Computer Networks 55 (2011) 3604–3629

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Survey Paper

A survey on the communication architectures in smart grid

Wenye Wang *, Yi Xu, Mohit Khanna

Department of Electrical and Computer Engineering, North Carolina State University, Raleigh NC 27606, United States

ARTICLE INFO

Article history:
Received 29 June 2011
Accepted 5 July 2011
Available online 27 July 2011

Keywords:
Smart grid
Power communications
Communication networks
Communication protocols
Grid standards

ABSTRACT

The next-generation electric power systems (smart grid) are studied intensively as a promising solution for energy crisis. One important feature of the smart grid is the integration of high-speed, reliable and secure data communication networks to manage the complex power systems effectively and intelligently. We provide in this paper a comprehensive survey on the communication architectures in the power systems, including the communication network compositions, technologies, functions, requirements, and research challenges. As these communication networks are responsible for delivering power system related messages, we discuss specifically the network implementation considerations and challenges in the power system settings. This survey attempts to summarize the current state of research efforts in the communication networks of smart grid, which may help us identify the research problems in the continued studies.

1. Introduction

The current electric power systems have been serving us for more than five decades. They rely heavily on the fossil fuels, including oil, coal, and natural gas, as the energy sources. These fossil fuels are nonrenewable and the reserves on the earth are being consumed rapidly. The emerging energy crisis has called for global attention on finding alternative energy resources that can sustain long-term industry development. The identified renewable energy resources include wind, small hydro, solar, tidal, geothermal, and waste [1], which are also called *green energy* for the fact that they do not release carbon dioxide (CO_2) into the atmosphere in the process of electric energy generation. The renewable energy resources are important complements to and replacements of the fossil fuels for their exploitation durability and environment friendliness. In fact, active research studies and deployment activities are underway across the world [1,2] for effective harness of the renewable energy resources.

In the next-generation electric power systems that incorporate diversified renewable energy resources, automated and intelligent management is a critical component that determines the effectiveness and efficiency of these power systems. The management automation and intelligence are envisioned to offer a variety of advantages over the current systems in terms of digitalization, flexibility, intelligence, resilience, sustainability, and customization [3], which entitles the name *Smart Grid* to the next-generation power systems. The smart control centers are expected to monitor and interact the electric devices remotely in real time; the smart transmission infrastructures are expected to employ new technologies to enhance the power quality; and the smart substations are expected to coordinate their local devices self-consciously [3]. Enabled by the significant advancements in system automation and intelligence, the concept of *Energy Internet* [4] has been proposed that envisions an exciting prospect of the future energy utilization paradigm throughout all the energy generation, storage, transmission and distribution phases.

As one of the enabling technologies, a fast, reliable and secure communication network plays a vital role in the power system management. The network is required to connect the magnitude of electric devices in distributed

* Corresponding author. Tel.: +1 919 513 2549; fax: +1 919 515 5523.
E-mail addresses: wwang@ncsu.edu (W. Wang), yxu2@ncsu.edu (Y. Xu), mkhanna@ncsu.edu (Mohit Khanna).

1389-1286/$ - see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.comnet.2011.07.010

locations and exchange their status information and control instructions. The system-wide intelligence is feasible only if the information exchange among the various functional units is expedient, reliable and trustable. The current communication capabilities of the existing power systems are limited to small-scale local regions that implement basic functionalities for system monitoring and control, such as power-line communications [5–8] and the Supervisory control and data acquisition (SCADA) systems [9–12], which do not yet meet the demanding communication requirements for the automated and intelligent management in the next-generation electric power systems. The future power systems comprise of a diversity of electric generators and power consumers that are located distributively over vast areas and connected all together into the same management network. Real-time bidirectional communications are the foundations to support the comprehensive power system management tasks which, in certain cases, require time-sensitive and data-intensive information exchange.

Apart from power systems, networking technologies have gained tremendous development in the past decades as a separate industry sector. The creation of the Internet, mobile cellular networks, satellite networks, community networks, wired and wireless local area and personal networks, as well as the invention of diversified networking services has enormously enhanced our capability for information exchange. However, the modern networking technologies have not been leveraged sufficiently in power systems for optimized management. When we develop the smart grid, it is critical to take advantage of the advancements in networking technologies to enable the automated and intelligent system management. Although the currently available networking technologies have greatly satisfied our personal communication needs, applying them to power systems and addressing the specific requirements for power communications are challenging by all means. We need to identify the communication scenarios and characteristics in power systems and develop practically usable network solutions. Particularly, our network infrastructures should be able to meet the promptness, reliability and security expectations of the power system communications.

At this transitional phase of shifting to the next-generation electric power systems, the study on the communication architectures for automated and intelligent system management is still at a primitive stage. Many technical challenges are awaiting solutions. To position our current research work and direct our future research effort, we are motivated to present this survey on the network infrastructures to be used in the next-generation electric power systems. As the research and development of these power systems are evolutionary, this survey may not include all the relevant information exhaustively, but it provides a preliminary summary of the current status and the future expectation of the smart grid research.

The rest of this survey is organized as follows. Section 2 describes the smart grid structures and expectations. Section 3 presents the communication architecture in the smart grid and the communication requirements. Sections 4 and 5 discuss the most challenging communication issues in the smart grid, namely, the delay, reliability and security. Section 6 describes the typical communication scenarios. The communication standards and experiments are discussed in Sections 7 and 8 respectively. Section 9 concludes this survey.

2. Smart grid framework and expectations

The communication architectures to be used in the smart grid provide the platform to build the automated and intelligent management functions in power systems. The functional requirements of communication architectures depend on the expected management tasks. To better understand our research goals on the communication networks that support the system management, we first discuss the vision and framework of smart grid. For ease of presentation, we list in Table 1 all the smart grid related acronyms used in this article.

2.1. Smart grid reference model

In the smart grid, many distributed renewable energy sources will be connected into the power transmission and distribution systems as integral components. The typical renewable energy sources include wind, solar, small hydro, tidal, geothermal, and waste. These sources generate extra electricity that supplements the electricity supply from large power plants and, when the electricity generated by distributed small energy sources exceeds the local needs, the surplus is sold back to the power grid.

Table 1
Acronyms in smart grid.

Acronym	Definition
AMI	Automatic metering infrastructure
AMR	Automatic meter reading
BAS	Building automation system
DER	Distributed energy resource
DLC	Direct load control
DMS	Distribution management system
DR	Demand response
EMS	Energy management system
ESI	Energy services interface
GPS	Global positioning system
IED	Intelligent electronic device
IEM	Intelligent energy management
IFM	Intelligent fault management
IHD	In-home display
ISO	Independent system operator
LMS	Load management system
MDMS	Metering data management system
OMS	Outage management system
PEV	Plug-in electric vehicle
PLC	Power line communication
PMU	Phasor measurement unit
PTP	Precision time protocol
RTO	Regional transmission operator
RTP	Real Time Pricing
RTU	Remote terminal unit
SCADA	Supervisory control and data acquisition
STNP	Simple time network protocol
WACS	Wide area control system
WAMS	Wide area monitoring system
WAPS	Wide area protection system
WASA	Wide area situational awareness

With the addition of renewable energy sources, bi-directional dynamic energy flows are observed in the power grid. We illustrate in Fig. 1 the framework of smart grid.

To effectively manage this complex power system that involves an enormous number of diversely functional devices, a co-located communication infrastructure is required to coordinate the distributed functions across the entire power system. This system consists of seven functional blocks [13,14], which are, namely, bulk generation, transmission, distribution, operation, market, customer, and service provider.

2.1.1. Bulk generation

Electricity is generated by using resources like oil, coal, nuclear fission, flowing water, sunlight, wind, tide, etc. This domain may also store electricity to manage the variability of renewable resources such that the surplus electricity generated at times of resource richness can be stored up for redistribution at times of resource scarcity. The bulk generation domain is connected to the transmission domain. It also communicates with the market domain through a market services interface over Internet and with the operations domain over the wide area network. It is required to communicate key parameters like generation capacity and scarcity to the other domains. It comprises of electrical equipments including RTUs, programmable logic controllers, equipment monitors, and fault recorders.

2.1.2. Transmission

The generated electricity is transmitted to the distribution domain via multiple substations and transmission lines. The transmission is typically operated and managed by a RTO or an ISO. The RTO is responsible for maintaining the stability of regional transmission lines by balancing between the demand and supply. The transmission domain may also support small scale energy generation and storage. To achieve self-healing functions and enhance wide area situational awareness and control, a lot of information will be captured from the grid and sent to the control centers. The control centers will also send responses to the devices in remote substations. The bidirectional communications between control centers and substations are handled in the transmission domain too.

2.1.3. Distribution

The dispatch of electricity to end users in the customer domain is implemented by making use of the electrical and communication infrastructures that connect the transmission and customer domains. This domain includes distribution feeders and transformers to supply electricity. It interacts with many different equipment, such as DERs, PEVs, AMI, and sensors with communication capability. The distribution domain takes the responsibility of delivering electricity to energy consumers according to the user demands and the energy availability. In order to provide quality electricity, the stability of this domain is monitored and controlled.

2.1.4. Operation

This domain maintains efficient and optimal operations of the transmission and distribution domains using an EMS in the transmission domain and a DMS in the distribution domain. It uses field area and wide area networks in the transmission and distribution domains to obtain

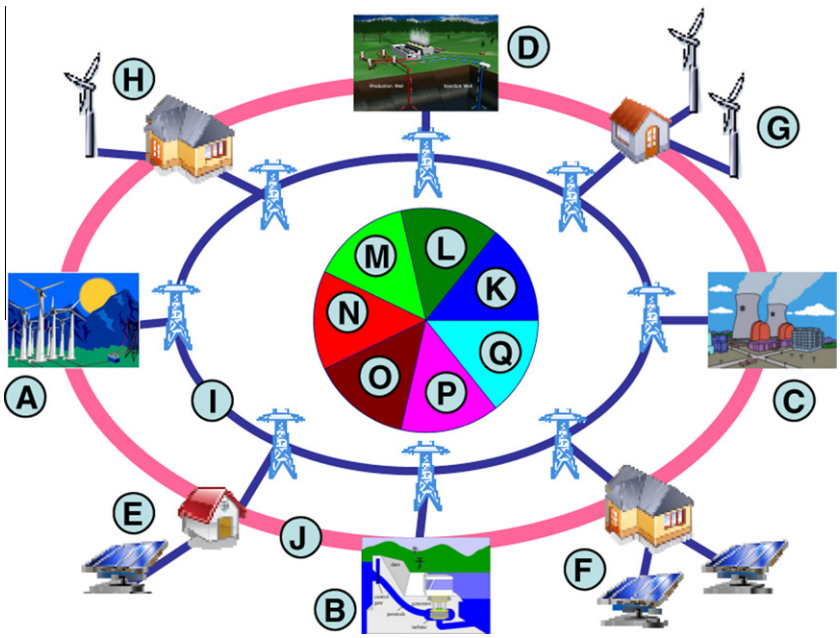


Fig. 1. An illustrative framework of next-generation power grid, where A is a wind power plant, B is a large hydro power plant, C is a coal-fire power plant, D is a geothermal power plant, E and F are houses with solar-electricity generation, G and H are houses with wind-electricity generation, I is the power transmission infrastructure, J is the communication infrastructure, and K–Q are the seven constituent domains that are bulk generation, transmission, distribution, operation, market, customer, and service provider, respectively.

information of the power system activities like monitoring, control, fault management, maintenance, analysis and metering. The information is obtained using the SCADA systems. The operations domain may be subdivided into sub-domains for transmission, distribution, and RTO/ISO operations. These sub-domains may be controlled by different organizations.

2.1.5. Market

The balance between the supply and the demand of electricity is maintained by the market domain. This domain consists of retailers who supply electricity to end users, suppliers of bulk electricity, traders who buy electricity from suppliers and sell it to retailers, and aggregators who combine smaller DER resources for sale. Effective communications between the bulk producers of electricity, the DERs and the market is essential to match the production of electricity with its demand.

2.1.6. Customer

Customers consume, generate (using DERs), or store electricity. This domain includes home, commercial or industrial buildings. It is electrically connected to the distribution domain and communicates with the distribution, operation, service provider and market domains. The customer domain also supports the demand response process. To allow customers to actively participate in the grid, a two-way communication interface between the customer premises and the distribution domain in required. This is generally referred to as an ESI and is present at the customer premises. A communication network within the customer premises is required to allow exchange of data and control commands between the utility and the smart customer devices. This network is referred to as a home area network. It is expected to support applications such as remote load control, DER monitoring and control, IHD support for customer usages, reading of non-energy meters, and integration with building management systems.

2.1.7. Service provider

Electricity is provided to customers and utilities through service providers. They manage services like billing and customer account management for utility companies. It communicates with the operation domain to get the metering information and for situational awareness and system control. It must also communicate with HANs in the customer domain through the ESI interface to provide smart services like management of energy uses and home energy generation.

2.2. Smart grid expectations

The next-generation electric power systems will not only address the existing problems in the current power systems, but also add in advanced new features. Visions and expectations of such modernized power systems have been proposed and endorsed by a number of independent organizations all over the world [15–17]. We summarize them below.

2.2.1. Support for diverse devices

Unlike the existing electricity distribution grid, the future grids will accommodate different kinds of electricity generation and storage devices and allow for bidirectional energy exchange on the existing grid. This will involve support not only for the DERs like the photovoltaic cells, storage batteries and wind energy, but also for the traditional electric loads, smart devices (loads with communication capability) in households and PEVs. The use of DERs will have environmental and monetary benefits for the customers, as they can use the electricity generated and stored by themselves or sell it back to the grid. The bidirectional energy exchange mechanism will be useful in times of electricity shortage at the customer or utility end and will have operational benefits for the both of them.

2.2.2. Superior power quality

Power quality is the ability of the supplied electricity on the distribution grid to adhere to the specified peak levels or root mean square (RMS) voltages. Any deviation in the level (e.g. increasing, decreasing or random RMS voltage) can harm the loads attached to the grid which are generally designed to function at specified levels of electric voltage and frequency. The affected load in turn can harm the gird. For example, it might cause a dip in the voltage levels on the grid affecting other customers that share the infrastructure with the affected site. In severe cases, it might even lead to a power outage resulting in revenue loss. One of the ways to avoid such a situation is to make the loads more resistant to transients in the electric distribution network. The other way is to improve the power quality. The modern grid handles such problems by improving the power quality through monitoring (using sensors) and conditioning. It provides power quality in accordance with load sensitivity. Thus there could be different levels of power quality at different prices. The digital appliances and gadgets of today require higher power quality than what is provided by the traditional grid.

