Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

CEESAR - Center of Excellence for
Embedded Systems Applied Research

EnerBee - Example of an Advanced Metering Infrastructure based on ZigBee

Rolf Kistler, Stefan Knauth and Alexander Klapproth
Lucerne University of Applied Sciences and Arts
CEESAR – Center of Excellence for Embedded Systems Applied Research
Technikumstrasse 21, 6048 Horw, Switzerland
{rolf.kistler, stefan.knauth, alexander.klapproth}@hslu.ch

Abstract

An advanced metering infrastructure (AMI) unites all the various metering devices of a building in one network and provides the metering data in real-time, locally and from remote. And it opens the door for advanced energy management features. This paper presents an AMI that utilises ZigBee to build up home area networks of connected metering devices. The work is conducted in the context of EnerBee, an industrial applied research project. EnerBee is partly influenced by the AMI group of the ZigBee Alliance and its efforts to create a Smart Energy application profile.
After a short glance at the motivation and history of AMI, high-level features as well as technical requirements are listed. We go through interesting topics relevant in order to build a prototype. Those include physical issues like transmission frequency and frequency agility up to the definition of device types and clusters in the Smart Energy Profile. Finally, we show an example of such a network and focus on how meters can be addressed and read out using existing metering application protocols.

I. Introduction

The term “Energy efficiency” has become increasingly popular nowadays. The demand for energy in the globalized world is continuously growing and with it the competition for the precious resources. A sustainable approach to face these global energy issues and their environmental consequences will incorporate strategies to save energy. Politicians and public authorities have put the topic on top of their schedule and the average consumer is willing to play his part (considering his shrinking wallet and without too much loss of comfort). New ideas and technical solutions are needed. The AMI is one of them.
Initially, energy utilities and meter manufacturers developed a technology of automatically collecting metering data on-site and transfer it to a remote central backend [1]. AMR (Automatic Meter Reading) was born. For the utility, it came with the benefits of simplified billing procedures, more accurate, up to date data and less employee trips as it replaced the manual meter reading and data tracking processes. And it increased the transparency of the personal energy usage for the customer. AMR has evolved and led to a more advanced solution. An AMI consists of a “two-way fixed network and associated systems for providing advanced metering data and energy management capability. And it provides the capabilities to improve data tracking above and beyond AMR with the goal of influencing energy usage” [2].
The Smart Meters of an AMI can be accessed and controlled from remote at any time. They are able to communicate among each other, record data and provide it in real-time, handle events and alarms, send diagnostic information, detect leaks or tampering, handle pricing information and come with extensive logging and monitoring features. Even more interesting

concerning the energy efficiency are load control and demand response[1] scenarios based on peak load detection and actual pricing information from the utility. Moreover, such an infrastructure opens the door for new services such as in-house energy visualisation terminals, prepayment, outage control, maybe even an energy "stock market".
Data communication from the customer to the utility happens over power line, wired DSL or the mobile technology GPRS (maybe WiMax could be an interesting alternative in some cases). Where already applied, the different meters within a house are connected via power line or dedicated wires (proprietary current loops, M-Bus etc.). The ZigBee Alliance has discovered the huge potential of connecting various types of meters delivering up to date data to utilities, technicians, customers and household appliances. It has identified Smart Metering as one of the most important applications for the ZigBee technology [3]. As a result, major players in the field have joined the alliance and formed the AMI/Smart Energy profile task group (AMI_PTG). The definition of the according profile is still work in progress.
In the reminder of the document, requirements and technical issues of such a ZigBee based AMI are discussed and possible solutions are laid out. The work has been done in the context of EnerBee, an industrial applied research project conducted together with Landis+Gyr. Landis+Gyr, headquartered in Zug Switzerland, is the global market leader in electricity metering and pioneer in advanced metering solutions. EnerBee's main goal is to build a "Reliable, monitored network infrastructure for wireless advanced metering devices". The project has defined ZigBee as base technology for the in house communication but was started before the AMI group had formed. So, at this stage, we are able to compare our initial thoughts with the ones of the official AMI group and draw conclusions for the project and the definition of the ZigBee profile, which are both still going on.

II. Requirements

In the introduction, the features of an AMI were mentioned. This chapter gives a rough overview over the requirements identified on different levels. Let's start with the business view and the most important ***high level features*** [4].

