Evaluation of Short-Range Wireless Technologies for Automated Meter Reading (AMR) Systems

Cs. A. Szabó, K. Farkas

Budapest University of Technology and Economics
Department of Networked Systems and Services
2 Magyar Tudósok krt., Budapest, 1117 Hungary
Phone: +36 1 463 2049
e-mail: szabo@hit.bme.hu

Abstract: The paper presents the results of the evaluation of some short-range wireless technologies suitable for communications in AMR systems. The typical AMR system structure is described, an overview of three candidate technologies, Wi-Fi, ZigBee and wireless M-Bus, is provided. The evaluation of these technologies is given, based on a selected set of properties, and the results of measurements in two real-world scenarios are summarised.

Keywords: AMR, automated meter reading, Wi-Fi, ZigBee, M-Bus

1. Introduction

Automatic meter reading (AMR) is the technology of automatically collecting consumption, diagnostic, and status data from different utility metering devices and transferring that data to a central database for billing, analysing and troubleshooting. AMR devices are basically water, gas, electricity, and heat meters. However, automatic meter reading requires the deployment of an appropriate infrastructure. An enhanced variant of such an infrastructure is called AMI (Advanced Metering Infrastructure) that, besides collecting metering data, also enables two-way communications with the meter. AMIs usually include hardware, software, communications, consumer energy displays and controllers, customer associated systems, meter data management software, and supplier business systems. The AMR/AMI technology saves utility providers the expense of periodic visits to each physical location to read a meter and the metering data can be collected remotely with arbitrary periodicity in an efficient and economic way. In addition to that, thanks to the continuous monitoring of the meters failures or misuse can be detected immediately making possible instant intervention. Moreover, billing can be based on near real-time consumption rather than on estimates. This timely information and its analysis can help both utility providers and customers to better control the production and consumption of public utility services.

The paper is organized as follows. In Section 2, we give an overview of a typical AMR/AMI system architecture. The current general AMR/AMI system architecture follows a two-level, hierarchical model with the main elements as follows: i) meters – traditional ones with transmitters attached to it via optical or electrical interface or

integrated meters; ii) data collection unit, concentrator or gateway; and iii) data processing centre – usually at the site of the utility company, or at a central controlling site in case of a municipality network with AMR service. This architecture can be extended to a three-level one by adding an intermediate level, in which a concentrator collects data from individual house or apartment concentrators. For communications between the meters and the (lower level) concentrator, wired connections (e.g., PLC, Ethernet, M-Bus) or wireless connections (e.g., ZigBee at 868 MHz and 2.4 GHz, Wireless M-Bus at 868 MHz, Wi-Fi, proprietary radio), while between the individual concentrators and the processing centre wired connections (e.g., PLC, PSTN) or wireless connections (e.g., cellular radio/GPRS, Wi-Fi, WiMAX) are typically used.

Section 3 contains an overview of the potential wireless technologies and their comparative evaluation, based on a set of properties that are important for AMR systems. We highlight Wi-Fi, ZigBee, and Wireless M-Bus technologies. We do not include cellular solutions, like GSM/3G/4G, in this overview even if such implementations can be found on the market, because they seem to be technologically and economically suboptimal for AMR systems. For evaluating the aforementioned technologies the following set of properties will be used: i) network topology and architecture; ii) propagation properties and area coverage; iii) possibilities for QoS provisioning; iv) manageability; v) security and privacy issues; and vi) existing applications, products, vendor support. Based on the outcome of this comparison we selected the 868 MHz version of ZigBee and the Wireless M-Bus (also operating in this frequency band) technologies for further investigation and carried out some real field measurements.

The last part of this paper, Section 4, contains our measurement results. For the tests we used standard-based Wireless M-Bus adapters produced by Amber Wireless, with built-in antennas only, and we also used Texas Instrument's 868 MHz chips on evaluation boards. The measurements were carried out in two realistic scenarios: in a family house and in a multi-dwelling house environment.

2. AMR/AMI system architecture

This section gives an overview of AMR system architectures, and deals with local data collection and forwarding the data to the central site with the appropriate communication technologies and protocols.

Based on our survey of AMR system suppliers we can arrive to a conclusion that the current general AMR/AMI system architecture is a two-level, hierarchical one, see Figure 1, with the main system elements as follows:

1 Meters (traditional ones with transmitters attached to it via optical or electrical interface or integrated meters)

2 Data collection unit, Concentrator, Gateway (different names used by different vendors)

3 Data processing centre (usually at the site of the utility company, or at a central controlling site in case of a municipality network with AMR service)

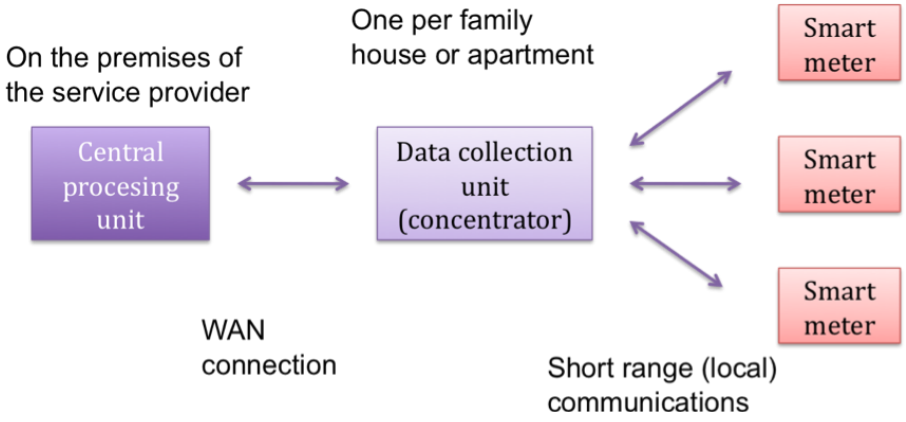

Figure 1. Typical high-level AMR system architecture

This architecture can be extended to a three-level one by adding an intermediate level where a concentrator collects data from individual house or apartment concentrators.

