendors. Beside previously mentioned aspects the main problem lies in unavailability of open standard that would be sufficiently widespread and complex to cover whole field of intelligent household control. However there are two standards HVAC and DLNA (*Digital Living Network Alliance*) which can provide some of the intelligent household functionality, but both of them are dedicated to separate function fields and even combining them will not result in sufficient complexity that would not limit different hardware components. As a resolution of this crisis we have

ISBN 978-80-261-0386-8,

designed and implemented our own standard that will be open source and will meet all established specifications for functionality.

III. SYSTEM SPECIFICATIONS

The main objective of the project was to design and implement a system of intelligent household management which will consist of several modules performing specified tasks. The system is composed of a central unit and numerous sensor modules, which may be combined with actuators. The central unit serves as a register of external modules and provides an intuitive user interface for easy configuration of the whole system. The proposed system consists of modules that are:

- *Modular* – which allows user to change or expand the functionality of modules.
- *Autonomous* – and capable of self-determining action.
- *Decentralized* – system allows dynamic addition or removal of different modules without the need for a central unit.
- *Standardized* – communication protocol between modules should be standardized and thus allowing future design and implementation of additional modules with different or extended functionality.
- *Cheap* – design goal is to minimize implementation cost mainly through usage of standardized components and existing communication network.

A. Network communication

One of the main pillars of the project is to incorporate already existing network infrastructure, which brings many advantages but also some disadvantages, whose impact can be minimized by appropriate system design. The modules are connecting to other elements through the standardized Ethernet (*IEEE 802.3*) or WiFi (*IEEE 802.11*) network. As embedded systems provide limited hardware resources to fully support extensive TCP (*Transmission Control Protocol*) we have decided to design and implement our own communication protocol based on a simple UDP (*User Datagram Protocol*) which we have expanded by the number of elements known from TCP. The result is a fast and reliable communication protocol with minimal memory requirements and ability to de-duplicate, retransmit and recover from errors.

In the main design we have specified various types of communication messages that are divided into Broadcast and Unicast communication. Whilst the *Hello* message is broadcasted through the whole network segment, all other messages including *Identify*; *Request*; *Post*; *Configure* and *Acknowledgment* are directly exchanged between two nodes. Periodically broadcasted message *Hello* builds up communication between the central unit and all external modules. Upon receiving the *Hello* packet follows the unicast message *Identify* containing all information about module identification and configuration. Afterwards all previously stored sensor readings and unsent data are transmitted via *Post* messages. Central unit could solicit readings update or revoke data transmission through *Request* message. Configuration changes are committed by central unit which sends *Configuration* messages to desired modules. All messages need to be confirmed via *Acknowledgment* message or retransmitted due to packet loss or corruption.

All messages consist of a header, encrypted message body and completion segment. In order to ensure correct messages order all packets include fields with sequence number, checksum and time stamp (Tab. 1). Control logic is using these fields to ensure message integrity as in the case of TCP.

B. Security measures

Security system is divided into several layers that provide advanced security against intrusion. The transport layer performs drop of duplicated, replicated and delayed messages that could be fabricated by attackers. To ensure confidentiality symmetric XTEA encryption is used together with dynamic password generation which makes it virtually impossible to perform brute-force attack. XTEA uses bock size of 64 bits (8 B) and therefore all messages must be stuffed with padding data of size (8x–2 B) to align encrypted data.

The application layer of user interface provides access from Intranet or Internet and therefore advanced security features must be provided. Limited resources of embedded systems do not allow usage of asymmetric cryptography well known from HTTPS (*Secure Hypertext Transfer Protocol*) and therefore we used standard HTTP interface with user authentication hidden in BASE64 encoding. This approach does not provide sufficient level of security and thus we incorporated 2-stage GSM (*Global System for Mobile Communications*) authentication. One-time access codes are transferred via SMS messages. Successful security breach may be achieved only through compromising both communication channels.

The operation layer is secured through Watchdog timer which is able to restore system upon unpredictable operation which may lead to system hangout and failure.

IV. SOLUTION PROPOSAL

For implementation of a central unit and external modules we have used *Arduino* platform which provides wide developer base and many open source projects.

TABLE I. COMMUNICATION MESSAGES FORMAT

Field	Description	Size (B)	Encrypted
Identification Header	Message type	1	No
	Sequence number	4	
Data body	Data size	1	Yes
	Padding	8x – 2	
	Checksum	1	
Completion	Time stamp	4	No

Arduino platform provides various development kits suitable for the prototype realization. Whilst external modules do not need fast processor and should be power efficient we decided to choose popular *Arduino UNO* kit with *Atmel ATmega 328* [6] processor together with *Ethernet* [7] or *Wireless* shield [8]. Central unit needs more processing power as it collects sensors data and provides user interface and therefore we have chosen *Arduino Mega 2560* based on Atmel *ATmega 2560* [9] processor.

