Secure data networks for electrical distribution applications

David M. LAVERTY (✉), John B. O'RAW,
Kang LI, D. John MORROW

Abstract Smart Grids are characterized by the application of information communication technology (ICT) to solve electrical energy challenges. Electric power networks span large geographical areas, thus a necessary component of many Smart Grid applications is a wide area network (WAN). For the Smart Grid to be successful, utilities must be confident that the communications infrastructure is secure. This paper describes how a WAN can be deployed using WiMAX radio technology to provide high bandwidth communications to areas not commonly served by utility communications, such as generators embedded in the distribution network. A planning exercise is described, using Northern Ireland as a case study. The suitability of the technology for real-time applications is assessed using experimentally obtained latency data.

Keywords Telecoms, Latency, WiMAX, Security

1 Introduction

Security of telecommunications is an important concern in the development of Smart Grid applications, especially those involved with real-time protection and control of grid infrastructure. Since the electrical grid spans a large geographical area, it is necessary to use a wide area network (WAN) for communication. Typically, the applications use packet switched protocols, usually internet protocol (IP). In the last number of years, there have been several high profile cyber security attacks on notable large corporations, and significant vulnerabilities have been found in software technologies which underpin Internet communications [1–3]. The security technologies developed for use in enterprises (banks, businesses) may not be sufficient for security of industrial control systems. Although it is desirable to avoid connection with public networks, for some applications this may prove unavoidable. The authors propose the use of WiMAX radio technology as an affordable solution for an electrical utility to create an independent WAN, isolated from public Internet infrastructure. This would have application where secure, high bandwidth communication is required to enable real-time applications. Many such applications are proposed in [4], including control of distribution applications such as embedded generation and electric vehicles [5, 6].

This paper presents a technical summary of WiMAX, with range and throughput calculations being developed. Based on these figures, a radio planning study is conducted using professional software to ITU standards. Northern Ireland is used as a case study in this exercise, considering connectivity at wind farm generation sites. The technical suitability of WiMAX for real-time power systems applications is considered in light of experimentally obtained performance data. It is shown that throughput is greatly in excess of the requirement for synchrophasor streaming [7], while the latency easily meets the relevant IEEE standard [8].

The authors recommend that WiMAX is an available solution that may be rapidly deployed to service remote areas of the utility with data telecoms. WiMAX is of low cost, meets immediate needs, and as the utility transitions to fiber for telecoms WiMAX will continue to provide telecoms diversity. WiMAX technology offers a cost effective solution which meets the needs of current Smart Grid applications.

Crosscheck date: 10 March 2014

Received: 30 September 2014 / Accepted: 1 April 2015 / Published online: 15 May 2015

D. M. LAVERTY, J. B. O'RAW, K. LI, D. J. MORROW,
School of EEECS, Queen's University Belfast, 125 Stransmillis Road, Belfast BT9 5AH, UK
(✉) e-mail: david.laverty@qub.ac.uk

2 Telecoms network modernisation in electric utilities

Electrical utilities operate many essential telemetry and telecontrol functions over telecoms delivery technologies with many decades of track record in terms of reliability. Modern applications, such as phasor measurement units [4, 9], and optimizing control of embedded generation [5, 6, 10], are demanding bandwidths beyond what established telecoms delivery technologies were designed for [4, 11]. The defacto solution for high bandwidth telecoms needs is to install a data network, typically operating on IP. This can be achieved in a number of ways, including extending the company enterprise network, or provisioning an internet service at the remote substation through a local provider.

Understandably, there is reluctance amongst utility personnel to abandon proven systems for new telecoms solutions, especially those operating IP. Recent press coverage highlights intentional sabotage of high profile networks by 'hacktivist' groups [12], the 'Stuxnet' worm tailored to attack industrial control systems [1], the 'Heartbleed' vulnerability in OpenSSL [2], and the 'Shellshock' vulnerability in Bash [3]. All of these scenarios give rational cause for alarm.

A solution to provide high bandwidth telecoms to remote endpoints that does not traverse public internet would go some way to alleviating many of the intrinsic security concerns.

2.1 Traditional utility substation telecoms

The traditional substation has long operated on the principle of fixed wiring between instrumentation, relays and intelligent electronic devices (IEDs) alongside growing use of low speed serial links [13, 14]. Early substation-to-substation communication, supervisor control and data acquisition (SCADA), was achieved through use of private or leased telephone lines, microwave, UHF radio or power-line-carrier (PLC) carrying either analogue signals or delivering low data-rates by modem (<56 kbps). In Northern Ireland, UHF scanning telemetry operates at 9600 baud.

Subsequently, utilities began to install fiber-optic cables between substations, operating E1 and/or synchronous digital hierarchy (SDH) multiplexers. E1 and SDH technologies are based on circuit-switched time division multiplexing (TDM), and are connection orientated. A dedicated circuit is created and used for a specific purpose and available to the application at all times. Bandwidth is constant and traffic transmitted at the speed allowed by the physical media, therefore the latency is very low. Available is of the order of 99.999% [13]. E1 circuits operate at 2.048 Mbps in Europe, or the nearest equivalent T1 at 1.544 Mbps in USA. A standard application circuit, E0, is 64 kbps. This allows 32 circuits on an E1 carrier in Europe, or 24 in USA. Given their excellent latency and constant bandwidth, utility telecoms engineers highly regard the performance of TDM communications.

