# A Security Standard for AMI Smart Meters

Coalton Bennett coalton@enernex.com
Darren Highfill darren@enernex.com
Stephen B. Wicker wicker@ece.cornell.edu

***Abstract--* There is a growing interest in 'Smart Grid' technologies in both industry and academic circles. Few attempts have been made to develop a written specification consummated with standards agreed upon by members of both coteries, due to lack of government support. Utilities in the state of California are obligated, by state legislature, to create a more: efficient, reliable, and intelligent electric power system. This initiative along with Florida Power & Lighting's 'Smart Grid' pilot program has created a sense of exigency within the industry regarding smart grid technologies and standardizations. Their accomplishments are beginning to shape the policies and standards with marginal input from academic societies, ushering in a very lopsided, and business acclimatized set of standards. We will present and analyze, a SCE 'Smart Grid' use case, in which the utilities back office applications interact with the customer's meter, and provide technical recommendations for system security improvements.**

## I. Introduction

THE need for a smart grid, and in particular: demand response, outage management, disaster prevention, and disaster recovery systems, has become a growing concern in many circles—utilities, academics, and energy/environmentally conscience customers [1][2][3][4][5]. This has been a driving (key) factor in utility and vendor communities alike, to integrate legacy physical infrastructure with new an emerging technologies. Currently there are several utilities that have taken steps towards integrating more avant-garde telecommunications technologies with new and improved solid-state metering devices. Most new meters being installed across the country are comprised of: a solid-state device responsible for monitoring electricity consumption, in addition to a two-way communications device—this comprises the AMI meter [4]. No standards documents exist yet formally defining, the Smart Grid, let alone demand response systems. Although some efforts have been made on behalf of the state of California to better define such a system [4]. An AMI system consists of four major components, namely the: meter, in home portal/display provided by the gateway, a neighborhood data collection point (collector/access point), and the central office. While each component is vital to the correct operation of, the AMI and demand response systems, for the purposes of this paper we restrict our investigation to the first three components: the meter, portal, and access point.

The work presented in this paper was supported in part by the Team for Research in Ubiquitous Secure Technologies (TRUST)

Affliations: Coalton Bennett is a graduate student at Cornell University in the Department of Electrical and Computer Engineering, Ithaca NY 14850 U.S.A.
Darren Highfill is with EnerNex Corporation, Knoxville TN 37932 U.S.A.

Our first objective in writing this paper is to identify and review certain communication technologies that we believe are critical for future demand response systems. Our second objective is to provide a basis from which industry and academic participants can draw upon as a reference guide when implementing, testing, and or simulating a demand response system. The components, we have chosen to include in the demand response system description, are by no means standard components, however the UCAIug[1] has considered these components to be an integral part of any demand response system. Even though we will reference material, which has yet to be approved by an official standards body such as IEEE, we feel confident that most utilities, many of which have contributed to the development of this material, will adopt a similar AMI system design if they haven't already.

In this paper we will present a few technologies currently being considered, or used, in AMI system deployments throughout the country, and analyze the networks necessary for transporting demand response information. In addition we will identify possible security and privacy vulnerabilities inherent in such a demand response system consisting of 5000+ nodes, with a particular focus on maintaining customer anonymity.

## II. Wireless Home Area and Neighborhood Area Network Solutions

In the author's previous work [6] they showed that it is possible to turn any appliance into a smart appliance, using a wireless radio and a relay, and network these appliances via PC using the 802.15.4 protocol. Two very forward thinking utilities in the United States, SCE (Southern California Electric) and FPL (Florida Power & Lighting), have began to deploy AMI meters equipped with 802.15.4 radios. An AMI meter is defined as a meter providing: two-way communications, automated meter data collection, outage management, dynamic rate structures, and demand response for load control [7]. These features make real time communication between appliances, the meter, and subsequently the utility a reality. Other technologies are also being considered as viable options for such communications [HomePlug references]. However this particular technology would have to send signals through transformers, which might prove to be problematic in an outage management situation, or something equally as important. Therefore a wireless link to the meter seems to be the most robust technology for a demand response system.