2.2.3. Operation efficiency and optimization

The smart grid will use information technology for extensive facility and electrical field equipment monitoring. This information can be used to operate the grid efficiently by minimizing system losses. The data obtained from the monitoring process will also be helpful in carrying out need-based maintenance and for improving the design of electrical power systems.

2.2.4. Grid security

The future grid will rely extensively on the use of communication technologies for critical functionalities such as control, protection and monitoring of electrical equipments. Hence the security of such a connected structure from any cyber attack is of paramount importance. Security against any physical attack would also be a concern. In case of any breach of security, it is expected that the grid will be able to detect and isolate such a breach to minimize its effect and raise an alarm to speed service restoration.

2.2.5. Grid self-correction

The future grid is expected to detect, analyze and respond automatically to changes where human intervention may not be required or the action is too critical to wait for human input. Thus the grid will be able to detect the occurrence or predict the possibility of a fault in the transmission or distribution system at the earliest. This would improve the reliability, power quality and efficiency of the grid and minimize service disruption.

2.2.6. Consumer participation

In future grids, by making use of the two-way communications and control capability, the utility companies can involve consumers by offering them dynamic electricity pricing with low rates in times of low load on the grid and temporary load reduction programs like demand response. The communication capability also allows consumers to monitor, using web-based EMS, the efficiency of individual smart appliances which can communicate with the grid and choose to replace or repair the inefficient ones. These features will be highly useful when used along with devices with storage backup. For example, PEVs, where the users can monitor the charging of the vehicles or DERs with storage where the users can monitor the stored electric charge.

2.2.7. Market boost

The future grid will allow a lot of new services to be offered to the consumers including the capability to sell and purchase electricity from different suppliers. In such a scenario, the markets shall become a way to connect the suppliers of electricity to the consumers of electricity. The competing price of electricity from various suppliers will keep the price of electricity in favor of the consumers. At the same time by using variable pricing, the market vendors can co-ordinate the demand of electricity with its availability. The markets will need to have detailed information about a particular distribution region to which it caters to, for example, capacity of the system, rate of capacity change, available electricity from suppliers, electricity demand, etc. The use of open standards of communication will allow the user data to be received by the authorized market vendor for processing and billing activities.

3. Communication architecture and functional requirements

3.1. Network architecture

The communication infrastructure in smart grid must support the expected smart grid functionalities and meet the performance requirements. As the infrastructure connects an enormous number of electric devices and manages the complicated device communications, it is constructed in a hierarchical architecture with interconnected individual subnetworks and each taking responsibility of separate geographical regions [18]. An illustrative example of this architecture is shown in Fig. 2. In general, the communication networks can be categorized into three classes: wide area networks, field area networks, and home area networks.

3.1.1. Wide area networks

Wide area networks form the communication backbone to connect the highly distributed smaller area networks that serve the power systems at different locations. When the control centers are located far from the substations or the end consumers, the real-time measurements taken at the electric devices are transported to the control centers through the wide area networks and, in the reverse direction, the wide area networks undertake the instruction communications from control centers to the electric devices.

For enhanced wide area situational awareness, RTOs require a lot of information about the state of the power grid. This is achieved by using fast, time-stamped and real-time information about the system from specialized electrical

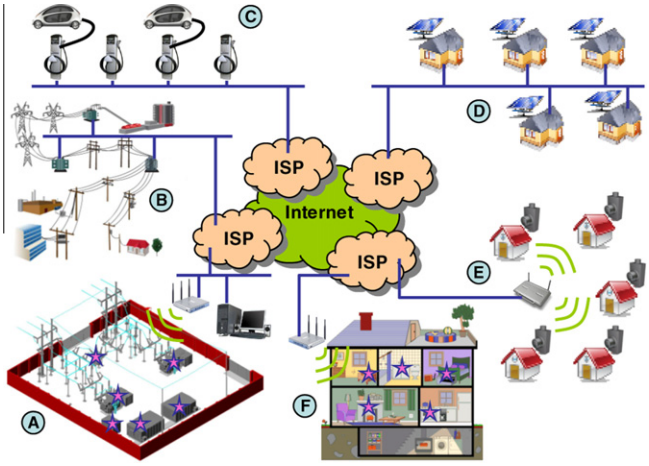


Fig. 2. An example of communication architecture in smart grid, where A is a power substation, B is a segment of power transmission lines, C is a PEV charging station, D is a residential subdivision installed with solar panels, E is a residential complex with AMI, and F is an energy smart house with electric appliances connected to the smart grid. The Internet and ISPs serve as the backbone in connecting the distributed subnetworks.

sensors (PMUs) at substations [19]. The PMU devices capture current and voltage phasor information from the electrical buses at the substations at sample rates up to 60 Hz. The information received from PMUs is used by the EMS systems at control centers for improved state estimation, monitoring, control, and protection.

The wide area networks also convey communications between the IEDs and the control centers. The IEDs are installed along transmission lines and in substations to capture local SCADA information and act upon the control and protection commands from the control centers. Moreover, to support the reception of high speed PMU data at the control centers, a high bandwidth network is required. Currently, the substations communicate with the control centers using point to point telephone or microwave links. Thus in the absence of high speed network, the sensed digital data from PMUs is only limited inside substations and cannot be effectively utilized by the control centers [20]. This underscores the need of a high bandwidth wide area network in the smart grid system.

3.1.2. Field area networks

Field area networks form the communication facility for the electricity distribution systems. The electrical sensors on the distribution feeders and transformers, IED devices capable of carrying out control commands from DMS, DERs in the distribution systems, PEV charging stations and smart meters at customer premises form the main sources of information to be monitored and controlled by the DMS at the control centers. The power system applications operating in the distribution domain utilize field area networks to share and exchange information.

These applications can be categorized as either field based (related to transmission lines, sensors, voltage regulators, etc.) or customer based (related to end customers, like houses, buildings, industrial users, etc.). Field based applications include OMS, SCADA applications, DER monitoring and control, etc. Customer based applications include AMI, DR, LMS, MDMS, etc. These two classes of applications operating in the distribution domain have different critical requirements. For example, customer based applications require the communication network between the utility and the customer to be highly scalable. This would allow addition of more applications and customers in future. Time sensitivity is not much of an issue for such applications. Field based applications on the other hand are more time sensitive in nature. Hence the utilities have a choice in adopting either communication networks dedicated to each class of applications or a single shared communication network for both classes. A shared field area network will be able to minimize development cost and issues while a dedicated network will have advantages of real-time communication capability and additional security.

3.1.3. Home area networks

Home area networks are needed in the customer domain to implement monitoring and control of smart devices in customer premises and to implement new functionalities like DR and AMI. Within the customer premises, a secure two-way communication interface called ESI acts as an interface between the utility and the customer. The ESI may support different types of interfaces, including the utility secured interactive interface for secure two-way communications and the utility public broadcast interface for one-way receipt of event and price signals at the customer devices [21]. The ESI may be linked (either be hardwired or through the home area networks) to a smart meter capable of sending metering information. This information is communicated to the utility. The ESI also receives RTP from the utility over the AMI infrastructure and provides it to the customers. The customers may use a display panel (called IHD) linked to the ESI or a web-based customer EMS (residing in the smart meter, an independent gateway, or some third party) and respond to pricing signals from the utility. The ESI and smart devices provide utility with the ability to implement its load-control programs by accessing the control-enabled devices at the customer site.

Using AMI, ESI and home area networks, the demand response process can be implemented in the following ways:

- DR through AMI gateway. An AMI gateway, though generally used for automatic billing through AMR, can be used to send load control commands to the smart devices using the secure interface of the ESI. Thus, the load control algorithm may reside with the ESI.
- DR through DLC. In this case, either the utility or an authorized energy service provider may directly control the smart appliances or DERs configured with such capability. The energy service provider may act as an aggregator of individual customers, negotiate RTP prices with the utility companies, and determine the demand response policy for the registered customers.
- DR through BAS. In this case, the BAS uses the RTP information available on the public channel of the ESI. A BAS has load controllers linked to security installations and building HVAC systems through wireline (e.g., ethernet) or wireless (e.g., ZigBee) communication medium and can exercise demand response.
- DR through embedded control. In this case, the smart device not only has a communication link to the home area network, but also its own load control algorithm. The smart device receives RTP information from the public ESI interface and exercises demand response. For example, a computer implements its own load control algorithm to take charge in accordance with RTP signals.

3.2. Supporting network technologies

Many network technologies can be used for communications in the transmission, distribution and customer domains in the smart grid, but none of them suits all the applications and there is always a best fit of a technology or a subset of technologies that may be chosen for a group of power system applications, either operating in the same domain or having similar communication requirements. Before a communication technology is chosen for a particular power system application, a thorough analysis is required to match the application requirements with the

technology properties. The available network technologies include the following categories:

- **Power Line Communication.** The power lines are mainly used for electrical power transmissions, but they can also be utilized for data transmissions [5,8,22–26]. The power line communication systems operate by sending modulated carrier signals on the power transmission wires. Typically data signals cannot propagate through transformers and hence the power line communication is limited within each line segment between transformers. Data rates on power lines vary from a few hundred of bits per second to millions of bits per second, in a reverse proportional relation to the power line distance. Hence, power line communication is mainly used for in-door environment [27] to provide an alternative broadband networking infrastructure [7,28] without installing dedicated network wires.
- **Wireline Network.** Dedicated wireline cables can be used to construct data communication networks that are separate from the electrical power lines. These dedicated networks require extra investment on the cable deployment, but they can offer higher communication capacity and shorter communication delay. Depending on the transmission medium used, the wireline networks include SONET/SDH [29,30], Ethernet [31], DSL, and coaxial cable access network. SONET/SDH networks transmit high-speed data packets through optical fibers with supported data rate between 155 Mbps and 160 Gbps. Ethernet is popularly used in our homes and workplaces, providing a data rate between 10 Mbps and 10 Gbps. DSL and coaxial cable can be used for Internet access. The currently available technology allows us to transmit data on DSL and coaxial cable up to 10 Mbps.
- **Wireless Network.** Advancement in wireless networking technology has enabled us to connect devices in a wireless way, eliminating the installation of wirelines. In general, wireless signals are significantly subject to transmission attenuation and environmental interference. As the result, wireless networks usually provide short distance connections with comparatively low data rates. The 802.11 networks [32] are the most popularly used local area wireless networks, which can communicate at a maximum data rate up to 150 Mbps and a maximum distance up to 250 m. In a smaller personal networking area around 10 m in distance, the 802.15 networks [33] provide wireless data exchange connections at rates ranging from 20 kbps to 55 Mbps. For broadband wireless Internet access, 802.16 networks [34] can support data transmissions up to 100 Mbps in a range of 50 km.

For WACS and WAPS applications, high bandwidth is required to meet the timing requirements. For example, it is suggested in [35] to use Internet Protocol (IP), Multi-Protocol Label Switching (MPLS) and Wavelength Division Multiplexing (WDM) to construct the communication backbone. It is proposed that 10/100 Mbps Ethernet be used within substations and 1 Gbps Ethernet be used to connect to the Internet over WDM backbone.

Different communication architectures and technologies may be deployed in the distribution domain. For field based applications, agent-based architectures [36–38] are considered where the agents communicate with each other in a peer to peer manner for local control and protection with the centralized SCADA control center. Various communication technologies may be used to support such communications, e.g., GPRS, Ethernet, SONET/SDH, IEEE 802.11, 802.15, and 802.16. Hybrid architectures may also be deployed where a group of local wireless sensors communicate with an agent to collect nearby electrical information. This approach is more cost effective than using a direct communication link for each agent. Products based on hybrid architectures using 900 MHz wireless mesh technology and cellular technology (GSM and CDMA) are already commercialized [39].

For home area applications and control, IEEE 802.11 WiFi and 802.15 ZigBee networks can be used for convenient and low cost data exchange. Power line communication also provides an alternative network to connect the electrical devices. Through home area networks, the smart meter installed at each household is able to monitor the electricity usage in real time and make adjustment when necessary. Research and standardization efforts are currently underway to unify the home area networking technologies to enable smart energy management for home energy devices [40,41].

3.3. Communication functionalities

The communication infrastructure enables a number of automated and intelligent energy management possibilities in the smart grid. Particularly, the National Institute of Standards and Technology has identified the following priority applications [13] in the smart grid deployment.

3.3.1. Wide area situational awareness

The WASA system collects large amount of information about the current state of the power grid over a wide area from electric substations and power transmission lines. Using this information, monitoring (Wide Area Monitoring Systems – WAMS), control (Wide Area Control Systems – WACS) and protection (Wide Area Protection Systems – WAPS) functionalities can be implemented. Thus WASA gives utility companies the ability to gather information, analyze it and predict any future disturbance or power disruption, thereby preventing the occurrence of blackouts. For example, the information can be used for contingency analysis, which is the ability of the power system to withstand the outage of critical elements. It may also be used for inter-area oscillation damping. Automation of these applications will provide self-healing capability in the future grid. Load shedding and dynamic islanding are examples of such self-healing control applications. Typical WAPS actions include automatic tripping of generators and interruptible loads. The WASA systems use wide area networks in the transmission domain for their operation.

3.3.2. Distribution grid management and automation

The future power grid will see extensive penetration of active elements (which can act as sources of energy) like

DERs into the distribution grid that can exchange energy with the grid in a bidirectional manner. However, the existing utility electric power systems were not designed for active generation and storage at the distribution level [42]. This makes the traditional distribution grid with unidirectional power flow very complex in nature. The distribution grid also needs to support the monitoring of PEVs and consumer based functionality, e.g., automatic metering and demand response systems. These expected changes to the distribution grid call for extensive real-time monitoring of the grid. The monitoring process involves gathering of information from distribution feeders, transformers equipped with electrical sensors and communication capability, PEV charging stations, DER sites and customer premises. This information may be fed to an automated centralized DMS for information analysis, state estimation, and control (using SCADA). This adds to the reliability of the distribution system. These applications use field area networks in the distribution domain for operation.

3.3.3. Advanced metering infrastructure

The AMI system provides a two-way communication capability for interaction between the utility companies and end customers with smart meters. These are mainly used to automatically gather the metering information from the customer side (Automatic Meter Reading – AMR) thereby reducing operational costs. Moreover, by using AMI, bidirectional communication capability, additional functionalities like the demand response system can be implemented. The AMI communication infrastructure can also be used by third party vendors to interact with the customer equipment for equipment monitoring and control. It can also aid in outage detection at the customer site and remote restoration. The AMI systems use field area networks in the distribution domain for operation.

