2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing

Integrating Building Automation Systems and IPv6 in the Internet of Things

Markus Jung, Christian Reinisch, Wolfgang Kastner
Vienna University of Technology, Automation System Group, Vienna, Austria
{mjung, cr, k}@auto.tuwien.ac.at

***Abstract*—The vision of the Internet of Things is a seamless integration of diverse physical objects in the Internet through a virtual representation. In recent years, the target area of IoT constantly broadened from products within supply chains and nowadays encompasses all objects that are summarized under the label of ubiquitous and pervasive computing. Therefore also building automation devices are considered for an integration in the IoT, where they are for example used to realize a smart and sustainable building operation. Ubiquitous access to the objects is facilitated by the concept of building automation systems (BAS) that already provide a virtual representation of physical objects, mainly sensors, actuators and control devices.**

In practice, BAS follow a layered system architecture which defines a management, an automation and a field tier. In the field tier, non-IP communication based on twisted pair, power line or radio frequency technologies is prevalent. For the backbone infrastructure at the automation and management tier, IPv4 has become the de-facto standard. At this level, the transition towards IPv6 is the most promising technology to enable the full realization of the Internet of Things vision. New features like the larger address space, self-configuration, quality of service mechanisms and security promise a better integration of building automation technology in the IoT. Therefore this article investigates the readiness and compatibility of existing BAS technologies with IPv6. The integration challenges and new opportunities of IPv6 for these technologies are presented. Furthermore, possible integration scenarios for IPv6 using BACnet as example use case are sketched.

***Index Terms*—Internet of Things, IPv6, Building Automation**

I. Introduction

The *Internet of Things* (IoT) has been a popular research topic in recent years and still has a large momentum that can be seen in the high number of current research projects. The core concept of the future IoT is the integration of physical objects into a global information network. Information about the objects should be represented in the Internet and direct interaction with and between physical objects should be possible. The term *Internet of Things* was first mentioned in 2001 in a publication on the Electronic Product Code (EPC) [1]. The paper describes a naming scheme which provides a large enough address space to enumerate all physical objects, starting from simple items over containers to pallets and transportation vehicles. The IoT later gained widespread attention when in 2003 members of the Auto-ID center at MIT presented their vision of the EPC network in [2]. Main idea was to automatically identify the flow of goods within supply chains, which is a central aspect there. In this context, the IoT allows to optimize these process chains and, by providing real-time data, enables timely business intelligence that offers current data to business analysis tools.

In the following years the term IoT broadened and simultaneously encompassed the concept of seamless integration of physical objects into the Internet through their virtual representations. In Figure 1, the different view points on the Internet of Things as presented in [3] are shown. The concepts required and used to build an Internet of Things thus come either from a "Things"-centered point of view, an Internet- and communication-oriented approach or from the semantic visions of the IoT.

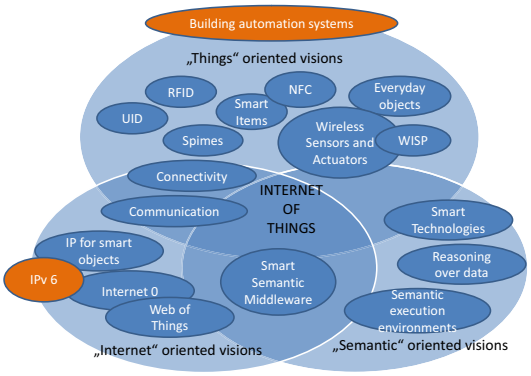

Fig. 1: Aspects of the Internet of Things [3]

This work focuses on the analysis how existing building automation technologies [4] can contribute to the future IoT and how they can be best integrated in the IoT. The paper thus mainly follows the "Things" vision of the IoT. However, since particular emphasis is given to an analysis of the role of IPv6 for these efforts, also the "Internet" oriented viewpoint is considered. In Section II, related work and previous research in the areas is reviewed and commented. Then, possible use case scenarios for building automation systems in the future IoT are sketched in Section III. Furthermore, possible integration scenarios and arising challenges are outlined. Section IV evaluates how IPv6 can help to address the identified challenges and validates assumptions for the BACnet technology as example use case. Finally, SectionV provides a discussion of the results and gives an outlook on future work.

