Resilient Communication for Smart Grid Ubiquitous Sensor Network: State of the Art and Prospects for Next Generation

Yakubu Tsado[a,1], David Lund[b], Kelum A.A. Gamage[a]
[a]Department of Engineering, Lancaster University, Lancaster, Lancashire, LA1 4YR, UK
[b]HW Communications Ltd., Parkfield, Greaves Rd, Lancaster, Lancashire, LA1 4TZ, UK

Abstract—Smart grid combines a set of functionalities that can only be achieved through ubiquitous sensing and communication across the electrical grid. The communication infrastructure must be able to cope with an increasing number of traffic types which is as a result of increased control and monitoring, penetration of renewable energy sources and adoption of electric vehicles. The communication infrastructure must serve as a substrate that supports different traffic requirements such as QoS (i.e. latency, bandwidth and delay) across an integrated communication system. This engenders the implementation of middleware systems which considers QoS requirements for different types of traffic in order to allow prompt delivery of these traffic in a Smart grid system. A heterogeneous communication applied through the adaptation of the Ubiquitous Sensor Network (USN) layered structure to smart grid has been proposed by the International Telecommunication Union (ITU). This paper explores the ITU's USN architecture and presents the communication technologies which can be deployed within the USN schematic layers for a secure and resilient communication together with a study of their pro's and con's, vulnerabilities and challenges. It also discusses the factors that can affect the selection of communication technologies and suggests possible communications technologies at different USN layers. Furthermore, the paper highlights the USN middleware system as an important mechanism to tackle scalability and interoperability problems as well as shield the communication complexities and heterogeneity of Smart grid.

Keywords- USN architecture; Resilience; Smart grid; Heterogeneous communication; Middleware

1. INTRODUCTION

Smart grid deployment is motivated by ambitious goals such as energy savings, efficient and sustainable power supply, reducing greenhouse gas emission and attaining satisfactory levels of security and quality of energy supply [1]. Achieving the smart grid goals will involve a set of functionalities within generation, distribution and consumer premises rather than a set of individual appliances or technologies [1], [2]. Self-healing, Demand Side Management (DSM) and seamless integration of renewable energy through distributed generation are desired functionalities that can only be achieved by having a converged and secure communication infrastructure that can intelligently and reliably deliver the aforementioned smart grid functionalities [4]. Converged communications networking, routing and transport protocols and QoS support for smart grid functionalities will enable the system to increase its efficiency to a much greater extent [53]. The electrical grid incorporates different types of systems, devices and communication media with specialised procedures for exchanging data. For example, Supervisory Control and Data Acquisition (SCADA) system with Remote telemetry Unit (RTU) and Programmable Controllers are used on the power grid for monitoring and control purposes using wired or wireless communications with proprietary protocols [54-55]. Expanding the communication network by integrating the existing communication infrastructure with new ones will introduce new complexity and vulnerabilities such as: (i) security, (ii) efficiently aggregating, storing and analyzing data, and (iii) coordinating diverse technologies (communications and electricity) which have diverse capabilities and characteristics that are not well defined [3], [53]. Neither agreement nor consensus has been reached on which communication technologies should be chosen to achieve a cost effective and reliable smart grid communication, in order to integrate, secure and manage the next-generation smart grid. However in the absence of standardisation for interoperable smart grid protocols, there is an assumption that all smart grid traffic types will use Internet Protocol (IP). IP can provide addresses to numerous communication devices on the grid thus ensuring a flexible communication platform with improved interoperability and also providing support for asset management as compared to bespoke protocols [4]. It has become an increasingly used

[1] Corresponding author- Tel: +44 1524 888604; *E-mail address:* y.tsado1@lancaster.ac.uk

protocol stack in supervisory and control applications in the energy sector and a document on how best to profile the IP suit in Smart Grid has been presented in [5]. Therefore, it is a boost that existing IP communication technologies will play significant roles in incorporating:

- DSM interaction between customers and suppliers through smart meters
- Self-healing power restoration capability; and
- Distributed Energy Resources (DER) from renewable energy that will be used to supply energy during peak loads.

Deploying existing communication technologies for smart grid functionalities depends on certain properties which may be influenced by a number of requirements from smart grid applications. Several articles have been published, with emphasis on and selecting and optimisation of communication technologies that will meet these requirements. In [6], a number of candidate communications technologies for Home Area Network (HANs) have been compared with emphasis on DSM and dynamic pricing. Factors affecting the choice of communication technologies have also been discussed, which provide a comparison based on different scenarios. In [7], a review of wireless communication technologies for HANs and Neighborhood area Networks (NANs) together with their smart grid applications is discussed. They highlighted the network issues and challenges and concluded that the choice of communications technology (CT) for smart grid essentially depends on a particular utilities budget and policies. Furthermore, a critical overview of communication systems in smart grids was presented in [53], with a special focus on the role that communication, networking and middleware technologies will have on the transformation of the existing power system in to smart grid.

Nonetheless a flexible and scalable communication network architecture is required to tie together the functions of "Home Energy Management (HEM)", "Distributed Automation (DA)", "DSM", "self-healing", "monitoring" and "control" in smart grid. Consequently, different bodies or groups have been setup to develop interoperability standards for smart grid architectures among which are the IEEE standard P2030 "guide for Smart Grid Interoperability of Energy and Information technology operation with the electrical power system and End-Use Applications and load" and CEN-CENELEC-ETSI Smart Grid Coordination Group were initiated to mention but a few [8]-[9]. The International Telecommunication Union's (ITU) Ubiquitous Sensor Network (USN) architecture is an Information and Communication Technologies (ICT) solution initially designed to mitigate effects of climate change by monitoring the environment through pervasive coverage of sensor networks to support context-aware information services through processing collected climate information. A holistic network architecture based on USN to integrate all the communications required by smart grid applications in a single system has been proposed in [19]. They stated that if the five USN schematic layers is applied to smart grid, it can provide a unified and seamless heterogeneous network that is capable of comprehensively supporting stringent communication requirements of smart grid. The schematic layers of the USN architecture and the corresponding smart grid network components is presented in fig. 1, with the anticipation that this architecture will integrate all the smart grid communication components.

This paper explores the USN architecture for smart grid traffic management and attempts to review candidate communication technologies, to understand which may be best deployed within different parts of the smart grid USN system. The factors that may determine the choice of communication technologies for each USN layer and a use-case to implement the USN architecture for smart grid are also presented in this paper. Also, vulnerabilities and challenges of the USN architecture were discussed and factors that will minimise their effect have been highlighted. The remainder of this paper is organised as follows: Section 2 presents background and overview of related work on smart grid architectures, applications and networks. Section 3 describes the adaptation of the USN architecture for smart grid. The factors necessary for the choice of a secure and resilient communication technology in smart grid are discussed in section 4, while section 5 presents the benefits and limitation of available communication technologies that can be deployed in smart grid heterogeneous network. Smart grid vulnerabilities are discussed in section 6 and section 7 presents a use-case for smart grid heterogeneous communication. Challenges of USN Architecture for Smart Grid are presented in section 8 and finally section 9 outlines the conclusion.

Fig. 1 USN layers with corresponding smart grid network components

2. BACKGROUND AND RELATED WORK ON SMART GRID COMMUNICATION

The network infrastructure in smart grid is expected to be a heterogeneous communication in order to successfully achieve smart grid functionalities and meet performance requirements. There has been an increase in research activities and surveys on smart grid communications network [2], [3], [4], [10], [11], [53], and [57]. This section presents a background on smart grid architectures and smart grid network components. Also, it highlights the smart grid applications and their requirements.

2.1 Background on Smart grid communication Architecture

Smart grid definition by several entities has reiterated the relevance of the communication network to the success of smart grid. Cisco defined smart grid as a data communication network integrated with the electrical grid for capturing information on the activity of transmission, distribution and consumption in near real time [12]. The smart grid technology will then analyse the captured data to provide useful information and recommendation to energy suppliers and consumers on the best way to manage power. Other definitions by the US Department of Energy (DOE) and National Institute of Standards and Technology (NIST) have also emphasised on ICT to be the connection between the smart grid applications and the physical energy infrastructures that use and distribute energy [4]. Key motivations of the new and improved communications infrastructures such as: enhanced customer experience; improved energy utilisation; lower fossil fuel dependence and renewable generation, which are related to power grid efficiency, environment and cost, are highlighted in [13]. The existing systems and services on the power grid include SCADA systems [14], [54] and Automatic Meter Reading (AMR). AMR is a one-way communication to accomplish meter readings primarily for monthly billing purposes [15]: it may use both wired and wireless communication media with specialised rules for exchanging data. Similarly, new services and applications such as Demand Response (DR) and load management will also require the deployment of new wired or wireless communication infrastructures with specific traffic rules and requirements. The specialised rules and requirements discussed here refer to the protocols, routing, network topology (point to point/point to multi-points) and capability to deliver critical communications offered by different communication media in the network. SCADA transmission for remote and local area nodes in wired or wireless networks together with their real time user application protocols are discussed in [14], [54], [55], [56], indicating their needs and requirements. A survey on protocols for Automatic Metering Infrastructure (AMI) communication [16], presented Device Language Message Specification and Companion Specification for Energy Metering (DLMS/COSEM) as a communication standard which enables a data collection system to establish connections over metering devices of different communication protocols and media, thereby allowing a smooth migration from legacy meters to smart ones. They went further to propose Session Initiation protocol (SIP) to handle the communication sessions between a meter and a data collection system. The complexity of meeting the needs of these requirements has led to research activities by institution and government bodies to come up with solutions or architectures to provide a seamless end to end communication network.

A model for smart grid information networks which identifies actors, communication pathways, domain interactions, potential applications and capabilities enabled by the interactions in smart grid was proposed by the US NIST [4]. The model does not define any solution and its implementation, but it aids the analysis of smart grid networks. In an attempt to summarise current research effort in smart grid communication, Baker et al [5] categorised communication networks together with their requirements and identified the need for a hybrid structure with core networks and many edge networks that connects all the suppliers and customers [5]. Another smart grid architecture proposed in a report by the US DOE [17] stated that the scope of smart grid architecture should include market operators, reliability coordinators, generation wholesalers, transmission providers, balancing authorities, energy service retailers, distribution providers, and end users [3]. The West Virginia white paper also proposed that smart grid should be composed of four elements: sensing and measurement, advanced control methods, improved interfaces and decision support, and advanced components [18]. Gao et al [3] and Saputro et al [11] carried out a review of communication/networking and survey of routing issues in smart grid and highlighted the need for more investigations to interoperability, QoS and network optimisation, control and management of operations in smart grid. Furthermore, a comprehensive survey of the role of communication systems in smart grid was also presented in [53] in which they identified the smart grid communication infrastructure as a hierarchical network with a three-tier architecture consisting of: (i) access tier, (ii) distribution tier, and (iii) core tier. The authors went further to analyse the communication infrastructure and middleware systems for smart grid and also stated their challenges in the field. Though the views on communication model shared by the aforementioned research bodies and authors describe and support a heterogeneous communication for a functional smart grid. However these models and architecture have not presented a coherent heterogeneous end to end communication architecture and structure for smart grid.

Zaballos et al [19] proposed a communication paradigm based on smart grid network requirements to support end to end information flow between the application domains in smart grid. This paradigm aims to achieve end to end integration of all communications required by smart grid using the USN architecture. The network architecture successfully adapts and applies the ITU-Telecommunication Standardisation Sector USN Next Generation Network (ITU-T USN /NGN) system to smart grid architecture to allow better management of QoS and facilitate interoperability with other technologies. The vulnerabilities of implementing this architecture and ways by which the architecture will be resilient to failures in the network where not discussed. The next section presents a summary of smart grid network components and smart grid applications that will communicate through the network.

2.2 Smart Grid Network Components

Communications network viewpoint of IEEE P2030 provides network components that interconnect the smart grid generation and distribution as well as the transmission and customer premises to form an end to end smart grid communication model. Figure 2 derived from [8] and [11] shows communication model for the transferal of information from home, business and field areas to the control centers. In [8], IEEE P2030 end to end communication model is made up of a number of sub networks which are described briefly in the following sub sections.

2.2.1 Home Area Networks (HANs)

HANs are private networks located in the customer premises or domain and they can be used to implement Home Energy Management System (HEMS) and home automation that allows monitoring and control applications for user comfort, efficient home management, and DR application of in-home appliances [11]. They also provide access to in-home appliances by allowing every home device send their power readings over the network to the home meter or gateway outside the house for Automatic Metering Infrastructures (AMI) application. HANs are similar to other private networks such as: (1) Industrial Area Networks (IANs): a communication network coupling industrial equipment. Monitoring a network of smart industrial equipment for user comfort, DR and billing and metering data; (2) Building/Business Area Network (BANs): a network of automation implemented to support a building or business premises.