3.3.4. Demand response

The DR system temporarily changes the electricity consumption by loads on the distribution grid in response to market (e.g., high electricity tariff due to high demand) or to maintain the reliability on the grid. The customer DERs may also contribute towards demand response by supporting the electricity demand temporarily. Implementation of a DR system is beneficial for both the utility companies and the customer. DR systems allow the utility companies to control the peak power conditions on the grid and flatten the consumption curves by shifting consumption times. The utility is therefore able to avoid a short term peak by delaying some of the existing usages and buy itself time to start of additional power plants. This avoids the inefficient operation of running backup power plants to cover the peak loads on the grid. Based on consumption curves, the utility companies can provide dynamic Real-Time Pricing (RTP) information to the customers, thereby encouraging them to shift their usage to times of lower electricity demand. This will maximize the use of available power and increase overall system efficiency. Customers on the other hand can use an energy management interface and smart appliances (which communicate with a smart meter) and schedule their electricity usage in synchronization with the low price signals. The process can also be automated and controlled by the utility as per the customer preferences. Moreover, by setting up DERs and energy storage devices at their premises, customers can sell the excess electricity back to the utility. The DR systems use the AMI infrastructure and field area networks of the customer domain to implement their functionalities.

3.3.5. Electric transportation

The introduction of large number of PEVs at homes, PEV charging stations or commercial buildings provides unique challenges to the utility companies. The simultaneous charging of large number of PEVs will put a lot of load on the grid and thus some co-ordination is required to keep the load low at a particular instant and to distribute it over time. This will require the PEV vehicles to shift their charging times in synchronization with the load on the grid or the RTP signals. The PEV batteries can also act as temporary sources of electricity and hence can contribute some electricity to the grid in times of peak demand. Thus, the applications for electric transportation are required to communicate with the PEVs to monitor their charging processes and send them RTP information. It also needs to obtain data from PEVs, like the authentication information, the amount of charging required, the rate of charging, the capacity of the battery, etc. Overall, the impact of PEV charging process on the electricity distribution system needs to be closely monitored by the utility companies. The utility can use this information for load forecasting.

Besides these new functionalities, the existing data traffic in power systems must also be supported by the enhanced utility communication network. The existing data sources include SCADA, protection and control applications, power trading information, event notification from fault recorders, and signals from offices to substations [43].

3.4. Communication requirements

The communication infrastructure in smart grid undertakes important information exchange responsibilities, which are the foundations for the function diversified and location distributed electric power devices to work synergetically. Unsatisfactory communication performance not only limits the smart grid from achieving its full energy efficiency and service quality, but also poses potential damages to the grid system. To protect the smart grid and ensure optimal operation, the communication infrastructure must meet a number of requirements [44,45].

3.4.1. Network latency

Network latency defines the maximum time in which a particular message should reach its destination through a communication network. The messages communicated between various entities within the power grid, may have different network latency requirements. For example, the protection information and commands exchanged between intelligent electronic devices (IEDs) in a distribution grid will require a lower network latency than the SCADA information messages exchanged between electrical

sensors and control centers. Moreover, the messages exchanged can be event driven (e.g., protection and control related) or periodic (e.g., monitoring related). The network architecture and communication medium must support the diverse requirements. The network architecture will determine if the message sent from one communicating entity to the other will reach its destination in one or more hops. This will directly affect the latency. Similarly, the data rates supported by the communication medium also dictate how fast an entity can communicate an event observed or reply to a message received.

3.4.2. Data delivery criticality

The protocol suite used for a particular power system application must provide different levels of data delivery criticality depending on the needs of the application. This need may be decided at the time of connection establishment between two applications. The following levels of data delivery criticality may be used: (a) *high* is used where the confirmation of end-to-end data delivery is a must and absence of confirmation is followed by a retry. For example, this may be used for delivery of SCADA control commands for settings and changes of switch gear position; (b) *medium* is used where end-to-end confirmation is not required but the receiver is able to detect data loss, e.g., measured current and voltage values and disturbance recorder data; (c) *non-critical* is used where data loss is acceptable to the receiver. In this case reliability can be improved by repetitive messages. For example, this may be used for periodic data for monitoring purpose.

3.4.3. Reliability

The communicating devices in the power grid rely on the communication backbone in their respective domains to send and receive critical messages to maintain the grid stability. Hence, it is extremely important for the communication backbone to be reliable for successful and timely message exchanges. The communication backbone reliability is affected by a number of possible failures. These failures include time-out failures, network failures, and resource failures. A time-out failure occurs if the time spent in detecting, assembling, delivering and taking action in response to a control message exceeds the timing requirements. A network failure occurs when there is a failure in one of the layers of the protocol suite used for communication. For example, a routing protocol failure might prevent a message from reaching its destination in spite of existence of a physical link. Noise and interference in the physical medium may also disrupt the communication. A resource failure implies failure of the end node which initiates communications or receives messages. Hence, there is a need to assess the reliability of the system in its design phase and find ways to improve it.

3.4.4. Security

In the future power systems, an electricity distribution network will spread over a considerably large area, e.g., tens or hundreds of miles in dimension. Hence physical and cyber security from intruders is of utmost importance. Moreover, if a wireless communication medium (like WiFi or Zigbee) is used as part of the communication network, security concerns are increased because of the shared and accessible nature of the medium. Hence, to provide security protection for the power systems, we need to identify various communication use cases (e.g., demand side management, advanced meter reading, communication between intelligent energy management (IEM) and intelligent fault management (IFM) devices, and local area communication by IEM devices) and find appropriate security solutions for each use case, for example, authorized access to the real time data and control functions, and use of encryption algorithms for wide area communications to prevent spoofing.

3.4.5. Time synchronization

Some of the devices on power grid need to be synchronized in time. The requirements for time synchronization of a device depend on the criticality of the application. Tolerance and resolution requirements for time synchronization are strict for IEDs that process time sensitive data. For example, phasor measurement units (PMUs) have the most strict need of time synchronization as they provide a real-time measurement of electrical quantities (voltage and current) from across an electricity grid for analysis, measurement and control [44]. Time synchronization can be obtained through a number of ways depending upon the resolution and jitter requirements. Precision time protocol (PTP) defined by the standard IEEE 1588 provides time synchronization with up to nanosecond precision over ethernet networks. Global positioning system (GPS) and simple time network protocol (STNP) are other ways of achieving time synchronization.

3.4.6. Multicast support

The multicast concept is crucial for power system applications in which a message containing a given analog value, state change or command may have to be communicated to several peers at the same time [46]. Thus, instead of multiple individually addressed messages, a single multicast message is sent to a switch that forwards it to all outgoing ports. Receiving devices are simply configured to listen to a particular multicast address, thus making it possible to disregard unwanted network traffic, which is useful for IED devices to share protection related information with their peers.

4. Critical timing requirements

Timing is critical in smart grid communications, which is the most fundamental difference from other communication networks. Some types of information exchanges between electric devices is useful only within a predefined time frame. If the communication delay exceeds the required time window, the information does not serve its purpose any more and, in the worst case, damage might be incurred in the grid. For example, in the common practice for power device protection, the circuit breaker must be opened immediately if the voltage or current on a power device exceeds the normal values. Such protection actions must be made within a time window as small as 3 ms in order to be effective. In fact, IEEE and the International

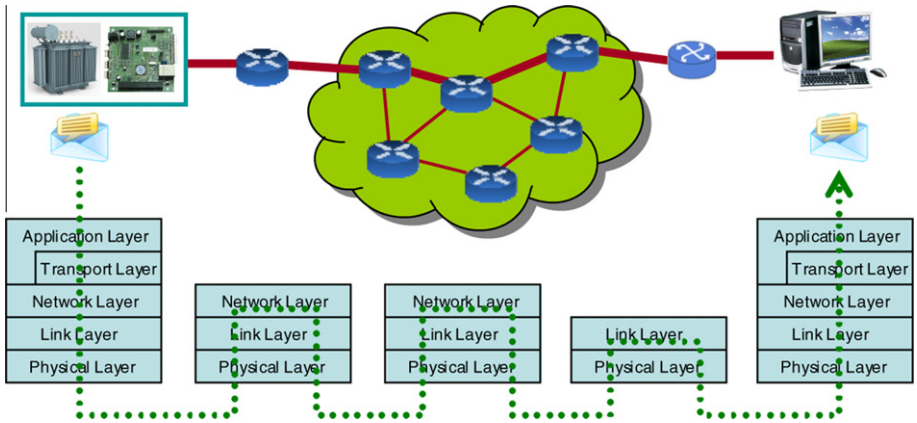


Fig. 3. The message delay in smart grid communications is defined as the end-to-end delay between the two communicating end systems, including the message processing and transmission times at the source, destination and every intermediate forwarding node.

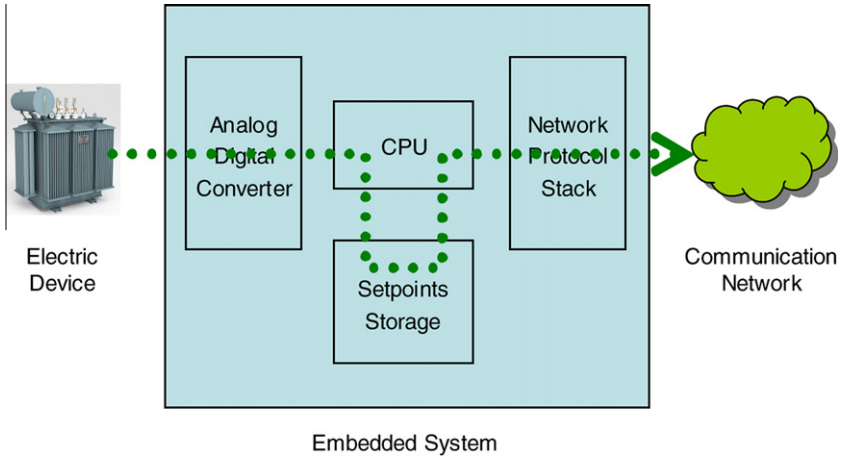


Fig. 4. The processing time spent in an IED device.

Electrotechnical Commission (IEC) have defined rigorous communication delay requirements in smart grid for different types of information exchanges. When we design and implement the communication infrastructure in the grid, these timing requirements must be satisfied.

4.1. Delay definition

The communication delay in smart grid is defined as the time lapse between the sending of a message at the source IED and the receiving of message at the destination IED. It is measured end-to-end between the two applications running at the source and destination systems. An illustration of the delay definition is shown in Fig. 3. As observed in the figure, the end-to-end delay is the sum of all the time pieces spent by the message during its processing and transmission at every traversed node: the source IED incurs some delay to format the message for transmission, each intermediate forwarding node adds in extra delay to process and relay the message, and the destination IED spends additional time to decode the message and present it to the application program.

As the electric power devices do not have communication capability by themselves, each electric device is attached with an embedded computer system to serve as the communication interface to the network infrastructure. The electric device and the embedded computer system together form an IED. The message processing steps within an IED are illustrated in Fig. 4, in which a message containing the device status data is generated and transmitted through four modules in the IED: (i) the analog–digital converter transforms a status measurement into digital data, (ii) the CPU processes the measurement data, (iii) the setpoint structure stores the current measurement data, and (iv) the network protocol stack formats the message and sends it into the network. The time spent within an IED is part of the end-to-end delay as described in Fig. 3.

4.2. Timing classifications

IEEE classifies the message exchange events in power systems into several categories and requires the delays experienced in the communication networks be strictly less than these guideline values [44]. We summarize these

Table 2
IEEE 1646 standard: communication timing requirements for electric substation automation.

Information types	Internal to substation	External to substation
Protection information	4 ms ($\frac{1}{4}$ cycle of electrical wave)	8–12 ms
Monitoring and control Information	16 ms	1 s
Operations and maintenance information	1 s	10 s
Text strings	2 s	10 s
Processed data files	10 s	30 s
Program files	1 min	10 min
Image files	10 s	1 min
Audio and Video data streams	1 s	1 s

Table 3
IEC 61850 communication networks and systems in substations: communication requirements for functions and device models.

Message Types	Definitions	Delay requirements
Type 1	Messages requiring immediate actions at receiving IEDs.	1A: 3 ms or 10 ms; 1B: 20 ms or 100 ms
Type 2	Messages requiring medium transmission speed	100 ms
Type 3	Messages for slow speed auto-control functions	500 ms
Type 4	Continuous data streams from IEDs	3 ms or 10 ms
Type 5	Large file transfers	1000 ms (not strict)
Type 6	Time synchronization messages	No requirement.
Type 7	Command messages with access control	Equivalent to Type 1 or Type 3.

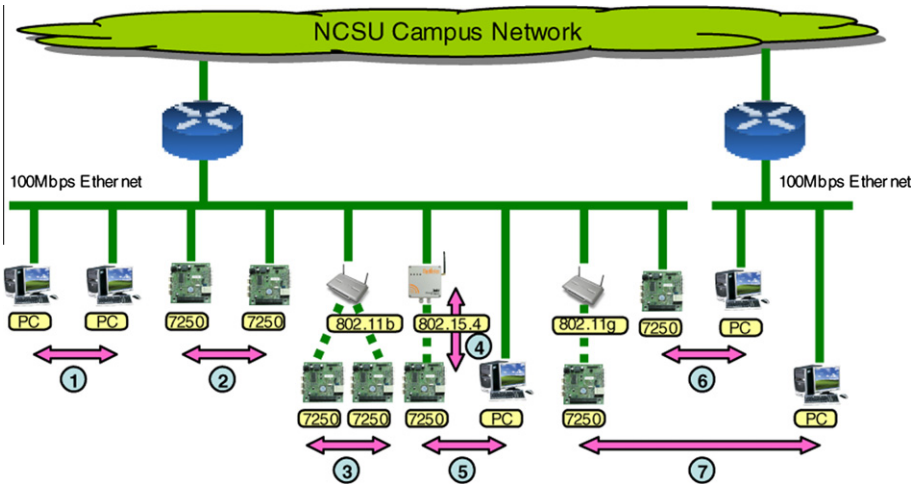


Fig. 5. The delay measurement testbed used in [48] and [49].

delay categories in Table 2. Similarly, IEC has also specified the expected communication delays in different information categories [47], which we summarize in Table 3.

