Wi-Fi® for the Smart Grid

Mature, Interoperable, Secure Technology for Advanced Smart Energy Management Communications

Wi-Fi Alliance®

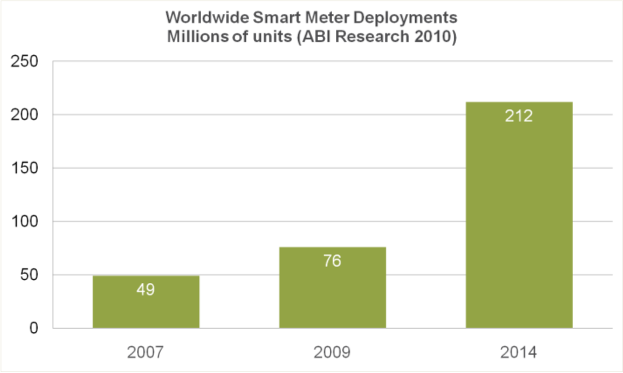
September 2010

The following document, and the information contained herein regarding Wi-Fi Alliance programs and expected dates of launch, is subject to revision or removal at any time without notice. THIS DOCUMENT IS PROVIDED ON AN "AS IS", "AS AVAILABLE" AND "WITH ALL FAULTS" BASIS. THE WI-FI ALLIANCE MAKES NO REPRESENTATIONS, WARRANTIES, CONDITIONS OR GUARANTEES AS TO THE USEFULNESS, QUALITY, SUITABILITY, TRUTH, ACCURACY OR COMPLETENESS OF THIS DOCUMENT AND THE INFORMATION CONTAINED IN THIS DOCUMENT.

Executive Summary

Smart Grid solutions are being driven by the desire for more efficient energy usage worldwide. The Smart Grid communications network will be a heterogeneous network based on many different standards. Wi-Fi® technology will certainly be part of any future Smart Grid.

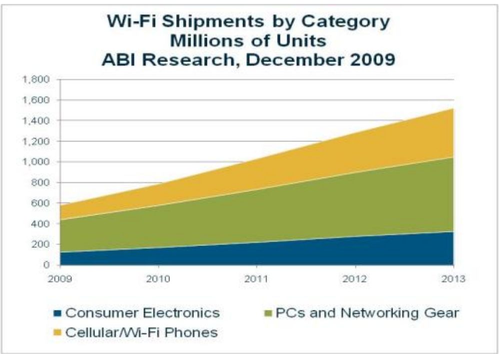
Wi-Fi is mature, proven technology that implements many of the Smart Grid application scenarios today. Wi-Fi networks can be deployed to meet the Smart Grid requirements for robustness, manageability, performance and security. Wi-Fi is cost effective, scales to cover large geographies and many endpoints, and requires no new cabling. Moreover, Wi-Fi technology has an ongoing roadmap of innovation and established mechanisms for collaboration (via the Wi-Fi Alliance® and IEEE) to meet the evolving needs of Smart Grid applications well into the future.



The US Department of Energy recently estimated that if Smart Grid benefits were fully realized in the United States, 442 million metric tons of carbon emissions could be saved – the equivalent of 66 coal fired power plants.[1] Grid modernization stimulus funding totaling US$3.4B has been approved. There is also strong private investment in the US and worldwide. There was marked growth in venture capital funding during the second half of 2009, and private investments totaled US$1.9B in the first quarter of 2010. [2]

In the US, utilities have begun or accelerated Smart Grid deployments. Pacific Gas & Electric in California is targeting 100% deployment in 2012. Worldwide deployment of Smart Grid meters was 76M in 2009 and is predicted to reach 212M by 2014.[3]

Worldwide adoption of Wi-Fi has been an unconditional success story. Sales have grown at double-digit rates every year[4] since the Wi-Fi Alliance introduced the term Wi-Fi in 2000, and that rate of growth is expected to continue in the future. Wi-Fi complements broadband infrastructure investment – providing high-performance local area mobility at the residential endpoint. Wi-Fi also complements 3G technology – extending coverage indoors and allowing service providers to offload data-intensive communications. For these reasons and more, about half a billion Wi-Fi devices shipped in 2009 and annual shipments are expected to grow to 1 billion by 2012.[5]



[1] US Department of Energy
[2] *Smart Energy News*
[3] ABI Research 2010
[4] ABI Research, Wi-Fi IC Market Data, 3Q 2010
[5] ABI Research, Wi-Fi IC Market Data, 3Q 2010

Background

The need for Smart Grid solutions is being driven by the emergence of distributed power generation and management/monitoring of consumption, and the desire for more efficient energy usage worldwide. Smart Grid advancements will apply digital technologies to the grid, enabling two-way communications and real-time coordination of information from generating plants, distribution resources and demand-side end points.

