Wireless Technologies in Home and Building Automation

Christian Reinisch, Wolfgang Kastner, Georg Neugschwandtner, Wolfgang Granzer

Abstract— **The use of wireless technologies in automation systems offers attractive benefits, but introduces a number of new technological challenges. The paper discusses these aspects for home and building automation applications. Relevant standards are surveyed. A wireless extension to KNX/EIB based on tunnelling over IEEE 802.15.4 is presented. The design emulates the properties of the KNX/EIB wired medium via wireless communication, allowing a seamless extension. Furthermore, it is geared towards zero-configuration and supports the easy integration of protocol security.**

I. Introduction

In recent years, wireless technologies have become very popular in both home and commercial networking applications. The use of wireless technologies offers distinctive advantages in the field of home and building automation (HBA) as well. First, installation costs are significantly reduced since no cabling is necessary. Neither conduits nor cable trays are required. Wireless technology also allows placing sensors where cabling is not appropriate for aesthetic, conservatory or safety reasons. Examples include representative buildings with all-glass architecture, historical buildings, and industrial environments. In the latter case, long cables can cause differences in electrical potential to build up, which – while harmless to network devices and users – are unacceptable safety hazards in explosive environments.

Moreover, associating mobile devices such as PDAs and Smartphones with the automation system gets easier in wireless networks.The exact physical location of a device is no longer crucial for a connection, as long as the device is in reach of the network.

For all these reasons, wireless technology is not only an attractive choice in renovation and refurbishment, but also for new installations. The ability to reconfigure and extend the network easily when faced with new or changed requirements in the future makes wireless installations a seminal investment.

However, protocols must be tailored to the specific requirements of sensor/actuator networks to deliver these benefits at an attractive price/performance ratio. The recent years have seen a lot of development in this respect. The present paper briefly reviews these requirements in Section II and design implications in Section III. Section IV then presents the relevant standards that have emerged.

Especially in the field of building automation, the active lifetime of installations is high. Hybrid and downward compatible solutions significantly ease the transition towards new technology. Therefore, Section IV also reviews KNX RF, an extension to a well-established HBA field bus. In Section V, we present an alternate approach using tunnelling over IEEE 802.15.4 and its advantages over KNX RF.

The authors ({creinisch,k,gn,wgranzer}@auto.tuwien.ac.at) are with the Automation Systems Group, Institute of Computer Aided Automation, Vienna University of Technology, Treitlstrasse 1-3, 1040 Vienna, Austria.

II. Requirements

Regarding the performance criteria of data throughput and latency, building automation applications have relaxed requirements. Since HVAC (heating, ventilation and air conditioning) control has to deal with high system inertia anyway, the only notable exception regarding latency is open loop lighting control.

However, the market requires this performance to be delivered at low system cost compared to, e.g., industrial automation. Thousands of nodes may be needed to provide automation for a building, so every single node has to be as cheap as possible to make the investment sensible.

The devices of a building automation system are dispersed over a large area. This makes going wireless especially attractive. Yet, maximum benefit is only obtained if all wires are cut – including power wires. While this is seldom possible for actuators, it is a realistic perspective for sensors. However, due to the high node count in the system, having to change or charge the batteries of each wireless sensor every few days is not feasible. This adds another constraint: Measures must be taken to achieve battery lifetimes of at least several months, better years. The ultimate goal in this respect are nodes which draw their power entirely from the environment, e.g. via piezoelectric elements, thermocouples, or solar cells (energy scavenging).

A number of challenges stem from the very nature of the wireless medium itself. The same amount of design complexity typically buys less transmission capacity in a wireless than in a wire-bound transceiver. A wireless link also has far less predictable characteristics than a wired one. In particular, carrier sensing (i.e., node visibility) is locally dependent: it is possible that A and B can see C, but not each other (hidden node problem). Also, channel quality is time variant. [1] discusses the properties of wireless channels (and their implications on the design of wireless fieldbus systems) in more detail.