2.2.2 Neighborhood Area Networks (NANs)

NAN can be regarded as a logical representation of AMI system that connects customer premises and the utility control center. HANs have been described earlier as a communication network of appliances and devices within a home which consist of sensors and actuators to carry out end-user activities (monitoring and control applications, metering and DR) [20]. NANs can be said to involve networks of multiple HANs that deliver the metering data to data-concentrators and also deliver control and information data to HANs. Many wireless metering gateways of home/field areas may connect to each other to form a possible wireless mesh network [3]. For example smart meters acting as gateways for in-home application data can be used as wireless mesh nodes to transfer information. Smart meters are the major constituent of NAN which acts as the interface between private networks and Utility control centers. NAN end points are either smart meters at the customer end or data concentrators to a group of smart meters at the utility end which send the aggregated information to the Meter Data Management System (MDMS) via a backbone network [21].

2.2.3 Field Area Network (FANs)

A FAN is a network of field devices such as feeder equipment, transformer, switches and circuit breakers in the transmission and distribution substations that facilitates information exchange between utility control centers. High voltages are usually converted to low voltage as required by homes, businesses and industries. Also, the electricity supplies to customer premise are carried out through the distribution feeder equipment which includes transmission lines, cable poles. Smart grid FANs will include remote terminal units (RTUs), Phasor Measurement Units (PMUs) and Programmable controllers to perform substation automation functions. Automation functions using this terminal unit may be carried out according to their embedded logic or by an external operator/utility command which overrides the internal or local commands. FAN is also responsible for communicating information on DER/micro grids connected to the distribution grid with the utility control [10], [53], and [58].

Fig. 2 Communication network components for end to end communication in Smart Grid

2.2.4 Wide Area Networks (WAN)

WANs are the largest networks for communications to/from data centre. WAN connects smart metering gateways, NANs and FANs with core utility systems and the distribution control system. WAN comprise two types of networks: Backhaul and Core networks [11]. Backhaul networks are used to connect NAN to the Core network while the Core network is used to connect metro network of the utility and substations. WAN coverage spans over thousands of square miles and is used to deliver the large amount of data collected by the highly dispersed smart grid network components to the controls centre.

2.2.5 Mobile Workforce Networks

Mobile Workforce networks are used to provide routine maintenance and operation services by the utility workforce/employees. The network requirements include broadband connectivity that will enhance VOIP, Virtual Private Network (VPN) and geographic information system (GIS) based applications for asset management and logistics. In addition in-vehicle applications and fleet telematics such as Automatic Vehicle Location (AVL) and location-based services (LBS) with global positioning system (GPS) based tracking and navigation are expected to be integrated with WMN [22].

2.3 Smart Grid Applications

There are various smart grid applications that will utilise the network components in section 2.2. These applications have been classified into six functional categories by the US DOE stated in [11], and are expected to have high security, reliability and QoS requirements. The functional categories are briefly explained in the following section:

2.3.1 Advanced Metering Infrastructure (AMI):

The AMI is regarded as the most fundamental and crucial part of smart grid. It is designed to read, measure, and analyse the energy consumption data of consumers through smart meters in order to allow for dynamic and automatic electricity pricing. AMI data requires a two way communication and spans through all the network components of smart grid from the private networks and FANs to WANs. AMI goes beyond Automatic Meter Reading (AMR) scenarios which according to IEC 61968-9 only have to do with meter reading, meter events, grid events and alarms. AMI will include customer price signals, load management information, power support for prepaid services, Home Energy Management Systems (HEMS) and Demand Response (DR) [22]. It can also be used to monitor power quality, electricity produced or stored by DER units as well as interconnect intelligent electronic devices (IED) [53]. In addition, AMI is also expected to support customer switch between suppliers and help in detection and reducing electricity theft. Electricity theft has plagued many utilities companies especially in developing countries. To address these issues, authors in [23] have reviewed electricity theft and reduction issues using security and efficient AMI infrastructures.

2.3.2 Demand Side Management (DSM*)*

DSM is the action that influences the quantity or pattern of energy consumption by end users. These actions may include targeting reduction of peak demand by end users during periods when energy supply systems are constrained. Energy peak management does not necessarily decrease the amount of total energy consumption, but it will reduce the need for investments on power generation sources or spinning reserves at peak periods [10], [47]. DSM includes the following:

- DR which enables the utility operator to optimally balance power generation and consumption either by offering dynamic pricing programs or by implementing various load control programs.
- Load management through dynamic pricing which helps to reduce energy consumption during peak hours by encouraging customers to limit energy usage or shifting demand to other periods. Existing dynamic pricing programs include: Time-of-use (TOU), Real Time Pricing (RTP), Critical Peak timing (CPT) and Peak time Rebates (PTRs)
- Conservation of energy through load control program which involve performing remote load control programs where communicating networks are used to control usage of appliances remotely to use less energy across many hours.

2.3.3 Wide Area Situational awareness (WASA)

WASA involves near real-time monitoring, protection and control of power grid across large geographical areas. In simple terms it requires collating information on the description of the current state of the power grid over a large geographical. Then, this information can be analyzed, for instance to diagnose current situation or predict the evolution of the power grid state under different operational conditions and energy control strategies [60]-[62]. This application requires very high frequency or granularity of information in order of milliseconds collected from the transmission networks and electric substations about the state of the power grid [10], [15]. The information is used to provide timely prevention of power disruption and also optimise the performance of the grid. WASA information is used to implement monitoring (Wide Area Monitoring Systems -WAMS), Control (Wide Area Control Systems -WACS) and for Protection (Wide Area Protection Systems -WAPS) [21], [59].

2.3.4 Distributed Energy Resource (DER) and Storage:

Energy resources from renewable sources that can be integrated in to the power grid to complement bulk generation may reside at the transmission, distribution or even at end user systems. Energy storage is also necessary to allow storage of surplus electricity at a given time for distribution thereafter or to compensate for the energy generation fluctuation from renewable sources. A reliable and effective communication infrastructure is needed with low latency all through the Smart Grid network to coordinate and integrate the DER activities with Distribution Management Systems [15], [48].

2.3.5 Electric Vehicle (EV) Monitoring and Control*:*

This involves monitoring the activities of plug-in electric or hybrid electronic vehicles (PEV or PHEV) that are expected to enhance or replace fossil fuel transportation systems. Electric Vehicles (EV) use one or more electric motors which are powered by a rechargeable storage in the vehicle. The connection of the electric storage or EV to the electrical grid to recharge is called Grid to Vehicle (G2V) flow. While in situations where an EV is used to reduce peak demand when it is not being used by connecting it to the electrical grid to discharge electric power back to the grid, is known as Vehicle to Grid (V2G). Consequently, EV charging systems must be well managed as high concentrations of charging requests within a short period can cause severe overloading in distribution network. Smart charging concepts which enables controlled charging have been proposed in several literatures to mitigate the problem of overloading the distribution circuit [21], [49].

2.3.6 Distributed Grid Management (DGM)*:*

This encompasses the various smart grid automation technologies for real-time information and remotely controlled devices. This also provides utilities with a comprehensive suite of applications and tools for efficient, reliable and cost effective management of distribution network. The applications involve technologies that can integrate different grid applications with each other such as Distribution Automation (DA), Video Surveillance, SCADA and Automatic Vehicle Location (AVL) which is used to give the workforce direction to the fault location that needs to be repaired [22], [48].

Smart grid application requirements, including criticality factors such as bandwidth and latency, across the network components differ for different applications as illustrated in Table 1. Integrating the smart grid network components that will allow functionality of the applications will therefore require good interoperability among different technologies and meet QoS for different traffic classes. Essentially, the criticality of each smart grid application must be enabled through the resilience of the integrated network components and their capabilities to deliver application data with the most appropriate QoS for the application.

Table 1 Smart grid Applications network bandwidth and latency requirement [4]

3. ADAPTATION OF USN SCHEMATIC LAYERS FOR SMART GRID

Integrating the actions of consumers and generators in an electrical grid will involve a system of distributed sensor nodes that will interact with both themselves and the electrical infrastructure, to provide and process information extracted from the physical world. Applications of sensor nodes can be assigned to any of the following three broad categories which are very useful elements in smart grid applications [24]:

- Detection – e.g., temperatures of transformers, intruders on electrical equipment.
- Tracking – e.g., house hold items or equipment, supply and distribution of electricity, plug in electrical vehicles in intelligent transport systems.
- Monitoring – e.g., monitoring of inhospitable environments such as volcanoes, hurricanes and storm that may affect the grid.

To achieve communication over long distances, sensor networks may require routing and multi-hop protocols which can increase delay and reduce the reliability of the communication network. Adapting the USN architecture for smart grid sensors network will allow communication over long distance and provide reliable heterogeneous communication systems which define interoperability with a NGN as the smart grid back bone [19]. Fig. 3 shows the proposed schematic model of USN architecture applied to smart grid. USN's capabilities to support requirements for AMI have been discussed in ITU Telecommunications standardisation sector (ITU-T) Question 25/16, "Framework of USN applications and services for smart metering (F.USN-SM)". Zaballos et al [19] also discussed a similar approach but with emphasis on a network architecture that will integrate all the communications requested by smart grid applications in a single system. The schematic model in Fig. 3 depicts communication between the USN sensor networking layer through the access network to the USN applications and services. The description of smart grids activity in each layer together with the required network component is presented in the following section.

Fig 3 Schematic layers of the USN sensor network applied to smart grid [24]

3.1 USN sensor network layer for Smart Grid application

The areas of the electricity system where tracking, monitoring, detection and physical quantities are measured are the FANs, IANs, BANs and HANs. Energy management and automation of equipment and appliances in residential and institutional buildings, industrial facilities, transmission lines, substations and distribution systems require the use of sensors and actuators. A network of interconnected sensor nodes are expected to measure and exchange sensed data within BANs, IANs, FANs and HANs through wired or wireless

processing and then communicate with other networks through USN gateways or Access points. For example in HAN, appliances and related fittings can be monitored through the activities of sensor nodes and communicated to the sensor gateway or access point which is mostly smart meters. The aim of home automation and energy management as discussed earlier is to bring about control and monitoring signals from appliances, and basic services. A similar interconnection of sensor nodes is also expected in the FAN which comprises substation monitoring, control and protection of distribution system and transmission system.

3.2 USN access network layer for smart grid application

Access networks basically involve USN intermediary or "sink nodes" collecting information from a group of sensors or sensor networks that will facilitate communication with a control center or with utilities. For example, transmitting information received from smart appliances in HAN to the Utilities/AMI control center through smart meters or NANs. Similarly in FANs, field devices such Remote Terminal Units (RTUs) and Programmable logic controllers can be used to send information about the electrical grid to external operators or utilities. Sending the information to utilities can be achieved by having a field device to transmit information to the utility/control centers through WANs or backbone networks that are connected to FANs. Smart meters and RTU's can serve as access points/gateways and have WANs provide the links to Utilities, Distribution Management Systems (DMS), AMI, and other smart grid applications control centres.

3.3 USN NGN layer for smart grid application

In simple terms the USN NGN is a backbone network infrastructure expected to perform only data transport that will enhance a two-way communication between the sensor nodes and the USN access network. Selection of a common transport layer based on the internet protocol (IP) for smart grid is advocated by many authors and research groups [20]. However achieving this goal requires a number of developments to successfully encapsulate legacy protocols within IP [25], whilst addressing the need for strict QoS. The development of protocols for sensor networks as well as internetworking with backbone network infrastructures such as NGN is one of the most important standard issues for USN [24]. For this purpose, ITU-T's recommendation in Y.211 defines a generic end-to-end architecture for the Quality of Service (QoS) resource control in NGNs. It aims to provide QoS management of new end-to-end services and multimedia communications through diverse NGNs. The ITU NGN model has also suggested an Open Service Environment (OSE) capability [26] that will allow the creation of enhanced and flexible services based on the use of standard interfaces, reuse, portability, and accessibility of services.

3.4 USN middleware layer for smart grid application

Middleware system is a software layer running above the communication network, which enables communication and data management services for distributed applications. In [53], the middleware system was described as a major component of smart grid communications because it provides standard interfaces between applications and smart grid devices. Middleware solutions also provides different set of abstraction and programming interfaces to applications which include distributed objects, event notifications, distributed content management and synchronous/asynchronous communication functions.[53], [63].

