A Survey of Routing Protocols for Smart Grid Communications

Nico Saputro*, Kemal Akkaya

Department of Computer Science, Southern Illinois University, Carbondale, IL 62901 USA

Suleyman Uludag

Department of Computer Science, Eng. & Phy., University of Michigan Flint, Flint, MI 48502 USA

Abstract

With the recent initiatives to upgrade the existing power grid to the Smart Grid (SG), there has been a significant interest in the design and development of an efficient communications infrastructure for connecting different components of the SG. In addition to the currently used underlying networks and protocols, new wired/wireless approaches are being planned for deployment for different components/applications of the SG. Based on the data requirements of the applications, new challenges have arisen at the network layer of the protocol stack with respect to routing and data forwarding. In this paper, we focus on the routing issues in the SG communications infrastructure which consists of different network components, such as Home Area Networks (HANs), Neighborhood Area Networks (NANs) and Wide Area Networks (WANs). We provide a comprehensive survey of the existing routing research and analyze the advantages and disadvantages of the proposed protocols with respect different applications areas. We also identify the future research issues that are yet to be addressed with respect to the applications and network components. This survey is the first to identify routing design issues for the SG and categorize the proposed routing protocols from the SG applications perspective. We believe that this work will be valuable for the utilities and other energy companies whose target is to develop and deploy a specific SG application that may span different network components. In addition, this work will provide valuable insights for the newcomers who would like to pursue routing related research in the SG domain.

Keywords: Smart Grid, Smart Grid Communications Network, Routing, HANs, NANs, WANs

1. Introduction

The modernization of the electricity grid that can accommodate future demand growth is underway [1, 2]. In addition to the use of the more advanced electrical power components, the modernization of the power grid involves an extensive use of the information technology which will lead to the Smart Grid (SG). Two driving forces to move toward SG are: (1) The aging, inadequate, and outdated current electricity grid which needs to be improved to meet the future demand challenges, (2) The benefits of the SG in consequence of the improvements in six key value areas: reliability, economics, efficiency, environmental, security, and safety [2]. As a result of these improvements, the following benefits are expected: 1) a reduction of the rate and length of outages; 2) a reduction in the number of disruptions due to power quality issues; 3) lower electricity bills; 4) lower operation and maintenance costs; 5) better asset utilization; 6) lower CO_2 emissions due to the deployment of electric vehicles; 7) an increase in physical security as well as cyber-security in the whole power grid systems; and 8) an increase in the safety from electricity hazards.

An important part of the motivation for the SG is to be able to provide built-in two-way flow of information among different components, a feature lacking in the current power grid. Current systems that are based on Supervisory Control and Data Acquisition (SCADA) are mostly used in control centers for monitoring the power grid components and provide communications among these centers as well as the substations. The proposed communications infrastructure for SG will have many interconnected systems with various ownership and management to provide end-to-end services among stake holders as well as among intelligent devices. Through this communications infrastructure, several new applications can be realized. For instance, Advanced Metering Infrastructure (AMI) allows utilities to collect, measure, and analyze energy consumption data; Demand Response (DR) uses the AMI infrastructure to adjust power demands and the prices. Similarly, Wide Area Situational Awareness (WASA) can improve the monitoring of the power system across large geographic areas. We refer to this communications infrastructure as *SG Communications Network* hereafter.

While there has been an increasing interest in identifying the components of the SG and possible applications [3][4], specific research challenges at each protocol layer have not been elaborated yet. In particular, several key issues need to be addressed in order to support network interconnectivity across the

*Corresponding author

Email addresses: nsaputro@cs.siu.edu (Nico Saputro), kemal@cs.siu.edu (Kemal Akkaya), uludag@umich.edu (Suleyman Uludag)

SG communications networks [1] that consists of HANs, NANs and WANs. For instance, security is required since SG will consist of multiple-interconnected networks with diverse underlying communications technologies, ownerships and management. While providing availability and reliability, certain privacy information, such as power usage data from each household, needs to be protected. Furthermore, the communications infrastructure will require network management functionality, network activities, and network devices, including status monitoring, fault detection, isolation, and recovery. Finally, the ability to uniquely identify elements in the network and routing capabilities to all network end points for a wide range of applications with different requirements will need to be addressed.