- **Metering**: Getting the information out of the meters is the core feature of any AMI. It should be possible to get metering data from multiple commodities such as electricity, gas, water, and thermal (sub metering, multi energy metering). The system should be flexible enough to support different measuring units and internationalisation. An AMI must provide state of the art measurement types including load profiles, summation etc. Further, metering data (consumption/production) should be available in real-time and recorded in a history for later use. Data can be retrieved locally on-site and from remote. The network incorporates mains powered and battery driven devices. Selected data can be accessed from the utility, a technician or the customer with sensible restrictions and privacy. And, last but not least: Legacy support for already available and powerful metering protocols must be assured.
- **Demand Response and Load Control**: As already mentioned this is ability of the system to control energy consuming and generating devices depending on inputs from the utility and/or the customer. This includes management and scheduling of multiple events, the ability to individually or simultaneously target specific groups of devices (HVACs, water heaters, lighting etc.), randomisation of start and end times and so on.
- **Pricing:** It shall be possible to distribute, visualise and process tariff based on the spot market prices for energy (real-time pricing) or special rates such as the much higher "Critical Peak Prices" etc. Smart Appliances are able to access this pricing information publicly and act accordingly. A flexible architecture supports different international

[1] In the ZigBee Smart Energy Profile these two terms are grouped under the term "Load Curtailment" and are differentiated as follows: "Typically in load control scenarios, the utility is allowed to take control of a device in a customer-premise based on some pre arranged agreement. In demand response, the customer is informed that demand needs to be reduced and can choose to act or not act on this information"

Requirement		Remarks
Reliability	Data	No data must be lost. This regards the over the air communication itself as well as metering data being collected or temporarily stored within network nodes.
	Availability	Metering data of all meters must be available > 90% of the time of a day.
	Robustness	Non-ZigBee active sources of interference in the ISM Band (microwave ovens, WLAN Access Points, Bluetooth devices,…) shall not lead to more than 5% data packets being retransmitted (given that its possible to achieve a distance of at least 3m between interfering devices).
	Latency	Response times to data requests should be < 10s.
	Durability	The system should be up and running autonomously for at least 10 years.
Physical Limitations	Range	The metering network shall be accessible up to 30 m distance away from the house it is installed (Drive-By).
	Penetration	Meters are often in cellars. It must be possible to get through a concrete wall of 20cm.
Ease of Use, Cost sensitivity	Acquisition	A communication unit or add-on shall cost no more than 10 Euros for a quantity of 100'000 pieces/year.
	Installation and Set-up	Set-up time of a new network node shall be <5 minutes. If possible, no additional on-site configuration shall be needed (plug and play). Simple tools shall help to set-up and form the network, find appropriate places for nodes, bind devices, initialise security settings and bring the network up.
	Operation and Maintenance	It should be possible to monitor the state of the network and the health of its nodes in real-time and diagnose and find errors (locally and remote).
Special Nodes	Mobile Nodes (Ad-Hoc)	The system needs to be prepared for nodes which dynamically join the network at any time and are moving around.
	Battery Nodes	The system shall be prepared for battery powered nodes. These nodes must work for around 10 years without replacing or recharging the battery (manually). The “Latency” requirement from above also applies this kind of nodes.
Security		Sensible data must be protected against tampering and plain text sniffing.
Standards Based		Communication between nodes must base on an open standard.

Table 1: Technical Requirements

units, currencies and a variety of rates, rate based services and multiple providers within the same system.

- **Customer Information Services:** Features like the distribution of simple informational text messages between devices or new types of devices such as special in-house units. The text messages allow informing the customer about energy usage alerts, errors, system states, billing information, rates, current energy consumption, value added services such as weather forecasts etc. In-house units visualise metering data and text messages and allow interaction of the customer with the load curtailment services.