Whilst highly suitable for many serial telecoms applications including protecting signaling, 64 kbps TDM circuits are inadequate in terms of bandwidth for many smart grid applications. While circuits may be multiplexed for additional speed, this adds complexity and is not a long term solution to growing bandwidth needs.

2.2 Transition to packet switched networks

Current practices by IED manufactures are pushing the utility telecoms towards standardization on common communications architecture. Protocols such as DNP3 [15], IEC 61850 [16] and IEEE C37.118.2 [7] have Ethernet as the underlying technology, leading to a growth in use of Ethernet/IP for data transport within and between substations [17].

Ethernet is a packet-switched technology. Messages are separated into segments and transmitted individually across dynamically created connections, which results in a more efficient use of network bandwidth [18]. Ethernet networks are less costly [17] and provide better scalability than TDM networks. The downside is that latency is non-deterministic in the packet network, such that data may arrive early, late or fail to arrive at all. Protocols such as TCP/IP build upon IP to provide correct sequencing of data and guarantee of delivery. Protocols and products exist which attempt to emulate E0/E1 connections over IP networks [14].

As it enters into legacy support and availability, the cost of TDM technology is prohibitive to development of a telecoms network suitable for smart grid. Indeed, given the diversity of applications, it is apparent that no single delivery technology can yield a comprehensive solution to meet all utility telecom needs. However, the use of standardized protocols and addressing schemes will allow messages to traverse many types of media. The authors consider the trend towards a fully IP smart grid is rational in terms of cost and bandwidth, and will show that such networks demonstrate adequate latency, security and reliability. "There is no doubt that Ethernet/IP-based networks are the emerging trend in modern substation communications [17]."

3 WiMAX technology overview

Following the success and almost universal adoption of Wi-Fi (802.11 a/b/g/n) on the local area network (LAN), it became clear to equipment vendors and standards groups that demand existed for similarly flexible and utilitarian standards over greater distances.

The IEEE standards board established the IEEE 802.16 working group in August 1998 to develop standards appropriate to fixed wireless access (FWA) broadband. The first standard (802.16-2001) was released in April 2002, dealing with point-to-multipoint line-of-sight propagation in the 10–66 GHz band using single carrier modulation.

To facilitate non line-of-sight, propagation 802.16a was ratified in 2003. This amendment allowed for operation at lower frequencies, 2–11 GHz, and the physical standard was extended to use orthogonal frequency division multiplex (OFDM) modulation, allowing increased throughput for the same radio bandwidth. IEEE 802.16d [19] was released in 2004, harmonizing some aspects of the 802.16 standard with the European HIPERMAN [20] and consolidating previous revisions. For the current generation of licensed "last-mile" broadband installations, this is the defacto standard. Alongside the standardized developments in WiMAX, a range of proprietary FWA solutions have emerged, many using adaptations of the original 802.11a protocols. Subsequently IEEE 802.16e-2005, referred to as "mobile WiMAX", was developed. However, in the mobile communications sector, mobile WiMAX has been largely sidelined by greater operator adoption of long-term-evolution (LTE). In this work, the fixed version of WiMAX, IEEE 802.16d, and proprietary FWA solutions are used.

Comparison between WiMAX and Wi-Fi requires caution since the two technologies have different applications. Wi-Fi offers insufficient range for wide area networks such as required in utility applications. Table 1 lists the key differences, note that Wi-Fi is intended for short range/indoor applications and WiMAX, in its fixed form, is primarily for long range infrastructure applications, i.e. WAN. The quoted maximum speed of typical Wi-Fi and WiMAX products [21, 22] are included in Table 1 for reference but, as will be developed later in this paper, the actual throughput is subject to a complex range of interrelated factors. The quoted typical speeds are based on practical experience and offer a more realistic comparison, but regard that the distance covered by WiMAX is two orders of magnitude greater than for Wi-Fi.

Table 1 WiMAX and Wi-Fi comparison

	Wi-Fi (802.11n)	WiMAX (802.16d)
Range	300 m	30 km
Speed (max)	54–300 Mbps	300 Mbps
Speed (observed)	50 Mbps (at 10 m)	30 Mbps (at 15 km)
Quality-of-service	Poor	Good
Frequency	2.4, 5 GHz	900 MHz to 66 GHz
Spectrum	Unlicensed	Licensed/Unlicensed

The quality-of-service (QoS) mechanisms of WiMAX and Wi-Fi are different. WiMAX provides quality of service through a connection orientated scheme operated at the base station. This delivers packets to subscriber units based on priority, and similarly schedules subscriber units to transmit based on the priority of their data. Wi-Fi uses contention based quality of service, where subscribers try to access the access point based on random time intervals. This is a poor mechanism for time sensitive data.

Wi-Fi operates in the license exempt industry, science and medical (ISM) bands at 2.4 GHz and 5 GHz. WiMAX can also operate in these bands, or a license may be applied for and the network operated in a licensed part of the spectrum. This is useful for utilities as there is no mechanism for recourse for interference in a license exempt band. Wi-Fi operates acceptably indoors at short ranges, while WiMAX usually requires line-of-sight when used over long distances.

