U.S. DEPARTMENT OF ENERGY

PNNL-20374

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Home Area Networks and the Smart Grid

SL Clements
TE Carroll
MD Hadley

April 2011

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle Since 1965

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service,
U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161
ph: (800) 553-6847
fax: (703) 605-6900
email: orders@ntis.fedworld.gov
online ordering: http://www.ntis.gov/ordering.htm

PNNL-20374

Home Area Networks and the Smart Grid

SL Clements MD Hadley
TE Carroll

April 2011

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99352

Table of Contents

[Page intentionally left blank]

Home Area Networks and the Smart Grid

Abstract

With the wide array of home area network (HAN) options being presented as solutions to smart grid challenges for the home, it is time to compare and contrast their strengths and weaknesses. This white paper examines leading and emerging HAN technologies.

Introduction to Home Area Networks and the Smart Grid

The de facto standards of Ethernet and 802.11 Wi-Fi for home area networking should expect to welcome other players to the field. Home area networks emerged in earnest in the late 1990s and early 2000s fueled by the growth of the Internet. Now with the onset and development of the smart grid, other players are entering the HAN market where their key differences revolve around data rates and power consumption. The Internet and the technologies surrounding it are developed to move large amounts of data quickly through a network at somewhat intermittent intervals (e.g. graphics, music, video, etc.). The needs of the smart grid are significantly different; requiring relatively low bandwidth but regular communications. These differences open the door for other players to enter the HAN market.

Most existing home networks allow desktop and laptop computers to communicate with each other to share resources and often a common connection to the Internet. Granted, the types of devices on existing networks are beginning to expand to include media servers, televisions, game consoles and other entertainment devices, all of which fit the intermittent and high bandwidth requirements. Achieving a vision of the smart grid at the consumer level to allow homeowners to better understand and manage their energy consumption will require many new types of devices with lower bandwidth but regular and consistent data stream requirements. Devices such as thermostats, HVAC systems, major appliances, home automation systems, home energy management systems, lighting, gas meters, water meters, and electric meters will all be networked and communicating information that allows the homeowner to better understand and manage energy use.

There are myriad standards and protocols vying for dominance in the smart grid market. With so many devices needing to be connected to the network it is in the consumers and manufacturers best interests to identify the most worthy candidates and settle on those for purposes of interoperability, economies of scale and ease of adoption. We will focus primarily on three leading standards: HomePlug Green PHY, ZigBee, and IEEE 802.11n and briefly identify competing technologies.

Architecture

With such a diverse and large number of devices to be incorporated into smart grid networks, it is important to understand the technologies and architectural models being used. So how are we going to connect all these devices together? There appear to be two distinct trains of thought with variations of

the HAN architecture as it relates to the utility. The first is that the utility, which has traditionally controlled the majority if not all the electrical infrastructure, will be able to control all the appliances within the home to better manage the grid. This is currently in use in some areas where consumers opt-in to allow the utility to shut off their Air Conditioning units during peak demand.