Various aspects of interference are a particular challenge in wireless systems, since their communication channel is always open for other users as well. Next-door installations using the same protocol are only a small part of the problem. Especially in the particularly attractive license-free ISM (Industrial, Scientific, Medical) frequency bands, a variety of wireless technologies from garage door openers to wireless presenters are competing for access to the medium, all using different access control strategies. Only recently, coexistence aspects have begun to receive more attention in protocol design. The ISM bands also accommodate devices creating radio frequency (RF) emissions merely as a by-product of their intended use. Thus, a wireless network node is much more likely to find its channel jammed than a wired one. This especially has to be taken into account for safety related applications.

Operating on an open medium has implications for communications security as well. Attackers now can take over unsecured systems without ever having entered the building. As an additional difficulty, protocol security features such as crypto-algorithms are limited by the requirement of low power consumption in the nodes – a limitation attackers do not face.

Especially security critical applications like surveillance, access control, and alarm systems also require protocol support for e.g., encryption. However, all this must be achieved while meeting the requirement of low per-node costs.

III. Design implications

The sensor portion of (wireless) HBA networks shares key characteristics with wireless sensor networks (WSN). Rabaey et al. [2] trace the vision of ubiquitous WSN and point out that specific protocol support and design trade-offs are necessary to build the required ultra-low-power and low-cost nodes.

The need for a bespoke design starts with the obligatory use of energy efficient hardware (e.g., low supply voltages and support for sleep modes in microcontrollers). A Hardware-Software-Co-Design approach is required to obtain the most efficient implementation of the protocol stack. However, the design of the communication protocol is of leading importance. For example, it has to allow nodes to enter these sleep modes as often as possible by minimizing the time they have to be in a "listening" state. This can go as far as allowing sensor nodes entirely without radio reception capability – largely a necessity for energy-scavenging approaches. In this case, other nodes cannot acknowledge the successful reception of a message. Instead, alternative approaches such as retransmission at random intervals (in order to counter periodic interference signals) have to be taken.

Since devices in a building automation system are dispersed over a large area, it cannot be assumed that sensors can reach associated controllers or actuators directly. An infrastructure of access points and a wired backbone network is not an option. Therefore, mesh networking schemes are an essential concept. The high node count of building automation systems comes to help here. With such schemes, nodes that are not in direct reach of their communication partner receive its messages through message forwarding from other nodes. This has the added benefit of redundancy, i.e., if a single device fails, communication can be upheld through redundant paths (which do not have to be pre-established at installation time).

To minimize interference and maximize range, wireless applications should select a frequency band whose regulations and physical characteristics best match their communication characteristics. Of the ISM bands, the 2.4 GHz band is currently most popular since it is available license-free almost worldwide. However, it is excessively crowded, too. While high data rate applications have no alternatives, HBA applications get by with far lower throughput. This enables the use of lower frequencies, which have the advantage of better radio wave propagation with the same amount of power spent.

Thus, the ISM bands in the 900 MHz region are of particular interest. Unfortunately, their frequency ranges differ in Europe (863-870 MHz) and US (902-928 MHz). However, they are close enough to allow a single transceiver design which can be adapted by adjusting the oscillator only. Though narrower than its US counterpart, the European range is attractive since it is well regulated. For example, channel-hogging audio applications (e.g., cordless headphones) are not allowed between 868 and 870 MHz, but have their own frequency at 864 MHz. The 868-870 MHz sub-range is further subdivided into sections with varying limitations on duty cycle and transmission power. In contrast, devices using the US 902-928 MHz range are only subject to a transmit power limit of 1 W. Therefore, e.g., cordless phones are a major source of interference.

Further, robust modulation and transmission techniques can spread the signals over a larger part of the available frequency spectrum, reducing the effects of narrow band interference.

