Smart Grid Networks: Promises and Challenges

Abdulrahman Yarali
Murray State University
Email: ayarali@murraystate.edu

Saifur Rahman
Virginia Polytechnic & State University
Email: srahman@vt.edu

Abstract—**Integration of information and communication technologies with the traditional of electric power infrastructures and creation of an interoperable, scalable, and flexible smart grid will require numerous technological innovations and advancements. The purpose of this paper is to take a detailed look at the various technologies which may be utilized in the data transmission for the smart grid and the problems or difficulties that must be overcome to effectively use them. A variety of wireless systems are analyzed and we discuss the security of these mediums as privacy remains a major obstacle for implementing smart grid technology.**

Index Terms—**smart grid, wireless systems, security, information and communication, SCADA.**

I. Introduction

The U.S. electricity generating and distribution infrastructure is undergoing dramatic changes. Historically, the industry has been driven from the production and supplier side where very large base load plants (mainly coal and nuclear) have maintained enough supply to handle the normal requirements with excess capacity available on demand. Recently, interest in renewable energy has greatly increased leading to more wind farms and solar plants. While these comprise only a very small fraction of the total electrical generation capability of the nation, their contribution is expected to grow in the coming decades. However, if these energy solutions are ever to have a major impact, several technological challenges must be met and solved. Among these are efficient, large scale energy storage solutions and the establishment of an extensive, responsive communications network to control the entire power grid.

The buzz phrase for this updated and improved electrical system is "the Smart Grid." The smart grid is intended to more efficiently operate this network of generators and distributors of power with automatic control and operation of the various systems in response to user needs and power availability. The Smart Grid will acquire and process real time data as the power is being used by each and every consumer and this will allow utilities to achieve increase stability of the distribution network, allow variable tariffs in accordance to time of day in order to reduce fluctuation which would allow the overall electrical grid to achieve a more constant load throughout the day, and efficiency by remote maintenance and operation of grid.

The reality is that there is no defined standard or picture of what the smart grid is. It is an emerging technology whose full purposes and requirements will only become clearer as the marketplace drives it. Will wind and solar become a major factor in electricity generation, entailing the grid's need to balance the load to deal with their discontinuous supply? If so, is there money available to build new high voltage lines to transport this production from their sometimes remote locations to the population centers of the nation? Will the public embrace electric cars, further taxing the electricity supply? Will viable energy storage solutions come to fruition? All of these factors will play a role in determining if the smart grid is implemented and what it will look like. As the grid moves forward, several questions have yet to be answered on the communication front. What and how much data is really needed? What will be the required bandwidth needed for communication? Will the industry settle on a particular technology or protocol?

Presently, there are projects in place or ongoing throughout the U.S. to install smart meters on customer premises which take the place of the old electric usage meters which simply recorded the total usage for a given time period (typically one month.) At a minimum, these smart meters will allow the utility to obtain readings automatically through any of several possible communication channels. However, this is simply the first step in the smart grid process. Eventually, these meters are expected to provide constant, real time data back to the utility in order to constantly monitor usage rates, detect problems, and adjust the grid accordingly [1].

This change is itself simply an intermediate step as the true power of a smart grid lies in two way communication between the utility and the customer. Ideally, the customer will be sent information through the smart meter providing items such as power rate pricing which fluctuates based on the time of day and usage rates. The smart meter may communicate directly with appliances such as a washer and dryer, the stove and refrigerator, the heating and air unit, and the charging station for an electric car.

doi:10.4304/jcm.7.6.409-417

Communication in the smart grid can be divided into two primary sections - short range communication such as a home area network (HAN) which connects the varied devices of the home to its smart meter and the longer range transmission necessary to span the distance from the utility to the customer. In fact, a smart grid requires further communication between the interconnected utility generators and suppliers but that is beyond the scope of this paper. Ensuring security in each of these networks (which may each have different media) will be required as all of them must work together for the smart grid to function properly.

Many of the communication and security components are common between these energy subsystems. Supervisory Control And Data Acquisition (SCADA) is the core subsystem of smart grid. A second and a key component to smart grid is a number of secure, highly available wireless networks. These wireless technologies include WiMAX, WLAN, WAN, all generations of cellular technologies and wireless sensor protocols. Comprehensive security solution is a third key component as privacy remains a major obstacle for implementing smart grid technology [2].

This paper is presenting challenges, benefits and how, where, and what type of wireless communication systems are suitable for deployment in the electric power system. Various wireless technologies are discussed and analyzed for implementation. A concise summary of the technical underpinnings of each wireless technology with its strength and weakness is provided.