4 WiMAX network topology

The network topology used to service wind farms with high speed data connectivity is that of fixed base stations serving numerous fixed subscriber units. Before radio planning can commence, it is necessary to calculate the distance subscriber units can be from their base station so that base stations can be appropriately placed.

The link between the base station and the subscriber unit, in this work, is considered to be the 'last-mile'. The radio frequency band used is 5.8 GHz, a license exempt/light licensed band. In other applications, it may be more appropriate to operate under license in the 3.5 GHz band, but the same methodology will apply. Although microwave links can be established without line-of-sight, experience suggests that at 5.8 GHz adequate performance in range and throughput can only be achieved with line-of-sight to the base station.

The data throughput possible on a radio link is determined by the link budget, a complex mix of interacting factors typically modeled by standards such as ITU-R P.530 [23]. However, in rural areas with predicable and well understood topology and with clear line of sight links (LOS) only, the service area from any base site can be related to the received signal level (RSL) at the receiver. For this exercise, factors such as clutter, noise floor and urban topology are ignored or included in the fade margin. For any given RSL, there are three main parameters which determine the throughput; namely the modulation, coding (e.g. QPSK/16-QAM/64-QAM) and spatial streams. Modern equipment dynamically adjusts these parameters to achieve the maximum throughput given the actual RSL. With the test equipment used, the minimum data rate, when modulation and coding are adjusted for poor RSL, is 6.5 Mbps. Adjusted for excellent RSL, the equipment can theoretically achieve 300 Mbps of throughput. Experience suggests that actual throughput will be of the order of 60% of what the modulation and coding scheme rating allows. In this work, the RSL is engineered so as to achieve an actual throughput of 30 Mbps, indicating a theoretical throughput of 50 Mbps is required.

A full derivation of how RSL is determined is beyond the scope of this article. Briefly, the limiting factor is the equivalent isotropically radiated power (EIRP). The maximum allowable EIRP in the UK is 36 dBm (4 W). EIRP is a function of the output power of the transmitter (P_t) and the gain of the transmit antenna (G_t). When higher gain antennas are used, the transmitter must limit its power so as not to exceed the legal EIRP. That is, $(P_t + G_t) = 36$ dBm.

The RSL can be determined using the logarithmic version of the Friis equation [24], where P_r is the power at the receiver (RSL), Pt the power output at the transmitter, G_t and G_r are the transmitter and receiver antenna gains, λ is the wavelength of the signal, and d is the distance between the transmitter and receiver. Rearranging and substituting λ for f in MHz yields (2) which allows range D to be calculated in kilometers.

$$P_r = (P_t + G_t) + G_r + 20\log_{10}\left(\frac{\lambda}{4\pi d}\right) \tag{1}$$

$$D = \frac{10^{(P_t+G_t+G_r-P_r)/20}}{41.88 \times f} \tag{2}$$

The WiMAX base station is configured with three 120° sector antennae, or four 90° sector antennae, which allow for communication with subscriber units close to the base station. This mode of operation is described as point-to-multipoint (PtMP), since one base station antenna serves many subscribers. Subscriber units further away will require a dedicated high gain antenna on the base station. This mode of operation is described as point-to-point (PtP). These modes are illustrated in Fig. 1. Note that subscriber units (SU) close to the base station are served by four 90° sector antennae in PtMP mode, while distant units are served by dedicated high gain antennae in PtP mode.

Since the link is bidirectional, each antenna both transmits and receives. As EIRP is limited to the same value at both the subscriber unit and the base station, the range will be limited by the lower of the two antenna gains. Directional antennae may be used at the subscriber unit, so in practice the base station antennae will limit range.

From the equipment datasheet [21], an RSL of −86 dBm is required to achieve 50 Mbps throughput. It is normal practice to consider a fade margin to allow for variations in RSL due to changes in environmental conditions. Allowing a 6 dB fade margin yields $P_r = -80$ dBm.

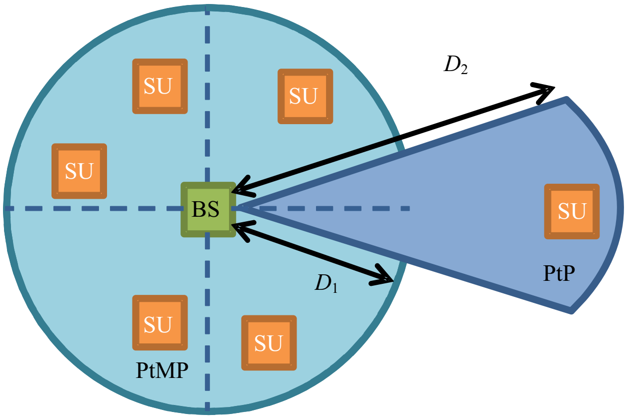

Fig. 1 Modes of operation of the fixed WiMAX base station (BS)

The equipment will pass data with an RSL of −96 dBm, thus the functional fade margin is 16 dB.