IV. Wireless protocol standards overview

As was pointed out previously, the demands of sensor/actuator networks are different from the demands of "office networking" or "short range cable emulation" scenarios. This eliminates a number of popular wireless standards, in particular Wireless LAN (IEEE 802.11, designed for the former) and Bluetooth (IEEE 802.15.1, for the latter). Being designed for different applications such as media streaming and the corresponding high data rates, they cannot meet our requirements regarding energy consumption and cost.

In the following, a selection of relevant wireless control networking technologies applicable in HBA is presented. Table I provides an overview of common features. All technologies supporting the 868 Mhz frequency band, except KNX RF, also support 908 MHz operation. A protocol is considered "published" if the protocol specification is available to the general public for a "non-discriminating" fee. All protocols employ at least some kind of mesh networking scheme.

A. Z-Wave

The proprietary Z-Wave protocol [3] was developed with an explicit focus on home control applications. Z-Wave operates at 908.42 MHz +/- 12 kHz in the US and 868.42 MHz +/- 12 kHz in Europe, using FSK (frequency shift keying) modulation and a data rate of 9.6 kbit/s. A single network may contain up to 232 devices. Higher counts can only be obtained by bridging networks.

Z-Wave uses source routing, meaning only devices which are aware of the entire network topology can send ad-hoc messages to any destination (controllers). Another device class, routing slaves, communicate with predefined destinations using routes that are downloaded to them during the association process. Mains powered routing slaves will also use these routes to forward messages on behalf of another node. Finally, nodes which only receive messages to act upon them are called (non-routing) slaves.

There is always a single controller (primary controller) that holds the authoritative information about the network topology. It is involved every time a device is to be included in or excluded from the network. Routes are automatically found, and defective routes are automatically removed to cope with devices changing their location and RF transmission paths becoming blocked over time.

TABLE I
SUMMARY OF PROTOCOL FEATURES

	Frequency band	*Data rate*	*Security*	*Published*	*Max. node count*	*Modulation*
$Z-Wave$	868 MHz (EU)	9.6 kbit/s	advertised	no	232 per network	FSK
$EnOcean$	868 MHz (EU)	120 kbit/s	no	no	2^{32}	ASK
$nanoNET$	2.4 GHz	2 Mbit/s	yes	no	2^{48}	CSS
$KNX\ RF$	868 MHz	16.4 kbit/s	no	yes	256 per line	FSK
$IEEE\ 802.15.4/ZigBee$	868 MHz (EU), 2.4 GHz	20, 250 kbit/s	AES	yes	65536	PSK

B. EnOcean

EnOcean has commercially pioneered the concept of energy scavenging. Entirely solar powered modules are available as well as pushbutton sensors driven by piezoelectric elements.

EnOcean operates at 868.3 MHz, using ASK (amplitude shift keying) modulation. An unusually high data rate of 120 kbit/s together with a maximum payload of 6 bytes ensures a short frame transmission duration (below 1 ms). This not only minimizes power consumption, but also results in a low statistical probability for collisions. Also, EnOcean transceivers use a novel RF oscillator that can be switched on and off in less than 1 μs. Thus, it can be switched off at every "zero" Bit transmission, further reducing energy consumption.

The low collision probability is also presented as a key argument that the protocol will scale towards networks with a large number of nodes. The available radio modules do not appear to support security mechanisms.

C. NanoNET

NanoNET [4] operates at 2.45 GHz and supports data rates of up to 2 Mbit/s. The modulation scheme used is called Chirp Spread Spectrum (CSS). Symbols are transmitted as linear chirps, i.e., sinusoidal waveforms whose frequency increases (upchirp) or decreases (downchirp) over time. These chirps have a bandwidth of 80 MHz and a fixed duration of 1 μs. Their broadband nature makes them resistant against disturbances. CSS is part of a broader concept called Multi Dimensional Multiple Access (MDMA), a combination of phase, amplitude and frequency modulation. A CSS based physical layer related to nanoNET technology is under consideration as an alternative physical layer for IEEE 802.15.4 (802.15.4a).

