# A Survey of Communication Protocols for Automatic Meter Reading Applications

Tarek Khalifa, Kshirasagar Naik and Amiya Nayak

***Abstract*—Utility companies (electricity, gas, and water suppliers), governments, and researchers have been urging to deploy communication-based systems to read meters, known as automatic meter reading (AMR). An AMR system is envisaged to bring on benefits to customers, utilities, and governments. The advantages include reducing peak demand for energy, supporting the time-of-use concept for billing, enabling customers to make informed decisions, and reducing the cost of meter reading, to name a few. A key element in an AMR system is communications between meters and utility servers. Though several communication technologies have been proposed and implemented at a small scale, with the wide proliferation of wireless communication, it is the right time to critique the old proposals and explore new possibilities for the next generation AMR.**

**We provide a comprehensive review of the AMR technologies proposed so far. Next, we present how future AMRs will benefit from third generation (3G) communication systems, the DLMS/COSEM (Data Language Messaging Specification/Companion Specification for Energy Metering) standard and Internet Protocol-based SIP (Session Initiation Protocol) signaling at the application level. The DLMS/COSEM standard provides a framework for meters to report application data (i.e. meter readings) to a utility server in a reliable manner. The SIP protocol is envisaged to be used as the signaling protocol between application entities running on meters and servers. The DLMS/COSEM standard and the SIP protocol are expected to provide an application level communication abstraction to achieve reliability and scalability. Finally, we identify the challenges at the application level that need to be tackled. The challenges include handling failure, gathering meter data under different time constraints (ranging from real-time to delay-tolerance), disseminating (i.e., unicasting, multicasting, broadcasting, and geocasting) control data to the meters, and achieving secure communication.**

***Index Terms*—Automatic meter reading (AMR), smart meters, wireless communications.**

## I. Introduction

THE TERM Automatic Meter Reading (AMR) or Smart Metering System refers to the technology whose goal is to help collect the meter measurement automatically and possibly send commands to the meters. Automation ranges from Connecting to a meter through an RS-232 interface, via Infrared, or short range radio frequency to transmitting the meter measurements all the way from the meter to the utility company.

Manuscript received 16 June 2009; revised 17 November 2009 and 13 January 2010.

T. Khalifa is with the Dept. of Electrical & Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada, N2L3G1 (e-mail: tkhalifa@uwaterloo.ca).

K. Naik is with the Dept. of Electrical & Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada, N2L3G1 (e-mail: knaik@swen.uwaterloo.ca). Dr. Naik acknowledges the Natural Sciences and Engineering Research Council of Canada for supporting this work with a Strategic Grant.

A. Nayak is with the School of Information Technology & Engineering, University of Ottawa, Ottawa, Ontario, Canada, K1N 6N5. (e-mail: anayak@site.uottawa.ca).

Digital Object Identifier 10.1109/SURV.2011.041110.00058

### *History of Meters*

Over the past years, metering devices have gone through much improvement, and are expected to become even more sophisticated, offering more and more services. Meters in the past, and today in a few countries, were electromechanical devices with poor accuracy and lack of configurability. Theft detection was also a challenge. Such meters are limited to providing the amount of energy consumption on site. Today, meters are digital devices enjoying a higher accuracy, added control and configuration functionality, and better theft detection ability. For data collection, the meter can be read through a serial port (e.g., RS232) or wirelessly (Infra Red (IR) or Radio Frequency (RF)). Next generation meters (called smart meters) should make full use of AMR, and a whole lot of sophisticated services would be available through modern communication facility that will be available on chip. Data collection, theft reporting, and control can be remotely achieved from the utility company.

Smart meters enjoy high hardware/software capabilities that enable them to run TCP/IP suite and have the ability to run applications on top of TCP or UDP. Smart meters are equipped with processing capability ranging from SoC (system on a chip) microcontrollers to 32-bit processors (e.g., Cortex CPU M series and Cirrus Logic's CS7401xx series) (Fig. 1). The operating system, supporting an extensive library of routines and applications, has a task scheduler that rotates between a number of tasks such as communication, measurement and database management [1].

### *AMR Benefits*

- Real time Pricing: Customers are charged tariffs that vary over a short period of time, hourly for example. It helps customers control their consumption and helps utility providers to better plan for the energy market. Barbose et al. [2] provide an in-depth study of the real time pricing.
- Power quality measurement: The electric utility engineers need more detailed readings than Kwhr so that they can efficiently plan the network expansion and deliver a higher quality of supply [3]. Power quality involves the measurement of voltage sags, swells, under and

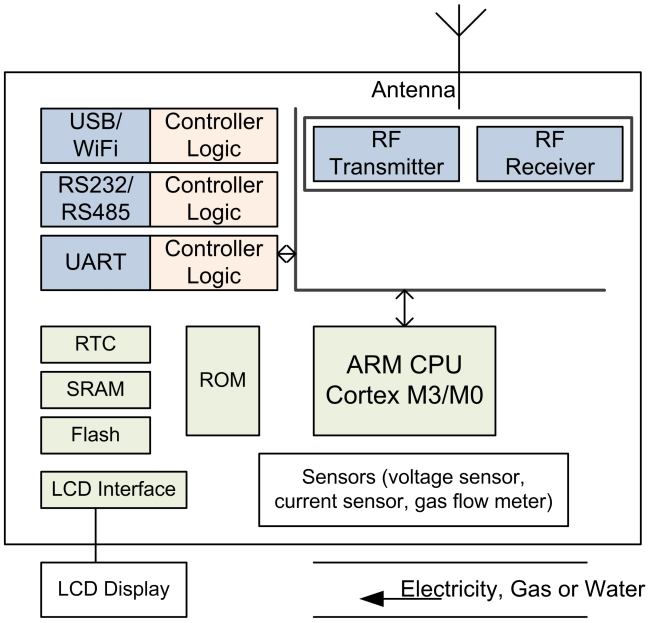



Fig. 1. Smart Meter H/W Architecture

over voltages, harmonics distortion, voltage and current imbalances, and record duration of each event [4] [5].

- Automated Billing: Once the metering data is available at the utility company premises, billing, acknowledgement of received payments, and power consumption reports can be fully automated and made available to customers, on the web for example.
- Load management: This is another industrial area that will be feasible after having an AMR system in place. The service allows sending control signals to appliances such as air conditioners, and heaters. Surrat [6] discusses the importance of load management to electricity providers as well as to customers in terms of power saving.
- Remote Connect/Disconnect: The utility provider can remotely and quickly configure the meter to enable or disable energy to certain customers.
- Outage notification: This offers an effective way to improving response time. Liu et al. [7] propose an algorithm that involves two steps: outage locating and outage confirmation through meter polling.
- Bundling with water and gas: The ultimate objective behind a fully functional AMR is to serve all kinds of meters, electricity, water and gas, under one communication technology and one protocol standard.

What AMR can offer is not limited to what has been mentioned above. Generally speaking, having a two way communication facility in place definitely enables many sophisticated services such as the above bullets and others in [8] [9]. However, without a reliable AMR network, none of the above can be met.

Various communication technologies have been proposed recently, with Power Line Carrier (PLC) being atop the list because cabling infrastructure is already available. Nonetheless, due to its limited bandwidth, PLC alone can hardly scale to support a large network in addition to other shortcomings (Section II-A). Other communication paradigms are needed to implement a full-scale AMR, not only for electricity meters but also for gas and water meters. Electricity providers seem to be at the front today, but in fact all utility providers are interested in collecting high frequency of data and ultimately in enhancing the quality of utility provision and quality of service. Soon, the AMR network will eventually have to serve all meters together. Two issues are to be taken into account. First, the proposed communication technology should be scalable in terms of the capacity as well as the area of coverage. The second issue is to comply with a standardized approach to allow diversity of meters and communication media.

This paper makes the following contributions.

- It provides an extensive survey of all the communication technologies that have been used or proposed as the AMR backhaul network, with the pros and cons of each of them.
- It highlights the experiences learned from wireless sensor networks. Although very similar to the AMR network, sensor networks require investigation as how the protocols may be of benefit and whether they fit.
- It investigates as well the suitability of the 3G wireless technologies as the backhaul network for AMR.
- It discusses the Data Language Messaging Specification/COmpanion Specification for Energy Metering (DLMS/COSEM) standard and proposes using SIP as the signaling protocol.
- Finally, it presents the challenges that the AMR application must address for a proper design.

The rest of this work is organized as follows. Section II provides an extensive survey of the major technologies that have been proposed as the AMR backhaul networks. Section III provides directions for designing the AMR system in light of 3G wireless technologies. This section discusses the technical requirements and data collection mechanisms that should be considered and highlights the differences between meters and wireless sensors. The proposed technologies (3G wireless) are assessed here as well. Section IV discusses the international communication standards to be taken into consideration along with the possibility of using a session control protocol. In Section V, the challenges from the end-to-end application communication stand point are discussed. Finally, Section VI provides concluding remarks for this work.

## II. AMR Current Technologies

Some manufacturers such as CellNet Systems [10], Hunt Technologies [10], and Leach Industries [11] have already worked on digitizing and equipping the currently available meters with various communication facilities. The major part of an AMR system then is the underlying communication technology over which to deliver packets from both sides. There are four major types of AMR communication networks: power line carrier (PLC), cellular network, telephone/Internet, and short range radio frequency.

### *A. Power Line Carrier (PLC)*

In this technology, data is transmitted over voltage transmission lines along with electrical power. Factors such as

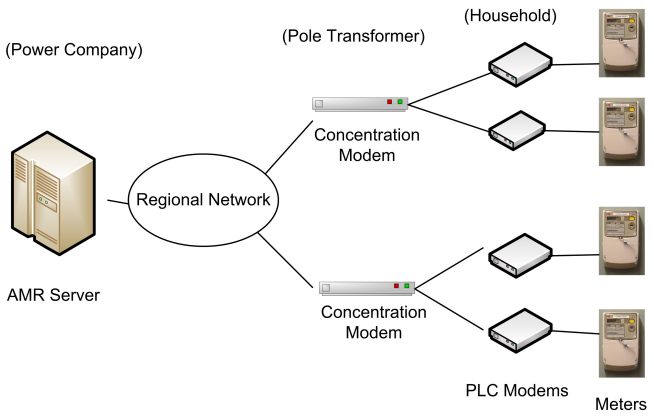



Fig. 2. PLC AMR Diagram

the choice of frequency, propagation speed, voltage level carried, distance between the two communicating points and the existence of transformers affect the PLC communication properties.