We observe in Tables 2 and 3 that the communication networks to be used in the smart grid are responsible for delivering a diversity of messages used in substation automations and some of them have critical delay requirements. The most time urgent messages are related to the most important system protection functions and require a delivery delay as small as 3 ms, which is measured round trip from the IED to the control station for problem alarming and back to the IED for emergency responding. It is paramount to guarantee the timely and reliable delivery of these messages within the specified delay windows. Note that these delay demanding messages are usually transmitted on the shared networks together with other less time critical but possibly rate intensive messages, so it remains a challenging research problem to guarantee the satisfactory delay performances of time critical messages.

4.3. Delay realities

The currently available network technologies were not designed with the communication delay performance as the first priority and hence they may not always be able to meet the strict delay requirements of power system communications. Preliminary experimental results on the communication delay in several substation networks are reported in [48,49], which show that in many communication scenarios the packet delays experienced in typical substation networks exceed the maximum allowed for the most time critical messages. Specifically, end-to-end

Table 4
Delay measurements in [48] and [49].

Test scenarios	Delay ranges (ms)
1	0.2–0.7
2	0.8–1.6
3	3.2–17
4	12–86
5	32–173
6	18–97
7	19–622

delays are measured in [48,49] under seven different network settings as illustrated in Fig. 5 for variable-length packets (from 16 to 4096 bytes) that are transmitted through the TCP/IP protocols.

(1) PC-PC via Ethernet. Two Linux workstations are connected through a 100 Mbps Ethernet switch. The CPU speed of each Linux workstation is 2.6 GHz and each workstation is installed with 1.5 GB memory.
(2) TS7250-TS7250 via Ethernet. Two Technologic Systems TS7250 embedded computers are connected through a 100 Mbps Ethernet switch. Each TS7250 is equipped with a 200 MHz ARM-9 CPU and 64 MB memory, and installed with Linux operating system.
(3) TS7250-TS7250 via 802.11b. Two TS7250 embedded computers are attached with WiFi dongles on their USB ports and communicate by connecting to a shared 802.11b access point.
(4) TS7250-Gateway via 802.15.4. A TS7250 embedded computer is attached with an Xbee-Pro communication board through serial link and exchanges data with an 802.15.4 gateway.
(5) TS7250-PC via 802.15.4-Ethernet gateway. A TS7250 embedded computer exchanges data with a PC connected to the Ethernet interface of the 802.15.4 gateway.
(6) TS7250-PC via Ethernet and university campus network. A TS7250 embedded computer is connected to an Ethernet and communicates with a PC located in another Ethernet through a university campus network.
(7) TS7250-PC via 802.11 g and university campus network. A TS7250 embedded computer is connected to a 802.11 g access point and communicates with a PC in a separate Ethernet through a university campus network.

We summarize the experimental results on the testbed used in [48,49] in Table 4. The results show that the communication delay within a single Ethernet is below 2 ms, while the delay increases significantly on wireless networks and multihop networks, as observed in the test scenarios 1–2 and 3–7 respectively.

The communication delays within substations have also been investigated through simulations. The simulation results in [50,51] show that the 10/100 Mbps Ethernet in general can provide satisfactory delay performance for communications inside a substation. The delay measurements in the simulated network settings in [50,51] are less than 1 ms in most cases, which are consistent with the experimental results on Ethernet in [48,49]. It is meanwhile observed that the communication delay increases with the distance between communicating devices and therefore the delay performance in large-size Ethernet may need further investigation.

The most time critical messages in smart grid communications require a delay bound as small as 3 ms, as defined in Tables 2 and 3. It is observed from the experimental results that Ethernet can meet all the delay requirements. Therefore, Ethernet will be a good choice to implement control automation within a substation. Single-hop WiFi network cannot be used to transmit system protection messages, but it meets the delay requirements of all the other messages, for example, system monitoring and control, operation and maintenance, text files, images and videos. ZigBee network and multihop network with wireless access, however, can only be used to transmit time insensitive data. They cannot be used to transport system protection, monitoring and control messages. Note that the delay performances will become even worse when the networks experience heavier background traffic loads or more complicated multihop networks are used. Hence, the design of short-delay networks is a critical research problem in the smart grid in order to support effective energy management functions.

4.4. Research challenges

Given the importance of communication networks in the smart grid management, many research efforts [12,43,52–59] have been made in proposing and constructing various network architectures to connect the distributively located electrical devices for automated control. To achieve satisfactory communication delay performance, a number of open research problems must be addressed carefully.

4.4.1. Understanding delay components

The communication infrastructure in smart grid will incorporate many network technologies and assume a hierarchical and hybrid composition. Different types of networks are used to provide communication facilities to different portions or regions of the grid and they are interconnected to form the entire infrastructure. The delay experienced by a message consists of many components as the message travels within each subnetwork and through the interfaces between subnetworks. The various delay components can be generally categorized as follows.

- Data acquisition delay. The status measurements, such as voltage, current and temperature, are acquired periodically from the electric devices and converted from their original analogue formats into the digital representations. The digital information is then processed by the attached embedded system, which functions as a low-profile computer, for transmission through the communication networks. A data acquisition delay is

incurred between the event occurrence, for example a voltage change, and the actual digital information capture.
- Packet processing delay. Data is transmitted through a communication network by following the specified network protocols. Different layers of packet headers and trailers are added, inspected, modified and removed along the transmission path taken by the packet. Each step in packet processing adds extra delay to the total time spent by the packet in the network.
- Packet transmission delay. The current link layer mechanisms append a data integrity check field to each data frame to detect possible data errors. Every intermediate node on the packet transmission path verifies the data correctness after receiving the complete data frame and before forwarding the packet to the next relay node. Transmission delay is incurred on each link for the sending and receiving of the data frame.
- Medium access delay. Multiple data sending nodes that share the same transmission medium, such as wireless spectrum and wireline cable, compete for the medium access in order to transmit their respective data. A node has to wait until its turn for transmission. Similarly, a packet in a node has to wait until all the other packets scheduled ahead have been cleared from the buffer.
- Event responding delay. For some types of IED status reporting messages, actions are required in response to the events. For example, a measured voltage exceeding the normal value should trigger a circuit breaker off command from the control station. The intelligent energy and fault management system residing at the action responsible node may spend some time in deciding what response to take.

A detailed analysis of all the delay components between any pair of communicating IEDs is required to understand the delay performances in the communication infrastructure. A comparison between the actual delay performances and the expected delay bounds is needed to evaluate the supportive feasibility of communication networks. Given the diversity of equipments and protocols used in the smart grid, accurate delay evaluation is a challenging research issue.

4.4.2. Minimizing end-to-end delay

In order to meet the strict delay requirements in the smart grid communications, efforts are required in three delay reduction perspectives, namely, choosing the appropriate network equipments, utilizing the fast communication mechanisms provided in the current network equipments and protocols, and designing new protocols to speed up the transmission of time urgent messages.

- Network technology selection. There are many different network technologies available for use, which have different communication capacities and delay performances. Selection of the appropriate network technology for each application scenario is the first step toward meeting the delay requirements. However, besides the delay requirements, many other consideration factors like the deployment convenience and equipment cost also affect the decision on network selections.
- Network service mapping. Some network technologies offer fast communication mechanisms to support time critical message delivery, for example the DiffServ service classes in the Internet and the coordination functions in the wireless LANs. As the smart grid communications consist of multiple delay classifications, each type of messages should be mapped to the corresponding delay service provided by the underlying network technologies. The mapping is determined by whether the chosen delay service meets the delay requirement.
- New protocol design. Due to many reasons, such as deployment convenience and equipment cost, high-profile fast networks may not always be the best selection for particular application scenarios. When low speed networks are used, alternative network protocol design may be needed to improve the delay performance. Re-engineering of network protocols is possible by modifying and updating the protocol stack programs in network equipments, but the side effects of changing standard protocols must be fully considered, such as the compatibility problems.

The communication delay is defined in the smart grid from end to end including all the network segments traversed by a message. Therefore, it is also important to design and deploy simple network structures that involve the least number of intermediate hops to minimize the communication delay.

4.4.3. Enforcing delay guarantees

The communication infrastructure is shared by all the types of messages, which have diverse delay requirements. Protecting the time critical message deliveries from the resource competition of delay insensitive messages is hence necessary, especially when the delay insensitive messages are rate intensive. Two strategies can be used to enforce the delay guarantees for time critical messages.

- Message prioritization. Different types of messages may be prioritized differently with the priority levels corresponding to the time urgencies. High priority messages should be allocated network resources for speedy transmission before low priority messages. For example, a dedicated buffering queue may be provided to serve high priority messages and a node with high priority messages in its queue may be scheduled for transmission before other nodes.
- Admission control. When congestions occur in the network, low priority messages may be limited from entering the network to solve the congestion problem. Admission control hence ensures the communication availability for the high priority messages to meet their delay requirements. However, carefully designed control schemes should not excessively limit the network access of low priority messages such that reasonable network utilization is still maintained.

The prioritization and control strategies are general methods. Given the complex network structures and diverse communication classes, many design and implementation details need to be worked out, for example, the number of priority levels, resource allocation in each level, priority mapping to each communication class, priority transition between different networks, admission control criteria, and dynamic control adjustments.

4.4.4. Evaluating enforcement capabilities

Under certain power system situations that affect massive number of devices, a large number of time critical messages may be generated, all with high delivery priority. It is necessary to understand the network capabilities in meeting the delay requirements of multiple simultaneous time urgent messages. Specifically, the research challenges exist in two perspectives.

- Maximal delivery support. When multiple time critical messages require simultaneous transportation and delivery, the available network processing and transmission resources should be carefully assessed and allocated such that maximal network support is provided to accommodate the delay expectation of each individual message. For example, if there exist multiple disjoint paths that can be used, the messages may be distributed over different paths to speed up their transmissions.
- Support capability determination. Given the limitation of network resources, such as the relay node processing speed and the link bandwidth, there exists an upper bound on the number of simultaneous time critical messages that can be delivered in time by the communication infrastructure. Evaluation of this network support capability limit is important and necessary as it determines the feasibility of simultaneous delay guarantees for multiple messages.

5. Reliable and secure communications

Reliability and security are fundamental concerns in power systems. As the power systems provide electricity to almost every aspect of our lives, they must be operated in the normal functioning status in design conformance. By reliability, we require that system faults occur with minimum probability and, should some component go wrong, its impact to the whole power system is minimized and the dysfunctional component is restored to the normal working status in the shortest time. Security on the other hand addresses the power system malfunctions due to human reasons, such as intentional attacks and unauthorized alterations. Since the communication networks play a vital role in the intelligent and automated energy system management, their reliability and security issues are a critical part of the power system reliability and security, and thus need to be addressed carefully. More importantly, given the time urgency of some types of messages in power systems, it is challenging to find reliability and security solutions that meet the strict delay requirements at the meantime.

5.1. Research challenges in communication reliability

Communication networks are not deployed extensively in traditional power systems. As such, the existing research efforts on power system reliability have mainly focused on identification of reliability problems [60–63], definition of reliability metrics [64], and evaluation of reliability models [65,66] for power devices. Communication network reliability [67–70] and its connection to the power system reliability [71–73] still stay in a primitive research stage. The research challenges in power system communication reliability can be classified into several categories.

5.1.1. Reliability mapping

The communication networks in power systems are responsible for information exchange among distributed power devices to assist the functioning of management systems. The reliability of communication networks is hence coupled with the reliability of power management systems. Power systems cannot work correctly unless the communications among intelligent electronic devices are transported as expected. To determine the reliability requirements on the communication networks, it is necessary to understand the performance expectations on communication infrastructure from the power management systems first, and then map the communication expectations into the network reliability requirements. Given the diversified communication performance expectations from the energy management systems, multiple-class network reliability requirements should be defined correspondingly.

5.1.2. Network reliability

Messages may be delayed, altered or lost during transmissions in networks. The communication networks should be designed and implemented by taking these possible transmission problems into account to ensure that each message reaches its destination correctly and timely. Many network problems can result in unsatisfactory message transmissions, including for example network congestions, protocol errors, and link disruptions. Message prioritization and resource reservation mechanisms may help mitigate network congestions to allow the most important messages to be delivered on time. To prevent protocol errors and link disruptions, periodic network maintenance checkups are needed to identify and locate possible network problems. Besides, early detection mechanisms are also needed to discover network connection problems such that they can be fixed promptly.

5.1.3. Communication restoration

Communication problems can be largely reduced if the networks are carefully implemented and operated, but they can never be eliminated. Having backup communication solutions is always a good practice to improve the network reliability further. For every important end-to-end connection path, one or more alternative routing paths should be planned ahead of failure occurrences. The original and alternative paths should have minimum intersections to enhance the robustness of each individual path. Automatic failure detections and path

switchings are needed to resume communications instantly at the time of disruption in the original path. Additionally, mechanisms should be implemented to retransmit the messages that are lost during the path transition intervals.

5.1.4. Reliability responsiveness

For some types of messages in power system communications, there are critical timing requirements on their maximally allowed transmission delays. The communication network reliability should be inspected under these strict timing bounds. Therefore, the definition and evaluation of reliability are based on the corresponding timing requirements. For example, the power system protection messages must be correctly delivered within a time frame as small as 3 ms. An acceptable reliability solution should hence guarantee that the retransmitted or rerouted messages reach the intended destination devices within 3 ms from the time that the first attempted message is sent. Any delayed messages received after this 3 ms time window do not serve the reliability purpose. Therefore, it is challenging to address the communication network reliability problem.

5.1.5. Reliability evaluation

The communication network reliability should be modeled and analyzed by defining quantitative reliability metrics, such as error probabilities and restoration delays. Understanding the specific reliability performances is necessary in order to predict the likelihood of network problem occurrences and allocate the limited network resources to the most important performance perspectives. Furthermore, the impact of communication problems on the power grid operations and services should also be evaluated. For example, analysis should be provided to estimate the possibility of equipment damages and the extent of service outages if certain types of messages cannot be delivered correctly and timely due to network reliability problems. As the communication networks assist in the power grid functions, the reliability evaluation of communication networks should be mapped back to the power grid ability in providing continuous electricity services without disruption.

5.2. Research challenges in communication security

Communication security is a research issue as important as the network reliability regarding the correct functioning of power system management. Different from reliability, security problems arise from malicious human behaviors and hence they are more challenging to solve. As the communication networks undertake the responsibilities for information exchange used in power management, they could become targets of attacks that attempt to distort the management functions. Attackers can possibly gain monetary benefits or simply cause impactful damages to the power systems. Therefore, it is imperative to protect the communication networks from cyber attacks. The security problems in power systems have been discussed widely in the literature [74–86].