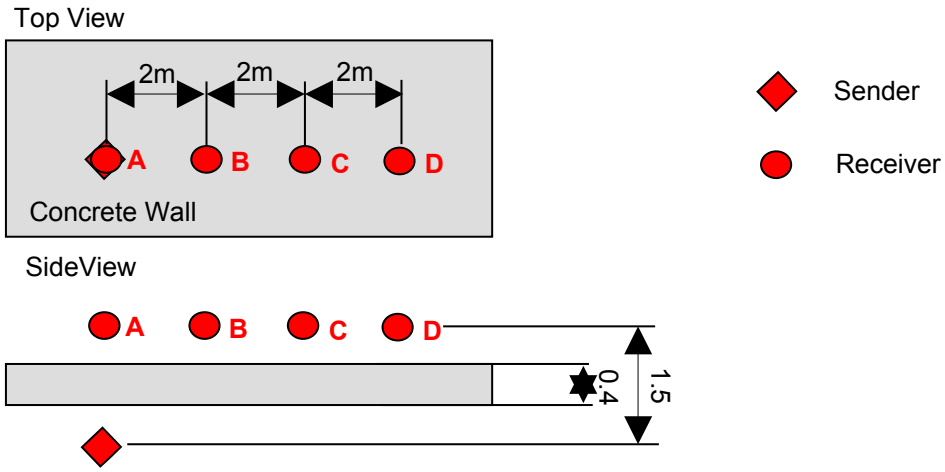

Figure 1: 868MHz/2.4GHz Tests, Building Situation

- **Mobile AMR/Commissioning:** Mobile AMR allows a mobile ad-hoc device such as a handheld/laptop (walk-by) or automobile mounted device (drive-by) to join the network and access metering data. Mobile devices may also host commissioning tools for technicians to set-up, monitor, diagnose and fix networks and nodes.

These features are one side of the story. But if an AMI shall be accepted by the customer, commercially successful and widely spread, serious technical challenges need to be met. For ZigBee, they involve some of the most criticised drawbacks of wireless solutions: Reliability, physical limitations, ease of use and security. Table 1 lists the technical requirements we pose on the AMI concerning the communication technology: It lies out of the scope of this paper to go through all the requirements stated above. However, the following sections will focus on selected topics we consider worth mentioning concerning our project.

III. Physical Issues

868 MHz vs. 2.4 GHz: One of the first questions coming up with ZigBee in the building is the ISM frequency band. Today, almost all of the (non-ZigBee) indoor wireless installations use frequencies bellow 1GHz (mostly 868 MHz in Europe and 915 MHz in the U.S.). Physical laws state that overall range and penetration decreases with the wavelength of the signal. A legitimate concern, especially regarding metering devices often located in cellar rooms. But today's state of the IEEE 802.15.4 specification and the implemented hardware show that using a frequency other than 2.4 GHz is not really an option. This has its well known reasons: 868MHz can only be used in Europe, 2.4GHz globally. So far there is only one channel available at 868 MHz, there are duty cycle restrictions, bigger antennas are needed etc. Vendors explain us that using ZigBee mesh routers and enough power one can extend the range beyond any limits even no matter what frequency… In the course of the project, we conducted basic measurements to form our own opinion. Picture 2 shows a graph with the attenuation for one specific scenario (sending through a 40 cm concrete wall). Shortly put, our measurements led us to the following statements:

- Both 868 MHz/0dBm and 2.4 GHz/0dBm senders penetrate a 40 cm concrete wall.
- Yes, 868 MHz waves are less absorbed through the concrete wall. In our case, the difference between the senders was around 15 dBm[2].
- In line of sight scenarios or scenarios were only a cement wall was in between, the differences were close to negligible.

[2] Although always asked by marketing personal it is very hard to give something like a rule of thumb about ranges, penetration etc. All we can say is that in that specific scenario on that specific time with specific hardware we gained that result and that were able to reproduce it.