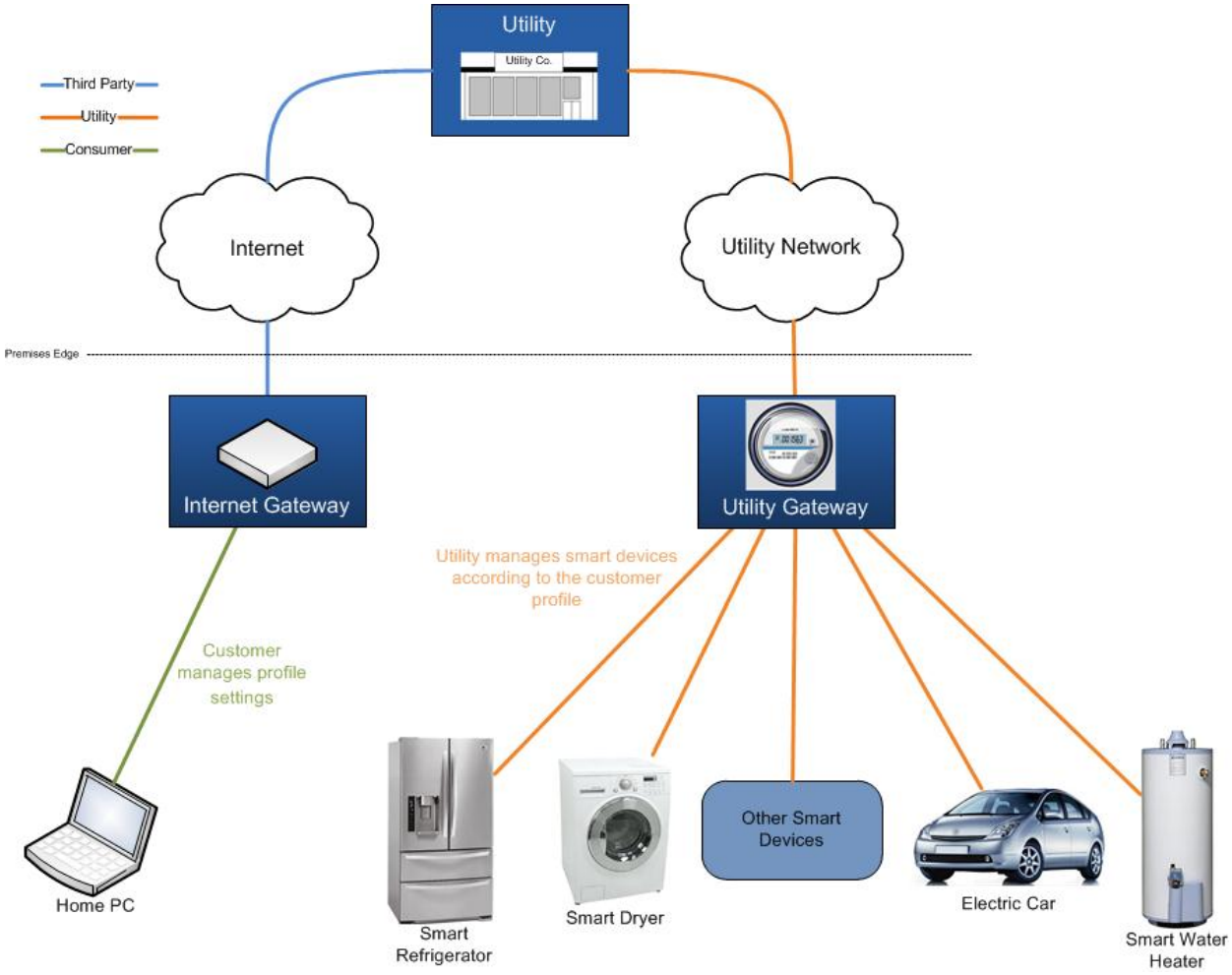

Figure 1 Utility Managed Smart Devices (Image derived from [1])

The other camp sees the utility having access to a gateway within the home and then the consumer controls what happens in the home or delegates that to a third party.

