Wireless Communication in KNX/EIB

KNX Scientific Conference 2006

Christian Reinisch,
Wolfgang Granzer, Georg Neugschwandtner,
Fritz Praus, Wolfgang Kastner

Automation Systems Group
Institute of Automation
Vienna University of Technology

www.auto.tuwien.ac.at/knx

AUTOMATION
SYSTEMS
GROUP
TU
WIEN

Abstract

This paper presents an overview on the use of wireless technologies in home and building automation (HBA). Benefits of applying wireless technologies are summarized. Requirements specific to the field and particular challenges to be faced and solved by these technologies are discussed. This includes the security concerns evolving with the integration of wireless devices in HBA installations. The key contenders Z-Wave, EnOcean, KNX RF, and IEEE 802.15.4/ZigBee are presented. Specifics of each network protocol are pointed out. Finally, a KNX/IEEE 802.15.4 tunneling bridge which can act as a secure, wireless, transparent KNX/EIB repeater is presented.

References

[AES] NIST, "Advanced Encryption Standard," http://www.nist.gov/aes

[EIBsec] W. Granzer, W. Kastner, G. Neugschwandtner, and F. Praus, "Security in Networked Building Automation Systems," Proc. 6th IEEE WFCS, pp. 283 - 292, 2006

[EnO] F. Schmidt, "Wireless Sensors Enabled by Smart Energy – Concepts and Solutions," EnOcean GmbH, http://www.enocean.com

[IEEE] IEEE, "IEEE 802.15.4," 2003, http://standards.ieee.org/getieee802/download/802.15.4-2003.pdf

[IP802] G. Montenegro, N. Kushalnagar, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks," Internet-Draft, 2006, http://www.ietf.org/internet-drafts/draft-ietf-6lowpan-format-04.txt

[KNX] Konnex Association, "KNX Specification," Version 1.1, 2004

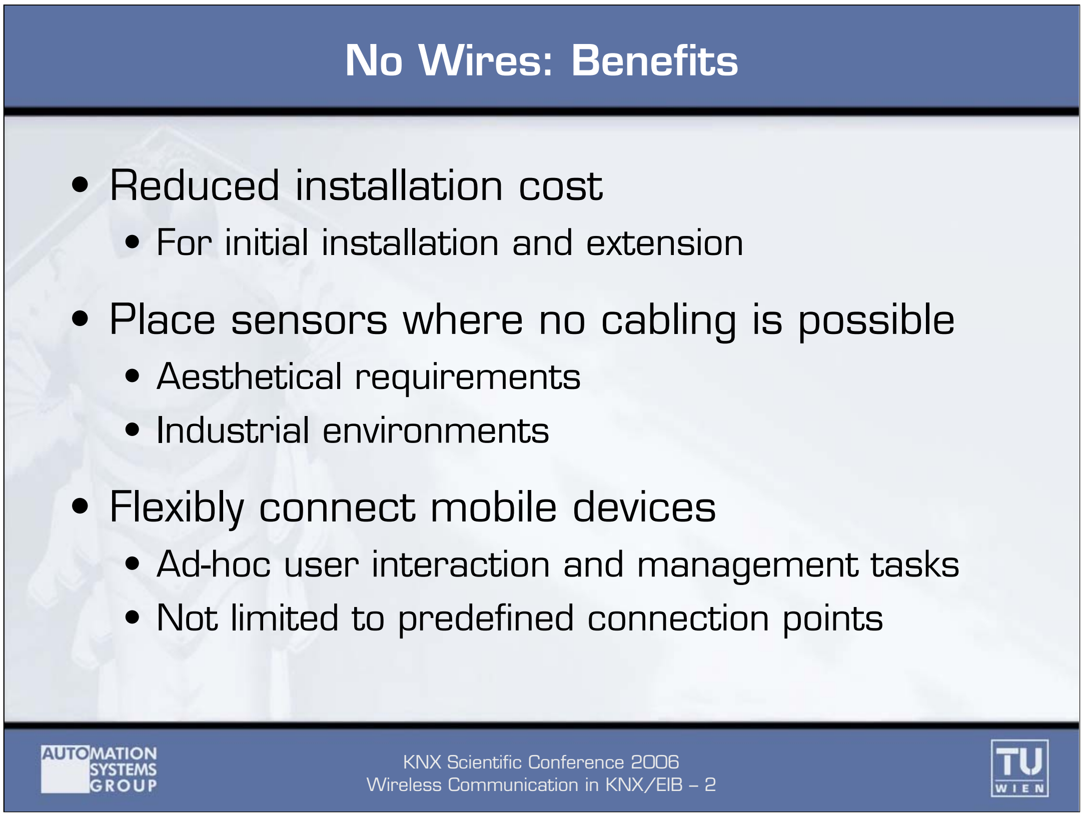
[Mill] B. Grohmann, "Milliardenmärkte durch drahtlose Kommunikation", funkschau 22/2005, http://www.funkschau.de/heftarchiv/pdf/2005/fs22/fs_0522_s16.pdf

[RFCN] A. Gupta, M. R. Tennefoss, "Radio Frequency Control Networking: Why Poor Reliability Today Hampers What Could Be a Viable Technology in the Future," Echelon Doc.# 005-0171-01B, Echelon Corp., 2005, http://www.echelon.com/support/documentation/documents/005-0171A_RF_White_Paper.pdf

[ZIG] ZigBee Alliance, "Zigbee Specification,"Version 1.0, 2004

[Z-Wave] Zensys A/S, "Z-Wave System Design Specification: Z-Wave Protocol Overview," Document Part # 903100105, 2005

[ZHome] T. Jorgensen, N. T. Johansen, "Z-Wave as Home Control RF Platform," Zensys A/S, 2005, http://www.zen-sys.com/media.php?id=321



No Wires: Benefits

- Reduced installation cost
  - For initial installation and extension
- Place sensors where no cabling is possible
  - Aesthetical requirements
  - Industrial environments
- Flexibly connect mobile devices
  - Ad-hoc user interaction and management tasks
  - Not limited to predefined connection points

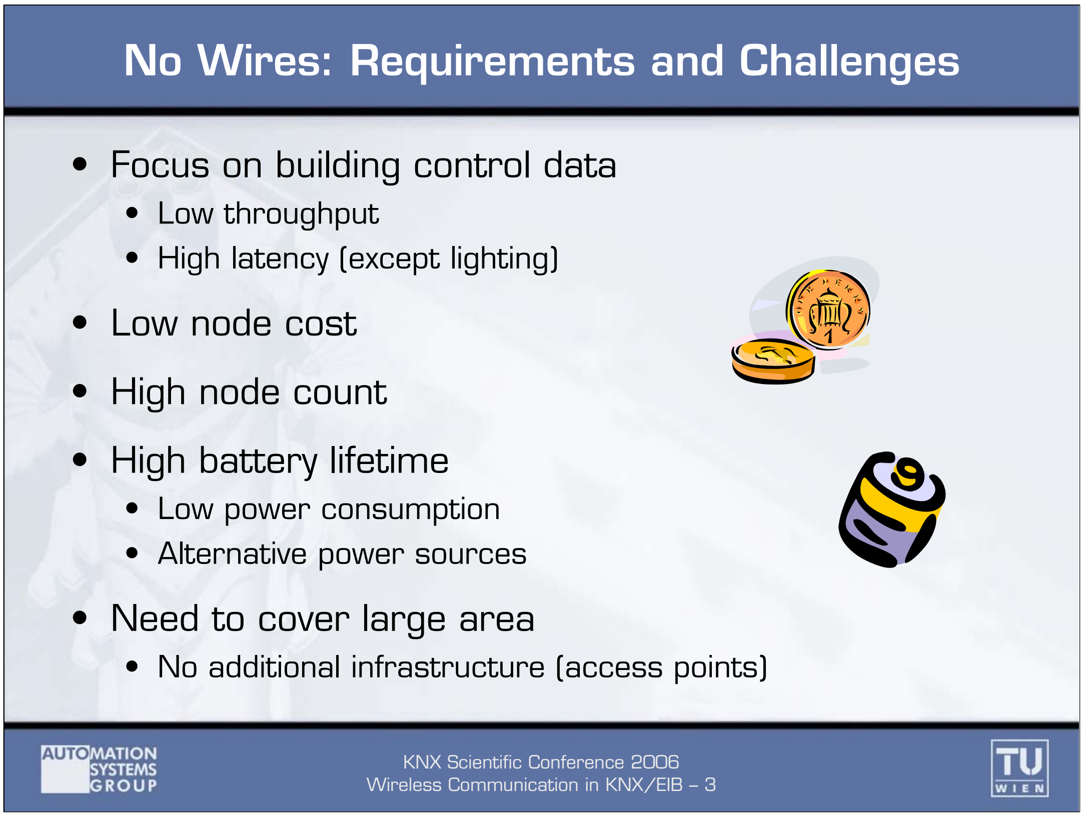
KNX Scientific Conference 2006
Wireless Communication in KNX/EIB – 2

The use of wireless technologies in home and building automation (HBA) offers several advantages. First, installation costs are significantly reduced since no cabling is necessary. This is especially advantageous when, due to new or changed requirements, extension of the network is necessary. Wired solutions require conduits or cable trays, whereas wireless nodes can be easily added. This makes wireless installations a seminal investment.