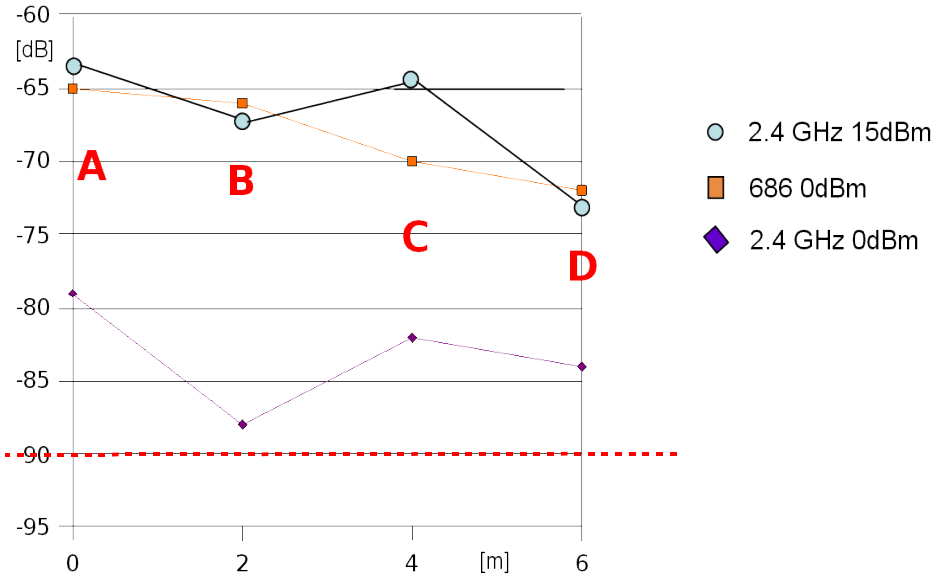

Figure 2: Example of 2.4 GHz transmission through a 40 cm concrete wall with 3 different transmitters. Red dotted line indicates the "critical Area", levels below -90 dB are not sufficient for reliable communication.

As our requirements were fulfilled with 2.4 GHz (and we wanted to use ZigBee), the issue was closed.

Frequency Agility: WLAN hotspots and other ISM band devices influence ZigBee devices. That's an undeniable fact [5][6]. How much is again very much depending on the scenario. We found (qualitative tests and show cases on exhibitions) that if the distance between the ZigBee receiver and the disturbing sender is big enough (several meters), ZigBee devices work just fine.
So far, ZigBee restricted itself to an energy scan of the coordinator when forming the network to find a channel that will stay the same for the lifetime of the network. If a more dynamic behaviour is wanted, one can implement his own channel selection scheme based on the IEEE802.15.4 API if access to the hardware is provided by the stack vendor. But as this scheme is not standardised, one loses ZigBee standards conformity[3]. The ZigBee Alliance has noted the gap. In the ZigBee PRO feature list the "Frequency Agility" first appeared as standard feature [7]. However, this frequency agility only goes as far as defining a standard API and messages to tell a device to change the channel. Sending these messages to tell them when to do change to what channel is still up to some kind of undefined control device.

In our example it is planned to implement such functionality to find out about the behaviour of the network. However, in the final system, the approach will probably be to provide tools and guidelines to easily find the proper installation spots, simple indicators to warn about missing network performance and simple procedures to find reasons for it (a new hotspot or opening of a steel door etc.). Overall, in the AMI scenario we don't assume that the channel needs to be changed within short time periods.

Transmission Power: Another value to be determined is the transmission power (and receiver sensitivity) to achieve the tasks at hand. Do we need power amplifiers (PA) to improve the range or are the out of the box ~0..7dBm of the most transceiver types enough? Is the much higher complexity and increased costs of PA designs worth the gain? Which devices in the network need more transmission power (and can cope with the drastically increased

[3] One option for a device that does not support the proprietary scheme is to include mechanisms to find out that the network it belongs to has changed the channel, scan again (on all channels or a specified set) and rejoin again on the new channel. That change will not be very fast, however.

Figure 3: WeBee and EtherBee Module Family of CEESAR

power consumption)? What is the maximum transmission power we can achieve with ZigBee (and still conform to the regulations)?

The last question remains somehow mysterious and depends on whom you ask. Our interpretation of the European laws [8][9] came up with ~15dBm, other sources go down to 10dBm. What's clear is that battery driven end devices and routers will not work 10 years with the power consumption of a 15dBm sender and the sizes of ZigBee (Smart Metering) messages.

We use various ZigBee module types. For most occasions (and all battery powered devices), 5dBm or less should do (including usage of range extenders). For special occasions - e.g. a central gateway unit - we've developed a module with up to 15dBm transmission power and improved receiver capabilities. Energy consumption is reduced by sending with just as much power as needed. As most chip vendors allow setting the transmission power of the chip dynamically, we try to find the ideal transmission power depending on the RSSI/LQI value of the incoming packets. We are not yet sure whether it's possible to use battery powered routers. Unfortunately, the unsynchronised ZigBee routers need to listen for traffic all the time and listening takes even more power than sending.

Hardware: [10] states, that "for annual volumes not well in excess of 25'000 pieces, the economics of a third party module approach are compelling". However, AMI environments, if successful, will even exceed this quantity.