Authors express their acknowledgement to the consortium of the project IoT6 (www.iot6.org). The IoT6 project is supported by funding under the Seventh Research Framework Program of the European Union, with the grant agreement FP7-ICT-2011-7-288445.

978-0-7695-4684-1/12 $26.00 © 2012 IEEE
DOI 10.1109/IMIS.2012.134

II. Related Work

The concept of connecting building automation systems (BAS) to the Internet is not a completely novel idea. Rather, possible integration approaches for building automation using IP have already been described in [5]. There, the author outlines that BAS are often designed and optimized for certain domains and their requirements with a focus on cost-effectiveness and efficiency. The topic of effective integration of control networks with other networks like the Internet is not being touched. This is different in [6], where problems and challenges of integrating control networks and data networks are identified. The main issue is found in TCP/IP being designed for data networks and thus being tailored transport of large files and a slow response time compared to the dynamic exchange of small-sized packets in control networks. As a second drawback, the large protocol stack as well as the message size of TCP/IP is identified as problem for the highly resource-constraint devices typically found in control networks. Furthermore, it is argued that real time operating systems running on IP enabled embedded devices have only a limited scope and that there is still a need for small and low cost devices connected in a low-cost and interoperable fashion.

A main focus of the paper is put on the Web based remote access, e.g. a system operator having access to the control network from a remote location through an Internet connection. In this case, gateway devices enable Web communication using HTTP on top of TCP/IP to access the BAS. While the gateways are responsible for protocol translation, the author points out that such gateways add cost, increase the processing burden and provide only a legacy solution to system integration. Therefore, an IP-every solution where each device has its own IP address is the preferred solution that eliminates the need for such a gateway. Furthermore, this approach enables direct digital control running over the Internet, a scenario that is also described in [7]. There, the presented concept focuses on how operators can access a building automation system through a Web browser. However, the focus is clearly put on the interaction of human beings with the BAS, while the proposed solution of this work aims at enabling device interaction through the Internet. This vision is also shared in a scenario presented in [8], where the term *Internet 0* is used to reflect that each device is natively connected to the Internet. Furthermore, it is shown how end-to-end modulation of IP packets can be accomplished also for embedded devices.

III. Building automation and Internet of Things

Building and home automation covers the control and management different aspects of HVAC, lighting, shading, security, safety, entertainment and household devices. A typical BAS operates within the local context of a functional building or private dwelling, where it links sensors and actuators of the field tier with control devices at the automation tier. Additionally, information can be aggregated at the management tier and offered to external information systems. The tiers of BAS are illustrated in Figure 2. The main addition that the IoT can provide to BAS is the crossing of these local borders, since also building automation "things" now have virtual representations in the Internet. This enables the direct interaction among all kinds of things, human beings and a variety of other services such as business processes.

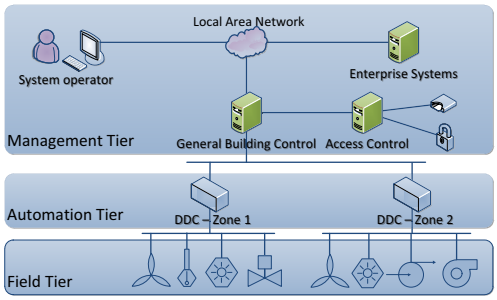

Fig. 2: Building automation model [9]

A. Use case scenarios

Once building automation devices become accessible in the Internet the doors to several, previously not realizable, use case scenarios are opened. The following list provides some example scenarios.