[1] The UCA® International Users Group is a not-for-profit corporation consisting of utility user and supplier companies dedicated to promoting the integration and interoperability of electric/gas/water utility systems through the use of international standards-based technology.

### *A. IEEE Low Rate Wireless Personal Area Network Energy Specifications*

The low-rate wireless personal area network standard, (LR-WPAN 802.15.4), was developed so as to provide the same functionality of a traditional sensor network, while optimizing the lifetime of the devices. Most traditional sensor networking stacks, which are based on the 802.11.x protocol, were not designed with this focus in mind. In order to maximize the lifetime of a battery powered 802.11 device, the physical(PHY) and media access control(MAC) layers must be modified [18][19][20]. The 802.15.4 MAC layer was designed to increase the expected lifetime of a device, thus making it the preferred solution. This becomes especially important for appliances that have higher duty cycles.

In [9] the authors state that, "application-specific energy-aware cross-layer optimization can improve network performance." The Media Access Control (MAC) and Physical (PHY) layer standards of the 802.15.4 radio were created for a multitude of network organization designs. This serves as a driver for the development of a collection of different higher-level protocols. Zigbee is an open standard thus making it one of the more popular 802.15.4 networking solutions. There is also a proprietary solution offered by MicroChip, which also uses the 802.15.4 standard. However this solution limits vendors to MicroChip components when designing products for utilities, third parties, or consumers [21].

### *B. Overall System Design*

In the system that we consider, the meter serves as a PAN (Personal Area Network) coordinator, or a full-function device (FFD), for each appliance, or reduced-function device (RFD) in the network [11]. In addition to the meter's ability to coordinate appliances within the Home Area Network(HAN), the meter will also provide a communication link to the Neighborhood Area Network(NAN) access point using an 802.15.4 radio. For this paper we have chosen the Zigbee networking standard because of its ability to form self-organizing self-healing mesh networks. Given the fact that 802.15.4 radios can successfully transmit packets a distance of 50 meters—nearly half the length of a football field—the meters can form either a mesh or star network with other meters in the neighborhood. Within an average size residential dwelling, the distance between the appliance and the meter will be at most 30 meters. Thus appliances can transmit packets using a lower power setting.

Appliance registration can also be accomplished, if a customer has enrolled in a direct load control program with their electric utility. This would in turn give the utility the ability to toggle the state of an appliance within the home. This being said the utility should keep customer data private and, under no circumstance should a utility release customer data to an unauthorized entity.

In the next section we will reference a system requirements specification document, which has been ratified by twelve investor-owned North American utilities, and endorsed by two others [22]. This document outlines the Guiding Principles, Use Cases, System Requirements, Architectural Drawings, and Logical Device Mappings for platform agnostic Home Area Network devices. The OpenHAN System Requirements section of [22] provides information about five different fundamental components, however in this paper we will only address the system components necessary for successful communication between devices within the HAN. The neighborhood area network will be discussed in the second section, and the wide area network will be discussed in the third. In conclusion we show how all three sections can be tied to together to create a comprehensive network of smart appliances and AMI smart meters.

## III. Home Area Network

In this section we will briefly outline the communication and security requirements listed in [22] and show how the open standard networking protocols developed by the Zigbee Alliance satisfy the requirements in this specification with little, or, no modification.

### *A. Communication Requirements*

There are two components necessary for "reliable message transmission" between the customer's HAN devices and the utility's back office systems. The first requirement is Commissioning: which is responsible for identifying new appliances(nodes) and adding/removing them from a self-organize network. The second requirement is Control: which is responsible for maintaining the communication link between appliances within the network.

