Using VPN technology for networking intelligent building automation via the Internet

Tobias TEICH
Department of economics, University of Applied Sciences Zwickau
08012 Zwickau, Saxony, Germany

Matthias ZIMMERMANN
Department of economics, University of Applied Sciences Zwickau
08012 Zwickau, Saxony, Germany

Markus SCHRADER
Department of economics, University of Applied Sciences Zwickau
08012 Zwickau, Saxony, Germany

Susan FRANKE
Department of economics, University of Applied Sciences Zwickau
08012 Zwickau, Saxony, Germany

and

Franziska JAHN
Department of economics, University of Applied Sciences Zwickau
08012 Zwickau, Saxony, Germany

ABSTRACT

In modern times, when climate change is getting more and more drastic and issues like CO_2 emission and energy efficiency are becoming more and more important, it is necessary to find possible energy savings in every area. To achieve these possible savings also in the residential area it is essential to establish Intelligent Building Automation in residential buildings. Therefore, within the framework of a research project, two apartment buildings are equipped with the field bus KNX, which is used i.e. for control of heating, ventilation and lighting to realize an energy-efficient habitation .In the field of heating alone savings up to 50% of energy are to be expected [1]. For the intelligent control of the buildings a facility server is needed. But this will not only manage one apartment building but several simultaneously, and thus linking them together. To test this concept two KNX-Networks were connected with each other by two apartment buildings through the Internet using a virtual private network connection.

Keywords: Building Automation, Building Services, KNX, VPN, Facility Management.

1. INTRODUCTION

The development of intelligent building control permanently moves forward. Since few years, the KNX standard is supporting the IP transmission medium. Due to the combination of KNX and IP, there is a great potential of opportunities opening up in terms of intelligent building control and their users. Some of these new opportunities, such as the connection of intelligent building control in distributed networking buildings on the Internet or Intranet and so to create a single, coherent network that sets barely any limits. Thus, also applications such as an overall control and operation, or a central malfunction management are easy to realize.

2. PRINCIPLES OF BUILDING SERVICES ENGINEERING

Conventional Building Services

In conventional building services, each trade (i.e. lighting, heating, air conditioning, ventilation, etc.) is planned and running by an appropriate specialist. Basically the built-in actuators and sensors are connected via a point-to-point connection to the devices that are responsible for control and visualization. However, this creates a significant complexity on the planning, the cabling and its installation, as well as for troubleshooting during commissioning and maintenance. Furthermore, a large quantity of cables causes a correspondingly large fire load. If the various trades, for example be linked for a joint operation of all components, this is often not feasible or only with great effort. In conventional building services an increasing comfort and increased functionality result in complexity, high effort and enormous costs. However, the building bus engineering with KNX offers a solution to this problem [2].

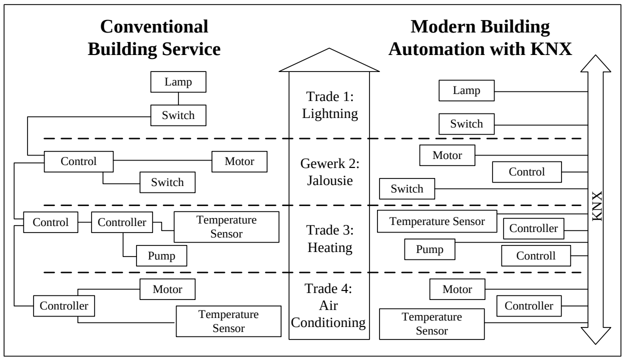

Figure 1: Comparison: conventional building service – modern building automation with KNX

Modern Building Automation with KNX

KNX is a standardized (EN 50090, ISO/IEC 14543), OSI-based network communications protocol for intelligent buildings. The field bus KNX was developed with the requirement that an application is ensured in all key installations of the Building services. Because of this aspect and the easily planning and integration of KNX components, the single trades can finely tuned work together. So that a communication between the components of the trades is guaranteed, there are devices with a KNX-interface conforming to standards of the Konnex Association for each trade. The use of the KNX bus provides, without any additional effort, a much higher functionality and comfort as well as a greater flexibility. KNX also affords networking and the use of different house engineering like energy meter, heating system, alarm equipment, etc. in the course of building automation in a smart home. In this context, the smart metering and smart grid concept must be mentioned. In each KNX device there is a microcontroller, so that a central station is not needed. By a corresponding parameterization, that is changeable at any time, the device is to be advised what it has to do. That is the reason why a KNX-System is very flexible and why it can be always adapted to new needs. Due to the use of KNX an automatic control of heating, ventilation, lighting and safety installations can be integrated, no matter it is whether a family home, apartment house or a functional or commercial building. Owing to KNX, estate can be used economically and comfortable.

A disadvantage of the KNX-Products, however, is that they are quite expensive compared to the conventional installation technology. In general, an investment is only worthwhile when several trades are to be linked together or there is a demand to flexibly and quickly adapt a system to future changes of use [2].

