Available online at www.sciencedirect.com
SCIENCE DIRECT®
Computer Networks 50 (2006) 877–897
Computer Networks
www.elsevier.com/locate/comnet

A survey on communication networks for electric system automation

V.C. Gungor [a,*], F.C. Lambert [b]

[a] Broadband and Wireless Networking Laboratory, School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332, United States
[b] National Electric Energy Testing, Research and Applications Center, Georgia Institute of Technology, Atlanta, GA 30332, United States

Received 18 January 2006; accepted 26 January 2006
Available online 21 February 2006

Responsible Editor: I.F. Akyildiz

Abstract

In today's competitive electric utility marketplace, reliable and real-time information become the key factor for reliable delivery of power to the end-users, profitability of the electric utility and customer satisfaction. The operational and commercial demands of electric utilities require a high-performance data communication network that supports both existing functionalities and future operational requirements. In this respect, since such a communication network constitutes the core of the electric system automation applications, the design of a cost-effective and reliable network architecture is crucial. In this paper, the opportunities and challenges of a hybrid network architecture are discussed for electric system automation. More specifically, Internet based Virtual Private Networks, power line communications, satellite communications and wireless communications (wireless sensor networks, WiMAX and wireless mesh networks) are described in detail. The motivation of this paper is to provide a better understanding of the hybrid network architecture that can provide heterogeneous electric system automation application requirements. In this regard, our aim is to present a structured framework for electric utilities who plan to utilize new communication technologies for automation and hence, to make the decision-making process more effective and direct.

Keywords: Electric system automation; Internet based Virtual Private Network; Power line communication; Satellite communication; Wireless sensor networks; Wireless mesh networks; WiMAX

1. Introduction

Electric utilities, particularly in urban areas, continuously encounter the challenge of providing reliable power to end-users at competitive prices. Equipment failures, lightning strikes, accidents, and natural catastrophes all cause power disturbances

* Corresponding author. Tel.: +1 404 894 5141; fax: +1 404 894 7883.
E-mail addresses: gungor@ece.gatech.edu (V.C. Gungor), frank.lambert@neetrac.gatech.edu (F.C. Lambert).

1389-1286/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.comnet.2006.01.005

and outages and often result in long service interruptions. Electric system automation, which is the creation of a reliable and self-healing electric system that rapidly responds to real-time events with appropriate actions, aims to maintain uninterrupted power service [6]. The operational and commercial demands of electric utilities require a high-performance data communication network that supports both existing functionalities and future operational requirements. Therefore, the design of the network architecture is crucial to the performance of the system.

Recent developments in communication technologies have enabled reliable remote control systems, which have the capability of monitoring the real-time operating conditions and performance of electric systems. These communication technologies can be classified into four classes, i.e., Power Line Communication, Satellite Communication, Wireless Communication, and Optical Fiber Communication. Each communication technology has its own advantages and disadvantages that must be evaluated to determine the best communication technology for electric system automation. In order to avoid possible disruptions in electric systems due to unexpected failures, a highly reliable, scalable, secure, robust and cost-effective communication network between substations and a remote control center is vital [11,14]. This high performance communication network should also guarantee very strict Quality of Service (QoS) requirements to prevent the possible power disturbances and outages [10].

When the communication requirements of electric system automation are considered, Internet can offer an alternative communication network to remotely control and monitor substations in a cost-effective manner with its already existing communication infrastructure. However, Internet cannot guarantee very strict QoS requirements that the automation applications demand, since data communication in Internet is based on *best effort service* paradigm [32]. Furthermore, when a public network like the Internet is utilized to connect the substations to a remote control center, security concerns arise. In this context, Internet based Virtual Private Network (Internet VPN) technologies, which are transforming the Internet into a secure high speed communication network, constitute the cornerstone for providing strict QoS guarantees of electric system automation applications [7]. Internet VPN technologies offer a shared communication network backbone in which the cost of the network is spread over a large number of users while simultaneously providing the benefits of a dedicated private network. Therefore, Internet VPN technology as a high speed communication core network can be utilized to enable minimum cost and highly reliable information sharing for automation applications.

Although Internet VPN technologies can provide the necessary reliable communication for substations in urban areas, this may not be the case for substations in remote rural locations where the high speed communication core network, e.g., Internet, might not exist. Therefore, when the individual communication capabilities and locations of electric systems are taken into account, it is appropriate to consider the overall communication infrastructure as a hybrid network as shown in Fig. 1. This hybrid network consists of two separate parts:

- *High speed communication core network*: It can be either a private network or public network. Due to several technical advantages [32], Internet based Virtual Private Network can be considered as a cost-effective high speed communication core network for electric system automation.
- *Last mile connectivity*: It represents the challenge of connecting the substations to the high speed communication core network. The communication technologies for last mile connectivity can be classified as: (i) Power line communication, (ii) Satellite communication, (iii) Optical fiber communication, and (iv) Wireless communication. Each possible communication alternatives for last mile connectivity introduces its own advantages and disadvantages.

Many researchers and several international organizations are currently developing the required communication technologies and the international communication standard for electric system automation. In Fig. 2, the summary of these communication system development activities is presented [14]. Despite the considerable amount of ongoing research, there still remains significantly challenging tasks for the research community to address both benefits and shortcomings of each communication technology. Since a cost-effective data communication network constitutes the core of the automation applications, in this paper, the opportunities and challenges of a hybrid network architecture are described for automation applications. More specifically, Internet based Virtual Private Networks,

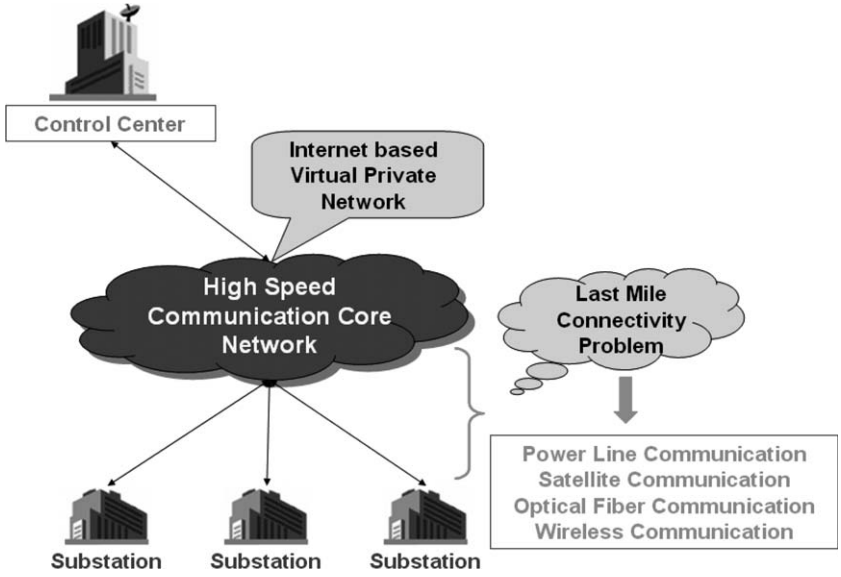

Fig. 1. The overall communication network architecture for electric system automation.

Phase	Years	System Characteristics	Network Architecture	Communication Media	Communication Protocols & Standards
Non-Standardized	Up-to 1985	• Many proprietary systems • Single vendor per system • Basic data collection	• Hierarchical tree • Single master • Isolated substations	• RS232 and RS485 • Dial up • Trunked radio • Power-line carrier • Less than 1200 bps	• Modbus • SEL • WISP • Conitel 2020
Standards Development Begins	1985-1995	• Multi-vendor systems • Protocol Conversion	• Hierarchical tree • Multiple masters • Redundant links	• Leased lines • Packet radio • 9600 to 19200 bps	• DNP3 Serial • IEC 60870 • TASE 2
Local Area Networks (LANs) and Wide Area Networks (WANs)	1995-2000	• Introduction of LANs in substations • Merging protection and SCADA networks	• Peer-to-peer comm. in substation • Joining substations via WAN	• Ethernet • Spread Spectrum Radio • Frame relay • Megabit data rates	• TCP-IP • FTP • Telnet • HTTP • DNP3 WAN/LAN • UCA 2.0
Integration into Business	2000 to present	• Merging automation and business networks • Corporate IT departments • Asset Management	• Linking of utility WAN to corporate network • Extension of network to customer premises • Use of Internet	• Digital cellular • IP radios • Wireless Ethernet • Gigabit backbones	• TCP-IP • IEC 61850 • XML

Fig. 2. Summary of communication system development activities for electric utilities.

power line communications, satellite communications and wireless communications (wireless sensor networks, WiMAX, and wireless mesh networks) are discussed in detail. The motivation of this paper

is to provide a better understanding of the hybrid network architecture that can provide heterogeneous electric system automation application requirements. In this respect, our aim is to present a structured framework for electric utilities who plan to utilize new communication technologies for automation and hence, to make the decision-making process more effective and direct.

