Ubiquitous Smart Grid Control Solution based on a Next Generation Network as Integration Platform

Robin Acker, Nicolas Buchmann, Thorsten Fugmann, Christopher Knöll, Maximilian Porzelt and Michael Massoth
Department of Computer Science
Hochschule Darmstadt University of Applied Sciences
Darmstadt, Germany
e-mail*: nextfactor@h-da.de, michael.massoth@h-da.de*

Abstract—**This paper describes the architecture of an ubiquitous control solution for smart grids, distributed process control nodes, home automation and wide-area measurement systems. The proposed architecture is based on a next generation network as control and integration platform. Every network entity, like sensors, actors or process control nodes, has a Session Initiation Protocol Uniform Resource Identifier and presence status. The real-time, two-way information and process control communication between the network entities on the one side, and the grid and process control network operators or facility manager and house owners on the other side, will be realized via the Session Initiation Protocol and Presence Service. The main achievement of this paper is a detailed system design with a description of the used components and a first prototype implementation.**

Keywords - KNX; Home Automation; Next Generation Network; Presence Service; SIP.

I. INTRODUCTION

The current mega trend leads to smart cities and a more intelligent way of energy management. Every part of those cities, such as traffic control or smart grids is connected with each other and can be controlled from central points. Smart grids are intelligent electricity networks where suppliers and consumers are connected via a digital bidirectional communication. As a part of smart cities, smart buildings (facilities or houses) play an important role in this intelligent city management. The facility manager or owner can remotely monitor and control his house or facility where-ever and whenever he or she likes. A Smart Home should enable interaction with its owner, including the ability to monitor the status and control of home appliances and devices remotely from anywhere in the world. Such devices may consists of alarm systems, keyless access control, smoke detectors, light, heat, water or other energy management systems, medical devices, and all types of sensors, e.g., room, door, window or security surveillance, monitoring and control, statistics and remote metering to every automated system and appliance in the home.

A. Requirements

Smart grids, distributed process control networks, home automation and wide-area measurement systems should be able to identify and respond to man-made or natural disruptions. Grid and process control network operators should be able to isolate affected areas and redirect electric power flows around the damaged facilities. Facility manager and house owners should be able to react on abnormal energy consumption.

One of the most important issues is smart state monitoring of the power grids, which is basis of control and management of smart grids and distributed process control networks in order to avoid or mitigate the system-wide disruptions like blackouts. A real-time, two-way information and process control communication is essential key.

B. Purpose and Relevance

The purpose of this paper is to sketch a new approach and draft of a mobile ubiquitous home and facility control solution based on the Session Initiation Protocol (SIP) and Presence Service, to realize a near-real-time push solution. The described draft uses the advantages of the IP Multimedia Subsystem (IMS) to remotely monitor and control Home Automation Systems via a mobile device using open source licensed software. The IMS is standardized next generation network architecture to deliver IP-based multimedia (voice, video, and data) services across fixed and mobile networks.

According to Infonetics Research, the worldwide IMS equipment vendor revenue has reached US$ 426 million in 2009. The IMS equipment market, including IMS core and IMS application servers, continues to grow strong and healthy to US$ 1.44 billion in 2014 [11]. This promising forecast shows the business opportunity and relevance of the proposed draft for ubiquitous home control service.

C. Structure of the Paper

Following this introduction, Section 2 describes related work and further interesting projects suitable for this concept. In Section 3 and 4, an overview of the general approach is given. The components of a possible system design are discussed in Section 5. Section 6 details the system design. A view over the possible security functions is given in Section 7. Section 8 concludes the paper and gives an outlook of future work.

II. RELATED WORK

Smart Home Control is, of course, not such a new topic. Many companies and institutions are working on solutions for energy efficient management for buildings. But there are only a few who try to build a complete concept with open standards. Most systems focus on the inside or outside system of the building only. This means that the goal is to build a solution either for the management of actors and sensors, or to develop a good communication solution for existing bus systems.

 ISBN: 978-1-61208-136-6

The new idea is to connect the technology of Next Generation Networks (NGN) with Smart Home Control. The next step is to use SIP, with all its benefits, as the main communication protocol and connect it with a bus system standard (like KNX [15]) for the sensors and actors. Some approaches to this topic already exist.