5.2.1. Security objectives in power system communications

In literature, information security problems can be classified into five general categories in respect to their objectives, namely, availability, integrity, confidentiality, authenticity, and non-repudiation. In power system communications, mechanisms to achieve information availability, integrity and authenticity must be provided, among which availability is the most critical requirement. The confidentiality and non-repudiation objectives may not always be required, depending on the particular communication scenarios.

- Information availability. The communication networks should be able to perform communication functions as normal when attacks happen that attempt to block the information passage in the networks. Availability is the foundation of other security concerns. The communication networks must first guarantee message deliveries to their intended destinations and then protect the messages from other security threats. As the communication networks used in the smart grid will be a large-scale comprehensive infrastructure that involves a diversity of components and protocols, attackers may exploit the security vulnerabilities at various network nodes and protocol layers to deny the legitimate communications from network accesses and usages.
- Information integrity. The messages transmitted in the communication networks in smart grid should be protected against unauthorized changes. The contents of these messages are related to power system measurements, controls and user data, falsification of which will endanger the smart grid operations. For example, an altered status measurement may miss a component failure alarm, a falsified control command may interrupt the power system functions, and an incorrect user data exchange may result in wrong operations in the energy management system. Mechanisms must be provided to verify the integrity of the information contained in the transmitted messages.
- Information authenticity. Forged messages in the communication networks should also be discernable. False messages injected into the communication networks by attackers interrupt the normal power system operations in a similar way as altered messages. They convey incorrect information between distributed power devices and result in wrong management decisions. Therefore, the communication networks must have mechanisms that are able to verify the message genuineness, i.e., the messages are from the senders as claimed. Messages that do not pass the authenticity inspection must be ignored and, under certain cases, the actual sources of false messages should be identified.
- Information confidentiality. Sensitive information transmitted through the communication networks should be kept confidential. Such information includes for example the user account and transaction data. Disclosure of user sensitive information may violate the user rights, cause user financial losses, and compromise the creditability of the power service providers.

Methods should be used to prevent unauthorized users from accessing the sensitive information both during transmission and at storage. The degree of confidentiality protection should be commensurate with the secrecy period required by the protected data.

- Information non-repudiation. The non-repudiation objective refers to the fact that a user cannot deny the transmission of a message after the message has been sent. Non-repudiation is related to the information forensics. In the smart grid communications, most messages do not require assurance of non-repudiation.

5.2.2. Security solutions in power system communications

The importance of communication security has been recognized by the research community in power system communications. Solutions have been proposed to construct secure communication networks to support the smart energy management in the power grid. Specifically, the security solutions in the literature are observed in the following categories corresponding to the security objectives discussed above.

- Denial-of-service defense. All the information availability attacks interfere with the normal information exchanges by injecting false [87] or useless [88] packets into the communication networks. The false information confuses the packet recipients in recognizing the correct information. The useless packets consume a significant share of network bandwidth such that the legitimate traffic is knocked out in the network. Both types of attacks deny the information availability in the communication networks. Solutions to defend against the denial-of-service attacks rely on a careful discretion of the legitimate traffic from the attack traffic. An effective solution must be able to filter out the attack traffic to protect the legitimate information exchanges.
- Integrity protection. To prevent messages from unauthorized changes during transmission, mechanisms are needed for the message recipients to verify the originality of the received messages. The integrity protection solutions rely on the established agreements between message senders and receivers on the use of message encryption keys [86,89–92]. The message senders use the encryption keys to compute a message digest for each message and the message receivers use the corresponding decryption keys to verify the correctness of the received message digest. The encryption and decryption keys can be either identical or asymmetric. Usually identical keys have lower computational overhead than asymmetric keys. In order to establish the encryption and decryption key pairs, key exchange protocols must be completed before the message integrity can be protected.
- Authenticity enforcement. Message origins must be verified in the power system communication networks to prevent sophisticated attackers from impersonating legitimate power devices to transmit forged messages. The solutions to guarantee message authenticity are built on top of the mechanisms that require message senders prove their identities [93–96]. The identity proofs are usually presented in the form of demonstrating the knowledge of certain secrets that are known by the message senders. The secrets used for identification are usually the same message encryption keys used for integrity protection and therefore the authenticity enforcement schemes employ either the symmetric or the asymmetric encryption and decryption key pairs. Key exchange protocols are necessary in order to establish the key pairs.

In power system communications, the information confidentiality and non-repudiation are not always required. Except for certain types of messages, such as the customer transactions, messages do not need to be protected against unauthorized reading. There is also no requirement in most cases for the communication networks to prevent message senders from denying message transmissions. Most of current research efforts on the power system communication security are targeting the information availability, integrity and authenticity objectives, which are critically important in power systems.

Other than the five major security objectives discussed above, research efforts have also been reported in the intrusion detection systems [97], access control schemes [98], and communication anonymities [99]. Intrusion detection systems and access control schemes supplement the other security solutions to strengthen the power system defense against security threats. The communication anonymity, on the other hand, addresses the user privacy concerns while preserving the security requirements.

5.2.3. Research challenges

The smart grid is a large-scale complex power system interconnecting an enormous number of power devices that are equipped with significantly diverse computation and communication capabilities. It is challenging to address the security problems in the smart grid communication networks due to the network size and heterogeneity. Specifically, the research challenges exist in the following categories.

- Requirements mapping. The communication networks in power systems transmit diversified classes of messages. Different types of messages may require different security protections. For example, the system control messages must be protected with information availability, integrity and authenticity, while the system status sampling data without emergency may only need integrity and authenticity and the availability requirement may not always be necessary, as occasional packet loss is acceptable. A careful classification of the message types and their mapping to the security objectives must be determined.
- Minimum-latency solutions. Security protection mechanisms for emergent messages must incur minimum latency to satisfy the message delay requirements. For the time critical messages, delivery beyond their acceptable delay windows renders the messages useless. The delays introduced by the security computations and protocol setups add on top of the message transmission delays and therefore they should be kept minimum. In general, computationally intensive

security solutions provide strong protection but incur long delay, so a practical tradeoff between the security performance and the computational delay may be reached in the design of security solutions.

- Security evaluation. Each security scheme used in the power system communication networks must be carefully evaluated on its strength. Typical evaluation metric is the computational time required for compromising the security scheme. The security strength should be sufficiently high such that it is practically impossible to compromise the scheme within a reasonable amount of time. For a security protocol design, every step in the protocol should be inspected to preclude any potential security holes. The security evaluation should also include an assessment of the possible equipment damages and service losses in case that the scheme is compromised.

6. Typical communication scenarios

In this section, we describe a few typical communication scenarios in power systems. These scenarios represent various data communications in the network infrastructure that provides intelligent support to energy management. Specifically, as the smart grid power systems are featured by automated bi-directional information exchanges in every phase of energy generation, distribution and usage, we illustrate in Fig. 6 the communications involved in these phases.

6.1. Substation control

The electrical substation (case 1 in Fig. 6) is an important component in power systems. It changes the voltages on the electrical transmission lines and controls the power flow in the transmission system. A substation is a complex system composed of many elements such as transformers, capacitors, voltage regulators, and circuit breakers. Automated substation control will be implemented extensively in the smart grid systems to provide real-time monitoring and control through local area networks. The possible network technologies to be used in a substation include Ethernet and wireless LAN. To connect the various equipments in a substation, specialized sensors are attached to the equipments to take their status samples. The sampled values are then digitized and transmitted through the local area network to the control station in the substation. An example of the communication network in a substation is shown in Fig. 7.

The transmitted messages may be continuous data streams or isolated packets, depending on the particular controlling applications. A message generated by the sensor attached to an electrical equipment is processed by the network protocol stack and then transmitted on the network. The network may consist of a number of subnets connected through switches. Each switch on the path of packet transmission processes and forwards the packet. When the packet is received by the control station, a response may be made by the control station and a configuration message may be sent back to the electrical equipment. As many equipments are monitored and controlled in a substation, all the communications share the network bandwidth.

When the messages are used for maintenance purposes, a maximum network delay of about 1 s is allowed. When the messages convey real-time monitoring and control information, the network delay should be limited to around 10 ms. In case that the messages carry urgent equipment fault information, the delivery to the control station should be within 3 ms. When the control station sends response messages, the delays should be comparable to those of the messages received by the control station.

6.2. Transmission line monitoring

Electricity is transmitted and distributed from power generation plants to customers through power lines (case

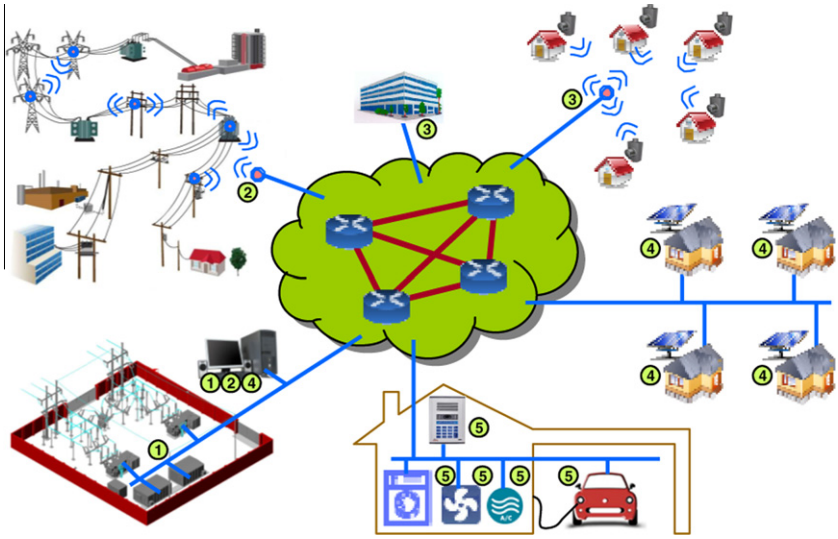


Fig. 6. Typical communication scenarios: (1) substation control, (2) power line monitoring, (3) automatic meter reading, (4) demand response decisioning, (5) energy usage scheduling.

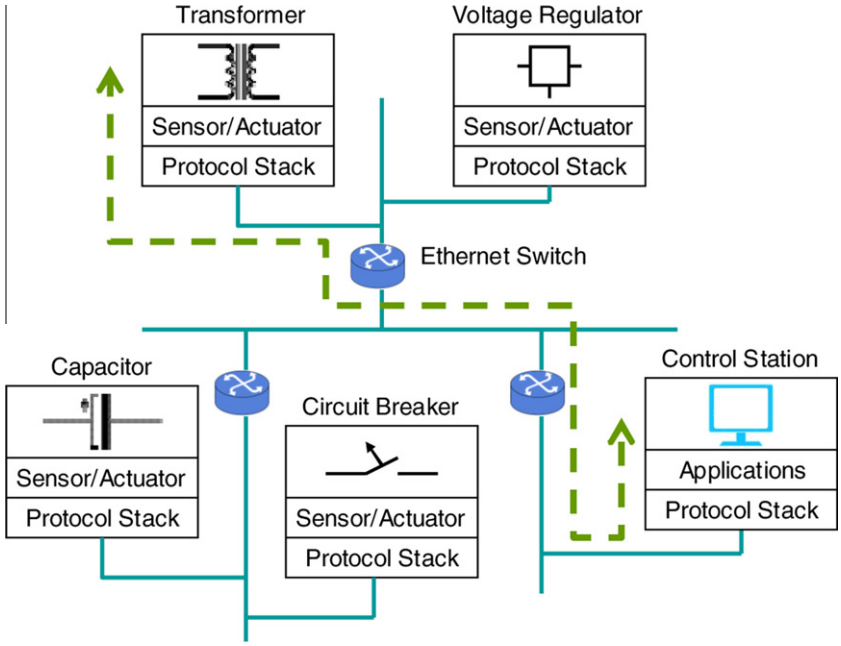


Fig. 7. Communications in a substation.

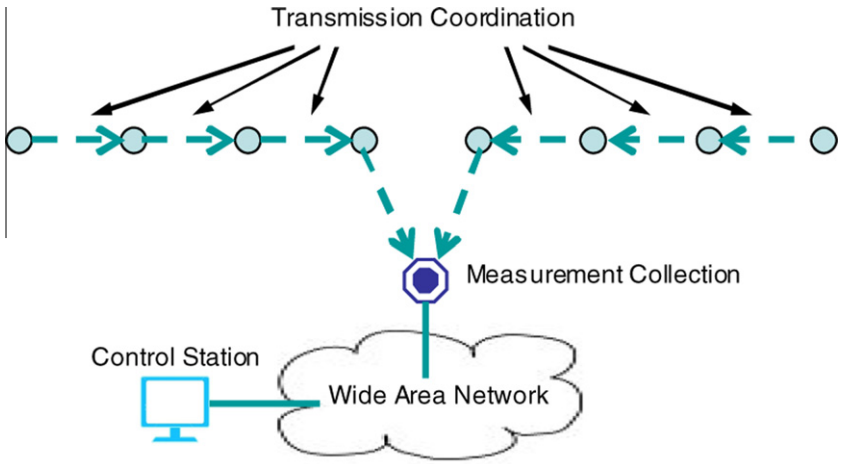


Fig. 8. Monitoring of power transmission lines.

2 in Fig. 6). The power lines may span over long distance and some segments may travel through less populated areas. Prompt detection of transmission anomalies is critical to ensure satisfactory power quality and service. One method of automated transmission line monitoring is to install sensors along the lines to collect the real-time status measurements. Each sensor is equipped with wireless communication capability to exchange data with neighbors. The real-time measurements are relayed through the sensors until they reach a measurement collection site, which is connected to the wide area networks for communications to the control office. An example of the transmission line monitoring is illustrated in Fig. 8.

Sensors communicate with neighbors using wireless links, which are subject to interferences. It is therefore important to coordinate the sensor transmissions to ensure successful communications. Besides sending own measurements, some sensors also relay packets for others. The traffic loads on different sensors may be unbalanced, which should be considered in scheduling their transmissions. Sensors will higher loads should be allowed to transmit for longer time to maintain the communication network stability.

The delay requirements are determined by the type of measurements transmitted. For periodic maintenance measurements, a 1 s communication delay is permissible. For constant and continuous monitoring of important working states, such as voltages and currents, the communication delay should be within 10 ms. If failures occur with the transmission lines, the messages reporting failures should be delivered to the control station within 3 ms.