Wireless technology also allows to place 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, strong electromagnetic interference may be harmful to the nodes. Long cables are also prone to building up differences in electrical potential, which – while harmless to network devices and users – may generate sparks and thus are unacceptable safety hazards in explosive environments (unless expensive protective measures are taken).

With wireless networks, associating mobile devices such as PDAs and Smartphones with the automation system becomes possible everywhere and at any time, as a device’s exact physical location is no longer crucial for a connection (as long as the device is in reach of the network). A typical example is an engineer who connects to the network, performs a particular management task, and disconnects after having finished the task.

For all these reasons, wireless technology is not only an attractive choice in renovation and refurbishment, but also for new installations.



No Wires: Requirements and Challenges

- Focus on building control data
  - Low throughput
  - High latency (except lighting)
- Low node cost
- High node count
- High battery lifetime
  - Low power consumption
  - Alternative power sources
- Need to cover large area
  - No additional infrastructure (access points)

AUTOMATION SYSTEMS GROUP

KNX Scientific Conference 2006
Wireless Communication in KNX/EIB – 3

TU WIEN

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

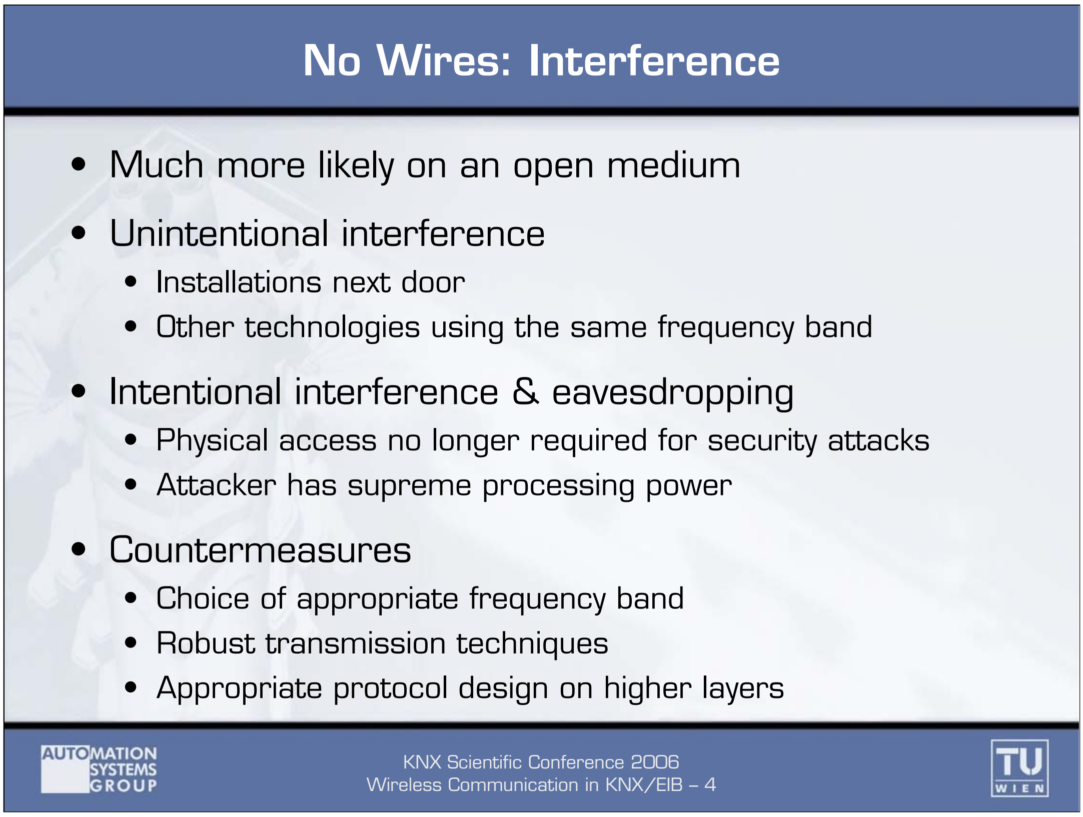
However, the market requires this performance to be delivered at low system cost compared to, e.g., industrial automation. Hundreds of nodes may be needed to provide automation for a building, so every single node has to be as cheap as possible to make the investment sensible.

Going wireless adds (or tightens) another constraint. For maximum benefit, all wires have to be cut – including power wires. Due to the high node count in the system, having to change or charge the batteries of each wireless device every few days is not feasible.

Thus, measures in hard- and software must be taken to achieve battery lifetimes of at least several months. The goal of minimizing power consumption also affects the design of the communication protocol. For example, it has to allow nodes to enter power-saving sleep modes as often as possible. It could even allow sensor nodes entirely without radio receivers.

Another challenge lies in the fact that devices of a building automation system are dispersed over large areas. Since transceivers must not consume too much power, they cannot be built with a transmission range sufficient for sensors to reach associated controllers or actuators directly. Also, they cannot rely on an infrastructure of access points and a wired backbone network (or particularly sensitive receivers) for reasons of cost.

The high node count of building automation systems comes to help here, as it allows to employ mesh networking schemes. 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).



No Wires: Interference

- Much more likely on an open medium
- Unintentional interference
  - Installations next door
  - Other technologies using the same frequency band
- Intentional interference & eavesdropping
  - Physical access no longer required for security attacks
  - Attacker has supreme processing power
- Countermeasures
  - Choice of appropriate frequency band
  - Robust transmission techniques
  - Appropriate protocol design on higher layers

AUTOMATION SYSTEMS GROUP

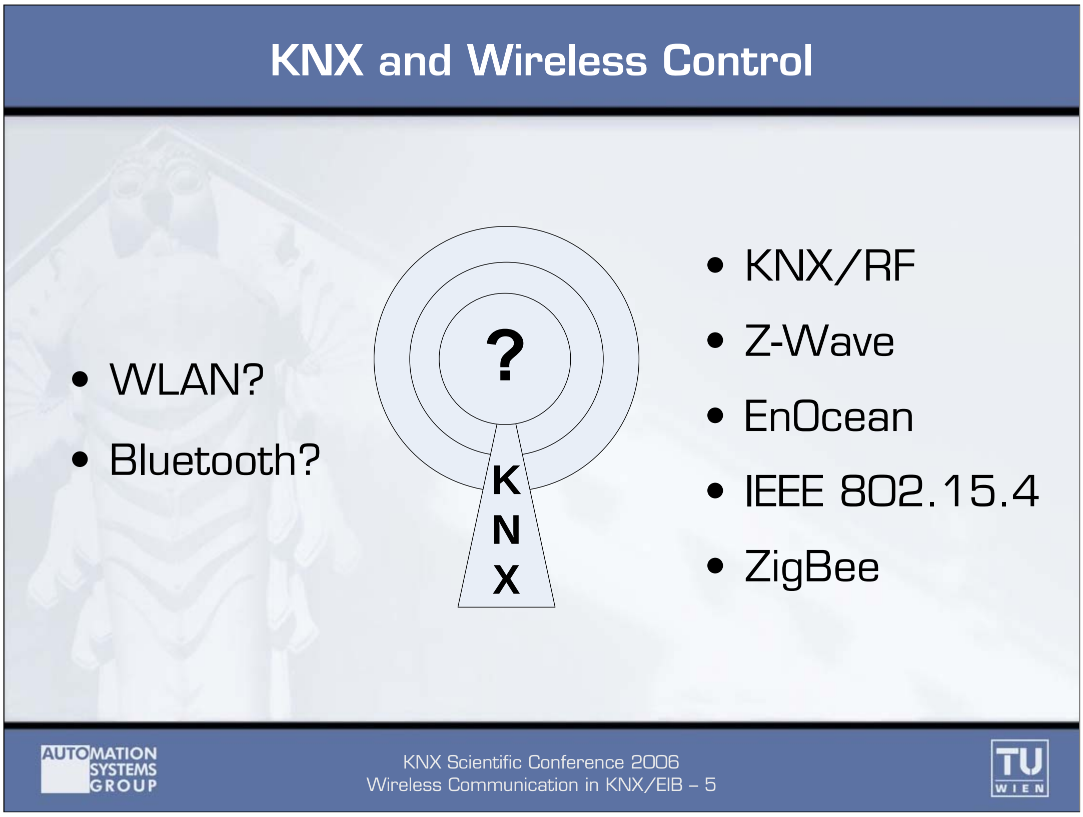
KNX Scientific Conference 2006
Wireless Communication in KNX/EIB – 4

TU WIEN

Wireless systems have to address the particular challenge that 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 license-free ISM (Industrial, Scientific, Medical) frequency bands, a variety of wireless technologies from garage door openers to baby monitors are competing for access to the medium, all using different access control strategies. These bands also accommodate devices creating radio frequency (RF) emissions merely as a by-product of their intended use, such as microwave ovens (which operate at 2.4 GHz). 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. Security attacks such as eavesdropping and replaying no longer require access to a medium buried within walls or ceilings. Attackers now can take over unsecured systems without ever having entered the building. As an additional difficulty, protocol security features such as cryptographic algorithms are limited by the requirement of low power consumption in the nodes – a limitation the attacker does not face.