Government and Regulatory Forces

The U.S. Department of Energy is accelerating the development of a smart electric grid system targeting long-term savings for consumers by improving the efficiency and operation of the grid. The Smart Grid Policy Statement sets priorities for work on development of standards crucial to a reliable Smart Grid.[6]

As defined by the Department of Energy, the Smart Grid Standards must:

Table of Contents

- Provide two-way communication among grid users, e.g. regional market operators, utilities, service providers and consumers
- Allow power system operators to monitor their own systems as well as neighboring systems that affect them so as to facilitate more reliable energy distribution and delivery
- Coordinate the integration into the power system of emerging technologies such as renewable resources, demand response resources, electricity storage facilities and electric transportation systems
- Ensure the cyber security of the grid

Standards are critical to enabling interoperable systems and components. Mature international standards are the foundation of markets for the millions of components that will have a role in the future Smart Grid.

In the US, NIST has established the Smart Grid Interoperability Panel (SGIP) as a public/private partnership through which industry and government stakeholders can guide the identification, development, and certification of standards for the Smart Grid. The Wi-Fi Alliance and many of our member companies are voting participants in the SGIP, including representation on the Test and Certification Committee and active leadership within the Wireless Priority Action Plan (PAP) currently underway.

The Wi-Fi Alliance

In the ten years since its inception, the Wi-Fi Alliance has provided an important forum for innovation. In addition to interoperability testing, the organization is the birthplace of widely-deployed specifications including Wi-Fi Multimedia™ (WMM®) for Quality of Service on multimedia networks and Wi-Fi Protected Setup™ to ease setup of security-protected home and

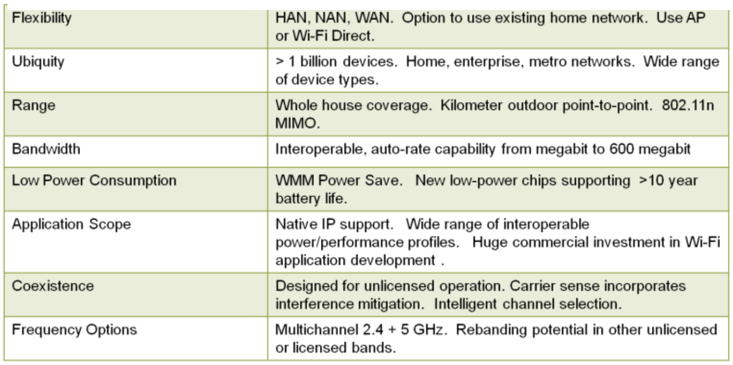
[6] Federal Energy Regulatory Commission

small office networks. Wi-Fi Alliance task groups address industry opportunities by developing testing programs which address market needs for interoperability, security protection, and performance.

Wi-Fi offers many benefits for Smart Grid applications:

- Mature technology with an established worldwide testing network
- Suitable for personal-area, home-area, and even wide-area networking
- Government-grade WPA2™ security
- Portfolio includes low bandwidth/low power designs, high-gain/high performance systems and points in between – *all can interoperate*
- Advanced mechanisms for reliability, robustness and manageability
- Continued technology innovation now and in the future, leveraging an interoperable set of baseline standards
- Economies of scale drive cost effectiveness

Wi-Fi Benefits for Smart Grid Application



Flexibility	HAN, NAN, WAN. Option to use existing home network. Use AP or Wi-Fi Direct.
Ubiquity	> 1 billion devices. Home, enterprise, metro networks. Wide range of device types.
Range	Whole house coverage. Kilometer outdoor point-to-point. 802.11n MIMO.
Bandwidth	Interoperable, auto-rate capability from megabit to 600 megabit
Low Power Consumption	WMM Power Save. New low-power chips supporting >10 year battery life.
Application Scope	Native IP support. Wide range of interoperable power/performance profiles. Huge commercial investment in Wi-Fi application development .
Coexistence	Designed for unlicensed operation. Carrier sense incorporates interference mitigation. Intelligent channel selection.
Frequency Options	Multichannel 2.4 + 5 GHz. Rebanding potential in other unlicensed or licensed bands.