6.3. Automatic meter reading

Facility companies need to read the electricity meter from each household for billing purpose. The traditional method is to send technical staffs to take the readings manually. With the deployment of communication infrastructure, meter reading can be automated and simplified (case 3 in Fig. 6). Electricity meters equipped with communication capability can send the meter readings automatically over the network to the facility companies. There are a number of advantages to replace the traditional meters with the networked intelligent meters. First, the billing cost is lowered. Facility companies do not need to send staffs for meter reading any more. Second, the billing process can be completely automated. The readings received from the network can be processed immediately to generate customer bills. Third, accurate and detailed usage information can be collected from customers. Readings can be made in periods shorter than the monthly billing cycle such that facility companies are able to analyze customer usages with improved data accuracy. The communications between automatic meters and a facility company are illustrated in Fig. 9.

To read the electricity meters automatically, a facility company installs a reading collection device in each household subdivision. The meters send their readings to the collector through wireless links. As the collector location can be planned carefully, each meter communicates directly with the collector. A scheduling mechanism should be implemented to coordinate the transmissions from different meters to avoid transmission collisions. The collector then relays the readings through the wide area network to the facility company. The collector may either forward each reading as a separate packet or assemble a number of readings for group sending. Forwarding group readings reduces the communication overhead, but collection delays may be incurred. As meter readings are not sensitive to communication delay, it is acceptable to receive the readings with a delay of about a few seconds.

6.4. Demand response decisioning

In the smart grid power systems, electricity is generated distributively. Supplementary to large power plants, many households are installed with solar panels to convert sunlight into usable electricity. Wind turbines, small hydros and geothermal plants can also be constructed in regions with renewable energy resources to generate electricity. The electricity market will become diversified due to the participation of many small to medium sized suppliers. The communication infrastructure will connect all the energy suppliers and all the energy customers to provide a platform for energy trading (case 4 in Fig. 6). The supply and demand of electricity change dynamically on the market due to the time varying properties of electricity generation and usage. Communications regarding the electricity availability and price are exchanged through the network for each supplier and each customer to reach a balance between the supply and the demand. The communications among the distributed energy suppliers and customers are illustrated in Fig. 10.

Each electricity supplier or customer publishes its amount of energy availability or demand through the wide area network. Different network access technologies may be used to connect the energy market participants. For example, a large business may have its own local area network through which its electricity usage information is sent out to the wide area network, and a household may access the wide area network through a dial-up phone line or a cable modem. The communications on the energy market are from multiple sources to multiple destinations, and each participant exchanges information with multiple others to look for the most favorable energy price. The path taken by a message consists of the segments in the access networks and the wide area network respectively. Because there are potentially many participants on the market, the communication delay perceived by individual packet may vary significantly. The smart grid users may expect a communication delay within a few seconds to catch up with the dynamic market states.

6.5. Energy usage scheduling

The electricity price changes in the market as determined by the supply and demand. The price is usually higher during the daytime and lower at night. In the daytime, electricity is largely consumed by factories and all types of office buildings. At night, the demand for electricity decreases when factories and office buildings are closed. Accordingly, energy price varies at different times

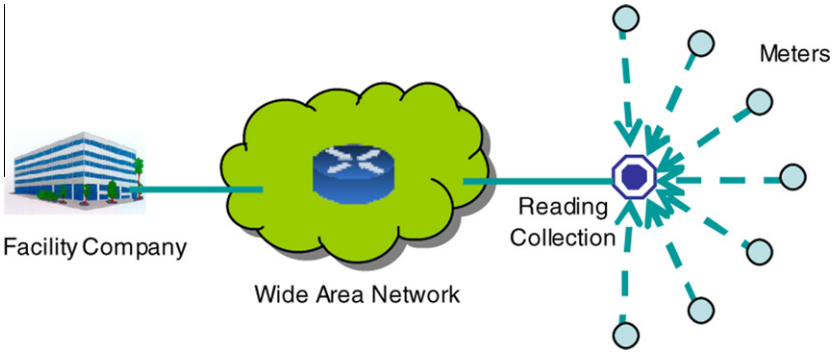


Fig. 9. Communications for automatic meter reading.

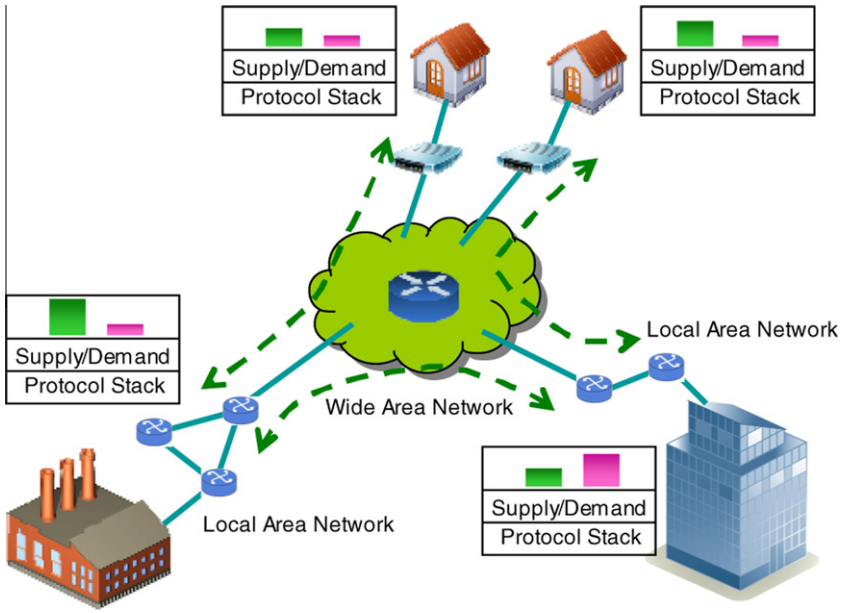


Fig. 10. Communications among distributed energy suppliers and customers.

of a day. Customers can take advantage of the dynamic energy prices to reduce the energy cost by scheduling time flexible energy usages at the time of low energy prices (case 5 in Fig. 6). For example, the washer and dryer are used at night and the electric vehicle is charged at night. Home area networks can be deployed to connect the electrical appliances in a house to a scheduler, which activates each appliance at the appropriate time to minimize the cost of using electricity. We illustrate an example home network in Fig. 11.

To schedule the energy usage according to the electricity price, the electrical appliances in a home are connected to a scheduling controller through a home area network. Usually, a wireless router is sufficient to set up a home network. The electrical appliances under scheduling may include washer, dryer, aircon, fan, light, and electric vehicle. These appliances can be connected into the home network either with wirelines or with wireless links. The scheduling controller requests electricity prices periodically from the energy market, based on which the controller determines an economic operation schedule to activate each appliance at appropriate time. The communications between the scheduling controller and the energy market and the communications between the controller and the electrical appliances do not have strict delay requirement. A delay of a few seconds is reasonably good to schedule energy usages.

7. Standardization activities

Many standards have been proposed to guide the development of next generation electric power systems. These standards cover a vast number of technical aspects of the power systems, including power equipments, electricity services, management automations and system protections. As our focus in this paper is the communication architecture, we present next the standards on the communication aspect of the electric power systems.

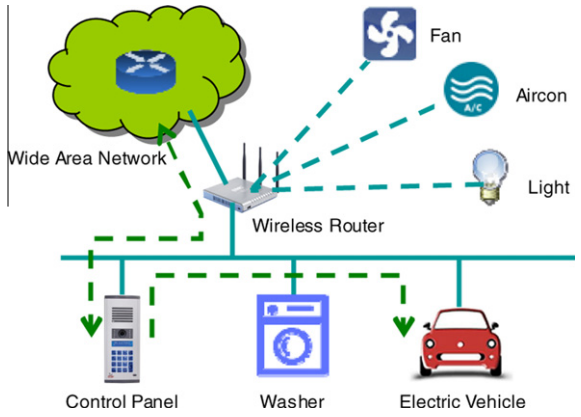


Fig. 11. Communications in a home network to schedule electricity usages.

7.1. Distributed network protocol

The distributed network protocol (DNP) first appeared in 1998, which went through a number of revisions to become the current version (DNP3) [100]. The DNP3 standard prescribes the protocols used for substation automation through local or wide area networks. It is used to implement the SCADA control system in a substation. Electric devices compatible with the DNP3 communication protocols can exchange status and control information to automate substation management. The DNP3 standard employs the Internet protocol suite to transport packets. Accordingly, it assumes a layered architecture and all the DNP3 defined

packets are encapsulated into TCP or UDP packets during the transmission. Security mechanisms are provided in the forms of virtual private network (VPN) and IPsec, which are functions of the Internet protocol suite.

DNP3 is currently used in substations for equipment monitoring and control. It implements the basic functions of an automated system to communicate equipment states to the control station and deliver configuration commands to the electric equipments. However, the communication quality in DNP3 is not strictly guaranteed. Especially, communication delays are not defined and delay requirements are not specified. Due to the absence of communication quality provisions, DNP3 cannot be used in the smart grid power systems, which will require a comprehensive network protocol with guarantees in the communication quality.

7.2. IEEE standards

IEEE has proposed a number of standards related to the communications in power systems, including C37.1, 1379, 1547, and 1646.

7.2.1. IEEE C37.1

The IEEE standard C37.1 [101] describes the functional requirements of IEEE on SCADA and automation systems. This standard provides the basis for the definition, specification, performance analysis and application of SCADA and automation systems in electric substations. It defines the system architectures and functions in a substation including protocol selections, human machine interfaces and implementation issues. It also specifies the network performance requirements on reliability, maintainability, availability, security, expandability and changeability.

7.2.2. IEEE 1379

The IEEE document 1379 [102] recommends implementation guidelines and practices for communications and interoperations of IEDs and RTUs in an electric substation. It provides examples of communication support in substations by using existing protocols. Particularly, it describes the communication protocol stack mapping of the substation network to DNP3 and IEC 60870-5. Processes are also discussed to expand the data elements and objects used in substation communications to improve the network functionalities.

7.2.3. IEEE 1547

The IEEE standard 1547 defines and specifies the electric power system that interconnects distributed resources. It consists of three parts: the electric power system [103], the information exchange [104], and the compliance test [105]. In the power system part, the standard specifies the requirements on different power conversion technologies and the requirements on their interconnection to provide quality electricity services. General guidelines are described to ensure power quality, respond to power system abnormal conditions, and form subsystem islands. The information exchange part specifies the requirements on power system monitoring and control through data networks. Important network aspects are described, including interoperability, performance and extensibility. Protocol and security issues are also considered in the standard. The conformance test part provides the procedures to verify the compliance of an interconnection system to the standard. As an electric power system is complicated in components and functions, the standard describes a variety of tests to guarantee an implemented system to work as expected.

7.2.4. IEEE 1646

The IEEE standard 1646 [44] specifies the requirements on communication delivery times within and external to an electric substation. Given the diversity of communication types, the standard classifies substation communications into different categories and defines the communication delay requirement for each category. For example, system protection messages are required to be transmitted within 4 ms and operation maintenance messages within 1 s. Furthermore, it defines the communication delay as the time spent in the network between the applications running at the two end systems. Therefore, the packet processing time should also be considered into the delay such that the combination of processing and transmission times does not exceed the required delay bound. Since delays are introduced in both the end system processing phase and the network transmission phase, the standard discusses further on the system and communication capabilities required to deliver information on time, including for example real-time support, message priority, data criticality, and system interfaces.

7.3. IEC standards

The International Electrotechnical Commission (IEC) has proposed a number of standards on the communication and control of electric power systems. The standard 60870 [106] defines the communication systems used for power system control. Through the standard, electric equipments can interoperate to achieve automated management. The standard 60870 contains six parts, which specify the general requirements on the power system interoperability and performance. The standard 61850 [107] focuses on the substation automated control. It defines comprehensive system management functions and communication requirements to facilitate substation management. The management perspectives include the system availability, reliability, maintainability, security, integrity and general environmental conditions. The standards 61968 [108] and 61970 [109] provide common information model for data exchange between devices and networks in the power distribution domain and the power transmission domain respectively. Cyber security of the IEC protocols is addressed in the standard 62351 [110], which specifies the requirements to achieve different security objectives including data authentication, data confidentiality, access control and intrusion detection.

7.4. NIST standards

The National Institute of Standards and Technology (NIST) has also published standards to provide guidance

to the smart grid construction. The NIST Special Publication 1108 [111] describes a roadmap for the standards on smart grid interoperability. It states the importance and vision of the smart grid, defines the conceptual reference model, identifies the implementation standards, suggests the priority action plans, and specifies the security assessment procedures. In particular, it presents the expected functions and services in the smart grid as well as the application and requirement of communication networks in the implementation of smart grid. The NIST report 7628 [112] particularly focuses on the information security issues of the smart grid. It explains the critical security challenges in the smart grid, presents the security architectures, and specifies the security requirements. Security objectives and strategies are discussed, including cryptography, key management, privacy and vulnerability analysis. The report 7628 aims to ensure trustable and reliable communications for the automated energy management in the smart grid.

8. FREEDM communication testbed

The Future Renewable Electric Energy Delivery and Management (FREEDM) Systems Center, headquartered on the Centennial Campus of North Carolina State University, is one of the largest research centers funded by the National Science Foundation for the next generation electric power system research and development. The FREEDM center aims to prototype a small scale smart grid with all the fundamental function support for intelligent energy and fault management. The prototype energy system will include a number of electric equipments, such as transformers, circuit breakers and solar panels, and different power transmission topologies. Communications among distributed electric devices are implemented through a dedicated data network with interface to each electric device. The communication testbed used in the FREEDM center targets two research objectives: (i) functional demonstration of real-time power system monitoring and control and (ii) network performance and security enforcement through protocol design and experiment.

8.1. Network functional demonstration

A DNP3 standard compliant protocol suite has been implemented to demonstrate management automation in an electric substation. At this prototyping stage, an example substation model is constructed using the Real Time Digital Simulator (RTDS). The substation model simulates a number of interconnected electric equipments and outputs real time equipment states. The communications between each simulated equipment and the control station are implemented as a master–slave paradigm. The DNP3 protocol running at the RTDS is the slave and the protocol running at the control station is the master. The demonstration setup is illustrated in Fig. 12.

The control station requests equipment states periodically for real time monitoring. The requests are processed by the DNP3 protocol and sent into the local network connecting the RTDS and the control station. The DNP3 protocol running at the RTDS samples the equipment states accordingly and sends back the sampled values to the control station. In addition to state polling, in which the RTDS replies to the control station, the RTDS can also send unsolicited state samples to the control station. When system configuration needs to be changed in the simulated substation, the control station sends control commands remotely. For example, the control station can open or close a circuit breaker in RTDS through the communication network.