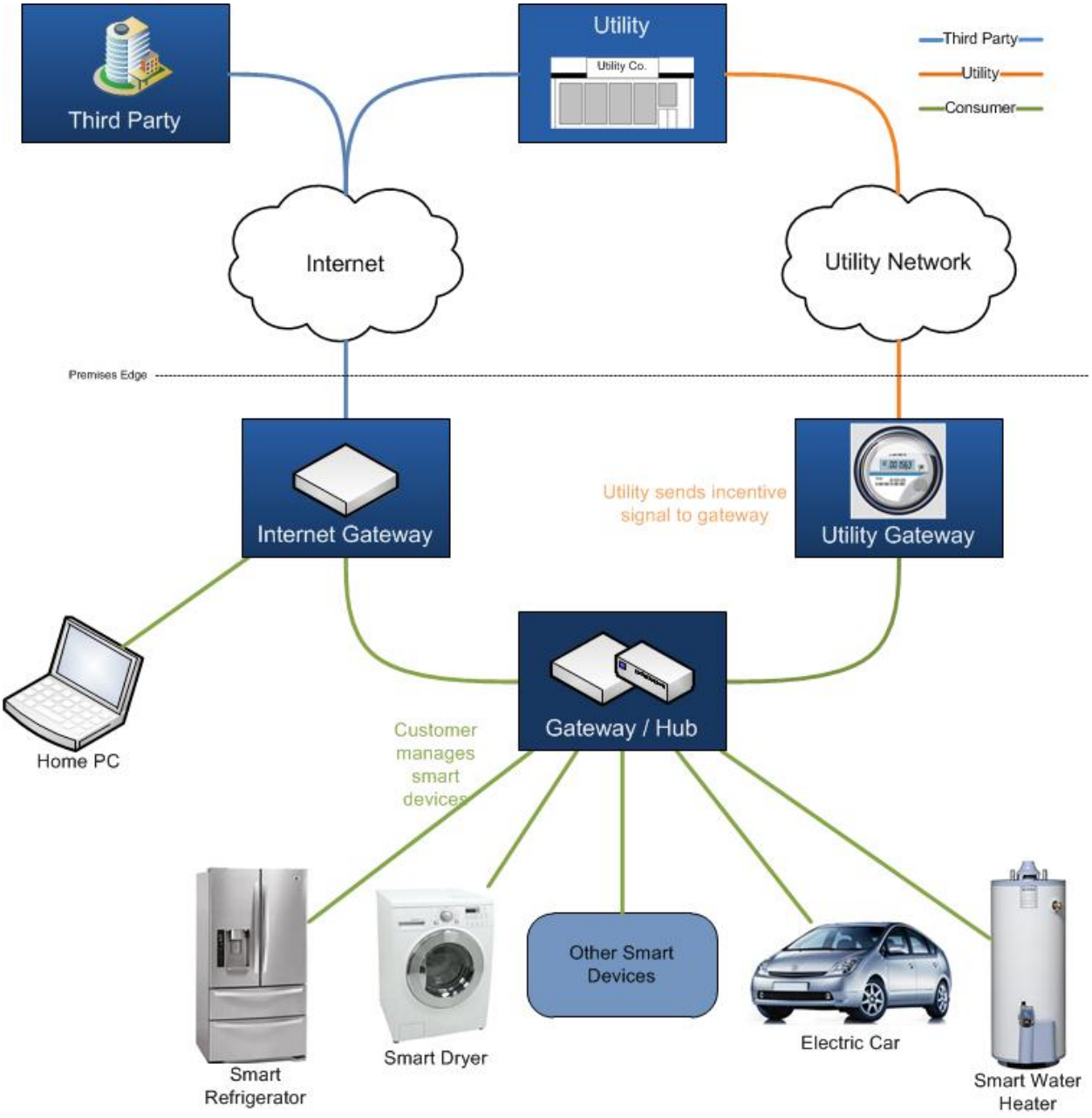

Figure 2 Consumer Managed Smart Devices (Image derived from [1])

The authors favor the latter architecture. The gateway architecture fits well for both the consumer who is uneasy with a utility being able to control devices within his or her home as well as the vendor and manufacturers concerned with interoperability[1].

[1] Association of Home Appliance Manufacturers. Assessment of Communication Standards for Smart Appliances. http://www.aham.org/ht/a/GetDocumentAction/i/50696%20. February 2011.

The HAN standards we will be addressing are often categorized into three bins, new wires, no new wires, and wireless. Each a category has distinct strengths and weaknesses. Though there is not a clearly defined best option it is certain the standards most likely to be adopted will interoperate with other standards. As would be expected, the leading standards are mature and widely understood.

New Wires

The de facto standard for wired networking is Ethernet. There really are no competitors. Most homes built before 2000 and many built afterward do not have Ethernet run throughout the house. The effort and cost of retrofitting a home or building with new wires is extremely daunting. Installing Ethernet or other wires during construction is affordable but as a retrofit it is often too costly. Speed, reliability and security are often the reasons considered to justify the expense of installing new wires. The demands for most HAN smart grid applications are between 10Kbps and 500Kbps [2] thus the need for speed is not a valid argument for installing Ethernet for smart grid needs though the reliability and security arguments are still quite valid. We will only briefly touch on Ethernet.

IEEE 802.3 Ethernet

IEEE 802.3 or Ethernet as it is more commonly known is used in nearly every business and to some extent in homes. We will not spend time discussing how it works as this technology is quite mature and well known. Rather we will highlight the advantages and disadvantages of this nearly ubiquitous technology. Those wanting more information can find it referenced below[3,4].

Advantages

- Mature, proven and widely supported technology
- Reliable and able to utilize multiple physical mediums (fiber, copper)
- More than adequate data rates for smart grid requirements
- Strong security mechanisms are available
- Easily connects to other technology

Disadvantages

- Often requires new cables which are laborious and thus expensive to install
- Each device on the network needs its own cable
- Cables may not be present for all appliances, load controllers, or smart grid devices in pre-wired installations

No New Wires

Using existing wires within a home offers many benefits over installing a new network with all the inherent costs and frustrations. The two options that exist in nearly every home are telephone lines and power cabling. There are technologies and standards that exist for both types of wires but since one of the major goals of the smart grid is to monitor and minimize electric power usage we will evaluate

[2] Fuhr, P., Manges, W., Kuruganti, T. *Smart Grid Communications Bandwidth Requirements – An Overview* Oak Ridge National Laboratory
[3] IEEE 802.3 Standard http://standards.ieee.org/about/get/802/802.3.html
[4] Wikipedia http://en.wikipedia.org/wiki/Ethernet

HomePlug Green PHY which uses electrical wiring for data transmission. Another factor influencing our decision not to explore phone line use is the limited coverage of phone lines in home construction.