In this paper, unlike the other existing SG communications surveys, we focus on the routing component of the SG communications. Our goal is fourfold: 1) to facilitate a better understanding of the components of the SG (i.e., HANs, NANs and WANs), how they interact and where they are situated in the big picture of the communications network of the SG, 2) to elaborate on the routing design issues in the communications network with respect to various SG applications, 3) to survey and categorize the existing routing approaches for HANs, NANs and WANs, and 4) to list possible future research issues and challenges. We believe that laying out the infrastructure for the SG and discussing the research challenges as part of the communications network will be beneficial for the newcomers to this research area. In addition, application designers/companies/utilities looking to implement any SG application can use this survey as a starting point to determine their applications' routing needs.

The organization of the paper is as follows: Section 2 starts with an overview of SG. Section 3 presents the existing surveys on different aspects of the SG. Section 4 presents the communications network of the SG along with the applications it can support. Routing design issues in the SG communications network are also introduced. Section 5 presents the classification of the routing protocols for the SG based on various criteria. Sections 6, 7 and 8 summarize/classify the existing routing approaches in HANs, NANs and WANs respectively. In Section 9, future research issues pertaining to routing on HANs, NANs and WANs are enumerated. Finally, Section 10 concludes the paper.

2. Smart Grid Background

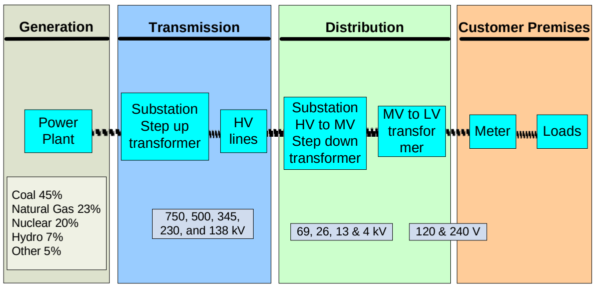

Figure 1: Current Power Grid Components and flow of electricity.

Today, the electricity is generated and distributed in a hierarchical power grid that has three distinct subsystems: Generation, Transmission, and Distribution. The power plants generate electricity and then step-up transformers at the transmission substations convert it into high voltage electricity for long-distance transmission on the grid. At the distribution substations, this high voltage electricity is converted into medium voltage and transported over the distribution grid to the end users. Before entering the end user premises, the medium voltage is converted into low voltage. This process is shown in Fig. 1. This basic flow of electric power in power grid has remained unchanged for a little over a century. However, each electric power subsystem has evolved over time with a different pace. Hence, the level of automation varies considerably at different components of the SG.

The electric grid has transformed from a set of isolated of power plants into interconnected grids. The current electric transmission grids are interconnected into regional or national electric grids to provide multiple redundant alternate routes for electric flow in case of unbalanced supply and demand or failures, such as generation plants or transmission equipment failures.

Dispatching electricity is centrally managed through a control center which has the responsibility for controlling several regions from a central location. The control center uses computer-based monitoring and control system, called Supervisory Control and Data Acquisition (SCADA) system. SCADA system contains various electronic monitoring or control devices as well as automation equipment to measure, monitor, and control electric power grid components. SCADA systems came into life after the major blackout in 1965 and later evolved into Energy Management System (EMS) at the Control Centers. Remote Terminal Units (RTU) at transmission and distribution substations are deployed to collect real-time data with relatively low time granularity (2-10 samples / sec). EMS uses Automatic Generation Control (AGC) for state estimation, contingency analysis, optimal power flow, etc.

Thus, generation and transmission portions of the current power grid are fairly "smart" but still there is not much automation at the control centers and thus human intervention is required. After the 1990s, limited real-time monitoring capabilities to distribution and customer premises have been introduced. Distributed automation, Advanced Meter Reading (AMR) and Infrastructure (AMI) applications are some examples of these efforts. However, these were locally deployed only as pilot projects and thus their usage is not widespread on the power grid. As a result, this current advancement of the electric power grid is considered inadequate and too localized to address many critical issues.