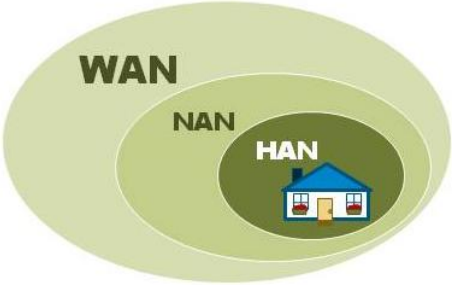
The Wi-Fi CERTIFIED™ program tests devices based on the IEEE 802.11 family of standards for interoperability and quality. The Wi-Fi CERTIFIED program provides a widely-recognized designation of interoperability and quality and has contributed to the success of Wi-Fi technology. Key attributes of Wi-Fi include:

- Mechanisms to deliver robust performance in shared-spectrum and noisy RF environments including listen-before-talk protocol, RF noise awareness and reporting, and received signal strength
- Transports all IPv4 and IPv6-based protocols, thereby supporting all IP-based applications, including Smart Energy Profile 2.0 for Smart Grid applications
- Extensive radio performance and network management mechanisms to provide radio link quality, history reports and channel selection optimization
- One standard that allows implementation of several interoperable performance/power dissipation profiles
- Rates ranging from 1 Mbps (802.11b) to 600 Mbps (802.11n)
- Networks scaling from a single pair of devices to thousands of access points and clients
- Security protections: Link-, network-, and application-level security based on international standards which meet FIPS 140-2 certification[7]
- Rogue device and intrusion detection tools
- Support for 2.4 GHz and 5 GHz ISM bands, U.S. 3650 MHz lightly licensed band and 4.9 GHz public safety band, and ongoing work on standardization for frequency bands below 1 GHz

[7] Sheila Frankel et al., “Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i,” February 2007, NIST Special Publication 800-97, http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf (8 September 2009).

Smart Grid Communications Networks and Wi-Fi

The Smart Grid communications network is typically partitioned into three segments: Home Area Network (HAN), Neighborhood Area Network (NAN), and Wide Area Network (WAN) or Backhaul. Wi-Fi technology addresses all three segments.



Wi-Fi in the Home Area Network

The HAN for the Smart Grid is used to gather sensor information from a variety of devices within the home, and optionally send control information to these devices to better control energy consumption. The electric meter on each residence is a natural place to aggregate this information and possibly act as a bridge to the NAN. Other architectures are also contemplated in which a bridging device separate from the meter serves as the interface between the utility and the customer-premise equipment. Wi-Fi can support both architectures.

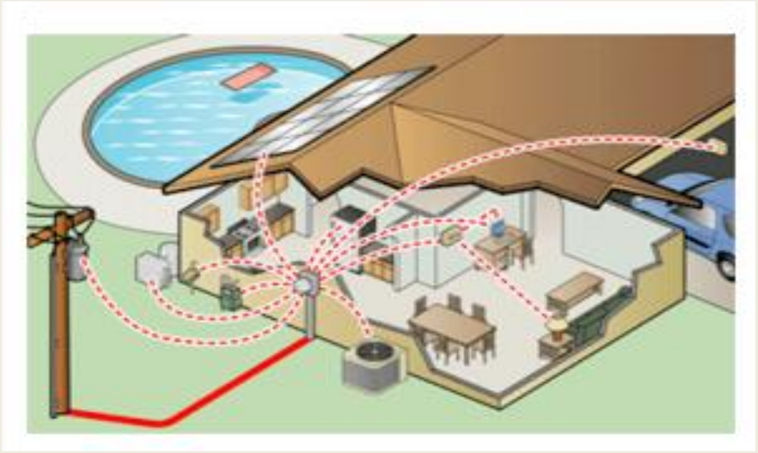
Wi-Fi is a superior technology for the HAN of the Smart Grid. Wi-Fi is based on very mature technology and has a large installed base in home networking - estimated at more than 100 million households worldwide[8]. The latest generation, Wi-Fi CERTIFIED n, is capable of distributing high definition video throughout the home, and Wi-Fi devices are also capable of supporting low data rate/low power applications as well. Wi-Fi is being included in a very wide range of portable and stationary consumer electronics devices, and its home market share will only increase. The Wi-Fi Smart Energy Home illustration shows a wide variety of devices that are already Wi-Fi enabled in the home. Wi-Fi is the key connection for all these devices to accessing the internet, and Smart Grid, and managing their energy usage.

Wi-Fi Smart Energy Home

Utility AMI Network
Internet

Wi-Fi operates in unlicensed spectrum and is designed to operate in this uncontrolled spectrum so as to be resilient to many types of interference. Wi-Fi coexists very well with other technologies that share these bands.

Wi-Fi has a mature ecosystem, with widely-demonstrated interoperability. The Wi-Fi Alliance's certification program is the benchmark for all other wireless technologies. Hundreds of vendors implement the technology in a wide range of devices. Ongoing innovations in power management are bringing tremendous improvements to Wi-Fi power dissipation profiles. Already the network of choice in millions of homes, Wi-Fi is ready to be the HAN standard for Smart Grid.