For example, Schulzrinne et al. described how ubiquitous computing could be integrated into home networks [12]. For his approach he prefers SIP. Another approach was done by an IETF Working Group. The idea is based on the assumption that in the future every building is equipped with a full featured IP network. Therefore, SIP will be used for home control [8].

Another approach was made by the HomeSip project team [7][13][14]. Its goal is to create a SIP-based Home Control System. The important parts of the system are the SIP proxy and the SIP sensor network gateways. The SIP proxy is the central part for communication. The sensor network gateways are embedded Linux systems which are used to control the sensor networks and connect them with the SIP proxy. So, SIP should be used for communication between the sensor networks, the SIP proxy and the mobile controlling devices, like mobile phones or smartphones. All information from and to the sensor networks are transported via SIP.

III. CONCEPT

The big advantage and unique selling point of the IMS is the Presence Service which enables the control and integration platform to accept, store and distribute presence information about SIP identities. With this feature every sensor and actor, connected to the KNX bus which is described in Subsection 5.C., gets its own address (i.e., SIP URI) to log on to the service. After the registration the device can set its own current status, like “deactivated” or “active”. The sent KNX telegram is mapped to a SIP request and sent to the Presence Server. Now the user can monitor and even change the current settings on his mobile device.

IV. OVERALL SYSTEM DESIGN

The advantages of Next Generation Networks are used to build a communication platform between mobile devices and an intelligent building with a Home Automation solution. As depicted in Figure 1, a so-called “Gateway” interconnects the NGN core network and the Smart Home.

With the used standards a full near-real-time push solution for Home Automations status messages should be realized.

To interconnect the two architectures a special gateway (Bridge) is needed. The gateway manages connections between the SIP-based NGN and the single appliances of the Home Automation System. One significant function of the IP Multimedia Subsystem is the Presence Server, throughout it is possible to represent different Home Automation appliances as “users” to the Presence Server. Each “user” can set its own current status. Thus it is possible to register a mobile device at the SIP network, and in this way at the Presence Server. Hence, the status information of the different Home Automation appliances (i.e., the users) can be viewed on a mobile device.

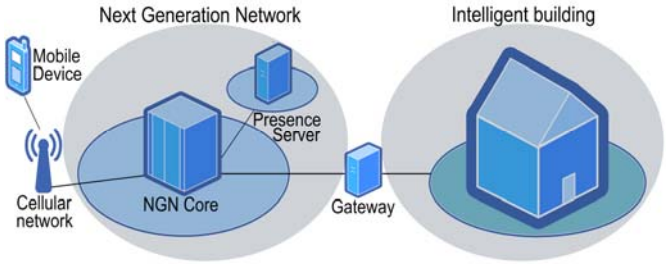

Figure 1: Overall system design (high level)

The gateway is responsible for updating the status information at the Presence Server. For example, any time a sensor in the Home Automation System changes its status, an update has to be sent by the gateway.

In order to control appliances in the Smart Home, such as switching lights on or off, a message must be sent by the mobile device to the specific Home Automation component. Therefore, a SIP message is generated and sent to the gateway, which forwards the information to the Home Automation System.

V. COMPONENTS

The following section introduces the components which are needed for the proposed concept.

A. Next Generation Network Core

To set up the NGN Core networks, we evaluated two Solutions to guarantee, that the Signaling Gateway is able to work with different NGN platforms.

The IP Multimedia Subsystem (IMS) [1] is a control architecture based on the standardized SIP [2] designed by the wireless standards body 3rd Generation Partnership Project (3GPP). It aims to standardize access to different networks. Therefore, all communication is based on the Internet Protocol (IP).

As lightweight solution to realize the NGN Core, a SIP Server with a Registrar and a Presence Service could be used. A common SIP server can also provide all the functionality which are needed to set up a SIP-based communication platform.

SIP is a signaling protocol for controlling multimedia communication. It can be used to create, modify, or terminate a multimedia session which can exist between two (unicast) or multiple parties (multicast).

With the Session Description Protocol (SDP) [3] properties of multimedia streams are described. SDP is used by SIP for negotiation regarding media codecs, transport protocols, and transport addresses.

SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE) [4] describes a presence and instant messaging protocol suite based on SIP.