So far, we have used third party modules for our tests. As we already produced our own designs in form of the WeBee family of ZigBee nodes [11], we intend to take a ZigBee Certified Platform (Transceiver + Software) and build our own hardware around it. We also look at directional antenna designs with the goal of improving the performance of drive-by nodes.

IV. Devices, Profiles, Clusters

Device Categories: A crucial question is what kind of devices or network members are taking part in an AMI? On the ZigBee network level it is clear: Each network consists of one coordinator and many end devices and routers. As for the application level, we've identified the following device categories:

- **Gateway:** A device with a ZigBee transceiver on one side and some kind of link to the remote utility on the other (GPRS, power line).
- **Metering Device:** A device with a measurement task. It measures energy of some sort and is equipped with a ZigBee end device to transfer the data over the air.

- **Display Unit:** A device that is capable of visualising metering data and informational text messages to the customer. A display unit may also be used as control entity to influence load curtailment.
- **Load Control Device/Smart Appliance/Programmable Thermostat:** A group of devices that can participate in energy management activities in order to reduce energy consumption.
- **Range Extender:** A stand alone device with ZigBee routing functionality.
- **Ad-hoc Device:** A device with the ability to dynamically join the network to read-out meters or for commissioning and diagnostic tasks.
- **Concentrator:** Is able to collect, store and forward metering data from other meters. Concentrators are mainly thought to manage metering data from meters that are not always online (sleeping devices such as battery powered water meters).

Various combinations of ZigBee functions and application functions are possible. As an example: A metering device can be a simple end device or additionally act as router. Furthermore, it is possible to have multiple application functions that share one transceiver in one physical device. A gateway for instance must not be a stand alone device. More likely, the gateway functionality is built into a metering device that could additionally act as concentrator etc.

Profiles: What ZigBee stack profile shall we take for the new application? Since its first draft the alliance has published various versions of the ZigBee core specification resulting in different stack profiles (ZigBee V1.0, ZigBee 2006, ZigBee 2007, ZigBee Pro…). As we know, with changing requirements and new features, interoperability between the different versions is no longer guaranteed. A decision needs to be taken on which devices can take part in the ZigBee AMI.
Another decision to be made up with the start of a new ZigBee application, is whether to define a new profile or take an existing one. And if a completely new profile is defined, shall it be kept private or is it presented to the public, maybe even to become officially recognised? If there is an existing one, does it have all the functionality needed for the application or shall it be extended with manufacturer specific items?

For our project, we decided to go for the ZigBee Pro Stack and implement all devices with the latest stack profile. That's the only way to be sure that all the features we rely on are there (and not optional). This decision has been taken in the strong belief that the ZigBee core specification is now more or less stable with the Pro version.
Of course, it makes sense to take the official ZigBee Smart Energy profile in the AMI project. And although the specification has not yet been finished, it seems that all the basic functionality we need is there. Beyond that, it is allowed to extend the profile with additional (vendor specific) clusters.

Clusters: The functionality of an application in ZigBee is implemented in the commands and attributes of the clusters that make up a profile. The ZigBee Alliance has created the ZCL (ZigBee Cluster Library) that consist out of a repository of common clusters with functionality that can be shared across multiple profiles. For a new profile, the ideal case would be to just find the right set of clusters in the ZCL and take the already implemented functionality to form the new application. So if a new application is to be created, it's a good starting point to go through the ZCL specification and see what is already around to be used. Additional clusters or even additional features to existing clusters maybe defined to fulfil the complete application requirements. Clusters and attributes may be marked as "mandatory" or "optional". The ZigBee discovery process (descriptors) helps to find out, what clusters a specific device implements. If one of the newly defined clusters is interesting for other profiles, it could find the way into the ZCL later on.