In the design we have used three types of external modules as exemplary demonstration of project capabilities (Fig. 1). Each of the module collects data about the environment through selected sensor and interferes with the surrounding environment via dedicated actuator. For monitoring of environment we have used light sensor (*PERKIN ELMER FW300* [10]), digital temperature sensor (*MAXIM DS18B20* [11]) and RFID card reader (*ID Innovations ID-12* [12]) which will be mounted inside front door and grant access to authorized users only.

Actuators can directly regulate environmental characteristics that are linked with chosen sensors. The lighting control is based on a LED (*Light-emitting diode*) with direct PWM (*Pulse-width modulation*) regulation, the door lock is linked with electronic release mechanism connected to the opening relay and room temperature is regulated via stepper motor, which may control heating valves in a different areas.

V. Implementation

A. Hardware realization

All modules are based on the development platform of Arduino which allows to use stackable headers shields to further extend functionality. Every module has 2 shields stacked on the top of the mainboard. Whilst the first shield provides network connectivity (Ethernet or WiFi) the second shield created by us attaches specified sensors and actuators. GSM module with external communication antenna is located on the top of central unit. All WiFi adapters have integrated antennas which are sufficient for our use case. Two of the modules are connected through Ethernet and powered via POE (*Power over Ethernet*). Remaining modules with wireless connectivity must rely on batteries or power adapters.

B. Software realization

The most important parts of the proposed system include sensor value readings and associated actuators control. In case of power failure all measured values are safely stored into built-in EEPROM memory or SD Card storage. Network communication layer performs not only sending and receiving packets, but also packets analysis, processing and data encryption. In addition to the proposed protocol we have used standardized NTP (*Network Time Protocol*) and DHCP (*Dynamic Host Configuration Protocol*) protocols as well.

The central unit is in comparison to the external modules quite complex due to additional processing of GSM shield [13] communication, providing user interface and data handling. Data inputs form all modules including their settings, sensors readings and error messages are stored at the SD card. The central unit also provides a web-based user interface through HTTP protocol. This interface enables interoperability across a wide variety of different devices.

In the software part of the implementation we had modified and adapted some of the existing libraries to meet our requirements: *Ethernet* communication library, *WiFly interface, SoftwareSerial*, *MemoryFree*, *WebServer* and *GSMshield*. Our specifically implemented software parts contain:

- Proposed network protocol implementation.
- XTEA encryption library to enhance system security via symmetric encryption.
- Different sensors readings interpretation via Serial, OneWire or Analog interfaces.
- Several methods of actuator control via PWM, Relay switching or Stepper motor control.
- EEPROM data structures and operations.
- SD Card functions allowing sensor data retention and their graphic representation.
- GSM communication to send user SMS messages with One-Time-Passwords.
- Unique user interface – compatible with HTTP protocol accessible via various devices.
- WOL (*Wake on LAN*) and Watchdog reset.

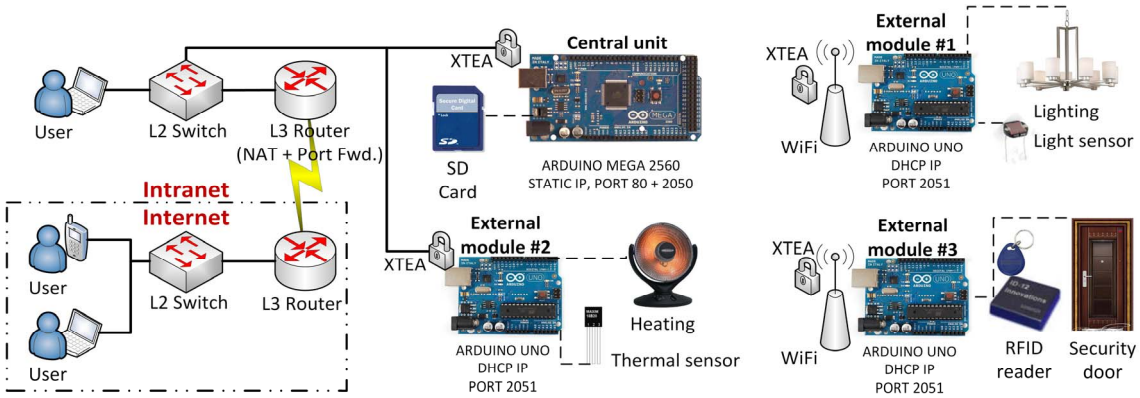

Figure 1. Block diagram of the implemented solution.

C. Implementation challenges

During implementation process we have encountered a number of problems, which were mainly based on various embedded hardware limitations. The biggest problem was the lack of RAM, where we were forced to optimize our code and libraries several times to fit the whole functionality into the available memory of capacity only about 1800 Bytes. RAM size would not allow us to utilize graphical user interface and therefore we outsourced graph rendering to the online graphical framework known as *Xively*. Perhaps the most problematic area was network communication implementation, which is prone to flooding and overload of maximum active TCP sessions. We had to carefully tune whole network communication.