Instant messaging enables users to communicate in near-real-time by text. For the Presence Service, a User Agent (UA) has to register at a Presence Server. The server acts as a Presence Agent. It stores the status of the UA. Other users

 ISBN: 978-1-61208-136-6

(subscribers) can subscribe to the UA's presence information. Every time when the UA changes its status, the subscribers will be notified near-real-time by the Presence Agent.

B. Sipdroid

Sipdroid 2.0 [5] is a VoIP client for the mobile operating system Android. The program is capable of establishing VoIP calls and sending messages over the network. The Protocol used is SIP.

C. KNX

KNX [9] is an open standard for Home Automation in intelligent buildings. In December 2003 KNX became European standard (CENELEC EN 50090, CEN EN 13321-1 and 13321-2). At the end of 2004 it was decided that the "European Norm" (EN 50090) should become international standard. In November 2006 the KNX protocol became ISO/IEC standard (ISO/IEC14543-3). The high interest in China led to adoption of the ISO/IEC 14543 standard to the Chinese norm (GB/Z 20965). Additionally for the US market there is the US standard (ANSI/ASHRAE 135).

KNX is the only open, internationally acknowledged standard for Home Automation and Intelligent Building Control.

The KNX standard is administrated by the KNX Association and supports the following communication media: Twisted pair wiring, powerline networking, radio, infrared and Ethernet (EIBnet/IP or KNXnet/IP).

KNX was invented in response to the following shortcomings: In conventional home installations, the control line and the powerline are not detachable. For example, normal lights are controlled by giving them energy or turning the energy off. Complex control mechanisms are hard to implement.

One of KNX's main features is that it detaches the control line from the power line. KNX is a dedicated control bus over which every connected device can exchange information with other devices. Devices of different manufacturers can communicate with each other if they fulfill the KNX standard and are certified by the KNX Association.

KNX devices are divided into "actors" and "sensors". An actor can be, for example, a device which can open or close a window or a device which controls the sunblind. Sensors can be polled for physical status information. For example a window's status can be open or closed, or a sensor for outdoor temperature can report back the temperature.

Many complex scenarios are possible. For example, with the help of an outdoor temperature sensor and sunlight intensity sensor a sunblind actor could control the sunblind depending on the data which the sensors deliver. Another scenario would be an actor for controlling an awning, combined with a wind strength sensor which would pull up the awning if the wind is to strong.

How the actors and sensors communicate with each other is specified in the KNX standard.

The KNX bus works with a 9.6 kbit/s transfer rate which is enough for more than 60,000 connected devices to the KNX bus.

Every device connected to the KNX network can be addressed with a unique 16-bit address, depicted in Figure 3. A KNX bus can theoretically have a maximum of 65,536 devices.

The topology of the KNX bus is based on lines. [10] In Figure 2 there is only one single Backbone Line. Up to 15 Main Lines can be connected to the Backbone Line, which are numbered from 1 to 15. The Backbone Line is Main Line 0. Main Lines are connected to the Backbone Line via Backbone Couplers. The Backbone Couplers belong to the Main Lines and not to the Backbone Line. A Backbone Coupler always has the Device-number 0.

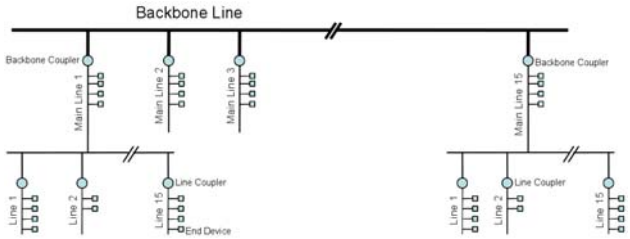

Figure 2: KNX bus topology

The hierarchical subordinates to the Main Lines are the lines. Every Main Line can have up to 15 lines which are numbered like the Main Lines from 1 to 15. A Main Line always has the line number 0. Just as Main Lines are connected with Backbone Couplers to the Backbone Line, Lines are connected to the Main Lines via Line Couplers.
A Line Coupler has the device number 0.