The operation of the current power grid is inefficient. Due to the inefficient power storage, the supply is required to keep up with the demand, resulting in a forced just-in-time paradigm. However, the demand fluctuations strain the aging and outdated infrastructure of the power grid during the peak demand hours and hence pose reliability, availability, and power quality issues. The current power generation that relies on the non-renewable resources also has environmental and resource scarcity issues. Besides vehicles, traditional electricity plants that rely on fossil fuels also emit gases and other pollutants when burning fuel to generate electricity. Finally, utility companies realize that they must shift their dependence from the knowledge of their aging workforce to systems-based knowledge through information management and automation.

All these contribute to the motivation of developing an intelligent power grid to improve the power grid in the following areas: reliability, economics, efficiency, environmental, security, and safety [2]. More detailed information regarding SG characteristics and proposed models can be found in [1, 2, 3, 4, 5]. In what follows, our focus will be on the routing in the SG.

3. Related Work

There has been an increasing research activity and survey papers on SG communications recently. Several survey and positional papers on SG can be found in the literature [6] [7] [8] [4] [3].

The work in [6] focuses solely on HANs and discusses the whole protocol stack from physical to application layer as well as making a comparison of some wireless proprietary technologies/protocols. The work in [7] reviews and classifies various works of SG found in the literature. More specifically, the authors review the works in the aspect of communication/networking architecture and technologies, Quality of Service (QoS), optimization, and control and management of SG. A mathematical model of power delivery system and bandwidth are also reviewed in this work. The work in [8] provides the current status of SG communications, specifically research challenges, standardization, and industry perspectives. The authors focus on the challenges that must be addressed for fully robust, secure, and functional SG networks together with their view for applying some existing networking technologies to solve energy management problems. The work in [4] provides a survey on three major systems of the SG, namely the smart infrastructure system, the smart management system, and the smart protection system. For each major system, the authors provide potential research directions. Each major system is divided further into subsystems and the classification of the related work pertaining to each subsystem is also provided. Its focus is more on the industrial perspective and standardization in terms of the used technologies for all aspects of the SG. Finally, [3] in a comprehensive survey summarizes the current state of research efforts on the communications architectures for the SG including the network architecture, technologies, functions, requirements, and research challenges. This is more like an introduction to the SG notation, devices, and applications and with a primary focus on reliable and secure communications.

As summarized above, none of these survey-like papers focus on the theoretical and practical challenges of routing functionality and protocols by considering HANs, NANs and WANs. While some of them can be complementary to our study by providing background on the notation and underlying communications architectures, our survey is distinct and unique in the sense that it is specific to network layer and differentiates the approaches based on the underlying network.

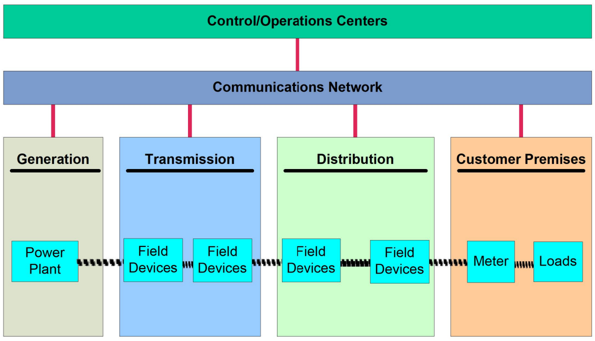

Figure 2: Envisioned SG Communications Network along with the Grid Components.

4. Routing on Smart Grid

Routing on the SG is to be performed on its communications network among various parties such as customer premises, utilities, control centers, substations and mobile workforce. In order to understand the routing problem and challenges, we first need to understand the communications network along with the possible applications that will be utilizing different portions of the communications network. In this section, we describe the underlying communications network in details and then identify the design issues for routing in this communications network.

4.1. Smart Grid Communications Network

We refer to the communications infrastructure of the current power grid as the *Communications Network*. The electric power grid has employed a communications network to support its operations. This communications network uses a variety of communications technologies, ranging from wired, such as copper cables, optical fiber, power line carrier, to wireless networks. The crucial component for communications is between control centers and individual substations.