The commissioning of a node to a network requires that thirteen criteria be met. In the table below we compare the rudimentary requirements for both the OpenHAN Network System Requirements Specification (NSRS) and the Zigbee Specification. Several of the OpenHAN requirements are met with the Zigbee specification. Although these are, at most, a very basic set of requirements we believe that as the OpenHAN (NSRS) is developed, a number of the requirements will coincide exactly with the Zigbee specification. Thus making the tasks for utilities and vendors much less complicated when offering demand response service and products. The only requirement is that the services and products meet the standards outlined below.

| OpenHAN Device Commissioning Requirements | Zigbee Device Commissioning Requirements |
|---|---|
| **Comm.Commision.1**<br>HAN Device shall accept network configuration data which allows for private Utility networking (e.g. private address/ID) | **Capability Information Bit-Field.7**<br>The joining device must be issued a 16-bit network address, except in the case where a device has self-selected its address while using the network rejoin command, to join a network for the first time in a secure manner. |

| | |
|---|---|
| **Comm.Commission.2** HAN Device shall accept commissioning configuration data by the manufacturer (e.g., link key). | **Mixing Standard and Proprietary Profiles** If manufacturer extensions (e.g. commissioning configuration data) are not supported, or the type of desired manufacturer extensions are not in a public profile, then the manufacturer may deploy the extensions in a separate manufacturer-specific profile identifier within the same physical device.[2] |
| **Comm.Commission.3** HAN Device shall accept commissioning configuration from the Installer. | **End Device Binding** Provides the ability for an application to support a simplified method of binding where user intervention is employed to identify command/control device pairs. Typical usage would be where a user is asked to push buttons on two devices for installation purposes. |
| **Comm.Commission.4** When Energy Services Interface is triggered (e.g., Allow Join Command), HAN Device location-/contact-specific data shall be provided to other HAN Devices in the premise. | **Network Layer Management Entity (NLME)** *Neighbor discovery*: this is the ability to discover, record, and report information pertaining to the one-hop neighbors of a device. |
| **Comm.Commission.5** When a HAN Device is triggered (e.g. Power-on, button), HAN Device shall provide the Energy Services Interface with device-specific information including device ID and device type. | **Creating a Zigbee Profile** The key to communicating between devices on a ZigBee network is agreement on a profile. An example of a profile would be home automation. This ZigBee profile permits a series of device types to exchange control messages to form a wireless home automation application. These devices are designed to exchange well-known messages to effect control such as turning a lamp on or off. |
| **Comm.Commission.6** When a HAN Device is triggered (e.g. power on, button), HAN Device shall provide the Energy Services Interface with device specific Utility information, including network ID, gateway ID, and Utility ID, if pre-configured with Utility information. | **Device and Service Discovery** Device and Service Discovery are distributed operations where individual devices respond to discovery requests. The device address of interest field enables responses from the device regarding the device and the services that it offers.[3] |
| **Comm.Commission.7** Energy Services Interface shall have the ability to accept or reject a request based on device type. | **Application Support Sub-Layer Management Entity (APSME) Key Establishment** This primitive provides the responder with an opportunity to determine whether to accept or reject a request to establish a key with a given initiator, based on any number of different criteria (e.g. device type). |
| **Comm.Commission.8** Energy Services Interface shall have the ability to accept or reject device requests based on Utility-specific information (e.g., network ID, gateway ID, or Utility ID). | **Trust Center** The trust center can be configured such that devices without an identifiable IEEE address will be either accepted or rejected. [23] |
| **Comm.Commission.9** HAN Device shall acknowledge successful commissioning requests (i.e., provide acknowledgement to the requesting HAN Device). | An acknowledgement is issued per frame. |
| **Comm.Commission.10** When a HAN Device is communicating with the Energy Services Interface, HAN Device shall indicate link connectivity. | **Network Management** This includes several capabilities including: energy detection scan results for link connectivity between devices. |
| **Comm.Commission.11** HAN Device shall provide notification to the Installer of the commissioning status. Status conveyed shall be either: successful/unsuccessful. | **End Device Binding** Provides the ability for an application to support a simplified method of binding where user intervention is employed to identify command/control device pairs. Typical usage would be where a user is asked to push buttons on two devices for installation purposes. |
| **Comm.Commission.12** Energy Services Interface shall maintain an updated list of commissioned (i.e., connected) HAN Devices. | **Trust Center Application** The center is required to maintain a list of: devices, master keys, link keys, and network keys that it needs to control and enforce the policies of network key updates and network |