Consider transmission from the subscriber unit to the PtMP array on the base station. The subscriber unit has gain $G_t = 27$ dB, thus $P_t = 9$ dBm (8 mW). Frequency f is 5745 MHz. If three 120° sector antennae ($G_r = 16$ dB) are used at the base station and ($P_t + G_t = 36$ dB), from (2) the range D_1 is found to be 16.5 km. Changing configuration to four 90° antennae ($G_r = 20$ dB), the range D_1 is increased to 26.2 km. Repeating for PtP mode, a subscriber unit type antenna at the base station ($G_t = 27$ dB) yields $D_2 = 58.7$ km. These parameters and results are summarized in Table 2.

Since PtP links require that their own frequency and bands are limited at 5 GHz, PtP operation is discouraged. OFCOM regulations [25] currently allow for only 4 channels in the 5 Ghz Band C, the preferred band for FWA. Although 11 channels exist in Band B, these may only be used at much lower power (1 W or 30 dBm) and are only suited for short range FWA. Thus, it seems prudent to design the network for 4-sector antennae. This will increase the range for PtMP links and reduce the number of base stations required for a small additional equipment cost. Thus, subscriber units closer than 26 km from the base station operate in PtMP mode via sector antennae,

Table 2 WiMAX base station range parameters

Mode	3-sector	4-sector	PtP
P_t	9 dBm	9 dBm	9 dBm
G_t	27 dB	27 dB	27 dB
G_r	16 dB	20 dB	27 dB
P_r	−80 dBm	−80 dBm	−80 dBm
D	16.5 km	26.2 km	58.7 km

Note: Subscriber unit (P_t, G_t) to base station (P_r, G_r), f = 5745 MHz while more distant units operate using PtP mode up to 58 km. This is in line with the commercial WiMAX operator's practice and experience. Note that subscribers closer to the base station than D_1 or D_2 would expect better than designed performance for their mode. The above discussion is a very simplified summary of the process involved in PtMP FWA planning.

5 Wireless network planning

Using the ranges calculated in the previous section, and assuming line-of-sight operation is required, it is possible to simulate radio propagation and determine appropriate placement of base stations to serve known subscriber sites. This section will consider a case study in which it is desired to provide high speed connectivity to wind farms in Northern Ireland. In this study, there are 51 wind farms that require a connection, Fig. 2.

The radio propagation is modeled in the ICS software package from ADTI Ltd [26] and uses ITU-R P.525 [27] for the calculation of free space attenuation. This software is used professionally for such studies and allows the use of many data sets to assist radio planning. In this study, where line-of-sight operation is required, geographical terrain data is obtained from the NGA/NASA "Shuttle Radar Topography Mission" [28].

5.1 Existing 452 MHz SCADA towers

It is first worth considering if broadband communication is possible from utility radio towers that presently operate wireless SCADA at 452 MHz. At this frequency, line-of-sight is not a requirement. Fig. 3 shows the radio propagation from the 21 SCADA sites available. Since the SCADA sites are low lying, range is limited and many of the SCADA sites are located in areas far from the wind farms. Using these sites, 36 of the 51 wind farms are serviced from 9 SCADA sites. Although this seems favorable, the propagation path is not ideal and individual site surveys would be necessary.

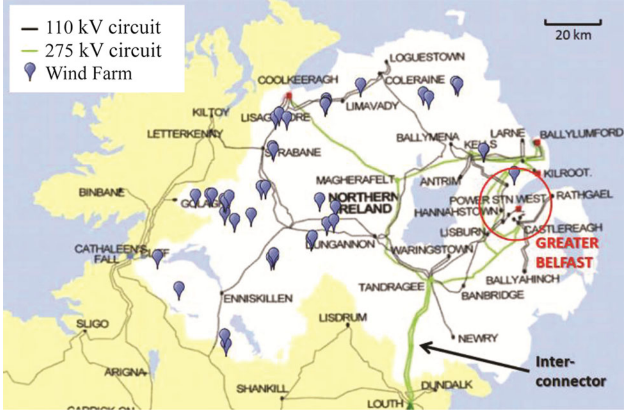

Fig. 2 Map of Northern Ireland transmission system and wind farms

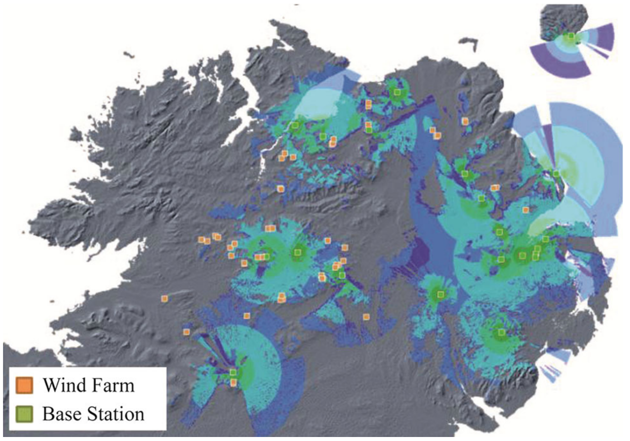

Fig. 3 Range from 452 MHz SCADA sites if operated as WiMAX base stations (with very limited coverage of wind farms)

5.2 Using preferred 'high-sites'

The objective of any commercial FWA provider is to provide service to the maximum number of subscribers with the minimum cost in infrastructure. The ideal sites will be those situated on mountain tops with a clear view of the surrounding land and other mountain tops. These are typically already identified on maps as 'trig points' or triangulation pillars, by the government mapping department. It is sometimes possible to acquire a radio site adjacent to such points, or these may be used as a starting point to determine an optimum position. Factors such as local planning considerations and the availability of land for rent/purchase are limiting factors. Additional concerns include vehicular accessibility and the potential for electrical power supply.