A typical practical architecture is more complicated than the high level one described above. This is mainly because usually more than one short-range communications technology is used for connecting the meters to the concentrator. For example, the system architecture of Holley Metering [1] consists of several sub-systems, as follows:

1. Meters connected via wired connection, using a RS485 repeater.
2. Meters connected via PLC, using a PLC/RS485 converter.
3. Meters connected via low frequency wireless network, using a wireless/RS485 converter.
4. Meters connected via ZigBee, using a ZigBee/RS485 converter.

In the Holley Metering architecture, the last part is actually a wireless mesh network.

Solutions for the communications between the meters and the (lower level) concentrator include:

- wired connections: PLC, Ethernet, M-Bus,
- wireless connections: transceivers in 450-470 MHz band (FCC), 433 MHz, ZigBee 868 MHz and 2.4 GHz, Wireless M-Bus (868 MHz), Wi-Fi, proprietary radio.

Solutions for communications between the individual concentrators and the processing centre include:

- wired connections: PLC, PSTN,
- wireless connections: cellular radio (most frequently GPRS), Wi-Fi, WiMAX.

Note that municipal/community wireless networks are often used as a communications infrastructure for AMR system, mainly in the USA (see [2]). In these cases, the wireless technology is mostly Wi-Fi mesh and occasionally WiMAX is used as a backbone.

As for the wireless communications between the meters and the concentrator, which was our main subject of study, *ZigBee*, *Wireless M-Bus and Wi-Fi* are based on

worldwide standards and gained wide acceptance in the solutions of large vendors. We provide an overview and a comparative evaluation of these three technologies in the next section.

3. Wireless technologies for AMR systems

3.1. Wi-Fi

3.1.1. Overview

Wi-Fi is a trademark of the Wi-Fi Alliance and the term was originally created as a simpler name for the IEEE 802.11 standard family [3] to create wireless local area networks (WLANs). The original version of the IEEE 802.11 standard was released in 1997 and clarified in 1999, but is today obsolete. In the meantime, several amendments to the original standard were developed, and in 2007 a single document was created merging 8 amendments (802.11a, b, d, e, g, h, i, j) with the base standard and named to the current base standard IEEE 802.11-2007. In 2009, the IEEE has approved the 802.11n amendment that improves upon the previous 802.11 standards, and this can be considered as the latest standard, widely supported by the device manufacturers.

To position Wi-Fi among the relevant wireless communication technologies we can say that it belongs to wireless LAN technologies providing up to some hundred meters communication range and up to some hundred Mbps bandwidth

3.1.2. Main characteristics

A) Network topology and architecture

Wi-Fi can work either in infrastructure or in ad hoc mode. In infrastructure mode, Wi-Fi wireless LANs follow a cellular architecture. Each cell (called Basic Service Set or BSS) consists of mobile nodes (MN) and is controlled by a base station (called Access Point or AP). Most wireless LANs are formed by several cells, where the APs are connected through some kind of backbone (called Distribution System or DS). This backbone is typically wired, using e.g. Ethernet technology. The whole interconnected wireless LAN, including the different cells, their respective APs and the Distribution System, is known as Extended Service Set (ESS) and also called as SSID (Service Set IDentifier).

In ad hoc mode, the users build up the wireless LAN without using APs. Such a network is a kind of wireless self-organized network built of a collection of diverse nodes. The nodes are basically hosts and at the same time mobile routers that are connected by Wi-Fi links and communicate spontaneously, and which form a multi-hop network with an arbitrary network topology without relying on any pre-existing infrastructure or central administration. These routers organize themselves in a self-configuring manner, thus the network's wireless topology may change rapidly and unpredictably. An ad hoc network may operate in a standalone fashion, or may be connected to the Internet.

The infrastructure and ad hoc communications can be combined into a mesh topology. An infrastructure Wi-Fi mesh network is a communication network built of static Wi-Fi nodes organized in a mesh topology in an ad hoc manner. End hosts can access this mesh cloud via the Wi-Fi nodes that serve as APs. However, Wi-Fi nodes do not necessarily play an AP role, they can be just mesh points, but all the Wi-Fi nodes act as routers to transmit data from nearby nodes to peers that are too far away to be reached in a single hop, resulting in a network that can span larger distances. A mesh network is reliable, can self form and self heal and offers redundancy. It has a relatively stable topology except for the occasional failure of nodes or addition of new nodes. The traffic, being aggregated from a large number of end users, changes infrequently. When a node can no longer operate, the rest of the nodes can still communicate with each other, directly or through one or more intermediate neighbors.

B) Propagation properties and area coverage

The 802.11 protocol covers the physical and MAC (Media Access Control) layers. The original standard defines a single MAC layer that interacts with three physical layers (later on this was revised and extended by additional physical layers).

The four major physical layer specifications are defined in 802.11a, 802.11b, 802.11g and 802.11n. These standards use different ISM (Industrial, Scientific and Medical) license free frequency bands and radio modulation techniques resulting in different data rates and interoperability properties. The physical layer specified by 802.11a works in the 5 GHz frequency band, since 802.11b/g standards specify the 2.4 GHz frequency band for operation, thus 802.11a devices cannot interoperate with 802.11b/g devices. The 802.n standard specifies the use of both bands. The 5 GHz frequency band, for much of the world, offers at least 23 non-overlapping channels rather than the 2.4 GHz frequency band, where only 13 (in some countries 11, in Japan 14) channels are available and all the neighbouring channels overlap (channels far enough from each other, such as channels 2 and 7, or channels 1, 6 and 11, are non-overlapping in this range). Because of this choice of frequency band, 802.11b/g/n devices may occasionally suffer from interference from microwave ovens, cordless telephones and Bluetooth devices.

Table 1 summarizes the channel bandwidth, modulation technique, data rates and communications range of these physical layer standards.