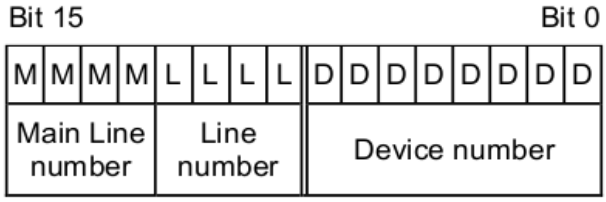

Figure 3: KNX address scheme

As depicted in Figure 3 the 16-bit Address is divided into 3 different fields: 4 Bits for addressing the Main Line, 4 Bits for addressing the appropriate line and 8 Bits for addressing the specific device. For example 3.8.10 addresses the 10th device connected to line number 8 at Main Line 3. Accordingly 0.0.4 addresses the 4th device directly connected to the Backbone Line. Consequently 4.0.10 addresses the 10th device connected to the 4th Main Line.

In conclusion, every line can have up to 255 devices, because device 0 is always the coupler. As seen in Figure 2, not only the lines are able to have connected devices, the Main Lines and the Backbone Line can respectively have up to 255 connected devices. By subtracting the reserved coupler addresses from the theoretical maximum of 65,536 devices, a maximum of 61,455 end devices are possible, which can be connected to a single KNX bus installation.

D. Calimero

Calimero 2.0 is a collection of Java APIs that form a high level framework for communication with a KNX/EIB

installation with the use of KNXnet/IP. The framework helps build high level applications which need to communicate with the KNX bus systems for remote access and control. It can receive/decode KNX messages and send/encode its own KNX messages.

E. Signaling Gateway

The signaling gateway, depicted in Figure 4, is the main part in this concept. This software service connects the KNX bus to the IMS network.

As already mentioned, with a KNXnet/IP device, KNX telegrams could be transferred to the IP network. The whole telegram is packed into the payload of an UDP packet and is sent over the network. Thus, one function of the signaling gateway is to receive these IP packets sent by the KNXnet/IP device. Further, the information contained in the telegram has to be extracted. This could consist of sensor values or other status messages of different Home Automation appliances.

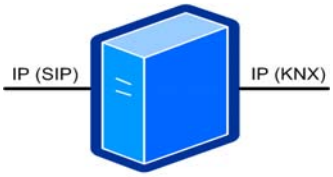

Figure 4: Connection interfaces of the signaling gateway

The KNXnet/IP device is also able to receive IP packets sent via the IMS from the IP network and forward the containing telegram to the KNX bus. Thus, in order to control appliances which are associated with the bus installation the signaling gateway has to have the ability to generate KNX telegrams.

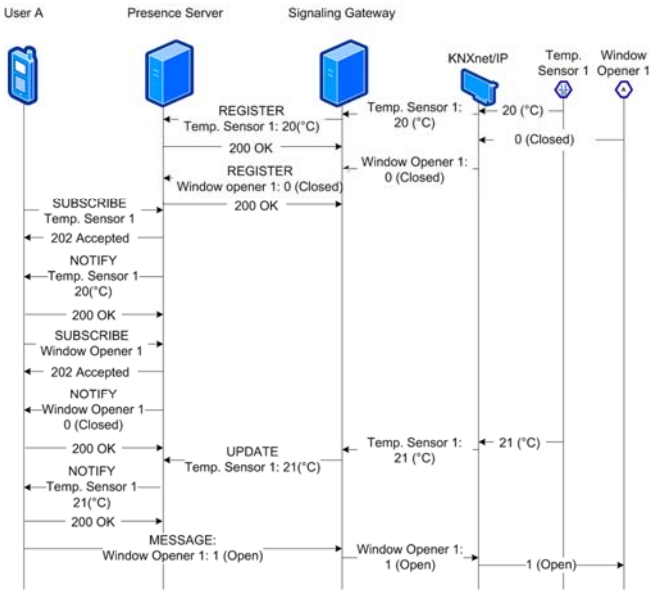

Figure 5: Message flow

With the open source Java Framework Calimero, it is possible to parse and generate KNX telegrams. This framework will be used in the signaling gateway to handle communication with the KNX bus.

Once the information of the telegram is filtered, the status change must be transmitted to the Presence Server located in the IMS. This brings out the second main function of the signaling gateway: The connection to the IMS. The signaling gateway registers every appliance of the KNX bus installation as a "user" at the Presence Server. To set the status of a user, a SIP message must be sent through the IMS network. This message flow is depicted in Figure 5. To view the current status of a part of the Home Automation System the mobile device just has to subscribe to the Presence Server.