Suitable base station locations have been assessed using the method above by an incumbent WiMAX operator in the region. This operator has 103 base station locations, constructed of wooden monopole in a concrete base. Many of these sites provide fill-in for areas where other base stations cannot reach (e.g. valleys). Since wind farms are usually located on high sites, Fig. 4 shows that only a fraction of the available sites are necessary to provide coverage of wind farms. All 51 wind farms can be served using 16 base stations, however optimizing for distance and performance using the ATDI tool, 21 sites would be preferred.

5.3 Costs

The cost of deploying the WiMAX network is subject to a number of factors, including availability and suitability of

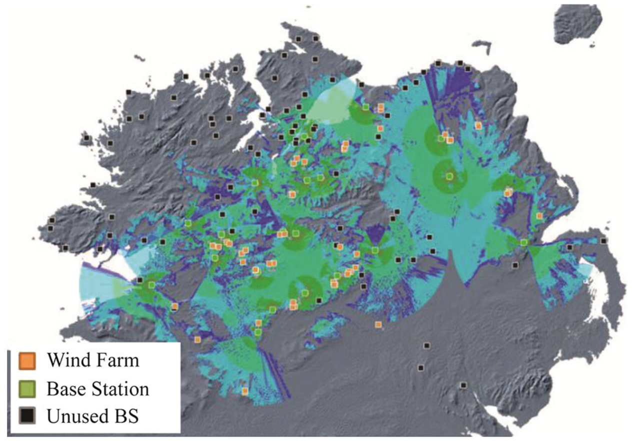

Fig. 4 Complete coverage of all 51 wind farms using 21 base stations from WiMAX operator's available sites (Available but unused base station sites are indicated in black.)

sites, availability of services (electricity, backhaul) and accessibility (roads, rights of way). The figures stated in this paper are indicative of experience and should serve as a guide.

The capital cost of a base station assumes that electrical supply is available nearby and that rights-of-way can be negotiated. The most economical base station structure, a 10 m monopole mast, will cost circa US$30 k including civil engineering works. For more complex sites using a steel tower, costs will be a multiple of this. Electronic equipment to serve per sector (antennas, transceivers, power supply) will cost of the order $8 k, while licensed microwave/MPLS equipment to provide backhaul between base stations is of the order of $80 k Ongoing costs will include electricity consumption ($150/year) and site rental (varies between urban/rural sites). A typical 4-sector base station can be considered to cost $120 k to install, turnkey and complete.

The cost of subscriber units varies by the technology used. An unlicensed band PtMP subscriber unit typically costs $150, or circa $800 for a licensed band unit. PtP equipment costs circa $3000 for an unlicensed band, or $6000 for a licensed band unit.

6 Technical performance

The technical performance of WiMAX has been assessed experimentally by using a commercial WiMAX network in operation in Northern Ireland, owned by Northwest Electronics (NWE). Network performance has been assessed using data from two computers connected at wind farms for the purpose of synchrophasor monitoring. The topology of the network is shown schematically in Fig. 5. Each subscriber unit is connected via unlicensed WiMAX at 5.8 GHz, while the core network operates licensed microwave. The two wind farm computers communicate via a total of 9 core network sites. The link between the SUs and their nearest base stations is PtMP. These base stations link to the core network using 5.8 GHz PtP links. The core network, comprising 6 of the links, operates licensed, MPLS links which give near fiber like performance. Through agreement with the service provider, the authors' equipment is operated in the same manner as it would be on a private installation. Thus the performance data shown is reflective of what a private utility installation would achieve.

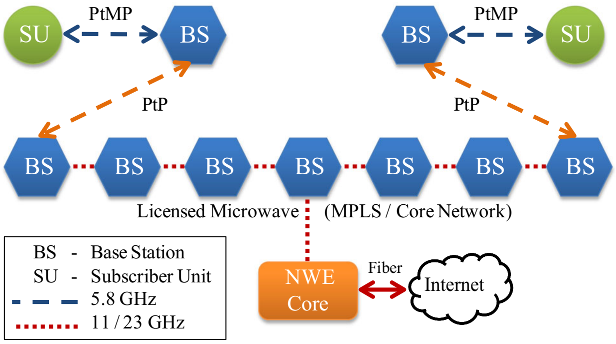

Fig. 5 Schematic of system used in testing performance of the WiMAX network

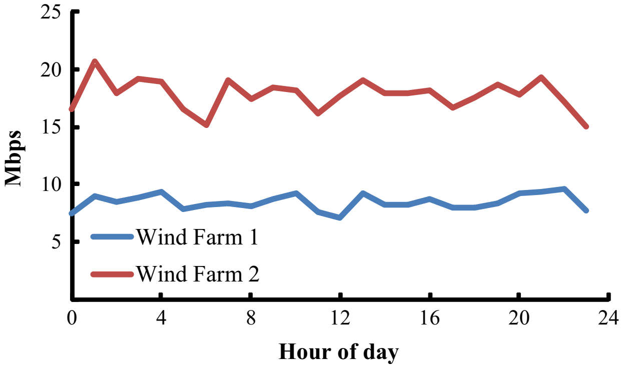

Fig. 6 Throughput measured on WiMAX connections at wind farms at hourly intervals