Table 1. Comparison of 802.11 standards

Standard	**Freq. [GHz]**	**Chnl bwidth [Mhz]**	**Mod. techn.**	**Compa-tibility**	**Max. data rate, Mbps**	**Commun. range [m]**
802.11a	5	20	OFDM *)	802.11n	54	Indoor: 30-90 Outdoor: 100-300
802.11b	2.4	20	DSSS **)	802.11g /n	11	
802.11g	2.4	20	DSSS/ OFDM	802.11b /n	54	
802.11n	2.4/5	20/40	OFDM	802.11a/ b/g	600	

*) *Orthogonal Frequency Division Multiplexing*

**) *Direct Sequence Spread Spectrum*

C) Possibilities for QoS provisioning

The IEEE 802.11e standard defines a set of Quality of Service enhancements for wireless LAN applications through modifications of the MAC layer. The standard is considered to be of critical importance for delay-sensitive applications, such as Voice over Wireless LAN and streaming multimedia.

The basic medium access method of IEEE 802.11 is the DCF (Distributed Coordination Function), which is basically a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). This method uses a collision avoidance mechanism together with a positive acknowledgement scheme. The CSMA/CA-based MAC protocol does not provide any QoS. Beyond the basic DCF, there is an optional MAC mechanism called PCF (Point Coordination Function), which may be used to implement time sensitive services, like voice or video transmission. This PCF makes use of higher priority access and the AP issues polling requests to the stations for data transmission, hence controlling medium access. In order to still enable regular stations to access the medium, there is a provision that the AP must leave enough time for distributed access, too. Unfortunately, most of the off-the-self products do not support PCF.

The 802.11e enhances the DCF and the PCF, through a new coordination function: the hybrid coordination function (HCF). Within the HCF, there are two methods of channel access, similar to those defined in the legacy 802.11 MAC: Enhanced Distributed Channel Access (EDCA) and HCF Controlled Channel Access (HCCA). Both EDCA and HCCA define Traffic Categories (TC). With EDCA, high priority traffic has a higher chance of being sent than low priority traffic. In addition, EDCA provides contention-free access to the channel for a period. The HCCA works like PCF. However, the HCCA, which is not mandatory to implement for 802.11e APs, allows for the controlled access phases being initiated almost anytime during a contention period.

HCCA is generally considered as the most advanced (and complex) coordination function. With the HCCA, QoS-enabled stations have the ability to request specific transmission parameters (data rate, jitter, etc.) that should allow advanced applications like VoIP and video streaming to work more effectively on a Wi-Fi network.

D) Manageability

The 802.11 standards define 'frame' types for use in transmission of data as well as management and control of wireless links. Frames are divided into very specific and standardized sections. Each frame consists of a MAC header, payload, and frame check sequence (FCS). Some frames may not have the payload (e. g., control frames). The first two bytes of the MAC header form a frame control field specifying the form and function of the frame. The maintenance of communications is done by the management frames. They provide functions for device authentication, association, sending beacons to announce the existence of the network, etc.

Furthermore, power and radio management possibilities are also provided in 802.11 networks. When the transceiver is off, it is in sleeping or power-saving mode. When the transceiver is on, it is active or awake. Power conservation in 802.11 is achieved by minimizing the time spent in the latter stage and maximizing the time in the former one. Power management can achieve the greatest savings in infrastructure networks. All traffic for mobile stations must go through APs, so they are an ideal location to buffer traffic. By definition, access points are aware of the location of mobile stations, and a mobile station can communicate its power management state to its AP. Access Points have two power management related tasks. First, because an AP knows the power management state of every station that is associated with it, it can determine whether a frame should be delivered to the wireless network when the station is active or buffered when the station is asleep. An AP's second task is to announce periodically which stations have frames waiting for them. Moreover, it is possible on most of the Wi-Fi interface cards to tune the transmission power, which extends the battery lifetime of the mobile node in certain scenarios.

E) Security and privacy issues

The WLAN lacks even the minimal privacy provided by a wired LAN. The 802.11 Wired Equivalent Privacy (WEP) mechanism provides protection at a level that is felt to be equivalent to that of a wired LAN. Data frames that are encrypted are sent with the WEP bit in the frame control field of the MAC header set. The receiver decrypts the frame and passes it to the higher layer protocols. Only the frame body is encrypted, this leaves the complete MAC header of the data frame unencrypted and available to even the casual eavesdroppers. Unfortunately, WEP provides only minimal protection to frames in the air and is not too difficult to decrypt the frames even for a causal attacker.

Thus, the Wi-Fi Alliance announced an interim specification called Wi-Fi Protected Access (WPA) based on a subset of the then current IEEE 802.11i draft. The final IEEE 802.11i standard (also known as WPA2) uses Advanced Encryption Standard (AES)

instead of RC4. The modern recommended encryption for the home/consumer space is WPA2 (AES Pre-Shared Key) and for the enterprise space is WPA2 along with a RADIUS (Remote Authentication Dial In User Service) authentication or similar, and a strong authentication method such as EAP-TLS (Extensible Authentication Protocol – Transport Layer Security).

F) Existing applications, products, vendor support

There are many applications of Wi-Fi connectivity, starting from home-based Wi-Fi enabled devices to many public places that are supplied with Wi-Fi connectivity to access Internet, like cafés, restaurants, hotels and clubs to attract the clients. Wi-Fi hotspot concept is popular among business communities and mobile workers, too. Applications like VoIP (Voice over IP), videoconferencing and multimedia streaming are getting popular with the latest Wi-Fi standards providing high data rates and QoS support.

On the market, a huge number of Wi-Fi products are available, including access points, gateways/routers, interface cards, adapters, antennas, Internet radios, spectrum analyzers, power supplies, bar code scanners, cameras, compact flash cards, intrusion prevention systems, multimedia devices, handheld devices/PDAs. Among the biggest Wi-Fi vendors are Cisco/Linksys, Intel, Ericsson, Nokia, Netgear, D-Link, Proxim, Apple.