- **Device Maintenance:** Assume your device (your coffee machine, dish washer, cooling aggregate or blind controller, ...) reports that it requires maintenance or that some of its parts are faulty and need replacement. Typically these devices indicate such errors either via some visual feedback method like a blinking light or in the best case via a error reporting interface. In an interconnected IoT it becomes possible that the devices themselves notify the device supplier, send a spare part order to the ERP system of the vendor or even arrange a service appointment with a technician. The arrangement can even take into account the availability of the private house owner or the responsible system operator using information stored in an online calendar or groupware tool.
- **Smart Grids and Energy Efficiency:** Considering the gaining importance of energy efficiency and the increased deployment of smart grids the IoT can function as an enabler for solutions that allow to realize the smart grid. In functional buildings, energy can be saved by shifting energy consumption of HVAC devices to times when there is a lot of renewable energy available or when the electric grid is not overloaded. The implementation of such use cases requires that the BAS have connections and interfaces not only within the building but also to services and devices of the outside world. Current solutions and technologies like the Open Automated Demand Response (OpenADR) [10] partly provide these interfaces with the help of a gateway approach, where a separate protocol is used that shields the local building automation system. However, gateway-based integration comes with several drawbacks, e.g. the configuration effort, and can thus not be regarded as ultimate solution.

In the context of a private dwelling there are several use cases how energy can be saved or used more efficiently. If all persons leave a room, many devices can be switched off automatically. Likewise, if the online calendar indicates a two week vacation the whole building can enter a kind of sleep mode, which means that all devices are switched off instead of residing in standby mode. Furthermore, the heating or climate set points can be decreased significantly, since the occupancy of rooms needs not be expected. This scenario requires an interconnection of a variety of device types with information systems that have – until now – hardly been considered in home and building automation.

- **Buildings integrated into business processes:** For example in the case of a conference center, the building itself is a vital part of the business process. Occupancy of meeting rooms or conference halls requires to adjust the HVAC settings accordingly. The best settings thereby depend on a variety of influence factors such as the external temperature, the number of people in the room, scheduled sessions and many more. One idea to achieve better control is to determine an exact occupancy of people in real-time and adjust the control parameters accordingly. This can be achieved, for example, by persons identifying themselves with access cards containing RFID chips. Furthermore, if there is a change in the schedule kept in the conference groupware or ERP system, it is possible to save considerable amounts of cooling or heating energy in any room that will not be occupied within the next hours. Again, this use case requires the interconnection of globally distributed systems in the Internet or via cloud computing.

It is important to note that most of the presented use cases could already be realized on the application layer of some software system. The main challenge is rather found in the integration effort that is required to support the different systems and probably legacy protocols. The desired seamless end-to-end communication between things and information systems that would significantly reduce this integration effort is the vision of the future IoT.

B. Integration building automation systems in the future IoT

The integration of building automation in the future IoT can happen at different layers of the BAS. Taking connectivity as point of view, a BAS can be divided into backbone and field level. On the field level non-IP technologies like twisted pair, power line communication or radio frequency technologies are frequently used where BAS specific network and application protocols are used on top of the data link layer. At the backbone level, IP connectivity is prevalent due to the fact that existing IP cabling of the functional building can be reused to tunnel BAS specific protocols.

Figure 3 identifies the three possible integration scenarios for establishing connectivity with the Internet.

*a) **Centralized server**:* A centralized server can act as the linking element for the IoT. The server hides the complexity of the various BAS specific protocols and provides a central gateway using a single IP address.

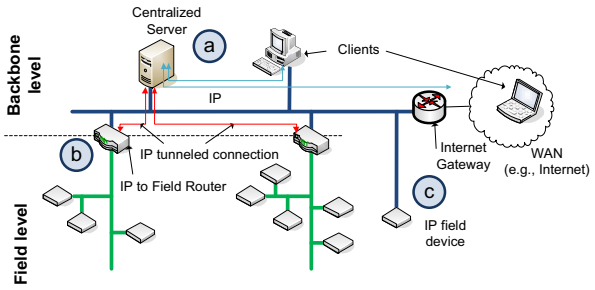

Fig. 3: BAS integration into IoT

*b) **Field to IP router devices**:* Another option to connect to the IoT is the connection to an IP backbone. A field/IP router operates as a proxy to the IoT and emulates an IP address for each connected field device, thus imitating native IP support of the device.