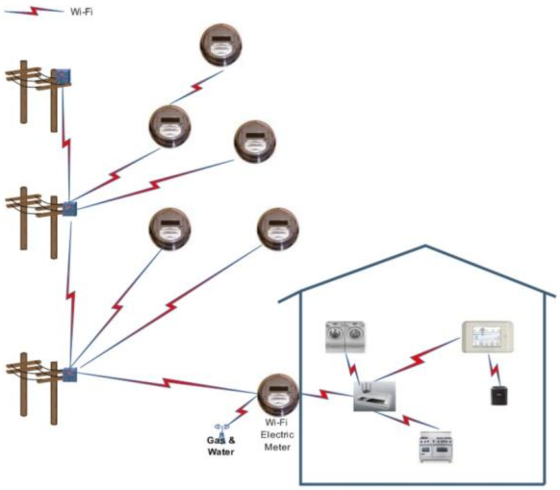
The Home Area Network

[8] Kurt Scherf, Parks Associates, "Networks in the Home: Global Growth; A Report for the Wi-Fi Alliance".

Wi-Fi in the Neighborhood Area Network

The NAN of the Smart Grid will collect information from many households in a neighborhood and connect them to a WAN. NAN endpoints may be utility meters mounted on the outside of single family houses or on the roof of multiple dwelling units, or alternatively may be separate interface units between the NAN and the customer premise. The transmission range should be at least 500 meters and can potentially incorporate a multi-hop mesh approach.

Municipal-scale Wi-Fi network infrastructure has already been deployed using 802.11 technology. This includes systems, for example, that provide access covering up to 500 meters from the AP, interconnected by point-to-point links based on 802.11 technology and using proprietary mesh protocols. Modern municipal Wi-Fi networks typically also support 4.9 GHz access for public safety networks that are also based on 802.11 technology. Newer developments in the 802.11n standard, including support for transmit beam forming, may further enhance the use of Wi-Fi for these outdoor applications.



The Neighborhood Area Network

Existing municipal 802.11-based networks are the appropriate scale for the Smart Grid Neighborhood Area Network. Wi-Fi can connect hundreds of devices on buildings and pole tops in a variety of terrains. The 4.9 GHz public safety application shows that Wi-Fi can be re-banded to support lightly licensed spectrum with different channel sizes. The Smart Grid NAN networks might benefit from operating in lightly licensed spectrum similar to the 4.9 GHz spectrum that has been set aside for public safety applications in the US.

Enhancements for the Smart Grid NAN can come from work being done within the IEEE 802.11s Task Group to standardize a mesh networking protocol and IEEE 802.11ah Task Group to standardize operation in bands including 902-928 MHz to extend range up to 1 km.

Wi-Fi in the Wide Area Network

The WAN for Smart Grid will aggregate data from multiple NANs and convey it to the utility private network.   Such “backhaul” can be implemented via point-to-point and/or point-to-multipoint wireless links. Smart Grid WANs may cover a very large area and could aggregate ten thousand supported devices. Multi-megabit capacity will be required, and the links involved may range from sub-kilometer to multi-kilometer distances.

Existing city-wide deployments of Wi-Fi networks demonstrate the clear applicability of Wi-Fi as a Smart Grid WAN technology. Minneapolis is just one example of a metropolitan installation in which Wi-Fi is used not only for neighborhood network access but in the WAN backhaul portion of the system as well.[9] Today such metropolitan area WANs incorporating standard 802.11 Wi-Fi in

[9] James Farstad, “Wireless Minneapolis a Growing Source of Promising Practices,” 13 March 2008, W2i Wireless Government Report, http://w2i.com/resource_center/the_w2i_report__weekly_newsletter/news/p/id_203 (8 September 2009).

point-to-point or point-to-multipoint links embody a variety of proprietary network management approaches, demonstrating that Wi-Fi technology could be similarly incorporated into the future standardized Smart Grid management framework for WAN communication. As more cities around the globe join Shanghai, Beijing and London in announcing plans to blanket large areas with Wi-Fi networks, there are more opportunities for these systems to link to Smart Grid applications.

A key advantage of Wi-Fi for the WAN Smart Grid is its use of free, unlicensed spectrum. This makes it practical for a city or utility to own and operate a large private wireless network for Smart Grid. Cellular data networks can provide the required service, but are usually owned and operated by large carriers who pay for the frequency licenses.

Wi-Fi Network Security

With WPA2, today's generation of Wi-Fi security, Wi-Fi CERTIFIED equipment offers advanced security tools to enterprise, home, and mobile users worldwide, across a wide and ever expanding range of devices. WPA2 functionality is supported in all new Wi-Fi CERTIFIED devices and access points and it is activated and used on a daily basis by a growing number of Wi-Fi users.

WPA2 is founded on two key protocols: (1) Advanced Encryption Standard (AES), the encryption protocol used by the United States and other governments to protect confidential and classified information, and by the enterprise to secure WLANs, and (2) IEEE 802.1X, a standard widely used in corporate networks to provide robust authentication and sophisticated network access control features. WPA2 is based on IEEE 802.11i and provides 128-bit AES-based encryption. It also provides mutual authentication with Pre-Shared Key (PSK; in Personal mode) and with IEEE 802.1X / EAP (in Enterprise mode).