3.1.3. Summary

Wi-Fi is the dominant wireless technology today to build wireless LANs. With the proliferation of Wi-Fi devices many vendors' products are available for very low price with strong support. The long history, operation experience, high data rate, low cost, enhanced security and QoS support make attractive this technology also in a wide range of application scenarios, such as cordless connection among devices or wireless VoIP using Wi-Fi connections.

On the other hand, this high level of popularity converts one of the most beneficial properties of Wi-Fi, the license free operation, to a serious drawback. The different Wi-Fi applications and devices can interfere with each other, which can result easily in performance degradation, or interruption of operation. This factor should be kept in mind when one considers Wi-Fi technology for new application areas.

3.2. ZigBee

3.2.1. Overview

ZigBee is the specification of the Zigbee Alliance [5], which is based on and enhances the IEEE 802.15.4 standard. 802.15.4 is a member of the IEEE 802.15 PAN (Personal Area Network) family which aimed at standardizing protocols for low cost, low energy consuming devices communicating with each other, without or with a minimal infrastructure (as opposed to the 802.11/Wi-Fi). The technology intended to be less

expensive and more energy-efficient than the other PANs such as Bluetooth. As usual, the IEEE standard only embraces 1.5 layers, the physical layer and the MAC (Medium Access Control) layer. ZigBee extends the IEEE basic architecture with network and security layers and an application framework. ZigBee Alliance, just like Wi-Fi Alliance, focuses on interoperability and certification testing of ZigBee compliant devices and publishes the list of certified products. In addition to the base standards (the so-called ZigBee 2012 and ZigBee IP), ZigBee Alliance developed a number of specific standards to address the needs of a particular application area, including: Commercial building management, Consumer electronics, Energy management, Health care and fitness, Home management, Retail management, Telecommunications.

3.2.2. Main characteristics

A) Network topology and architecture

Three types of network elements are specified:

- ZigBee Coordinator: controls the creation and maintenance of a network;
- ZigBee Routers: extends the range of networks;
- ZigBee End Devices: limited functionality devices that perform specific sensing or control functions.

The Coordinator (there is only one in a network) initiates the network and stores information about the network. All devices communicate with the Coordinator, it has also routing functionality and can serve as a bridge to other networks. The Router is an optional component, when exists, performs routing between nodes thus extending network coverage. It also manages local address allocation/de-allocation. The End Device is the cheapest device type and it is optimized for low power consumption. End Devices communicate only with the Coordinator.

In a ZigBee network, the basic topology is mesh. Point-to-point, star of tree structures are also possible. A network consists of maximum 65535 nodes, each node having a unique 64-bit identifier. Each network needs a central controller that has a permanent power supply and is responsible for sending beacon messages, setting up the network and communications among the nodes.

The protocol architecture consists of three layers: silicon, ZigBee stack (firmware) and applications. The silicon layer is basically what is covered by the IEEE 802.15.4 standard. The ZigBee protocol stack consists of logical networking, security and data protection procedures and application profile. The latter can be user-defined, however, only public profile by Zigbee Alliance ensures interoperability among different vendors's devices ("ZigBee Certified Product").

The physical layer specification is different for the different frequency bands. In the 2.4 GHz band, O-QPSK (Orthogonal QPSK - Quadrature Phase Shift Keying) modulation scheme is used, with 4 bits per symbol rate while in the 868/915 MHz band BPSK (Binary Phase Shift Keying) is used (1 bit/symbol rate). In both cases, interference protection is achieved by using DSSS (Direct Sequence Spread Spectrum) technique with spreading factor of 32 and 15 bits, respectively.

The MAC layer is responsible for multiple access. The MAC protocol offers both contention-based access and controlled (reserved) access in beacon mode. The

contention procedure is the CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) protocol, a method widely used in the case of Wi-Fi devices. There are two types of access mechanisms, depending on whether the network is a beacon-enabled or non-beacon enabled one. In the former case, a slotted CSMA/CA access is used, while in non-beacon-enabled mode, unslotted CSMA/CA is the channel access mechanism.

B) Propagation properties and area coverage

Propagation properties and area coverage are defined by the characteristics of the frequency bands where ZigBee is allowed to operate, see Table 2.

Table 2. ZigBee frequency bands

Band	Usage	Availability	Data rate [kbps]	No of channels
2.4 GHz	ISM	worldwide	250	16
868 MHz	with restrictions	in Europe	20	1
915 MHz	ISM	in America	40	10

In Europe, the 2.4 GHz ISM band is the obvious possibility. Here the average distance range that can be covered by ZigBee devices is 10 m to 75 m, sometimes more, in line-of-sight (LOS) conditions. Non-LOS propagation, in particular the penetration through concrete walls, is typically not very good (1-2 concrete walls can be allowed at best). Mutual interferences with devices using this band, especially with Wi-Fi, should be investigated. The two UHF bands could offer better propagation in NLOS environment, however, the 915 MHz band is only available in America, and the 868 MHz band, generally available for use in Europe, can be used under specific circumstances (limitation of the output power) [6]. For example, the output power is limited to 25 mW ERP and the duty cycle should be at most 1%.

C) Possibilities for QoS provisioning

Time-critical data can be sent via a timeslot reservation mechanism. The GTS (Guaranteed Time Slot) mechanism allows a device to operate in a specified portion of the superframe. A GTS can only be allocated by the PAN coordinator that can allocate up to seven GTSs at the same time. GTS allocation is performed by the coordinator based on (i) requirements of the GTS request, and (ii) the currently available capacity in the superframe. A GTS can be de-allocated by the coordinator whenever it decides to do so or based on the request of the device.

D) Manageability

The Network Layer (NWK) of the ZigBee protocol architecture is responsible for network management and offers a number of services to accomplish it such as initialization, maintenance and control of the network. Routing protocols are defined at the network layers for star, tree, and mesh topologies.