However, the existing communications network is inadequate, inflexible, and expensive. The inadequacy stems from several factors: First, the existing communications network only covers generation and transmission segments. It does not cover the distribution side where the major changes are expected to occur. Second, the capacity and speed of the installed communications network are inadequate to accommodate the future capacity growth and speed requirements of SG applications. Third, performing modifications to the existing network is difficult and cumbersome. The addition of new participants may require additional communications network installations or modifying the existing applications to accommodate these participants. This is not only expensive in terms of design, hardware, and programming costs, but also it may increase latency for data delivery [9]. Therefore, a new extended communications network is needed to support a wide range of applications as well as to meet the future demand.

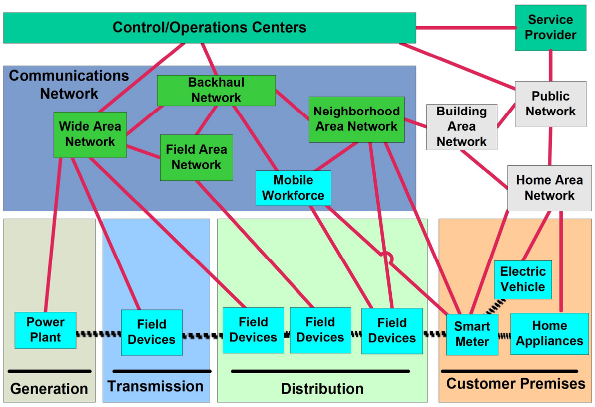

Figure 3: Smart Grid multi-tier communications network.

As a result, an integrated communications network is added to the electric power grid to control and enable a reliable and safe operation of bi-directional electric power grid. This integrated communications network covers the whole electric power grid, from generation to distribution as shown in Fig. 2.

SG will not use just one type of communications network. There is not a single solution or a representative network for the SG as each utility will have different topographies, regulatory regimes, and legacy communications systems. SG is expected to be a multi-tier network supported by a hybrid mesh of different communications technologies to provide efficient and reliable access to grid components in diverse environments [10] as illustrated in Fig. 3. Mainly, there will be three components of this multi-tier network which can be deploying a variety of communications networks, including wired and wireless, licensed and unlicensed, private and commercial, fixed and mobile, narrow-band and broadband.

4.1.1. Home Area Network (HAN)

HAN is located in the customer domain and provides access to in-home appliances. Every home device will send their power readings over this network to the home meter or gateway outside the house for AMI application. HAN also enables home automation networks for monitoring and control applications for user comfort, efficient home management, and DR application.

Home automation networks consist of various sensors and actuators to perform a variety of applications [6], such as light control, remote control, smart energy, remote care, and security and safety. For instance, light control application enables lights to be controlled from any switch or activated by remote control or turned on/off automatically based on sensors information or DR request from the utility company. Building/Business Area Network (BAN) is used to refer to similar networks when implemented in businesses, and Industrial Area Network (IAN) when applied to an industrial setting.

The wireless communications in HAN/BAN/IAN is preferred over wired since it allows flexible addition and removal of devices and reduces installation costs. Furthermore, the sheer volume of home automation networks with high node density may make wired approaches impractical. However, the wireless solution is operated in a multipath environment due to the presence of reflective surfaces at home and subject to interference since there are a variety wireless device deployments at home, from cordless phones to microwave ovens, to WLAN, etc.

The data generated from each in-home appliance and the communications requirements of each appliance in HAN may differ. In [11], appliances are classified into four groups based on their communications needs.

Small load appliances form the first group, such as light bulbs, phone charger, and laptop computer. Managing these appliances will not have a significant reduction on the total load profile. Control centers only need simple information, such as when they are connected or disconnected. Hence minimal communications from this group to the control center is adequate. The second group is *uncontrollable large load appliances*, such as a stove. A stove is used whenever needed and hence it cannot be controlled. This group also requires minimal communications to the control center. The third group is *controllable large load appliances*, such as air conditioners, washers, and dryers. Control centers require detailed information from this group, such as the expected load, duration of usage, and duration of availability from the appliance. Unlike the previous categories, these appliances require an acknowledgment from the control center to begin the operation. Hence, this group requires extensive communications between the appliances and control center. The last group is *Electric Vehicles (EVs)*. EVs require very large loads and hence managing their charging time in advance is very important. This group also requires extensive communications between EVs and control center.