II. COMMUNICATIONS SECURITY

Placing a smart grid into operation is intended to produce a more reliable and resilient electrical system. However, the introduction of two way communication between the millions of devices on the grid may in fact greatly increase the problems associated with securing it. Therefore, placing the control of this grid onto computers and other smart devices which can affect its reliability means that extreme diligence must be used to protect the integrity of both the data and the infrastructure that collects and transmits it. In fact, it has been reported that cyber spies from Russia and China have already gained access to the U.S. electrical grid and may have even planted software into the system to cause future disruptions [3]. A recent report from the security firm McAfee details a wide ranging network hacking scheme that affected dozens of companies and government agencies around the world [4].

Looking at an individual household that is on the smart grid, there are privacy concerns as well. With theproper resources and ineffective security, a hacker with a malicious intent could even gain control of portions of the grid by compromising the communication system causing a widespread blackout. Since the grid is interconnected, this could in turn lead to power disruptions and control problems through a large region of the country [3]. Although not directly affecting the electrical grid, in November 2011, an attacker was able to gain access to the control system of an Illinois municipal water supplier and remotely disable operating equipment, highlighting the very real danger posed by these types of attacks [5].

In order to achieve comprehensive energy management and utility control, smart meters will also be applied to gas and water meters. This expansion of the smart grid infrastructure brings further complexity to the system. Like any computer network, the smart grid must meet several requirements. High reliability and availability are essential for proper control and operation of the grid so the system must be robust and include levels of redundancy for critical applications. The communication architecture must be able to span the large distances of the grid and effectively handle the large number of nodes (all of the individual smart meters) and the data they produce without excessive delays. The network should also be maintainable – i.e. updates and improvements should be simple to perform and not require physical modifications at each node. Lastly and perhaps most importantly, the network should contain these foundational supports in regards to security management [6]. First is the issue of trust. To work effectively, one must have assurance that the devices on the network are legal, that their messages are valid and that the data has not been manipulated. There must be a means of controlling who can access the network and send messages on it [7]. This is normally managed by some type of key protocol and an authentication mechanism. Privacy is also a paramount concern in order to prevent unauthorized users from being able to capture and read the data on the network [8].

While these security factors are software related, smart grid security must also rely heavily on physical protection. Whereas a typical network's infrastructure is located inside locked communication cabinets or rooms, many of the devices on the smart grid are in accessible locations where anyone can gain access. Smart meters are normally located on the outside of houses and incorporating elaborate security mechanisms for them is either impractical or too expensive. Electrical substations and power lines are located in remote locations in many instances, making oversight and protection problematic. These concerns mean that it is likely that a component of the smart grid will be compromised.5 Having protocols in place to detect and bypass or eliminate these effected components is another essential aspect of smart grid security. NIST released its smart grid security guidelines, NISTIR 7628, in 2010. While this document provides a broad overview of the security concerns and generic instructions on what should be done to protect the system, details have yet to be published [9].

Generally, securing a wired network is easier, as the attacker must force access to the system. With firewalls, proper password protocols, and a strong understanding by the people involved of what vulnerabilities exist, good security can be accomplished. This will be vitality important for the wired portions of the smart grid as well but wireless networks can be more problematic.

As wireless communication becomes more and more widespread, however, this comes with a price as radio waves are free to be intercepted by anyone who chooses to listen. The architecture for most smart grid applications involves at least some element of wireless communication meaning that the data and control information of the electrical grid is exposed to those with the proper equipment and knowledge. The followings are various types of attacks to which a wireless system may be vulnerable [10].

- Passive attacks are those in which the attacker simply listens to the network transmissions.
- Active attacks can take the following forms. Masquerading is when an attacker impersonates a valid user to gain access to the network. A replay attack occurs when an attacker captures valid transmissions (by eavesdropping) and then retransmits the messages to appear as a legitimate user. Message modification or tampering occurs when a valid message is altered in some way.
- A Denial of Service (DoS) attack is intended to completely halt network traffic.
- A Man in the Middle (MITM) attack can occur when an attacker gains access to the network between two valid nodes.

Wireless mesh networks are vulnerable to some special attacks which affect their routing mechanism. A blackhole attack occurs when a malicious node in the mesh claims to have a link to the destination when in fact it does not. The message is then dropped and never retransmitted. A wormhole attack relies on the attacker capturing or installing two malicious nodes into the mesh. Messages that are sent through the wormhole can be analyzed or dropped to cause disruptions. Along similar lines as a DoS attack, a resource depletion attack may target a battery powered node and force it to respond to or send so many messages and requests that its power is depleted [11].