*c) **Field devices**:* Field devices can be directly connected to the IoT using IP to transport any higher-level protocol. The advantage is the gateway-less approach but it comes at the cost of having to implement an IP stack within every (simple) device like light switches or temperature sensors.

The possible integration scenarios illustrate how a BAS can be connected to a future IoT, but the solutions only solve the connectivity problem. A reasonable bigger challenge is to provide true **interoperability** in the sense of the multitude of existing BAS using their custom protocols or even a tailored layer model with respect to the ISO/OSI reference model. For the centralized server integration scenario different approaches like BACnet/WS [11], oBIX [12] or OPC UA [13] already exist. These standards typically propose a centralized server that offers platform independent interfaces like Web Services or RESTful APIs to access the underlying BAS. The central idea behind these technologies is to provide an easily applicable way for remote access. For example, an OPC UA server can provide interfaces to building automation technologies like KNX, BACnet or LON and itself offers a uniform interface and information model for all these technologies. Via this interface, a remote system operator application that is realized as OPC UA client can be used to access all data points, receive alarms and change of value notifications regardless of the underlying technologies. Furthermore, it enables the integration into enterprise applications or an enterprise service bus (ESB) based on Web Services following the paradigm of a Service-oriented architecture. However, these technologies are not intended to realize the IoT vision to full extent and rather should be regarded as application level gateways to building automation.

The most promising integration scenarios are those that provide an IP address for each device. However, demanding an IP address for each device leads to several issues that need to be solved, such as **address space**, **end-to-end communication**, **interoperability**, **security** and **scalability**.

The Internet was designed to globally connect computers that form a large data network spanning the whole globe. To cater for this interconnection, several protocols on different OSI layers are used. The key protocol in this family is IPv4, which takes care of the network layer. Within the responsibility of IP is the addressing of networks and hosts that reside in the networks. Routers forward IP datagrams from one to another network based on routing tables, either maintained statically or configured dynamically by routing protocols. Using 32bit for addressing, the address space is limited to to approximately 4 billion computers that can be connected. Considering the fact that not only computers should participate in the future IoT and that the address space is already exhausted[1], the use IPv4 addresses for new devices is not possible. Furthermore, computers and devices typically reside within a private IPv4 network, which complicates to directly connect to them, a features that is, however, required for a native **end-to-end communication**. An approach to solve both the address space and the end-to-end communication problem can be seen in peer-to-peer networks which define their customer overlay network addressing schemes and protocols. Mechanisms like UDP hole punching allow to provide end-to-end or client-to-client communication, but by using an overlay, the underlying network layer protocol is degraded. Additionally, exposing each device to the Internet imposes a great security risk. Whereas the topic security in building automation has been more or less neglected due to the traditionally closed networks, strong security mechanisms are required for the future IoT. Finally, the scalability of the future IoT needs to be considered. The existing building automation technologies are designed to be deployed in the scope of buildings. Although in the case of huge office towers there can be some thousands of sensors and actuators linked within a BAS, these systems were never designed to link billions of devices. While the issues of interoperability and scalability remain, solutions to the problems of address space, end-to-end communication and security can be provided by the IPv6 protocol. Therefore, the next section will investigate how IPv6 can become an enabler for the future IoT.

IV. Building automation and IPv6

This section investigates how IPv6 can ease the integration of BAS into the future IoT. It analyzes that relevant IPv6 features and afterwards sketches possible integration scenarios of IPv6 in BACnet.

A. IPv6 and BAS

IPv6[2] is a standard specified by the IETF in 1998. According to the specification the primary changes fall into the categories i) expanded addressing capabilities, ii) header format simplification, iii) improved support for extension and options, iv) flow labeling capability, and v) authentication and privacy. Changes that are of more interest for solving the stated problems are explained in more detail below.