In 2004, the Wi-Fi Alliance introduced WPA2 certification. In 2006, WPA2 certification became mandatory for all Wi-Fi CERTIFIED equipment. In addition, in 2007 the Wi-Fi Alliance introduced the Wi-Fi Protected Setup™ program to simplify and encourage the activation of WPA2 in residential networks. With WPA2, Wi-Fi technology has reached a mature state that allows it to provide excellent, state-of-the-art security to all Wi-Fi users, across different device form factors, vendors, and geographical regions.

- **Mutual authentication.** WPA2 uses IEEE 802.1X (WPA2-Enterprise) and PSK (WPA2-Personal) to provide mutual authentication. With one-way authentication, the client device sends its credentials and, if access is authorized, the client device is connected to the network. Mutual authentication requires the client device to verify the network credential before establishing the connection, to prevent the user from connecting to unauthorized access points.
- **Strong encryption.** AES is defined as a Federal Information Processing Standard (FIPS Publication 197) and is the first publicly available encryption mechanism that meets the requirements of the U.S. government for protecting sensitive and classified information[10]. To date, AES has proved to be extremely resilient in the face of the high number of published attacks triggered by AES's wide adoption. The data travelling across a WPA2 network is encrypted using the CCMP algorithm with AES, which together provide the most advanced standards-based data encryption method available. AES support is required by many protocols and applications used worldwide in enterprise networks.
- **Interoperability.** WPA2 is a standards-based solution, supported by all Wi-Fi CERTIFIED equipment that has undergone testing since 2006. WPA2 can be activated within any session in which the access point and the client device support WPA2, regardless of the equipment

[10] Confidential information can use 128-bit AES; classified information requires 192- or 256-bit AES.

brands involved. This greatly expands the availability of WPA2 and gives confidence to network operators and users that their networks, devices, and data flows can be protected everywhere.

- **Ease of use.** WPA2 is not only a powerful tool to protect Wi-Fi users, it is also easy to activate. In 2007 the Wi-Fi Alliance introduced a separate certification program, Wi-Fi Protected Setup, to simplify the configuration of WPA2 and to accelerate its adoption in residential networks.

See the appendix section of this paper for a discussion on commonly asked questions regarding Wi-Fi and Smart Grid security.

Wi-Fi Network Measurement and Management

All wireless networks require network measurement and management to help optimize RF performance. Wi-Fi has extensive network management capabilities that integrate with existing enterprise network management systems and that make Wi-Fi suitable for very large scale deployments in the Smart Grid. Ensuring that these networks securely and reliably serve the hundreds of thousands of users that rely upon them requires both autonomous and centrally administered problem diagnosis and performance optimization.

Wi-Fi Network Management systems in place today provide:

- Visibility into device performance and usage
- Historical trend reporting
- Threshold-based alerts
- Scheduled events and reports
- Device configuration and reconfiguration, including multi-vendor management when networks are comprised of wireless devices from more than one manufacturer
- Centralized software updates

One major addition to the IEEE 802.11 standard, 802.11k, provides network measurement protocols. A second addition, 802.11v, adding a new suite of network management capabilities, is nearing completion. These two standards extend existing commercial device and management system product capabilities, allowing Wi-Fi devices to measure and report radio link and traffic characteristics. Availability of this information enables optimization in performance and reliability through both local responses (e.g. transmit power control and radio channel change of a wireless Access Point or client device) and centralized management of these extended Wi-Fi networks.

Smart Grid Wireless Use Cases

Wi-Fi can be advantageously employed in a variety of Smart Grid Use Cases -- here are just some examples.

Home Thermostats

A central application of the Smart Grid in a HAN is the thermostat. Between thirty-five and sixty percent of a home’s energy consumption can be measured and controlled through networked thermostats which control the Heating Ventilating and Air Conditioning. By adding low-power Wi-Fi sensor devices and networking capability to appliances, heating systems, air conditioning systems, water heaters and thermostats, homeowners and utility providers benefit by reducing their energy consumption and supporting conservation initiatives. Homeowners can monitor and control energy consumption with minimal effort and also benefit from incentives sponsored by their utility providers for energy conservation. Wi-Fi technology represents a massive installed base that already exists in many homes and buildings, and utility providers, by extending a Smart Grid inside the house using Wi-Fi, can better manage peak demand.

Since Wi-Fi devices are designed to operate within an IP networking environment, there is no specific requirement for a gateway element to handle network address translation or custom provisioning.

Advanced Metering Infrastructure (AMI)

AMI provides communications between the consumer end-points of the grid and the backhaul. A major element in the communication networks required to support AMI is the NAN which couples the consumer premises to the WAN of the utility company.