PLC has gained great interest as the AMR backhaul network because no extra cabling is required. Kerk [12] and Soh [13] argue that a PLC AMR combined with a wireless technology network is the only solution to reduce the tariff price and be able to serve more houses in India and Singapore.

Park et al. [14] discuss the technical features and the available standards for PLC modems, and propose a combination of PLC network and data network (Fig. 2). Every electricity meter is connected to a PLC modem through RS232 data port. Multiple PLC modems, corresponding to a group of houses under the same pole transformer, connect to a single concentrator modem. The concentration modem bridges the PLC network to a data network. Meters report their measurement when they are polled. The PLC modem buffers the frames until an ACK is received, or otherwise the frame is retransmitted. No evaluation of the system is provided.

Choi et al. [15] propose the use of PLC as means for delivering the electricity, gas and water measurements to the utility providers. The system involves various devices and different communication technologies (Fig. 3); water, gas, and electricity meters transmit their measurements over wireless links to a device called Home Concentration Unit (HCU), which is to be installed in every household. A number of HCUs, normally from different households, send the measurements to a device called Data Concentration Unit (DCU), which eventually sends the metering data in DLMS (Device Language Message Specification) format via a PLC modem to the utility company. Traffic direction is only from the meters to the utility provider. No metrics for evaluation or comparison with other designs are provided.

Moghavvemi [16] focuses on digitizing the meter and detecting tampering. The author uses an optical encoder to generate signals and counts them as the electro-mechanical disk rotates. For tamper detection, the data concentrator analyzes the data received and checks whether abnormalities appear. Similarly, Raja and Sudhakar [17] focus on the technical design of the PLC modems. Nevertheless, they do not show how to communicate between the modems from a long distance and how to bypass the transformers. Oska et al. [18]

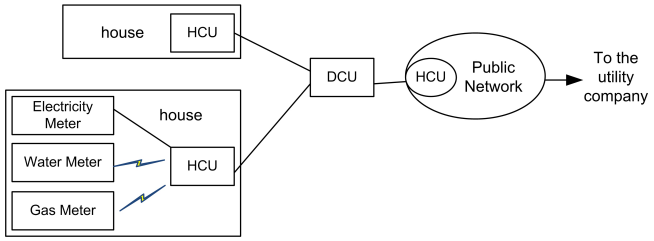



Fig. 3. IMR System Diagram

provide testing results for using one hop communication over power lines. They conclude that the length of the cable and the structure of the electrical network affect the throughput, causing a reduction of 65% when the cable length reaches 10 meters.

Selga et al. [19] work on the MAC (Medium Access Control) layer. They borrow a wireless sensor network MAC protocol called “Ripple Control" for PLC-based AMR networks. They assume having a chain of meters ending at a concentrator and forming a star-like topology. The concentrator acts as a controller and aggregator. They argue that the best capacity can be achieved when a receiver initiates the connection.

Yu et al. [20] study the problem of the so-called silent node. When a base station (BS) polls all the metering nodes, it may fail to communicate with certain nodes due to environment noise. The paper proposes modifying the polling mechanism to resolve this issue. The system is modelled as a number of buildings (50-80 apartments per each) connected to the same distribution transformer, thus having the same BS (Fig. 4). In simple polling, where the silent node problem may occur, the BS polls all the meters in a cyclic order. Each meter responds immediately with its available data. If a certain meter does not respond, the Enhanced Polling (EP) mechanism is used. The BS re-polls the node in question after having finished the cycle. A third proposed mechanism, called Neighbor Relay Polling (NRP), which lets the BS attempt to communicate with the not-responding node through a neighboring node. Three metrics are used to evaluate the simulation: data collection success rate, collection delay, and number of additional polls. In the simulation, 504 units are assumed. A complete cycle to poll all the meters is as high as 30 minutes.

PLC technology however faces a number of challenges: noisy medium, high signal attenuation, and susceptibility to interference from nearby devices, leading to high loss rate. Scalability of PLC-based AMR is also in question. There is no work to show how much geographical area a PLC network can cover or how frequently the metering data can be reported. Lastly, PLC has already been deployed for broadband services in many countries. However, in certain countries such as Australia, Russia, and United States, such deployments have been terminated. The reason is the high cost involved and the fact that other means of communication of higher stability and reliability are available.

### *B. Messaging over GSM Network*

Short Message Service (SMS) has become a communication protocol allowing parties to exchange delay-tolerant short text messages. It is supported by different standards, namely

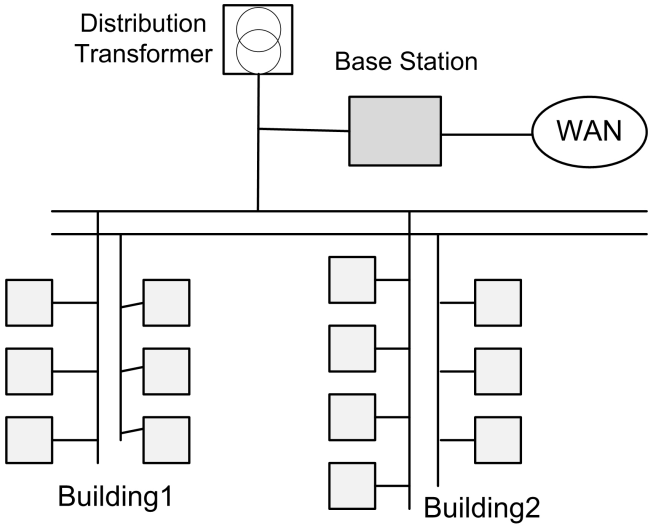



Fig. 4. PLC-based AMR in Singapore

Global System for Mobile communications (GSM), Code-Division Multiple Access (CDMA2000) and Digital Advanced Mobile Phone Service (D-AMPS). The popularity and wide coverage of cellular networks have attracted researchers to consider the use of SMS service.

Tan et al. [21] propose an AMR system design that utilizes a GSM network. The system constitutes at the consumer site a digital meter with RS232 interface and a GSM modem containing an SIM card dedicated for only SMSing; and at the energy provider site an SMS gateway to send and receive messages. Measurements are reported once a month. An SMS message contains six digit KWh with one decimal point of the energy consumption. The SIM card number acts as a unique number to identify a customer. To boost reliability, the meter stores the latest reading in an Electrically Erasable Programmable Read-Only Memory (EEPROM), and it keeps trying to send the SMS multiple times. Nevertheless, metrics are not identified for evaluating the reliability and strength of the system.

Abdollahi et al. [22] also suggest the use of GSM networks. Communication can be either one way or two ways. In the uni-direction setup, meters send readings at predefined intervals and switch off otherwise to conserve energy. In the bidirectional setup, the energy provider can have more control over the meter but requires the meter to be active all the time. Measurements are reported once a month as OBIS (Object Identification System) codes. However, no evaluation of the system performance or comparison with other designs is provided.

Scalability and reliability of such a network however is questionable, especially under high load. Zerfos et al. [23] have analyzed real data taken from a real GSM network in India. SMS delivery success rate was found to be 94.9%; 73.2% of the successfully delivered messages reach to the destination within 10 seconds; about 5% of them require more than an hour and a half. Using SMS for AMR service will definitely increase the flow of messages tremendously. Meng et al. [24] provide analyses of latency and failure ratio under high load. For example, on a New Year eve, the volume of SMSing increases eight times. Consequently, latency grows from several minutes to an hour. Failure rate shows an increase to 20% as well. All in all, SMS should be further investigated before being used for AMR. For example, can cellular networks support messaging frequency of up to a message every 15 minutes? How reliable is the network in that case?

### C. Telephone Lines

Telephone lines are desirable, for they offer a highly reliable, relatively inexpensive, and simple to operate solution. An AMR system can use telephone lines for inbound, outbound, or bidirectional communication. The connection is initiated from the customer site in the inbound mode, while initiated from the energy provider in the outbound mode. In the bidirectional mode, connection is initiated from either site, enabling more services such as sending out queries and collecting measurements. Utilizing telephone lines for this purpose is an old proposal ( [25]), but continuous to interest developers such as COMETECH M2M [26] and as proposed recently in [27].

Lee et al. [25] describe an AMR system that utilizes the public switched telephone network (PSTN). They describe the hardware of the two end points: Remote Reading Unit (RRU) and Communication Front End (CFE). At the customer site, RRU is installed, where it can connect up to three meters, possibly of different kinds. At the utility company site, the CFE is installed. It consists of a regular computer and a modem. The RRU and CFE communicate with each other through the telephone network in both directions, allowing the RRU to send data frames, and the CFE to send commands. Measurement reporting can take place either on demand or periodical. The CFE collects the information sent by all the RRUs, and transmits them to processing and billing servers. The ability of having two-way communication allows the utility company to reprogram the RRUs, for example, to change the reporting schedule. An RRU can store the measurements until it is successfully delivered to the CFE. NACK and timeout are used to learn about any failure. However, no evaluation or performance metrics were introduced.

Kim [27] provides a design description of a telephone line AMR system. In this system, the meter device comprises the following parts: an interface module to connect to the remote control center through a telephone line, a main control unit (MCU) to generate control signals that embed the Caller ID (CID), a CID decoder to decode the meter reading request signal and CID, and a memory to temporally store measurements. Meter data and control signals from the control center are transmitted in the form of dual tone multi-frequency signals (DTMF).

The availability of a telephone line at each meter is a requirement that can not be always satisfied, especially in developing countries. However, telephone lines can be considered for far and isolated locations, in which wireless coverage is missing.