The remainder of the paper is organized as follows. In Section 2, the benefits and open research challenges of Internet based Virtual Private Networks are discussed for electric system automation. In Section 4, both advantages and disadvantages of alternative communication technologies are described for last mile connectivity. In Sections 5 and 6, the opportunities and challenges of wireless sensor networks, wireless mesh networks and WiMAX are explained, respectively. Finally, the paper is concluded in Section 7.

2. Internet based Virtual Private Networks

Recent advances in Internet technology and Internet-ready IEDs (Intelligent Electronic Devices) have enabled cost-effective remote control systems, which makes it feasible to support multiple automation application services, e.g., remote access to IED/relay configuration ports, diagnostic event information, video for security or equipment status assessment in substation and automatic metering. While traditional private Supervisory Control and Data Acquisition (SCADA) systems constitute the core communication network of today's electric utility systems, the Internet based Virtual Private Network (Internet VPN) technology provides an alternative cost-effective high speed communication core network for remote monitoring and control of the electric system.

Specifically, Internet VPN technology is a shared communication network architecture, in which the cost of the network is spread over a large number of users while simultaneously providing both the functionalities and the benefits of a dedicated private network. Therefore, the main objective of an Internet VPN for electric system automation is to provide the required cost-effective high performance communication between IEDs and a remote control center over a shared network infrastructure with the same policies and service guarantees that the electric utility experiences within its dedicated private communication network. In order to achieve this objective, the Internet VPN solution should provide the following essential performance attributes:

- *Quality of Service* (*QoS*): Internet technology itself cannot guarantee very strict QoS requirements that utility applications require, since data communication in the Internet is mainly based on a best effort service paradigm. In this respect, QoS capabilities of Internet VPN technologies ensure the prioritization of mission critical or delay sensitive traffic and manage network congestion under varying network traffic conditions over the shared network infrastructure.
- *Reliability*: The communication network should be able to operate continuously over an extended period of time, even in the presence of network element failures or network congestion. To achieve this, the communication network should be properly designed with the objective of no losses in all working conditions and able to deal with failure gracefully. Service providers support Service Level Agreements (SLAs), which define the specific terms and performance metrics regarding availability of network resources and offer the Internet VPN subscriber a contractual guarantee for network services and network uptime. Therefore, Internet VPN technology should deliver data in a reliable and timely manner for automation applications.
- *Scalability*: Since the number of substations and remote devices is large and growing rapidly, the communication system must be able to deal with very large network topologies without increasing the number of operations exponentially for the communication network. Thus, the designed hybrid network architecture should scale well to accommodate new communication requirements driven by customer demands.
- *Robustness*: In order to avoid deteriorating communication performance due to changing network traffic conditions, the dimensioning process to assign the bandwidth to the virtual links of the Internet VPN should be based not only on the main bandwidth demand matrix, but also on other possible bandwidth demand matrices to provide a safe margin in network dimensioning to avoid congestion [28]. In case the network congestion can not be avoided with the current network traffic, low priority non-critical data traffic should be blocked so that the most critical data can be transmitted with QoS guarantees [26]. This way, additional bandwidth for high

priority data becomes available to enable the real-time communication of critical data, which is particularly important in case of alarms in electric systems.

- *Security*: Security is the ability of supporting secure communication between a remote control center and field devices in order to make the communication safe from external denial of service (DoS) attacks and intrusion. When a public network like the Internet is utilized to connect the field devices to a remote control center, security concerns can arise. Hence, Internet VPN has to provide secure data transmission across an existing shared Internet backbone and thus, protect sensitive data so that it becomes confidential across the shared network.
- *Network management*: In order to provide the communication requirements of automation applications, electric utilities demand flexible and scalable network management capabilities. The primary network management capabilities of Internet VPN include: (i) bandwidth provisioning, (ii) installing security and QoS policies, (iii) supporting Service Level Agreements, (iv) fault identification and resolution, (v) addition and removal of network entities, (vi) change of network functions, (vii) accounting, billing and reporting. In addition to these network management capabilities, Internet VPN technology can enable rapid implementation and possible modifications of the communication network at a reasonable cost. Therefore, Internet VPN technology with effective network management approaches provides a flexible cost-effective solution that can be easily adapted to future communication requirements that utility automation applications demand.

Despite the extensive research in Internet VPN technologies [32], there are still several open research issues, e.g., efficient resource and route management mechanisms, inter-domain network management, that need to be developed for automation applications. In the current literature, two unique and complementary VPN architectures based on Multi Protocol Label Switching (MPLS) and IP Security (IPsec) technologies are emerging to form the predominant communication framework for delivery of high performance VPN services [32]. In Fig. 3, we compare both the advantages and disadvantages of MPLS based VPN and IPSec VPN architectures in terms of performance attributes described above. As shown in Fig. 3, each Internet VPN technology supports the performance attributes to varying degrees and thus, the most appropriate choice depends on the specific communication requirements of the electric utilities.

In Fig. 4, a decision tree for choosing an appropriate Internet VPN technology for electric system automation is illustrated. As shown in Fig. 4, if an electric utility requires a high performance communication network ensuring very strict Quality of Service (QoS) requirements, the next decision point in the decision tree can be the size of the communication network, i.e., the number of communication entities that need to be interconnected. Electric utilities that need to connect a large number of substations and a remote control center should prefer cost-effective MPLS based Internet VPN technology, since they can reduce the communication cost significantly compared to dedicated private leased communication lines. If the number of sites is not large in the network, electric utilities can utilize a hybrid network including IPSec Internet VPN and layer 2 technologies such as Frame Relay and ATM for the automation applications. If there are no QoS communication requirements, the possible options include either using public Internet when no secure communication is required or using an IPSec Internet VPN when secure communication is required in automation applications.

In fact, the actual selection of Internet VPN technology depends on several factors such as the cost of communication architecture, geographic coverage of the communication architecture, the locations of substations and a remote control center, service level agreements, network management types, i.e., customer based or network based management, etc. As a result, electric utilities should evaluate their unique communication requirements and the capabilities of Internet VPN technologies comprehensively in order to determine the best Internet VPN technology for automation applications.

3. Last mile connectivity for electric utilities

In this section, both advantages and disadvantages of possible communication technologies for last mile connectivity are explained in detail. The communication technologies evaluated for last mile connectivity are: (i) Power line communication, (ii) Satellite communication, (iii) Optical fiber communication, (iv) Wireless communication.

Performance Metrics	MPLS Internet VPN	IPSec Internet VPN
Quality of Service (QoS)	Provides QoS and supports service level agreements (SLAs) through its Internet Traffic Engineering capabilities.	Does not address QoS, service level agreements (SLAs) and service-level guarantees (SLGs) directly.
Reliability	Enables reliability with its efficient fault detection and management methods.	Tries to maintain reliability by establishing two virtual tunnels, one to the primary router and the other to the backup router.
Scalability	Highly scalable since full end-to-end site peering across the network is eliminated. It is typically capable of supporting thousands of VPN groups over the same shared communication network.	Greatly suffers from scalability problems due to the operational challenge of managing large VPNs. Additional planning required for peering configuration, key management and distribution.
Robustness	Ensures robustness with its dimensioning processes which assign the bandwidth to the virtual links of the network not only based on the main bandwidth demand matrix, but also on other possible bandwidth demand matrices to provide a safe margin.	Robustness of the communication depends on the traffic condition in the network. Although IPSec technology provides secure connection through its encryption and encapsulation techniques, it might not ensure a robust connection due to the lack of predictable communication performance across the Internet.
Security	Provides security with traffic separation over the shared network using unique route distinguishers.	Provides data confidentiality with encryption and tunneling mechanisms that protect data packets over the shared communication network architecture.
Network Management	Provides network management with its traffic engineering mechanisms. Resource and route management algorithms ensure efficient network management.	Centralized network level provisioning can decrease operational and network management expenses for customer premise equipment (CPE) based service.

Fig. 3. Comparison of MPLS based Internet VPN and IPSec Internet VPN for electric system automation applications.