As described earlier, Wi-Fi is capable of providing the IP-based NAN capability from a meter to a data collection device in each neighborhood and thus can support the AMI. By leveraging high gain antennas and other antenna technology such as beam steering, a Wi-Fi radio can provide line-of-sight range to pole-top access points of more than one kilometer.

Grid Intelligence

Efficiency in the transport and delivery of electricity through the grid represents an enormous savings to the utility provider, and ultimately the end consumer of electricity. The current electric grid infrastructure is comprised primarily of legacy, latency-sensitive equipment with one-way or no communication with utility back-end systems.

With the use of Wi-Fi, one can layer a reliable, high-speed, low-latency IP two-way communications network on top of these legacy grid elements. This will allow these elements to respond to conditions in the grid by providing distributed intelligence. Such responsiveness is not possible without a two-way communications network. Incorporating Wi-Fi in the grid intelligence also allows utilities to further reduce operational expenses due to the self-healing, proactive measures possible with a high-speed, IP-based electric grid.

Gas and Water Metering

Many electric utilities are also responsible for natural gas and water delivery to the end customer. Accordingly, there is a need to collect the usage information from gas and water meters in addition to electric meters. The same communications infrastructure being deployed in an electric utilities service territory can be used to collect gas and water usage information. Leveraging Smart Grid assets for these purposes will reduce the capital and operational expense of an integrated utility responsible for gas and electric delivery to the consumer. In cases in which different utilities provide gas, water, and electricity, infrastructure-sharing can improve efficiency and cost of deployment.

Gas and water meters do not typically have access to a power source. Low-power battery-operated endpoints are critical for mass adoption of wireless communications in these meters. Using the latest low-power technology from Wi-Fi solution providers can result in 10 or more years of battery life.[11] Until recently, Wi-Fi enabled devices have not met the 15 to 20 year battery life requirements of such devices as it relates to lower power consumption. However, several new Wi-Fi chip sets have sub uA leakage and are capable of working in systems where the total current in low-power mode is far less than 1 uA.[12] In such a state, battery life can be radically extended. While a low-power host micro-controller maintains the application in the meter, the Wi-Fi radio can be kept in an off position. Information can then be cached and burst through the NAN periodically.

[11] GainSpan, 8 September 2009, "Gainspan Unveils Wi-Fi Sensor Network Solution with Years of Battery Life".

[12] Redpine Signals, 8 September 2009, "Redpine Signals Launches Sensifi an Ultra Low-Power 802.11n (Wi-Fi) Wireless Sensor Module," http://www.redpinesignals.com/18feb09.html.
ZeroG Wireless, 8 September 2008, "ZeroG Wireless Announces Availability of the Industry's First 'Wi-Fi I/O' for Embedded Systems".
GainSpan, 8 September 2009, "Gainspan Unveils Wi-Fi Sensor Network Solution with Years of Battery Life".

Enterprise Mobility for Utility Companies

Utilities will need to have high-speed, reliable communications throughout their service territory for Smart Grid communications. The utility's private Wi-Fi NAN used for AMI could also be used to carry both voice and data to support mobile applications for service technicians and field personnel, complementing existing cellular data and voice networks. Wi-Fi is an obvious choice for this wireless network since low cost interoperable Wi-Fi clients are available and already integrated into mobile phones, laptops, and tablet PCs. Cellular carriers today are using Wi-Fi to offload data and voice traffic.

Wi-Fi for Smart Grid: Gap Analysis

As discussed in the Report to NIST on the Smart Grid Interoperability Standards Roadmap, gap analysis is a critical part of the overall Smart Grid protocol requirements determination.[13] Of particular importance here with respect to the IEEE 802.11 standard is the identification of any potential gaps with regard to Smart Grid application support.

IP Protocol Support

All Wi-Fi devices support the Internet Protocol (IP), both IPv4 and IPv6. No new work is needed for full support of IP.

Smart Energy Profile

The Smart Energy Profile helps build a framework for Smart Grid Applications. Version 2.0 of the Smart Energy Profile was specified by NIST as a PHY independent protocol, which therefore could be implemented in Wi-Fi systems. The only work required for an implementer would be to port SEP 2.0 software to Wi-Fi-based devices. In March 2010, the Wi-Fi Alliance and the ZigBee Alliance announced a collaboration agreement regarding the development of SEP 2.0 supporting both Wi-Fi and ZigBee.

Substation Automation

The IEC 61850 protocol has been defined for substation automation. There is some work underway to expand the applications for IEC 61850. This is a high level message oriented protocol which can be carried over IP and thus Wi-Fi. The only new work required for an implementer would be porting IEC 61850 to Wi-Fi-based devices.

[13] Electric Power Research Institute, 10 August 2009, "Smart Grid Interoperability Standards Roadmap".