[2] A profile identifier permits the profile designer to define the following:

- Device descriptions
- Cluster identifiers

[3] A complete listing of the values reported by the device can be found in section 2.4.2.1 of the Zigbee Specification document.

| | |
|---|---|
| | admittance. |
| **Comm.Commission.13** Energy Services Interface shall have the ability to remove HAN Devices from the Utility HAN. | **Remove Device Commands** There are command frames designed in the APS for removing devices. |

*B. Control Requirements*

HAN technologies should provide autonomous functions, enabling: efficient, robust, and reliable communication paths. These qualities can be ensured if control primitives are implemented. In this section we provide a comparison between the requirements outline in the OpenHAN SRS document and the standard features offered within the Zigbee stack.

| OpenHAN Device Control Requirements | Zigbee Device Control Requirements |
|---|---|
| **Comm.Control.1** HAN Device shall accept network organization messages from the Energy Services Interface (e.g., gateway location, routing table, address). | **Establishing a New Network** Each device which is not a Zigbee coordinator, and hence a parent device, is a child device, and network organizational tasks are disseminated from parent to child accordingly. [4] |
| **Comm.Control.2** HAN Device shall accept network organization messages from peer devices (e.g., hidden node). | **Joining a Network (Child Procedure)** All child devices which, attempt to join a new network, are required to use the information provided in their neighbor table entry in order to determine which available parent devices would work best. [5] |
| **Comm.Control.3** HAN Device shall use the most reliable path to the Energy Services Interface (e.g., based on signal strength/quality). | **Link Status Messages** Wireless links may be asymmetric, that is, they may work well in one direction but not the other. This can cause route replies to fail, since they travel backwards along the links discovered by the route request.<br><br>For many-to-one routing and two-way route discovery, it is a requirement to discover routes that are reliable in both directions. To accomplish this, routers exchange link cost measurements with their neighbors by periodically transmitting link status frames as a one-hop broadcast. The reverse link cost information is then used during route discovery to ensure that discovered routes use high-quality links in both directions. |
| **Comm.Control.4** HAN Device shall only use Utility designated routes | |
| **Comm.Control.5** HAN Device shall have the ability to automatically adapt to communications interference through detection and analysis of environmental conditions (e.g., channel hopping, channel avoidance, signal-to-noise ratio). | **Network Interference Reporting and Resolution** A single device can become the Network Channel Manager. This device acts as the central mechanism for reception of network interference reports and changing the channel of the network if interference is detected. The default address of the network manager is the coordinator. |
| **Comm.Control.6** HAN Device shall include a data integrity mechanism for all communications (e.g., checksum). | **Message Integrity Code** Each Zigbee network frame is accompanied by an integrity code, which is responsible for protecting network information during transit |
| **Comm.Control.7** Energy Services Interface shall have the ability to activate and deactivate its HAN communication. | **Network Manager** The network management function provides support for essential elements of the network (e.g. Network Discovery, Network Formation, Association and Disassociation, Radio Receiver State Enable/Disable) amongst other things. |
| **Comm.Control.8** HAN Device shall communicate its availability (i.e., 'heartbeat') to the Energy Services Interface at least once per day. | **Network List Record** The network list record provides a field, which allows users to specify the beacon order. The beacon order specifies how often the MAC sub-layer beacon is to be transmitted by a given device on the network. |
| **Comm.Control.9** HAN Device shall have a configurable availability communication (i.e., heartbeat) frequency to the Energy Services Interface. | **Network List Record** |
| **Comm.Control.10** Energy | **Cluster Identifier** |

[4] A coordinator does not have to be a parent device, and more than one parent device can exist on the network. However in the design of this system it was seemingly efficient to include just one coordinator as the sole parent device of the network.