### D. Short Range Radio Frequency

Short range Radio frequency (RF) in this context refers to low-power RF facility at the customer site. A number of

technologies can be classified under RF: Bluetooth, WiFi, Zigbee, depending on the signal power and frequency band. It is unlikely that the gas and water meters will share the same power line communications infrastructure because utility companies may not share their network infrastructure [28]. Koay et al. [29] propose to equip electricity meters with Bluetooth modules to deliver the readings wirelessly to a nearby PC (or PDA) directly. Metering data is then forwarded through a dial-up connection to the energy provider or collected by a walking by person. Meters transmit their data either periodically or whenever they are polled. Bluetooth as a solution to AMR is not plausible anymore today; however, it stays a viable solution in certain circumstances (e.g., at AMR early deployments). For example, meters with Bluetooth modules already installed may send their data to nearby devices, which in turn forward the data using a better technology.

Wesnarat and Tipsuwan's work [30] aims at networking water meters as a wireless sensor network. Because the meters feed on battery, and because fusion (aggregation) is not possible, the problem tackled here is how to arrange these meters such that power consumption is kept low, mainly by avoiding long packets. Meters form sub-trees with a base station being the root node. Every meter reports its measurement through other meters. The BS then sends all the received measurements from all the sensors to the final control station using SMS or GPRS. Spencer [31] claims that compression can also reduce the packet length due to two facts: (i) Data reported from different households tend to follow a certain probability distribution. (ii) Successive data from the same meter correlate. However reduction is only 3 bits.

Zhu and Pecen [32] propose to let the meters create a wireless mesh network with IEEE802.15.4 as the underlying technology and Zigbee standard for the upper layers protocols. The authors claim that this combination of protocols and network setup guarantee real time collection of data, but no experimental validation is provided. Zigbee has received big attention as a solution to AMR because the technology is already designed for low rate applications and consumes minimal energy, enabling a device to last for a number of years. Also it supports a variety of strong routing protocols. However, it is worth noting a number of drawback. Bandwidth is very low (20 kbps at 868 GHz and 250 kbps at 2.4 GHz ) [33]. With the increase of the number of nodes, interference increases dramatically. That makes its connections and routing paths unstable and incurs high delay, thus making the technology hardly reliable and scalable for AMR.

Although RF has been actually used for AMR in many countries, the services it provides are very limited. With sensor networks, connecting to all meters may fail due to far nodes or those whose parent nodes fail. Thus an alternative is necessary to implement a fully automated, full-scale AMR system.

## III. The Future of AMR

This section discusses four main points to study for a successful AMR system deployment. First, it is important to distinguish between an automatic meter network and a wireless sensor network in terms of their characteristics. Second, design a network under certain technical requirements and evaluate the network according to certain measurement metrics. Third, select a reporting mechanism. Fourth, select a communication technology. Emerging wireless technologies are expected to have large deployments in the near future. Thus, it is just time to explore their suitability for AMR.

### A. Metering Devices As Wireless Sensors

A meter device functionally is a sensor node that provides energy (electricity, gas, or water) consumption measurement. The number of meters can grow to thousands, and data are typically fused and delivered to a centralized location for processing and decision making. Such characteristics make metering equipment viewable as a regular wireless sensor that can form a wireless sensor network (WSN), which is investigated extensively, and for which a good number of protocols have been proposed that can be benefited from for AMR. Wireless sensor networks are diverse in the application objectives, density of nodes, H/W constraints and nature of traffic (direction and urgency of data). The recent research in the field of WSN typically takes the approach of considering those factors to optimize communication protocols to best satisfy the overall application objectives [34]. AMR as a sensor network compares to those of large-scale sensor with the combination of traffic types: sensor to sink (upstream) event-driven data and periodic data gathering, and sink to sensor (downstream) sink-initiated querying. Thus, while referring to WSN, it is important to highlight the special characteristics of AMR that may be involved in choosing or designing the right protocol.

- At the application layer, before data transfer can take place, a connection must be established between the end points, which requires to maintain end-to-end reliability semantics. This end-to-end connection is not recommended for large-scale sensor networks because of the lack of unique Internet-like addressing for each node, and because it results in large in-network packets and high end-to-end delay [35]. In such networks sensors typically send their available readings to the nearest in-range nodes [36] [37]. For that reason, most of the work focuses on maintaining hop-by-hop reliability (e.g., [38] [39] [40] [41]). End-to-end reliability semantics work is also available however. Dunkles et al. [42] proposes a version of TCP/IP that is tailored to sensor networks by maintaining end-to-end semantics combined with hop-by-hop reliability. The protocol caches packets in nodes to reduce the burden of end-to-end retransmission of lost packets. Park et al. [43] propose a downstream reliability protocol for delivery of control data and queries. Another way of addressing reliability semantics is event reliability, which may suite AMR event-driven data. That is to make sure an event is reliably reported to a base station with a certain degree of accuracy (e.g., [44]).
- To achieve scalability and elongated battery life in large-scale sensor networks, instead of having homogenous sensors rotating the role of clusterhead among themselves, heterogeneity is introduced [34]. That is, nodes that have sophisticated hardware and higher battery energy take on the role of a clusterhead to perform

complex computations and long range communication. Each clusterhead manages its cluster autonomously. The cluster may consist of nodes with different hardware capabilities. Mhatre et al. [45] explain about such a design of heterogeneous networks, and in [46] Mhatre and Rosenberg present a cost-based comparison between homogeneous and heterogeneous networks. The positioning of clusterheads, however, is a question of optimality problem. In AMR, meters are also diverse in their hardware capabilities. Electricity meters feed on main power supply. Gas meters feed on batteries (for safety measures.) Water meters feed on both. That makes an electricity meter a good candidate to be a clusterhead to fuse traffic from the other meters that feed on battery. Positioning of the meters, however, is not controllable.

- To reduce traffic load of a sensor network and reduce energy cost, the amount of data transmitted in the network is reduced by means of data aggregation. Typically, in large-scale sensor networks (e.g., habitat monitoring [47]), the sink is not interested in the individual measurements, but requires a distributed computation of some function of the sensor readings. Data aggregation allows nodes to combine multiple readings into one report containing the result of a function such as average, median, Min or Max [48]. Different algorithms are available to achieve that. For example, Tiny Aggregation (TAG [49]) and [50] allow the sink to send queries to a certain set of nodes and let the nodes along the path perform the requested data aggregation type. In [51], in addition to aggregation of data, the protocol increases the energy saving by increasing the path sharing among different sources. In AMR, however, packets carry unique information identifying a specific meter and the exact time of the measurement. Therefore, measurement data from individual meters must reach the collection center while preserving its information.
- In large WSN with sensors distributed over a large geographical area, because sensors have limited energy and because they sometimes exist in harsh environment, node failure occurs commonly, which leads to service degradation [52]. In sensor network deployments (e.g., glacier monitoring and tracking military vehicle applications) node failure is tackled in two ways: deployment of redundant nodes and use of algorithms to detect and isolate faulty nodes [53]. In AMR, meters are distributed deterministically with zero redundancy at every energy distribution location (e.g., residential houses). However, if a meter ceases to operate or malfunctions, immediate investigation and maintenance must take place. In other words, a fault detection mechanism is essential. Fault detection protocols for sensor networks are available in literature with a common objective; that is to be energy- and time-efficient. Jiang [54] presents a review of fault detection protocols and proposes an enhancement to increase accuracy when number of neighboring nodes decreases. Yamanouchi et al. [55] evaluate the reliability of sensor networks under different weather conditions using a fault detection algorithm that investigates the collected sensory data. AMR characteristics such as the periodicity of data reporting and static topology should be considered to optimize fault detection mechanisms.
- With regard to routing, WSN protocols may be considered for AMR, but attention should be paid to the fact that meters have fixed positions. As such, a protocol that considers the node location is preferred (e.g., [56]). Nevertheless, if meters communicate to a base station in one hop, then such protocols are not suitable. Moreover, large sensor network routing protocols use attribute-based addressing. The sink issues an attribute-based address composed of attribute-value pair queries. Meters, in contrast, need to be uniquely identified. For example, the control station may need to connect/disconnect energy for a specific customer. Thus, routing should be looked at in light of a different addressing mechanism, which leads to the use of IPv6 as being currently discussed by IPv6 over Low power WPAN (6LoWPAN) Working Group in [57].
- AMR must support bidirectional communication to allow for meter set-up and reconfiguration at any time. In most of WSN applications, this requirement does not necessarily hold.
- Meters may have similar real time constraints to certain sensor applications. Nonetheless, one should stress that the delay in AMR is tolerable within a defined time window, determined by the meter measurement schedule.
- Security is a serious concern in both, meters and sensors [58]. However, the biggest concern in meters is the provision of data integrity as opposed to data privacy.

The aforementioned differences between meters and sensors must be taken into account when designing a new protocol for AMR. Rather than employing or even modifying a protocol that is generic for wireless sensors, identifying the differences and the unique meters characteristics definitely leads to a successful and efficient AMR design.

### *B. AMR Technical Requirements and Performance Metrics*

One missing aspect in the previously discussed design proposals is evaluation. An AMR network should meet certain quality requirements. Thus any new design has to be assessed according to a number of quality metrics as following:

Reliability: The AMR network must guarantee the arrival of all meter readings as well as all utility server control packets. The success rate or the loss rate performance metric shall give us a fair assessment of the given network.

Scalability: A designed network shall be assessed according to its ability to providing support to a large number of meters covering a large geographical area. Furthermore, the frequency of such readings should be high enough to support the desired AMR services (e.g. real time pricing.)

Real time communication: Data reported from a given meter must arrive within a given amount of time. Certain traffic types (e.g. fault detection) mandate a short time delay. A performance metric of end-to-end delay is required to provide a good evaluation of response time of the different traffic types.

Order: Packets representing different readings should be stamped with the time of measurement so that packet ordering at the receiving station can be guaranteed.

Security: The level of security can be expressed in terms of the cryptographic tools implemented at different protocol stack layers and the number of key bits used. Hop-by-hop security is implemented at lower layers while end-to-end security is implemented at both ends of the AMR application.

### C. Data Collection Mechanism

All the previous work focuses on gathering power consumption information, in which AMR data is pushed from meters into the network at certain fixed times. As utility providers are interested in a large variety of data with much higher frequency, three modes of communication are required to be supported: fixed scheduling, event-driven and demand-driven. Each mode is more suitable for a certain kind of data and as such the three modes must co-exist. Each mode poses a different design challenge.