6.1 Throughput

The throughput has been monitored by performing a speed test using an Internet based tool at hourly intervals. The results, presented in Fig. 6 show that speeds of greater than 7 Mbps are consistently available on the PtMP sector of Wind Farm 1 (Tappaghan, Co. Fermanagh), while 15 Mbps is the lowest speed seen on Wind Farm 2 (Elliot's Hill, Co. Antrim). Throughput at both wind farms are capped by the ISP at 10 Mbps and 20 Mbps respectively. These speeds are far in excess of the 75 kbps requirement for synchrophasor streaming.

Table 3 Latency requirements of IEEE Std 1646

Speed required	Typical application	One-way latency
Very high	Streaming VT and CT samples and protection signals to switchgear	<2 ms
High	Event notification for protection	2～10 ms
Medium	Exchange non-critical information between protection units, exchange information between control functions, synchrophasor measurements	10～100 ms
Low	Message delivery external to the substation (control centre) or the substation computer or IEDs	>100 ms

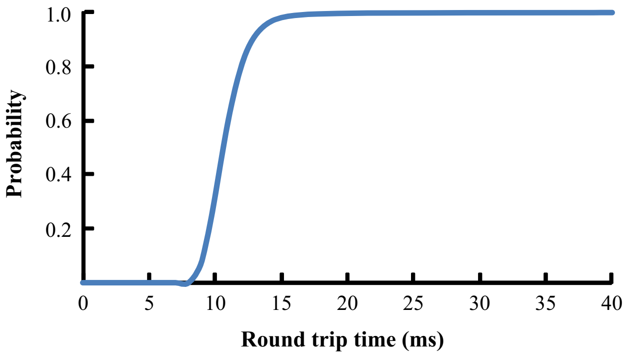

Fig. 7 Round trip time (latency) to traverse WiMAX network from one wind farm to another

6.2 Latency

Latency requirements for various power systems applications have been defined in IEEE Std. 1646 and are summarized in Table 3. The performance of the WiMAX network has been assessed by performing a ‘ping’ test between two wind farm sites connected to the network. A ping sends a packet from one computer to a remote computer and requests an echo. The time until the echo is received is recorded by the sending computer. The ping test operated over the course of one month is summarized as a cumulative probability distribution in Fig. 6. Note that each wind farm is on a PtMP sector.

Fig. 7 shows the round trip time, the time taken by a ping packet to across the WiMAX network both to the remote computer and back to the sending computer. After 15 ms, 98.0% of ping requests are returned, and by 29 ms, 99.9% of pings are returned. The latency in one direction is found by halving the round trip time.

Data can reliably traverse the WiMAX network from one site to another in better than 15 ms. This places the performance, according to IEEE 1646, in the ‘High’ category. Further analysis using the ‘trace route’ reveals that most of the latency experienced arises from the base station to subscriber unit link at each end, approximately 3 ms in each case. The latency across the core part of the network, which uses licensed microwave/MPLS, is approximately 2 ms.

6.3 Reliability

Standard models exist for estimation of link availability and reliability, however a detailed analysis is beyond the scope of this paper [27]. Any detailed analysis will consider the climate, terrain and link parameters to arrive at a fade margin and an availability figure, normally expressed as a percentage. The equipment under test uses 2 × 2 multi-input multi-output (MIMO), there are two spatial streams where both horizontal and vertically polarized signals are utilized. Fading is generally uncorrelated for horizontal and vertically polarized signals and the probability that both signals will fade below their margin is the product each individual fade probability. The overall availability in this case will be better than 99.99% using the carrier’s heuristic fade margin of 16 dB. No complete losses in connectivity were seen during the duration of the network testing, thus the reliability of the network has been considered on the basis of meeting the ‘medium’ category of IEEE Std. 1646, which specifies synchrophasor measurements as one of the functions which should meet this standard. Over the course of testing, 99.99% of packets traversed the network in less than 100 ms. To put this into perspective, a PMU reporting at 50 frames per second would experience delays on 464 of the 4.32 million frames reported during each day. Note that no frames would be lost during the time the connection was under observation.

7 Security

From a network engineering perspective, WiMax provides an alternative to a wired Ethernet network. In ISO terms [29], it is the layer 1 physical transport for layer 2 frames. Of the devices used and tested, all supported operation as a layer 2 device (a switch) or as a layer 3 device (a routed connection).