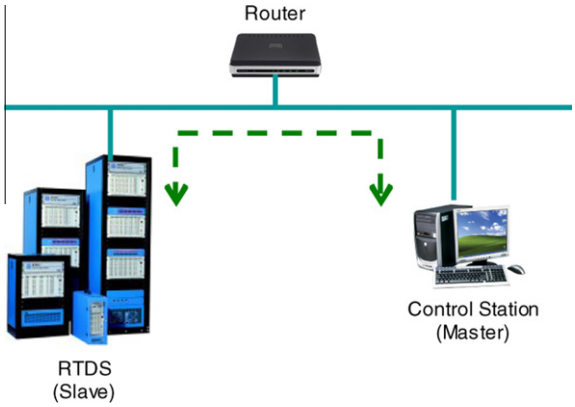


Fig. 12. DNP3 testbed in the FREEDM center.

DNP3 implements the basic networking functions for automated management in a substation, but it does not guarantee that the communication performance meets the substation control requirements. The DNP3 standard does not specify important network performance issues, such as communication delay, criticality and security. Therefore, the implementation of IEC 61850 protocol suite is ongoing at the FREEDM center, which expects improved communication performance in the next demonstration phase.

8.2. Network performance and security

A communication testbed has also been set up in the FREEDM center to evaluate the delay performance in an emulated substation network, as illustrated in Fig. 13. In a substation, each electric device is attached with a controller board, which is an embedded system that samples the analog states from the electric device, converts them into digital forms, and communicates the digital measurements to the remote master station. In the reverse communication direction, the controller board receives commands issued by the master station through the network, converts digital signals to analog values, and changes the device configurations accordingly. Depending on the hardware implementation, the controller board can be either a single embedded system that integrates both the controlling and the communication functions or one controlling system and one communication system that are connected through a point-to-point data exchange link. The latter approach is used in the testbed of FREEDM center. Specifically, a SST controller is used for a solid state transformer and a solar panel controller is used for a solar panel. As the AMR already integrates the controlling functions, the

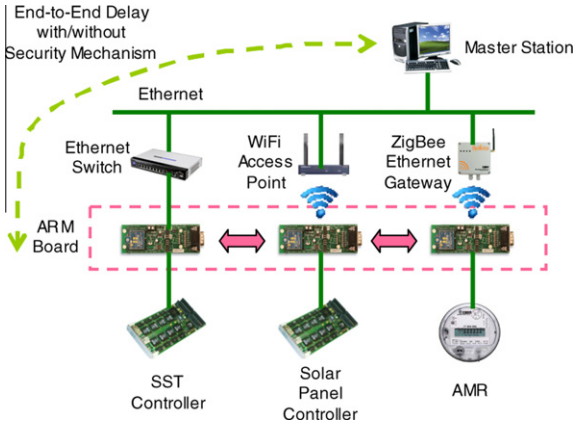


Fig. 13. Communication performance testbed in the FREEDM center.

AMR is connected to the communication system directly. The communication system is implemented on a Technologic Systems TS7250 embedded computer with 200 MHz ARM-9 CPU and 64 MB memory. The communication system accesses the network through Ethernet, WiFi or ZigBee, which is connected to the master station through an Ethernet.

The communication performance of the emulated substation network is tested between the communication system (ARM board) and the master station in three scenarios. In the first scenario, the ARM board communicates with the master station using DNP3 protocol. In the second scenario, the ARM board and the master station are installed with the GOOSE/SMV subset of IEC 61850 protocol implementation. The GOOSE/SMV protocol defines a fast communication mechanism to meet the delay requirement of time critical messages. In the third scenario, GOOSE/SMV messages are authenticated by using three algorithms: RSA [113], HORS [114,115] and HMAC [116,117].

Experiments show that DNP3 may or may not meet the 3 ms delay requirement of the most time critical messages. In the two operational modes specified in DNP3, the event-driven mode has shorter delay than the non-event-driven mode, because the event-driven mode sends a message immediately after event occurrence rather than wait until the next poll. However, as all the DNP3 messages are processed through TCP/UDP/IP network layers, DNP3 messages experience significant amount of CPU scheduling delays. The average DNP3 message delay observed in the experiments is 1 ms in the event-driven mode and at least 20 ms in the non-event-driven mode. In contrast, the GOOSE/SMV messages experience 0.3–0.4 ms delay under the same test conditions as DNP3. All the GOOSE/SMV messages are sent as event-driven and encapsulated into Ethernet frames directly, so they are faster than DNP3 messages. The authentication procedure incurs extra delays to the GOOSE/SMV messages. Experiments show that RSA involves the most complicated computations and the message delay may not meet the 3 millisecond requirement for the time critical messages. The authentication algorithms HORS and HMAC have less computational delays and they can be used on the most time critical messages.

9. Conclusion

The next generation electric power system is expected to alleviate the energy shortage problem by exploiting renewable energy resources. The new system is fundamentally different from the current system in energy management. Communication network will be an indispensible component in the new power system for effective energy management. In this survey, we have characterized and presented the communication network architectures, performance requirements and research challenges for intelligent power system management. We have made several key observations. First, as the energy suppliers and customers are located distributively, the communication network will assume a hybrid structure with core networks and many edge networks that connect all the suppliers and customers. Second, communication delay is the most critical network performance metric. To protect the power system effectively, the communication network must guarantee correct message delivery within the required time window. Third, communication reliability and security must be provisioned with the delay constraint. Reliability and security are thus very challenging problems in the communication network. Fourth, preliminary experiments indicate that a communication network must be planned carefully in order to meet the performance requirement in energy management. Our survey summarizes the current research status on communication networks in the next generation power systems. Many research efforts are still required before the communication infrastructure can be implemented for intelligent energy management.

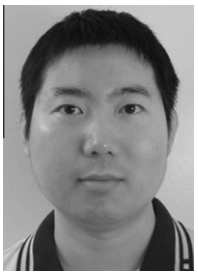
References

[1] L.A. Barroso, H. Rudnick, F. Sensfuss, P. Linares, The Green Effect, IEEE Power & Energy Magazine 8 (5) (2010) 22–35.
[2] R. Moreno, G. Strbac, F. Porrua, S. Mocarquer, B. Bezerra, Making room for the boom, IEEE Power & Energy Magazine 8 (5) (2010) 36–46.
[3] F. Li, W. Qiao, H. Sun, H. Wan, J. Wang, Y. Xia, Z. Xu, P. Zhang, Smart Transmission grid: vision and framework, IEEE Transactions on Smart Grid 1 (2) (2010) 168–177.
[4] A.Q. Huang, J. Baliga, FREEDM system: Role of power electronics and power semiconductors in developing an energy internet, in: Proceedings of International Symposium on Power Semiconductor Devices, 2009.
[5] N. Ginot, M.A. Mannah, C. Batard, M. Machmoum, Application of power line communication for data transmission over PWM network, IEEE Transactions on Smart Grid 1 (2) (2010) 178–185.
[6] J. Anatory, N. Theethayi, R. Thottappillil, Channel characterization for indoor power-line networks, IEEE Transactions on Power Delivery 24 (4) (2009) 1883–1888.
[7] V.K. Chandna, M. Zahida, Effect of varying topologies on the performance of broadband over power line, IEEE Transactions on Power Delivery 25 (4) (2010) 2371–2375.
[8] C. Konate, A. Kosonen, J. Ahola, M. Machmoum, J.-F. Diouris, Power line communication in motor cables of inverter-fed electric drives, IEEE Transactions on Power Delivery 25 (1) (2010) 125–131.
[9] V.I. Nguyen, W. Benjapolakul, K. Visavateeranon, A high-speed, low-cost and secure implementation based on embedded ethernet and internet for SCADA Systems, in: Proceedings of SICE Annual Conference, 2007.
[10] J.D. McDonald, Developing and defining basic SCADA system concepts, in: Proceedings of Rural Electric Power Conference, 1993.
[11] I. Ali, M.S. Thomas, Substation communication networks architecture, in: Proceedings of Joint International Conference on Power System Technology and IEEE Power India Conference, 2008.
[12] Q. Yang, J.A. Barria, C.A.H. Aramburo, A communication system architecture for regional control of power distribution networks, in:

Proceedings of IEEE International Conference on Industrial Informatics, 2009.
[13] National Institute of Standards and Technology, NIST framework and roadmap for smart grid interoperability standards, Release 1.0. <http://www.nist.gov>.
[14] E.W. Gunther, A. Snyder, G. Gilchrist, D.R. Highfill, Smart grid standards assessment and recommendations for adoption and development. <http://osgug.ucaiug.org>.
[15] L.D. Kannberg, M.C. Kintner-Meyer, D.P. Chassin, R.G. Pratt, J.G. DeSteese, L.A. Schienbein, S.G. Hauser, W.M. Warwick, Gridwise: the benefits of a transformed energy system, Technical report. <http://www.pnl.gov>.
[16] National Energy Technology Laboratory, The modern grid initiative. <http://www.netl.doe.gov>.
[17] Smartgrids Advisory Council, Driving factors in the move towards smartgrids. <http://www.smartgrids.eu>.
[18] V.C. Gungor, F.C. Lambert, A survey on communication networks for electric system automation, Elsevier Computer Networks 50 (7) (2006) 877–897.
[19] D. Tholomier, H. Kang, B. Cvorovic, Phasor measurement units: functionality and applications, in: Proceedings of Power Systems Conference, 2009.
[20] C.H. Hauser, D.E. Bakken, A. Bose, A failure to communicate: next generation communication requirements, technologies, and architecture for the electric power grid, IEEE Power and Energy Magazine 3 (2) (2005) 47–55.
[21] OpenHAN task force of the utility AMI working group, Utility AMI 2008 home area network system requirements specification. <http://www.utilityami.org>.
[22] F. Gianaroli, A. Barbieri, F. Pancaldi, A. Mazzanti, G.M. Vitetta, A novel approach to power-line channel modeling, IEEE Transactions on Power Delivery 25 (1) (2010) 132–140.
[23] A. Kosonen, J. Ahola, Communication concept for sensors at an inverter-fed electric motor utilizing power-line communication and energy harvesting, IEEE Transactions on Power Delivery 25 (4) (2010) 2406–2413.
[24] Z. Marijic, Z. Ilic, A. Bazant, Fixed-data-rate power minimization algorithm for ofdm-based power-line communication networks, IEEE Transactions on Power Delivery 25 (1) (2010) 141–149.
[25] N. Andreadou, F.-N. Pavlidou, Modeling the noise on the OFDM power-line communications system, IEEE Transactions on Power Delivery 25 (1) (2010) 150–157.
[26] J. Zhang, J. Meng, Robust narrowband interference rejection for power-line communication systems Using IS-OFDM, IEEE Transactions on Power Delivery 25 (2) (2010) 680–692.
[27] J. Anatory, N. Theethayi, R. Thottappillil, Channel characterization for indoor power-line networks, IEEE Transactions on Power Delivery 24 (4) (2009) 1883–1888.
[28] J. Anatory, N. Theethayi, R. Thottappillil, Performance of underground cables that use OFDM systems for broadband power-line communications, IEEE Transactions on Power Delivery 24 (4) (2009) 1889–1897.
[29] American National Standards Institute, Synchronous optical network (SONET) - sub-STS-1 interface rates and formats specification. <http://www.ansi.org>.
[30] American National Standards Institute, Transmission and multiplexing (TM) – digital radio relay systems (DRRS); – Synchronous Digital hierarchy (SDH); – System performance monitoring parameters of SDH DRRS. <http://www.ansi.org>.
[31] IEEE, IEEE 802.3 Standard. <http://www.ieee.org>.
[32] IEEE, IEEE 802.11 Standard. <http://www.ieee.org>.
[33] IEEE, IEEE 802.15 Standard. <http://www.ieee.org>.
[34] IEEE, IEEE 802.16 Standard. <http://www.ieee.org>.
[35] X. Tong, G. Liao, X. Wang, S. Zhong, The analysis of communication architecture and control mode of wide area power systems control, in: Proceedings of International Symposium on Autonomous Decentralized Systems, 2005.
[36] S. Sheng, K.K. Li, W.L. Chan, X. Zeng, X. Duan, Agent-based self-healing protection system, IEEE Transactions on Power Delivery 21 (2) (2006) 610–618.
[37] M. Pipattanasomporn, H. Feroze, S. Rahman, Multi-agent systems in a distributed smart grid: design and implementation, in: Proceedings of IEEE/PES Power Systems Conference and Exposition, 2009.
[38] Z. Jiang, Agent-based control framework for distributed energy resources microgrids, in: Proceedings of IEEE/WIC/ACM International Conference on Intelligent Agent Technology, 2006.
[39] Silver Spring Networks. <http://www.silverspringnet.com>.
[40] M. LeMay, R. Nelli, G. Gross, C.A. Gunter, An integrated architecture for demand response communications and control, in: Proceedings of Hawaii International Conference on System Sciences, 2008.
[41] ZigBee HomePlug Joint Working Group, Smart energy profile marketing requirements document (MRD). <http://www.homeplug.org>.
[42] IEEE Standards Coordinating Committee 21 (IEEE SCC21), IEEE standard for interconnecting distributed resources with electric power systems. <http://ieeexplore.ieee.org>.
[43] K. Hopkinson, G. Roberts, X. Wang, J. Thorp, Quality-of-service considerations in utility communication networks, IEEE Transactions on Power Delivery 24 (3) (2009) 1465–1474.
[44] IEEE, IEEE standard communication delivery time performance requirements for electric power substation automation. <http://ieeexplore.ieee.org>.
[45] M. Adamiak, R. Patterson, J. Melcher, Inter and intra substation communications: requirements and solutions. <http://pm.geindustrial.com>.
[46] V. Skendzic, A. Guzma, Enhancing power system automation through the use of real-time ethernet, in: Proceedings of Power Systems Conference: Advanced Metering, Protection, Control, Communication, and Distributed Resources, 2006.
[47] IEC, IEC 61850-5 communication networks and systems in substations – Part 5: communication requirements for functions and device models. <http://www.iec.ch>.
[48] M. Khanna, Communication challenges for the FREEDM System, master thesis. <http://www.lib.ncsu.edu>.
[49] M. Khanna, A. Juneja, R. Rajasekharan, W. Wang, A. Dean, S. Bhattacharya, Integrating the communication infrastructure of the FREEDM System with the IEM and IFM Devices: hardware and software developments, in: Proceedings of the FREEDM Annual Conference, 2010.
[50] T.S. Sidhu, Y. Yin, Modelling and simulation for performance evaluation of IEC61850-based substation communication systems, IEEE Transactions on Power Delivery 22 (3) (2007) 1482–1489.
[51] T.S. Sidhu, Y. Yin, IED Modelling for IEC61850 Based Substation Automation System Performance Simulation, in: Proceedings of IEEE Power Engineering Society General Meeting, 2006.
[52] C.-L. Chuang, Y.-C. Wang, C.-H. Lee, M.-Y. Liu, Y.-T. Hsiao, J.-A. Jiang, An adaptive routing algorithm over packet switching networks for operation monitoring of power transmission systems, IEEE Transactions on Power Delivery 25 (2) (2010) 882–890.
[53] M. LeMay, R. Nelli, G. Gross, C.A. Gunter, An integrated architecture for demand response communications and control, in: Proceedings of Hawaii International Conference on System Sciences, 2008.
[54] L.A.O. Class, K.M. Hopkinson, X. Wang, T.R. Andel, R.W. Thomas, A robust communication-based special protection system, IEEE Transactions on Power Delivery 25 (3) (2010) 1314–1324.
[55] J.-Y. Cheng, M.-H. Hung, J.-W. Chang, A zigbee-based power monitoring system with direct load control capabilities, in: Proceedings of IEEE International Conference on Networking, Sensing and Control, 2007.
[56] M. Qureshi, A. Raza, D. Kumar, S.-S. Kim, U.-S. Song, M.-W. Park, H.-S. Jang, H.-S. Yang, A communication architecture for inter-substation communication, in: Proceedings of IEEE International Conference on Computer and Information Technology Workshops, 2008.
[57] M. Kim, J.J. Metzner, K.Y. Lee, Design and implementation of a last-mile optical network for distribution automation, IEEE Transactions on Power Delivery 24 (3) (2009) 1198–1205.
[58] S. Kirti, Z. Wang, A. Scaglione, R. Thomas, On the communication architecture for wide-area real-time monitoring in power networks, in: Proceedings of Hawaii International Conference on System Sciences, 2007.
[59] I. Ali, M.S. Thomas, Substation communication networks architecture, in: Proceedings of Power System Technology and IEEE Power India Conference, 2008.
[60] K. Moslehi, R. Kumar, A reliability perspective of the smart grid, IEEE Transactions on Smart Grid 1 (1) (2010) 57–64.
[61] G. Andersson, P. Donalek, R. Farmer, e.a.N. Hatziargyriou, Causes of the 2003 major grid blackouts in North America and Europe, and recommended means to improve system dynamic performance, IEEE Transactions on Power Systems 20 (4) (2005) 1922–1928.
[62] B.D. Russell, C.L. Benner, Intelligent systems for improved reliability and failure diagnosis in distribution systems, IEEE Transactions on Smart Grid 1 (1) (2010) 48–56.
[63] J. Eto, V. Budhraja, C. Martinez, J. Dyer, M. Kondragunta, Research, development, and demonstration needs for large-scale, reliability-enhancing, integration of distributed energy resources, in: Proceedings of Annual Hawaii International Conference on System Sciences, 2000.