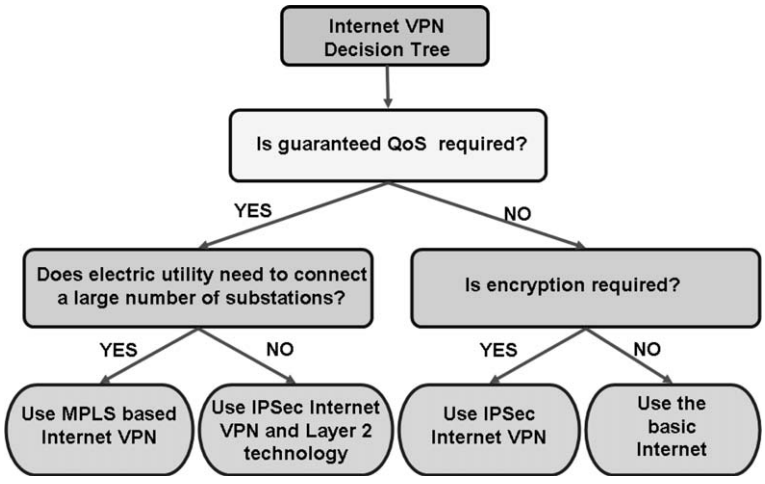

Fig. 4. A basic Internet VPN decision tree for electric system automation.

3.1. Power Line Communication

Power Line Communication (PLC) is transmission of data and electricity simultaneously over existing power lines as an alternative to constructing dedicated communications infrastructure. Although PLC has been in operation since the 1950s as low data rate services such as remote control of power grid devices, it has become more important in recent years due to developments in technology, which enable PLC's potential use for high speed communications over medium (15/50 kV) and low (110/220 V) voltage power lines [5]. However, there are still several technical problems and regulatory issues that are unresolved. Moreover, a comprehensive theoretical and practical approach for PLC is still missing and there are only a few general results on the ultimate performance that can be achieved over the power line channel. As a result, commercially deployable, high speed, long distance PLC still requires further research efforts despite the fact that PLC might provide an alternative cost-effective solution to the last mile connectivity problem. In the following, we explain both advantages and disadvantages of power line communication technologies for automation applications.

3.1.1. Advantages

- *Extensive coverage*: PLC can provide an extensive coverage, since the power lines are already installed almost everywhere. This is advantageous especially for substations in rural areas where there is usually no communication infrastructure.
- *Cost*: The communication network can be established quickly and cost-effectively because it utilizes the existing wires to carry the communication signals. Thus, PLC can offer substations new cost-saving methods for remotely monitoring power uses and outages.

3.1.2. Disadvantages

- *High noise sources over power lines*: The power lines are noisy environments for data communications due to several noise sources such as electrical motors, power supplies, fluorescent lights and radio signal interferences [27]. These noise sources over the power lines can result in high bit error rates during communication which severely degrade the performance of PLC.
- *Capacity*: New technological advances have recently enabled a prototype communication modem which achieves a maximum total capacity of 45 Mbps in PLC [1]. However, since power line is a shared medium, the average data rate per end user will be lower than the total capacity depending on coincident utilization, i.e., the number of users on the network at the same time and the applications they are using. Thus, possible technical problems should be comprehensively addressed with various field tests before the PLC technology is widely deployed.
- *Open circuit problem*: Communication over the power lines is lost with devices on the side of an open circuit [14]. This fact severely restricts the usefulness of PLC for applications especially involving switches, reclosers and sectionalizers.
- *Signal attenuation and distortion*: In power lines, the attenuation and distortion of signals are immense due to the reasons such as physical topology of the power network and load impedance fluctuation over the power lines. In addition, there is significant signal attenuation at specific frequency bands due to wave reflection at the terminal points [12]. Therefore, the communication over power lines might be lost due to high signal attenuation and distortion.
- *Security*: There are some security concerns for PLC arising from the nature of power lines [22]. Power cables are not twisted and use no shielding which means power lines produce a fair amount of Electro Magnetic Interference (EMI). Such EMI can be received via radio receivers easily. Therefore, the proper encryption techniques must be used to prevent the interception of critical data by an unauthorized person.
- *Lack of regulations for broadband PLC*: In addition to technical challenges, fundamental regulation issues of PLC should be addressed for substantial progress to be made. The limits of transmitted energy and frequencies employed for PLC should be determined in order to both provide broadband PLC and prevent the interference with already established radio signals such as mobile communications, broadcasting channels and military communications. In this respect, the Institute of Electrical and Electronics Engineers (IEEE) has started to develop a standard to support broadband communications

over power lines [18]. The standard is targeted for completion in mid 2006.

3.2. Satellite communication

Satellite communication can offer innovative solutions for remote control and monitoring of substations. It provides an extensive geographic coverage, and thus, can be a good alternative communication infrastructure for electric system automation in order to reach remote substations where other communication infrastructures such as telephone or cellular networks might not exist. In practical applications, Very Small Aperture Terminal (VSAT) satellite services are already available that are especially tailored for remote substation monitoring applications [33]. Furthermore, with the latest developments in electric system automation, satellite communication is not only used for remote control and monitoring of substations but also used for Global Positioning System (GPS) based time synchronization, which provides microsecond accuracy in time synchronization [38]. In addition, satellites can be used as a backup for the existing substations communication network. In case of congestion or link failures in communication, critical data traffic can be routed through satellites [8]. In the following, we present both advantages and disadvantages of satellite communication technologies.

3.2.1. Advantages

- *Global coverage*: Satellite communication supports a wide geographical coverage (including remote, rural, urban and inaccessible areas) independent of the actual land distance between any pair of communicating entities. In case no communication infrastructure exists, especially for remote substations, satellite communication provides a cost-effective solution.
- *Rapid installation*: Satellite communication offers clear advantages with respect to the installation of wired networks. A remote substation can join a satellite communication network by only acquiring the necessary technical equipment without the need for cabling to get high-speed service [20]. Cabling is not a cost-effective nor a simple job when the substation is located in a remote place. Due to economical reasons, some utilities have already installed satellite communication for rural substations monitoring [33].

3.2.2. Disadvantages

- *Long delay*: The round-trip delay in satellite communication, especially for Geostationary Earth Orbit (GEO) satellites,[1] is substantially higher than that of terrestrial communication links. The transport protocols developed for terrestrial communication links such as TCP are not suitable for satellite communication, since necessary data rate adjustments of TCP can take a long time in high-delay networks such as satellite networks [16]. On the other hand, it is possible to reduce the round-trip delay by using satellites in lower orbits. Particularly, LEO satellites offer significantly reduced delay, which is comparable to that of terrestrial networks.
- *Satellite channel characteristics*: Different from cabled and terrestrial network communications, satellite channels characteristics vary depending on the weather conditions and the effect of fading, which can heavily degrade the performance of the whole satellite communication system [16]. Therefore, these communication challenges should be taken into account while evaluating the communication technologies for electric system automation.
- *Cost*: Although satellite communication can be a cost-effective solution for remote substations if any other communication infrastructure is not available, the cost for operating satellites (the infrastructure cost and monthly usage cost) for all substation communication networks is still higher than that of other possible communication options. High initial investment for satellite transceivers is one of the limitations of satellite communication.

3.3. Optical fiber communication

Optical fiber communication systems, which were first introduced in the 1960s, offer significant advantages over traditional copper-based communication systems. In electric system automation, an optical fiber communication system is one of the technically attractive communication infrastructures, providing extremely high data rates. In addition, its Electro Magnetic Interference (EMI) and Radio Frequency

[1] Satellites can be classified into Geostationary Earth Orbit (GEO) satellite, Middle Earth Orbit (MEO) satellite, Low Earth Orbit (LEO) satellite according to the orbit altitude above the earth's surface [9].

Interference (RFI) immunity characteristics make it an ideal communication medium for high voltage operating environment in substations [14]. Furthermore, optical fiber communication systems support long distance data communication with less number of repeaters[2] compared to traditional wired networks. This leads to reduced infrastructure costs for long distance communication that substation monitoring and control applications demand. For example, the typical T-1 or coaxial communication system requires repeaters about every 2 km whereas optical fiber communication systems require repeaters about every 100–1000 km [13].

Although optical fiber networks have several technical advantages compared to other wired networks, the cost of the optical fiber itself is still expensive to install for electric utilities. However, the enormous bandwidth capacity of optical fiber makes it possible for substations to share the bandwidth capacity with other end users which significantly helps to recover the cost of the installation. In this respect, optical fiber communication systems might be cost-effective in the high speed communication network backbone since optical fibers are already widely deployed in communication network backbones and the cost is spread over a large number of users. As a result, fiber optic networks can offer high performance and highly reliable communication when strict QoS substations communication requirements are taken into account. In the following, we describe both advantages and disadvantages of optical fiber communication for automation applications.