If a user wants to control an appliance of the Home Automation System, a SIP message is sent from the mobile device to the signaling gateway. Further, the information in the SIP message body, depicted in Figure 6, must be mapped into a KNX telegram. This body is optional and can include e.g. SDP, SOAP, XML or ASCI.

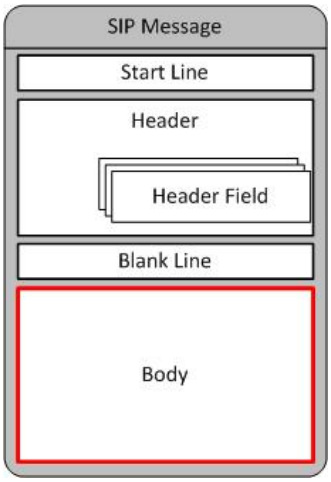

Figure 6: SIP message structure

VI. TECHNICAL FEASIBILITY

The intention of this concept is to use the advantages of the IP Multimedia Subsystem (IMS) and Presence Service in order to control Home Automation Systems, like the KNX bus installation, with a mobile device. KNX was chosen because it is the only open, internationally acknowledged standard for Home Automation and Intelligent Building Control.

A. Requirements

First of all, the IMS network infrastructure is needed, including the IMS core and application servers, as shown in Figure 7. The IMS core has the main functions of the IP Multimedia Subsystem like proxies and a user registration server. The application server in this case provides a Presence Service. The so called Presence Server handles a list of “users” and their own current statuses. Further, a mobile handset is needed that is capable of communicating with the IMS. To accomplish this, a special SIP User Agent

 ISBN: 978-1-61208-136-6

is required. In the next step a Home Automation System must be installed. In this concept the KNX automation system is used, also depicted in Figure 7. With this internationally standardized bus installation, it is possible to build up huge and powerful automation systems to control and monitor many different components in a building. With KNXnet/IP devices, status and control messages (telegrams) of the KNX bus can be transferred to IP networks. The most important part of this concept is the signaling gateway between the IMS network and the KNX bus installation

This software service provides the main functions for the communication between a mobile device and the Home Automation appliances.

B. *Overview*

The KNX bus installation implements the network connections and the addressing scheme for the different actors and sensors. Actors are appliances which can perform different actions, for example switching lights on or off. They provide a switching state and can receive telegrams from physical switches, sensors or software tools. Sensors are appliances which can detect different conditions like temperature or brightness. They are capable of sending telegrams to specific actors or software tools.

With the functions of the Presence Service of the IMS every sensor and actor of the KNX bus can be built up into a single “user” (entry in the Presence Service list). Therefore, each sensor or actor gets its own SIP address (URI) to register at the Presence Server. Every device which is registered to this service can set its own current status. Mainly this function is used to realize a service of messenger applications to set their own status in the contact list to “Not Available”, for example. In this concept we use the Presence Service to provide a list of all sensors and actors connected to the Home Automation System. Thus, every appliance sets its own status. For example the status of the temperature sensor may be 20.0°C.

Now it is possible for the user to get a list of his appliances displayed on his mobile device. For this purpose an SIP client is needed. Every SIP client also has a SIP URI to be identifiable in the IMS network. Making it possible to register to the Presence Server in order to view the list of appliances connected to the KNX bus installation.

With this system design a full push solution can be realized. The list of Home Automation appliances is updated automatically in real time. So there is no need to update the status of every single device manually.

This feature enables the ability to use the mobile device as a full alarm and critical state indicator. Thus, a push solution in mobile home control would give some whole new ways to use it.

The second step is to control different actors of the Home Automation System. To do this the user has to choose the specific actor and the operation which should be performed on the mobile device. The information is packed into a SIP message and sent through the IMS to the signaling gateway. The signaling gateway runs a user authentication to ensure the message was sent by an authorized mobile device. As shown in Figure 8, the information of the actor and the specific action of the SIP message is packed into a UDP packet and sent to the KNXnet/IP. Further, the KNXnet/IP device generates KNX telegram out of the UDP packet information and passes it to the bus installation. When the actor has performed the switching operation, the new status is sent to the Presence Server.