III. ARCHITECTURE AND TECHNOLOGIES

As utilities move from proof-of-concept trials to planning and deployment of the wireless infrastructure in order to enable their smart grid initiatives, they face a wide array of decisions that will determine their long-term success. The smart grid will revolutionize the way they run their business—and perhaps it will change their business entirely. Electric utilities' focus is likely to shift from selling power to managing its production and consumption, with economic incentives to increase power efficiency in generation, distribution and consumption, rather than sales.

How can utilities choose the wireless infrastructure that is best suited to their current and future requirements? How can they pick the technology that will most smoothly evolve along with their smart grid applications?

The first step is to get a solid understanding of their overall requirements—initial ones and long-term ones. This might seem straightforward, but it can easily become challenging, since the requirements are dependent on new operational processes that have not been introduced yet. Utilities are bound to find that smart grid applications will, to some extent, work differently than anticipated, so they need some leeway to accommodate change.

For the smart grid home area network (HAN), various media are available with the ZigBee standard currently dominating this industry segment. Many appliance manufacturers have joined the ZigBee consortium which has given it a solid lead for this market. Bluetooth is another viable technology for this area and the Bluetooth consortium is currently pushing to expand their role in the smart grid [12]. With the preponderance of Wi-Fi networks in many homes, it must also be considered as a potential solution. While not significantly mentioned in the discussion of the smart grid, it would seem that power line communication within the home could also be a logical choice for transferring data between the smart meter and the items within a house. For the problem of communication between the customer and the supplier, wireless mesh networks seemed to have taken the lead in the U.S. at this point in the implementation. However, broadband over power lines (BPL) which is also called power line carrier (PLC) has been utilized for many years for other applications and may play a factor in the smart grid. WiMAX as well as cellular phone service networks have also been employed recently.

This report is analyzing how, where, and what type of wireless communications are suitable for deployment in the electric power system and to inform implementers of their options in wireless technologies. We provide a concise summary of the technical underpinnings of each wireless technology. We also outline the feature set and the strengths and weaknesses of each technology.

A. SCADA

Although not the focus of the paper, the existing computerized infrastructure of the electric grid must not be overlooked in regards to security. The U.S. electrical industry has utilized computer control systems for many years to assist in operating the power grid. Supervisory Control and Data Acquisition (SDADA) systems consist of remote terminal units (RTU) located at power generating stations, and substations, and other grid positions along with centralized operator stations. RTUs collect and transmit instrument readings and process control actions from the operator stations. These systems have been designed for supplier and distributor control and monitoring and not for data collection or control of individual customers. They were also predominantly built from proprietary vendor hardware and software and were not necessarily connected to a network. These facts made system security relatively easy to implement with little danger of attack. However, in recent years, the trend has been to software applications run on "off the shelf" hardware [13]. The author recently assisted with the replacement of a SCADA system for a large industrial facility. Even if an attacker was given access to the original system, it is unlikely that much could have been accomplished given the archaic and antiquated hardware and software. However, the new system is built on PC platforms from a known large supplier running a

Microsoft Windows OS. Obviously the number of potential knowledgeable attackers that could penetrate the system has now risen dramatically. For this location, mitigating these potential attackers meant ensuring that the SCADA system has no connection to any other network. However, for the smart grid to work, this is not an option for most power producers and distributors. Not only must their systems interconnect more than ever, they must now also interface with thousands or even millions of smart meters located throughout their systems – each a possible point of a network breach.

B. *Smart Meters*

According to a recent report by Bell Labs, smart meters are the perhaps the weakest link in smart grid security, but they will undoubtedly be the heart of the system [14]. The current method of recording the electricity usage of most customers in the U.S is through the typical manually read meters that have been used for decades. Approximately twenty years ago, some advances in this technology began to be made with the introduction of automated meter reading (AMR) [15]. In many cases, these devices incorporated short range radio transmitters which could be read by a utility employee driving nearby with a receiver. Some more advanced applications used low bandwidth data transmission over the power lines to send this data back to an aggregation point. As with most projects, cost is normally a major factor and smart meter installations are no exception. With tens of millions of potential installations throughout the U.S., the meters must be inexpensive in order to justify their use. However, this also means that their physical protection is limited. To minimize costs, they don't incorporate anti-tampering devices such as pressure sensors to alert the system that a problem exists or a system breach may have occurred. In addition, due to the priority of maintaining low cost devices, the processing power is comparatively small. This restricts the complexity of the security algorithms that can be used by such devices.

With smart meters sending data to the electricity supplier automatically, there would actually not be a need to have the meter mounted outside the customer premises. Placing the meters inside a garage or other room would provide a much more protected location and aid in the security of the smart grid. This would require moving or extended the power line terminus from their normal location to the interior which would add considerable expense and most likely be prohibitive for any extensive smart grid projects. However, for any new homes built in areas with existing smart meters infrastructure, this may be a useful option.