To minimize interference, wireless applications should select a frequency band whose regulations best match their communication characteristics. The maximum allowable transmission power and duty cycle are key parameters here. Also, robust modulation and transmission techniques can for example spread the signals over a larger part of the available frequency spectrum, reducing the effects of narrow band interference. These measures must be complemented by appropriate protocol design on higher layers. This includes methods like acknowledged transmissions or automatic retransmission to increase the reliability of transmissions. Especially security critical applications like surveillance, access control, and alarm systems also require protocol support for authentication, encryption, message integrity, and replay protection. However, all this must be achieved while meeting the requirement of low per-node costs.



KNX and Wireless Control

- WLAN?
- Bluetooth?

- KNX/RF
- Z-Wave
- EnOcean
- IEEE 802.15.4
- ZigBee

AUTOMATION SYSTEMS GROUP

KNX Scientific Conference 2006
Wireless Communication in KNX/EIB – 5

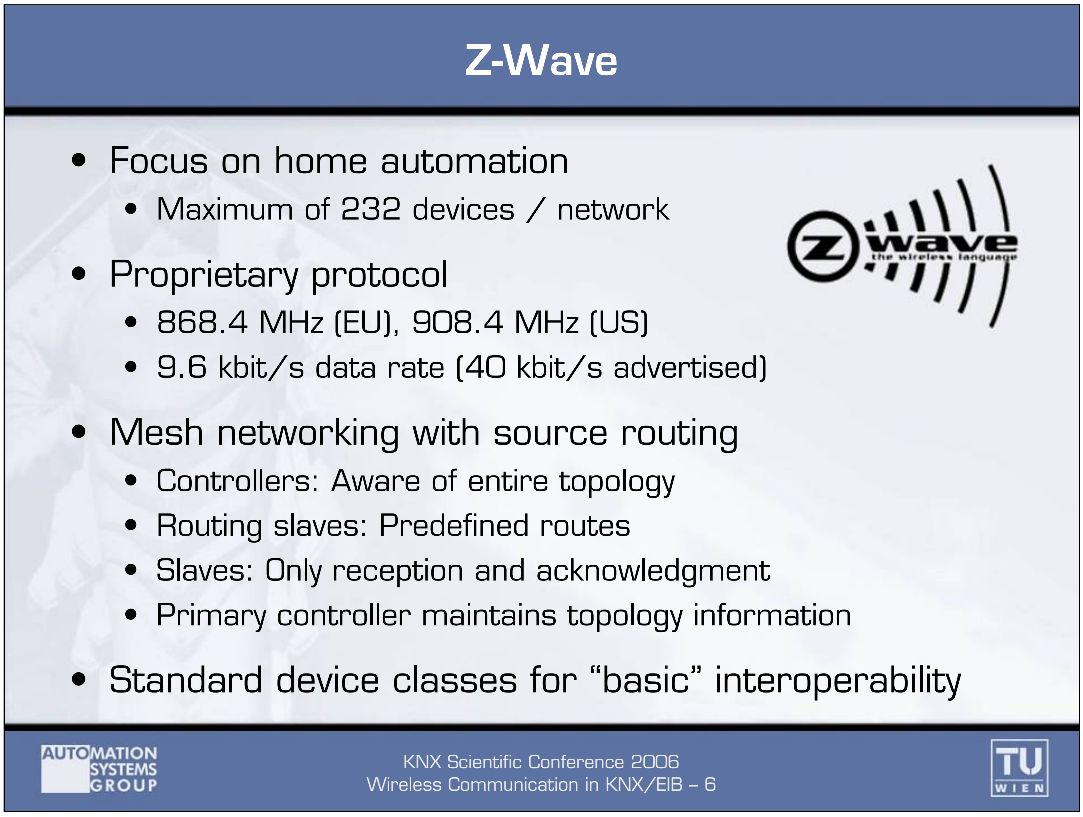
TU WIEN

Although KNX already has its custom RF extension, this should not keep us from having a look at other wireless technologies and considering possible synergies. This paper deals specifically with control networking, that is, extending KNX with wireless sensors, actuators and controllers. This rules out popular contenders from the beginning, in particular Wireless LAN (IEEE 802.11) and Bluetooth, since they cannot support the required battery lifetimes. They also do not provide the required area coverage (without resorting to wired access points). Their network stacks contain some features like security methods which would be useful also in HBA, but make it hard to reach the goal of low cost per node due to their complexity.

WLAN and Bluetooth operate in the 2.4 GHz ISM band which allows them to support the data rates required for media streaming. This band also has the big advantage of being available license-free almost worldwide. However, this also means it is excessively crowded. 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. For license-free communication, the ISM bands in the 900 MHz region are of particular interest. Unfortunately, their frequency ranges differ in Europe (863-870 MHz) and the USA (902-928 MHz). However, they are close enough to allow a single transceiver design which can be adapted by adjusting the oscillator only.

Although narrower than its US counterpart, the European 863-870 MHz range is particularly attractive since it is well regulated. For example, channel-hogging audio applications such as 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.

In the following, a selection of relevant wireless control networking technologies applicable in home and building automation is presented.



Z-Wave

- Focus on home automation
  - Maximum of 232 devices / network
- Proprietary protocol
  - 868.4 MHz (EU), 908.4 MHz (US)
  - 9.6 kbit/s data rate (40 kbit/s advertised)
- Mesh networking with source routing
  - Controllers: Aware of entire topology
  - Routing slaves: Predefined routes
  - Slaves: Only reception and acknowledgment
  - Primary controller maintains topology information
- Standard device classes for “basic” interoperability

AUTOMATION SYSTEMS GROUP

KNX Scientific Conference 2006
Wireless Communication in KNX/EIB – 6

TU WIEN

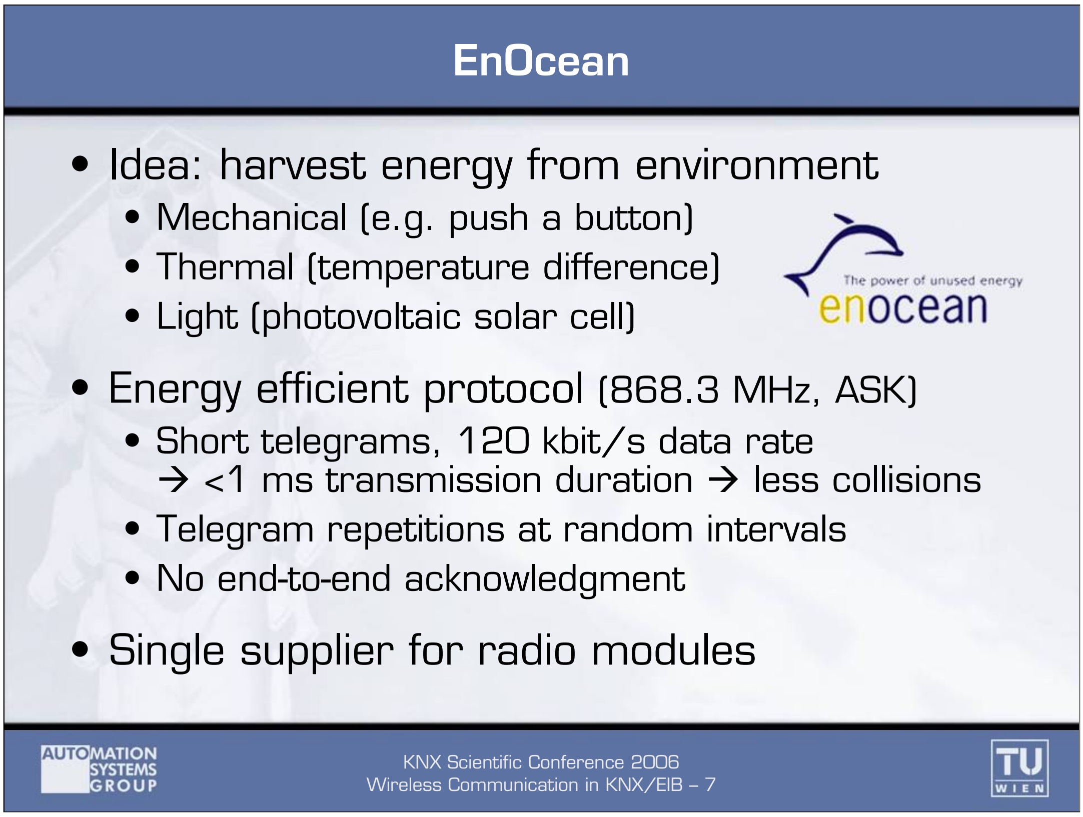
The Z-Wave protocol [Z-Wave, ZHome] was developed with an explicit focus on home control applications. Z-Wave operates at 908.42MHz +/- 12kHz in the US and 868.42MHz +/- 12kHz in Europe, using FSK (frequency shift keying) modulation. The RF data rate is 9.6 kbit/s (with a raise to 40 kbit/s advertised). A single network may contain up to 232 devices. Higher counts can only be obtained by bridging networks.