In the context of the USN architecture, middleware is responsible for translating information between the NGN and USN application layer, which refers to the smart grid application and control center. USN has different standardisation activities [24] which have identified the need for a middleware in order to have an efficient heterogeneous operation system between various sensors and communication technologies. Without a middleware system direct interaction between components of the smart grid communication architecture will lead to a large number of use cases and complexity of the system. This is because direct communication with smart grid application through different communication technologies will bring about consideration of loads of specification. One method of alleviating the complexity of such a system is by using a lower number of communication standards in the middleware. The middleware can also provide a level of abstraction from the complexity and heterogeneity of the communication networks and management of distributed applications, by providing an API that encapsulates the access to technologies being used. Instead of having a smart grid communication on direct application-to-application connections, a USN architecture middleware solution should be preferred. A middleware communication bus is illustrated in fig. 4.

The Electronics and Telecommunications Research Institute's (ETRI) Common System for Middleware of Sensor Networks (COSMOS) was recommended as a middleware for the smart grid USN architecture for in [19]. COSMOS is designed to provide integrated data processing over multiple heterogeneous sensor networks based on sensor network abstraction (called the sensor network common interface) and to support real field applications [27]. However, enhancement of COSMOS using a service oriented middleware system is required to access devices (sensor nodes) and also support criticality and QoS for smart grid applications [51] [52]. A classification of research trends in the area of middleware systems based on three main categories (middleware

services for data management; object-oriented middleware, and multi-agent systems) have been presented in [53].

Fig. 4 USN middleware communication bus

4. SECURE AND RESILIENT SMART GRID USN ARCHITECTURE

The selection of communication mechanisms to be deployed at different smart grid USN layers will depend on technical and economic factors. This section describes the economic and technical factors necessary for the selection of communication mechanisms to be deployed at the appropriate elements of the smart grid USN.

4.1 Economic factors

- *Accessibility*: Ease of access or the degree to which a communication technology is available to be deployed for smart grid networking purposes. Monitoring and controlling electrical components may be located in remote areas with limited accessibility, i.e. underground feeder cables and meters. Consideration for this limitation must be put in place when deploying a smart grid communication technology.

- *Ownership*: Due to the heterogeneous nature of the smart grid, the communication network infrastructures may span across different owners. They could be public, private or even have a combination of public and private ownership of smart grid communication networks and devices.

- *Installation*: This has impact with respect to the cost, challenges and risks, associated with setting up a communication network. Some communication infrastructures are expensive or take time to install. Assessing the practicalities associated with installation will influence a utility or grid operator in their decision upon which technologies and mechanisms to use for smart grid communications.

- *Running cost*: This is the cost or amount of money expended to operate and manage a communication network over a period of time. It has a huge impact as it recurs throughout the lifetime of the technology.

4.2 Technical Factors

- *Latency*: Latency can be measured as one way or round trip latency. One-way is the time it takes for information to reach its destination from its source while round trip is a measure of one-way from source to destination plus a return transaction (from destination to source). Round trip is mostly quoted because it can be measured from a single point and may represent the 'time-to-acknowledgment, confirmation of delivery or querying data' of a communication event. The time a system spends on deciding the response may or may not be included. Smart grid Latency can be defined as the time between when an event occurred and when it was acted upon by an application. Many critical application have tight delay constraints such that the latency requirements corresponds with a physical reaction time (i.e. control signals may be required to switch a relay to mitigate a short circuit failure within a defined time). Among different types of delays, communication delays which comprise of transmission delays, propagation delays, processing delays and queuing delays add up to smart grid latency. If these delays exceed a required time window the information may not serve its purpose, therefore delays must be examined to understand the overall behaviour of the communication network. For example, application classes like WAMS systems comprise hundreds of Phase Measurement Units (PMU) deployed at various location in a national electrical grid system. Measurements from PMU's are first collected by a PMU data concentrator (PDC) via a local communication network before it is sent to the central control network (CCN) located at the utilities core network via the backhaul communication networks. Communications between PMU's and PDC must be within a strict delay (< 1s) [28]. Similarly, in distribution automation the IEDs deployed in substations are required to send their measurements to data aggregators within 4 ms, while communications between data aggregators and utility control centers require a network latency $\leqslant$8–12 ms [64].

- *Bandwid*th: Bandwidth is measure of the width of a range of frequencies measured in hertz. The ranges of frequencies (i.e. difference between the upper and lower frequencies) are used as boundaries by which data is transmitted in different communication technologies. Every wireless and wired smart grid communication system has a frequency band for transmitting data. The size of frequency bands and payload size affects the quantity of data delivery.

- *Resilien*ce: The ability of a communication network to be able to absorb or mitigate the effect of disruptive challenge. Disruptive challenges could be man-made (power failure, hacker) or natural (weather effects). An operational resilient network for smart grid is expected to continue delivering

essential services even under adverse operating condition and rapidly recovers its full operational services once the conditions *impro*ve. Smart grid system requires a guaranteed data delivery system.

- *Throughput*: Throughput is the actual measure of the amount of data a network channel can deliver when delay is considered. It is measure by calculating the average rate of successful data delivery over a communication channel measured in bits per second (bps). The smart grid network must take in to consideration the throughput of the network being deployed for smart grid in order to ensure the application data requirements are met. Node processors of communication networks must be able to support data volumes for supported applications. For example, PMU's are deployed jointly with Transient fault recorder (TFR) and they generate data volumes about transient fault, voltage swings and trends of 100 MB daily [28]. Data rates of PMU's also ranges between 6kbps – 24 kbps for reporting cycle of under 50 Hz (10 and 25 Hz respectively) [21].

Based on the aforementioned technical factors, table 2 presents latency and data sizes of some smart grid application classes which can also be classified as periodic semi-periodic and event based. The communication technologies deployed for these applications must be able to meet or optimized to me this requirement.

Table 2. Technical Requirement for Smart grid application classes

5. SMART GRID COMMUNICATION TECHNOLOGIES AND THEIR LIMITATIONS

As already stated earlier, networking of smart communications can be carried through wired or wireless media to achieve the required smart grid functionalities. It is also very important for communication systems such as SCADA systems, advanced Intelligent Electronic Devices (IED), as well as advanced distribution sensors have reliable and low latency communication technologies, with good interoperability in order to bring about efficient smart grid functionality. This section presents available wired and wireless communication technologies that may be used in the smart grid USN architecture. A summary of the characteristics the communication technologies for smart grid discussed in the following sections is presented in Table 3.

Table 3 Characteristics of smart grid communication technologies

5.1 Wireless network IEEE 802.15 (WPAN) communications technology

Technology that creates wireless personal area networks (WPAN) can be reused to implement local smart grid networks. Out of all the wireless standards that address mid to high data rates for voice, PC and LANs, [29] stated that there hasn't been any other standard that meets the unique needs of sensors and control devices as well as Zigbee (IEEE 802.15.4). WPAN supports star, tree, and mesh topologies and has standardised 'layers' that facilitate and trade-off features such as low cost, easy implementation, short-range operation, adequate security and very low power consumption. Power consumption varies depending upon the topology being used [29]. Zigbee operates on the 2.4 GHz, 915 MHz and 868 MHz frequency band with direct-sequence spread spectrum (DSSS) modulation technique and, offers data rates of 20-250 kbps [30]. Zigbee network layer provides three routing protocols namely: (1) On-demand mesh routing (2) Tree routing (rooted at the Zigbee coordinator for data collection) and source routing (for sink node to reply back to the end device in many to one communication). The routing protocol that is being used is hinged on the network topology that is deployed [20]. Other Zigbee routing protocols matching the needs of the HAN such as 6LoWPAN, WirelessHART and Enhanced least-hop first routing protocol are discussed in [11].

Zigbee is a good candidate for the sensor network layer such as HAN and FAN where, there is an interaction between sensors and power grid equipment [32]. Zigbee is suitable for Wireless Sensor Networks (WSN) due to its aforementioned features and will find application in smart grid operations such as the control of home appliances by forming HANs and direct load monitoring and control in a substation [31]. Low running cost and implementation as well as low power consumption can be considered as advantages of Zigbee, however, sensors have small physical size that can limit internal memory and processing capacity as well as the battery energy supply.

5.2 Wireless network IEEE 802.11 (WLAN) communications technology

Wireless LAN has experienced phenomenal growth from its inception. It is commonly found on computers and internet access devices such as routers and cable modems, and almost all laptops and tablets. The growth and pervasiveness of WLAN has helped the technology to grow in to consumer electronics devices such as Internet telephony, music streaming, gaming and in-home video transmission [29]. IEEE 802.11n is an extension of 802.11 a/b/g technology that delivers both higher data rates and increased reliability [29]. IEEE 802.11s defines how wireless devices can be connected to create ad hoc WMN networks over the physical layer in the IEEE 802.11 a/b/g/n [19]. Sensor networks can use a combination of IEEE 802.11n and IEEE 802.11s. Detail information of WLAN standards that can be utilized for smart grid can be found in [65], [66], [67], [68].

WLAN, as for any wireless technology, is vulnerable to threats such as traffic analysis, passive/active eavesdropping; man in the middle attack; session hijacking that can lead to Denial of Service (DoS); and replay attacks. WLAN is a potential technology to be used in HAN and FAN [53]. Its challenges are bandwidth, multiple users will reduce the reliability of the network, and installation of WLAN over long distances is expensive thus it's more suitable for short distances and will find application in the sensor network layer of the USN architecture.

Wireless LAN can be deployed for Substation automation and protection, Monitoring and control of remote distributed energy resources and redundant link for distribution automation system. Other areas also include enhanced transformer differential protection, Communication aided line protection, and Inter-substation communication [31]. The capability of 802.11 to meet the data rate requirement of smart grid applications is its major advantage, however, the limited availability of industrial wireless LAN equipment and the fact that wireless LAN security mechanism are well known to be vulnerable. Security considerations must be improved to provide additional protection.

5.3 Wireless network IEEE 802.16 (WIMAX) communications technology

World Interoperability for Microwave Access better known as WIMAX is an IEEE 802.16 approved standard for wireless wide band access. The technology supports speeds of as high as 70 Mbps and a range of up to 48 km [29]. It can be used for wireless networking like the popular Wi-Fi and allows very high data rates for relatively long distances as well as makes ubiquitous internet possible. WIMAX supports point to point, point to multipoint or mesh and hybrid (multi-hop relay) topologies.

WIMAX can be considered for long and short distance communications in smart grid and can find application in core and backhaul network components of smart grid. WIMAX can also be used for real-time pricing; AMR and outage detection and restoration [31]. High data rates are considered as the advantage of WIMAX, nonetheless, the expensive cost, of. WIMAX equipment such as Radio frequency tower and spectrum license that may be required is a limitation..

5.4 LTE and 3GPP cellular networks for smart grid operations

Cellular network technology has constantly evolved to achieve performance and scalability breakthrough across different network generations with varying cell site ranges for different deployment scenarios. It covers huge number of devices and provides ubiquitous coverage worldwide. Third-generation (3G) and fourth-generation (4G) cellular technology Long Term Evolution (LTE) operational frequency bands differs for different countries with higher data transmission rate of 768 kb/s - 100MB/s [31], while the distance depends on the availability of cellular service coverage. The cellular network enables topologies that facilitates non interrupted data flow and can also receive and transmit data from Ethernet and other wired and wireless interfaces [31]; hence it is suitable for adoption for NAN communication mechanism or the USN access layer in terms of the USN architecture. Threats in LTE and 3GPP cellular networks can be classified in to three main sections [32]: (1) the air interface which include traffic analysis and user tracking; (2) attacks on base station which include physical tampering with the base station, fraudulent configuration changes, DOS attacks, and cloning of the base station authentication token; (3) attack against the core network. Both WIMAX and 3GPP cellular network have very good coverage and are most suitable for WAN transmission links between the USN access layer and the application layer systems. Customers will have to pay for using their services and the cost may even be higher if a particular QoS (or critical service level) is required for smart grid traffic.

LTE and 3GPP cellular can also be deployed as SCADA interface for remote distribution substation and Monitoring of remote DERs, wide coverage, and high data rates are considered as the advantages of LTE and 3GPP cellular technologies. Recent developments on Critical features (multipoint communication and point to point modes) currently being added to the 3GPP standards which is to be available in 3GPP release 12 in 2015 will strengthen its capability for smart grid. However, the technology is faced with limitation such as: (1) Call establishment may take time and delay, (2) Drop calls experienced in the network as a result of congestion, poor radio coverage and radio interference can hinder data exchange of critical applications, and (3) QoS capability is available within 3GPP standards but there is no evidence of its thorough implement, nor use beyond basic prioritisation (for consumer) methods.