Fixed Scheduling: In this mode, a meter reports data at fixed intervals. This is a straight forward mechanism with the advantage of guaranteeing a certain rate for every meter under the knowledge of the available bandwidth. However, the traffic that results is significantly high. It may impact other Internet traffics at bottleneck nodes. As a result, packets will be dropped and data reports may not meet the delivery deadline. Sbai and Barakat [59] discuss the problem of gathering data from a large number of sources and propose a pulling mechanism at transport level to shorten the duration of a collection session and to reduce the ratio of packet loss.

Event-driven: Data are generated and transmitted as a result of events at meters. Examples of this mode include packets generated when consumption reaches a certain threshold value, power quality when it starts to degrade, and includes alarm data. This mode may cut down the amount of traffic though it will vary from time to time; however, a tradeoff must be considered as a contention overhead and possible delay will be introduced.

Demand-driven: Upon a request from the data collection center, data packets are generated and transmitted back. A utility company uses polling to identify faults, or gets a consumption report at a certain time for a subset of meters. Polling requires extra messaging for the end parties to re-authenticate and set up other communication parameters every time. Demand-driven data typically require realtime response. Therefore, such data should be distinguished from the rest and given a higher level of priority.

### D. 3G Wireless Technology for AMR

Technologies such as PLC, GSM, telephone, and RF (Section II) have not been completely satisfactory. To support more services, AMR demands investigation into more sophisticated technologies with higher bandwidth. Third generation (3G) wireless technologies are getting more and more attention today for their flexibility, easiness and high speed of deployment, cost-effectiveness, scalability, and business needs.

Various 3G wireless technologies have been introduced to the community, some of which had actual implementations. Long Term Evolution (LTE), High Speed Packet Access (HSPA) and IEEE 802.16 (known as Worldwide Interoperability for Microwave Access or WiMAX) comply with International Mobile Telecommunication (IMT-2000). WiMAX

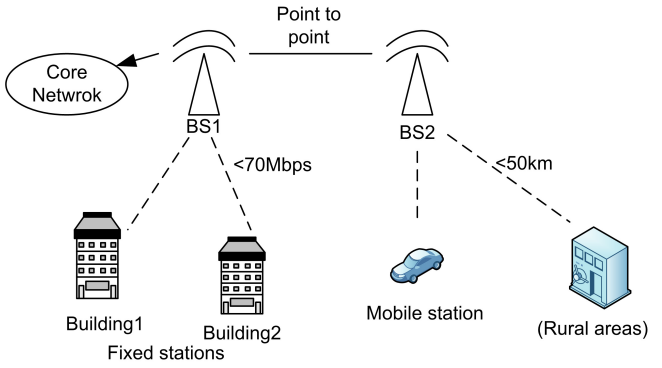



Fig. 5. WiMAX: Typical Architecture

was added in 2007, giving it significantly larger global popularity.The solutions engineered tend to be similar since the goal and the underlying technical solutions are fundamentally the same: wideband transmission, high-order modulation, fast scheduling, advanced receivers, and multi-carrier. What will make either of the technologies more popular than the others will be determined by industry. Currently, WiMAX and LTE are atop the list, and with regards to AMR both of them are good candidates.

WiMAX is described as Metropolitan Area Network (MAN). Its first version was developed for fixed wireless broadband access in the 10-66 GHz bands and line-of-sight communication in 2001. IEEE802.16a (2-11 GHz bands, 2003) supports non-line-of-site communication. Typically, a WiMAX system consists of two parts (Fig. 5):

- A WiMAX base station consists of indoor electronics and a WiMAX tower. A range of 7-10 km is a typical cell size, although 50km is proposed in theory. Several base stations can be connected with one another by use of high speed backhaul microwave links, forming a mesh network.
- A WiMAX receiver (a PCMCIA card or stand alone box) enables a device (e.g. electricity meter) to get access to the wireless network with a data rate that may reach up to 70 Mbps.

Similar to WiMAX, LTE has a great potential in being widely deployed in the near future as it can flexibly operate on different frequency spectrums (1.25 MHz to 20 MHz). It offers high data rates with low delay and large cells: data rate of 100 Mbps and 50 Mbps at 20 MHz spectrum for downlink and uplink respectively, 5 ms latency to send a packet from a terminal to radio access network edge, cell size of 5 km typically, and up to 100 km but with relaxed performance requirements.

Typically, an LTE system will have two types of network elements: (i)The evolved NodeB (eNodeB), which is in charge of a set of cells, and it controls Radio Resource Management (RMM), Handover, and scheduling of users. (ii) Access Gateway (AGW), which provides access to the IP core network [60].

*WiMAX Example:* The following scenario illustrates the WiMAX capability as to what extent it can serve in terms of the number of meters. For that, we assume a fixed WiMAX system (IEEE802.16-2004), with a signle BS. The air trans-

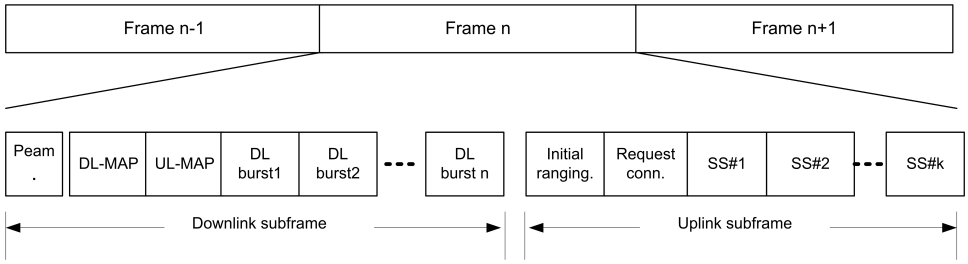



Fig. 6. WiMAX TDD Frame Structure

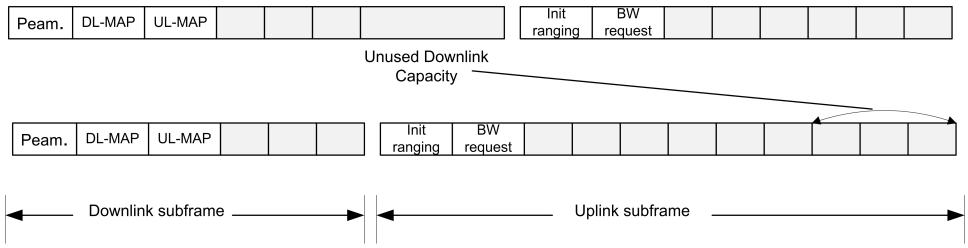



Fig. 7. Downlink/Uplink TDD Slots Ratio

mission scheme uses OFDM of 256 subcarriers, of which 192 subcarriers are used for data transmission. TDD is assumed, for it is more common and has more advantages than FDD [61].

Fig. 6 shows the TDD framing structure. Time is divided into frames of a length of 2ms to 20ms. Each frame is split into a downlink and an uplink sub-frame. At the start of a frame, the base station sends a list of downstream media access protocol (MAP) messages containing information about the physical-layer properties that will be used in the subsequent bursts within the frame. The physical layer properties include modulation scheme, coding, and error-correction parameters. The base station selects the set of subscribers to which it will transmit during this frame on the basis of the estimated current channel conditions to each subscriber. For the uplink, the base station also schedules the subscriber stations access to the channel through UL-MAP messages. These messages specify the amount of time assigned to a subscriber within the uplink sub-frame. Two more fields can be noticed in the uplink sub-frame: the initial field is used for subscribers to transmit radio link control messages requesting admission and authentication, and the request connection field, during which subscribers may contend to send their bandwidth requests.

Each burst (a.k.a slot) can be assigned to a different subscriber, i.e. a meter. Meters skip the bursts that contain no relevant traffic, thus reducing the processing load. A good feature as well is that a downlink burst can be shared among multiple meters, for example, for broadcasting a certain information. The downlink/uplink number of slots ratio can be configured according to the traffic type, typically 70/30, 60/40, 50/50, or adaptively [62] (Fig. 7). Although it would be more efficient to assign more slots for the uplink than for the downlink in AMR, we assume only half of the slots are for the uplink.

Numerically, we assume a WiMAX cell configured with TDD duplexing, a frame size of 5 ms, symbol size of 50 s, and 2 symbols per time slot. Thus, a single frame consists of 50 time slots. Taking out the time assigned for control signaling, the number of data slots would be 40 slots. Assuming 50/50 downlink/uplink ratio leaves 20 time slots for uplink. In a TCP/IP setting (Section IV-B), a meter may send packets of size of 100 bytes typically. However, to calculate how much data can fit in a single slot, we need to learn what modulation and coding techniques could be used. In the worst case scenario, when the channel is noisy, BPSK with a coding rate of $\frac{1}{2}$ is used. A slot of 2 symbols with 192 subcarriers results in 24 bytes in a single slot. However because of the coding mechanism, it is 12 bytes only that correspond to the actual data. The rest are redundant. On the other hand, when the channel is at its best, 64-QAM modulation with $\frac{3}{4}$ coding rate results in 72 bytes of actual data in a slot. In this case, a meter may need two to ten time slots to send a single packet, depending on the channel conditions. Furthermore, a complete session to retrieve information from a meter consists of three stages: 1) establishing the connection, 2) data transfer, and 3) connection release. Thus, depending on the type of information collected, a session may involve a number of message exchanges between the data collection system and the meter (for examples see [63]). Assuming an average of 100 bytes packet size and 5 upload packets per session, the following estimation holds. a rate of 20 slots per 5 ms corresponds to 2.4 million slots in 10 minutes. With each meter reporting its measurement once within this time window, this channel may support up to 48 thousand to 240 thousand metering devices ideally.

In conclusion, technologies such as WiMAX and LTE offer a truly scalable solution to the AMR system, supporting a large number of meters and frequent measurement reporting.