- **Expanded addressing capabilities:** The address space of IPv6 is extended from 32 to 128bit. The calculation provided in [8] $2^{128}/(4 * \pi * 6378137^2) = 6.6 * 10^{23}$ indicates the number of possible devices per square meter using such a large address space. This allows to provide each device with an IPv6 address, to use it for identification in the future IoT and to avoid any overlay mechanism with custom addressing schemes and overlay routing mechanisms. With the extended address space additional improvements regarding auto-configuration of nodes and the scalability of multicast routing are defined. Furthermore, a new address type *anycast* is introduced, which allows to send a packet to any one of a group of nodes.
- **Header format simplification:** The header simplifications introduced in IPv6 make the protocol more attractive for deployments on embedded or constrained devices.
- **Flow labeling capability:** The new flow labeling allows a sender to label the packets of particular flows and to request certain QoS properties. For example, real-time in the sense of non-interrupted video streaming or voice-over-IP are a use case for the flow label. However, the term real-time in this should not be confused with real-time constraints known from certain control network applications where certain timing guarantees need be given by control devices. In the area of building automation the flow label capability might be useful.
- **Authentication and privacy:** IPv6 comes with an extension to provide authentication, data integrity and data confidentiality, all features that are definitely required in the future IoT.

B. IPv6 and BACnet

The building automation and control network (BACnet) defines a communication protocol for building automation devices. This subsection provides a short introduction to BACnet and outlines scenarios for BACnet-IPv6 integration.

- **BACnet overview:** The history of BACnet starts in 1987 when the American Society of Heating, Refrigerating and Air-Conditioning Engineers began to develop a standard for building automation. In 1995, BACnet became an ANSI standard and soon the standard evolved to an international ISO standard. Since then recent advances in building automation technologies were incorporated into the standard. The latest version is the ANSI/ASRHAE 135 - 2010 standard with extensions provided through several addenda. As shown in Figure 4, BACnet uses a collapsed four layer architecture based on the OSI physical, data link, network and application layer.
  The intention of BACnet is to be used for local building automation control networks. Therefore, the whole system is tailored to the resource constrained needs of simple automation and control devices. It defines a custom application layer protocol based on application

[1]Theoretically, host addresses are still available, but network addresses are already nearly exhausted.

[2]http://www.ietf.org/rfc/rfc2460.txt

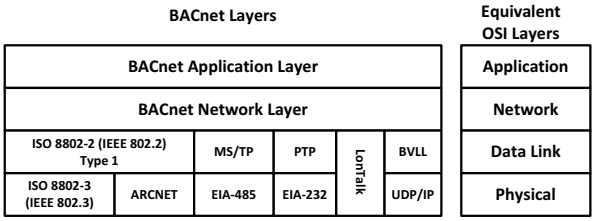

Fig. 4: BACnet collapsed architecture [14]

layer services providing access to devices which are represented through an object oriented ontology offering certain data points as objects as well as generic and uniform services to access them. The protocol itself uses a custom standardized binary serialization. The messages are exchanged in so called application protocol data units (APDUs) that are transmitted following a client/server communication model between communicating BACnet devices. The services provided by BACnet are grouped into alarm and event, object access, file access, remote device management and virtual terminal services. BACnet Building Interoperability Blocks (BIBBs) define a set of services that need to be implemented by a device in order to be compliant to this BIBB. Following these BIBBs, it is possible to have interoperable devices provided by different vendors. To create some control logic, all control devices are modeled as a collection of objects, having a central device object for each device. The device object provides an object identifier that is used as globally unique device identifier. The object identifier is 32bit long, being split into an object type of 10bit and an instance number of 22bit as listed in Figure 5.