E) Security and privacy issues

The ZigBee security architecture includes security mechanisms at two layers of the protocol stack. The NWK and APS (Application Support Sublayer) layers are responsible for the secure transport of their respective frames. Furthermore, the APS sublayer provides services for the establishment and maintenance of security relationships. The ZigBee Device Object (ZDO) manages the security policies and the security configuration of a device.

F) Existing applications, products, vendor support

ZigBee is being used as short range wireless communication technology for many AMR suppliers including Develco (Denmark), ELSTER (Germany), ITRON (USA), Holley (China), Honeywell (USA), Landys&Gyr (Switzerland), TBNEnergo (Russia), Nuri Telecom (Korea). Products include electricity, gas, water, and heat meters, and vendors offer complete solutions with concentrators and backhaul connections. The ZigBee technology itself is often purchased from Telegesis (UK), a leading vendor specialized in ZigBee modules.

3.2.3. Summary

The ZigBee technology is one of the best candidates for short-range data collection in AMR systems. It enjoys wide industrial support due to its standardization status (within the IEEE 802 family) as well as due to the additional standardization, interoperability testing and application development within the ZigBee Alliance.

From technical point of view, the data rates it offers are enough for AMR applications, real-time transmission is also supported by the medium access protocol, security and management tasks are also taken care of by the ZigBee protocol stack and the products based on it. Its limitations (in Europe), when operating in the 2.4 GHz ISM band, are similar to Wi-Fi: the large number of devices cause mutual interferences, and the propagation properties are also not ideal, in particular when reliable communications have to be established in NLOS environment, for instance in large buildings with concrete separating walls. Communications with remote water meters in rural and suburban environment can be a problem where the meters are usually installed in concrete shafts with metal lids at a depth of about a meter below the surface.

3.3. Wireless M-Bus

3.3.1. Overview

The Metering Bus, or in short M-Bus, originally developed as an interface for heat meters, is considered as a basis for new advanced metering infrastructure (AMI) installations in many regions of the world. Their wireless implementation brings a competitive advantage; also they are products easy to install and maintain. The M-Bus standard is a European Standard [8], actually a family of standards, and its Wireless M-Bus component [9] defines the wireless communication between meters for water, gas, heat and electricity, and the data concentrators.

3.3.2. Main characteristics

A) Network topology and architecture

M-Bus is a field bus, which is specialized for transmitting metering data from gas, heat, water or other meters to a data collector. It is described by the aforementioned European standard which includes the specification of wired and Wireless M-Bus. The specification is divided into five parts:

- *EN13757-1: Communication systems for meters and remote reading of meters - Part1: Data exchange.* It describes the basic communication between the meters and a central data collector and provides an overview of the communication system.
- *EN13757-2: Communication systems for meters and remote reading of meters - Part2: Physical and link layer.* This part includes the specification of the physical data transmission using wired connections. It also contains the description of the protocol to transmit the data.
- *EN13757-3: Communication systems for meters and remote reading of meters - Part3: Dedicated application layer.* The third part of M-Bus describes an application protocol, which allows the data transmission of meters' multivendor capability.
- *EN13757-4: Communication systems for meters and remote reading of meters - Part4: Wireless meter readout (Radio meter reading for operation in the 868 MHz to 870 MHz SRD band).* This part specifies the wireless communication of M-Bus. It includes the Physical and the Data Link Layer for wireless devices, and it corresponds to specification EN13757-2 for wired communication.
- *EN13757-5: Communication systems for meters and remote reading of meters - Part5: Relaying.* This last part includes different proposals for relaying the meter data to overcome the range problem between remote meters and data collectors.

The network architecture follows the OSI model but only Layers 1, 2 and 7 are implemented. Up to now, the application layer implements all other protocol layers required for a specific device. Especially if routing is required, it resides in the application layer. This lack of modularity might be one reason why standardized routing algorithms are not available currently for Wireless M-Bus. But the reduced modularity leads to compact implementations running on very small devices with minimum computing resources.

The M-Bus supports asymmetric network topologies with low-cost or low-power metering devices on the one side and data collectors or gateways with higher performance on the other side. Currently, only *point-to-point or star* network topologies apply. Mesh networking is not possible, as the required routing algorithms are not specified yet.

The wireless M-Bus standard specifies the communication between a meter and an "other" system component, e.g. mobile/stationary readout devices, data collectors.

Three different meter modes are defined, for the communication between a meter and an "other" device:

- S-mode - Stationary Mode;
- T-mode - Frequent Transmit Mode;
- R-mode - Frequent Receive Mode.

Sub-modes X.1 and X.2 specify whether one-way or two-way communication is

performed, respectively. Thus for example Mode T2 indicates a two-way T-mode device.

The EN13757-4 specifies the physical layer and the data link layer for communication between the meter and the concentrator. This includes:

- Radio parameters;
- Packet frame format;
- Access method.

The Wireless M-Bus specification has several options for the radio parameters. Three different data rates are specified: 4.8 kbps for R2, 32.768 kbps for S1/S2 and 100 kbps for T1/T2.

All the modes are specified to use the 868 MHz license-free ISM band for Europe, but each of the different modes has its own radio requirement such as the specific channel, frequency accuracy, data rate tolerances, etc.

One of the important features for Wireless M-Bus is that meters are battery-operated. Gas and water meters are normally not connected to the electricity network and therefore have limited energy available. In addition, the replacements of meters are costly so the battery lifetime should be several years. Actual lifetime requirements may vary from country to country, typically 10 – 20 years. To handle the battery lifetime requirements, the radio in the meters is in sleep mode for most of the time, and transmits only in small timeslots. The concentrator can never initiate any communications since the meter will be in sleeping mode most of the time. Two-way communications is enabled by the meter going into receive mode for a short time after transmission, thus allowing the concentrator to send messages at these specific timeslots. The timing is different for different modes and the timing is specified in the standard.

The addressing scheme in Wireless M-Bus is similar to the wired M-Bus. It is only the meters that have addresses, and the meter address is used both when transmitting to, and from, the meter. Hence, the concentrator must have a table of the meters connected to it. These meters will be registered at the concentrator during the installation phase.