[5] There is only one coordinator, which is the parent device, and that is the ESI located in the meter

| | |
|---|---|
| Services Interface shall store a list of available, commissioned HAN Devices in the premise and make that list available to the AMI System upon request. | This is a reference to an enumeration of clusters within a specific application profile or collection of application profiles. The cluster identifier is a 16-bit number unique within the scope of each application profile and identifies a specific cluster. Conventions may be established across application profiles for common definitions of cluster identifiers whereby each application profile defines a set of cluster identifiers identically. Cluster identifiers are designated as inputs or outputs in the simple descriptor for use in creating a binding table.[6] |

We believe that if vendors adhere to, at the least, the OpenHAN SRS document when developing products it will provide customers with the opportunity to be more flexible in their selection of appliances. The Zigbee standard is open as well and meets the criteria outlined in the SRS document, thus simplifying the vendor's task when developing products that must comply with the OpenHAN standards. However there are other standards such as Bluetooth, which with the help of the Bluetooth Special Intrest Group (SIG), has become an open standard and is readily available for download on Bluetooth's website. This would be an ideal candidate for such an application, however Zigbee is the preferred choice because of the network lifetime [33]. The foremost difference between Zigbee and Bluetooth is the ability for Zigbee radios to consume far less power than Bluetooth radios. The obvious result is an increase in the life expectancy of the network. The lifetime of a Zigbee device is approximately 3.1 days, greatly contrasting with that of a Bluetooth device, which lasts for roughly 2.2 hours. The throughput, bandwidth, and spectral efficiency specifications for Bluetooth devices are greater than those of a Zigbee device. These quantities are not particularly relevant in our application, because the devices in the network will not be required to report large quantities of data. The most notable Zigbee attribute is it's exceptional transmission range. It is greater than twice the maximum range of a Bluetooth device making it extremely attractive for home automation applications. This would eliminate the need to include extra nodes in the network, which are not monitoring appliances, but rather serving exclusively as a router.

[6] The ESI would serve as the Cluster Identifier

## IV. Neighborhood Area Network

### A. *Neighborhood Area Network Basics*

In this section we introduce the next component of the demand response system, which is the Neighborhood Area Network. This consists of the meters attached to the houses, along with the access point, which forwards customer data to the utilities local office. Although a standard NAN definition does not exist yet, a few members of the UCAIug have identified components, which they deem necessary for successful communication between the residence and the utility. The network would consist of an AMI meter equipped with an 802.15.4 radio using the Zigbee Pro networking stack along with the Smart Energy(SE) profile. The SE profile defines the standard behavior of secure, easy-to-use, Home Area Network (HAN) devices [24]. The radio is responsible for the appliance-to-meter communication and meter-to-access point communication. Due to the ubiquitous nature of TCP/IP, and the shortage of IPv4 addresses, an IPv6-Zigbee internetworking solution has been proposed. The reason for this is simply because the neighborhood access points will communicate directly with a WAN access point, which is responsible for sending all polled meter data to the utility using a robust backhaul network such as: Ethernet, GSM, CDMA, 3G etc. The meter would be required to interface with two networks requiring two different protocols, which presents a network translation problem. IPv6 over Zigbee [25] is a promising solution.

### B. *NAN Address Translation*

IPv6 over Zigbee works by placing the IPv6 stack on top of the Zigbee network layer. The nodes(meters) are assigned a unique global unicast IPv6 address, the NAN access point should have a Zigbee address, and packet translation in the meter should easily be accomplished without violating the end-to-end model above the network layer. In reality however, the nodes only have a Zigbee address and the access point only has an IPv6 address. If for example the utility were to send a packet to the meter, then the access point would receive a standard IPv6 packet, which would consist of an IPv6 delegation prefix along with an IPv6 host ID—each 64 bits in length. The latter of the two represents the Zigbee address of the polling computer. After receipt of the packet, the access point removes the prefix and then forwards the packet to the designated Zigbee address.

Another possible configuration is 6LowPAN. 6LowPAN adds an adaptation layer to the 802.15.4 stack doing away with the Zigbee standard altogether [26]. The adaptation layer provides the same network translation described above although the application and transport layers are different from those offered in the Zigbee standard. IPv6 over Zigbee simply inserts an IPv6/UDP layer between the Zigbee network layer and the Zigbee application layer. This allows developers who want to comply with the OpenHAN standards the opportunity to do so, without having to reinvent the wheel. The exact opposite procedure is performed when sending information from a node to the access point.