Summary

The Smart Grid communications network will be a heterogeneous network based on many different standards. Wi-Fi technology will certainly be part of any future Smart Grid. Wi-Fi is cost effective, scalable to cover large geographies and many endpoints, and requires no new cabling.

Wi-Fi is the dominant home wireless networking standard today, and thus plays a central role in the HAN for Smart Grid. Wi-Fi is already integrated into home routers, set top boxes, high definition televisions, notebook PCs and smartphones. Wi-Fi enabled thermostats, refrigerators, and washing machines make perfect sense. Whether as a separate network or integrated into existing home networks, Wi-Fi should be the primary HAN for the Smart Grid.

There are many mature products based on 802.11 technology that implement large outdoor networks. These networks have been successfully deployed for years and there is broad expertise available to the industry for deploying and maintaining these types of networks. It is more practical to reuse these existing technologies for the Smart Grid application than to create a new wireless standard or develop a new ecosystem from scratch.

Wi-Fi technology has an ongoing roadmap of innovation and established mechanisms for collaboration (via the Wi-Fi Alliance and IEEE) to meet the evolving needs of Smart Grid applications well into the future. If a need is identified to extend the existing capabilities, the Wi-Fi Alliance provides a well-established forum for further innovation to occur and timely delivery of solutions. Using this expertise and experience, the Wi-Fi Alliance membership is exploring how it might quickly eliminate any real or perceived gaps in Smart Grid deployment phases.

The Wi-Fi Alliance is committed to supporting the spirit of the Smart Grid initiative and to deliver broad-based standards solutions that are broadly accepted by consumers, utilities, product vendors and the ecosystem. Today a vast array of Wi-Fi enabled products are available for Smart Grid HAN connectivity, including thermostats, appliances, automobiles and consumer electronics. And Wi-Fi is utilized in everyday industrial applications with proven reliability and resilience in environments with high and uncontrollable interference – a perfect match for the conditions faced in Smart Grid energy management.

About the Wi-Fi Alliance

The Wi-Fi Alliance is a global non-profit industry association of hundreds of leading companies devoted to the proliferation of Wi-Fi technology across devices and market segments. With technology development, market building, and regulatory programs, the Wi-Fi Alliance has enabled widespread adoption of Wi-Fi worldwide.

The Wi-Fi CERTIFIED^{TM} program was launched in March 2000. It provides a widely-recognized designation of interoperability and quality, and it helps to ensure that Wi-Fi enabled products deliver the best user experience. The Wi-Fi Alliance has completed more than 8,000 product certifications to date, encouraging the expanded use of Wi-Fi products and services in new and established markets.

APPENDIX: Wi-Fi Security and Smart Grid Frequently Asked Questions

Is Wi-Fi Secure?

WPA2 is the latest version of Wi-Fi security, and it should be used to protect all Wi-Fi devices. WPA2 was introduced in 2004 and has been required in Wi-Fi CERTIFIED products since April 2006. It supports Advanced Encryption Standard (AES), the most advanced encryption standard. AES is the encryption standard endorsed by the US government. The Wi-Fi Alliance recommends that users select equipment supporting WPA2 to help protect their network from known attacks to their security and privacy. With WPA2, Wi-Fi technology has reached a mature state that allows it to provide excellent, state-of-the-art security to all Wi-Fi users, across different device form factors, vendors, and geographical regions.

In the context of Wi-Fi technology, security means two things. First, controlling who can connect to and configure your network and equipment. Second, it means securing the data travelling wirelessly across your Wi-Fi network from unauthorized view.

Wi-Fi security is just one aspect of security for networks. A protected Wi-Fi network is a great start, but you should also consider measures to protect your computer (virus software, firewall, etc.) and your communications across the Internet (virtual private network (VPN), etc.)

What security technology is used in Wi-Fi? Is it NIST approved?

Wi-Fi security is based on IEEE 802 standards that use the cryptographic algorithms that are recommended by NIST (the National Institute of Standards and Technology). The IEEE 802.11 standard encrypts all communications with the AES that was selected by NIST. The authentication process for Wi-Fi is based on the IEEE 802.1X standard for port based access control. There are several ways to authenticate devices that allow simple home installation with passwords or enterprise grade solutions with central authentication servers. Authentication with RADIUS servers use the Extensible Authentication Protocol (EAP) with methods that have been defined by the Internet Engineering Task Force (IETF) and reviewed and approved by NIST.

What is WPA2?