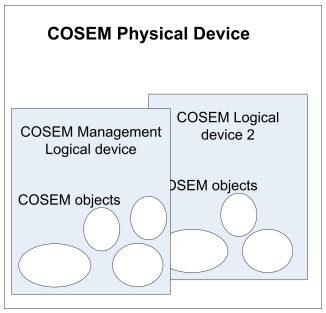



Fig. 8. COSEM Model

They can cover large areas of different demographics (urban, suburban, and rural), yet they are inexpensive solutions, easy, and fast to deploy. These features make a strong incentive to consider the 3rd generation wireless technologies such as WiMAX, HSPA or LTE to support the AMR system. The choice of the technology will be largely determined by industry as which will be implemented in a country or city.

However, although 3G technologies seem much superior, other technologies (Section II) are still of high interest to study. Practically, Meters could be densely deployed and thus can form mesh networks or, on the other hand, could be sparsely installed and therefore meter to meter communication is not feasible. using telephones for example can be a good solution for isolated meters. Moreover, some of the currently deployed meters are already equipped with old communication facilities such as Bluetooth and modems. Especially that early deployments will not demand high frequency of measurement reporting, such old technologies can still be accommodated. In other words, an AMR network may involve a hybrid installation of various technologies, including 3G network and the Internet.

In terms of capacity, Other technologies are meant to provide automatic meter reading based on one or two month scheduling. They are not suitable for every 5 or 10 minute schedules. For that reason, they are omitted in the calculations. 3G (possibly combined with other technologies), as shown above, can cover a large area and support frequent meter data reporting. However, that is not enough. Other issues should be addressed at different layers. Section V brings a number of challenging issues to discussion.

## IV. Communication Protocol Standard

### A. DLMS/COSEM Standard

As important as designing a scalable and reliable communication network is to conform to the international standards. The International Electro-technical Commission (IEC) is the organization that prepares international standards for all electrical and electronic technologies [64]. Cooperating with IEC, DLMS User Association [63] takes the metering devices (electricity, water, heat, and gas) to be its main focus. The objective is to ensure interoperability among energy distribution devices so that they can exchange information/control messages under various physical media and communication protocols.

The metering standard,supporting electricity, gas, heater and water equipment, is known as the Device Language Message Specification/COmpanion Specification for Energy

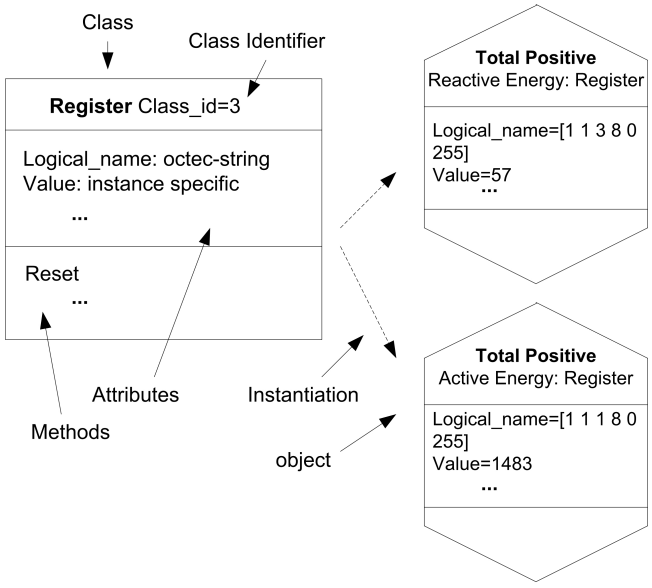
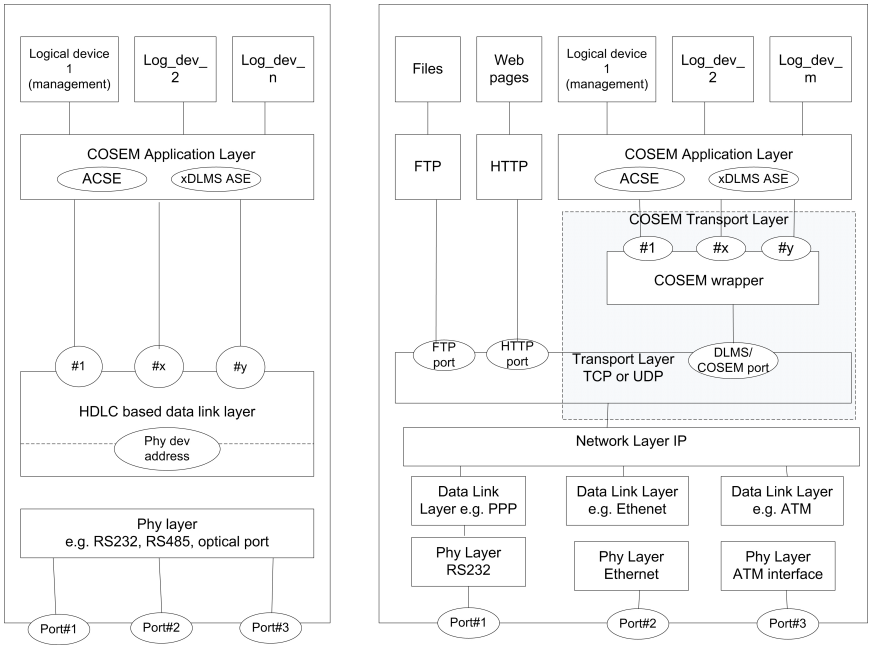



Fig. 9. An interface Class and its Instances


Fig. 10. OBIS Code Structure

Metering (DLMS/COSEM) [65]. DLMS is an application layer specification. COSEM presents an object oriented model for the meters, providing a view of their functionality through communication interfaces. In COSEM, the physical metering equipment is viewed as a set of logical devices (Fig. 8). Every logical device has a world-wide unique identifier and holds certain information, which is modelled by interface objects. The information is organized in attributes and can be accessed through methods, depending on the access rights (Fig. 9). These attributes and methods are accessed at the application layer using the xDLMS protocol services, which arrange the results into data packets (APDU) and delivers them through a stack of layers to the peer application. DLMS/COSEM provides standard codes to reference to all the information in the meter device (OBIS codes) and defines a protocol stack for communication as explained below.

*Object Identification System OBIS:* OBIS provides standard identification codes for all the data items, which are used for configuration or obtaining information about the behavior of the meter. OBIS codes are organized into a hierarchical structure using six value groups of size one byte each A to F (Fig. 10). The value group A defines the energy type to which the metering is related. Group B defines the channel number, assuming different connections, possibly from different sources. Group C defines the abstract or physical data items related to the information source concerned, for example, current, voltage, or temperature. Group D identifies the processing methods and country specific codes. Group E is used for identifying rates or can be used for further classification. Last, group F is used for identifying historical values or can be used for further classification. A list of OBIS codes for electricity, gas and water is available in [66].




(a) 3-layer,CO,HDLC-based profile (b)TCP-UDP/IP based Profile

Fig. 11. Communication Profile Models in DLMS/COSEM

### *B. DLMS/COSEM Communication Protocol Stack*

Data exchange between a metering equipment and data collection system is based on the client/server paradigm, with the meter device acting as the server and data collection device as the client. Exchange of messages such as *SERVICE.request/.response* goes through a protocol stack. DLMS/COSEM supports different communication profiles (set of protocol stacks.) A single device may support more than one profile so that communication can take place over various communication media (e.g., Ethernet and GSM)

Figure 11 shows two common profiles: the first is the layer, connection oriented (CO), HDLC-based profile. This consists of the COSEM application layer, the HDLC-based data link layer and a physical layer for connection-oriented asynchronous data exchange. It supports optical or electrical ports (e.g. RS232.) The second profile is the TCP-UDP/IP based communication profile. At the top is the COSEM application layer. Next is the transport layer, which involves TCP or UDP as well as a wrapper. The wrapper's role is to match the TCP or UDP ports to the logical device address. Since TCP and UDP are supported, other services such as FTP and HTTP can also be implemented. The IP layer is used for addressing the physical device and is supported by different sets of lower layers (data link and physical layers), depending on the media used, e.g., Ethernet, PPP or IEEE802 [67].

The support for these profiles as well as others is a strong point of the DLMS/COSEM standard. It enables a data collection system to establish connections with metering devices of different communication protocols and different communication media, thereby allowing a smooth migration from legacy meters to new ones.

### *C. Remote Device Control with SIP*

With the DLMS/COSEM communication standard, a communication session can take place. However, managing the sessions (setting up, modifying and terminating) requires other protocols to be involved. SIP [68] is an application layer protocol. It has been mainly presented in the area of multimedia communication such as voice and video (e.g. Internet telephony [69], and locating Voice Over IP (VOIP) mobile hosts [70].) However, it can be perfectly employed in any application that involves session initiation and event subscription and notification (e.g. file sharing [71].) In the same manner, the AMR system involves the creation, modification and termination of communication sessions. Thus, SIP has the potential in making communication between the meters and the data collection center devices highly flexible and better controlled. That can be seen in the following points:

- SIP determines the media and media parameters (e.g. addresses, port numbers, and media specific parameters.) More session details such as sampling rate and codec can be carried using Session Description Protocol (SDP) [72] encapsulated in SIP messages. Especially at the time of upgrading the AMR from old communication technologies to the third generation wireless technology, determining the media is essential as there will be a large variety of communication technologies.
- SIP determines the availability of the other party to be engaged with in a communication session. For example, the meters may need to determine the availability and the proper data collection device to report to.
- For addressing any of the AMR devices (metering devices, data collection devices, or proxy), SIP makes use of Uniform Resource Identifier (URIs) (e.g.

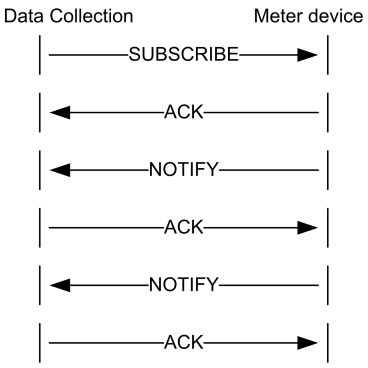



Fig. 12. SUBSCRIBE - NOTIFY Scheme

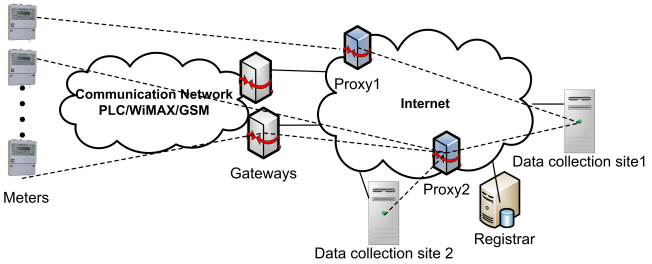



Fig. 13. Remote Device Control with SIP Protocol

user@domain.com), which is more practical.