Z-Wave uses a mesh networking approach with source routing, which means that the whole route is determined already at the creation of the frame in the sender. Therefore, only devices which are aware of the entire network topology can send ad-hoc messages to any destination. Such devices are termed controllers. Another device class, routing slaves, can send unsolicited messages to a number of predefined destinations. The required routes are downloaded by a controller to the routing slave (e.g., a motion sensor) 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 (e.g., a dimmer) 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.

Medium access control involves carrier sensing for collision avoidance with random back-off delays. End-to-end acknowledged unicast and unconfirmed multicast and broadcast communication is supported. To allow basic interoperability in multi-vendor systems, device class specifications define sets of mandatory, recommended, and optional commands. Self-association based on matching command definitions is advertised. There is currently only a single source for Z-Wave silicon: Zensys' mixed-signal ICs containing the transceiver, an 8051 microcontroller core, a Triac controller with zero crossing detection and an optional 3DES encryption engine. The microcontroller hosts both the Z-Wave protocol and the application software.

The protocol and device class specifications are not freely available, neither are the IC manuals. The material released to the public leaves many aspects obscure (for example, the self-healing, self-organization and security properties).



EnOcean

- Idea: harvest energy from environment
  - Mechanical (e.g. push a button)
  - Thermal (temperature difference)
  - Light (photovoltaic solar cell)
- Energy efficient protocol (868.3 MHz, ASK)
  - Short telegrams, 120 kbit/s data rate
    → <1 ms transmission duration → less collisions
  - Telegram repetitions at random intervals
  - No end-to-end acknowledgment
- Single supplier for radio modules

The power of unused energy
enocean

AUTOMATION SYSTEMS GROUP

KNX Scientific Conference 2006
Wireless Communication in KNX/EIB – 7

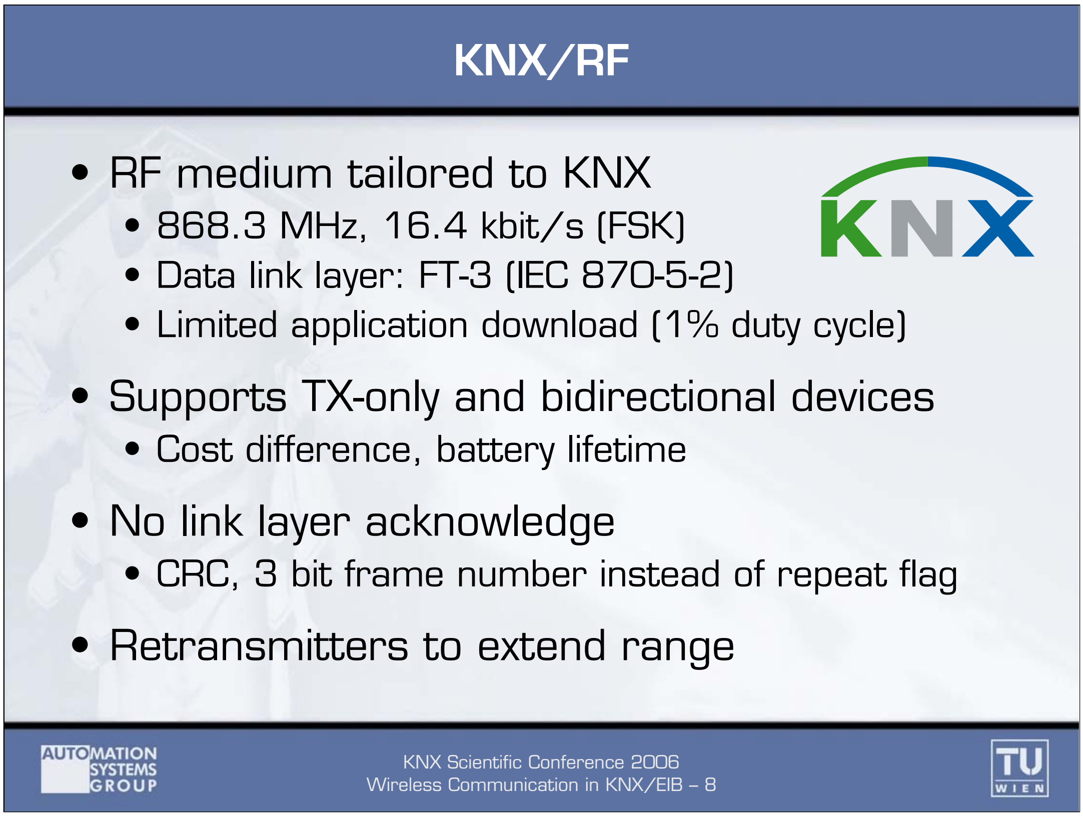
TU WIEN

The key idea behind EnOcean [EnO] is to harvest enough energy from the environment to power a wireless sensor node long enough to collect all sensor data and transmit a telegram. This results in a significant reduction in maintenance effort, as there are no more batteries in wireless sensors that need to be replaced. Instead, electricity is provided by piezoelectric elements, thermocouples (not yet implemented) or solar cells.

This concept could be realized thanks to recent technological advances such as efficient energy conversion, low power electronic circuits and reliable yet energy efficient radio transmission. These were brought together with a proprietary communication protocol highly optimized for energy saving. Messages are only a couple of bytes long (with a maximum payload of 6 bytes) and are transmitted at the comparatively high data rate of 120 kbit/s. Additionally, strategies such as not transmitting leading zeros are implemented. Thus, transmission takes less than 1 ms. EnOcean uses ASK (amplitude shift keying) modulation and a novel RF oscillator that can be switched on and off in less than 1 µs. Thus, the oscillator can be switched off at every "zero" Bit transmission, further reducing energy consumption.

The short frame transmission duration results in a low statistical probability for collisions. In addition, frame transmissions are repeated three times. The delay between repetitions is varied at random to reduce the influence of periodic interference signals. The protocol cannot increase transmission reliability by means of end-to-end acknowledgments since battery-less transmitter modules do not contain a RF receiver. The low collision probability is also presented as a key argument that the protocol will scale towards networks with a large number of nodes.

There is only one supplier of EnOcean radio modules. There are currently 4 radio telegram types (corresponding to the available transmitter modules) identifying various combinations of Boolean and 8-bit integer values, ensuring a basic level of interoperability. Documentation for these modules is freely available, but only allows guesses at the radio protocol. Although occasionally advertised, no security mechanisms appear to be included.