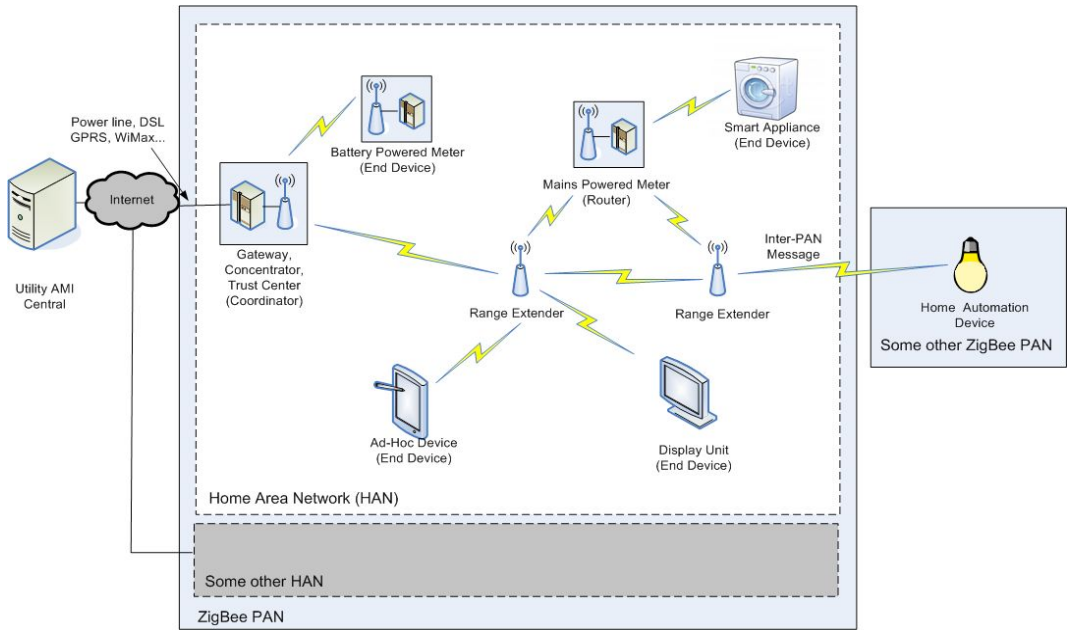

Figure 4: Example of an ZigBee Smart Energy Network

As the list of clusters of the Smart Energy profile is still under construction, we stick to to a short list of the ZCL clusters we intend to use. Be aware that the ZCL specification is a living document and still growing[4]. Some of the clusters of the following list (*) are not yet included in the public ZCL release [12].

- ***Basic:** Provides basic device information. This cluster is also mandatory for the other application profiles defined so far.*
- ***Power Configuration:** Allows access to information about the power sources of a device, configuration of under/over voltage alarms etc.*
- ***Identify:** Sets the device into the identify mode that lets other devices and users know which of several physical devices it is (e.g. Who is 123? 123 indicates its presence with a flashing light).*
- ***Alarms:** Sends alarm notifications and is used to configure alarm functionality.*
- ***Time:** Provides a basic interface to a real-time clock (setting time, synchronisation etc.)*
- ****Key Establishment:** Exchanges security keys and sets up security features.*
- ****Commissioning [13]:** Allows configuring devices and networks to achieve the needs of the specific installation.*
- ****Diagnostics:** Provides a standardised interface for monitoring and diagnostics .*
- ****Generic Tunnelling:** Defined in the context of the CBA Profile (Commercial Building Automation). Transports non-ZigBee protocols over ZigBee networks.*

*Another candidate not decided upon yet is the **Groups** cluster of the ZCL to manage and reach groups of devices.*

V. Network Architecture

ZigBee knows the notion of a PAN (Personal Area Network) that addresses one ZigBee network. In the AMI domain one can differentiate between a HAN (Home Area Network), BAN

[4] Stack providers ship their ZigBee software including a (more or less up to date) ZCL implementation. The ZCL is one of the reasons why the stack implementations of all vendors take up more and more space in the flash with each new release. However, depending on the modularity of the stack, the products differ in their flexibility to decide what goes into the binary in the end.

(Building Area Network) and a NAN (Neighborhood Area Network). Besides pure AMI networks, there could be other ZigBee networks around (e.g. a Home Automation or a Commercial Building Automation netwrok). For the scope of this paper, we focus on a HAN. A typical one is depicted in Figure 4.