3. KNX OVER IP

KNX-IP is the fourth transmission medium of the KNX standard. The data can also be transmitted via powerline (KNX-PL), radio frequency (KNX-RF) and twisted pair wire (KNX-TP) [2]. The appropriate transmission protocol is called KNXnet/IP [3]. With the aid of the Internet protocol, the communication between the devices that are certificated for KNX-IP can be realized. That means that the KNX-protocol is packed into the Internet Protocol (Figure 2). The combination of KNX and IP also offers a great potential of new opportunities for communication enlargement in the building automation beyond the borders of the building and thus beyond the local KNX-System. In the future, distributed KNX-subnets, such as several buildings, can be connected via the Internet and therefore a coherent network can be created, whereby a central control and operation of the whole sub-networks can be realized. Furthermore, the low performance (9,600 Bit/s) of KNX is increasing because of the coupling of a powerful IP-Backbone [3].

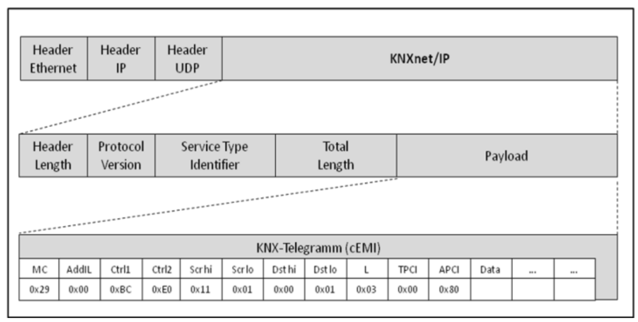

Figure 2: Telegram format KNXnet/IP

In the specification KNXnet/IP two types of communication are differentiated, on the one hand KNXnet/IP-Tunneling and on the other hand KNXnet/IP-Routing. KNXnet/IP-Tunneling defines how KNX-telegrams are exchanged via a point-to-point connection (unicast) by the IP-network. This alternative is used for programming and commissioning of the KNX-devices as well as for isolated solutions in the field of visualization. For the communication between the KNX-devices via Ethernet KNXnet/IP-Routing has to be attached. Thereby, KNX-Telegrams are exchanged in a 1:n relation (multicast). That means that a subscriber sends data to a group of participants.

4. IMPLEMENTATION

Two apartment buildings have been equipped with the field bus KNX as test objects. The KNX networks of the two apartment buildings will be linked via the Internet. The objective is to use a facility server which takes control of all functions of the building for both buildings. Therefore a facility server isn´t required for each building. Furthermore the cost of acquisition and maintenance will be reduced. Another advantage is that there is only one server needed to control the facility management. Perspective not only two multi-family house will be linked and controlled via a facility server but a whole network.

In networking of KNX systems the addressing of the devices should be aware. It must comply with rules of KNX topology and addressing. In a KNX network 65,536 end devices can be joined [4]. A KNX device in building A should not has the same physical address as a device in building B. Data exchange between the KNX devices and the facility server is realized by the protocol KNX IP in routing mode. It follows that between the networks are multicast connections. The problem for the data transmission using multicast packets over public network is that IP Multicast works only if the routers in the Net are multicast capable.

That means particular to support the protocols for coordinating the routing of IP packets for multicast groups, which is in the commercial Internet little or not at the case. As a solution to this problem, the authors propose the use of a virtual private network (VPN).

A virtual private network provides a private communications network over a shared public network infrastructure such as the Internet. There are basically three types of virtual private networks: Remote access VPN connection (end-to-site), Branch Office VPN connection (site-to-site) and Extranet VPN connection (end-to-end) [5]. For the integration of the two buildings only a site-to-site VPN connection is suitable because two physically separate networks are to be interconnected.

For installing a VPN special routers are needed, which support the VPN technology. Furthermore, these routers have to forward multicast packets as it is described above. The routers are used as a VPN gateway. Between the two VPN gateways a VPN tunnel is established on which the whole data traffic between the two apartment buildings is sent via the Internet [6]. Another advantage of using a VPN is the security compared to unauthorized access to the building systems.

5. CONCLUSION

This paper focused on a networking between two apartment buildings to link the building bus service. The authors propose to use a virtual private network for data exchange between the buildings. A field test was successfully run. The next important step will be that the facility server will control more than two buildings over a virtual private network. In the future, networking building automation will becoming more and more important, especially with regard to smart grid.

6. REFERENCES

[1] M. Mevenkamp, “50% Energy Savings – Bus Technology in Schools and University Building”, **Perpetuum 06 (International Edition)**, 2006, p. 39.

[2] Merz, H. Et al. **Gebäudeautomation – Kommunikationssysteme mit EIB/KNX, LON und BACnet**, München: Carl Hanser Verlag, 2007, pp. 62-64.

[3] Konnex Association, “KNX IP – a New Class of KNX Devices”, **KNX Journal**, No. 1, 2008, pp. 12-13.

[4] Konnex Association, **KNX System Specifications – Architecture**, 2009, p. 10.

[5] M. Lipp, **Virtuelle Private Netzwerke – Aufbau und Sicherheit**, München: Addison-Wesley, 2001, p. 40-45.

[6] W. Böhmer, **VPN – Virtual Private Networks**, München: Hanser Verlag, 2005, p. 10.