KNX/RF

- RF medium tailored to KNX
  - 868.3 MHz, 16.4 kbit/s (FSK)
  - Data link layer: FT-3 (IEC 870-5-2)
  - Limited application download (1% duty cycle)
- Supports TX-only and bidirectional devices
  - Cost difference, battery lifetime
- No link layer acknowledge
  - CRC, 3 bit frame number instead of repeat flag
- Retransmitters to extend range

KNX Scientific Conference 2006
Wireless Communication in KNX/EIB – 8

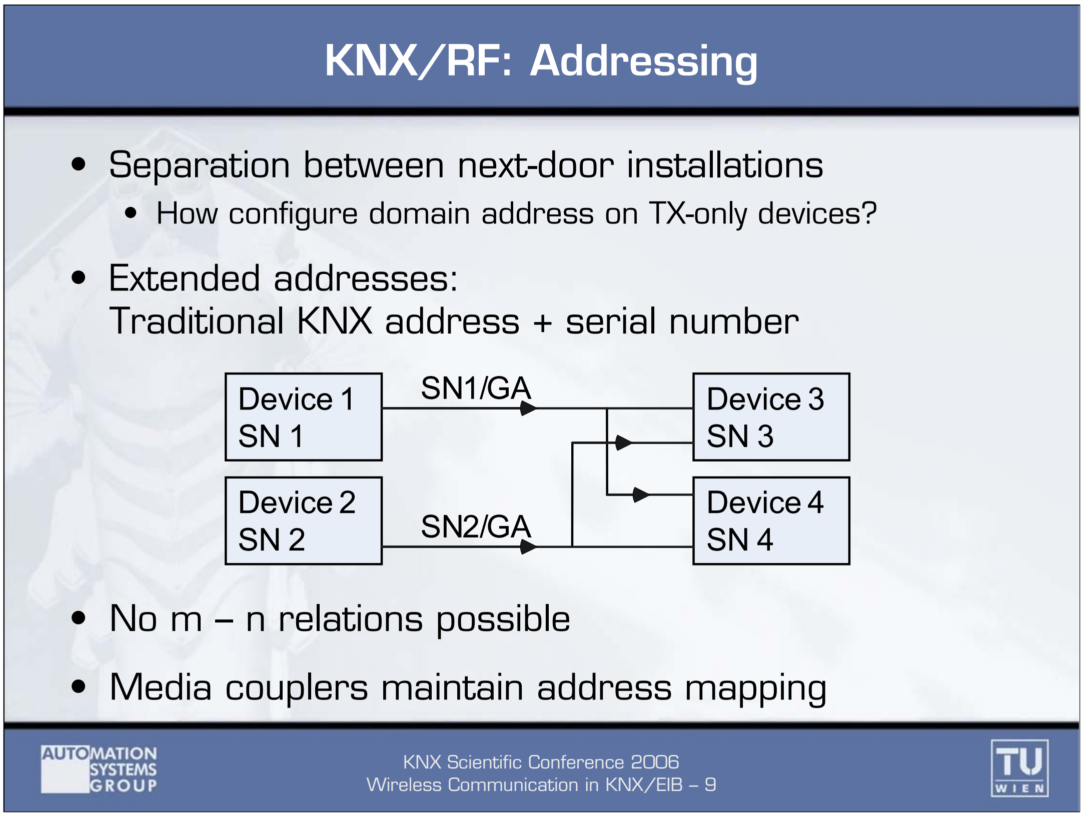
In addition to the twisted-pair and power line media, a wireless transmission medium called KNX RF has been specified in Supplement 22 of the KNX Specification 1.1 [KNX]. KNX RF operates at 868.3 MHz +/- 40-80 kHz using FSK modulation at a data rate of 16.4 kbit/s. The data link layer uses the FT-3 protocol defined in IEC 870-5-2. The bottom two layers of KNX RF were defined jointly with the wireless meter readout standard EN 13757-4:2005.

As a trade-off between functionality and the goals of low power consumption and low cost, KNX RF allows unidirectional (transmit-only) devices in addition to conventional bidirectional ones. Eliminating the receiver extends the battery lifetime of sensors as well as making them cheaper, also because only a subset of the protocol stack has to be implemented. On the other hand, it has the drawback that these devices cannot be configured via the network. This also excludes the possibility of downloading applications. Application download is however also significantly impaired for bidirectional devices due to the 1% duty cycle limitation which is in effect for the used frequency band. Current KNX RF devices focus on the Easy configuration modes, where this restriction is less relevant.

KNX RF does not use link layer acknowledgments for a couple of reasons. First of all, transmit-only devices would not be able to receive acknowledgments. Also, acknowledgments would have to include a unique identification of their sender to be meaningful. This applies to multicasts in particular, but also in general since on an open medium data frames and acknowledgments of multiple individual transmissions may be mixed up. Instead of adding this overhead, KNX RF suggests implementing end-to-end acknowledgments at the application level where required.

To detect and recover from transmission errors, KNX RF frames contain a CRC with hamming distance 6. The repeat flag available 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. Retransmitters resend all frames they receive. To avoid resending a particular frame multiple times, a history list is used. In this list, the serial number (SN) and the LFN of each received frame are stored. If the SN and LFN of a received frame are already in the history list, the frame is not relayed but discarded.



KNX/RF: Addressing

- Separation between next-door installations
  - How configure domain address on TX-only devices?
- Extended addresses:
  Traditional KNX address + serial number

- No m – n relations possible
- Media couplers maintain address mapping

KNX Scientific Conference 2006
Wireless Communication in KNX/EIB – 9

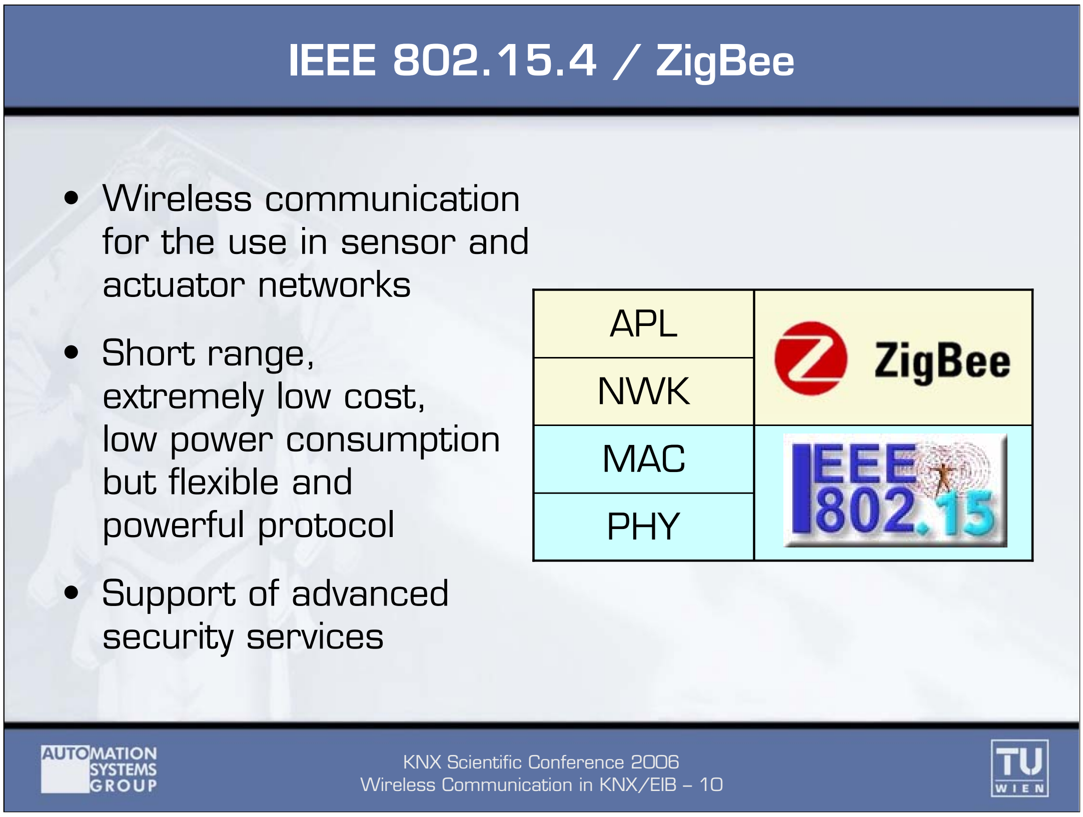
Due to the nature of wireless communication and the support of transmit-only devices, KNX RF uses its own addressing scheme which is different from (although similar to) the standard KNX addressing scheme. Since RF is an open medium, the address spaces of neighbouring installations would interfere with each other. Therefore it has to be guaranteed that each KNX RF installation has its own address space. For the Powerline medium, this was ensured by adding a 16 bit domain address that identifies the installation. This was not possible for KNX RF, since transmit-only devices cannot receive the domain address via the network and entering it manually would be unfeasible. (Moreover, it would be unclear which device should maintain this identifier in a distributed configuration approach.)

Instead, extended addresses are used. An extended address is defined as the combination of the traditional KNX address and the serial number (SN) of the device. Since the SN is 6 octets long, an extended address uses 8 octets. Due to the uniqueness of the SN, 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 neighbouring installation. Since the SN is already unique, the traditional 16 bit part of extended individual addresses is always 05FF.

A drawback of this addressing scheme is that m – n relations are no longer 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. Therefore, only 1 – n relations are possible.

An advantage of the exclusive use of extended addresses can also be found in the fact that it provides an additional barrier for security attacks due to the vastly increased address space. An attacker has to figure out the 48 bit SN of a device before injecting forged frames, which is impossible by brute force. Nevertheless, an experienced adversary can simply listen in to the packets transmitted via KNX RF and extract the serial number contained in clear in every message.

Because different addressing schemes are used in KNX and KNX RF, media couplers are not only needed for physical interconnection. They also provide the necessary mapping between the different address spaces which has to be set up during system configuration.