- *We assume that a HAN will not contain more than 30 ZigBee network nodes*
- *Security is an important (and mandatory) feature in an AMI environment*
  - *Networks are secured with ZigBee network security features.*
  - *In most cases, the network will be private with keys only known to the utility.*
- *If there are other HANs in a building, they all belong to the same ZigBee PAN. Privacy between neighbours is again assured over ZigBee's application security features.*

There exists a requirement to involve devices which are not part of the highly secured AMI network (e.g. to send pricing information or text messages to insecure HA devices). ZigBee routers are not made to route messages between PAN networks[5]. In the literature this issue is addressed under the term "inter-PAN" communication. In our view, there are two possibilities to achieve inter-PAN routing in our prototype network:

- There exists a yet unpublished proposal for a mechanism whereby "ZigBee devices can perform limited, insecure, and possible anonymous exchange of information in their local neighbourhood without having to form or join the same ZigBee network".
- One can try to build a ZigBee bridging device that consists out of two separate physical routers that join two PAN networks and transfer their data between them.

We decided that the requirements can be met with the limited inter-PAN proposal.

VI. Addressing and Reading Out Meters

As already mentioned, the core functionality of an AMI is to read out and transfer metering data. A Smart Metering profile will contain possibilities to fetch data from a meter using a ZigBee application specific protocol. However, electronic meters are around for quite some time and companies have spent much time and money on creating powerful ways to describe and read out metering data. Metering protocol standards have evolved such as DLMS/COSEM or IEC62056-21. As with protocols like BACnet in the building domain, the metering community intends to stick with these protocols. Still it does not want to abandon the advantages of a state of the art wireless mesh communication standard. So, there must be a way to transport these native protocols over ZigBee[6]. The mechanism of choice is tunnelling. Tunnelling allows sending any protocol within ZigBee AMI packets. The need to tunnel BACnet packets over ZigBee has already lead to specific ZigBee clusters in the CBA profile. And tunnelling clusters are certainly candidates to be included in the ZCL.

Addressing: An existing metering protocol does not know anything about ZigBee specific address schemes and vice versa. How then can we determine the ZigBee destination address of a tunnelling packet? A mechanism is needed to find out the ZigBee node address depending on a protocol specific meter address.

The result is a Smart Metering specific implementation of something like the ARP (Address Resolution Protocol) in IP or the ZDO (ZigBee Device Object) with it's capabilities to match 64-Bit IEEE MAC addresses to 16-Bit node addresses and vice versa. In general, this request is issued on demand, whenever new data with unknown destination is received. A small table cache and timers are used in each node to temporarily store address tuples and cut down

[5] Unlike IP, were routing explicitly means sending messages across networks (Layer 3), ZigBee messages stay in the same PAN and routers can only be part one network at the same time.

[6] A similar problem on another level had the 6loWPAN group of the IETF that issued an RFC to transport IPv6 packet data over IEEE802.15.4 [].

traffic regarding these "address match requests". We decided to go for this distributed approach and not build up a "central address repository" similar to e.g. the Internet's DNS (Domain Name Service) or binding tables in ZigBee.

But what if the meter address is unknown? This is the case if e.g. a DLMS request is received over the gateway from the central. There are two conceptual approaches:

- The gateway works on layer 7 which means it needs to parse the incoming data, identify the protocol and find out the metering address. Afterwards, an address match request finds the according ZigBee node address. A tunnelling header is added to the data with fields for the type of protocol (DLMS) and the meter address.
- The gateway does not look into the data stream. It sends out the data "as it is" to all known neighbours. If a meter in the network understands the metering protocol and recognises its embedded meter address, it will respond. The gateway is then able to determine the ZigBee node address of the meter ("get sender") and temporarily save it for the current read out session.

Both approaches have their advantages and drawbacks. If the gateway knows the incoming protocol, it sends the data to the correct destination immediately without flooding the network at the beginning of a new read out request. Further, it is able to recognise packet borders and take those into account when forwarding the data in ZigBee packets. The gateway is able to handle several parallel data streams and distribute them across the network if the native metering protocol is laid out for this. However, the gateway needs in depth knowledge of all possible native metering protocols. The firmware is getting more complex, error-prone and inflexible. With each new protocol to be supported, a new parser needs to be implemented.
The second approach is generic. It can cope with any native protocol. The mechanism will generate more traffic and act slower, as timeouts need to be introduced to wait for the meter answer etc. It will only work with one metering "session" at a time and switch back to "send to all meters", as soon as it recognises a session end. Finding values for the various timeout parameters and the packet length - working for all native protocols and read-out tools - is tricky.