- SIP makes event-driven and polling reporting mechanisms possible. Data collection devices can register for event notification (e.g. a consumption value has reached some threshold) through the use of SUBSRIBE and NOTIFY [73] (Fig. 12). By setting the field “expires" to zero immediate response (polling mechanism) takes place.

As Fig. 13 shows, SIP involves a number of logical network elements to support the AMR network.

- SIP User Agent Client and Server(UAC and UAS). The UAC initiates the requests and the UAS returns the SIP response.
- Proxy server which is an intermediary entity that makes requests on behalf of other clients.
- Registrar server which takes *REGISTER* requests that come from a UA to notify of its current IP address and the URIs of the devices with whom it can engage in a communication session.

A possible messaging scenario can be seen in Fig. 14 showing the basic functions of SIP. The end points (data collection device and meter) negotiate the session parameters through INVITE and ACK messages. The proxy helps forward the requests from both sides. The COSEM application session takes place next and continues until a termination message from either of the parties is submitted. Any of the end points can start up the SIP session, giving to the AMR high flexibility.

## V. Challenges

The AMR network poses certain challenges that come from the need to handle a large amount of data at a centralized location. The data constitutes small packets transmitted from

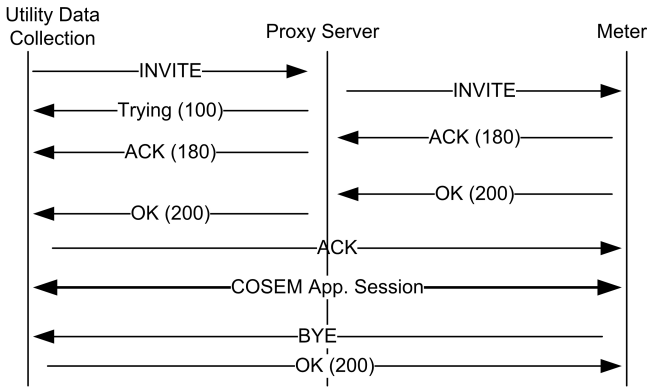



Fig. 14. Messaging Exchange in a SIP Session

hundreds of thousands of small devices (meters) very frequently and control data sent down to the meters. Electricity is at the front today, but the challenges apply to all metering data. The AMR application is particularly different in its management of various types of traffic, its tolerance and reaction to failure, its tolerance to delay, and its security needs. It is important to consider its properties in the application communication design. These distinctive characteristics are summarized in the following enumeration, followed by a discussion showing how they impact the design under their relevant titles.

- Sessions are short (granularity of seconds), with a long waiting period (granularity of minutes) between two sessions.
- Tolerance to delay is different according to the traffic type, ranging from real time delivery to a delay of until next session is due. Constraining jitter delay between successive packets is not necessary.
- Order of data packets can be ignored as long as there is a reordering mechanism at the receiver.
- Data aggregation is not feasible. The collection center must identify uniquely the meter ID and the time at which the consumption measurement is taken.
- Duration of consumption reporting is configurable.
- Loss of messages is not allowed. However, previous energy consumption measurements can be accessed and combined with the current measurement value.
- Identification of and response to failure must be quick.
- Multiple routes exist if a mesh network is created out of the meters. Alternative routes are not available if meters communicate with the base station through one hop only.
- Meters have diverse capabilities. Some meters relax the power constraint, while others feed on a limited source of power.
- AMR needs to be safe from unauthorized access, tampering with data, denial of service, and hijacking of session attacks.

### A. Handling Failure

The AMR system requires a protocol that provides reliability properties such that if failure occurs (e.g. packet loss or device break down), a detection mechanism and preferably an auto-recovery mechanism should take place. Application end-to-end reliable delivery of data is essential here. A transport

protocol such as TCP can guarantee reliability but would incur overhead. Thus, instead of using a generic transport protocol, one that is tailored to the AMR application has the potential of achieving better results. Device break down cannot be handled at the transport layer although it will disrupt the flow of data. Device failure is to be left to the application layer to recover from.

For example, multicasting traffic (e.g. control data from the utility server to the meters) may result in a large overhead if per recipient acknowledgement is employed. Instead, a collective ACK can be considered, in which a gateway node (Fig. 13) combines the ACKs from the meters and forwards a single ACK to the collection center. A similar approach to custody in delay tolerant networks (DTN) [74] can be considered. An intermediate node acknowledges reception from the collection center and then takes full responsibility for delivering the packet to the meters.

For upload traffic, consumption reporting is periodical. If the report is not received at the scheduled time, instead of persistent retransmission, the lost consumption report is aggregated with the next one.

### *B. Real time and Delay tolerance*

AMR Data traffic can be classified into realtime traffic that requires immediate delivery, and delay tolerant traffic. For upload traffic, consumption data can stand a delay of until the next scheduled consumption report is due. However, certain event-driven packets are realtime. Examples include tamper detection, and failure notification. On the the other side, download traffic such as connect or disconnect control packets constitutes realtime traffic.

Typically realtime transport protocol (RTP) [75] is used for the realtime data, and TCP or UDP for delay tolerant data. However, these transport protocols are irrelevant for AMR. RTP, for instance, is designed to deliver the packets while making sure the jitter time is bounded, and if a packet is delayed it gets dropped. With AMR, jitter is not a requirement while losing a packet is unaffordable. Second, the AMR real time sessions are short and occasional. Other transport protocols are either too light (e.g., UDP), which do not guarantee delivery of packets or excessively persistent (e.g., TCP), which do not take advantage of AMR characteristics and thus are inefficient.

### *C. Unicasting and Multicasting*

AMR data constitutes unicast and multicast traffic. The unicast traffic is initiated from both end points: from meters to a utility server and vice versa, with the first type being the dominant. The operation is similar to collecting sensory data in wireless sensor networks (WSN), for which plenty of sensor fusion protocols are available [76] [77]. Nonetheless, in AMR, a meter's data is unique; as such it cannot be aggregated with other meters' data, thereby making sensor fusion protocols irrelevant. Therefore, the AMR application must take this challenge into consideration and schedule the meter traffic accordingly.

Multicast traffic involves control data that is destined to all or a subgroup of meters, either residing in the same region or in different regions. Normally multicasting is supported at the IP routing level, in which the router creates optimal distribution paths to recipients. At the transport level, UDP can be used, but packet delivery is not guaranteed. For multicast reliability, Pragmatic General Multicast (PGM) [78] can be used, but with extra overhead.

As Fig. 13 shows, every group of meters is attached to the same gateway. Thus, the gateway can play an important role in reliably delivering the data to the intended meters. Additionally, data link layer features can be exploited. If WiMAX technology is incorporated, packets can be delivered to a set of meters simultaneously (same slot). If the meters form a mesh network, sensor network multicasting protocols can be considered. Lian et al. [79] provide a concise review of the multicasting protocols and propose a geocasting approach that guarantees reliable delivery of messages while keeping the transmission cost low.

### *D. Network Access and Routing*

AMR meters are stationary nodes distributed at fixed locations such as households. This forms a static topology and makes ensuring connectivity easy compared to other wireless networks, including sensor networks. However, although a great deal of routing protocols is available in the wired and wireless worlds, choosing or designing a one for AMR still requires a closer look at its specifics and requirements. The following points summarize the challenges and AMR special considerations:

- Transmission media and data link: Network layer is well coupled with the underlying layers. In a multi-hop setup, the traditional problems associated with a wireless channel (e.g., interference and fading) may affect the meter-to-meter communication, especially at areas with highly dense meters. Some isolated meters (e.g., in rural areas) need to have repeaters to connect to the rest of the AMR network. At the Medium Access Control (MAC) level, an energy efficient protocol is required. TDMA-based protocols are more energy efficient for flat network architecture than Carrier sense multi-access (CSMA). However, if the AMR network is clustered, then more work should be done to accommodate inter-cluster communication and to adapt the intra-cluster MAC in terms of number of nodes involved and MAC parameter such as frame length and slot assignment.
- Fault tolerance: MAC and routing protocols must form alternative links and routes when some nodes break down or lack energy to route traffic through. This may involve rerouting of traffic or adjusting transmission power levels.
- Scalability: the number of meters in a certain vicinity may be in the order of thousands. MAC and routing protocols must be able to work with such a large network size given that meters are limited in memory and buffer space.
- Quality of service: as introduced in Section III-C, AMR traffic involves information that must be delivered within a certain amount of time; otherwise the data will be useless. Bounded latency for data delivery is a condition to be considered.
- Adaptableness: Network conditions are changeable. The routing protocol should be able to use the node state and

change its route accordingly. For example, the energy level may change for some nodes (decrease or increase). Additionally, the routing protocol should be able to take advantage of the diverse node hardware specifications. It assigns nodes with large memory to store more routing information and let nodes with fixed energy source (e.g., electricity meters) perform long range communication.

Recent ongoing work by IETF Routing Over Low-power and Lossy networks (ROLL) group (RFC [80]) provides a comprehensive discussion of the routing requirements of Urban Low-Power and Lossy Networks (U-LLNs), which applies to AMR. The network architecture considered is a mesh network. Nodes (meters, actuators and metrological sensors) can provide measurements as well as perform routing. Routes lead to the sink or a gateway node that is connected to the Internet. Levis et al. [81] evaluate the suitability of standard protocols such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF) and Ad hoc On-Demand Distance Vector Routing (AODV) to act as the routing protocol for U-LLNs. Winter et al. [82] specify a Routing Protocol for Low Power and Lossy Networks (RPL). The protocol forms a directed acyclic graph. Edges form paths that are oriented toward and terminating at a root node, which could be a sink or a gateway to the Internet. Another network architecture option would be to let meters connect directly to a third generation base station. The issues to be tackled in this case are purely related to lower layers functionalities (MAC and data link). To achieve scalability, scheduling the meters should be considered. If multiple simultaneous transmissions are allowed, low level interference must be taken into account.