The protocol stack complementing the nanoNET transceiver is designed to be highly portable to different microcontrollers by separating HW dependent and independent code. Methods for acknowledged, unacknowledged, connectionless and connection oriented communication and frame routing are provided. Regarding security services, the stack offers 128 bit encryption using an undisclosed stream cipher with support of one time pads, and message authentication. The medium access controller within the transceiver supports Aloha, CSMA/CA and TDMA.

D. KNX RF

In addition to the twisted-pair and power line media, a wireless transmission medium called KNX RF has been specified in Supplement 22 of [5]. KNX RF operates at 868.3 MHz +/- 40-80 kHz using FSK modulation at a data rate of 16.4 kbit/s.

To detect and recover from transmission errors, KNX RF frames contain a CRC with hamming distance 6. The repeat flag which indicates resent frames in standard KNX is replaced by a 3 bit link layer frame number (LFN). This allows greater flexibility for additional frame repetitions at the data link level. To extend the transmission range, retransmitters can be used.

Due to the nature of wireless communication and the support of transmit-only devices, KNX RF uses its own addressing scheme which is different from the standard KNX addressing scheme. Since RF is an open medium, the address spaces of neighboring installations would interfere with each other. Therefore, it has to be guaranteed that each KNX RF installation has its own address space. Hence, extended addresses, defined as the combination of the traditional KNX address and the serial number (SN) of the device, are used. Since the SN is globally unique, an extended address of a group (extended group address) or of a particular device (extended individual address) does never interfere with an address from a neighboring installation.

However, the use of extended addresses comes along with two major drawbacks. First, only 1 – n instead of m – n relations are possible. Since the extended group address contains the SN of the sender, two different senders can never send a message to the same extended group addresses. Second, media couplers between KNX and KNX RF are needed not only for physical interconnection but also for address translation. Address mapping tables have to be set up during system configuration. KNX RF does not provide any security mechanisms.

E. IEEE 802.15.4 / ZigBee

The focus of IEEE 802.15.4 [6] and ZigBee [7] is to provide general purpose, easy-to-use and self-organizing wireless communication for low cost and low power embedded devices. While IEEE 802.15.4 defines the physical and the MAC layer, ZigBee defines the layers above.

The IEEE 802.15.4 physical layer specifies 3 different frequency bands: 868-868.6 MHz (1 channel, 20 kb/s), 902-928 MHz (10 channels, 40 kb/s) and 2.40-2.48 GHz (16 channels, 250 kb/s) all using PSK (phase shift keying) modulation. Devices are classified as Full Function (FFD) and Reduced Function devices (RFD) according to the complexity of the protocol stack. While FFDs can communicate in peer to peer fashion, RFDs can only communicate with coordinators, resulting in a star topology. IEEE 802.15.4 defines two different kinds of personal area networks (PANs): beacon enabled and non-beacon enabled networks. In a beacon enabled network, a superframe structure is used. The superframe is bounded

by network beacons which are sent by the PAN coordinator periodically. Between these beacons, the superframe is divided into slots which can be used by the PAN members to communicate using a CSMA-CA scheme (Contention Access Period). Optionally, the PAN coordinator can assign guaranteed time slots (GTSs) to devices, providing them with a fixed communication slot. In a non-beacon enabled network, all PAN members can communicate at any time using CSMA-CA. In contrast to other wireless technologies, IEEE 802.15.4 already specifies different security services which rely on AES.

ZigBee adds a network layer responsible for enabling a self-forming and self-healing mesh network by providing appropriate routing services including route discovery and maintenance. The application layer provides application support, such as a key-value-pair communcation service and standard data types. It also handles management operations such as discovering and joining a network, establishing and maintaining bindings, and configuring security services. Application profiles for various domains exist, but have not been published. ZigBee security is based on the mechanisms specified in IEEE 802.15.4 but extends them by introducing different keys for end-to-end and network wide security.