3.3.1. Advantages

- *Capacity*: Extremely high bandwidth capacity of optical fiber communication can provide high performance communication for automation applications. Current optical fiber transmission systems provide transmission rates up to 10 Gbps using single wavelength transmission and 40 Gbps to 1600 Gbps using wavelength division multiplexing[3] (WDM). In addition, very low bit error rates (BER $= 10^{-15}$) in fiber optic communication are observed. Due to high bandwidth capacity and low BER characteristics, optical fiber is used as the physical layer of Gigabit and 10 Gigabit ethernet networks.
- *Immunity characteristics*: Optical fibers do not radiate significant energy and do not pick up interference from external sources [13]. Thus, compared to electrical transmission, optical fibers are more secure from tapping and also immune to EMI/RFI interference and crosstalk.

3.3.2. Disadvantages

- *Cost*: Although fiber optic networks possess several technical advantages, the cost of its installation might be expensive in order to remotely control and monitor substations. However, fiber optic networks might be a cost-effective communication infrastructure for high speed communication network backbones, since optical fibers are already widely deployed in the communication network backbones and the cost is spread over a large number of users.

3.4. Wireless communication

Several wireless communication technologies currently exist for electric system automation [14]. When compared to conventional wired communication networks, wireless communication technologies have potential benefits in order to remotely control and monitor substations, e.g., savings in cabling costs and rapid installation of the communication infrastructure. On the other hand, wireless communication is more susceptible to Electro Magnetic Interference (EMI) and often has limitations in bandwidth capacity and maximum distances among communication devices. Furthermore, since radio waves in wireless communication spread in the air, eavesdropping can occur and it might be a threat for communication security. Electric utilities exploring wireless communication options have two choices; (i) utilizing an existing communication infrastructure of a public network, e.g., public cellular networks, (ii) installing a private wireless network.

Utilizing an existing communication infrastructure of a public network might enable a cost-effective solution due to the savings in required initial investment for the communication infrastructure. On the other hand, private wireless networks enable

[2] In long distance communications, it is necessary to introduce repeaters periodically in order to compensate for the attenuation and distortion of the communication signals.

[3] Wavelength division multiplexing (WDM) is an effective approach to exploit the bandwidth capacity available in optical fiber. In WDM, multiple wavelengths are used to carry several data streams simultaneously over the same fiber.

electric utilities to have more control over their communication network. However, private wireless networks require a significant installation investment as well as the maintenance cost [14]. In electric system automation, wireless communication technology has already been deployed. Recently, Short Message Service (SMS) functionality of the digital cellular network has been applied in order to remotely control and monitor substations [34]. The control channel of the cellular network is also utilized in some alarm-based substation monitoring cases [23]. However, both of these communication technologies are suited to the applications that send a small amount of data and thus, they can not provide the strict Quality of Service (QoS) requirements that real time substation monitoring applications demand. In the following, we describe both advantages and disadvantages of wireless communication technologies.

3.4.1. Advantages

- *Cost*: Utilizing an existing wireless communication network, e.g., cellular network, might enable a cost-effective solution due to the savings in required initial investment for the communication infrastructure. In wireless communication, cabling cost is also eliminated.
- *Rapid installation*: The installation of wireless communication is faster than that of wired networks. Wireless communication provides more flexibility compared to wired networks. Within radio coverage, communication entities can start to communicate after a short communication infrastructure installation.

3.4.2. Disadvantages

- *Limited coverage*: Private wireless networks provide a limited coverage, e.g., the coverage of IEEE 802.11b is approximately 100 m [21]. On the other hand, utilizing existing public wireless network, e.g. cellular network, or WiMAX technology can support much more extensive coverage compared to wireless local area networks. However, some geographical areas, e.g., remote rural locations, may still not have any wireless communication services.
- *Capacity*: Wireless communication technologies provide typically lower QoS compared to wired communication networks. Due to limitations and interference in radio transmission, a limited bandwidth capacity is supported and high bit error rates ($BER = 10^{-2}$–10^{-6}) are observed in communication. In addition, since wireless communication is in a shared medium, the application average data rate per end user is lower than the total bandwidth capacity, e.g., maximum data rate of IEEE 802.11b is 11 Mbps while the average application data rate is approximately 6 Mbps [21]. Therefore, each level in the communication protocol stack should adapt to wireless link characteristics in an appropriate manner, taking into account the adaptive strategies at the other layers, in order to optimize network communication performance.
- *Security*: Wireless communication poses serious security challenges since the communication signals can be easily captured by nearby devices. Therefore, efficient authentication and encryption techniques should be applied in order to provide secure communication.

Note that with the recent advances in wireless communications and digital electronics, hybrid network architectures have enabled alternative scalable wireless communication systems, which can provide strict quality of service (QoS) requirements of automation applications. The details of these recent wireless technologies, i.e., wireless sensor networks, WiMAX and wireless mesh networks, are described in the following sections.

4. Wireless sensor networks for automation

In this section, we explain the opportunities and challenges of wireless sensor networks (WSNs) and present design objectives and requirements of WSNs for electric system automation applications. In general, wireless sensor networks are composed of a large number of low cost, low power and multifunctional sensor nodes that are small in size and communicate un-tethered over short distances [4]. The ever-increasing capabilities of these tiny sensor nodes enable capturing various physical information, e.g., noise level, temperature, vibration, radiation, etc., as well as mapping such physical characteristics of the environment to quantitative measurements. The collaborative nature of WSNs brings several advantages over traditional sensing including greater fault tolerance, improved accuracy, larger coverage area and extraction of localized features. In this respect, wireless sensor networks enable low cost and low power wireless

communication for electric system automation applications, especially in urban areas.

Furthermore, in the area of electric utility measurement systems, WSNs are used in wireless automatic meter reading (WAMR) systems, which can determine real-time energy consumption of the customers accurately. WAMR systems are important for electric utilities, since they can reduce operational costs and enable remotely controlled flexible management systems based on real-time energy consumption statistics. Therefore, WSNs provide an alternative real-time monitoring system for electric utilities with the potential to improve business performance and technical reliability of various electric utility operations.

In WSNs, the architecture of the network depends on the purpose of the application. Based on the application requirements, the sensor nodes are scattered in a sensor field as shown in Fig. 5. Each of these scattered sensor nodes has the capability to collect data and route data back to the sink node in a multi-hop manner [3]. In this architecture, the role of the sink node is to monitor the overall network and to communicate with the task manager, e.g., control center in the power utility, in order to decide the appropriate actions. The sink node can communicate with the task manager via Internet or satellite.

4.1. Benefits of wireless sensor networks for automation

Wireless Sensor Network (WSN) technology has created new communication paradigms for real-time and reliable monitoring requirement of the electric systems. Some of the benefits that can be achieved using WSN technology are highlighted as follows:

- *Monitoring in harsh environments*: The sensors in WSNs are rugged, reliable, self-configurable and unaffected by extreme ambient conditions, e.g., temperature, pressure, etc. Thus, WSNs can operate even in harsh environments and eliminate the cabling requirement in electric systems.
- *Large coverage*: WSNs can contain a large number of physically separated sensor nodes that do not require human intervention. Although the coverage of a single sensor node is small, densely distributed sensor nodes can work simultaneously and collaboratively so that the coverage of the whole network is extended. Therefore, the coverage limitations of traditional sensing systems can be addressed efficiently.
- *Greater fault tolerance*: The dense deployment of sensor nodes leads to high correlation in the sensed data. The correlated data from neighboring sensor nodes in a given deployment area makes WSNs more fault tolerant than conventional sensor systems. Due to data redundancy and the distributed nature of WSNs, adequate monitoring information can be transported to the remote control center even in the case of sensor and route failures.
- *Improved accuracy*: The collective effort of sensor nodes enables accurate observation of the physical phenomenon compared to traditional monitoring systems [17]. In addition, multiple sensor types in WSNs provide the capability of monitoring various physical phenomena in the electric system.

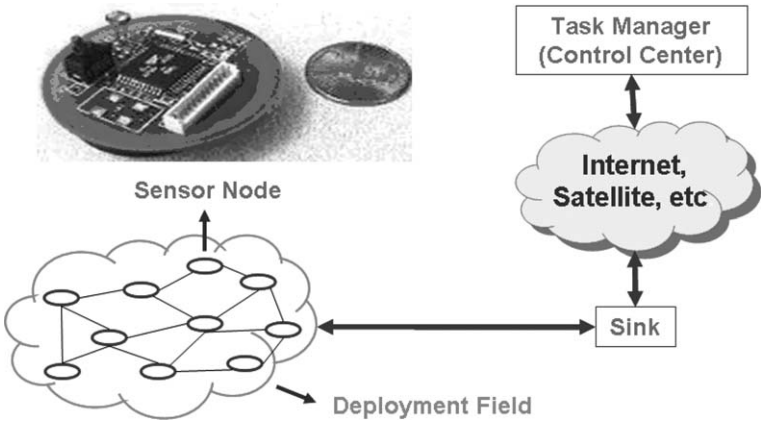

Fig. 5. An illustrated architecture of wireless sensor networks.