*C. Network Management*

Currently most deployments are using a mesh network to transport data from the endpoints to the access point. During normal operation this might be suitable for extracting data from the network, however during periods of irregular energy consumption and or during an emergency this might not suffice. The nodes closest to the access point will suffer from bottlenecking and as a result the entire system will become backloggedTake for example, a current deployment of AMI meters in FPL's Miami service territory, which include most of the components mentioned above. The meters are equipped with Zigbee Pro along with the Smart Energy (SE) Profile [27]. The network access point has two Network Interface Cards. One is used for WAN media, consisting of an EV-DO modem, and the other for NAN media, which consists of a Silver Springs Network 900MHZ Frequency Hopping Spread Spectrum (FHSS) technology using IPv6 and SNMP. The access point is capable of querying the meter in one of two ways, either asynchronously or by polling. Currently FPL is using the polling method, and the meter data rates peak at about 17-19Kbps, but is capable of a maximum data rate of 100Kbps [28]. The average meter to access point ratio is about 5000:1, which with the given data rate would be suitable under normal conditions, however in more mission critical situations (e.g. broadcasting messages to customers to reduce their demand in order to prevent a potential blackout) this might not be sufficient. This might suggest that additional access points might be necessary, however before considering this, it has been suggested that an asynchronous/exception based polling scheme be utilized [29]. This would allow high priority messages, which are critical for system survival, to reach their destinations in a timely manner. In a situation as such an alternate routing protocol might be necessary in order to relieve some of the pressure, and help with mission critical objectives [15][16].

*D. Security*

Given that the meters will have to communicate with one another, data of the network as a whole must be protected which means that communication between meters will have to be secure. Considering the fact that the utilities will be responsible for providing the customer with a meter equipped with the aforementioned functionalities, key management should not be an issue. The vendor could pre-install the key beforehand so that keys do not have to be exchanged before secure communication can occur. Each meter has a link key and a network key, both of which are 128-bits in length, and they are used for unicast and broadcast communications respectively.

Zigbee provides security services at both the network and application layer. Each of which is responsible for secure transport of data frames from one device to another. The application layer is responsible for the establishment and maintenance of the security relationships amongst devices. The network layer uses the Advanced Encryption Standard (AES) along with the Counter Cipher Block Chaining Message Authentication Code (CCM), which provides authenticity as well as privacy. This is important because HAN device vendors [30] are capable of providing real time information about their neighbor's energy consumption habits, constituting an invasion of privacy. As for the application layer frame security is based on either link keys or networks.

Key establishment is based on a piece of trusted information. Usually this is the master key, which should be installed prior to meter use. Using this key all other keys (i.e. link key and network key) can be created. Zigbee provides a transport key command allowing a sending device to send a: master, link, or network key, obtained from a trusted device within the network, to a receiving device. The trusted device is referred to as the Trust Center in the literature, and the sole purpose of the Trust Center is to provide keys for the network.

Zigbee security hinges on the ability of devices in the network to: secure frames generated at each layer of the stack, exchange keys between a source and destination device, and also to provide end-to-end security without encrypting and decrypting data at each hop. These attributes along with the requirements mentioned above fit together nicely providing a solution for the smart meter networking challenges that utilities are facing now.