B) Propagation properties and area coverage

Wireless M-Bus devices operate in the 868 MHz UHF band that offers good propagation in NLOS environment. This band is generally available for use in Europe, and can be used under specific circumstances (limitation of the output power). For example, the output power is limited to 25 mW ERP and the duty cycle should be at most 1%.

C) Possibilities for QoS provisioning

None.

D) Manageability

None.

E) Security and privacy issues

None.

F) Existing applications, products, vendor support

Several semiconductor/OEM vendors offer Wireless M-Bus modules that can be integrated into different components of an AMR system.

Radiocraft's RC1180-MBUS module can be used in several ways in the following devices: Concentrator; Bridge; Meter. The basic version on the standard RC1180-MBUS module comes with modem functionality. In this case, most of the control is done in the host controller, and the module is used as a communication port [10].

Texas Instruments has both single chip (SoC) and two-chip solutions for Wireless M-BUS. The two-chip solution is implemented with the RF transceiver CC1101 associated with the MSP430. The system on chip solution is based on a CC1110 device with an 8051 MCU core. TI provides software examples to support Wireless M-BUS [11].

Silicon Labs products include C8051 MCU and EZRadioPRO [12].

Analog Devices has a Wireless M-Bus transceiver ADF7020 [13].

Several AMR vendors support M-Bus and Wireless M-Bus interfaces for short-range communication between their data concentrator units and meters, e.g., ELSTER, Sagemcom.

3.3.3. Summary

M-Bus and Wireless M-Bus are European standards, specifically developed for smart metering systems. Wireless M-Bus devices operate in the license-free 868 MHz band thus offering adequate coverage for communications between concentrator and utility meters. Off-the-shelf RF modules are available from several large semiconductor manufacturers and AMR system vendors also support M-Bus and Wireless M-Bus interfaces.

3.4. Comparison of wireless technologies recommended for AMR systems

Table 3 gives a summary of the most important technical parameters of the three technologies dealt with in this chapter and serves as a comparison among them. Radio characteristics, communications and networking capabilities, security and reliability issues and possible application areas are addressed in this summary in detail.

Table 3. Comparison of wireless technologies

	Wi-Fi	**ZigBee**	**Wireless M-Bus**
Radio characteristics			
Frequency band(s) [GHz]	2.4/5	2.4 GHz (16 channels), 915 MHz (USA), 868 MHz (Europe)	868 MHz

Usable bandwidth [MHz]	83,5 (band 2.4 GHz), 200 (band 5.2 GHz), 255 (band 5.6 GHz)	80 MHz (16 channels), 2.4 GHz 20 MHz (10 chnls) in the 915 MHz band, 1 chnl at 868.3 MHz	1 channel at 868.3 MHz
Modulation method(s)	DSSS/OFDM	DSSS/QPSK, BPSK	FSK
Typical/maximal transmitting power	10 mW/100 mW (2.4 GHz), max. 1 W (5.6 GHz)	25 mW ERP allowed, with <=1% duty factor or technique as specified in 1999/5/EC	25 mW ERP allowed, with <=1% duty factor or technique as specified in 1999/5/EC
Typical receiver sensibility	-78 to -85 dBm @ 11 Mbps	-92 dBm	-102 dBm
Typical distance, LOS [m]	Some hundred meters	1500	N/d
Typical distance, NLOS [m]	30-90 (indoor), 100-300 (outdoor)	10-70	N/d
Communication and networking characteristics			
Simplex/half duplex/duplex	Half duplex	Half duplex	Simplex/half duplex
Data rate(s)	Up to 11/54/600 Mbps	250 kbps (2.4 GHz), 40 kbps (915 MHz), 20 kbps (868 MHz)	4.8, 32.768, 100 kbps
Frame size min./max.	Control frame: 14/20 octets, Max. mngment/data frame size: 2346 octets	76 Bytes max.	76 Bytes max.
Frame overhead	28 – 32 octets (management/data frame)	15 Bytes	15 Bytes
Supported topologies:			
- point-to-multipont (master-slave)	Yes	Yes	Yes

- point-to-point	Yes	Yes	Yes
- ad-hoc	Yes	Yes	No
- mesh	Yes	Yes	No
Addressing	MAC addresses	MAC addresses	Data link addresses
Medium access mechanism(s)	CSMA/CA	CSMA/CA, timeslot reservation	N/d
Delay and jitter	N/d	15 ms in sleep mode, jitter n/a	N/d
Security			
Encryption	WEP/WPA/WPA2	AES128	N/d, most likely none
Authentication	Yes		
Individual identification?	Yes, e. g. using RADIUS		
Reliability			
Error protection (ARQ/FEC)	FCS		CRC
ISM/licensed bands?	ISM	ISM bands, mutual interf. with Wi-Fi in 2.4 GHz band	ISM band
QoS capabilities?	Yes, 802.11e	Yes, via timeslot reservation mechanism	N/d, most likely none
Applicability			
Vendors implementing the protocol	Cisco, Ericcson, Netgear, etc.	Ember (leading chip manufacturer), Telegesis (leading vendor of ZigBee modules), AMR suppliers incl. Develco, Elster, Itron.	Radiocraft, Texas Instruments, Silicon labs, Analog Devices
Services using the protocol	Wireless Internet access, VoIP, etc.	AMR, building automation, home automation, health care, smart energy, remote control	Automated meter reading systems

Possibility of use on other (non-wireless) mediums	N/a	N/a	Compatibility with wired M-Bus within the same family of standards
Connection to other networks?	Yes	Yes	No direct connection, only via a concentrator device
Energy consumption and efficiency	Power management capability	Battery life 5...10 years	N/d

N/a - Not applicable, N/d – No data available

4. AMR measurements

4.1. Overview

Based on the comparative evaluation of wireless technologies for AMR systems, we selected the Wireless M-Bus and ZigBee (operating at 868 MHz) technologies for further experimental investigation.