- *Efficient data processing*: Instead of sending the raw data to the remote control center directly, sensor nodes can locally filter the sensed data according to the application requirements and transmit only the processed data. Thus, only necessary information is transported to the remote control center and communication overhead can be significantly reduced.
- *Self configuration and organization*: The sensor nodes in WSNs can be rapidly deployed and dynamically reconfigured because of the self-configuration capability of the sensor nodes. The ad hoc architecture of WSNs also overcomes the difficulties raised from the predetermined infrastructure requirements of traditional communication networks. More specifically, new sensor nodes can be added to replace failed sensor nodes in the deployment field and existing nodes can also be removed from the system without affecting the general objective of the monitoring system of the electric utility.
- *Lower cost*: WSNs are expected to be less expensive than conventional monitoring systems, because of their small size and lower price as well as the ease of their deployment.

4.2. Wireless sensor network applications for automation

WSN technology can enhance the performance of electric utility operations by enabling wireless automatic meter reading and real-time and reliable monitoring systems for electric utilities. In the following, WSN applications for electric system automation are described in detail.

4.2.1. Wireless automatic meter reading (WAMR)

Currently, traditional manual electricity meter reading is the most common method for the electric utilities. These systems require visual inspection of the utility meters and do not allow flexible management systems for the electric utilities. In addition, network connections between traditional meters and data collection points are basically non-existent; thus, it is impossible to implement a remotely controlled flexible management system based on energy consumption statistics by using traditional measurement systems.

With the recent advances in Micro Electro-Mechanical Systems (MEMS) technology, wireless communications and digital electronics; the development of low cost smart sensor networks, that enable wireless automatic meter reading (WAMR) systems, has become feasible. As the de-regulation and competition in the electric utility marketplace increase, so does the importance of WAMR systems. Wireless collection of electric utility meter data is a very cost-effective way of gathering energy consumption data for the billing system and it adds value in terms of new services such as remote deactivation of a customer's service, real-time price signals and control of customers' applications. The present demand for more data in order to make cost-effective decisions and to provide improved customer service has played a major role in the move towards WAMR systems.

WAMR systems offer several advantages to electric utilities including reduced electric utility operational costs by eliminating the need for human readers and real-time pricing models based on real-time energy consumption of the customers. Real-time pricing capability of WAMR systems can also be beneficial for the customers. For example, using the real-time pricing model, the electric utility can reward the customers shifting their demand to *off-peak* times. Therefore, the electric utility can work with customers to shift loads and manage prices efficiently by utilizing WAMR systems instead of once a month on-site traditional meter reading.

However, the real-time pricing model of electric utilities requires reliable two-way communication between the electric utility and customer's metering equipment. WSN technology addresses this requirement efficiently by providing low cost and low power wireless communication. In Fig. 6, a wireless automatic meter reading system using sensor network technology is illustrated. As shown in Fig. 6, the sensed data from the meter is collected by the utility control center through multi-hop wireless communication. This monitoring system can also provide flexibility to the electric utility so that utility personnel or mobile utility controller can monitor the system locally when it is required, e.g., in case of alarm situations.

In summary, wireless automatic meter reading systems can provide the following functionalities for electric systems:

- *Automatic meter reading functionalities*: WSNs enable real-time automatic measurement of energy consumption of the customers. The

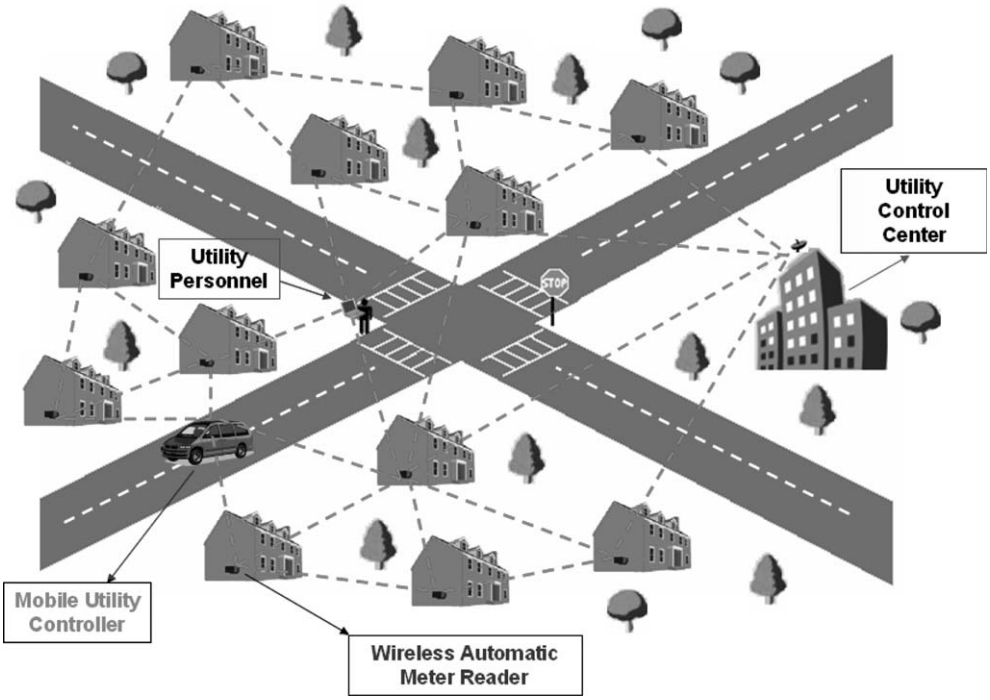

Fig. 6. An illustration of WAMR system using wireless sensor network technology.

automatic meter measurements can also be classified as individual meter measurements, cluster meter measurements and global meter measurements. Here, the objective is to provide flexible management policies with different real-time monitoring choices for electric utilities.

- *Telemetry functionalities*: The electric utility control centers can obtain real-time data from smart sensor nodes and control some elements located at selected points of the distribution network, e.g. control of the status of the switches [25]. Thus, distributed sensing and automation enhance electric utility services by reducing failure and restoration times.
- *Dynamic configuration functionality*: In electric system automation applications, reliability of the measurements should be ensured even in case of route failures in the network [31]. Thus, it is extremely significant to dynamically adjust the configuration of the network, e.g., dynamic routing, in order to provide reliability requirements of the applications. In this respect, the self-configuration capability of WSNs enables dynamic reconfiguration of the network.
- *Status monitoring functionality*: Monitoring the status of the metering devices, which are embedded by smart sensors, is another functionality of WAMR systems. This functionality can be very helpful to determine sensor node failures in the network accurately and timely. In addition, status monitoring functionality can be utilized in case of tampering with metering devices. For example, if someone tries to vandalize a metering device, the system can notify the police automatically [24]. This reduces the considerable costs of sending service crews out to repair vandalized metering devices.

As advances in WAMR technologies continue, these systems will become less expensive and more reliable. Most utility and billing companies have recognized that with the invention of low-cost, low power radio sensors, wireless RF communication is, by far, the most cost-efficient way to collect utility meter data.

4.2.2. Electric system monitoring

Equipment failures, lightning strikes, accidents, and natural catastrophes all cause power disturbances and outages and often result in long service interruptions. Thus, the electric systems should be properly controlled and monitored in order to take

the necessary precautions in a timely manner [36]. In this respect, wireless sensor networks (WSNs) can a provide cost-effective reliable monitoring system for the electric utilities [29]. An efficient monitoring system constructed with smart sensor nodes can reduce the time for detection of the faults and resumption of electric supply service in distribution networks.

In addition, electricity regulators monitor the performance of the electricity distribution network operators utilizing a range of indices relating to customer service. Distribution network operators have targets and incur penalties based on the length of time of service interruptions, i.e., both outage frequency and duration [30]. Continuity of electricity service is also crucial in today's competitive electric utility marketplace from the perspective of customer satisfaction.

In order to evaluate the performance of the electric system, several Quality of Service (QoS) indices can be obtained utilizing WSN technology. For example, average duration of service interruption and average repair time can be computed. Typically, for densely deployed urban areas, these performance indices are correlated with the time for remote or manual switching of supply circuits. In this context, smart sensor nodes deployed in the electric utility can provide rapid identification of service interruptions and timely restoration of the electric utility services. Therefore, WSNs can help electric utilities maintain regulatory targets for the performance indices.