5.5 Power Line Communication (PLC) for smart grid operations

PLC is a process of data transmission through the electric power grid which was initially just intended to monitor faults on distribution lines but has gained a lot of attention and development over the years for communication in Medium and Low voltage network of the electrical grid. PLC is categorised as Broadband Power Line Communication (BPLC) and Narrow Band Power Line Communications (NBPLC) according to the frequency of operation. NBPLC operates in frequency bands of 9 - 148.5 kHz in Europe and 450 kHz in the US and delivers bit rates from 2 kbps to 500 kbps [33]. While BPLC on the other hand provides throughputs

between 10- 300 Mbps and can be used in home LAN and USN access networks [34]. The power line carrier provides a harsh environment for data transmission which leads to a continuously changing channel conditions. This brings about varying throughput to ensure a required QoS [19]. A lot of research and pilot projects have been initiated with aims of investigating and developing communication platforms for smart grid applications [33].

A combination of Zigbee and PLC will provide a good concept of interconnecting sensor nodes in LV and MV levels of the grid. These solutions can be considered for smart grid applications such as AMI, SCADA and video surveillance. PLC is a suitable technology for the USN sensor network, USN access network and even for the NGN because it is potentially accessible to every customer and can reach every location on the grid even underground cables that are not readily accessible by wireless communication technologies.

PLC also has the advantage of being owned by the grid operator which allows control of the communication network. Furthermore, low cost of implementation and no license fees, nor service overhead from providers and the permanent connection accessibility compared to other technologies is considered as a major advantage of PLC technologies.

The down side of PLC is that signals cannot propagate across electrical transformers and high technical efforts are still required for improvement of this technology to address these limitations. Also, data rate limitations of NBPLC may affect transmitting information from USN NGN layer to the application layer or utility because of the large volumes of data that may be involved. In most PLC network deployment, transmissions over transformers have been carried out using a bridge (coaxial or optical cable) over the transformer.

5.6 Optical Fiber communication for smart grid operations

Transmission of data through pulses of light over optical fiber has been used by many communication applications and forms the main backbone of the internet that we all use daily. Optical fibers offer benefits over copper cables because they have very low interference and attenuation which enables transmission of data over long distances and suitable for high demand applications. The fiber optic cable distance coverage is an average of 62 miles compared to 1.2 miles distance coverage by copper before the signal is boosted or regenerated [35]. Fiber-optic is a potential candidate for smart grid applications because it is immune to electromagnetic interference, reliable, has low latency and high data capacity which are desired properties of a smart grid NAN and WAN communication technology [36]. They are suitable for the USN access network and NGN layers of the USN architecture for smart grid. Security concerns relate mainly to the physical intrusion onto the fibers. Once an intruder gains access to the fiber, information is easily compromised. Tight physical access control to fiber needs to be implemented [35]. The major factors affecting its choice are high cost of installation which may not be an issue if the running cost and maintenance cost are considered over a period of time. Applications of fiber-optics for smart grid operations are in areas of inter-substation communication. They can also be installed along transmission lines and underground facilities to provide communication links with back end systems. Despite the high data rates and throughput provided by fiber-optics technologies, cost of implementation and installation is a limitation that can undermine its deployment for smart grid.

5.7 Terrestrial Trunk Radio (TETRA) communications for smart grid operations

Tetra is targeted primarily at the mobile radio's need for critical communication from applications such as public safety (police, security services, military services, ambulance and fire departments) but has also attracted the attention of utility companies. TETRA's operating frequency is between 380 MHz to 470 MHz in the EU and 806 MHz and 912 MHz in Asia, defining 5 MHz band for emergency services and 10 MHz band for civil services. The standard defines 24 kHz carrier for both uplink and downlink channel [37]. The main objective of TETRA is to have standard interfaces, facilities and services such as guaranteed interoperability, versatility, efficiency, robustness and security. It is a standard solution for groups that use both Private/Professional Mobile Radio (PMR) and Public Access Mobile Radio (PAMR). It takes its features from several technology areas such as mobile radio, digital cellular telephone, paging and wireless data. TETRA Enhanced Data services (TEDs) has evolved from TETRA to address the needs of data extensive applications [37]. Tetra is applicable for USN access network for smart meters. TETRA is known to have good reachability (i.e. being able to penetrate through walls), makes it also suitable for the sensor network layer (HAN and smart metering communications).

Tetra can also provide WAN links between USN access networks and the application layer and will find application in smart metering or connecting residential to the grid. The challenge of using Tetra in smart grid is its low throughput and licensing and equipment cost. However, its implicit communication criticality, impulse resilience and resilience to other propagation constraints are very good advantages for smart grid. In addition,

Tetra's long range distance which is as a result of its low transmission frequency will also enhance its deployment for smart grid.

5.8 Digital Subscriber Lines (DSL) communications for smart grid operations

DSL refers to a family of technologies that carry out digital transmission over telephone lines. The technology is currently being used to provide broadband internet services to clients. The DSL technology family include the basic Asymmetric DSL (ADSL), ADSL2^{+}, ADSL2^{++} and the Very High bit rate DSL (VDSL or VHDSL). As the name implies VDSL provides the faster data transmission in short distances of up to (52 Mbps downstream and 16 Mbps upstream) over copper wire and (up to 85 Mbps down and up link) on coaxial [53]. The second generationVDSL2 systems are expected to improve on existing ones with achievable data rates of 100 Mbps on both up and down link at a range of 300 m. Key advantage of using DSL for smart grid technologies is the possibility of interconnecting residential areas with control centres thereby avoiding installation cost of deploying their own private network. However, it will attract a running cost or rental fee to the DSL communication operators.

5.9 Visible Light Communications (VLC) for smart grid operations

VLC is a sub-category of optical wireless communications amongst which are Infrared and Ultra Violet communications. VLC communications takes place by modulating the intensity of the LED light in such a way that it is undetectable to the human eyes then using a photo sensitive detector as a receiver to demodulate the light signal into electronic form [69]-[70]. In simple terms, it increases the purpose of LED light from just illumination to both illumination and communication. VLC can serve as an alternative to radio wave wireless technologies because of the growing challenges of radio wave communications such as: (i) increase in demand of spectrum and congestion in communication channels (ii) inefficient usage of power and (iii) reduce health risks associated with radio frequency signals on humans [71]-[72]. Current and potential VLC applications include: Transport systems, Smart traffic systems, Dangerous and extreme environments, real-time audio and video transmission, Hospitals, Industrials, Public sector, and Homeland Security Defense [71], [72], [73]. With regards to smart grid it can find application in HEMs, HANs and distribution grid management. VLC is still new and technical enhancements and standardization activities are still been carried out on physical and medium access layers such as the P802.15.7 IEEE draft standard published in November 2010. VLC can transmit signal for up to 500 Mbps for a distance of 5 meters and at low data rates it can transmit up to a distance of 1 to 2 km. The Home Gigabit Access Project (OMEGA) in 2010 enabled the transmission speed of 1 Gbps via a heterogeneous network which included VLC, Infrared and PLC.

The advantages of VLC when deployed for smart grid is that it is license-free and it is not associated with any charges. It also has low cost front end devices as well as an unregulated huge bandwidth for point to point communications. In addition, VLC can be combined with other communication technologies such as PLC to increase data rate and communication distance. There are many severe technical limitations with VLC since it is still in its early stages, this includes: Multipath distortion, Line Of Sight, interference from sun light etc. The ongoing VLC research activities and standardization can be extended towards its consideration for smart grid deployment.

6. VULNERABILITIES AND CHALLENGES OF SMART GRID COMMUNICATIONS

The distributed intelligence and ICT communication capabilities that will bring about a functional smart grid may create new vulnerability in the electrical grid that will compromise smart grid's success if the communications infrastructure is not deployed and operated with appropriate measures. In [38] and [39], it is argued that smart grid is a disaster waiting to happen "The 'smarter' the power grid is, the more vulnerable the power grid". Some power utilities are also sceptical about deploying smart grid applications because they are yet to grasp the implications of some of these vulnerabilities. Most of the vulnerabilities of communications technologies are in the areas of security and the imperfection of the communication systems. Security and communication imperfections are presented in the following subsections:

6.1 Security

The reality about smart grid is that because of the services that smart grid provides through interconnection and integration, the grid becomes a target for criminal acts terrorism and disruption. Even if motivations behind targeted attack on the smart grid is not driven by terror or disruption, the evolving threat scenarios shows that the potential financial gains can seduce individuals and the cybercriminal network. An intrinsic security strategy must be deployed to safe guard the critical infrastructure and gain the confidence consumers and utilities. Failure to address these problems will hinder the modernisation of the existing power system in terms of smart grid functionalities and the paying consumers trust and acceptance. Smart grid security comprises of

the following 3 classes- privacy, cyber and physical security and a brief explanation to this security classes is given in the following subsections.

6.1.1 Cyber security:

The extension of the power grid communications could make protecting the power grid from a cyber-attack a far more complicated mission, because extra nodes on a network can become new openings for intruders. Cyber vulnerability issues spans across all the information and communication infrastructures on the grid and they can be grouped in to the following categories:

- Operational systems: SCADA systems, energy management systems and other intelligent systems that control the flow of power.
- IT systems: PCs, servers, mainframes, applications, databases, web sites, web services, etc.
- Communications networks and protocols.
- End points: Smart meters, EVs, smart phones and other mobile devices.
- Human factors: Lack of training and awareness, social engineering attacks, phishing attacks, misuse of USB drives, etc.

The type of attacks on this infrastructures include, unauthorised smart metering data access, smart metering data repudiation, power theft without notice, attacking smart grid infrastructure to cause power outage, disrupt network availability or terrorist activities [50], [74], [75], [76]. Adequate security measures such as encryption, authentication, public key infrastructure and packet delivery integrity must be put in place [53], [77]. A report by European Smart Grid Coordination Group (SGCP) on Smart Grid Information and Security (SGIS) reported that the standards needed to establish the basis of smart grid security are available, but there is a need for enhancement [40], [41]. They also suggested additional standards to integrate smart grid specific needs with particular attention paid on implementing them at organisation and in system components.

6.1.2 Physical security:

Unlike the traditional power system, smart grid will simultaneously expand the infrastructure and network components (communication and electrical components) for transporting electricity. This will present a more physically challenging infrastructure to protect because most of these infrastructures are out of the customer, utility and grid operator's premises. This added component increases the number of insecure physical locations and makes them vulnerable to physical access. Four layers of physical security that must work to complement each other in smart grid include environmental design, mechanical and electronic access control, intrusion detection and video monitoring [42].

6.1.3 Privacy:

There are also concerns about the real identity of the customer during the power usage. Studies have shown that it is possible to extract personal information about people living in a household by analysing their meter data [39], [43]. Privacy has to do with protecting the customer's private information from the power operator, because from the customer's point of view power operators as well as its control centre and substations are only semi trusted. Concerns about privacy has called for several research work, such as the identity privacy preservation and message request confidentiality scheme based on blind signature credential presented in [44]. National data protection laws and regulations must be fulfilled, but also the operator has to maintain trust with their customers. Data breaches are on the increase and must be contained, especially when important monitoring information about a consumer daily, hourly or even real time usage of electrical/energy appliances are involved.

6.2 Communication system Imperfection:

Communication system imperfections refer to failures or distortion that can occur in a network from natural events which may lead to lost or delayed end to end delivery of smart grid data. Smart grid communication system must be resilient in delivering data in the network. For example, the network must be able to regain stability or mitigate the effect of disruption from jammed signals and interference network or when the network security is circumvented in a timely manner. Communication system imperfections can be resolved through the following:

6.2.1 Interoperability

An enhance interoperability system is require since smart grid will incorporate different types of systems, devices and communication media within the electrical grid belonging to different vendor and utilities. Vendors and utilities may adopt different communications technologies and protocols. Interoperability is the capability of the different communications technologies and protocols to exchange and use information securely,

efficiently, and easily. Hence it is a key requirement for smart grid data communication to prevent cascading failures and blackouts. For this reason, NIST has set up a Smart Grid Interoperability Panel (SGIP) [13] to develop a frame work that includes protocols and standards to identify and address additional standard gaps and provide on-going coordination to accelerate the development of smart grid standards.

The most common interoperability solution is achieved through deploying multiple interface gateway nodes in relevant positions in a communication network that can communicate with different entities. However, possibility of deploying gateways in every part of the electrical grid is not feasible especially when the increasing variety of application that will be introduced on the grid is considered. The development of standard protocols that can be deployed in all the network components (HAN, NAN, WAN, FAN) without gateways is another approach that has also been being considered. This implies a new routing algorithm must be designed that will consider the standardisation for hardwares and addressing architectures that will be used.