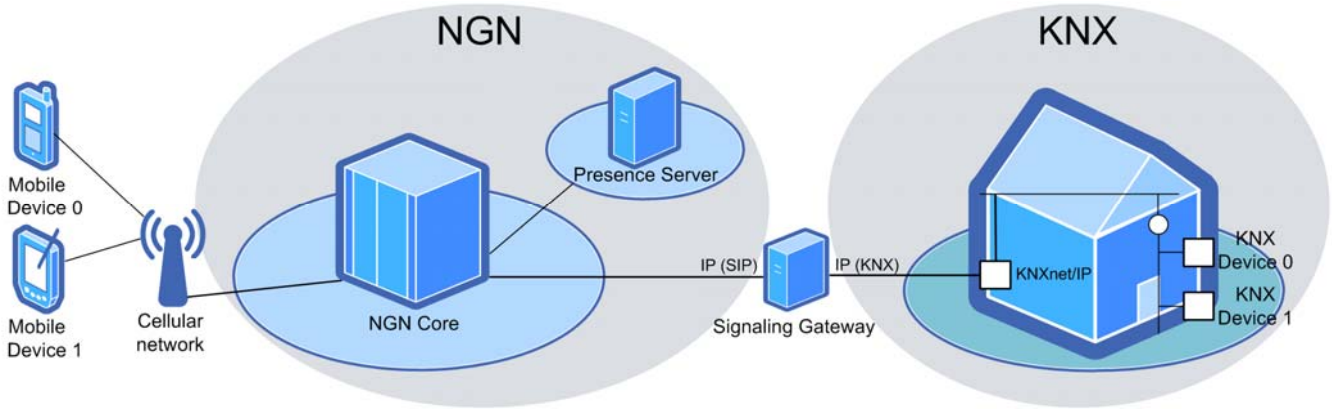

Figure 7: Detailed system design of the ubiquitous smart grid (home) control and integration platform prototype

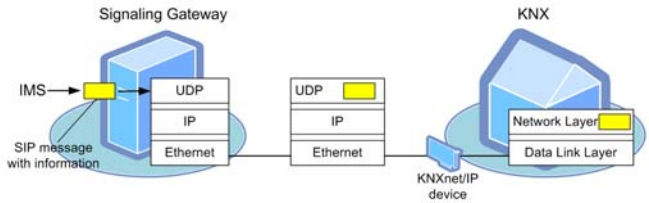

Figure 8: KNX telegram flow

VII. SECURITY

For a concept like this where communication over untrusted networks takes place, a strong security concept is important. To find a solution, the focus must set on two problems: The first is, of course, a secure connection

 ISBN: 978-1-61208-136-6

between the components. But on the other hand we have to think of the bandwidth usage and the computational workload. This is very important for mobile devices.

Therefore, one possible solution would be Multimedia Internet Keying (MIKEY) [6]. MIKEY is a key management solution for multimedia scenarios (e.g., SIP). The benefits are the simplicity, the low extra bandwidth consumption, the low computational workload and the time efficiency. So it is a well matching enhancement for the proposed concept to ensure an acceptable security level.

On the other hand KNX telegram security is also a must, due to local attacks on the KNX Bus. EIBsec is the common security extension for KNX [16]. The main goal of EIBsec is to protect the control network against local attacks. Services for providing a secure data transmission and authentication are included. The authentication mechanism allows verifying the identities of the involved communication partners including all sensors and actors. After proving the identities of the involved devices, the data are transmitted through a secure channel which guaranteed data confidentiality, integrity and freshness. The main advantage of EIBsec is that management services as well as the exchange of group messages can be secured. Another important feature of EIBsec is the compatibility to standard KNX protocol.

VIII. Actual Status of the Prototype

The actual prototype consists of a full addressed and configured KNX bus system with different kinds of sensors and actors like weather station, dimmers and digital/analog switches for lighting and power outlets. To communicate with the Signaling Gateway a KNX Net/IP device is also part of the KNX bus system. The Signaling Gateway is implemented as a converged application for a Glassfish Server. The application is based on the Sailfin (CAFE) extension and the Calimero 2.0 KNX-API, which provides functions to interact with the KNX bus. Sailfin offers the basis of a full featured Presence Service and SIP Call Control Functions. It is possible to connect the Signaling Gateway with an NGN core (e.g. Open IMS core) as an application server. With a standard SIP user agent for mobile devices (e.g. Sipdroid) it is possible to communicate with the Signaling Gateway to get status information of the KNX devices.