4.3. Wireless sensor network design considerations

When wireless sensor network technology for electric system automation applications is considered, there exist two key design elements which are critical to develop cost-effective wireless sensor network to support both existing functionalities and new operational requirements of the future electric systems. These key elements are described in the following.

4.3.1. Network topology and architecture requirements

The topology of a sensor network has significant implications on several network aspects, including network lifetime, routing algorithms, communication range of the sensor nodes and etc. The network architecture requirements contain the physical and logical organization of the network as well as the density of the sensor nodes. In general, the objective of sensor networks is to efficiently cover the deployment area. The logical and hierarchical organization of the network also impacts energy consumption and the selection of communication protocols. In addition, based on topology requirements, sensor networks can have a distributed organization or a clustered organization, where selected nodes can handle data forwarding. The network topology and architecture requirements for electric utilities can be determined by answering the following questions:

- What type of network topology best fits the application? (Is it one to one, one to many, many to one or many to many?)
- How will the monitoring network work? (Is it master–slave, point-to-point, point-to multipoint or peer to peer?)
- What are the worst case ambient conditions in the coverage area?
- How many substations should be controlled and monitored including both current and future requirements of the electric system?
- Are there any known potential interference problems due to physical obstructions, RF interference from power lines or large induction motors?

4.3.2. Application requirements

The required information that is to be relayed through the sensor network for electric utilities should be classified and quantified [2]. These requirements can be achieved by a comprehensive analysis of the electric system automation applications. Based on the application requirements, the properties of individual sensor nodes can also be identified which impact network modelling and communication protocol choices. The following questions can help electric utilities to determine these requirements:

- What are the QoS requirements of the application? (Does it require real-time monitoring or delay tolerant monitoring?)
- Does the system continuously poll for the information (periodic monitoring) or is it generated by exception (event-based monitoring)?
- What is the type of the sensor data, i.e., video, voice, data?

As a result, electric utilities should determine the network topology, architecture and application requirements comprehensively in order to establish the *best fit* wireless sensor network for their applications. Full consideration of the different sensor network options and how will they fit the electric utility application is critical for a successful implementation.

4.4. Design challenges of wireless sensor networks

Although WSNs bring significant advantages over traditional communication networks, the properties of WSNs also impose unique communication challenges. These challenges can be described as follows:

- *Limited resources*: The design and implementation of WSNs are constrained by three types of resources: (i) energy, (ii) memory and (iii) processing. Constrained by the limited physical size, sensor nodes have limited battery energy supply [15]. For this reason, communication protocols for WSNs are mainly tailored to provide high energy efficiency. It is also important to note that in electric systems, the batteries of the sensors can be charged by the appropriate energy supplies. In addition, the collaborative effort of sensor nodes can handle the problems of limited memory and processing capabilities of the sensor nodes.
- *Dynamic topologies and environment*: The topology and connectivity of the network may vary due to route and sensor node failures. Furthermore, the environment, that sensor nodes monitor, can change dramatically, which may cause a portion of sensor nodes to malfunction or render the information they gather obsolete. Thus, the developed communication protocols for WSNs should accurately capture the dynamics of the network [35].
- *Quality of service concerns*: The quality of service (QoS) provided by WSNs refers to the accuracy between the data reported to the control center and what is actually occurring in the environment. In addition, since sensor data are typically time sensitive, e.g., alarm notifications for the electric utilities, it is important to receive the data at the control center in a timely manner. Data with long latency due to processing or communication may be outdated and lead to wrong decisions in the monitoring system. Therefore, the developed communication protocols for WSNs should address both real-time and reliable communication simultaneously.

5. WiMAX and wireless mesh networks for automation

Recall that the proposed hybrid network architecture consists of various types of networks including Internet VPN, wireless sensor networks, WiMAX and wireless mesh networks. In the previous sections, we described the details of Internet VPN technologies (see Section 2) and wireless sensor networks (see Section 4) for electric utilities. In this section, we focus on wireless mesh networks and WiMAX technology for electric system automation applications.

In Fig. 7, an illustration of the hybrid network architecture utilizing WiMAX technology and wireless mesh networks is shown. In this hybrid architecture, a set of electric utility subscribers is clustered into wireless mesh domains, where each domain has a smaller dimension compared to the global network. Hence, each wireless mesh domain can be easily managed by the centralized communication entities, which are called as local control centers. Furthermore, in this architecture, each wireless mesh cluster is monitored by a remote control center using WiMAX. Therefore, with the integration of wireless mesh networks and WiMAX, electric utilities can fully exploit the advantages of multiple wireless networks. The main components of the proposed hybrid network architecture are briefly described as follows:

- *Wireless mesh domains*: In the proposed hybrid network architecture, wireless mesh domains constitute a fully connected wireless network among each electric utility subscriber. Different from traditional wireless networks, each wireless mesh domain is dynamically self-organized and self-configured. In other words, the nodes in the mesh network automatically establish and maintain network connectivity. This feature brings many advantages for electric utilities, such as low up-front cost, easy network maintenance, robustness, and reliable service coverage. In addition, with the use of advanced radio technologies, e.g., multiple radio interfaces and smart antennas, network capacity can be increased significantly. Moreover, the gateway and bridge

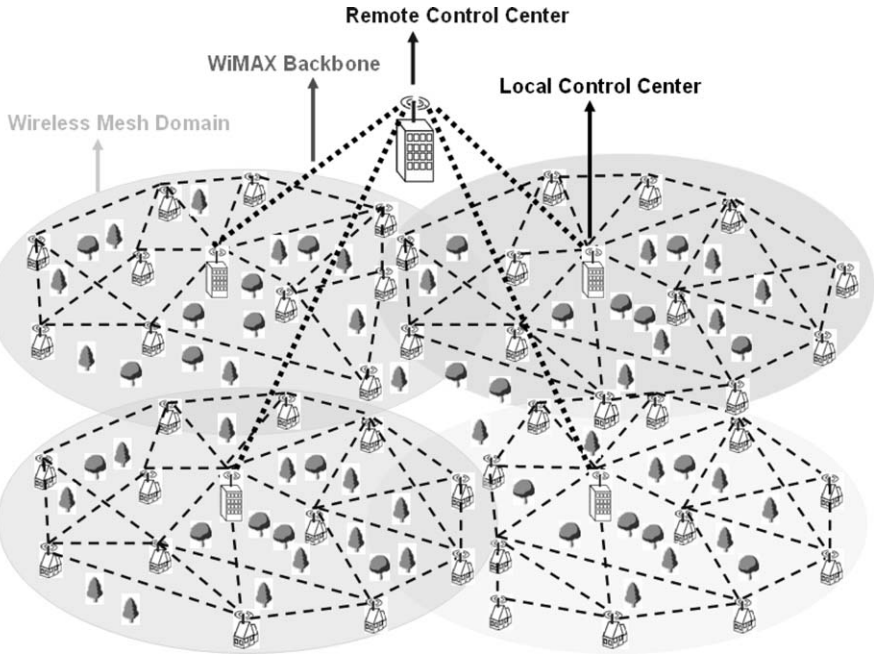

Fig. 7. An illustration of hybrid network architecture using WiMAX and wireless mesh networks.

functionalities in mesh routers enable the integration of wireless mesh domains with various existing wireless networks such as wireless sensor networks, wireless-fidelity (Wi-Fi), and WiMAX [3]. Consequently, through an integrated wireless mesh network, electric utilities can take the advantage of multiple wireless networks.

- *WiMAX backbone*: The necessary long distance communication (up to 31 miles) between local control centers and a remote control center is provided utilizing worldwide inter-operability for microwave access (WiMAX) technology. With the integration of WiMAX technology, the capacity of the network backbone can be increased up to 75 Mbps. In addition, WiMAX offers a standardized communication technology for point-to-multipoint wireless networks, i.e., IEEE 802.16 standard [37]. This enables interoperability between different vendor products, which is another important concern for electric utilities. Furthermore, different from traditional point-to-multipoint networks, WiMAX technology also supports non-line of sight communication. Hence, electric systems suffering from environmental obstacles can benefit from WiMAX technology to improve the performance of their communication system. WiMAX technology, particularly the IEEE 802.16e standard [37], also focuses on low latency handoff management, which is necessary for communications with users moving at vehicular speeds.