6.2.2 Quality of service (QoS):

OoS is ensuring a certain level of performance in terms of bandwidth, delay, packet delivery reliability and jitter for application traffic. Traditionally all network traffics are given same level of performance (best effort), the concept of QoS gives some critical application traffic preferential treatment over other traffic. To provide high reliability and availability for the different smart grid application traffic, it is necessary to have guaranteed QoS for both single and integrated communication mechanism implemented in (FANs, HANs, NANs, BANs and WANs) to realise full smart grid potential. The channel resources, routing techniques and communications architectures across different communications network technology may not be able to guarantee a required QoS such as bandwidth latency and traffic priority for smart grid traffic. Communication mechanisms are already improving the QoS of there technologies to support critical infrastructure. i.e. the TETRA and Critical Communications Association (TCCA) are lobbying hard to ensure that broadband critical communications are available soon in order improve the capacity available for critical communication system such as the smart grid [45]. QoS parameters that may need to be guaranteed for smart grid are: traffic classification (i.e critical and non-critical), data rate, latency (one way or round trip), jitter (packet delay variation), type of traffic (periodic or random), and Packet Error Rate and Bit Error Rate (PER and BER). The parameters are mostly implemented on the node application layer, Media Access (MAC) layer and routing layers in the network.

7. USE-CASE OF SMART METERING COMMUNICATION ARCHITECTURES

In an effort to reach smart grid goals and objectives some countries in Europe have set deadlines to either roll out smart meters by 2022 or at least make efforts to try. The inconsistency in most of these countries, market structure, motivation, and even their definition of what a smart meter constitutes [46] have resulted in adopting different communication solutions for smart meter roll out. Communication solutions deployed in different countries for smart metering applications use most of the technologies discussed in section 5. However the automation of the distribution grid for a functional smart grid does not only involve smart metering data but also data from other applications that will help to remotely control and secure the grid. This section describes different communication solutions adopted by some European countries towards the roll out of smart meters and demonstrate a use case of PLC and wireless communication system used as a communication platform for automating the MV/LV distribution grid in urban and rural settlements.

7.1 A summary of smart grid communication solutions in Europe

Italy has been in the forefront of smart metering deployment in Europe where Enel, the dominant utility, has launched its ‘Telegestore’ project which has already rolled over 32 million smart meters [46]. The smart meter use NBPLC to pass on consumption data to Enel’s enterprise servers via data concentrators owned by Echelon. Even though the meters do have features to support DR and time-of-use tariff capabilities, there is dispute that they are not really smart because they are mainly for debt management through prepayment [46]. Wireless smart meters may be considered.

Germany’s national policy is to gradually phase out existing nuclear power stations and replace them with renewable generation. The goal set by the Energy Law (Energiegesetz) to generate at least 30% of total energy through renewables by 2020 has accelerated the roll out of smart meters and smart grid deployment. The Energy Law uses a decentralised system which entitles every customer to choose a ‘meter point operator’, Energiegesetz is essentially an energy service company that gets an annual fee for installing and maintaining a meter and can also sell the customer energy management services. An example of the smart meter deployed is the Automated Metering and Information Systems (AMIS). AMIS smart meters are designed to transmit data and load profiles either via telecommunication lines or via low-voltage network to a central processing station. Siemens has developed a proprietary DLC communications application based on spread spectrum signal modulation for the purpose of transmission through the low voltage network [40]. The reason for a decentralised system is an attempt to introduce competition into the market. It was however disliked by equipment vendors as they sold lower numbers of smart meters than in more centralised regimes [46].

UK has opted for a centralised architecture in which the government has designated the Data Communications Company (DCC) to control all 52 million electricity and gas meters in the country [46]. The idea is that the DCC will provide a control point from which data will be passed to energy retailers, Distribution Network Operators (DNOs), the regulator, service companies and customers as appropriate. One of the reason for the choice of a centralised system is to help keep down the cost of customers switching between retailers. The DCC is designing a private network specifically for smart meters in Britain called the SmartReach solution that will utilise Long Range Radio (LRR) connectivity on dedicated Spectrum. SmartReach is collaboration between Arqiva, British Telecom (BT), BAE System's Detica and Sensus. Arqiva will provide the telecommunications infrastructure; Detica tasked with the responsibility to provide security for the network and Sensus Flexnet is responsible for AMI. The LRR will transmit on the 400 MHz band spectrum owned by Arqiva which is a relatively low frequency signal with resilience to communicate with signals situated indoors or buried under ground. Furthermore because it is a private network, managing the smart meters will be easier, i.e a single software update or a time sensitive pricing signal can be broadcast by a utility to all meters on the network [46]. However there are concerns on whether the communication solution by the DCC is going to be able to set up a complex information system that will communicate with multiple devices in tens of millions of homes. Another concern is how the DCC solution for smart meter will interact with in home appliances.

7.2 Use case scenario for smart grid heterogeneous communication

First and foremost the USN architecture is about the network components communicating through a middleware system with the application control. The characteristics of communication technologies discussed in section 5 and the summary of smart meter deployment in Europe presented in section 7.1 has indicated that deploying a communication network across all network components in smart grid, to guarantee timely and secure delivery of application traffic, will require a hybrid combination of wired and wireless technologies.

HAN and FAN communication mostly involves sensor nodes which are well suited for WPAN technologies because of the size of traffic generated by appliances and devices. The cost of installation is also an important factor that influences the choice of WPAN technologies such as IEEE 802.15.4 as a communication network between home appliances. However communication between AMI and multiple HANs will require a hybrid combination of both local and backhaul communication technologies (presented in Table 3).

Assume a power generation source supplying two cities, urban settlement "A" and a rural settlement "B" is undergoing a transformation to smart grid and a communication technology to carry out all the smart grid applications (presented in section 2.3) is about to be deployed. Urban settlement "A" has underground feeder and transmission lines connecting the distribution substation to premises and a 33 KV MV/LV distribution substation supplies electricity to about 3000 premises in a densely populated settlement "A". If each of the meters send billing reading information of 512 bytes every 15 seconds to the data concentrator. The data rate for each meter is 273 bps, while the data rate required for the 3000 meter is 0.82 Mbps. The data rate may increase if other traffic such as DR and Voltage quality monitoring information are considered. For a similar substation presented in [21], the data rate of the total traffic mix for DA is estimated to be 12.75 Mbps. Therefore, IEEE 802.15.4 communication technology can be deployed for HAN communication with appliances and PLC can be used to send metering traffic to a data concentrator located at the substation. IEEE 802.11.15.4 can also deployed for sensor network communication with distribution grid devices and a PLC communication system network acting through a local concentrator. PLC will help monitor the cables underground and to minimise the number of communication technologies being deployed. This provides a dedicated communication path for smart grid applications such as DSM, AMI, DER, electric transportation and distributed grid management from home premises and field devices through PLC smart meters and nodes to a data concentrator. WLAN can then be used to provide resilience in form of redundancy for both PLC and IEEE 802.11.15.4.

A back haul communication technology such as WIMAX can be used to provide communication between the data concentrator and the application control centre. The selection of the communication technologies are based on the fact that they can meet the requirement of smart grid traffic based on the characteristic presented in Table 2.

Rural settlement "B" on the other hand is sparsely populated with about 600 premises, if it has similar packet size and sending interval as settlements 'A', each meter will also have a data rate of 273 bps and total traffic of 0.17 Mbps. IEEE 802.15.4 can also deployed for HAN and FAN in this settlement. Contrary to the urban settlement, the rural settlement has overhead feeder and electricity cables to the premises. The major difference is that because the rural settlement has fewer premises and overhead electrical cables, a wireless mesh network for NAN using smart meters as nodes for access network is deployed in the settlement. The smart meters will communicate to a data concentrator while the data concentrator will communicate through a backhaul technology to the application control centre. The communication platform deployed for the

distribution grid of settlement “B” is a hybrid combination of IEEE 802.15.4 and IEEE 802.11, while WIMAX is also suitable as a backhaul technology for WAN communication in rural settlement “B”. Both settlements “A” and “B” are presented in Figure 5.

Fig 5 Use-case scenario of smart grid heterogeneous communication

Figure 3 shows the middleware interaction between the data received from the heterogeneous communication infrastructure deployed in settlements “A” and “B”, and the application control centers. The figure illustrates the process of communication between smart grid application control wants and sensor or actuator nodes through the middleware to collect data or send a set of instruction. It is based on the adaptation of the USN architecture discussed in Figure 2 and, also illustrates the use case of smart grid communication deployment in urban and rural settlement. The resulting communication architecture for smart grid must be able to integrate whichever communication technology that may be deployed for smart grid based on communication characteristics and, the economic and technical factors discussed.

8. CHALLENGES OF USN ARCHITECTURE

Managing legacy components is a major barrier in the implementation of the USN architecture for smart grid. This include ensuring that all traffic speak the same language and bringing traffic components that are local and offline to the internet or online. The following challenges for the implementation of a resilient communication network for smart grid will need to be considered and addressed.

- The communication path for the data in the network must be sized to deal with peak activities in order to meet up with requirements and response time for different smart grid traffic.
- Most existing PLC and wireless hybrid system are designed for specific smart grid application [32]. For efficient routing of data in the smart grid network, the hybrid system needs to support more application traffic (delay critical, random).
- Harmonising already existing communication technologies and protocols (bespoke protocol) on the electrical power grid with new technologies and protocols.
- Secure, QoS aware middleware system is also required to support traffic types.
- In wireless technologies where self-organising functionality is employed, the self-organising functionality is limited to specific technology or subnet it implements. The self-organising functionality does not extend across the integrated network.
- Interoperability of the security system needs to be considered in other to preserve the integrity of the information throughout the system.

The vulnerabilities and challenges of smart grid communication highlighted in this paper can be minimized if the communication technology deployed meets the requirement of smart grid application classes. In selecting the communication technologies the value of higher bandwidth over lower bandwidth must be considered to guarantee implicit resilience due to bandwidth redundancy should there be any interception in the network. Resilience can also be achieved by deploying redundant communication networks to allow the ability to retain performance of the system. Also, the selection of heterogeneous combination of technologies must be able to meet QoS requirements and latency of smart grid application classes.

Deploying communication technologies with similar network specifications (i.e communication protocols) will reduce complexity. The USN middleware system can provide a QoS aware system to meet traffic QoS for smart grid application classes even at the utilities core network. In addition, increasing threat on security must bring about new security techniques because existing intrusion detection methods are not efficient in addressing threats like semantic attacks. The USN middleware provides a platform to implement other intrusion detection techniques that involve continuous network monitoring to find anomalies that may detect this type of attacks and also make decisions to counter the attacks.

Furthermore, addressing the challenges and vulnerability through selecting appropriate communication technologies and implementing a secure and QoS aware USN middleware system will enable the USN architecture provide an end to end communication model for smart grid network. The model will integrate the communication infrastructure which provides connectivity service among individual electrical devices, and a middleware system which is responsible for data management and services for the distributed infrastructure. USN architecture will not only enhance interaction of all smart grid applications, but also offer smart grid actors an opportunity to select a communications technology most favorable in carrying out smart grid functionalities.

9. CONCLUSION

The success of smart grid functionalities relies principally on ICT. The objective of the USN architecture is to provide ubiquitous coverage and interaction with sensors anywhere all over the globe. Smart grid also aims to achieve a similar objective as the USN on the electrical grid, albeit more constrained geographically and politically.

In this paper, we have proposed the USN architecture for smart grid communication. We explore smart grid communication application and network components and suggested layers of the USN architecture they will be deployed. It was highlighted that requirements of smart grid communication differs from one another and the choice of communication technology will depend on technical and economic factors and their capability to guarantee security, reliability and resilience for smart grid network. For this reason, a review of existing communication technologies was carried out with emphasis on technologies that can combine to form a heterogeneous network that will meet the requirement of different smart grid application classes. In addition, a study on smart meter communication systems being deployed in some European countries and a use case to highlight the heterogeneous nature of smart grid communication was presented. Zigbee and an IP centric PLC/WLAN technology which involves smart meters and other application access networks to a central process were recommended for the USN Sensor network and Access network layer respectively. WAN and backhaul technologies such as WIMAX was recommended to serve as the USN network infrastructure/NGN layer but other backhaul technologies such as LTE and optical fiber can also be used. Furthermore, the vulnerability and challenges of communication technologies in USN architecture were highlighted and suggested a secure and QoS aware USN middleware system to minimize the vulnerabilities and challenges.

In conclusion, the choice of communication technologies does not only depend on utility budget and policies but also the capability of the communication technology and architecture to meet security, latency, delay and QoS requirements of smart grid applications.