V. Wireless communication and KNX/EIB

As mentioned in Sec. I, wireless communication is clearly the way to go. Choosing a standard which is tailored to the specific requirements of HBA is important. A number of interesting technologies are available and have been discussed. However, it has to be taken into account that HBA installations are long-lived. Compatibility is of major concern. Therefore, we shall extend a well established technology.

Our system of choice is KNX/EIB which is popular in Europe. Its wireless extension KNX RF leaves ample room for improvement. By replacing it with IEEE 802.15.4, we easily obtain security support as well as a potential cost reduction since IEEE 802.15.4 transceivers are already being produced in large numbers. It is an open, well proven technology. An IEEE 802.15.4 link also easily accommodates the data rate on the KNX/EIB twisted pair medium, which operates at 9.6 kbit/s. As a particular improvement over KNX RF, we aim at zero configuration and better routing. IEEE 802.15.4 is also an excellent basis for future work regarding integration with ZigBee.

A. Tunneling considerations

We propose a tunneling approach, illustrated in Fig. 1. The sender receives frames from the control network (CN) and wraps them into tunneling packets. These packets are transmitted over the tunneling medium (TM, host network) to the receiver where they are unwrapped and forwarded to the other CN segment. A major benefit of this solution is that it is completely transparent to the control network. CN frames remain unchanged.

In the simplest case, every tunneling endpoint (tE) always has a fixed association with another single tE. In this setup, tunneling devices always come in pairs.[1] Such a tunneling

[1]Although there may be multiple pairs, a member of one pair will never communicate with a member of another.

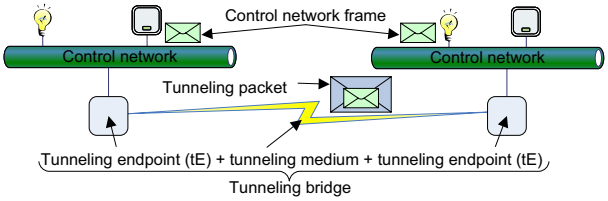

Fig. 1. Connecting control network segments via tunneling

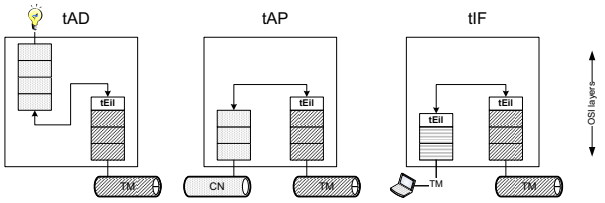

Fig. 2. Tunneling device classes

bridge can be likened to cutting the network cable and splicing it back together via the bridge. It requires almost no configuration effort. Setting the network address of the associated tunneling end-point is sufficient.

This approach is very suitable for providing remote access to a HBA installation (e.g., via the Internet). However, it is of limited use in practice when a short range wireless network is targeted as the tunneling medium. One possible application would be connecting two parts of a low-traffic segment over a public street. Another would be easy connection of a mobile device (i.e., laptop or PDA with engineering software). For convenient use in practice, however, the latter application would already require some sort of discovery protocol. Otherwise connecting the mobile device to network segments – all with separate tEs – would be cumbersome.

Obviously, there is no need to implement the control network down to the physical layer if only a single node is connected to a tE. As an example, consider the mobile device just discussed. As another, a wireless light switch. We call such devices tunneling application devices (tADs). They implement the tunneling medium interface and the CN application layer.

Devices as suggested in Fig. 1 which actually implement CN and TN both down to the physical layer are named tunnel access points (tAP). As a special case, PC-based nodes are typically connected to the CN via an adapter which does not implement any higher layers of control network (tunneling interface, tIF). It does however implement a second tunneling connection (which is typically point-to-point) to the PC.

Compared to the classification presented in [8], this classification focuses on network protocol aspects rather than functional points of view. It is illustrated in Fig. 2. The tunneling endpoint implementation layer (tEil) mediates between the CN and TM layer 3 SAPs.