5.1. Benefits of hybrid network architecture using WiMAX and wireless mesh networks

With the recent advances in wireless communications and digital electronics, hybrid network architectures have enabled alternative scalable wireless communication systems, which can provide strict quality of service (QoS) requirements of electric system automation applications in a cost-effective manner. Some of the benefits of hybrid network architectures are highlighted as follows:

- *Increased reliability*: In wireless mesh domains, the wireless backbone provides redundant paths between the sender and the receiver of the wireless connection. This eliminates single point failures and potential bottleneck links within the mesh domains, resulting in significantly increased communications reliability [3]. Network robustness against potential problems, e.g., node failures, and path failures due to RF interferences or obstacles, can also be ensured by the existence

of multiple possible alternative routes. Therefore, by utilizing WMN technology, the network for electric utilities can operate reliably over an extended period of time, even in the presence of a network element failure or network congestion.

- *Low installation costs*: Recently, the main effort to provide wireless connection to the end-users is through the deployment of 802.11 based Wi-Fi Access Points (APs). To assure almost full coverage in a metro scale area for electric system automation, it is required to deploy a large number of access points because of the limited transmission range of the APs. The drawback of this solution is highly expensive infrastructure costs, since an expensive cabled connection to the wired Internet backbone is necessary for each AP. Installation of the required cabling infrastructure significantly increases the installation costs as well as it slows down the implementation of the wireless network. As a result, the deployment of APs for wireless Internet connection is costly and unscalable for electric system automation applications. On the other hand, constructing a wireless mesh network decreases the infrastructure costs, since the mesh network requires only a few points of connection to the wired network. Hence, WMNs can enable rapid implementation and possible modifications of the network at a reasonable cost, which is extremely important in today's competitive electric utility environment.
- *Large coverage area*: Currently, the data rates of wireless local area networks (WLANs) have been increased, e.g., 54 Mbps for 802.11a and 802.11g, by utilizing spectrally efficient modulation schemes. Although the data rates of WLANs are increasing, for a specific transmission power, the coverage and connectivity of WLANs decreases as the end-user becomes further from the access point. On the other hand, WiMAX technology enables long distance communication between local control centers and a remote control center without any performance degradation. As a result, the WiMAX backbone in the hybrid network can realize high speed long distance communication that automation applications demand.
- *Automatic network connectivity*: In the proposed hybrid network architecture, wireless mesh domains are dynamically self-organized and self-configured. In other words, the nodes in the mesh network automatically establish and maintain network connectivity, which enables seamless multi-hop interconnection service for the electric utilities. For example, when new nodes are added into the network, these nodes utilize their meshing functionalities to automatically discover all possible routers and determine the optimal paths to the control centers [3]. Furthermore, the existing mesh routers reorganize the network considering the newly available routes and hence, the network can be easily expanded. The self-configuration feature of wireless mesh networks is so crucial for electric system automation applications, since it enables electric utilities to cope with new connectivity requirements driven by customer demands.

5.2. Design challenges of hybrid architecture using WiMAX and wireless mesh networks

Hybrid network architectures can provide an economically feasible solution for the wide deployment of high speed wireless communications for electric system automation applications. Some companies already have some products for sale and have started to deploy wireless mesh networks and WiMAX towers for various application scenarios. However, field trials and experiments with existing communication protocols show that the performance of hybrid network architectures is still far below what they are expected to be [3]. Therefore, there is a need for the development of novel communication protocols for hybrid network architectures and thus, many open research issues need to be resolved. Some of these research issues are described as follows:

- *Harsh monitoring environment*: In substations, wireless links exhibit widely varying characteristics over time and space due to obstructions and extremely noisy environment caused by power lines and RF interferences. To improve network capacity and limit radio interferences, advanced radio technologies, such as multiple-input multiple output (MIMO) techniques, multiple radio interfaces and smart antennas, should be exploited while developing communication protocols.
- *Optimal placement of WiMAX towers*: In the proposed hybrid architecture, it is important to design an efficient and low cost network

infrastructure, while meeting the deadlines of the time-critical monitoring data. Thus, the WiMAX towers, equipped with expensive RF hardware, should be optimally placed in the deployment field in order to both reduce infrastructure costs and meet QoS requirements.

- *Mobility support*: Low latency handover management algorithms are required to support the communication services of mobile utility controllers. This way, mobile utility controllers can also monitor the system locally, when it is necessary, e.g., in case of alarm situations.
- *Integration of heterogeneous networks*: Existing networking technologies have limited capabilities of integrating different wireless networks. Thus, to increase the performance of the hybrid network architectures, the integration capabilities of multiple wireless interfaces and the corresponding gateway/bridge functions of network routers should be improved.
- *Scalability*: In today's competitive dynamic market environment, electric utilities might be able to deploy new substations and provision large service requests rapidly. In this respect, the designed hybrid network architecture should scale well to accommodate new communication requirements driven by customer demands.
- *Coordinated resource management*: Distributive and collaborative network resource management is required to effectively respond to system changes due to wireless channel characteristics, contention and traffic patterns. This way, system-wide fairness and self-configuration of the network can be realized.
- *Security*: Denial of service attacks in the network may cause severe damage to the operation of the deployed hybrid network. Using efficient encryption and cryptography mechanisms, security problems can be solved.

To solve all of these existing problems of hybrid network architectures, the protocol stack from physical to application layers needs to be improved or re-invented. In this regard, a *cross-layer design* is required to jointly optimize the main networking functionalities and to design communication protocol suites that are adaptive to the dynamic characteristics of the wireless channel. This way, the hybrid network architecture can provide rapid identification of service interruptions and timely restoration of the electric utility services.

6. Conclusion

Electric utilities, especially in urban areas, continuously encounter the challenge of providing reliable power to the end-users at competitive prices. Equipment failures, lightning strikes, accidents, and natural catastrophes all cause power disturbances and outages and often result in long service interruptions. In this regard, electric system automation, which is the creation of a highly reliable, self-healing electric system that rapidly responds to real-time events with appropriate actions, aims to maintain uninterrupted power services to the end-users. However, the operational and commercial demands of electric utilities require a high-performance data communication network that supports both existing functionalities and future operational requirements. Therefore, the design of a cost-effective and reliable network architecture is crucial.

As the individual communication capabilities and locations of electric systems are taken into account, it is appropriate to consider the overall communication infrastructure as a hybrid network architecture. This hybrid network architecture consists of various types of networks such as Internet, wireless sensor networks, WiMAX and wireless mesh networks. In this hybrid architecture, the communication network can be dynamically self-configured. This brings significant advantages for electric utilities, such as low up-front cost, easy network maintenance, robustness, and reliable service coverage. Furthermore, with the integration of different networks, electric utilities can fully exploit the advantages of multiple wireless networks. For example, while low power and low range wireless sensor networks can be utilized for urban areas, WiMAX technology, which enables reliable long distance communication, can be used for rural areas. As a result, the proposed hybrid network architecture enables a fully connected communication network for electric system automation applications, such as real-time grid and equipment monitoring and wireless automatic meter reading systems.

In this paper, the opportunities and challenges of hybrid network architecture are discussed for electric system automation applications. More specifically, Internet based Virtual Private Networks, power line communications, satellite communications and wireless communications (wireless sensor

networks, WiMAX, wireless mesh networks) are described in detail. The motivation of this paper is to provide a better understanding of the hybrid network architecture that can provide heterogeneous electric system automation application requirements. Consequently, our aim is to present a structured framework for electric utilities who plan to utilize new communication technologies for automation and hence, to make the decision-making process more effective and direct. Based on our comprehensive research, we make the following recommendations for the electric utilities:

- *Internet-ready IEDs*: Recent advances in digital electronics and communication technology have enabled the development of Internet-ready Intelligent Electronic Devices (IEDs). International standards are being developed (IEC 61850) to promote rapid configuration and integration into the utility automation system [19]. Integrating these IEDs into electric systems can offer various benefits, e.g., remote access to IED/relay configuration ports, diagnostic event information, and video for security or equipment status assessment. To make sure these benefits are fully exploited, there is a need for the appropriate digital simulators in order to test and evaluate the performance of multi-vendor IEDs and make more informed decisions.
- *Novel communications protocols*: Although the hybrid network architecture offers many opportunities for electric utilities, field trials and experiments with existing communication protocols show that the performance of hybrid network architecture is still far below what they are expected to be. Therefore, there is a need for the development of novel communication protocols for hybrid network architectures and thus, many open research issues, such as coordinated network management, security, mobility support, integration of heterogeneous networks, need to be resolved.
- *Cost vs. benefit analysis*: While providing communication requirements of automation applications, the hybrid network architecture should enable rapid implementation and possible modifications of the electric utility network. In this regard, the cost of the network should also be considered in order to make it feasible subject to budget constraints of the electric utilities. Hence, a detailed cost vs. benefit analysis is required to evaluate the performance of the hybrid network architecture.
- *Wireless communications technologies*: Wireless communications technologies (WiMAX, wireless sensor networks, wireless mesh networks) should be developed for deployment in electric system automation applications (see Sections 4 and 5). WiMAX is expected to become commercial in 2007–2008 and brings several advantages, such as mobility support and large coverage area. Wireless sensor networks and wireless mesh networks are under development and offer electric utilities low installation costs, increased reliability and self-configuration.
- *Power line communications technologies*: Power line communications (PLC) technologies should be developed for deployment in electric system automation applications. PLC has become important in recent years due to developments in technology, which enable PLC's potential use for medium and high speed communications over medium (15/35 kV) and low (120/240 V) voltage power lines. However, there are still several technical problems and regulatory issues that are unresolved (see Section 3.1). Moreover, a comprehensive theoretical and practical approach for PLC is still missing and there are only few general results on the ultimate performance that can be achieved over the power line channel. As a result, commercially deployable, high speed, long distance PLC still requires further research efforts. International standards are also needed for building power system applications and customer services on top of PLC technologies.