At the present time, there is no standard solution for communication between the smart meters and the electrical supplier's networks. Figure 1 shows a group of smart homes connected to the grid. Data could be sent wirelessly to an access point at the local power pole or via communication over the low voltage power lines. Large amounts of smart meter data could be collected at a substation and then sent back to the utility. The backhaul connection to the utility might be via a common carrier or a utility owned network. Much depends on the density of meters in a particular area and the distance of those meters from data collection points. No one technology may fit every situation. The design of the smart grid for rural areas may look very different from those in an urban setting. As mentioned previously, the final design and capabilities of the smart grid has not been determined either. For instance, if the smart meters are simply to provide real time usage data every 15 minutes, a relatively slow bandwidth network may be sufficient. If it is expected that the meters will themselves be data collection points for all of a household's appliances and will report this information several times per minute, the transmission of this information may require a very high speed network. The remainder of this paper will closely examine the possible mediums for both the in house network and the meter to supplier side.

C. *ZigBee*

IEEE 802.15.4 defines standards for the MAC and PHY layers for personal area networks. ZigBee is the trade name for a set of applications that run on these standards as defined by the ZigBee alliance. It is a low power, wireless mesh network that is designed to be used in a wide range of applications, including smart home control systems. Although the devices have a short range (10-100m, less in practice), the mesh design means networks can cover fairly large areas. Many smart meters have ZigBee chip sets in order to communicate with smart devices in the home.

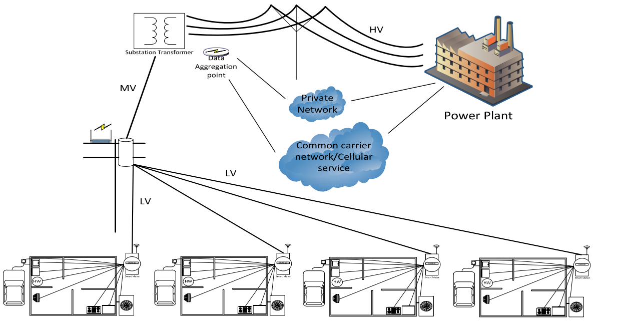

Figure 1: Overall grid diagram

For security, ZigBee relies on 128 bit AES encryption (discussed earlier.) It also includes a 32 bit message integrity code (MIC) and frame counter to address replay concerns. Security is applied by default at the network layer but higher level security is optional and not required.

With its low cost, low power usage, mesh networking, and strong vendor support, ZigBee has many attractive characteristics for a smart home network that can easily attach to a smart meter for total integration. However, its security issues may be a cause of concern. As its importance and use increases, more and more hackers will be drawn to attacking it which may expose even more problems. To use ZigBee for complete power control from the utility, the smart meter will need to share keys with the various appliances of the homeowner. However, due to security concerns, it remains to be seen if the utility would be willing to share these keys, possibly making system integration difficult [16].

D. Bluetooth

Similar to ZigBee, Bluetooth is the trade name for a wireless personal area network (WPAN). Although this technology holds a commanding position in the cell phone accessory industry, it has not made a large impact in the HAN/smart home market. However, the industry consortium behind the technology is promoting itself for smart grid applications. Unlike ZigBee, Bluetooth is not a mesh network but it is able to transmit at greater speeds (~1 Mbps) while using only slightly more power with an advertised range up to 100 m.

For one aspect of security, Bluetooth utilizes frequency hopping during communication but there are devices available on the market which can match the changes and therefore eavesdrop on any transmissions. One of Bluetooth's features is the ease of "pairing" two devices so that they can communicate. This can be accomplished by placing the device in a discoverable mode. However, if let in such a state, the device may be open to attack. Another possible avenue of attack is the fact that Bluetooth addresses are not encrypted during transmission, even when in asecure mode that encrypts the rest of the message. With a known address, the attacker can initiate communication with a device and potentially upload viruses or other malicious software.[25]

Like other wireless technologies, Bluetooth also uses the 2.4 GHz spectrum so interference is possible with Wi-Fi and ZigBee. Without a mesh network, Bluetooth is more limited than ZigBee in the total area it can cover. It is also at a disadvantage since most smart meters are already designed and shipped with embedded ZigBee chips. However, it does have one advantage in that most computers and smart phones can communicate via Bluetooth which would make integrating the controls for the smart home with devices we already use very simple.

E. Ethernet over Power

Power line networking or power line carrier (PLC) is a potentially attractive means of connecting the smart meter to the electrical devices in the home. The latest versions of this technology use orthogonal frequency division multiplexing (OFDM) and claim speeds of up to 200 Mbps. Although practical results are probably far lower in most instances, it would still be more than adequate for smart home communication.