IEEE 802.15.4 / ZigBee

- Wireless communication for the use in sensor and actuator networks
- Short range, extremely low cost, low power consumption but flexible and powerful protocol
- Support of advanced security services

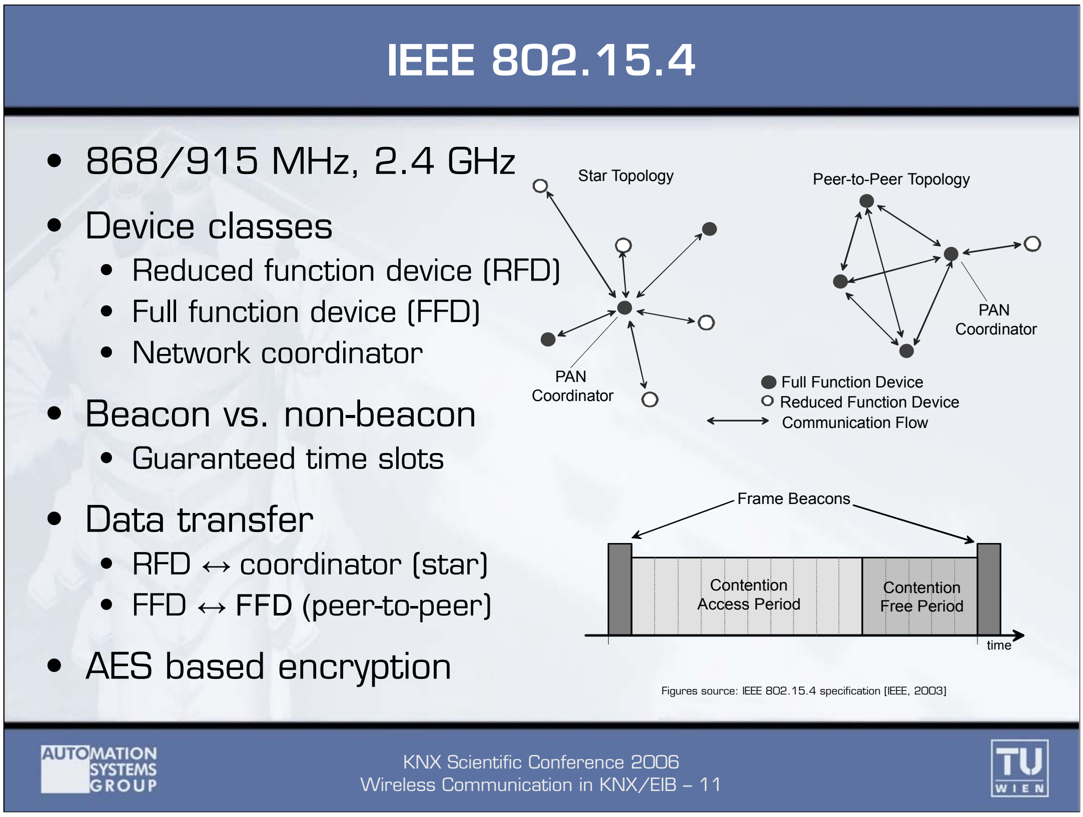
APL NWK	ZigBee
MAC PHY	IEEE 802.15

KNX Scientific Conference 2006
Wireless Communication in KNX/EIB – 10

KNX RF does not provide any security mechanisms. Since the transmitted data are neither encrypted nor an integrity check is performed, KNX RF cannot fulfil the high demands of security critical applications. Therefore, alternative technologies have to be used for these kinds of applications.

Two wireless standards which fulfil the requirements of the home and building automation domain are IEEE 802.15.4 [IEEE] and ZigBee [ZIG]. The focus of IEEE 802.15.4 and ZigBee is to provide general purpose, easy-to-use and self-organizing wireless communication for low cost and low power embedded devices. These technologies were designed for the use in actuator and sensor networks, including the HBA domain. The used protocol is compact yet flexible and powerful enough to meet relevant demands of these applications. A variety of manufacturers provides 802.15.4/ZigBee silicon, including systems-on-chip.

ZigBee is specified on top of IEEE 802.15.4. While IEEE 802.15.4 defines the physical and the MAC layer, ZigBee only adds network (NWK) and application (APL) layers. Strictly speaking, 802.15.4 is therefore an entirely independent protocol. Actually, applications and protocols can be (and are) realized on top of IEEE 802.15.4 that have nothing to do with ZigBee. Practically, however, the two standards are closely related to each other. They are not only complementary, but have mutually influenced the development of each other.



IEEE 802.15.4

- 868/915 MHz, 2.4 GHz
- Device classes
  - Reduced function device (RFD)
  - Full function device (FFD)
  - Network coordinator
- Beacon vs. non-beacon
  - Guaranteed time slots
- Data transfer
  - RFD ↔ coordinator (star)
  - FFD ↔ FFD (peer-to-peer)
- AES based encryption

Figures source: IEEE 802.15.4 specification [IEEE, 2003]

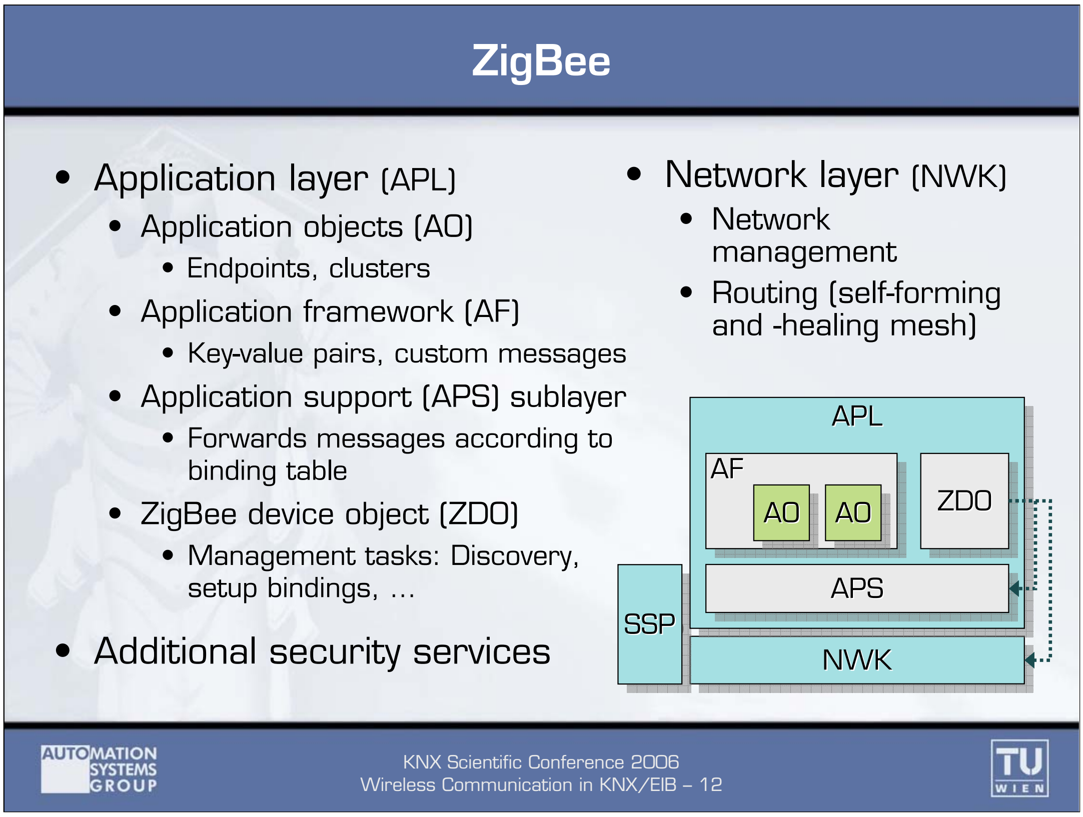
KNX Scientific Conference 2006
Wireless Communication in KNX/EIB – 11

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). Different PSK (phase shift keying) modulation types are used for the sub-GHz bands and the 2.4 GHz band, all use DSSS (direct sequence spread spectrum). System designers can choose the must suitable frequency for the application.

IEEE 802.15.4 classifies devices as Full Function (FFD) and Reduced Function devices (RFD) according to the complexity of the protocol stack. As shown in the Figure, each network segment which is referred to as Personal Area Network (PAN) has exactly one special FFD called the PAN coordinator. These coordinators are responsible for the network management (e.g., address assignment) as well as for providing information about the network (e.g., PAN identifier). While FFDs can communicate in peer to peer fashion, RFDs can only communicate with coordinators, resulting in a star topology. Coordinators can act as PAN bridges, resulting in a topology referred to as "clustered stars".