### *E. Security*

AMR security must be end-to-end to prevent unauthorized access to the metering equipment or any of the AMR intermediate devices and to prevent tampering with data. Adding security cryptosystems however incurs extra load on the device processing and impacts the energy consumption and bandwidth. Thus, selecting the right cryptographic tool is critical. For example, confidentiality of the AMR data is not as critical an issue as is data integrity. Therefore, a strong message authentication protocol is preferred while encryption cryptography can be kept simple.

Security is typically implemented at different layers. Taking WiMAX as an example, frame encryption and device authentication are implemented at the link layer, which secures the wireless signal (meter to base station), ensuring that only those legitimate devices access the WiMAX network. At the application layer, extra security mechanisms can be implemented to ensure end-to-end security. COSEM application layer supports three levels of security: 1- No security. 2- Low level security, which uses a password to authenticate the client. 3- High level security, which assumes no encryption is in place, and as such a more complicated authentication procedure is adopted to authenticate both the client and the server.

Key management is another issue to tackle here. Given the large number of meters, how can unique keys be distributed for every meter? Pre-deployment provisioning of keys might be difficult to realize. Asymmetric cryptography might also be impractical to be implemented in the metering devices due to the burden that public cryptographic key generation and security primitives add to such a resources-limited device; that is, consuming more processing power, using more memory storage space, and needing to transmit larger packets. Although recent publications such as [83] argue that certain public cryptographic security primitives are viable today on small devices, research is still ongoing to confirm this possibility.

## VI. Conclusion

In this paper, we have provided extensive coverage of the AMR system, starting from discussing the potential benefits and past development stages to giving directions of future generations of AMR. More specifically, this work has summarized and evaluated previous proposals published in this area. Based on that, we have discussed the suitability of the new communication paradigms, namely, sensor networks and 3G wireless systems. Furthermore, we have presented DLMS/COSEM as a communication standard and proposed SIP to handle the communication sessions between a meter and a data collection system.

We have also discussed the major challenges to be addressed in the future AMR. Such challenges include dealing with failures, managing real-time and delay-tolerant traffic, unicasting and multicasting of packets, and security of the system.

## References

[1] M. MAJCHRAK, J. HEINRICH, P. FUCHS, and V. HOSTYN, "Single phase electricity meter based on mixed-signal processor msp430fe427 with PLC modem," in *Radioelektronika, 17th International Conf.*, Apr. 2007.

[2] G. Barbose, C. Goldman, and B. Neenan, "A survey of utility experience with real time pricing," Lawrence Berkeley National Laboratory, Tech. Rep., Dec. 2004.

[3] T. Chandler, "The technology development of automatic metering and monitoring systems," in *IEEE International Power Eng. Conf.*, Dec. 2005.

[4] G. T. Heydt, "Virtual surrounding face geocasting in wireless ad hoc and sensor networks," *Electric Power Quality: A Tutorial Introduction*, vol. 11, no. 1, pp. 15–19, Jan. 1998.

[5] M. Faisal and A. Mohamed, "A new technique for power quality based condition monitoring," in *17th Conf. Electrical Power Supply Industry*, Oct. 2008.

[6] J. Surrat, "Integration of cebus with utility load management and automatic meter reading," in *IEEE Trans. Consumer Electron.*, vol. 37, no. 3, Aug. 1991, pp. 406–412.

[7] Y. Liu, R. Fischer, and N. Schutz, "Distribution system outage and restoration analysis using a wireless AMR system," in *IEEE Power Eng. Society Winter Meeting*, Aug. 2002.

[8] M. Baker, "Added value services through the use of AMR in commercial and industrial accounts," in *International Conf. Metering Tariffs Energy Supply*, May 1999.

[9] The Independent Electricity Syst. Operator, "Smart metering start-up guide," Apr. 2009.

[10] "CellNet + Hunt Data Systems Inc," [Online]. Available: www.cellnethunt.com.

[11] "Leach industries," [Online]. Available: www.leachindustries.com.

[12] S. Kerk, "An AMR study in an Indian utility," in *IEEE Power Eng. Conf.*, Dec. 2005.

[13] S. Soh and S. Kerk, "The electricity and metering trends in Singapore," in *IEEE Power Eng. Conf.*, Dec 2005.

[14] B. Park, D. Hyun, and S. Cho, "Implementation of AMR system using power line communication," in *IEEE/PES Transmission Distribution Conf. Exibition*, Oct. 2002.

[15] M. Choi, S. Ju, and Y. Lim, "Design of integrated meter reading system based on power line communication," in *IEEE International Symp. Power Line Commun. Its Appl.*, Apr. 2008.

[16] T. Moghavvemi, "PIC-based automatic meter reading and control over the low voltage distribution network," in *Student Conf. Research Development*, July 2002.

[17] G. Raja and T. Sudhakar, "Electricity consumption and automatic billing through power line," in *Internation Power Eng. Conf.*, Dec. 2007.

[18] P. Oksa, M. Soini, L. Sydanheimo, and M. Kivikoski, "Considerations of using power line communication in the AMR system," in *IEEE International Power Line Commun. Its Appl.*, Oct. 2006.

[19] J. Selga, A. Zaballos, G. Corral, and J. Vives, "Lessons learned from wireless sensor networks with application to AMR and PLC," in *IEEE International Symp. Power Line Commun. Its Appl.*, Mar. 2007.

[20] J. Yu, P. Chong, P. So, and E. Gunawan, "Solution for the 'silent node' problem in automatic meter reading system using power line communications," in *IEEE International Power Eng. Conf.*, Dec. 2005.

[21] H. Tan, H. Lee, , and V. Mok, "Automatic power meter reading system using GSM network," in *IEEE International Power Eng. Conf.*, Dec. 2007.

[22] A. Abdollahi, M. Dehghani, and N. Zamanzadeh, "SMS-based reconfigurable automatic meter reading system," in *IEEE International Conf. Control Appl.*, Oct. 2007.

[23] P. Zerfos, X. Meng, S. Wong, V. Samanta, and S. Lu, "A study of the short message service of a nationwide cellular network," in *ACM SIGCOMM Internet Measurement Conf.*, Oct. 2006.

[24] X. Meng, P. Zerfos, V. Smanta, S. Wong, and S. Lu, "Analysis of the reliability of a nationwide short message service," in *IEEE INFOCOM*, May 2007.

[25] S. Lee, C. Wu, M. Chiou, and K. Wu, "Design of an automatic meter reading system," in *Proc. IEEE IECON*, Aug. 1996.

[26] COMETECH M2M, "Machine-to-machine (m2m) communication solutions: Monitor, control and manage any remote equipment," 2008.

[27] S. K. Kim, "Automatic meter reading system and method using telephone line," in *United States Patent 7102533*, Sept. 2006.

[28] C. Brasek, "Urban utilities warm up to the idea of wireless automatic meter reading," *Comput. Control Eng.*, vol. 15, no. 6, pp. 10–14, Jan. 2005.

[29] B. Koay, S. Cheah, Y. Sng, P. Chong, P. Shum, Y. Tong, X. Wang, Y. Zuo, and H. Kuek, "Design and implementation of bluetooth energy meter," in *Inf. Commun. Signal Process.*, Dec. 2003.

[30] A. Wasnarat and Y. Tipsuwan, "A power efficient algorithm for data gathering from wireless water meter networks," in *IEEE International Conf. Industrial Informatics*, Aug. 2006.

[31] Q. Spencer, "An information-theoretic analysis of electricity consumption data for an AMR system," in *IEEE International Symp. Power Line Commun. Appl.*, Apr. 2008.

[32] J. Zhu and R. Pecen, "A novel automatic utility data collection system using IEEE 802.15.4-compliant wireless mesh networks," in *Proc. IAJC-IJME International Conf.*, Nov. 2008.

[33] B. Latre, P. D. Mil, I. Moerman, B. Dhoedt, P. Demeester, and N. V. Dierdonck, "Throughput and delay analysis of unslotted IEEE 802.15.4," *J. Netw.*, vol. 1, no. 1, pp. 20–28, May. 2006.

[34] A. Iyer, S. Kulkarni, V. Mhatre, and C. Rosenberg, "A taxonomy-based approach to design of large-scale sensor networks," in *Wireless Sensor Networks and Applications*, ser. Signals and Communication Technology. Springer, Feb. 2008, ch. 1, pp. 3–33.

[35] J. Jones and M. Atiquzzaman, "Transport protocols for wireless sensor networks: State-of-the-art and future directions," *International J. Distributed Sensor Netw.*, vol. 3, no. 1, pp. 119–133, Jan. 2007.

[36] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," in *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–114.

[37] B. Krishnamachari, "Networking wireless sensors," in *Cambridge University Press*, Dec. 2005.

[38] C. Y. Wan, S. B. Eisenman, and A. T. Campbell, "CODA: Congestion detection and avoidance in sensor networks," in *First International Conf. Embedded Netw. Sensor Syst. (SenSys'03)*, 2003.

[39] F. Stann and J. Heidemann, "RMST: Reliable data transport in sensor networks," in *IEEE International Workshop Sensor Netw. Protocols Appl.*, May. 2003.

[40] B. Hull, K. Jamieson, and H. Balakrishnan, "Mitigating congestion in wireless sensor networks," in *ACM Sensys 04*, Nov. 2004.

[41] C. Wang, K. Sohraby, and B. Li, "SenTCP: A hop-by-hop congestion control protocol for wireless sensor networks," in *IEEE INFOCOM*, 2005.

[42] A. D. A, J. Alonso, and V. T, "Making TCP/IP viable for wireless sensor networks," in *European Workshop Wireless Sensor Netw.*, Jan. 2004.