Using this simple point-to-point scheme, the only possibility to integrate a tAD (or tIF) is to pair it with a tAP. This means that two wireless tADs (sensor and actuator) would need two tAPs to communicate even if they are within transmission range of each other. This is obviously inefficient since each wireless end device would need its own tAP.

In the general case, it is desirable to model networks as in Fig. 3. In order to be able to fully replace a wired CN

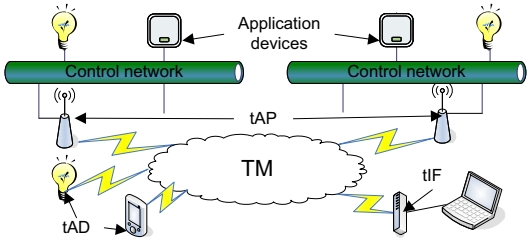

Fig. 3. Wireless enabled CN using tunneling

with a wireless one, it shall be possible to integrate wireless sensors, actuators and controllers and wireless management devices (e.g., light switch, PDA) using tADs. Furthermore with the use of tIFs the integration of PC-based configuration and management devices is also possible. tAPs still provide interconnections to wired CN segments.

To overcome the drawbacks of a simple point-to-point scheme, the tE would need to be able to communicate with other tEs on the tunneling medium. More precisely, it would have to communicate with the proper tE to reach the destination node in the control network. This cannot be achieved with a plain tunneling bridge, which does not have knowledge about the addressing scheme used on the CN.

A tunneling router must understand the routing scheme of the control network, and provide an appropriate routing scheme (e.g., mesh networking) on the tunneling medium. The required routing tables would have to be configured manually given the resource limitations of low-power wireless nodes.

B. KNX/EIB over IEEE 802.15.4

In KNX/EIB, process data are exchanged in communication groups exclusively (with corresponding messages referred to as group messages). Multiple senders are able to send process data to multiple receivers according to a producer-consumer scheme based on group addresses where senders and receivers are not aware of each other.

Since IEEE 802.15.4 does not offer support for multicast communication, another solution has to be found. One opportunity would be to simulate group communication by sending a tunneling packet (including the group message) to each member of the group using point-to-point communication.

Obviously, this approach is not applicable. What is a single group message on the native, wired KNX/EIB medium has to be sent to each group member sequentially. Since groups can be large, this approach will lead to high network traffic as well as to a significant delay of group communication. Furthermore, the configuration and maintenance effort will increase rapidly since elaborate routing tables are required in each node. This is a significant drawback since one of the most important benefits of the group communication facility of KNX/EIB is that the group members do not need to be aware of each other.

To overcome this deficiency, we chose a solution which is based on broadcasts using a simple flooding algorithm. Every KNX/EIB group message is encapsulated unchanged into an IEEE 802.15.4 broadcast telegram. The destination address is set to the IEEE 802.15.4 broadcast address and the PANID to a predefined value. Each wireless device which is within the transmission range of the sender receives this message and resends it. The IEEE 802.15.4 frame header and trailer are discarded and the KNX/EIB message is extracted. A tAD or tIF checks the group address. If it is configured to be a member of that group, it processes the message. Otherwise it discards it. On the other hand, a tAP simply inserts the message to the wired KNX/EIB segment where it is transmitted using the usual KNX/EIB multicast mechanism. If a tAP receives a message on the wired segment, it broadcasts it.

The retransmission scheme ensures that every KNX/EIB frame reaches every device as long as the network graph is connected.[2] However, it necessarily causes message duplications and cycles. To solve this problem, it must be ensured that every node repeats a received message exactly once. For this purpose, every message needs to be tagged with a message ID (mID). This mID consists of a local sequence number (sNR) and the IEEE 802.15.4 long address of the sender node (sAD).

The sNR is initialized with zero at power up and increases monotonically with every broadcast sent. Since the IEEE 802.15.4 long address is globally unique, it is guaranteed that each broadcast message can be uniquely identified in the whole network as long as its transmission is fully completed before the local sequence number is reused.