IEEE 802.15.4 defines two different kinds of PANs: beacon enabled and non-beacon enabled networks. In a beacon enabled network, a superframe structure is used. A superframe is bounded by so called network beacons which are sent by the PAN coordinator periodically. A beacon includes detailed information about the PAN (e.g., the PAN identifier). 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). Additionally, the PAN coordinator can assign guaranteed time slots (GTSs) to a device. These GTSs appear at the end of the superframe (Contention Free Period) and can be used by low-latency applications. In a non beacon enabled network, the coordinator does not send a beacon. Therefore, 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 at the data link layer which rely on AES [AES]. These are access control, message confidentiality, message integrity and replay protection [IEEE].



ZigBee

- Application layer (APL)
  - Application objects (AO)
    - Endpoints, clusters
  - Application framework (AF)
    - Key-value pairs, custom messages
  - Application support (APS) sublayer
    - Forwards messages according to binding table
  - ZigBee device object (ZDO)
    - Management tasks: Discovery, setup bindings, …
- Additional security services

- Network layer (NWK)
  - Network management
  - Routing (self-forming and -healing mesh)

AUTOMATION SYSTEMS GROUP

KNX Scientific Conference 2006
Wireless Communication in KNX/EIB – 12

TU WIEN

The ZigBee specification is divided into three parts: network layer, application layer, and security services. The network layer (NWK) is responsible for enabling a self-forming and self-healing mesh network by providing appropriate routing services including route discovery and maintenance. It also includes mechanisms for joining and leaving a network. In addition, the NWK of a ZigBee coordinator can start a network and assign addresses to new participants following a distributed scheme.

The ZigBee application layer (APL) consists of the application support sub-layer (APS), the ZigBee device object (ZDO), and the application framework (AF) hosting the application objects (AO). The manufacturer-defined application objects incorporate the actual functionality of the device. Each AO forms an independent functional sub-unit and can be addressed via its endpoint number. AOs communicate via free form messages or by manipulating each other's state variables.

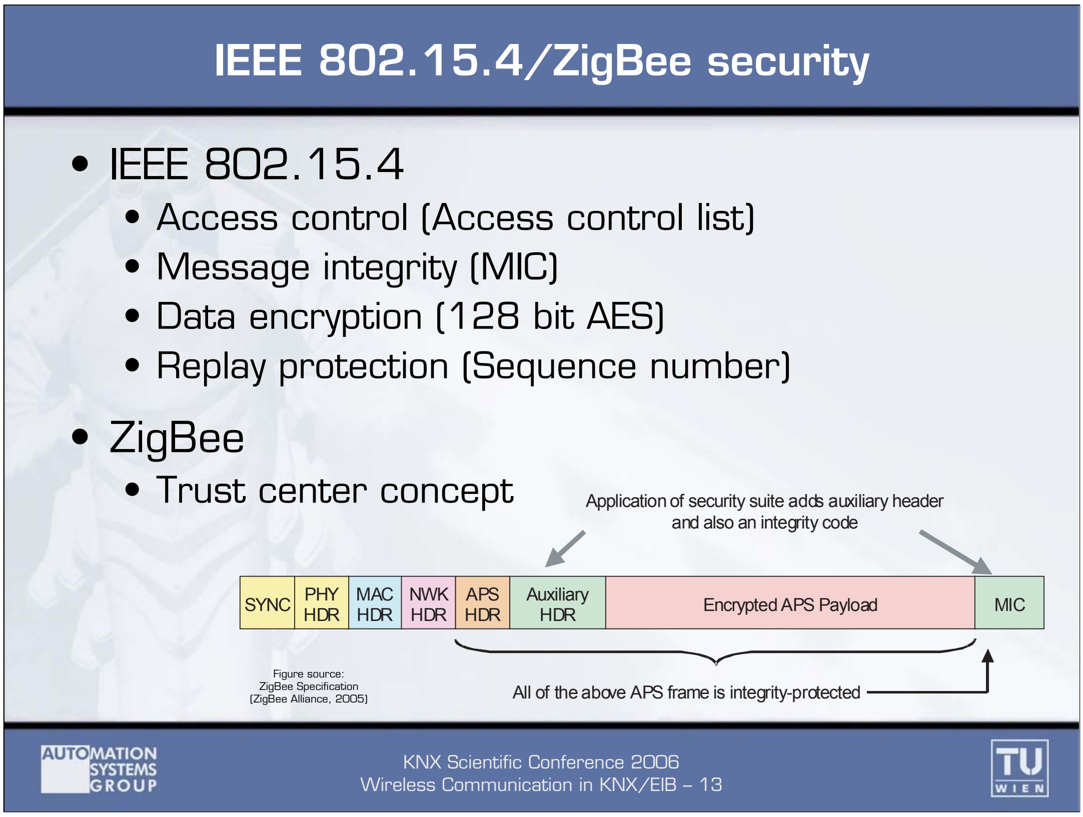
For the latter purpose, the AF provides the key value pair (KVP) service with acknowledged and unacknowledged get, set and event notification interactions. Standard data types are also defined. KVP allows tagged data structures using compressed XML (which a gateway can expand to textual representation for use by other systems).

The semantics of a free form message or a whole set of key-value pairs are encapsulated in its numeric cluster identifier. Cluster IDs thus allow accessing specific functionality within an AO.

The APS provides an interface between the NWK and the device and application objects. It is responsible for delivering messages to their destination endpoint and cluster. The APS of a coordinator maintains a binding table (which maps a source address/endpoint/cluster combination to one or more destination addresses and endpoints, keeping the cluster ID) and forwards messages accordingly.

The ZDO is a special application (residing at endpoint 0) that encapsulates management operations concerning APS, NWK, and other parts of the stack. These include discovering and joining a network, establishing bindings, and configuring security services (e.g., key establishment and authentication). The ZDO also handles device and service discovery. The services of the ZDO are available to the AOs via public interfaces.

Security mechanisms are integrated into all layers. A security service provider (SSP) handles tasks such as encryption which are common to all of them.



IEEE 802.15.4/ZigBee security

- IEEE 802.15.4
  - Access control (Access control list)
  - Message integrity (MIC)
  - Data encryption (128 bit AES)
  - Replay protection (Sequence number)
- ZigBee
  - Trust center concept

Application of security suite adds auxiliary header and also an integrity code
SYNC
PHY HDR
MAC HDR
NWK HDR
APS HDR
Auxiliary HDR
Encrypted APS Payload
MIC
All of the above APS frame is integrity-protected

Figure source: ZigBee Specification (ZigBee Alliance, 2005)

AUTOMATION SYSTEMS GROUP

KNX Scientific Conference 2006
Wireless Communication in KNX/EIB – 13

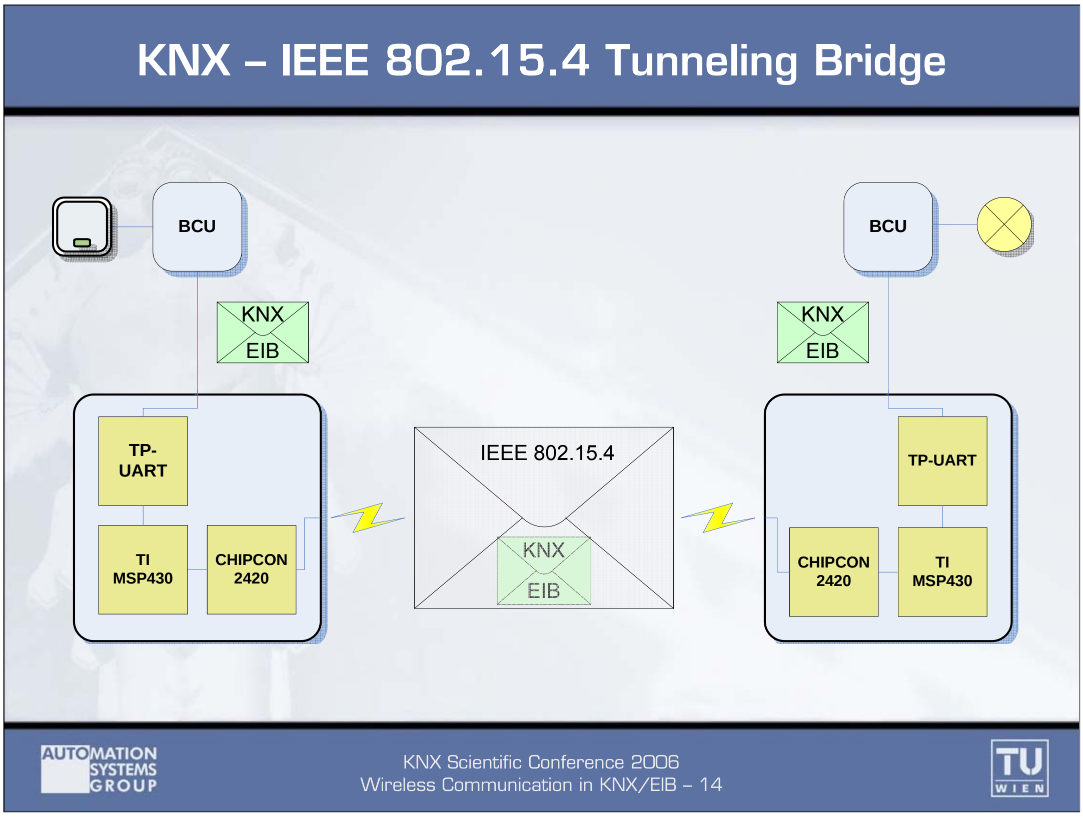
TU WIEN

IEEE 802.15.4 [IEEE] specifies its security mechanisms in the data link layer. Access control and message integrity are provided by means of adding a message authentication code (termed MIC, message integrity code) to outgoing frames. The MIC is a secure checksum of the message and is computed with the help of a secret key shared by the devices involved in the particular message exchange. Only if the MIC is correct an incoming frame will be accepted. Replay protection relies on adding a (typically monotonically increasing) sequence number to each frame. Incoming frames are only accepted if the sequence number is greater than the last one received. Finally confidentiality between sender and receiver is established by data encryption with the AES algorithm [AES]. Again, the symmetric key has to be shared between the communication partners.