This section contains the results of our measurements carried out by using some standard-based Wireless M-Bus adapters produced by Amber Wireless, with built-in antennas only, and with Texas Instrument's 868 MHz chips on evaluation boards. The measurements were carried out in laboratory as well as in two realistic scenarios: in a multi-dwelling house (Section 4.3) and in a family house (Section 4.4).

The measurements were focused on coverage, reliability, security and energy consumption issues.

4.2. Devices tested

We selected and purchased three different devices from two manufacturers (Texas Instruments and Amber Wireless). TI devices are very similar, but use different frequencies (433 and 868 MHz), while the Amber Wireless devices are Wireless M-Bus compatible ones thus operating in the 868 MHz band. These devices will be referred to as TI433, TI868, Amber868, respectively, in this section. The technical and other important parameters and capabilities of these devices based on datasheets and other vendor information are shown in Table 4.

Table 4. Comparison of measured AMR devices

	TI433	**TI868**	**Amber868**
			
Vendor	Texas Instruments	Texas Instruments	AMBER wireless GmbH
Model	CC1101 Evaluation Module 433 MHz	CC1101 Eval. Module 868 MHz	AMB8465-M
Chipset	CC1101	CC1101	AMB8425-M
Radio characteristics			
Frequency band(s) [MHz]	433	868	868
Usable bandwidth [MHz]	387-464	779-928	863.03 - 868.95
Channel spacing [kHz]	N/A	N/A	60
Modulation method(s)	2-FSK, 4-FSK, GFSK, MSK, OOK, ASK	2-FSK, 4-FSK, GFSK, MSK, OOK, ASK	2-FSK
Default/maximal transmitting power [dBm]	10	12	10
Receiver sensibility at lowest bit rate [dBm]	-116	-112	N/A
Maximum range [m]	N/A	N/A	100
Communication and networking characteristics			
Simplex/half duplex/duplex	N/A	N/A	N/A

Data rate(s) [kbps]	0.6 – 500	0.6 – 500	2.4/16.384/ 66.6 (up to 250)
Supported topologies:			
- point-to-multipont (master-slave)	N/A	N/A	OK
- point-to-point	OK	OK	OK
- ad-hoc	N/A	N/A	OK
- mesh	N/A	N/A	N/A
Medium access mechanism(s)	CSMA	CSMA	N/A
Wireless M-Bus compatible?	OK	OK	OK
OMS support?	N/A	N/A	OK
Security			
Encryption	N/A	N/A	AES-128 in prep.
Authentication	No	No	No
Individual identification?	No	No	No
Reliability			
Error protection (ARQ/FEC)	FEC (½ rate convolutional code)	FEC (½ rate conv. code)	N/A
ISM/licensed bands?	ISM	ISM	ISM
Operation temperature range [°C]	-40 to 85	-40 to 85	N/A
Energy consumption (available only for chipsets)			
Energy consumption in TX [mA]	13.1 to 29.2	16.4 to 34.2	N/A
Energy consumption in RX [mA]	15.0 to 17.1	14.6 to 16.9	N/A
Energy consumption in sleep [nA]	200	200	N/A

Sources: data sheets of the respective vendors [14]-[17]. Several of these important parameters were not available in datasheets. Therefore we had to complete this table with laboratory measurements that are not described in this paper.

4.3. Measurements in a condominium environment

The measurements were performed in a building including 221 apartments in a residential area of Budapest. The construction of the building consists of bearing walls and ceilings made of reinforced concrete and separating walls made of brick (being 30 cm in width). This environment significantly obstructs the propagation and decreases the operating range of the devices. Figure 2 illustrates the layout of the building where the measurements were performed (Floor 1, 2 and 3). The layouts of the three floors are

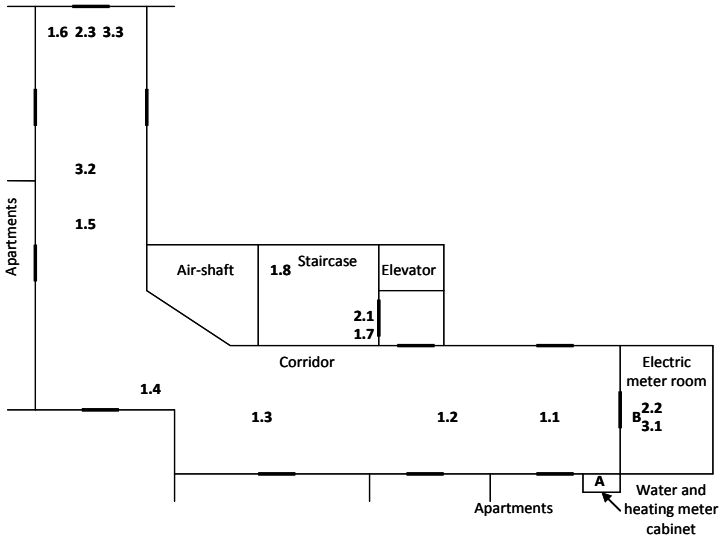

Figure 2. Layout of the condominium measurement area

the same, the floor height is 2.65 m and the thickness of the reinforced concrete ceiling is 0.33 m. The bold black lines indicate doors made of steel.

The receiver was installed in (i) the water and heating meter cabinet with wooden doors and (ii) behind the door of the electric meter room, which is made of steel (higher attenuation). The receiver positions are illustrated in Figures 3 and 4.

Figure 3. Receiver in water and heating meter cabinet

Figure 4. Receiver in electric meter room

During the testing we measured the average values of the Received signal Strength Indicator (RSSI) and Link Quality Indicator (LQI).

4.4. Measurements in a family house environment

In the family house environment, several difficulties can arise due to various circumstances, e.g. longer distances, water meter placed in an underground pit (often covered with a steel plate), various topography and facilities, etc.

The measurements were performed in a hilly, suburban like area of Budapest. 15 measurement points were chosen on this site, according to the potential locations of the AMR concentrator and other units, which allowed for measuring effects of range, walls, buttresses of soil, etc., see Figure 5.