Power Line Communication (HomePlug)

HomePlug GREEN PHY (GP) is a low-power, robust data communications technology that provides data rates of 4—10 Mbps over a building's existing electrical wiring. The GP specification defines the media access control (MAC) and physical layer (PHY) for power line communications (PLC) in home area networks (HANs) and has recently been adopted as a profile of the IEEE Standard 1901 for broadband over power line networks[5]. A complete network stack is achieved by utilizing the TCP/IP protocol suite on top of GP. AES-128 encryption is used to ensure the confidentiality of transmissions.

Even though HomePlug GREEN PHY implements a subset of the functionality decreed by the HomePlug AV specification, GP and HomePlug AV devices are compatible and can coexist on the same network. Combining the reduction with the ability to sleep delivers a 75 percent device power savings over HomePlug AV devices[6].

Power lines are noisy communication channels with many occupants. In the low range of the frequency spectrum is the 50/60 Hz, 120/240 VAC, followed by legacy security and control system signals such as X10. Furthermore, wideband appliance-generated noise and induced EMI/RFI (e.g., AM radio signals) create problems. GP operates in the 1.8—30 MHz range, well above the power and other carrier signals. Orthogonal Frequency Division Multiplexing OFDM is used to spread the signal among 1155, evenly spaced carriers. Carriers can be individually muted (masked) to remove interference they create so as to not interfere with wireless services such as amateur radio bands. Each unmasked carrier is orthogonally modulated with Quadrature Phase Shift Keying QPSK to minimize the bit error rate. Turbo convolutional codes, a type of Forward Error Correcting code (FEC), are utilized so that receivers can detect and correct transmission errors, limiting the instances where the sender is required to retransmit. Additional robustness is achieved by redundantly interleaving multiple copies of the data in the transmissions.

GP network communications are governed by a beacon-based MAC. Each network designates a Central Coordinator (CCo), a station with the responsibility of setting up and maintaining the logical network, managing the communication resource on the wire, and coordinating with neighboring networks that use the same wiring infrastructure. The CCo issues a beacon every two AC line cycles. The period between beacons is divided into allocations that can be used by stations for CSMA/CA-based transmissions. The MAC Protocol Data Unit (MPDU) consists of a 128-bit frame control block followed by one 136-octet physical data unit (PDU) or one, two, or three 520-octet PDUs.

Multiple HomePlug networks can coexist on the same wiring infrastructure. Each logical network is associated with an identifying name and one or more Network Management Keys (NMKs). Using the NMK as a master key, the CCo distributes a periodically changing Network Encryption Key (NEK) to each station in the logical network. Confidentiality of transmissions and enforcement of logical network

[5] IEEE Standard 1901-2010 http://standards.ieee.org/findstds/standard/1901-2010.html
[6] HomePlug Powerline Alliance 2010

separation is achieved by encrypting the data payloads of most PDUs sent in the logical network. Encryption is performed using AES-128 in Cipher Block Chaining (CBC) mode under the NEK. The Forward Error Correction (FEC) codes are computed subsequent to encryption so that receivers are able to reconstruct corrupted transmissions.

Advantages

- GP operates over the house's existing electrical power lines. Any appliance or device requiring power will be attached this system.
- Data rates of 4—10 Mbps surpass the Smart Grid requirements.
- The HomePlug AV and GREEN PHY standards have strong backing from major sponsors.
- Unlike Ethernet, no new wiring is required. Ethernet requires monitored devices to have two connections: one for power, and one for data. GP requires only a single connection—the power cord—that serves both functions.
- Electrical wiring systems already extend throughout buildings thus alleviating the need, in most cases, for network extending devices.
- AES-128 in CBC mode ensures confidentiality of the transmissions.

Disadvantages

- Even though development on the HomePlug standard began in 2000, it only recently has received wide spread acceptance.
- Limited devices are available on the market. Most HomePlug devices serve as Ethernet-to-HomePlug network bridges. At the time of the writing, a search did not return any GREEN PHY devices or devices that have integrated HomePlug AV support.
- FECs, while necessary, add cost and complexity to GP devices that the other technologies do not have.
- If not properly configured all networks within a building (e.g. Apartment building) will be viewable to each other.