To incorporate this technology in the smart grid, the smart meter would need PLC technology built in from the suppliers so that the signals could be injected into the home wiring from the source. Ideally, the smart appliances to be controlled in the home would also have embedded PLC devices but they could also simply connect via an adaptor as described above. In this application, the smart meter would act as the server (if necessary) and poll and/or send control messages to the attached devices?

Having a possibly more secure system is one of the benefits of using this technology. There would be no wireless transmissions like ZigBee, Bluetooth, or Wi-Fi which could be heard by an eavesdropper. However, this does not mean that there are no potential security vulnerabilities. Like all of the systems described, the smart meter itself is still vulnerable and could be attacked and compromised. Also, the typical residential power distribution system supplies several houses from one low voltage transformer. Since these locations are all tied together, any signals injected onto the lines from one house can be sensed at other houses as well. PLC device manufacturers recognize this and incorporate message encryption schemes into their products. Like wireless systems, any signals which are available can be probed by hackers for weaknesses and potentially exploited. The danger is significantly reduced with PLC as the actual power lines would have to be tapped so war-driving would not be possible. In addition, if this technology were to be used, a low pass filter could be installed in the smart meter to prevent these signals from going beyond the home.

Several variations of PLC are in existence and can be dependent upon what portion of the transmission grid is being utilized. As shown in figure 1, through equipment at the generating station, high voltage level (generally 161 kV – 345 kV) electricity is supplied to the grid and carried to substations located closer to the customers. Step down transformers at these substations drop the high voltage down to a medium voltage level (e.g. 14kV). From there it is sent through the local grid to various areas near the customers. Small transformers further reduce the level to the standard 120/240 V level for household use and reach the customer through the individual electric meters. Each of these transformers can act as a low pass filter which effectively blocks high frequency transmissions from passing through. In addition, dependent upon the frequency used, transmissions over power lines suffer from high signal attenuation. Therefore for many applications, repeaters may be required to transmit through the entire grid.

One potential problem with PLC relates to the irradiated signal from the placement of the carrier signal on the transmission lines. Some of the frequencies used overlap with those used by short wave radio operators and other systems and there is a concern that widespread use of PLC could be harmful to that media. In areas where it is currently being used, however, no mention has been found of problems being reported. No mention has been found of any security concerns in regard to these irradiated signals being picked up by eavesdroppers either. Due to the lethal voltages present on the transmission lines, there is built in security protection which the other mediums do not have. It is highly unlikely that an attacker would attempt to tap into this network.

F. Wi-Fi

Wi-Fi is an extremely popular wireless protocol that is found in many homes already for home area networks and Internet access. The latest version, IEEE 802.11n, boasts speeds of up to 300Mbps. While the outdoor range of Wi-Fi can exceed 300 feet, 100 feet or less is more typical of indoor applications. While this does give at a significant advantage over other technologies, this comes with a price as its power consumption is much higher than ZigBee and Bluetooth. Studies have shown that Wi-Fi would consume more than two times as much power as ZigBee in a standard smart home environment [17]. As the most popular wireless standard, Wi-Fi has garnered considerable interest from hackers and researchers which has revealed several security holes and concerns. However, this has led to improvements in its security protocols, possibly making it more secure than competing technologies now. Refer to the earlier section of this paper for a detailed look at Wi-Fi security.

For Wi-Fi to be used as the smart home communication medium, other concerns would need to be addressed, beyond security and power usage. Obviously, appliance manufacturers would need to add Wi-Fi capability to their products. If this is done, would the utility use the customer's personal Wi-Fi network (HAN) for the communication between these products and the smart meter? Or, as is more likely, would the utility install a separate network, with the smart meter as the access point? This could lead to interference concerns, especially in densely populated areas.

Furthering this problem is the use of Wi-Fi based wireless mesh networks for the communication between the smart meter and the utility itself. This method and competing technologies for this application will be investigated next.

G. Wireless Mesh Network

Wireless mesh networks are an easily deployable, inexpensive means of providing wireless network coverage over a large area. They are an accumulation of mutually supportive wireless access points (AP) which are arranged in such a manner to allow multiple paths back to some physical location which is normally a wired network or wireless hot spot. Since most mobile devices can communicate via Wi-Fi, mesh networks are normally based on 802.11 protocols with the addition of some means of routing control [18]. In relation to the smart grid, the smart meters could be the APs of the network with an aggregation node located at a local substation which is connected back to the utility through some other media. A mesh network could also be created by installing APs at various locations throughout a city or neighborhood with the smart meters being the clients. Data from the customers would be transmitted from the smart meters through the mesh network to some aggregation point where it would then make its way back to the utility. Some substations are already connected via copper wiring or fiber optic so additional networking infrastructure may not be required. Control commands and information from the utility would flow in the opposite direction. A mesh would provide an inexpensive, yet high speed network for the utility and could be implemented quickly.