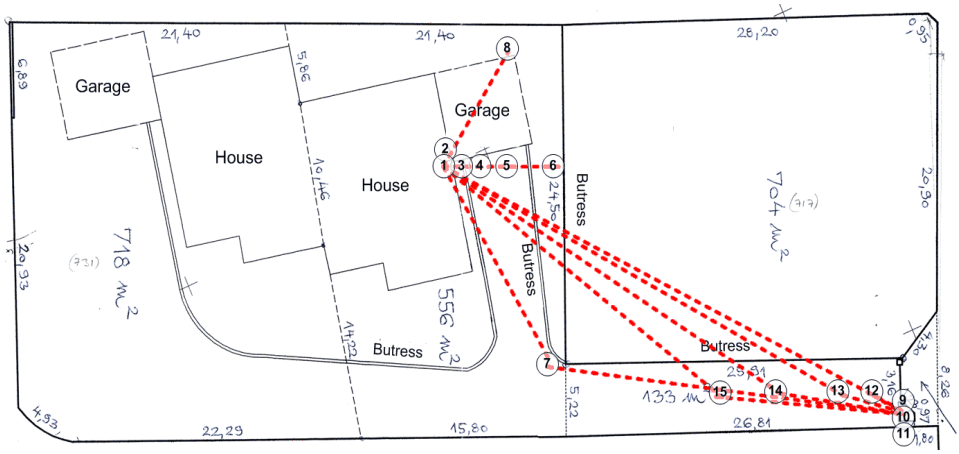

Figure 5. Map of the family house area with measurement points

4.5. Summary of and conclusions on the measurement results

Based on our measurements and tests, we can summarize our findings as follows.

A) Coverage and reliability

- Using 10 dBm transmitting power and 2-3 dBi antennas connected to appropriate devices (TI433 or TI868), a circle with 20 m radius can be covered in almost all circumstances (both condominium and family house environments), but often 35-40 m is available.
- 20 m range can be applied through 2-5 walls made of bricks or concrete, or through 3-4 steel doors, or from a water meter pit with 1 m depth and covered with a steel plate.
- The attenuation values for some obstacles can be estimated as follows:
  - concrete wall: 25-42 dB/m;
  - brick wall: 5-20 dB/m;
  - steel door: 5-15 dB/m.
- In the family house non-line-of-sight (NLOS) environment outdoor and long-range (>10 m) RSSI values are higher with 5-8 dB at 433 MHz than at 868 MHz.
- Locating an AMR device in a water meter pit decreased RSSI by 25-30 dBm, and by additional 10 dB when the steel cover was applied.
- By lowering the date rates higher receiving sensitivity (and larger coverage) can be achieved (but at increased power consumption).
- The LQI parameter is generally not useful (value is about 40 in most of cases), higher values come up only in very bad conditions and near to receiver sensitivity limit.
- At short distances (<8 m) and indoors, RSSI can fluctuate ±5 dB in time and in position due to near-field effects and reflections.
- AMR communication can interfere with remote door opening signals, but the possibility of this event is negligible.

B) Energy consumption

- Consumption of transmitter device can be double or higher than the consumption of its chipset version.
- TI868 devices have lower consumption values compare to TI433, although higher transmitting power (12 dBm compared to 10 dBm).
- Applying devices designed for low-energy consumption is very important.
- Using sleep mode and scheduled wake-up is crucial for long battery replacement period.
- Using higher data rate causes shorter transmission time, so battery replacement period can be 10 times longer or more! (But when using higher data rate the receiver sensibility decreases!)

C) Security issues

- The tested devices have no security features. Only Amber868 is designed to support AES128 block coding natively, but it was not yet implemented in the devices we used.
- Therefore, to ensure security extra effort is needed by implementing this functionality in software or hardware.

5. Conclusion

The three wireless technologies investigated in the paper are potentially suitable for AMR systems, although each of them is optimal for a specific setting and regarding a specific set of features and requirements. Final recommendation is not possible because of the limited scope of the measurements we have been able to carry out so far, however it is very likely that devices operating in the sub-gigahertz band are suitable for reliable communications in an AMR system as opposed to Wi-Fi and and ZigBee/2.4 GHz devices.

Acknowledgements

The research presented in this paper has been supported by Magyar Telekom. Károly Farkas has been partially supported by the Hungarian Academy of Sciences through the Bolyai János Research Fellowship.

The authors wish to thank Mr. Zoltán Németh and Mr. Zoltán Horváth for their contributions to the measurements.

References

[1] http://www.holleymeter.com/en/products.php?pid=7
[2] www.muniwireless.com
[3] IEEE 802.11 Standard Family. http://standards.ieee.org/getieee802/802.11.html
[4] M. S. Gast: 802.11 Wireless Networks: The Definitive Guide. O'Really, USA, 2002.
[5] ZigBee Specification. http://www.zigbee.org/Specifications.aspx
[6] ERC/REC 70-03
[7] EN13757
[8] EN13757:2005
[9] EN13757-4:2005
[10] http://www.radiocrafts.com/uploads/an009_implementing_with_rc1180-mbus_wireless_m-bus_module_1_0.pdf
[11] http://www.ti.com/lit/an/swra234a/swra234a.pdf
[12] http://www.silabs.com/Support%20Documents/TechnicalDocs/AN451.pdf
[13] http://www.analog.com/static/imported-files/application_notes/AN-0987.pdf
[14] CC1101 Development Kit 433 MHz, Texas Instruments, http://www.ti.com/product/cc1101
[15] CC1101 Evaluation Module 433 MHz, Texas Instruments, http://www.ti.com/tool/CC1101EMK433
[16] CC1101 Evaluation Module 868 MHz, Texas Instruments, http://www.ti.com/tool/cc1100emk-868
[17] AMB8465-M Wireless M-Bus USB Adapter, Amber Wireless, http://www.amber-wireless.de/189-1-AMB8465-M.html