Security Considerations

The HomePlug Alliance has done a good job of building security into the HomePlug AV/GP specifications. HomePlug GP uses a subset of the options available to HomePlug AV and thus has a smaller attack surface. As with many technologies the challenges in creating a secure environment are found in the implementation. Most devices have a Network Management Key from which all other keys are derived. Vendors often do this for interoperability reasons as it allows a user to quickly set up a network. The problem is then anyone with a device by the same vendor can also join, eavesdrop or inject data onto that network. Default NMKs need to be replaced by the end user. Another consideration is the pairing of two devices. In order to pair two devices there is frequently a button to press that activates a pairing session this session lasts for 60 seconds during which link keys are shared. An attacker no privy to the

NMK as described above still has this small window to capture the information necessary to eavesdrop on a network.[7]

Competing Technologies

HomePNA

HomePNA provides data networking over existing household telephone lines or coaxial cables. The most recent version of the standard has data rates of 320 Mbps. Telephone or coaxial cable outlets are unlikely to be located in proximity of all smart appliances and devices, thus giving GP an advantage over this technology.

G.hn

G.hn is an ITU standard for networking over power lines, telephone lines, and coaxial cables with data rates up to 1 Gbps. While G.hn offers greater medium choices, the standard is immature with few manufactures producing G.hn-compliant chips.

Wireless

The ability to network devices without running wires has tremendous appeal. The wireless market has seen enormous growth in the last ten years. This trend is expected to continue. Wireless technology is moving from the corporate IT environment into industrial and smart grid arenas. Within these areas there is a focus on low power (i.e. 5 year battery life) and low bandwidth versus the traditional wired power with high bandwidth. We will address some of the leading wireless technologies competing in the smart grid arena

IEEE 802.11n

The first standard IEEE 802.11 was published in June 1997 the current version is IEEE 802.11-2007[8]. Through the years it has seen numerous updates and amendments. The most commonly known are a,b,g,i and n of which all but "i" are protocol specifications. IEEE 802.11i is a security amendment. The most current protocol amendment is IEEE 802.11n-2009[9] and will be the focus for this section.

Of all the different network IEEE 802.11 protocol standards IEEE 802.11n is unique in that it can operate at both 2.4 GHz and 5 GHz, it adds 40 MHz channels, and incorporates multiple-input multiple-output (MIMO) technologies. Like many other technologies (ADSL, PLC, G.hn, LTE, HomePlug) IEEE 802.11n uses orthogonal frequency-division multiplexing (OFDM) as its modulation technique.

OFDM works by spreading the transmitted data onto orthogonal sub-carriers. This eliminates cross-talk between the sub-channels thereby removing the need for inter-carrier guard bands. In other words it limits the interference caused by the data one is sending and frees up the space that is necessary to protect against this interference. Having more space available for data sub-carriers allows for more

[7] Carcello, Xavier; Florian; FAIFA: A first open source PLC tool; Chaos Communication Congress 27-30 Dec. 2008 http://www.youtube.com/watch?v=0Ro_5LNp6zA [accessed 15 Aug. 2011]
[8] IEEE Standard 802.11-2007 http://standards.ieee.org/getieee802/download/802.11-2007.pdf 18 April 2011
[9] IEEE 802.11n-2009 http://standards.ieee.org/getieee802/download/802.11n-2009.pdf 18 April 2011

efficient use of the spectrum and increased throughput. The orthogonality also simplifies the design of both the transmitter and receiver; removing the need for filters on each sub-channel.

MIMO is the use of multiple transmit and receive antennas which work together to increase communication performance (i.e. throughput, range) without additional bandwidth or transmit power. The use of MIMO technology is one of the primary reasons for the increased data rates and range for IEEE 802.11n over IEEE 802.11g. The IEEE 802.11n standard allows for up to 4 transmit antennas, 4 receive antennas and 4 distinct data streams though most devices on the market do not reach the limit. Often a 3x3x3 configuration is used.

The table below shows a comparison of the different IEEE 802.11 standards.

802.11 network standards										
802.11 Protocol	Release	Freq. (GHz)	Bandwidth (MHz)	Data rate per stream (Mbits/s)	Allowable MIMO streams	Modulation	Approximate indoor range		Approximate outdoor range	
							(m)	(ft)	(m)	(ft)
-	Jun 1997	2.4	20	1, 2	1	DSSS, FHSS	20	66	100	330
a	Sep 1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM	35	115	120	390
		3.7[A]					-	-	5,000	16,000[A]
b	Sep 1999	2.4	20	5.5, 11	1	DSSS	38	125	140	460
g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM, DSSS	38	125	140	460
n	Oct 2009	2.4/5	20	7.2, 14.4 21,7, 28.9, 43.3, 57.8, 65, 72.2 [B]	4	OFDM	70	230	250	820
			40	15, 30, 45, 60, 90, 120, 135, 150[B]			70	230	250	820
[A] IEEE 802.11y-2008 extended operation of 802.11a to the licensed 3.7 GHz band. Increased power limits allow a range up to 5,000m. As of 2009; it is only being licensed in the United States bot the FCC [B] Assumes short guard interval (SGI) is enabled, otherwise reduce each data rate by 10%.										