Along with the normal security concerns of wireless transmission, the mesh network opens up a number of other worries in regards to the routing protocols that take the information back to the base station or aggregator. A mesh network for smart grid purposes will not be ad hoc, but rather a fixed network where all nodes are known. With fixed nodes, it is then assumed that all the nodes are friendly and there is an expected trust between nodes. Therefore, if an attacker gains access to an AP or smart meter, they may be able to severely disrupt network traffic. In order to maintain low costs for the mesh devices, physical protection is minimal so this is a very real threat. There are three crucial security goals in this regard: having some means of detecting a compromised node, securing the routing mechanism, and ensuring all nodes have equal access to the network [19]. Several articles that are available discuss means for detecting malicious nodes but intrusion detection is an area that must be further studied and improved. Secure routing mechanisms are also available and if used properly should aid in preventing attacks on this protocol. However, even with secure key exchange mechanisms, by physically attacking a node one may be able to gain this key data and impersonate a valid node. Since each node pair should have their own keys, this should not allow an attacker to successfully eavesdrop on other nodes. However, even if no data is compromised, the loss of any functionality to the smart grid with its expected constant data flow may cause reliability issues to the electrical system.

While mesh networks provide extreme flexibility, there very make-up also makes them vulnerable to attackers. In order to safely and effectively use this type of design for the aggregation of smart grid data, further improvements in physical protection and routing protocols may be required. Other technologies may not have the ease of deployment that a wireless mesh enjoys, but security concerns may override this benefit [20].

H. WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) is the trade name for a broadband wireless access medium defined under IEEE 802.16. Initially the standards were limited to fixed, line-of-sight transmission but have since also incorporated standards for mobile, non-line-of-sight access. While the range for WiMAX transmission can be up to 30 miles, three to five miles is more typical in practice. This does provide significantly greater range than Wi-Fi, making it a more useful medium for this application. In addition WiMAX uses the 2.5 GHz spectrum making it less prone to interference from other sources and wireless devices. The latest standards allow for data rates up to 1 Gbps although this bandwidth must be divided between the users. WiMAX service is provided by a base station which then allows connections by subscriber stations which would be the smart meters in our application. This is essentially the same as cellular phone service and WiMAX is one of the technologies being used for 4G implementations by the cellular providers [21].

For security, WiMAX utilizes the strong AES encryption method and also includes key management and authentication. The first version of its key management protocol was subject to attacks but this has since been strengthened. It is assumed that any new devices for the smart grid would include the latest protection. Like any wireless medium, WiMAX is susceptible to DoS attacks by jamming and scrambling attacks where the jammer only transmits during certain periods to disrupt control information. Other attacks have been proposed involving a weakness in the initial network entry and key exchange [22]. By eavesdropping at the proper time, one could gain enough information to implement a MITM attack, therebycompromising the security of all traffic routed through the node. One may also be able to gain enough access to the system to transmit various control messages which could effectively overload the system. However, since the devices tied to the smart grid are not mobile and constantly changing WiMAX base stations (and therefore exchanging keys and performing authentication routinely), there should be little opportunity to exploit these vulnerabilities in this application.

One question to be answered for a WiMAX implementation is who would own the network. Should a utility install its own private system or rent from a cellular provider? It is expected that a utility would want total control of any network tied to the smart grid but it may be much less expensive to lease network capacity. However, it would have to be determined if the required QoS could be maintained.

I. *Technology Implementation*

The desire to reduce electricity consumption, add renewable energy sources to the mix of supply options, and better control the entire electrical system, a new smart grid is being proposed and implemented. The development of smart grid is essential for achieving energy security, economic development and climate change mitigation. It is important to note that there is no single deployment that will define the communications architecture of the electric power systems. The electric power system will require communications with great flexibility and complexity. Common challenges associated with wireless communications are probabilistic channel behavior, interference and jamming, and eavesdropping and interception [23].

One of the challenges in deploying data communication networks is the number of variations in configuration and connectivity that are implemented. The following table shows examples of scenarios to wireless technology implementation.