The mID of each incoming broadcast message is stored in a local broadcast table (BCT). If another message with the same sAD is received, its sNR is compared against the one found in the BCT. If the incoming sNR is lower or equal, the message is discarded. Otherwise it is re-broadcast and its mID replaces the old one in the BCT. An entry is only removed when it can be guaranteed that no messages with this mID are present in the entire network. This is the case when the message corresponding by this entry has been resent by every node.

This time out is $time\_out = t_{hold_{max}} \cdot hop\_count_{max}$ with $t_{hold_{max}}$ being the maximum time that the node will hold and try to resend an incoming message until it is discarded, and hop_count_{max} being the longest path a packet can take through the network. If the sAD of an incoming message cannot be found in the BCT and the BCT can hold no more entries, the message is discarded.

This algorithm guarantees *source FIFO ordering* and *at-most-once semantics* for delivery. Note that the BCT size and sNR range are not critical to these properties. Both parameters only influence the probability for successful message delivery.[3]

Assuring these two properties is of particular importance since reordering and duplication cannot occur on the KNX/EIB wired medium. Thus, the higher stack layers cannot deal with these cases. Necessarily, it comes at the price of possibly losing some a message which could otherwise have been relayed. However, this is no restriction since the KNX/EIB network layer does not support reliable transmission anyway. Applications that require end-to-end reliable transmission have to handle this on their own.

[2]An edge in the network graph corresponds to a wired or wireless link between two devices (nodes).

[3]Even if the sNR of a particular sender wraps before $time\_out \cdot sNR\_range$ has elapsed, the consequence is only that the new message is ignored by those nodes which still hold the re-used mID in their BCT.

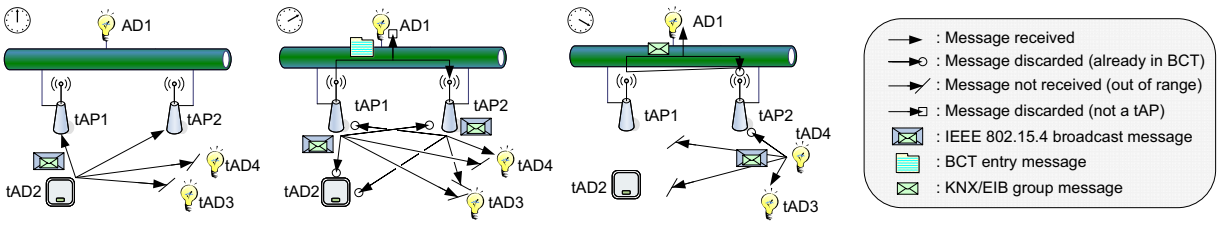

Fig. 4. Duplication prevention: Example sequence

While the BCT size and sNR range are not critical to these properties, the timeout is. Given that the maximum message hold time cannot be modified, we can only make better use of a given table capacity by limiting hop_count_{max}. In general, its lowest upper bound is given by the number of (wireless) nodes minus one. However, it can be lowered further by introducing a broadcast time to live (BCTTL) parameter in every message. It determines the maximum number of times a broadcast packet is retransmitted. This field is initialized by the originator (the initial value is common for all devices). Every time before a tunneling device resends a broadcast frame, the value of its BCTTL is decremented by one. If the result is zero, the frame is discarded. Otherwise, it is relayed.

The algorithm works as long as each wired network segment has no more than one tAP assigned. If multiple tAPs per segment are to be allowed, it has to be considered that a wireless link (direct or via intermediate nodes) between these tAPs can exist in addition to the wired connection.

First, we regard the case of a tunneling packet originating outside this wired segment. Since a wireless path exists between the tAPs, both tAPs will forward the encapsulated KNX/EIB frame to the wired network segment. Thus, the group message will be duplicated on the KNX/EIB network. Even worse, since the CN frame cannot be identified as having been inserted by a tAP, the other tAP will rebroadcast it, creating a loop. To avoid this, the tAPs must also create a BCT entry for such frames.