Table 1 - 802.11 Network Standards [derived from [10]]

IEEE 802.11n can be used in three modes of operation; ad hoc, infrastructure, and mesh. These are not a part of the standard and must be handled at a higher layer. There are many different vendors that provide applications to allow for these modes of operation.

The security of IEEE 802.11n is handled by IEEE 802.11i which is incorporated in the IEEE 802.11-2007 standard. 802.11i supersedes the previous security specifications of Wired Equivalent Privacy (WEP), and Wi-Fi Protected Access (WPA). 802.11i is commonly referred to as WPA2 and uses the Advanced Encryption Standard (AES) instead of the weaker RC4. WPA2 provides two main methods for accessing the network either through a pre-shared key (PSK) or 802.1X authentication. To facilitate out-of-the box interoperability for consumers, security is often disabled by default. Wi-Fi chipsets are inexpensive and appearing in handheld devices, portable entertainment devices, printers, barcode readers, and numerous other devices. Enabling security on these has introduced a challenge that laptops did not have; how to input authorization codes.

[10] http://en.wikipedia.org/wiki/IEEE_802.11n-2009

The Wi-Fi Alliance has provided various solutions to facilitate simple secure configurations through Wi-Fi Protected Setup (WPS). WPS can automate security configurations through any of the following techniques: personal identification numbers (PIN), push-button configuration (PBC), near-field communication (NFC) or USB. The PIN method requires the user to enter a unique PIN from the packaging or display of the device into a registration mechanism. The PBC method requires the user to push a button (either physical or virtual) on both the access point and the device to configure the security. The NFC method uses RFID or similar technologies to share information and configure the security settings. The last method is to use a USB device to transfer configuration settings between other devices.

Advantages

- Wi-Fi is a mature technology with a high adoption rate
- Many homes and businesses already have a Wi-Fi network in place upgrading to IEEE 802.11n is easy if necessary
- Data rates of 300Mbps exceed the Smart Grid requirements
- Backward compatible with IEEE 802.11 a, b and g
- Inside range of 70 meters which should cover all but the largest homes
- Mature and tested security
- Inexpensive chipsets make integration affordable
- MIMO technology helps resilience in the congested ISM bands

Disadvantages

- High power consumption limits battery powered options[11]
- Operates in the congested ISM bands
- Still susceptible to forged management frame attacks (e.g. disassociation/deauthorization and masquerading APs attacks)

Security Considerations

IEEE 802.11 has come a long way since the days of WEP. It is now possible to have a secure wireless network using IEEE 802.11i (aka WPA2). The most robust security comes from using WPA2 in enterprise mode with a backend authentication server to perform access control. Home based networks without the authentication server are subject to brute force password attacks on the shared key so the use of a robust password is essential. As mentioned previously IEEE 802.11n is still subject to management frame hacks that result in denial of service attacks and/or man-in-the-middle (MITM) attacks. The MITM threat is not generally a problem for point-to-point wireless using WPA2 but is more problematic for mobile devices that connect to multiple wireless networks over time.

ZigBee

ZigBee is a wireless protocol developed specifically for low power and low data-rate communications. ZigBee utilizes the IEEE 802.15.4 standard for the physical and MAC layers. Like IEEE 802.11n, IEEE

[11] General Electric *"Energy Efficiency Comparisons of Wireless Communication Technology Options for Smart Grid Enabled Devices"* 9 Dec 2010 http://www.brymercreative.com/geal_2010/images/120910_zigbee.pdf

802.15.4 radios operate on the ISM bands. Unlike IEEE 802.11n devices, ZigBee end devices are intended to be battery operated for up to five years on one charge. ZigBee attains this power savings through a number of design decisions namely: a simplified protocol stack, low data-rate transfers, short-range transmissions, and wall-powered networking devices[12]. The following diagram depicts the ZigBee protocol stack.