Configuring the WiMax base station unit (BSU) as a layer 2 device in PtMP results in receive stations units (RSU) appearing to be in the same layer 2 network segment. End nodes are accessible to each other and a range of attacks are feasible. Address resolution protocol (ARP) attacks such as impersonation, redirection and man-in-themiddle (MitM) have been demonstrated. Where the RSU connects directly to a remote network segment, local “housekeeping” traffic may be propagated to other RSUs in the same multipoint network, providing opportunities for an external attacker to reconnoitre the remote network segment. These are all clearly undesirable characteristics.

Configuring each link from a BSU as a layer 3 link allows each RSU to appear as a router on the network. Although this makes network planning more complex, it allows for separation of RSUs from a security perspective and depending on the BSU equipment, may allow for the implementation of access control lists (ACLs) and other measures to restrict inter-RSU traffic and unauthorised access to the remote network. It does however restrict layer 2 only protocols to the local network. Such protocols are often found in sub-station equipment, for example DNP3 specifies a layer 2 protocol. In pilot PtMP sites, RSUs were configured as layer 3 devices with a class C address assigned to each BSU. Dividing address space into/30 subnets gave 62 usable RSU connections per BSU.

PtP links were also evaluated. These are expensive in BSU hardware but the main limitation in using these links is that a dedicated frequency and bandwidth required, restricting scalability.

At layer 2 and above, all the normal security concerns exist and all the normal mitigation strategies may be applied. Typical applications tested by the authors use conventional VPN technologies for secure and encrypted communications from the sub-station/RSU to the control centre. Conventional routing protocols operate transparently on this network allowing the underlying secure infrastructure to be completely transparent to the applications running on it and to dynamically respond to changes in topology. This approach is also transparent to the sub-station applications, the underlying network appearing as a two hop routed network.

8 Conclusion

This paper has described the technical background of WiMAX/FWA and discussed the design procedure for using this technology as a delivery mechanism for data in Smart Grid/electric vehicle applications. The performance of WiMAX has been evaluated using empirical data obtained from a commercial WiMAX network in Northern Ireland. The WiMAX system is shown to operate satisfactorily in terms of throughput, latency and reliability.

A planning study has been conducted to determine the suitability of WiMAX for use as a telecoms delivery mechanism for wind farms. The study determined that while existing utility SCADA towers may be of some use, to achieve the necessary line of sight to the wind farms, new base stations are required. To service the 51 wind farms of Northern Ireland, 21 base station locations are preferred. Costs for base stations and subscriber units are indicated.

WiMAX is proposed as an immediately available solution to address the data connectivity needs demanded by synchrophasor applications. WiMAX technology may be rapidly deployed at reasonably low costs to areas where limited data alternatives exist. In utilities with long term objectives to operate ubiquitous fiber optic telecoms, WiMAX can serve as a diverse solution, providing backup connectivity in the event of failure of primary fiber connectivity.

With industry trends moving towards Ethernet/IP communication as standard, the availability of security solutions including licensed bands, MPLS segregation and VPN encryption makes WiMAX an attractive solution for providing data connectivity for remote smart grid applications.

Acknowledgments This work was supported by the EPSRC/NFSC co-funded Intelligent Grid Interfaced Vehicle Eco-charging (iGIVE) Project (EP/L001063/1). The authors would like to thank Letterkenny Institute of Technology, Ireland, for hosting equipment used during this study.

References

1. Chen TM, Abu-Nime S (2011) Lessons from Stuxnet. Computer 44(4):91–93
2. The heartbleed bug. http://heartbleed.com/ Accessed 28 Sept 2014
3. What is #Shellshock? https://shellshocker.net/ Accessed 4 Feb 2015
4. Patel M, Aivaliotis S, Allen E et al (2010) Real-time application of synchrophasors for improving reliability. North American Electric Reliability Corporation (NERC), Princeton
5. Best RJ, Morrow DJ, Laverty DM et al (2010) Synchrophasor broadcast over internet protocol for distributed generator synchronization. IEEE Trans Power Deliver 25(4):2835–2841
6. Laverty DM, Best RJ, Morrow DJ (2014) Loss-of-mains protection system by application of phasor measurement unit technology with experimentally assessed threshold settings. IET Gen Transm Distrib 9(2):146–153
7. IEEE Std C37.118.2-2011 (2011) IEEE standard for synchrophasor data transfer for power systems. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6111222
8. IEEE Std 1646-2004 (2004) IEEE standard communication delivery time performance requirements for electric power substation automation. http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=9645