For obtaining data communications coverage quickly and inexpensively over a large geographic area, both WiMAX and 3G/4G cellular technologies should be considered. WiMAX at the present holds a bandwidth and latency advantage over 3G cellular communications; however, with the imminent LTE deployment from multiple carriers, we believe this advantage will be short-lived. Unlike WiMAX deployments, LTE will mostly reuse existing cellular networks and should be a straightforward evolution of the 3G cellular networks. Both of these technologies operate over licensed spectrum and therefore should be protected against unintended interference. In terms of scalability, we know that the cellular networks are capable of accommodating hundreds of millions of subscribers while providing both voice and data communications. WiMAX networks have been deployed to provide wireless local loop service successfully. However, presently, WiMAX networks only support a small fraction of users compared to 3G cellular networks. Whether using WiMAX or 3G/4G cellular, we recommend a combination of application-level security and virtual private networking (VPN) for transporting electric power system information over these public networks. Smart grids can provide significant benefits to developing countries. Capacity building, targeted analysis and roadmaps – created collaboratively with developed and developing countries – are required to determine specific needs and solutions in technology and regulation.

TABLE 1. Wireless Technology Suitability (Example Scenarios to Wireless Technology Mapping) [23]

	Wi MAX	WI FI	IEEE 802.15.4			HSP A/E DVO	LTE/H SPA+ UMTS
			Wireless HART	ISA100 .11a	Zig bee		
Feeder Reconfiguration	S[1]	N [2,4]	NS [2]	NS[2]	NS [2,3]	S[1]	S[1]
Within a Customer Premise	NS [5]	S	S	S	S	NS [5]	NS[5]
Customer Premise to Ctrl Ctr	S[1]	NS[2]	NS[2]	NS [2]	NS [2]	S[1]	S [1]
Within a Bulk Generation Plant	NS [5]	Surveillance and Sensor Aggregation	Sensor Netwks	Sensor Netwks	NS [3]	NS [5]	NS[5]
Transmission System to Ctrl Ctr	S[1]	NS[2,4]	NS[2]	NS[2]	NS [2,3]	S[1]	S[1]
Bulk Plant to Ctrl Ctr	S[1]	NS[2,4]	NS[2]	NS[2]	NS [2,3]	S[1]	S[1]

S= Suitable NS= Not Suitable

i. Wide Area Networks may be overwhelmed by excessive demand created by an emergency, natural disaster, or large public gathering (e.g., Presidential Inauguration).
ii. Technology does not possess necessary geographic coverage area.
iii. Technology does not offer sufficient security.
iv. Unlicensed Spectrum susceptible to significant interference.
v. Wide-area technology not suitable for use within a confined area.

IV. CONCLUSION

The desire to reduce electricity consumption, add renewable energy sources to the mix of supply options, and better control the entire electrical system, a new smart grid is being proposed and implemented. At the present, there is no one solution to the problem or one network which the industry has settled on. Wireless options are easy to implement and enjoy wide support but present security concerns that could be compromised to disable and damage the infrastructure of the system.

Installing wired systemswould add excessive costs and power line communication has obstacles to overcome before it can be used in a fully implemented smart grid capacity. Based on the current situation, it is believed smart home networks will continue to be installed for household use but it is unlikely that any serious attempt to completely automate them with the grid occurs in coming years. Most likely we will see a movement toward the system design used by Florida Power and Light which can read meters a few times per hour and provide control messages to quickly drop load if necessary. In such a system, PLC may become the method of choice and would aid in minimizing the security issues of using wireless technology. Separating the hype from the reality of the smart grid is difficult. Even with government intervention and funding, the ultimate design will be driven by the marketplace. Over the coming years, it is predicted that an old technology (PLC) finds more use than the latest wireless infrastructure even with its high speed and ease of use.

Acknowledgment

The authors wish to thank Mr. Craig Wisner for his contribution to this work.

References

[1] INL Critical Infrastructure Protection/Resilience Center, "Study of Security Attributes of Smart Grid Systems – Current Cyber Security Issues," Department of Energy, 2009.

[2] Anthony R. Metke, Randy L. Ekl, "Security Technology for Smart Grid Networks," IEEE Transaction on Smart Grid, Vol. 1, No. 1, June 2010

[3] Clemente, Judy, "The Security Vulnerabilities of the Smart Grid," Journal of Energy Security, June, 2009.

[4] Alperovitch, Dmitri, "Revealed: Operation Shady RAT," McAfee White Paper, accessed via Internet from http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf, November 22, 2011.

[5] Finkle, Jim, "U.S. probes cyber-attack on water system in central Illinois," Reuters, accessed via Internet from http://www.msnbc.msn.com/id/45359594/ns/technology_and_science-security/t/us-investigates-cyber-attack-illinois-water-system/#.TtlFrlYlpI4, November 25, 2011.