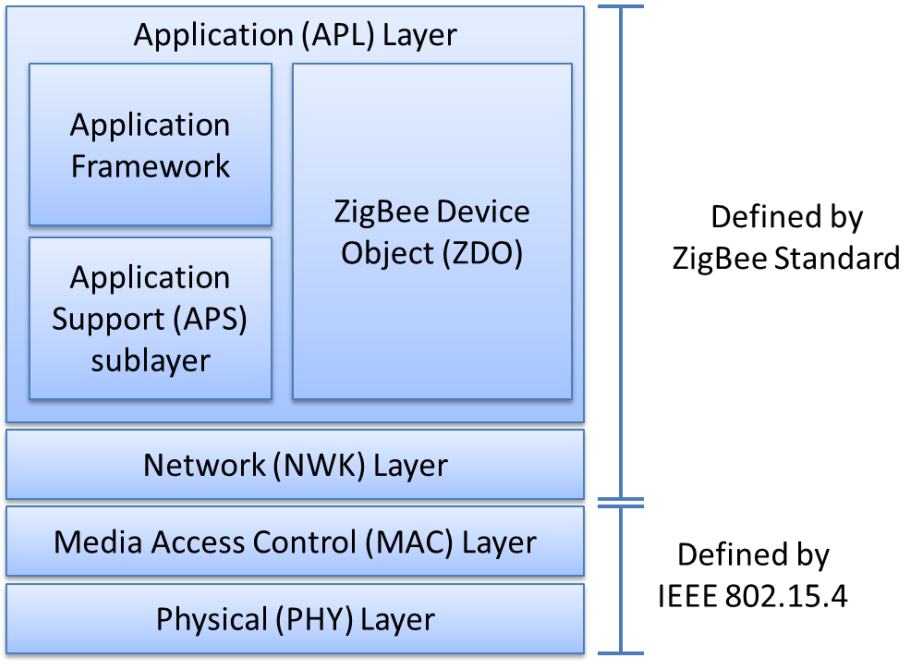

Figure 3 ZigBee Stack (derived from [12])

The data rate of ZigBee varies depending on the ISM frequency used. Table 2 details some of the basic technical details. For full technical specifications refer to the full standard[13].

ZigBee network standards on top of IEEE 802.15.4								
Freq.	Local	Data rate per channel (kbits/s)	Number of channels	Modulation	Approximate indoor range		Approximate outdoor range	
					(m)	(ft)	(m)	(ft)
2.4 GHz	Worldwide	250	16	DSSS w OQPSK	10	33	75	250
915 MHz	Americas	40	16	DSSS w/ BPSK	10	33	75	250
868 MHz	Europe	20	16	DSSS w/BPSK	10	33	75	250

Table 2 ZigBee Network Standards

ZigBee networks contain three different types of devices.

[12] Cache, J et. al. Hacking Exposed Wireless 2nd Edition
[13] www.zigbee.org/

1. **ZigBee Coordinator (ZC)** The ZC is a "full function device" (FFD). This device is the root of the network and manages connections to other networks. Each ZigBee network will have exactly one ZigBee Coordinator. The Coordinator serves as the network's Trust Center and is a repository for security keys and authorizes other ZigBee devices to join the network. ZCs are typically wall powered.
2. **ZigBee Router (ZR)** The ZR is also an FFD that routes data between ZigBee devices within a network but does not perform the network management tasks of the ZC (e.g. it does not communicate with other ZigBee networks). ZRs are typically wall powered.
3. **ZigBee End Device (ZED)** ZEDs have reduced functionality. These devices are designed with minimal functionality. End devices cannot relay data from other devices. The minimal functionality allows ZEDs to sleep a significant amount of the time thereby increasing battery life. ZEDs are typically battery powered.

ZigBee networks can be configured in either a star or mesh topology. The configuration will dictate whether ZRs are necessary.

ZigBee is used in a wide variety of devices; door locks, security sensors, load controllers, thermostats, energy management consoles and more recently remote controls. ZigBee is intended for low data rate, long battery life applications and is most often used as an electronic means to control physical devices. In addition to the core ZigBee specification, multiple standards exist for specialized applications in building automation, health care, home automation, input devices, remote control, retail services, smart energy, telecom services, and 3d sync. The areas most relevant to home area networks are building automation, home automation, and smart energy.

ZigBee Home and Building Automation focus on enabling smart homes and buildings that can control appliances, lighting, environment, energy management, and security as well as expand to connect with other ZigBee networks. ZigBee Smart Energy focuses on "interoperable products that monitor, control, inform and automate the delivery and use of energy and water."[14] These standards fit well into the HAN arena.