Although these components are useful in ensuring security at a very low level, security must be maintained overall so that the network is not compromised. This requirement can be met, by ensuring that the following security principles be upheld. The first is availability of the desired resource. In our case this would be the availability of all components necessary for the communication between a utilities back office network and the meter in their service territory. The second is integrity, which is provided by the integrity code attached to each of the frames leaving the meter. Confidentiality must be maintained and is accomplished by ensuring that only designated entities can access the meter under designated conditions. The fourth principle is access control, which ensures that only designated entities have the ability to establish and execute management mechanisms such as the: establishment, modification, or removal of meters or other criteria. Lastly, all transactions that take place should be accounted for. In a situation where a customer, whether knowingly or not, reduces their demand in response to a pricing signal there are three immediate security concerns—confidentiality, access control, integrity, and availability. The customer's meter obviously has to be available when the utility decides to poll it, but it also must provide a correct reading to the utility—integrity. This implies that the meter should not be capable of reporting false values under any circumstance. This is almost impossible to guarantee because there will inevitably be some human interaction because the customer "owns" the meter—access control. The last security concern is safeguarding against potential eavesdroppers who may attempt to access customer revealing data by sniffing the packets as they leave the residence. This can be accomplished through the use of the security protocols implemented in the Zigbee standard. This is just one of many use cases [34] which have been outlined by SCE and considered to be the basis from which all other utilities might begin to develop their demand response networks. A much more thorough investigation of these use cases is required in order to determine which entities in the system will be responsible for upholding these five core security requirements. As it stands now all of these responsibilities would be delegated to the access point, thus further constraining it's resources. This would defeat the purpose of having the system in the first place.

## V. Wide Area Network

Perhaps the most undefined part of the demand response system is the backhaul portion of the network. This could include any number of technologies from Ethernet to simple mobile phone standards such as GSM or CDMA2000 to carry the information extracted from the NAN to it's final destination—the utilities local office. In the latter case the utility would have to lease the lines from a private company (e.g. AT&T or Verizon), which could be costly. FLP is currently doing this because their access point uses EV-DO technology, which is a part of the CDMA2000 3G standard.

Another possibility is the one in which the NAN access point uses a broadband connection to transport data back to the utility. The type of connection could be one of many: Ethernet, Satellite, Cellular, Broadband over Power Lines (BPL), and possibly WiMAX in the future. In urban areas some technologies, take for instance Ethernet, Cellular, and WiMAX might be slightly more feasible options. However in more rural areas, Satellite and BPL are much more appealing options, because of their ability to reach remote areas.

## VI. Conclusion

In this paper we discussed the three major components of what might become the national standard for a public utilities demand response system. However before this can happen there are several questions, which need to be answered. In particular if the Zigbee protocol, is indeed the best option for the Home Area and Neighborhood Area Networks. If not then what other technologies should be considered. An obvious contender would be 802.11.x, which is used in several different industries, and would be a more than suitable candidate for the public utility space. Especially since most customers will be using a computer, equipped with 802.11.x, as an in-home display of the energy consumption habits. Another possible concern is that customers might be reluctant to have a meter installed which allows their neighbors to monitor their energy usage because of the network's dependency on a mesh network [30]. One might ask why their neighbor's meter should have to communicate with theirs, which is a fair question. A more attractive solution would be one in which relays collect data for a certain subset of houses directly and forward this information to the NAN access point [31]. In addition to this there are standards being developed now, which will be compulsory, for all communications to and from any device connected to the grid [32]. There is a tremendous disconnect between the requirements outlined in the ANSI C12.22 standard and what the Zigbee devices are capable of. Many of the protocols outlined in C12.22 assume that the communicating devices are wired, which would have to be the case when requiring a device to send tables of tables. There are thirteen decades, each of which might have multiple tables of varying size, that store relevant network information. Thus it is plausible to assume that the memory available on the devices, as it stands now, would be insufficient to hold the information let alone transmit it. However, it still remains to be shown whether or not the size of the decade and tables being accessed, require a bandwidth exceeding the amount available on a Zigbee device. Although for now Zigbee seems to be a feasible solution, a more in depth study is required in order to determine whether or not the energy and memory constraints of the device can support the storage and transmission of these tables. Armed with this information we will then be able to confirm whether or not Zigbee will be an ANSI certifiable solution.