IX. Conclusion and Future Work

This paper presents a full concept of a ubiquitous home control solution, using the advantages of the IP Multimedia Subsystem, to realize a near-real-time push solution.

Our approach to the topic of Smart Home Automation is a different one. Instead of developing new commands for SIP or evolving a new kind of appliance, our approach only uses standards.

The achieved advantages are enormous. Many buildings all over the world already have a system to manage their buildings. Furthermore, an increasing amount of companies convert their network infrastructure to SIP (mostly because of VoIP). With our approach these two technologies can easily work together. The economical and ecological advantages are obvious: The system of the building can be managed remotely. A facility manager is able to manage more buildings, because he or she does not need to be at a single building most of the time. The ecological aspect of a smart home consists of enormous amounts of saved energy.

In future work, the first point is to create an own client for remote building control. It has to be platform independent, so it could be used on every mobile platform.

Next thing is to look at other bus-systems which are available. Maybe it is possible that the approach shown in this paper could also be used for other bus-systems.

Finally, new approaches to remote building control have to be checked. For example SIP extensions for communicating with networked appliances [8].

Acknowledgment

This work has been performed within the “Smart Home Control und Sensornetzwerke” project, which is partly funded by the “Zentrum für Forschung und Entwicklung” (ZFE) at the Hochschule Darmstadt - University of Applied Sciences, Darmstadt. Additionally the authors would like to acknowledge the support of the Albrecht JUNG GmbH & Co. KG by their contribution of KNX actors, sensors and other KNX home automation devices.

References

[1] J. Soininen (Ed.), “Transition scenarios for 3gpp networks,” IETF, RFC 3574, Aug. 2003.

[2] J. Rosenberg, H. Schulzrinne, G.Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley and E. Schooler, “SIP: session initiation protocol,” IETF, RFC 3261, Jun. 2002.

[3] M. Handley, V. Jacobson, and C. Perkins, “SDP: session description protocol,” IETF, RFC 4566, Jul. 2006.

[4] SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE). IETF Working Group.

[5] sipdroid, http://sipdroid.org 10.12.2010.

[6] J. Arkko, E. Carrara, F. Lindholm, M. Naslund, and K. Norrman, “MIKey: multimedia internet keying,” IETF, RFC 3830, Aug. 2004.

[7] HomeSIP Project, http://www.enseirb.fr/cosynux/HomeSIP/ 10.12.2010.

[8] S. Moyer, D. Marples, S. Tsang, J. Katz, P. Gurung, T. Cheng, A. Dutta, H. Schulzrinne, and Roychowdhury, “Framework draft for networked appliances using the session initiation protocol,” IETF, Internet Draft, expired Dec. 2001.

[9] KNX Association, “KNX logical topology faq,” 2005.

[10] KNX Association, “KNX system specifications,” 2009.

[11] Infonetics Research, “IMS equipment and subscribers report”, Mar. 2010.

[12] H. Schulzrinne, X. Wu, and S. Sidiroglou, and S. Berger, “Ubiquitous computing in home networks,” IEEE Communications Magazine, vol. 41, Nov. 2003, pp. 128-135, doi: 10.1109/MCOM.2003.1244933.

[13] B, Bertran, C. Consel, P. Kadionik, and B. Lamer, “A sip-based Home Automation platform: an experimental study,” Proc. 13th International Conference on Intelligence in Next Generation Networks, 2009 (ICIN 2009), IEEE Press, Oct. 2009, pp. 1-6, doi: 10.1109/ICIN.2009.5357075.

[14] C. Bertran, C. Consel, W. Jouve, H. Guan, and P. Kadionik, “SIP as a universal communication bus: a methodology and an experimental study,” Proc. 2010 IEEE International Conference on In Communications (ICC 10), IEEE Press, Jul. 2010, pp. 1-5, doi: 10.1109/ICC.2010.5502591.

[15] KNX Association , http://www.knx.org/knx-standard/standardisation/ 10.12.2011.

[16] Granzer, Kastner, Neugschwandtner “EIBsec: A Security Extension to KNX” KNX Scientific Conference 2006

 ISBN: 978-1-61208-136-6