Beside the ZigBee specification the ZigBee alliance develops and makes available ZigBee Profiles. These profiles define the functionality of the device and interoperability requirements. The Smart Energy Profile (SEP), Home Automation (HA), Commercial Building Automation (CBA) are a few of the available profiles. Devices are designed and certified to meet specific profiles allowing the devices to be tailored to specific industries.

Advantages

- Many commercial products are available
- The certification process helps ensure interoperability
- Strong consortium of vendors support it
- Low cost / low power devices are available

[14] ZigBee Smart Energy Overview http://www.zigbee.org/Standards/ZigBeeSmartEnergy/Overview.aspx Accessed 19 Aug 2011

- ZigBee Profiles can be applied to other technologies allowing for interoperability between technologies

Disadvantages

- Bandwidth limitations of underlying IEEE 802.15.4 technology (250 Kbits/second per channel) may limit some smart grid applications for larger networks
- Security is optional
- Utilizes potentially congested ISM bands

Security Considerations

ZigBee has a number of security capabilities include within the protocol. It is possible to have a fairly robust security posture with a ZigBee network. The largest challenge facing ZigBee is in key management. The standard allows for individual link keys between any two nodes in a ZigBee network. But provisioning keys on the devices, storing, rotation and revocation of keys are all existing challenges. There are work-around solutions but they all have their problems. For instance ZigBee allows over-the-air (OTA) provisioning of keys which makes key rotation simple but the OTA provisioning is often done in clear-text which provides an opening for an attacker to obtain the keys. Another option is vendors can provision unique keys per consumer which works well for a large order but for small orders this becomes burdensome and so often the same key is put on every device.

Another implementation challenge is that the ZigBee specification allows essentially 4 different types of security.

1. No Security – Data is not encrypted or authenticated
2. AES-CBC-MAC (32,64,128) – Data is not encrypted but it is authenticated
3. AES-CTR – Data is encrypted but not authenticated
4. AES-CCM (32,64,128) – Data is encrypted and authenticated

End users must be vigilant that the correct type of security is enabled to meet the needs of their particular network or configuration and implementation errors are likely to occur.

Finally, ZigBee can be used as a stream cipher. Secure stream ciphers require a unique initialization vector (IV) or the encryption becomes trivial to break. In ZigBee the IV counter is a 32-bit value so there are ~>4.3 billion unique IVs thus reuse of IVs on a small network shouldn't be a problem for quite some time. The specification states that IVs must not be reused but how this is handled will vary by chipset manufacturer. No one wants their network to just quit working so how this is dealt with could leave open holes for exploitation.

Competing Technologies

ISA100.11a and Wireless HART

ISA100.11a and Wireless HART are both similar to ZigBee using many of the same building blocks found in IEEE 802.15.4 yet they both focus on the industrial sector with increased capabilities to mitigate interference from industrial environments.

Bluetooth

Bluetooth uses IEEE 802.15.1 as its base standard. It has three different classes 1, 2 and 3 with effective ranges of 1 meter, 10 meters and 100 meters respectively. Bluetooth has seen success as a point-to-point wire replacement and though it has limited networking capabilities it has not been used much in this area. Bluetooth may see limited action in the home area network but will not be a major player.

Summary

The emergence of the smart grid is bringing more networking players into the field. The need for low consistent bandwidth usage differs enough from the traditional information technology world to open the door to new technologies. The predominant players currently consist of a blend of the old and new. Within the wired world Ethernet and HomePlug Green PHY are leading the way with an advantage to HomePlug because it doesn't require installing new wires. In the wireless the realm there are many more competitors but WiFi and ZigBee seem to have the most momentum.

Acronyms

AC - Alternating Current
AES-128 - Advanced Encryption Standard 128 bit
AP - Access Point
CBC – Cipher Block Chaining
CCo – Central Coordinator (HomePlug)
CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance
EMI – Electro-Magnetic Interference
FEC – Forward Error Correcting
GP – Green PHY (Physical Layer)
HAN – Home Area Network
ISM - Industrial, Scientific and Medical
MAC – Media Access Control
MIMO - Multiple Inputs Multiple Outputs
MPDU – MAC Protocol Data Unit
NEK – Network Encryption Keys
NFC – Near-Field Communication
NMK – Network Management Keys
OFDM – Orthogonal Frequency Division Multiplexing
PBC – Push-Button Configuration
PDU – Physical Data Unit
PHY – physical layer
PIN – Personal Identification Number
PSK - Pre-Shared Key
QPSK- Quadrature Phase Shift Keying
RFI - Radio Frequency Interference
USB – Universal Serial Bus
WPS – Wi-Fi Protected Setup
ZED – ZigBee End Device