This means that the tAP must not simply discard the IEEE 802.15.4 header – and with it, the necessary information to create a BCT entry –, but rather transmit this information over the wired segment together with the CN frame. This is done by sending a BCT entry message before the CN frame. This message is a KNX/EIB extended frame containing the mID and BCTTL.[4] All BCT entry messages are sent to a group address predefined for this purpose. Fig. 4 illustrates this concept: tAD2 and tAD3 can communicate via tAP1 and tAP2 and the wired segment – without the installer having to take any special precautions even if tAP1 and tAP2 are within wireless communication range of each other.

The case of a "native" CN frame originating in the wired segment is almost symmetric. Again, the existence of a wireless path between the tAPs will lead to message duplication and loops. To retain at-most-once semantics, the tunnelling packets must be sent out with synchronized mIDs by all tAPs on the segment. This is achieved by every tAP transmitting an initialization message on the wired segment at power-up. This message (sent to the predefined, reserved group address) contains the sAD of the tAP. Every tAP receiving this message then uses this sAD instead of its own for the tunnelling packets it generates in response to incoming CN frames (and only for these tunnelling packets), starting with a sNR of zero. For added robustness, the current sNR for such packets can also be included in the BCT entry messages to allow resynchronization.

[4]Since another node could transmit a higher-priority CN frame between the BCT entry message and the CN frame, the BCT entry message also contains a hash value computed over its associated CN frame. This hash value allows the receiving tAP to correctly associate the BCT entry message.

VI. Conclusion and Outlook

Wireless sensor and actuator networks are becoming a more and more attractive alternative to wired solutions in the HBA domain. A number of technologies that fulfill the specific requirements of this class of wireless networks have reached commercial status, with none of them clearly in the lead.

Given the long life cycles of building automation technology, compatibility to established wired systems is essential for a new technology. A tunnelling solution that allows running KNX/EIB over IEEE 802.15.4 links was presented. Unlike KNX RF, it provides a basic level of communications security using a shared key "out of the box" by leveraging the standard IEEE 802.15.4 security mechanisms. No additional management overhead is incurred; rather, it is reduced since the address mapping that KNX RF has to perform is avoided.

As next steps, a closer evaluation of the broadcast algorithm performance by way of simulation is required. Also, the effects of contention occurring on the tunnelling medium and especially at the tAPs – where the lower data rate of the wired segment meets the higher one of the IEEE 802.15.4 link –, and the loss of segment-wide bit-wise arbitration in general must be studied more closely. Moreover, the shortcoming that multiple KNX/EIB segments (lines) containing tAPs will lead to these lines being logically shorted due to the shared PANID shall be addressed.

References

[1] A. Willig, K. Matheus, and A. Wolisz, "Wireless technology in industrial networks," *Proceedings of the IEEE*, vol. 93, no. 6, pp. 1130–1151, 2005.
[2] J. Rabaey, M. Ammer, J. da Silva, J.L., D. Patel, and S. Roundy, "Picoradio supports ad hoc ultra-low power wireless networking," *Computer*, vol. 33, no. 7, pp. 42–48, July 2000.
[3] *Z-Wave System Design Specification: Z-Wave Protocol Overview*, Zensys A/S, Fremont, 2005.
[4] Nanotron Technologies GmbH, "nanoNET chirp based wireless networks," Nanotron Doc. ID NA-04-0000-0298-1.03, Retrieved Dec. 12, 2006, from http://www.nanotron.com, 2005.
[5] *KNX Specification, Version 1.1*, Konnex Association, Diegem, 2004.
[6] *IEEE Std. 802.15.4-2003*, IEEE Computer Society, 2003.
[7] *ZigBee Specification 2004*, ZigBee Alliance, San Ramon, 2004.
[8] W. Granzer, W. Kastner, G. Neugschwandtner, and F. Praus, "A modular architecture for building automation systems," in *Proc. 6th IEEE WFCS*, 2006, pp. 99–102.