## VII. References


[1] Sergel Rick, Executive Remarks Critical Infrastructure Protection, NAURC Summer Meeting, July 20th, 2008

[2] Sergel Rick, Executive Remarks Demand Response & Reliability, NAURC Summer Meeting, July 20th, 2008

[3] Senator Padilla, Senate Bill No. 1438, Legislative Counsel's Digest, February 21st, 2008

[4] Woychick, C, E., "Optimizing Demand Response: A comprehensive DR business case quantifies a full range of concurrent benefits., " *Public Utilities Fortnightly*. 52-57 May 2008

[5] NERC News Feature Focus: Demand Response

[6] Bennett S.C., Cardell J., Wicker B.S., "Residential Demand Response Wireless Sensor Network", Fourth Annual Carnegie Mellon Conference on the Electricity Industry, Future Energy Systems: Efficiency, Security, Control, March 10th, 2008.

[7] SAIC Smart Grid Team, "San Diego Smart Grid Study Final Report", October 2006

[8] Tomic, S., "Network-Growing Scenarios in IEEE 802.15.4 Wireless Sensor Networks"

[9] Lewis, L.F., "Wireless Sensor Networks", *Smart Environments: Technologies, Protocols, and Applications* John Wiley Press, New York, 2004

[10] Adams, J.T. "An introduction to IEEE STD 802.15.4, " *Aerospace Conference 2006 IEEE*. March 2006

[11] Adams, J.T. "An introduction to IEEE STD 802.15.4, " *Aerospace Conference 2006 IEEE*. March 2006

[12] Lipson F. H., Fisher A. D., "Survivability—A New Technical and Business Perspective on Security, " *NSPW 1999*

[13] Nagaraja S., Anderson, R., "The topology of covert conflict," *CITRIS Europe Research Symposium 2007*

[14] Khandani E., Modiano E., Abounadi J., Zheng L., "Reliability and Route Diversity in Wireless Networks." *Conference on Information Sciences and Systems, The Johns Hopkins University* March 16th-18th 2005

[15] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-Resilient, Energy-Efficient Multipath Rounting in Wireless Sensor Networks," *Mobile Computing and Communications Review (MC2R),* 1, 2, 2002

[16] Krishnamachari B., *Networking Wireless Sensors* Cambridge University Press 2005

[17] Kjk

[18] Ye W., Heidemann J., Estrin D., "An Energy-Efficient MAC Protocol for Wireless Sensor Networks," *Infocom 2002. Twenty-First Annual*

*Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*

[19] Ye W., Heidemann J., Estrin D., "An Energy-Efficient MAC Protocol for Wireless Sensor Networks," *Infocom 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*

[20] T. van Dam and K. Langendoen. "An adaptive energy-efficient mac protocol for wireless sensor networks." In *Proceedings of the First ACM Conference on Embedded Networked Sensor Systems*, Nov. 2003.

[21] **http://www.microchip.com**

[22] UtilityAMI 2008 Home Area Network System Requirements Specification

[23] Chipcon Products from Texas Instruments, Z-Stack Developers Guide Document Number: F8W-2006-0022

[24] http://www.eetasia.com/ART_8800525232_499488_NP_2bc24fd0.HTM

[25] Wang C.R, Chang S.R, Chao C.H, "Internetworking Between Zigbee/802.15.4 and IPv6/802.3 Network" *ACM SIGCOMM 2007 Data Communication Festival* August 27th-31st 2007

[26] Montenegro, G., Kushalnagar,N., Hui, J., and Culler, D. *Transmission of IPv6 Packets over IEEE 802.15.4 Networks.* IETF Internet Draft draft-ietf-6lowpan-format-13 (work in progress), April 2007.

[27] **http://www.zigbee.org/en/markets/zigbee_smart_energy.asp**

[28] http://www.silverspringnetworks.com/pdfs/SSN-DS-NIC-kv2c.pdf

[29] UCAIug Face-to-Face meeting

[30] Olsen, Erik "Smart Meter Opens Market for Smart Apps", New York Times

[31] Miller, R.R., "4G Neighborhood Area Networks", IEEE 802 Plenary Tutorials, Atlanta GA. March 14th-18th

[32] American National Standard "Protocol Specification for Interfacing to Data Communication Networks" August 19th 2007

[33] http://www.bluetooth.com/Bluetooth/Technology/Works/Compare/Technical/

[34] http://www.sce.com/PowerandEnvironment/smartconnect/open-innovation/usecasechart.htm