9. Zuo J, Carroll R, Trachian P et al (2008) Development of TVA SuperPDC: phasor applications, tools, and event replay. In: Proceedings of the IEEE Power and Energy Society general meeting: conversion and delivery of electrical energy in the 21st century, Pittsburgh, PA, 20–24 Jul 2008, 8 pp
10. Schweitzer Engineering Laboratories (SEL) (2010) Smart anti-islanding using synchrophasor measurements. Schweitzer Engineering Laboratories (SEL), Pullman
11. Zweigle G (2009) Archive wide-area information with synchrophasors. AN2009-24, Schweitzer Engineering Laboratories (SEL), Pullman
12. BBC News (2011) "Anonymous" defends the use of Web attacks. BBC News, 28 Jan 2011. http://www.bbc.co.uk/news/technology-12307802
13. Duvelson E (2010) Bridging the gap between legacy and modern substation communications. UTC J (2nd Quarter): 37–44. https://www.cavs.msstate.edu/iPCGRID_Registration/presentations/2011/Duvelson%20i-PCGRID%202001%20Bridging%20the%20Gap.pdf
14. Ward S, Duvelson E (2010) Integrating legacy communications on the smart grid highway. In: Proceedings of the 2010 IEEE PES transmission and distribution conference and exposition, New Orleans, LA, 19–22 Apr 2010, 4 pp
15. DNP3 Users Group (2008) DNP3 secure authentication specification version 2.0. DNP3 Users Group Technical Committee. https://www.dnp.org/Lists/Announcements/Attachments/7/Secure%20Authentication%20v5%202011-11-08.pdf
16. IEC 61850 (2007) Communication networks and systems in substations. http://www.iec.ch/smartgrid/standards/
17. Duvelson E (2011) Global migration toward ethernet/IP networks in substation communications. UTC J (2nd Quarter): 33–41. http://www.bluetoad.com/publication/?i=70749&p=33
18. Baran P (1964) On distributed communications networks. IEEE Trans Commun Syst 12(1):1–9
19. IEEE Std 802.16-2001 (2001) IEEE standard for local and metropolitan area networks, part 16: air interface for fixed broadband wireless access systems
20. Abichar Z, Peng YL, Chang JM (2006) WiMax: the emergence of wireless broadband. IT Prof 8(4):44–48
21. NanoStation product datasheet. Ubiquiti Networks. http://www.ubnt.com. Accessed Jun 2012
22. Linksys router datasheet. Cisco networking. http://home.cisco.com/en-us/wireless/. Accessed 14 Sept 2014
23. ITU-R P.530-14 (2012) Propagation data and prediction methods required for the design of terrestrial line-of-sight systems. https://www.itu.int/dms_pubrec/itu-r/rec/p/R-REC-P.530-14-201202-S!!PDF-E.pdf
24. Friis HT (1946) A note on a simple transmission formula. P IRE 34(5):254–256
25. Fixed wireless access. OFCOM. http://licensing.ofcom.org.uk/radiocommunication-licences/fixed-wireless-access/?a=0. Accessed 14 Sept 2014
26. ICS Telecom. ATDI. http://www.atdi.co.uk/software/software-applications/ics-telecom/. Accessed 14 Sept 2014
27. ITU-R P.525-2 (1994) Calculation of free-space attenuation. https://www.itu.int/dms_pubrec/itu-r/rec/p/R-REC-P.525-2-199408-I!!PDF-E.pdf
28. NASA's Jet Propulsion Laboratory (JPL) (2000) Shuttle radar topography mission. NASA's Jet Propulsion Laboratory (JPL), Pasadena
29. ISO/IEC 7498-1:1996 (1996) Information technology—open systems interconnection—basic reference mode. http://webstore.iec.ch/preview/info_isoiec7498-1%7Bed2.0%7Den.pdf

David M. LAVERTY received the M.Eng and Ph.D. degrees from Queen's University Belfast, Belfast, UK, in 2006 and 2010 respectively. Since 2011 he has been a Lecturer with the Electrical Power and Energy Research Cluster at Queen's University Belfast, Belfast, UK. His current research interests include power system measurements, anti-islanding detection, phasor measurements, and Smart Grid telecommunications, messaging and security. Dr. Laverty is a member of the IEEE and volunteers with the Institution of Engineering and Technology (IET).

John B. O'RAW has been a IT Manager at Letterkenny Institute of Technology, Ireland, since 1996. Prior to this, he worked as a project leader with ABB in Milan specializing in large scale process automation and information systems and with Combustion Engineering in Dundalk. He holds a B.Sc in Information Technology, a Diploma in Electronic Engineering and separate Master's Degrees in Applied Computing and Maritime Archaeology. John is presently completing his PhD in secure utility communication systems at Queen's University Belfast.

Kang LI received the B.Sc. degree from Xiangtan University, Hunan, China, in 1989, the M.Sc. degree from the Harbin Institute of Technology, Harbin, China, in 1992, and the Ph.D. degree from Shanghai Jiaotong University, Shanghai, China, in 1995. He is currently a Professor of intelligent systems and control with the School of Electronics, Electrical Engineering, and Computer Science, Queen's University Belfast, Belfast, UK. He has published over 180 papers and edited 10 conference proceedings (Springer). His current research interests include nonlinear system modeling, identification, and control, bio-inspired computational intelligence, fault diagnosis and detection, with recent applications on power systems and renewable energy, polymer extrusion processes, bioinformatics with applications on food safety, healthcare, and biomedical engineering.

D. John MORROW received the B.Sc and Ph.D. degrees from Queen's University Belfast, Belfast, UK, in 1982 and 1987, respectively. Since 1987, he has been a Lecturer in electrical engineering at Queen's University Belfast, Belfast, UK, with research and consulting interests in electric power systems, power system instrumentation, and embedded generation. Dr. Morrow is a member of the IET and also a member of the IEEE PES Excitation Systems Subcommittee.