[6] Perrig, Adrian et al, "Security in Wireless Sensor Networks," Communications of the ACM, Jun2004, Vol. 47 Issue 6, p53-57.

[7] Khurana, Himanshu, "Smart-Grid Security Issues," IEEE Security & Privacy, Volume 8 Issue 1, 2010, pp. 81-85.

[8] Sauter, Thilo, "End-to-End Communication Architecture for Smart Grids," IEEE Transactions on Industrial Electronics, Volume 58 Issue 4, 2011, pp. 1218-1228.

[9] Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid, NISTIR 7628, August 2010, accessed via Internet from http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf, November 16, 2011.

[10] Souppaya, Murugiah et al, "Guidelines for Securing Wireless Local Area Networks (WLANs) (Draft)," NIST Special Publication 800-153.

[11] Yi, Ping et al, "A Survey on Security in Wireless Mesh Networks," IETE Technical Review, Volume: 27, Issue 1, 2010, pp. 6-14.

[12] Merritt, Rick, "Bluetooth group explores apps in smart grid," www.eetimes.com, 2/24/2010, accessed via Internet from http://www.eetimes.com/electronics-news/4087913/Bluetooth-group-explores-apps-in-smart-grid, November 14, 2011.

[13] Ericsson, Goran N., "Cyber Security and Power System Communication-Essential Parts of a Smart Grid Infrastructure," IEEE Transactions on Power Delivery, Volume 25 Issue 3, 2010, pp. 1501-1507.

[14] Budka, Kenneth C. et al, "Communication Network Architecture and Design Principles for Smart Grids," Bell Labs Technical Journal, Volume: 15 Issue: 2, 2010, pp. 205-227.

[15] Galli, Stefano, "For the Grid and Through the Grid: The Role of Power Line Communications in the Smart Grid," Proceedings of the IEEE, Volume 99 Issue 6, 2011, pp. 998-1027.

[16] Bialoglowy, Marek, "Bluetooth Security Review, Part 1," accessed via Internet from http://www.symantec.com/connect/articles/bluetooth-security-review-part-1, November 12, 2011.

[17] Electric Light & Power, "GE study: ZigBee is better than WiFi for smart grid home communications,"December 9, 2010, PennWell Corp., accessed via Internet from http://www.elp.com/index/display/article-display/1328413615/articles/electric-light-power/smartgrid/2010/12/GE_study__ZigBee_is_better_than_WiFi_for_smart_grid_home_communications_.html, November 14, 2011.

[18] A. Gerkis, "A Survey of Wireless Mesh Networking Security Technology and Threats," SANS Institute, 2006, accessed via Internet from http://www.sans.org/reading_room/whitepapers/honors/survey-wireless-mesh-networking-security-technology-threats_1657, November 4, 2011.

[19] Salem, Naouel Ben et al, "Securing Wireless Mesh Networks," Laboratory of Computer Communications and Applications, École Polytechnique Dédérale de Lausanne.

[20] Yarali, A. & Ahsant B., Rahman S. , "Wireless Mesh Networking: A Key Solution for Emergency & Rural Applications," MESH2009, June 18-23, 2009 - Athens Greece.

[21] Yarali, A., Rahman S. & Bwanga M.," WiMAX: The Innovative Wireless Access Technology," Journal of Communication (JCM), Academy Publisher, 3, (2), 53-63, 2008 .

[22] Nguyen, Trung, "A survey of WiMAX security threats,"Computer Science Department, Washington University, 2009.

[23] Ba, Akyol, H Kirkman et al, "A Survey of Wireless communications for the Electric Power System," Pacific Northwest national Laboratory, U.S. Department of Energy, January 2010.

A. Yarali (S'92, M'96-IEEE) is a faculty member of Telecommunication Systems Management and Industrial Engineering Technology at Murray State University where he has developed a wireless option program. He has worked as a technical advisor in wireless industry since 1995. Dr. Yarali is currently conducting research program in wireless mobile communication systems at Murray State University.

Saifur Rahman (S’75, M’78, SM’83, F’98 – IEEE) is the director of the Advanced Research Institute at Virginia Tech where he is the Joseph Loring Professor of electrical and computer engineering. He also directs the Center for Energy and the Global Environment at the University. Professor Rahman has served as a program director in engineering at the US National Science Foundation between 1996 and 1999. He has served on the IEEE Power Engineering Society Governing Board as VP of industry relations, and VP of publications between 1999 and 2003. In 2006 he served as the vice president of the IEEE Publications Board, and a member of the IEEE

Board of Governors. He is also a member-at-large of the IEEEUSA Energy Policy Committee. He has published over 300 papers on conventional and renewable energy systems, load forecasting, uncertainty evaluation and infrastructure planning.