At the moment, tests are run to find out, whether the generic approach is feasible. It is the preferred approach. As timeouts in the order of few seconds are not critical in a metering system and the number of nodes handled by one gateway is not very big, we believe it's possible.

Fragmentation: Fragmentation takes care of splitting a data stream into individual packets, adding sequence numbers and validation schemes, sending and reassembling them again. It's another standard feature of the ZigBee Pro specification.

The protocol tunnelling code needs fragmentation and will make use the ZigBee features implemented in the stack. We assume that it's possible to store one complete metering protocol packet and forward it to the fragmentation mechanism to be split and sent.

VII. Conclusion and Outlook

An AMI can save money and energy. It simplifies the management of energy data for the utility, informs the customer about his personal energy consumption and helps to increase the energy efficiency as a whole. The ZigBee Alliance has identified Smart Metering as one of the killer applications for ZigBee and it won't be long, until the official Smart Metering Profile will be released. The paper presented hints on how to use ZigBee as the local network technology in an AMI. In this short overview, we covered physical as well as application related issues. The main challenge for the AMI designers is to make the system reliable and easy to use. If advanced metering infrastructures shall become widely accepted and commercially

successful, set-up must happen with minimal user intervention. The system must be secure and run autonomously for about 10 years, new devices should be integrated seamlessly and the network detects and informs automatically in case of malfunctions. What's already clear is that the AMI application and its requirements really put the ZigBee technology to a serious test. Almost every feature of ZigBee (up to the latest PRO specification) should be in place and running. The next months and years are going to be exciting for the energy industry and the ZigBee Alliance - they will show whether the challenges can be met.

VIII. Acknowledgements

This work is funded by Landis+Gyr and the KTI/CTI programme of the Swiss government.

References

[1] Automatic Meter Reading - Wikipedia
[Online] http://en.wikipedia.org/wiki/Automatic_meter_reading
[2] Advanced Metering Infrastructure (AMI) – Daintree ZigBee Glossary
[Online] http://www.daintree.net/resources/glossary.php
[3] ZigBee sees strong growth for energy management and efficiency solutions – ZigBee News
[Online] http://www.zigbee.org/imwp/idms/popups/pop_download.asp?contentID=11241
[4] ZigBee Smart Energy Features – ZigBee Alliance
[Online] http://zigbee.org/imwp/download.asp?ContentID=12484
[5] V. Bella, T.S.Popescu, R. Giannantonio, C. Borean, Analysis of ZigBee Interference in WBANs, Proceedings of 1st European ZigBee Developer Conference (EuZDC07), Munich
[6] M. Binhack, New Investigations on ZigBee and WLAN Coexistence, Proceedings of 1st European ZigBee Developer Conference (EuZDC07), Munich
[7] ZigBee Pro Feature Set – ZigBee Alliance
[Online] http://www.zigbee.org/en/spec_download/zigbee_downloads.asp
[8] ETSI EN 300 328 - Electromagnetic Compatibility and Radio Spectrum Matters (ERM); Wideband Transmission Systems; Data transmission equipment operating in the 2.4 GHz ISM band and using wide band modulation techniques
[9] ETSI EN 301 489-17 - Electromagnetic compatibility and Radio Spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment; Part 17: Specific conditions for 2.4 GHz wideband transmission systems, 5 GHz high performance RLAN equipment and 5.8 GHz Broadband Data Tranmitting Systems.
[10] T. Cutler, ZigBee – Make or Buy?, Proceedings of 1st European ZigBee Developer Con ference (EuZDC07), Munich
[11] A. Klapproth, S. Bissig, M. Venetz, S. Knauth, D. Käslin, R. Kistler, Design of a versatile lowcost IEEE802.15.4 module for long term battery operation, Proceedings of 1st Euro pean ZigBee Developer Conference (EuZDC07)
[Online] http://www.ceesar.ch
[12] ZigBee Cluster Libarary, ZigBee Alliance
[Online] http://www.zigbee.org/en/spec_download/zigbee_downloads.asp
[13] Understanding ZigBee Commissioning, Daintree Networks

Contact

Prof. Alexander Klapproth
Head of CEESAR
Lucerne University of Applied Sciences and Arts
Technikumstrasse 21
CH-6048 Horw

Tel. +41 41 349 35 99
eMail: Alexander.klapproth@hslu.ch
Web: http://www.ceesar.ch