GLOSSARY

- AMI: Advanced Metering Infrastructure
- AMR: Automatic Meter Reading
- BAN: Building/Business Area Network
- COSEM: Companion Specification for Energy Metering)
- COSMOS: Common System for Middleware of Sensor Networks
- CPT: Critical Peak timing
- DA: Distribution Automation
- DER: Distributed Energy Resources
- DLMS: Device Language Message Specification
- DOE: Department of Energy
- DOS: Denial of Service
- DR: Demand Response
- DSM: Demand Side Management :
- DSSS: Direct Sequence Spread Spectrum
- ETRI: The Electronics and Telecommunications Research Institute
- EV: Electric Transportation
- FAN: Field Area Network
- HAN: Home Area Networks
- IAN: Industrial Area Networks
- IED: Intelligent Electronic Devices
- ITU: International Telecommunication Union
- LTE: Long Term Evolution
- NAN: Neighborhood Area Networks
- NIST: National Institute of Standards and Technology
- PHEV: Hybrid Electronic Vehicles
- PLC: Power Line Communication
- PTRs: Peak time Rebates
- RTP: Real Time Pricing
- RTU: Remote Telemetry Unit
- SCADA: Supervisory Control and Data Acquisition
- SGIP: Smart Grid Interoperability Panel
- TETRA: Terrestrial Trunk Radio

- TOU: Time-of-use
- USN: Ubiquitous Sensor Network
- WACS: Wide Area Control Systems
- WAMS: Wide Area Monitoring Systems
- WAN: Wide Area Networks
- WAPS: Wide Area Protection Systems
- WASA: Wide Area Situational awareness
- WIMAX: World Interoperability for Microwave Access
- WLAN: Wireless Local Area Network
- WPAN: Wireless Personal Area Networks

Acknowledgment

The authors would like to acknowledge the financial support of the ERDF through Centre for Global Eco-Innovation, Lancaster University, UK and, the HW Communications Ltd, UK.

References

[1] D. Balmert, K. Petrov, Regulatory Aspects of Smart Metering, ERRA Licensing and Competition Committee- Issue Paper, Dec. 2010.

[2] D. Von Dollen, Report to NIST on the Smart Grid Interoperability Standards Roadmap. EPRI. Contact No. SB1341-09-CN-0031 Deliverable 7; 2009.

[3] J. Gao, Y. Xiao, J. Liu, W. Liang, C. I. Philip Chen, A Survey of communication/networking in Smart Grids. Future generation computer systems. Elseveir 2011.

[4] National Institute of Standards and Technology (NIST), NIST framework and roadmap for Smart Grid interoperability standards, Release 1.0, January 2010. Available: http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf. 2014/11

[5] F. Baker, D. Mayer "Internet Protocols for the Smart grid" IETF, draft-baker-ietf-core-15, Apr.2011.

[6] M. Z. Huq, S. Islam, Home area network technology assessment for demand response in smart grid environment. In: Proceedings of the 20th Australasian universities power engineering conference (AUPEC); 2010. p. 16

[7] A. Mahmood. N. javaid, S. Razzaq, A review of wireless communications for smart grid. Renewable and sustainable energy reviews 41 (2015) 248-260

[8] IEEE Standards Coordinating Committee 21. IEEE Guide for Smart Grid Interoperability of Energy Technology and Information technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads. IEEE Std 2030™ – 2011.

[9] Smart Grid Reference Architecture. CEN-CENELEC-ETSI Smart grid Coordination group November 2012

[10] W. Wang, Yi Xu, M. Khanna, A survey on the communication architectures in smart grid. Computer networks journal. 2011.

[11] N. Saputro, K. Akkaya, S. Uludag, A survey of routing protocols for smart grid communications. Computer Networks, 56 (2012), pp. 2742–2771.

[12] Cisco, Internet protocol architecture for the Smart Grid. 2010. Available http://www.cisco.com/web/strategy/docs/energy/CISCO_IP_INTEROP_STDS_PPR_TO_NIST_WP.pdf.

[13] Ye. Yan, Q. Yi, S. Hamid, D. Tipper, A survey on smart grid communication infrastructures: motivations, requirements and challenges. IEEE Communications Surveys & Tutorials, First Quarter 2013, Vol.15(1), pp.5-20.

[14] The Instrumentation, Systems and Automation Society, The Instrumentation, Systems and Automation Society. Presented at the ISA 2004, 5-7 October 2004, Reliant Center Houston, Texas, www.isa.org.

[15] Department of Energy (DOE). Communications Requirement for Smart Grid Technologies October 2010

[16] K. Tarek, N. Kshirasagar, N. Amiya, A Survey of Communication protocols for Automatic Meter Reading Applications, IEEE

[17] Department OF Energy (D.O. E), Smart Grid system report. 2009. Available: http://www.oe.

[18] M. Cardei, J. Wu, M. Lu, Improving network lifetime using sensors with adjustable sensing ranges, International Journal of Sensor Networks 1 (1/2)(2006) 41–49.

[19] A. Zaballos, A. Vallejo, J. M. Selga, Heterogeneous Communication Architecture for the Smart Grid. IEEE Network; September/October 2011.

[20] C. Gomez, J. Paradells, Wireless home automation networks: a survey of architectures and technologies. IEEE Communications Magazine 48 (2010) 92–101.

[21] R. H. Khan, J. Y. Khan, A comprehensive Review of the application characteristics and traffic requirements of smart grid communications network. Computer Networks 57 (2013) 825-845.

[22] WIMAX, Forum, WIMAX Applications for Utilities, October 2008. <http: //www.wimaxforum.org>.

[23] M. Anas, N. Javaid, A. Mahmood, S. M. Raza, U. Qasim, Z. A. Khan. Minimising Electricity theft using smart Meters in AMI. In: IEEE proceedings on seventh international conference on P2P, parrallel, grid, cloud and internet computing (3PGCIC). Victoria, Canada; 2012.p.176-182

[24] Ubiquitous Sensor Network (USN) ITU-T Technology Watch Briefing Report Series, No. 4 (February 2008).

[25] M. Bauer, M. Plappert, C. Wang, and K. Dostert, Packet-oriented communication protocols for Smart Grid Services over low-speed PLC. Proc. ISPLC, Dresden, Germany, 2009, pp. 89–94.

[26] ITU-T Rec. Y.2234, "Open Service Environment Capabilities for NGN," 2008.

[27] M. Kim, J. W. Lee, Y. J. Lee, and R. Jae-Cheol, COSMOS: A Middleware of Integrated Data Processing Over Heterogeneous Sensor Networks. ETRI Journal, Volume 30, Number 5, October 2008.

[28] ETSI, Draft TR 102 935, Version: 0.1.3, Machine to Machine to Machine Applicability of M2M Architecture to Smart Grid Networks 2010.

[29] B. Sidhu, H. Singh, A. Chhabra, Emerging wireless standards - WiFi, ZigBee and WiMAX. World Academy of Science, Engineering and Technology.

[30] F. Cuomo, S. D. Luna, U. Monaco and T. Melodia, Routing in Zigbee: benefits from exploiting the IEEE 802.15.4 association tree.. IEEE ICC 2007.

[31] P.P. Parikh, G. Kanabar, T. S. Sidhu, Opportunities and challenges of wireless communication for smart grid.

[32] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debabi, C. Assi, Communication Security for Smart Grid Distribution Networks. IEEE Communications Magazine January 2013.

[33] B. Adebisi, A. Treytl, A. Haidine, A. Portnoy, R. U. Shan, D. Lund, H. Pille, B. Honary, IP-centric high rate narrowband PLC for smart grid applications. IEEE Communications Magazine,Volume: 49 , Issue: 12, pp 46-54, December 2011.

[34] INTEGRIS FP7 Project, INTelligent Electrical Grid Sensor Communications.

[35] SANS Institute Infosec reading room, Fiber Optics and its Security Vulnerabilities.

[36] M. Levesque, M. Maier, The Uber-FiWi Network: QoS Gaurantees for Triple-Play and Future Smart Grid Applications" ICTON 2012 IEEE.

[37] ETSI EN 300 392-1 Terrestrial Trunked Radio (TETRA);Voice plus Data (V+D);Part 1: General network design

[38] Science News, Magazine of the society for science and the public. http://www.sciencenews.org/view/generic/id/45868/description/Electric_grid_still_very_vulnerable_to_electromagnetic_weaponry

[39] The Economist Babbage Science and Technology. http://www.economist.com/blogs/babbage/2011/09/reliability-grid.

[40] European commission Energy, Single market for gas & electricity and Smart grid http://ec.europa.eu/energy/gas_electricity/smartgrids/taskforce_en.htm

[41] CEN-CENELEC-ETSI Smart Grid Coordination Group Smart Grid Information Security http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/xpert_group1_security.pdf 2013/12

[42] Journal of Energy Security http://www.ensec.org/index.php?option=com_content&id=198:the-security-vulnerabilities-of-smartgrid&catid=96:content&Itemid=345 2013/11

[43] C. Laughman, K. Lee, R. Cox, S. Shaw, S. Leeb, L. Norford, P. Armstrong. Power Signature Analysis, IEEE Power and Energy Magazine March/April 2003 pp 56–63

[44] T. W. Chim, S. M. Yiu, L. C. K. Hui, V. O. K. Li, Privacy-Preserving Advance Power Reservation, IEEE. Communications Magazine, 2012 Page(s): 18 - 23

[45] Tetra critical communication Association (TCCA) "Critical Communications Broadband for all users" http://www.tandcca.com/assoc/page/18100 2013/11.

[46] R. Anderson, S. Fuloria, Smart meter security: a survey, University of Cambridge Computer Laboratory United Kingdom

[47] B. Davito, H. Tai, R. Uhaner, The smart grid and the promise of demand-side management. 2010 McKinsey DSM

[48] Electric Power Research Institute (EPRI), Integrating Smart Distributed Energy Resources with Distribution Management Systems. September 2012

[49] E. Sortomme et al., Coordinated charging of plug-in hybrid electric vehicles to minimize distribution system losses, IEEE Transactions on Smart Grid 2 (1) (2011) 198-205.

[50] R. Di Pietro, S. Guarino, N.V. Verde, J. Domingo-Ferrer. Security in wireless ad-hoc networks – A survey. Computer Communications 51 (2014) 1-20.

[51] J. Martínez, J. Rodríguez-Molina , P. Castillejo, R. de Diego, Middleware Architectures for the Smart Grid: Survey and Challenges in the Foreseeable Future. Energies 2013, 6, 3593-3621.

[52] L. Zhou, J. J. P. C. Rodrigues, Service-Oriented Middleware for Smart Grid: Principle, Infrastructure, and Application. IEEE Communications Magazine January 2013.

[53] E. Ancillotti, R. Bruno, M. Conti, The role of communication systems in smart grids: Architectures, technical solutions and research challenges. Computer Communications Volume 36, Issues 17–18, November–December 2013, Pages 1665–1697

[54] D. Nordell, Communication systems for distribution automation, in: Proc. of IEEE/PES Transmission and Distribution Conference'08, 2008, pp. 1–14.

[55] IEC 61850-1, Communication networks and systems in substations – Part 1: Introduction and overview, 2003.

[56] Modbus organization, Modbus application protocol specification – V1.1b, December 2006.

[57] E. Ancillotti, R. Bruno, M. Conti, The role of the RPL Routing Protocol for Smart Grid Communications. Ultimate Technologies AND advances for future smart grid — UTASG. IEEE Communications Magazine January 2013

[58] T. Khalifa, K. Naik, A. Nayak A survey of communication protocols for automatic meter reading applications IEEE Communications Surveys & Tutorials, 13 (2) (2011), pp. 168–182.

[59] International Energy Agency (IEA), Technology Roadmap Smart Grids. OECD/IEA, 2011. https://www.iea.org/publications/freepublications/publication/smartgrids_roadmap.pdf

[60] P. Zhang, F. Li, N. Bhatt Next-generation monitoring, analysis, and control for the future smart control center IEEE Transactions on Smart Grid, 1 (2) (2010), pp. 186–192.

[61] V. Terzija, G. Valverde, D. Cai, P. Regulski, V. Madani, J. Fitch, S. Skok, M. Begovic, A. Phadke Wide-area monitoring, protection, and control of future electric power networks Proceedings of the IEEE, 99 (1) (2011), pp. 80–93 View Record in Scopus | Full Text via CrossRef | Citing articles (121).

[62] A. Johnson, J. Wen, J. Wang, E. Liu, Y. Hu, Integrated system architecture and technology roadmap toward wampac, in: Proc. of IEEE PES ISGT'11, 2011.

[63] Y.-J. Kim, M. Thottan, V. Kolesnikov, W. Lee A secure decentralized data-centric information infrastructure for smart grid IEEE Communications Magazine, 48 (11) (2010), pp. 58–65.