[64] J. Haakana, J. Lassila, T. Kaipia, J. Partanen, Comparison of reliability indices from the perspective of network automation devices, IEEE Transactions on Power Delivery 25 (3) (2010) 1547–1555.
[65] W. Zhao, F.E. Villaseca, Byzantine fault tolerance for electric power grid monitoring and control, in: Proceedings of the International Conference on Embedded Software and Systems, 2008.
[66] Y. Wang, W. Li, J. Lu, Reliability analysis of wide-area measurement system, IEEE Transactions on Power Delivery 25 (3) (2010) 1483–1491.
[67] Z. Xie, G. Manimaran, V. Vittal, A.G. Phadke, V. Centeno, An information architecture for future power systems and its reliability analysis, IEEE Transactions on Power Systems 17 (3) (2002) 857–863.
[68] B. Yunus, A. Musa, H.S. Ong, A.R. Khalid, H. Hashim, Reliability and availability study on substation automation system based on IEC 61850, in: Proceedings of IEEE International Conference on Power and Energy, 2008.
[69] M.G. Kanabar, S. Member, T.S. Sidhu, Reliability and availability analysis of IEC 61850 based substation communication architectures, in: Proceedings of IEEE Power and Energy Society General Meeting, 2009.
[70] M.S. Thomas, I. Ali, Reliable, fast, and deterministic substation communication network architecture and its performance simulation, IEEE Transactions on Power Delivery 25 (4) (2010) 2364–2370.
[71] H. Yang, H. Jang, Y. Kim, U. Song, S. Kim, B. Jang, B. Park, Communication networks for interoperability and reliable service in substation automation system, in: Proceedings of the International Conference on Software Engineering Research, Management and Applications, 2007.
[72] F. Cleveland, Enhancing the reliability and security of the information infrastructure used to manage the power system, in: Proceedings of IEEE Power Engineering Society General Meeting, 2007.
[73] A.Z. Faza, S. Sedigh, B.M. McMillin, Reliability analysis for the advanced electric power grid: from cyber control and communication to physical manifestations of failure, in: Proceedings of International Conference on Computer Safety, Reliability, and Security, 2009.
[74] D. Wei, Y. Lu, M. Jafari, P. Skare, K. Rohde, An integrated security system of protecting smart grid against cyber attacks, in: Proceedings of IEEE PES Conference on Innovative Smart Grid Technologies, 2010.
[75] G.N. Ericsson, Cyber security and power system communication – Essential parts of a smart grid infrastructure, IEEE Transactions on Power Delivery 25 (3) (2010) 1501–1507.
[76] G.N. Ericsson, Information security for electric power utilities (EPUs) – CIGRE developments on frameworks, risk assessment, and technology, IEEE Transactions on Power Delivery 24 (3) (2009) 1174–1181.
[77] T. Sommestad, M. Ekstedt, L. Nordstrom, Modeling security of power communication systems using defense graphs and influence diagrams, IEEE Transactions on Power Delivery 24 (4) (2009) 1801–1808.
[78] G. Ramos, J.L. Sanchez, A. Torres, M.A. Rios, Power systems security evaluation using petri nets, IEEE Transactions on Power Delivery 25 (1) (2010) 316–322.
[79] P. McDaniel, S. McLaughlin, Security and privacy challenges in the smart grid, IEEE Security and Privacy 7 (3) (2009) 75–77.
[80] H. Khurana, M. Hadley, N. Lu, D.A. Frincke, Smart-grid security issues, IEEE Security and Privacy 8 (1) (2010) 81–85.
[81] L. Nordstrom, Assessment of information security levels in power communication systems using evidential reasoning, IEEE Transactions on Power Delivery 23 (3) (2008) 1384–1391.
[82] S. Sheng, W.L. Chan, K.K. Li, X. Duan, X. Zeng, Context information-based cyber security defense of protection system, IEEE Transactions on Power Delivery 22 (3) (2007) 1477–1481.
[83] J. Jaeger, R. Krebs, Automated protection security assessment of todays and future power grids, in: Proceedings of IEEE Power and Energy Society General Meeting, 2010.
[84] N. Kuntze, C. Rudolph, M. Cupelli, J. Liu, A. Monti, Trust infrastructures for future energy networks, in: Proceedings of IEEE Power and Energy Society General Meeting, 2010.
[85] S. Clements, H. Kirkham, Cyber-security considerations for the smart grid, in: Proceedings of IEEE Power and Energy Society General Meeting, 2010.
[86] A.R. Metke, R.L. Ekl, Security technology for smart grid networks, IEEE Transactions on Smart Grid 1 (1) (2010) 99–107.
[87] Y. Liu, P. Ning, M. Reiter, False data injection attacks against state estimation in electric power grids, in: Proceedings of ACM Computer and Communication Security, 2009.
[88] J. Chou, B. Lin, S. Sen, O. Spatscheck, Proactive surge protection: a defense mechanism for bandwidth-based attacks, in: Proceedings of USENIX Security Symposium, 2008.
[89] D. Choi, H. Kim, D. Won, S. Kim, Advanced key-management architecture for secure SCADA communications, IEEE Transactions on Power Delivery 24 (3) (2009) 1154–1163.
[90] M. Kim, J.J. Metzner, A key exchange method for intelligent electronic devices in distribution automation, IEEE Transactions on Power Delivery 25 (3) (2010) 1458–1464.
[91] D. Choi, S. Lee, D. Won, S. Kim, Efficient secure group communications for SCADA, IEEE Transactions on Power Delivery 25 (2) (2010) 714–722.
[92] I.H. Lim, S. Hong, M.S. Choi, S.J. Lee, T.W. Kim, S.W. Lee, B.N. Ha, Security protocols against cyber attacks in the distribution automation system, IEEE Transactions on Power Delivery 25 (1) (2010) 448–455.
[93] K.M. Rogers, R. Klump, H. Khurana, A.A. Aquino-Lugo, T.J. Overbye, An authenticated control framework for distributed voltage support on the smart grid, IEEE Transactions on Smart Grid 1 (1) (2010) 40–47.
[94] B. Daemi, A. Abdollahi, B. Amini, F. Matinfar, Digitally-signed distribution power lines: a solution which makes distribution grid intelligent, IEEE Transactions on Power Delivery 25 (3) (2010) 1434–1439.
[95] H. Chan, A. Perrig, Round-effcient broadcast authentication protocols for fixed topology classes, in: Proceedings of IEEE Symposium on Security and Privacy, 2010.
[96] Q. Wang, H. Khurana, Y. Huang, K. Nahrstedt, Time-valid one-time signature for time critical multicast data authentication, in: Proceedings of IEEE INFOCOM, 2009.
[97] U.K. Premaratne, J. Samarabandu, T.S. Sidhu, R. Beresh, J.-C. Tan, An intrusion detection system for IEC61850 automated substations, IEEE Transactions on Power Delivery 25 (4) (2010) 2376–2383.
[98] G.M. Coates, K.M. Hopkinson, S.R. Graham, S.H. Kurkowski, A trust system architecture for SCADA network security, IEEE Transactions on Power Delivery 25 (1) (2010) 158–169.
[99] P. Venkitasubramaniam, L. Tong, Anonymous networking with minimum latency in multihop networks, in: Proceedings of IEEE Symposium on Security and Privacy, 2008.
[100] DNP Users Group, DNP3 Specification. <http://www.dnp.org>.
[101] IEEE, IEEE Standard for SCADA and Automation Systems. <http://www.ieee.org>.
[102] IEEE, IEEE Recommended practice for data communications between remote terminal units and intelligent electronic devices in a substation. <http://www.ieee.org>.
[103] IEEE, IEEE Application guide for IEEE Std 1547, IEEE standard for interconnecting distributed resources with electric power systems. <http://www.ieee.org>.
[104] IEEE, IEEE guide for monitoring, information exchange, and control of distributed resources interconnected with electric power systems. <http://www.ieee.org>.
[105] IEEE, IEEE standard conformance test procedures for equipment interconnecting distributed resources with electric power systems. <http://www.ieee.org>.
[106] IEC, International Standard IEC 60870. <http://www.iec.ch>.
[107] IEC, International Standard IEC 61850. <http://www.iec.ch>.
[108] IEC, International Standard IEC 61968. <http://www.iec.ch>.
[109] IEC, International Standard IEC 61970. <http://www.iec.ch>.
[110] IEC, International Standard IEC 62351. <http://www.iec.ch>.
[111] NIST, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0. <http://www.nist.gov>.
[112] NIST, Guidelines for smart grid cyber security. <http://www.nist.gov>.
[113] IETF RFC 3447, Public-key cryptography standards (PKCS) #1: RSA cryptography specifications version 2.1. <http://www.ietf.org/rfc/rfc3447.txt>.
[114] Q. Wang, H. Khurana, Y. Huang, K. Nahrstedt, Time valid one-time signature for time-critical multicast data authentication, in: Proceedings of IEEE INFOCOM, 2009.
[115] L. Reyzin, N. Reyzin, Better than biba: short one-time signatures with fast signing and verifying, in: Proceedings of Seventh Australasian Conference on Information Security and Privacy (ACISP), 2002.
[116] R. Canetti, J. Garayt, G. Itkid, D. Micciancios, M. Naore, B. Pinkasll, Multicast security: a taxonomy and some efficient constructions, in: Proceedings of IEEE INFOCOM, 1999.
[117] A. Perrig, R. Canetti, D. Song, J. Tygar, Efficient and secure source authentication for multicast, in: Proceedings of Network and Distributed System Security Symposium, 2001.

Wenye Wang received the M.S.E.E. and the Ph.D. degrees from the Georgia Institute of Technology, Atlanta, Georgia, in 1999 and 2002, respectively. She is now an Associate Professor with the Department of Electrical and Computer Engineering, North Carolina State University. Her research interests include mobile and secure computing, modeling and performance analysis of single- and multi-hop wireless networks, network topology and architecture design. Dr. Wang serves as the leader of the Reliable and Secure Communications Subthrust in the FREEDM Systems Center since 2008. Her research in the FREEDM Systems Center focuses on the provision of timely, reliable and secure information exchanges in the smart grid. Dr. Wang is a recipient of the NSF CAREER Award 2006. She is the co-recipient of 2006 IEEE GLOBECOM Best Student Paper Award – Communication Networks, and the co-recipient of 2004 IEEE Conference on Computer Communications and Networks (ICCCN) Best Student Paper Award. She has been a member of IEEE and ACM since 1998, and a member of Eta Kappa Nu and Gamma Beta Phi Honorary Societies since 2001.



Yi Xu received the B.E. degree from the Huazhong University of Science and Technology, China, in 1998, the M.E. degree from the National University of Singapore, Singapore, in 2002, and the Ph.D. degree from the North Carolina State University, USA, in 2010, respectively. He worked as a research engineer in the Institute for Infocomm Research, Singapore, from 2001 to 2005. He is currently a postdoctoral research associate in the Department of Electrical and Computer Engineering, North Carolina State University. His research interests include performance modeling and analysis of large-scale wireless networks, network resilience to mobility and failure, network security, and network applications in the smart grid power systems. He is an IEEE member.

Mohit Khanna completed his Bachelors in Technology in Electronics and Communication Engineering from Guru Tegh Bahadur Institute of Technology, Guru Gobind Singh Indraprastha University, India. He worked as a software engineer with Xansa, India (now Steria) for 1.3 years. He also worked with Mtree Solutions for 8 months. Mohit joined the Electrical and Computer Engineering Department at North Carolina State University in August 2007 for Masters in Computer Engineering. He did his summer internship (May–August 2008) with Qualcomm, San Diego, with the WCDMA Integration team. Since August 2008, Mohit has been working with Dr. Wenye Wang as a master's thesis student on the FREEDM project, with focus on a reliable and secure communication backbone for the FREEDM system. He graduated with the Master degree in May 2009.