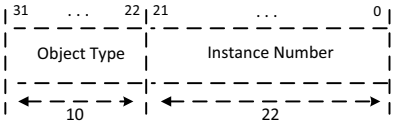

Fig. 5: BACnet object identifier [14]

This means that the global address space for BACnet devices within a BACnet internetwork is limited to 2^{22} devices, which will not be sufficient to fully realize the future IoT. Access to the objects residing on BACnet devices is encapsulated in APDUs which by themselves are passed to the network layer sending around network protocol data units (NPDUs). The network topology of BACnet is shown in Figure 5. The BACnet network layer connects different physical segments forming a single MAC address domain called BACnet network. Routers are used to interconnect these BACnet networks to form a BACnet internetwork. The BACnet network layer is quite constrained compared to the one of the Internet. It is only allowed to have a single path between each two devices. A connection of devices through the Internet is just out-of-scope of the BACnet specification, although UDP/IP is listed as data link layer in the collapsed architecture. The

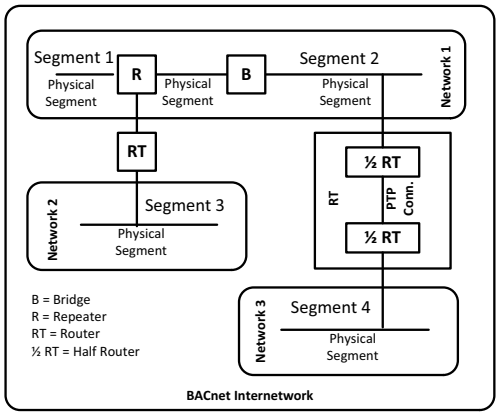

Fig. 6: BACnet network [14]

reason for the support of UDP on top of IP as data link layer is to enable the reuse existing IP networks, e.g. an office building IP backbone. For this reason, a BACnet virtual link layer (BVLL) is introduced and UDP/IP remains used at the same logical level like other media operating on Ethernet or Master Slave/Token Passing.

- **IPv6 as BACnet data link layer:**
  Using IPv6 as BACnet data link layer allows to send BACnet NPDUs over IPv6 networks. Operating BACnet on top of an IPv6 network segment raises several issues that are addressed in Addendum *aj* to BACnet 2008. As specified there, using IPv6 leads to 18-octet MAC addresses, where 16 octets are required for the IPv6 address and 2 octets remain for the UDP port. This adaptation has some severe side-effects since BVLL messages assume a fixed-length of 6 octets for a BACnet/IP address. Furthermore, the network layer header is defined to have a maximum length which would be exceeded. These issues can be fixed by adjusting the maximum protocol data unit lengths, a solution which would simultaneously introduce a potential incompatibility with existing BACnet devices. Another challenge is that several BACnet services rely on broadcasting in the media of a BACnet network. If multiple IP subnetworks are linked together to form a BACnet network, special measures have to be taken. Since IP broadcasts are not routed across the local network so called BACnet/IP broadcast management devices that forward broadcasts between the sub networks need to be used. Using IPv6 as BACnet data link layer allows to

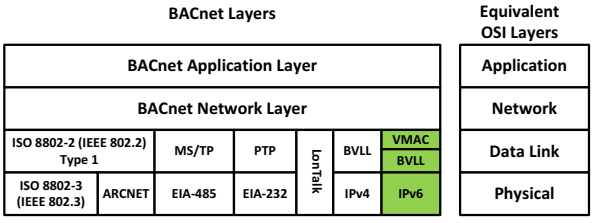

Fig. 7: BACnet - IPv6 as datalink layer [15]

	IPv6 as Data Link Layer	IPv6 as Network Layer
Address space	- No improvement	+ 128 bit address space
End-to-End communication	∼ IPv6 segments used for tunneling	+ Direct IPv6 communication between two devices
Security	∼ Security within IPv6 network	+ End-to-end security between two devices
Interoperability	∼ Backward compatibility possible	- Not compatible with non IPv6 BACnet devices
Scalability	+ Device limit remains the same	- Architecture not designed for IoT

TABLE I: BACnet and IPv6 integration scenario comparison

secure BACnet messages that traverse an IPv6 network, but it does not provide end-to-end security. Using IPv6 as data link layer does also not address the address space problem or the end-to-end communication problem, since IPv6 addresses are not used to identify devices and IPv6 is also not used for networking.