[64] IEEE 1646, Ieee standard communication delivery time performance requirements for electric power substation automation, 2005.

[65] E. Ancillotti, R. Bruno, M. Conti Design and performance evaluation of throughput-aware rate adaptation protocols for IEEE 802.11 wireless networks Performance Evaluation, 66 (12) (2009), pp. 811–825.

[66] S.-L. Tsao, C.-H. Huang A survey of energy efficient MAC protocols for IEEE 802. 11 WLAN Computer Communications, 34 (1) (2011), pp. 54–67

[67] IEEE, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements, IEEE Std 802.11e-2005, 2005.

[68] N. Saputro, K. Akkaya PARP-S: A secure piggybacking-based ARP for IEEE 802.11s-based Smart Grid AMI networks. Computer Communications 58 (2015) 16–28.

[69] C-C. Chang, Y-J. Su, U. Kurokawa, B. Choi, Interference Rejection Using Filter-Based Sensor Array in VLC Systems", IEEE Sensors Journal, Vol. 12, No. 5, pp: 1025-1032, 2012.

[70] Pure VLC, "Visible Light Communication: An introductory guide", [online] www.purevlc.net, 2012.

[71] M. V. Bhalerao, S. S. Sonavane, V. Kumar. A Survey of Wireless Communication using Visible Light. International Journal of Advances in Engineering & Technology, Jan. 2013. ISSN: 2231-1963. Vol. 5, Issue 2, pp. 188-197.

[72] IEEE 802.15.7, "VLC PHY/MAC Proposal-Samsung/ETRI", 2009. https://mentor.ieee.org/802.15/dcn/09/15-09-0733-00-0007-vlc-phy-mac-proposal-samsung-etri.pdf .

[73] R. Hou1, Y. Chen, J. Wu, H. Zhang. A Brief Survey of Optical Wireless Communication. Proceedings of the 13th Australasian Symposium on Parallel and Distributed Computing (AusPDC 2015), Sydney, Australia, 27 - 30 January 2015

[74] O. Kosut, L. Jia, R. Thomas, L. Tong Malicious data attacks on the smart grid IEEE Transactions on Smart Grid, 2 (4) (2011), pp. 645–658

[75] H. Khurana, M. Hadley, N. Lu, D. Frincke Smart-grid security issues IEEE Security Privacy, 8 (1) (2010), pp. 81–85

[76] P.-Y. Chen, S.-M. Cheng, K.-C. Chen Smart attacks in smart grid communication networks IEEE Communications Magazine, 50 (8) (2012), pp. 24–29

[77] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, H. Zhu Securing smart grid: cyber attacks, countermeasures, and challenges IEEE Communications Magazine, 50 (8) (2012), pp. 38–45

Figure

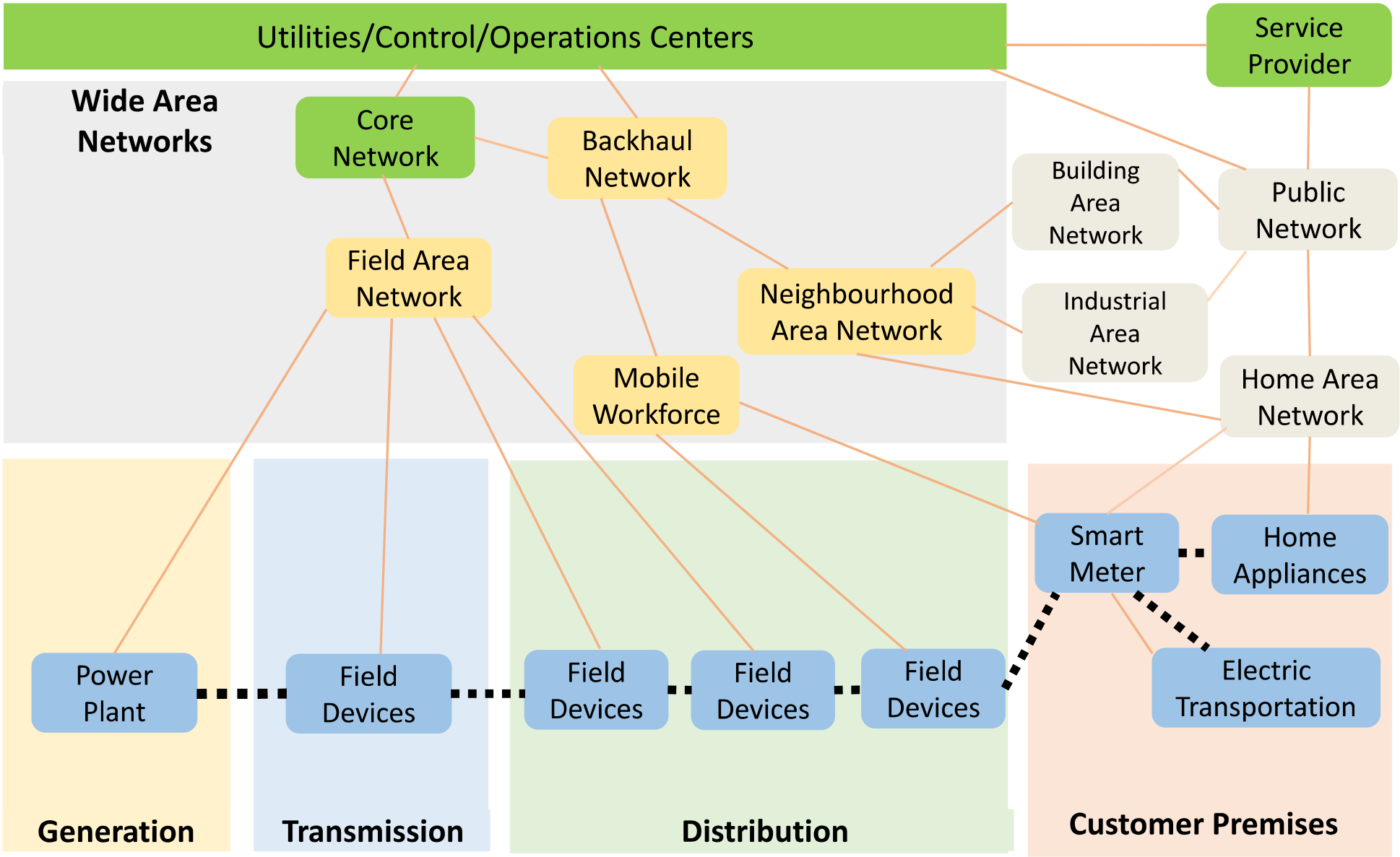

Fig. 2. Communication network components for end to end communication in Smart Grid