802.15.4 radio ICs maintain an access control list (ACL) that allows to specify the combination of security mechanisms (called “suite”) and key to be used separately for every communication partner. In practice, however, a single key is typically shared by all devices in the network.

The use of shared (symmetric) keys is clearly a drawback of IEEE 802.15.4 security mechanisms. It poses problems when thinking of topics such as key distribution over unsecured networks and supporting the temporary association of mobile devices. Moreover, acknowledgement frames are always sent unencrypted and unauthenticated so that system designers cannot rely on them as a security measure.

ZigBee security leverages the mechanisms provided by IEEE 802.15.4 and complements them with essential administrative aspects such as key generation, distribution and administration. ZigBee introduces different keys for network or end-to-end security as well as the concept of a Trust Center, a node which is trusted by others to handle security related operations. In a ZigBee network, the Trust Center authenticates devices wanting to join, provides them with keys and offers functions for establishing network-wide and peer-to-peer secure connections. Normally, the role of the trust center is assumed by the ZigBee coordinator, but mobile devices take it over as well.



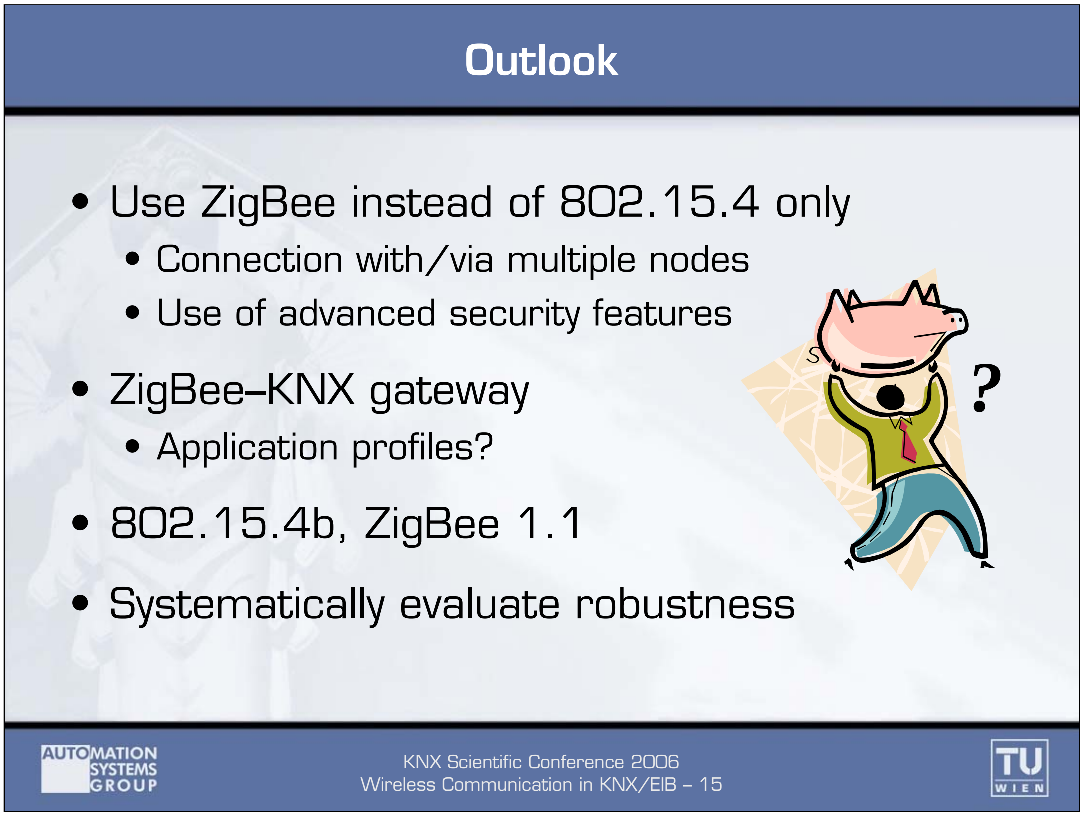
KNX – IEEE 802.15.4 Tunneling Bridge

KNX Scientific Conference 2006
Wireless Communication in KNX/EIB – 14

Our prototype implementation of a KNX/IEEE 802.15.4 tunneling bridge is comprised of three major parts. The TP-UART works as an interface between the KNX/EIB installation and a Texas Instruments MSP430 series microcontroller. The Chipcon 2420 RF transceiver is used for sending IEEE 802.15.4 frames in the 2.4 GHz band using a peer-to-peer, non-beacon network configuration. We chose the TI MSP430x149 because it is equipped with 2 USART interfaces (one is required for communication with the TP-UART, one for the Chipcon 2420) and supports different low power modes.

KNX/EIB frames are received via the TP-UART and handed over to the TI MSP430. The MSP430 application configures the Chipcon 2420 for IEEE 802.15.4 communication with the required parameters and enables its RF transceiver. IEEE 802.15.4 frames containing the unmodified KNX/EIB frame as payload are sent via the RF connection, received by the second (identical) tunneling bridge and are acknowledged by an ACK frame. KNX link layer acknowledgments are optional. The microcontroller at the receiving side extracts the KNX/EIB message and forwards it to the TP-UART that places it onto the second KNX/EIB segment. Simultaneous communication in both directions is possible.

Although the current implementation does not make use of any security mechanism, it establishes an excellent basis for extensions in that direction. First, only the tunneling connection could be secured by means of 802.15.4 security mechanisms. Such a solution would remain entirely transparent to the KNX/EIB devices. However, it does not provide protection against attacks on the KNX/EIB wired network. Such protection could for example be achieved by deploying EIBsec [EIBsec], which would be perfectly possible on this hardware platform.



Outlook

- Use ZigBee instead of 802.15.4 only
  - Connection with/via multiple nodes
  - Use of advanced security features
- ZigBee–KNX gateway
  - Application profiles?
- 802.15.4b, ZigBee 1.1
- Systematically evaluate robustness

AUTOMATION SYSTEMS GROUP

KNX Scientific Conference 2006
Wireless Communication in KNX/EIB – 15

TU WIEN

Regarding future directions, the tunneling bridge could utilize the ZigBee stack available on the Chipcon 2420 to make use of ZigBee protocol features such as flexible mesh networking and advanced security mechanisms (e.g., Trust Center).

Moreover, the same hardware platform could be used to implement a gateway between ZigBee and KNX/EIB. However, the required mapping between the respective data models is currently impossible since the ZigBee application profiles are not openly available.

It is also essential to keep an eye on the current development regarding 802.15.4 and ZigBee. Only recently, the 802.15.4b specification was published, including: additional sub-GHz PHY layers promising higher robustness and data rates; support for a shared time base; improvements of the security suite; making GTS support optional; more flexibility in the CSMA-CA algorithm; and reduced association time in non-beacon networks.

The ZigBee 1.1 specification, which has been finalized but is not yet publicly available, will take advantage of the developments in 802.15.4 and provide additional features such as device groups, targeted broadcasts, or over-the-air setup. It is also expected to address weaknesses in the security concept and the issue of the coordinator as a single point of failure. Another interesting direction is the use of IPv6 over 802.15.4 [IP802]. Further related technologies, such as NanoNET, also merit attention.

The robustness of wireless communication technologies with regard to interference is an important issue. However, existing reports and comparisons are typically biased and seldom take the differences between the US and European sub-GHz ISM bands into account [Mill, RFCN]. Conducting such comparisons on a sound, objective basis would provide important information to prospective users, but requires amounts of funding currently unavailable to us.