Meanwhile we discovered the strange behavior of WiFly module that does not fully comply with the specifications [8] and we had to modify the logic of network communication establishment. Another minor issue was the lack of control mechanism handling expiration of DHCP IP address lease and therefore we have implemented our own DHCP mechanism. In addition, digital temperature sensor has long processing delay of about 1 second, which caused data retransmission as opposite node presumed loss of connection. We have solved this problem by automatic sensor readings buffering which may slightly increase energy consumption but provides much faster response times.

VI. System verification

We had established thoughtful system verification of the final product prototype not only in terms of the available functionality, but also for long-term deployment in real homes. Test cases were divided into positive and negative verifications. Positive test cases were designed to verify defined system specifications and overall product capabilities. Network topology represented standard home local network where all external modules had dynamic IP addresses and Central unit was assigned with static IP address due to the static port mappings used for system accessing from the outside internet (Fig. 1).

Separate parts of test cases were dedicated to XTEA packet encryption and accuracy of data storage on both SD Card and embedded EEPROM memory. We have also verified proper functionality of all hardware sensors, actuators and developed Shields. Negative verification testing consisted of many attempts to disrupt the system in any way. We have simulated network attacks by sending some invalid and fabricated packets containing invalid requests to gain access to sensors or actuators. This attempt was unsuccessful thanks to XTEA encryption, however in case of rapid packet generation we could experience DOS (*Denial of service*) failure. This is a common problem caused by limited system resources of embedded devices and can be avoided with a proper Firewall. Another test part simulated central unit failure and random disconnection of the Internet or SD Card connectivity. The result of the test proved that autonomous external modules can automatically disconnect from Central unit and start to record measured data locally to EEPROM memory. During verification phase have we successfully discovered and fixed all errors and proposed system is sufficiently robust and suitable for home deployment.

VII. Conclusions and further work

During final product development we have analyzed, designed and implemented fully functional household management system. This system has in comparison to commercial solutions several benefits including modularity, autonomy and decentralization of external modules. The advantage is in the simple scalability of all modules and the system is therefore practically unlimited in this direction. During system design phase we have focused on minimizing of cost and energy consumption. In the design we have also paid attention to adequate security of the whole system against unwanted intrusion what is not a strong case of commercial solutions. The proposed system is currently in the prototype stage but can be immediately deployed in the home environment. The modularity of the system allows for future expansion of hardware capabilities or software control. Provided sensors and actuators provides good examples to introduce basic household functionality. In the future this system can be expanded to further improve user experience via applications primarily directed to various mobile phone platforms.

Acknowledgment

This work was partially supported by the Grant no. 1/0616/14 of the Slovak VEGA Grant Agency.

References

[1] P. Jombík, “Embedded system for remote monitoring and management of the household.” FIIT STU, Bratislava, 2011.

[2] S. Kišák, “Experimental embedded system for remote monitoring and management.” FIIT STU, Bratislava, 2011.

[3] Sensaphone, Web600 Web-Based Monitoring System. Online at: http://www.sensaphone.com/sensaphone_web600.php

[4] Lockstate, LS-90i Internet Thermostat. Online at: http://www.lockstateconnect.com/ProductDetails.asp?ProductCode=LS-90i

[5] Ecobee, The ecobee Smart Thermostat. Online at: http://www.ecobee.com

[6] Atmel, “ATmega 328 DATASHEET.” Online at: http://www.atmel.com/Images/doc8161.pdf

[7] WIZnet, “W5100 DATASHEET.” Online at: http://www.wiznet.co.kr/UpLoad_Files/ReferenceFiles/W5100_Datasheet_v1.2.2.pdf

[8] Roving Networks, “WIFLY GSX DATASHEET.” Online at: http://www.sparkfun.com/datasheets/Wireless/WiFi/WiFlyGSX-um2.pdf

[9] Atmel, “ATmega 2560 DATASHEET”. Online at: http://www.atmel.com/images/doc2549.pdf

[10] SOS, Fotorezistor PERKIN ELMER FW300. Online at: www.sos.sk/?str=371&artnum=28919&name=perkin-elmer-fw300-95503513

[11] Maxim, “Digital Thermometer DS18B20 DATASHEET”. Online at: http://datasheets.maxim-ic.com/en/ds/DS18B20.pdf

[12] SparkFun, “ID series DATASHEET”. Online at: http://www.sparkfun.com/datasheets/Sensors/ID-12-Datasheet.pdf

[13] SIMCom: GSM/GPRS Module – SIM900. Online at: http://wm.sim.com/producten.aspx?id=