Figure

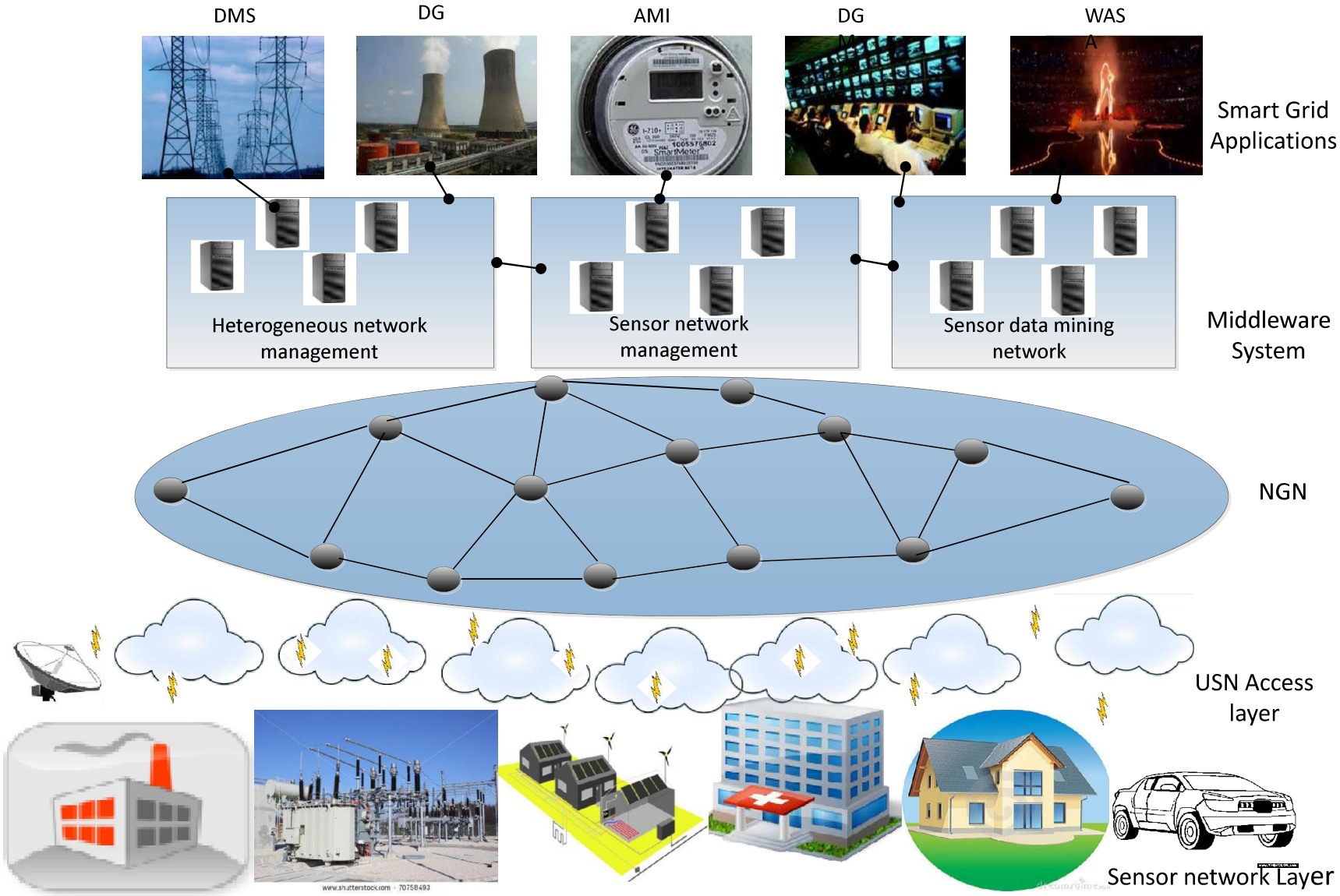

Fig. 3. Schematic Layers of the USN Sensor network applied to Smart Grid

Figure

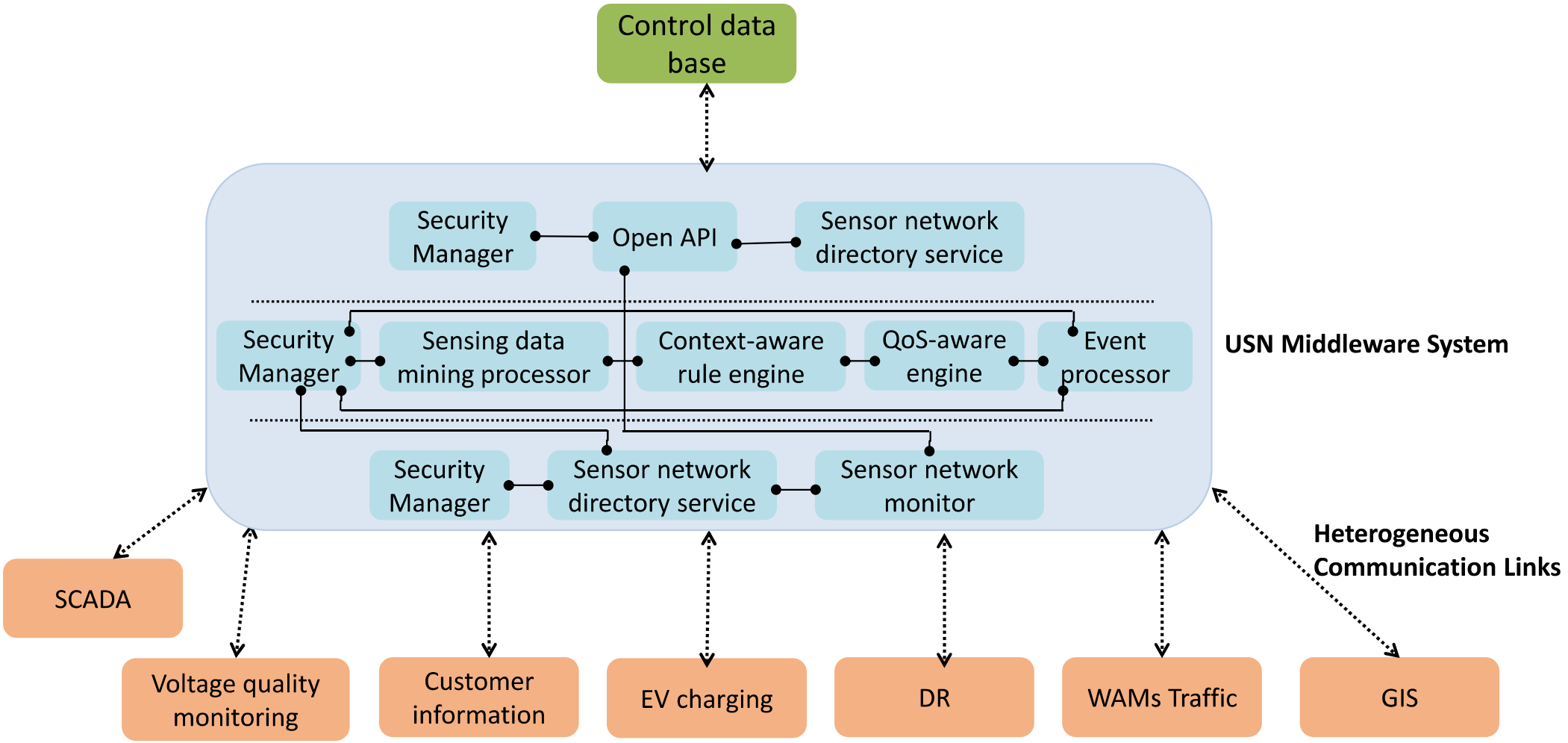

Fig. 4. USN middleware communication bus

Figure

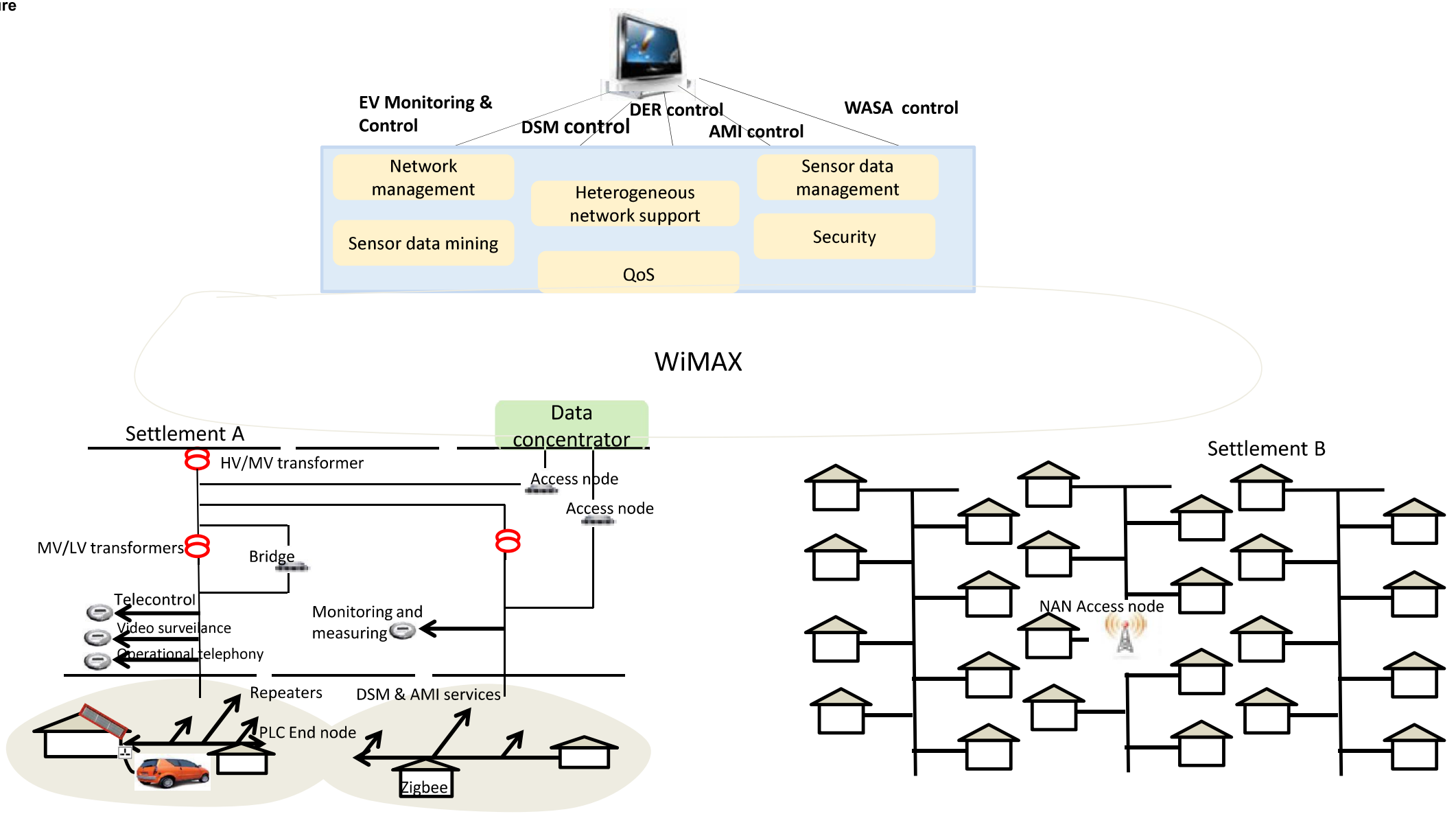

Fig. 5 Use-case of Smart Grid heterogeneous communication

Figure

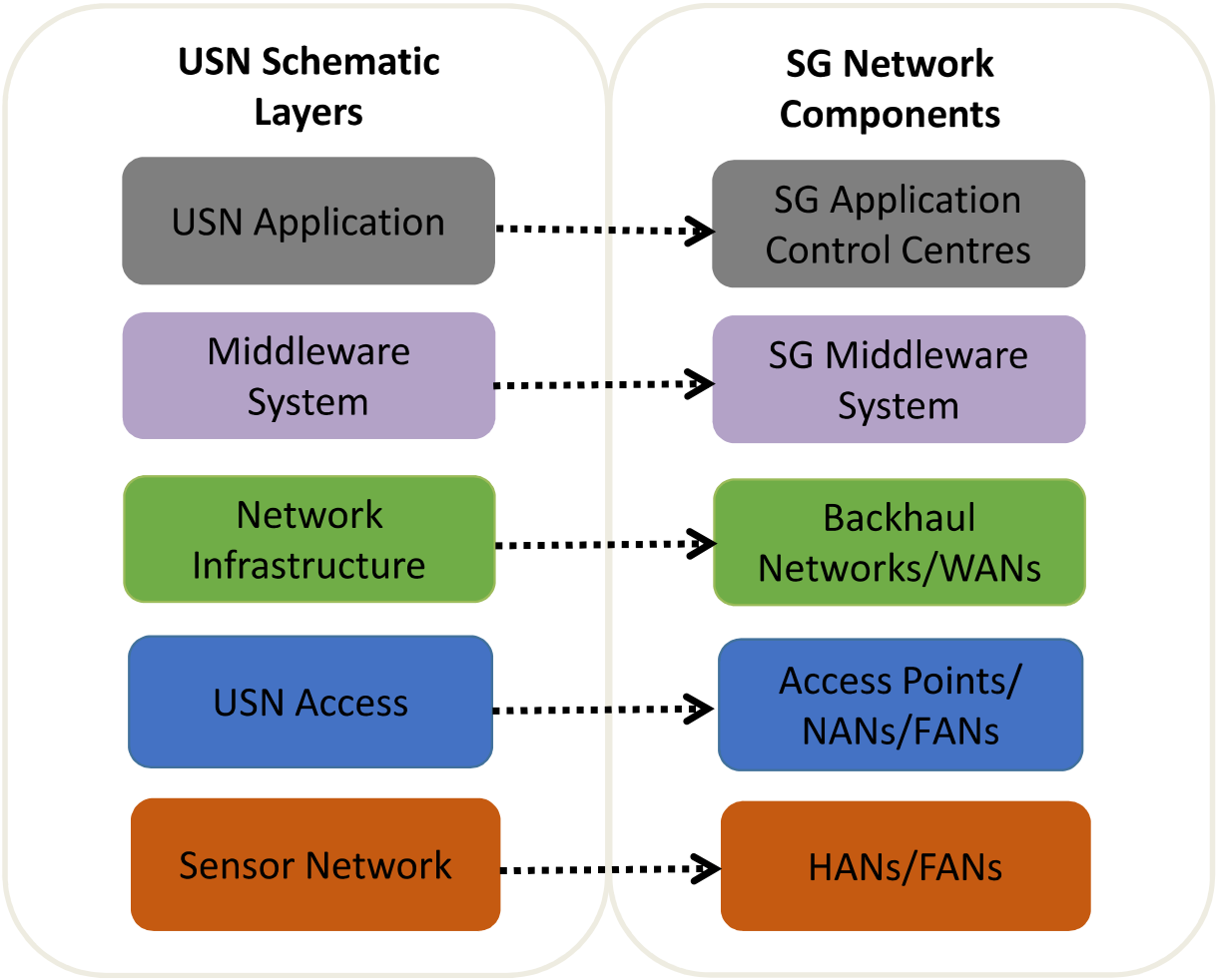

Fig. 1. USN layers with corresponding Smart Grid Components

Table

Table 1 Smart grid Applications network bandwidth and latency requirement [4]

Smart Grid Applications	Network Requirement (Throughput)	Traffic Type	Latency	Criticality
AMI (Billing, Metering,	10 - 100 kbps/node, 500 kbps backhaul	Periodic	2 - 15 s	Low
DSM (DR, Dynamic Pricing and Load Control)	14 - 100 kbps per node per device	Periodic/Random	500 ms to several min	Medium,/High (Depends on demand)
WASA (WAMS, WAPS, WACS)	600 - 1500 kbps	Random	20 - 200 ms	High
EV Monitoring	9.6 – 56 kbps, 100 kbps is a good target	Random	2s – 5 min	High
DGM	9.6 – 100 kbps	Periodic/Random	0.1 – 2 s	High/Medium
Video surveillance	15 – 128 kbps, camera	Random	1 s	Medium
Operational telephony	8 kbps, call	Random	1 s	High
SCADA	1.8 – 9.6 9.6 kbps	Random	< 0.5	High
DER and storage	9.6 - 56 kbps, depending on the number of energy sources	Periodic/ Random	0.02 – 15 s	High

Table

Table 2 Technical Requirement for Smart grid application classes

Application class	Internal substation	Maximum response time (External substation)	Data burst size
Meter/billing	-	Hours	Hundreds of bytes
Protection	4 ms (1/4 cycle of electrical wave)	1 - 10 ms	Tens of bytes
Reporting/software update	-	Days	Kb to mb
Control	16	100 ms	Tens of bytes
Monitoring	16 ms	1s	Tens to hundreds of bytes
Operation and maintenance information	1 s	10 s	-

Table

Table 3 Characteristics of smart grid communication technologies

Communication technology standards	Local or backhaul System	Maximum data rate	Approximate coverage	Potential smart grid application
IEEE-802.11 (WLAN)	Local	11 - 600 Mbps	Up to 300 m	HEMS, DSM, DA and protection
IEEE-802.15.4 (Zigbee)	Local	20 -250 kbps (2.4 GHz) 40 kbps (915 MHz)	10 -100 m	HEMS, DER, AMI
IEEE-802.16 (WIMAX)	Backhaul	Up to 1 Gbps for fixed users	30 -100 km	AMI, WASA, AMI,
3GPP CELLULAR (3G, 4G: LTE, LTE advanced)	Backhaul	500 Mbps up link 1Gbps down link	10-100 km	WASA, Electricity transport, AMI
Optical Fibers	Backhaul	155-2448 Mbps up, 1.244-2.448 Gbps down	Up to 60 km	WASA, Distributed Grid Management
PLC (NB-PLC & BPLC)	Local and Backhaul	1-500 kbps (NB-PLC) 1-10 Mbps	NB-PLC: over 150 km BB-PLC: ~ 15 km	AMI, Electric transportation monitoring, DSM, Distributed Grid Management
TETRA	Local and Backhaul	170 kbps	10 -50 km	AMI, DSM
Digital Subscriber Line (DSL)	Backhaul	256 kbps – 200 Mbps down	Up to 7 km	AMI, DSM
Visible Light Communication (VLC)	Local	10 kbps-500 Mbps	Over 5 meters	HEMS, Distribution grid management