- **IPv6 for device identification and networking:** The features of IPv6 can be fully utilized if the network layer of BACnet is replaced by IPv6 and used for end-to-end communication between two devices. Additionally, IPv6 addresses need to be used as BACnet device identifiers at the application layer. This solution allows to globally identify devices within a single address space. Furthermore, no network address translation is required and direct end-to-end communication becomes possible. Authentication and encryption features are available directly to the application layer, allowing to define new services taking benefit of this functionality. Applying these changes however leads to the definition of a new protocol that is no longer interoperable with existing BACnet devices. Another problem is that globally linking all devices into a single BACnet internetwork introduces scalability problems. Remote device management services like `Who-Has` or `Who-Is` relying on broadcasts that are spread in the whole internetwork would not scale and the mechanisms used for discovery and configuration provided by BACnet would not suit such an environment.

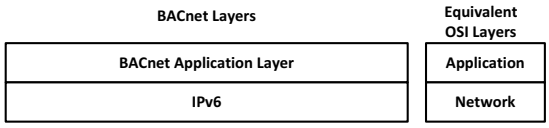

Fig. 8: BACnet - IPv6 as network layer

C. IPv6 Scenario Comparison

Table I summarizes the results of the last sections and provides an overview how the different integration scenarios deal with the challenges identified in Section III.

V. Conclusion

This paper addressed two new aspects, building automation systems and IPv6, in the context of the future IoT. Use cases show that it is required to also consider existing devices operating on legacy protocols for a realization of the vision of an IoT. IPv6 is a technology that provides several features, like a larger address space and end-to-end security, which can be useful in the context of an integration of building automation devices. The outlined integration scenarios that follow the BACnet system show that IPv6 cannot be simply used as network layer protocol for building automation devices. The reason for this shortcoming is that BACnet faces interoperability and scalability problems if IPv6 is used for device identification. Furthermore, the proper usage of IPv6 in BACnet would lead to a novel BAS, and hence again worsen the general interoperability problem among the variety of different BAS technologies. Therefore, existing BAS technologies are identified of not being capable of serving as a fundament for the future IoT. Rather, it is required to build a new system that uses IPv6 as first-class citizen and that provides an open protocol allowing interoperable devices to directly interact with each other.

References

[1] D. Brock, "The Electronic Product Code (EPC)," *A Naming Scheme for Physical Objects*, 2001.

[2] K. Ashton and S. Sarma, "Introducing the EPC Network," in *EPC Symposium, Chicago, USA*, 2003.

[3] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[4] W. Kastner, G. Neugschwandtner, S. Soucek, and H. M. Newman, "Communication Systems for Building Automation and Control," *Proceedings of the IEEE*, vol. 93, no. 6, pp. 1178–1203, Jun. 2005.

[5] E. Finch, "Is IP everywhere the way ahead for building automation?" *Facilities*, vol. 19, no. 11/12, pp. 396–403, 2001.

[6] R. Raji, "End-to-End solutions with LonWorks control technology," *Echelon Corporation*, 1998.

[7] M. Brambley, D. Chassin, K. Gowri, B. Kammers, and D. Branson, "DDC and the Web," *ASHRAE journal*, vol. 42, no. 12, pp. 38–50, 2000.

[8] N. Gershenfeld and D. Cohen, "Internet 0: Interdevice internetworking-end-to-end modulation for embedded networks," *Circuits and Devices Magazine, IEEE*, vol. 22, no. 5, pp. 48–55, 2006.

[9] ISO 16484-2, "Building automation and control systems (BACS)," 2004.

[10] M. Piette, G. Ghatikar, S. Kiliccote, E. Koch, P. Hennage D., Palensky, and C. McParland, "Open Automated Demand Response Communications Specifications (Version 1.0)," NIST Standard, 2009.

[11] "BACnet/WS," Addendum c to ANSI/ASHRAE Standard 135-2004, 2004.

[12] "oBIX 1.0 committe specification," OASIS, 2006.

[13] "OPC unified architecture specification," OPC Foundation, 2009.

[14] "BACnet – a data communication protocol for building automation and control networks," ANSI/ASHRAE 135-2010, 2010.

[15] "BACnet - Add support for IPv6," Addendum aj to ANSI/ASHRAE Standard 135-2008, 2010.