[43] S.-J. Park, R. Vedantham, R. Sivakumar, and I. F. Akyildiz, "A scalable approach for reliable downstream data delivery in wireless sensor networks," in *MobiHoc '04*, May 2004.

[44] O. Akan and I. Akyildiz, "Event-to-sink reliable transport in wireless sensor networks," *IEEE/ACM Trans. Netw.*, vol. 13, no. 5, pp. 1003–1016, Oct. 2005.

[45] V. Mhatre, C. Rosenberg, D. Kofman, R. Mazumdar, and N. Shroff, "A minimum cost surveillance sensor network with a lifetime constraint," in *IEEE Trans. Mobile Comput.*, Jan. 2005.

[46] V. Mhatre and C. Rosenberg, "Homogeneous vs heterogeneous sensor networks: A comparative study," in *International Conf. Commun. (ICC 2004)*, June 2004.

[47] P. Juang, H. Oki, Y. Wang, M. Martonosi, L. Peh, and D. Rubenstein, "Energy efficient computing for wildlife tracking: Design tradeoffs and early experiences with zebranet," in *IASPLOS-X*, Oct. 2002.

[48] K.-W. Fan, S. Liu, and P. Sinha, "Data aggregation in wireless sensor networks," in *Wireless Sensor Networks and Applications*, ser. Signals and Communication Technology. Springer, 2008, pp. 331–347.

[49] S. Madden, M. Franklin, J. Hellerstein, and W. Hong, "TAG: A tiny aggregation service for ad-hoc sensor networks," in *ACM SIGOPS Operating Syst. Rev.*, vol. 36, no. SI, 2002.

[50] A. Al-Yasiri and A. Sunley, "Data aggregation in wireless sensor networks using the SOAP protocol," in *J. Physics: Conf. Series 76 012039*, 2007.

[51] C. Intanagonwiwat, D. Estrin, R. Govindan, and J. Heidemann, "Impact of network density on data aggregation in wireless sensor networks," in *ICDCS*, 2002.

[52] S. Chessa and P. Santi, "Crash faults identification in wireless sensor networks," *Comput. Commun.*, vol. 25, no. 14, pp. 1273–1282, Sept. 2002.

[53] J. L. Bordim and K. Nakano, "Fundamental protocols to gather information in wireless sensor networks," in *Sensor Network Protocols*. Springer, 2006, ch. 6.

[54] P. Jiang, "A new method for node fault detection in wireless sensor networks," *Sensors*, vol. 9, no. 2, pp. 1282–1294, 2009.

[55] M. Yamanouchi, S. Matsuura, and H. Sunahara, "A fault detection system for large scale sensor networks considering reliability of sensor data," in *Appl. Internet SAINT '09*, July 2009.

[56] J. Lian and K. Naik, "Skipping technique in face routing for wireless ad hoc and sensor networks," *International J. Sensor Netw.*, vol. 4, no. 1/2, pp. 92–103, July 2008.

[57] E. Kim, D. Kaspar, C. Gomez, and C. Bormann, "Problem statement and requirements for 6LoWPAN routing," in *6LoWPAN Working Group Internet Drafts*, July 2009.

[58] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: a survey," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 2, pp. 52–73, 2009.

[59] M. Sbai and C. Barakat, "Experiences on enhancing data collection in large networks," *Computer Netw.: International J. Comput. Telecommun. Netw.*, vol. 3, no. 7, pp. 1073–1086, May. 2009.

[60] E. Dahlman, S. Parkvall, J. Skold, and P. Beming, "3G evolution HSPA and LTE for mobile broadband," in *ISBN: 978-0-12-372533-2*. Elsevier, 2008.

[61] J. Andrews, A. Ghosh, and R. Muhamed, "Fundamentals of WiMAX," in *ISBN: 0-13-222552-2*. Prentice Hall, 2007.

[62] R. Pries, D. Staehle, and D. Marsico, "IEEE 802.16 capacity enhancement using and adaptive TDD split," in *IEEE Veh. Technol. Conf.*, May. 2008.

[63] "DLMS user association," [Online]. Available: www.dlms.com.

[64] "IEC - international electrotechnical commission," [Online]. Available: www.iec.ch.

[65] P. Fuchs and T. Schaub, "DLMS user association - co-ordination between applications and channels," in *International Conf. Metering Tariffs Energy Supply*, Aug. 1999.

[66] Companion specification for energy metering, "Identification system and interface classes," in *Blue Book, DLMS User Association, 1997-2007.*

[67] Companion Specification for Energy Metering, "DLMS/COSEM architecture and protocols," in *Green Book, DLMS User Association, 1997-2007.*

[68] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "SIP: Session initiation protocol," in *RFC 3261*, June 2002.

[69] K. Singh and H. Schulzrinne, "Peer-to-peer internet telephony using SIP," in *Workshop Netw. Operating Syst. Support Digital Audio Video*, June 2005.

[70] B. Sarikaya and X. Zheng, "SIP paging and tracking of wireless lan hosts for VoIP," *IEEE/ACM Trans. Netw.*, vol. 16, no. 3, pp. 539–548, June 2008.

[71] EarthLink Research and Development, "SIPshare: SIP beyond voice and video," [Online]. Available: http://www.research.earthlink.net/p2p/, 2004.
[72] M. Handley and V. Jacobson, "SDP: Session description protocol," in *RFC 2327*, Apr. 1998.
[73] A. Roach, "SIP-specific event notification," in *RFC 3265*, June 2002.
[74] K. Fall and S. Farrell, "DTN: An architectural retrospective," in *IEEE J. Sel. Areas Commun.*, vol. 26, no. 2, June 2008, pp. 828–836.
[75] H. Schulzrinne, S. Casner, R. Fredrick, and V. Jacobson, "RTP: A transport protocol for real-time applications," in *RFC 3550*, July 2003.
[76] M. Zhao, M. Ma, and Y. Yang, "Mobile data gathering with space-division multiple access in wireless sensor networks," in *IEEE INFOCOM*, Apr. 2008.
[77] Z. Zhang, M. Ma, and Y. Yang, "Energy efficient multi-hop polling in clusters of two-layered heterogeneous sensor networks," *IEEE Trans. Comput.*, vol. 57, no. 2, pp. 231–245, Feb. 2008.
[78] T. Speakman, J. Crowcroft, J. Gemmell, D. Farinacci, S. Lin, D. Leshchiner, M. Luby, T. Montgomery, L. Rizzo, A. Tweedly, N. Bhaskar, R. Edmonstone, R. Sumanasekera, and L. Vicisano, "PGM reliable transport protocol specification," in *RFC 3208*, July 2007.
[79] J. Lian, Y. Liu, K. Naik, and L. Chen, "Virtual surrounding face geocasting in wireless ad hoc and sensor networks," *IEEE/ACM Trans. Netw.*, vol. 17, no. 1, pp. 200–211, Feb. 2009.
[80] M. Dohler, T. Watteyne, T. Winter, and D. Barthel, "Routing requirements for urban low-power and lossy networks," in *RFC 5548*, May 2009.
[81] P. Levis, A. Tavakoli, and S. Dawson-Haggerty, "Overview of existing routing protocols for low power and lossy networks," in *Internet Draft*, Apr. 2009.
[82] T. Winter and ROLL Design Team, "RPL: Routing protocol for low power and lossy networks," in *Netw. Working Group Internet Drafts*, July 2009.
[83] P. Szczechowiak, A. Kargl, M. Scott, and M. Collier, "On the application of pairing based cryptography to wireless sensor networks," in *WiSec '09: Proc. Second ACM Conf. Wireless Netw. Security*, Mar. 2009.

**Tarek Khalifa** received his B.Sc. degree in electrical and computer engineering from Alfateh University, Libya, in 2000. He received his M.Sc. from the University of Waterloo, Canada in 2007. He has five years of industrial experience in Networking with an Internet service provider (Libya Telecom and Technology) and with Schlumberger Overseas. Currently, he is a PhD student at the University of Waterloo. His research interests include network security, wireless sensor networks, transport control protocols, and communication protocols for the smart grid.

**K. Naik** received his BS and M. Tech degrees from Sambalpur University, India, and the Indian Institute of Technology, Kharagpur, respectively. He received an M. Math degree in computer science from the University of Waterloo and a Ph.D. degree in electrical and computer engineering from Concordia University, Montreal. He worked as a faculty member at the University of Aizu in Japan and Carleton University in Ottawa. At present he is an associate professor in the Department of Electrical and Computer Engineering, at the University of Waterloo. He was a visiting associate professor at the Research Institute of Electrical Communications at Tohoku University, Sendai, Japan, in 2003. He served as a program co-chair of the 5th International Conference on Information Technology held in Bhubaneswar, India, in December 2002. He was a co-guest editor of two special issues of IEEE Journal on Selected Areas in Communications published in June 2005 and January 2007. Now he is an associate editor for the Journal of Peer-to-Peer Networking and Applications and the International Journal of Parallel, Emergent and Distributed Systems. His research interests include dependable wireless communication, resource allocation in wireless, sensor networks, ad hoc networks, mobile computing, peer-to-peer communication, intelligent transportation systems, capability enhancement of handheld devices, and communication protocols for smart power grids.

**Amiya Nayak** received his BMath degree in Computer Science and Combinatorics and Optimisation from the University of Waterloo, Canada, in 1981, and PhD in Systems and Computer Engineering from Carleton University, Canada, in 1991. He has over 17 years of industrial experience, working at CMC Electronics, Defence Research Establishment Ottawa, EER Systems and Nortel Networks, in software engineering, avionics and navigation systems, simulation and system level performance analysis. He is in the Editorial Board of IEEE Transactions on Parallel & Distributed Systems, Int. J. Parallel, Emergent and Distributed Systems, Int. J. Computers and Applications, Int. J. Computer Information Technology and Engineering, Int. J. Computing and Information Science, Int. Journal of Autonomic Computing, and EURASIP Journal on Wireless Communications & Networking. Currently, he is a Full Professor at the School of Information Technology and Engineering at the University of Ottawa, Canada. His research interests are in the areas of mobile ad hoc and sensor networks, fault tolerance, and distributed systems/algorithms, with over 150 publications in refereed journals and conference proceedings.