WPA2 is today's generation of Wi-Fi security. It is founded on two key protocols: (1) AES, the encryption protocol used by the United States and other governments to protect confidential and classified information, and by the enterprise to secure WLANs, and (2) IEEE 802.1X, a standard widely used in corporate networks to provide robust authentication and sophisticated network access control features. WPA2 is based on IEEE 802.11i and provides 128-bit AES-based encryption. It also provides mutual authentication with Pre-Shared Key (PSK; in Personal mode) and with IEEE 802.1X / EAP (in Enterprise mode). In 2004 the Wi-Fi Alliance introduced WPA2 certification. In 2006 WPA2 certification became mandatory for all Wi-Fi CERTIFIED equipment. In addition, in 2007 the Wi-Fi Alliance introduced the Wi-Fi Protected Setup program to simplify and encourage the activation of WPA2 in residential networks. With WPA2, Wi-Fi technology has reached a mature state that allows it to provide excellent, state-of-the-art security to all Wi-Fi users, across different device form factors, vendors, and geographical regions.

- **Mutual authentication.** WPA2 uses IEEE 802.1X (WPA2-Enterprise) and PSK (WPA2-Personal) to provide mutual authentication. With one-way authentication, the client device sends its credentials and, if access is authorized, the client device is connected to the network. Mutual authentication requires the client device to verify the network credential before establishing the connection, to prevent the user from connecting to unauthorized access points.

- **Strong encryption.** AES is defined as a Federal Information Processing Standard (FIPS Publication 197) and is the first publicly available encryption mechanism that meets the requirements of the U.S. government for protecting sensitive and classified information.[14] To date, AES has proven to be extremely resilient in the face of the high number of published attacks triggered by AES's wide adoption. The data travelling across a WPA2 network is encrypted using the CCMP algorithm with AES, which together provide the most advanced standards-based data encryption method available. AES support is required by many protocols and applications used worldwide in enterprise networks.
- **Interoperability.** WPA2 is a standards-based solution, supported by all Wi-Fi CERTIFIED equipment that has undergone testing since 2006. WPA2 can be activated within any session in which the access point and the client device support WPA2, regardless of the equipment brands involved. This greatly expands the availability of WPA2 and gives confidence to network operators and users that their networks, devices, and data flows can be protected everywhere.
- **Ease of use.** WPA2 is not only a powerful tool to protect Wi-Fi users, it is also easy to activate. In 2007 the Wi-Fi Alliance introduced a separate certification program, Wi-Fi Protected Setup, to simplify the configuration of WPA2 and to accelerate its adoption in residential networks.

Is WEP still used?

Smart Grid applications will not use WEP. The AES replaced WEP security in 2004. The AES algorithm is NIST approved and is the basis of the WPA2 wireless security certified by the Wi-Fi Alliance. After 2013, no Wi-Fi CERTIFIED devices will contain WEP. There are some home wireless networks that only support WEP. Equipment that only supports WEP must be upgraded to connect to Smart Grid devices.

How will Wi-Fi security be used in the Smart Grid?

Wi-Fi today is used in homes, small and large businesses, industrial facilities, and in metropolitan-scale networks. Wi-Fi security is a key technology in all these environments. Wi-Fi's flexibility means that it will have a role to play in a wide variety of Smart Grid environments, including the home, neighborhood concentration, and backhaul – the HAN, NAN, and WAN. Wi-Fi is already being used in substation applications. Since Wi-Fi WPA2 security technology already supports both small and large deployments, it can be immediately adapted into all of these Smart Grid applications. But it is important to recognize that Wi-Fi security technology will be integrated into a comprehensive Smart Grid cybersecurity solution. Thus, while Wi-Fi WPA2 security is focused on protecting the Wi-Fi wireless link from security threats, it also will work in conjunction with additional end-to-end security protocols and authentication systems that together protect the complete Smart Grid.

Can Smart Grid usage data be accessed via a wireless Smart Grid device?

WPA2 data confidentiality ensures that over the wireless Wi-Fi link, only the sender and intended receiver of data sent on the link can read the data as it traverses the wireless link. Usage data sent on a WPA2 protected wireless link from an appliance, for example, to a network access device is protected from eavesdropping by other devices.

Storage of an end user's energy usage data by the end user, a utility or other energy management provider is independent from protected transfer of data on the wireless link.

[14] Confidential information can use 128-bit AES; classified information requires 192- or 256-bit AES.

The NIST DRAFT Smart Grid Cyber Security Strategy and Requirements document contains an analysis of data privacy concerns and recommended practices for data collection and availability of end user data in Section 4.

Is WPA2 end-to-end security?

WPA2 provides security at the Link Layer of the ISO model, thereby protecting the data as it traverses the Wi-Fi wireless link.   If the Wi-Fi network is connected via routers to non-Wi-Fi networks, other security protocols would be invoked to provide link-level security within those networks, and typically also to provide end-to-end protection. For example, banking transactions from a Wi-Fi laptop over the internet are ordinarily “double protected” as the data traverses the Wi-Fi link – protected first by WPA2’s link-level encryption provided over the Wi-Fi link, and also protected by end-to-end encryption over not just the Wi-Fi link but the entire internet.