Acknowledgements

The authors would like to thank Tom Weaver, James Bales, Doug Fitchett, Eric Rehberg, Ray Hayes (AEP); Brian Deaver (Baltimore Gas & Electric); Dan Landerman (Cooper Power Systems); Brad Black, Shawn Ervin, Jeff Daugherty (Duke Power); Jerry Bernstein (Entergy), Wayne Zessin, Mark Browning (Exelon); Pat Patterson, Martin Gordon (NRECA); Mark Gray, Bill Robey (PEPCO); David White (South Carolina Electric & Gas); Brian Dockstader (Southern California Edison); Larry Smith, Bob Cheney, Mac Fry, Bob Reynolds (Southern Company), Joe Rostron (Southern States); Frank Daniel (TXU) for their valuable comments that improved the quality of this

paper. This work was supported by NEETRAC under Project #04-157.

References

[1] Y. Abe et al., Development of high speed power line communication modem, SEI Technical Review 58 (June) (2004) 28–33.
[2] J. Adam et al., EHT control systems and wireless communications: the wave of the future, in: IEEE Industry Applications Society Petroleum and Chemical Industry Conference, September 2001, pp. 169–178.
[3] I.F. Akyildiz, X. Wang, W. Wang, Wireless mesh networks: a survey, Computer Networks Journal (March) (2005).
[4] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: a survey, Computer Networks 38 (4) (2002) 393–422.
[5] I.H. Cavdar, A solution to remote detection of illegal electricity usage via power line communications, IEEE Transactions on Power Delivery 19 (October) (2004) 1663–1667.
[6] F. Cleveland, R. Ehlers, Guidelines for implementing substation automation using UCA-SA (Utility Communications Architecture-Substation Automation), Electric Power Research Institute Technical Report 1002071, 2003.
[7] R. Cohen, On the establishment of an access VPN in broadband access networks, IEEE Communications Magazine 41 (February) (2003) 156–163.
[8] E. Ekici, I.F. Akyildiz, M.D. Bender, A multicast routing algorithm for LEO satellite IP networks, IEEE/ACM Transactions on Networking 10 (2) (2002) 183–192.
[9] B.R. Elbert, Satellite Communications Applications Handbook, Artech House Publishers, 2004.
[10] G.N. Ericsson, Communication requirements—basis for investment in a utility wide-area network, IEEE Transactions on Power Delivery 19 (January) (2004) 92–95.
[11] G.N. Ericsson, Classification of power systems communications needs and requirements: experiences from case studies at Swedish National Grid, IEEE Transactions on Power Delivery 17 (April) (2002) 345–347.
[12] S. Galli, A. Scaglione, K. Dosterl, Broadband is power: Internet access through the power line network, IEEE Communications Magazine 41 (May) (2003) 82–83.
[13] A.L. Garcia, I. Widjaja, Communication Networks: Fundamental Concepts and Key architectures, McGraw-Hill, 2004.
[14] F. Goodman et al., Technical and system requirements for advanced distribution automation, Electric Power Research Institute Technical Report 1010915, June 2004.
[15] V.C. Gungor, A forecasting-based monitoring and tomography framework for wireless sensor networks, in: Proc. of IEEE ICC, Istanbul, Turkey, June 2006.
[16] Y. Hu, V.O.K. Li, Satellite-based Internet: a tutorial, IEEE Communications Magazine 39 (March) (2001) 154–162.
[17] P.H. Ibarguengoytia et al., Real time intelligent sensor validation, IEEE Transactions on Power Systems 16 (4) (2001) 770–775.
[18] IEEE P1675: Standard for Broadband over Power Line Hardware. Available from: <http://grouper.ieee.org/groups/bop/>.
[19] IEC 61850: Standard for Substation Automation Systems. Available from: <http://www.61850.com/>.
[20] A. Jamalipour et al., Guest editorial broadband IP networks via satellites Part I, IEEE Journal on Selected Areas in Communications 22 (2) (2004) 213–217.
[21] J. Jun, P. Peddabachagari, M. Sichitiu, Theoretical maximum throughput of IEEE 802.11 and its applications, in: IEEE International Symposium on Network Computing and Applications, April 2003, pp. 249–256.
[22] W. Liu, H. Widmer, P. Raffin, Broadband PLC access systems and field deployment in European power line networks, IEEE Communications Magazine 41 (May) (2003) 114–118.
[23] J. Lowrey, Automation systems work best when they communicate with each other, Rural Electric (April) (2003) 38–41.
[24] A. Minosi et al., Intelligent, Low-power and low-cost measurement system for energy consumption, in: Proc. of IEEE VECIMS, July 2003, pp. 125–130.
[25] F.J. Molina, et al., Automated meter reading and SCADA application for wireless sensor network, in: Proc. of ADHOC-NOW, Canada, 2003, pp. 223–234.
[26] J.C. de Oliveira, C. Scoglio, I.F. Akyildiz, G. Uhl, New preemption policies for DiffServ-Aware traffic engineering to minimize rerouting in MPLS networks, IEEE/ACM Transactions on Networking 12 (August) (2004) 733–745.
[27] N. Pavlidou, A.J.H. Vinck, J. Yazdani, B. Honary, Power line communications: state of the art and future trends, IEEE Communications Magazine 41 (April) (2003) 34–40.
[28] D. Pompili, C. Scoglio, V.C. Gungor, VFMAs, Virtual-flow multi-path algorithms for MPLS, in: Proc. of IEEE ICC, Istanbul, Turkey, June 2006.
[29] J. Rabaey et al., Smart energy distribution and consumption: information technology as an enabling force, Technical Report of UC Berkeley, 2001.
[30] J. Roman et al., Regulation of distribution network business, IEEE Transactions on Power Delivery 14 (2) (1999) 662–669.
[31] M. Stephenson et al., Exploiting emerging tools in short range wireless technologies, in: International Conference on 3G Mobile Communication Technologies, June 2003, pp. 348–353.
[32] N.K. Tan, Building VPNs: with IPSec and MPLS, McGraw-Hill Networking, 2003.
[33] A. Tisot, Rio Grande electric monitors remote energy assets via satellite, Utility Automation & Engineering T&D Magazine (July) (2004).
[34] T. Tommila, O. Venta, K. Koskinen, Next generation industrial automation—needs and opportunities, Automation Technology Review (2001).
[35] M.C. Vuran, V.C. Gungor, O.B. Akan, On the interdependence of congestion and contention in wireless sensor networks, in: Proc. of ICST SenMetrics, San Diego, CA, July 2005.
[36] Z. Xie et al., An information architecture for future power systems and its reliability analysis, IEEE Transactions on Power Systems 17 (3) (2002) 857–863.
[37] WiMAX Forum. Available from: <http://www.wimaxforum.org>.
[38] G.E. Ziegler, Protection and substation automation, Electra 206 (February) (2003) 14–23.

Vehbi C. Gungor received his B.Sc. and M.Sc. degree in Electrical and Electronics Engineering from Middle East Technical University, Ankara, Turkey, in 2001 and 2003, respectively. He is currently a Research Assistant in the Broadband and Wireless Networking Laboratory and pursuing his Ph.D. degree at the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA. His current research interests include wireless sensor networks, wireless mesh networks, and WiMAX.

Frank C. Lambert received his B.E.E and M.S.E.E. degree from Georgia Institute of Technology, in 1973 and 1976, respectively. He is currently the Electrical Systems Program Manager at the National Electric Energy Testing, Research and Applications Center, Atlanta, GA. His current research interests include power delivery equipment, automation and systems; power quality; communications for electric utility automation, and grid connected hybrid vehicles.