Typical coverage for this type of network is expected to be in the order of thousands of square feet. The data rate is expected to be low, typically around 1-10 Kbps. Possible protocols for HAN include open wireless standards, such as IEEE 802.15.4 and IEEE 802.11, and proprietary wireless stacks, such as Z-Wave, or Powerline Communications (PLC) such as HomePlug.

4.1.2. Neighborhood Area Network (NAN)

NAN connects smart meters to local access points for AMI applications. This can be a network of smart meters creating a mesh, as well as part of a mesh network, which consists of smart meters and some gateways to relay data. The version of this network which is deployed to collect data from power lines, mobile workforce, towers, etc. for power grid monitoring is referred to as Field Area Network (FAN). In this paper, we will use NANs to refer to both types of networks. Coverage of a NAN would be around 1-10 square miles. The data rate would be higher than that of HANs, approximately around 10-1000 Kbps. The place of NANs in the SG Communications network can be seen in Fig. 3.

Possible protocols/standards for NANs would be based on both wireless and wired technologies. On the wireless side, IEEE 802.11s, RF Mesh [12], Worldwide Interoperability for Microwave Access (WiMAX) and cellular standards, such as 3G, 4G, and LTE, are some of the stronger candidates. On the wired side, Ethernet, Powerline Communications (PLC) or

Data over Cable Service Interface Specification (DOCSIS) are possible options to use.

As can be seen from the previous discussions, there are several options to implement these networks and often there is no SG-specific standard in the definition of these networks. In some cases, these networks can also serve as part of a larger distribution network or there may be a single network covering both NAN and FAN at the same time. Depending on the underlying technology, the network architecture in NAN can be using multiple hops or a single hop approach. For instance, use of WiMAX will imply that the data from smart meters can be relayed directly to the operations control center or to a Backhaul network. In this case, one can assume that either each smart meter will have a WiMAX radio or they will send their readings to a gateway (via IEEE 802.11 or 802.15.4 standards) which has a WiMAX radio. However, in case of an RF Mesh solution, the data may travel multiple gateways before reaching the Backhaul network.

4.1.3. Wide Area Network (WAN)

WAN provides communications link between the grid and core utility systems. WAN comprises two types of networks: Core and Backhaul. While the Core Network is used to connect metro network of the utility and substations, the Backhaul Network is used to connect NAN to the core network. The coverage of this network would be in the order of thousands of square miles while the data rates would be between 10-100 Mbps.

Underlying technologies may significantly vary based on the implementation. As far as the wireless technologies are concerned, similar protocols (e.g., WiMAX, 3GPP, RF Mesh) mentioned in NAN could be used for wide area access in the Backhaul Network. In fact, this Backhaul Network can be considered as part of the NANs. For wired options, DSL or Passive Optical Networks (PONs) can be used. Metro Ethernet for the Core Network can be implemented with some wired technologies such as Internet Protocol/Multi Protocol Label switching (IP/MPLS) and fiber (SONET).

4.2. SG Applications on the Communications Network

There are a lot of applications such as Demand Response or Grid Monitoring which can utilize either HAN, NAN or WAN or a combination of these as seen in Fig. 4. In its report in [13], the US Department of Energy (DOE) determines that most, if not all, applications in SG can be classified into six functional categories as explained in the following subsections. These applications are expected to have high security, high reliability, and various QoS requirements such as bandwidth and latency as shown in Table 1. While some of these requirements can be addressed at the routing layer of HANs/NANs/WANs alone, it is quite likely that cross-layer approaches may improve the performance. In any case, design of routing protocols is crucial in meeting most of the requirements of the applications.

4.2.1. Advanced Metering Infrastructure

Advanced Metering Infrastructure (AMI) is designed to collect, measure, and analyze energy consumption data of customers through smart meters in order to pave the way for dynamic and automatic electricity pricing. Given that AMI data travels from the appliances to the utility data center, it is one of the unique applications of the SG whose data spans all the sections of the SG, such as HANs, NANs and WANs. Typically, appliances report to a smart meter, smart meters report to a data aggregation point such as a gateway in distribution substation and the aggregation point relays this data to the utility center through the core backbone.

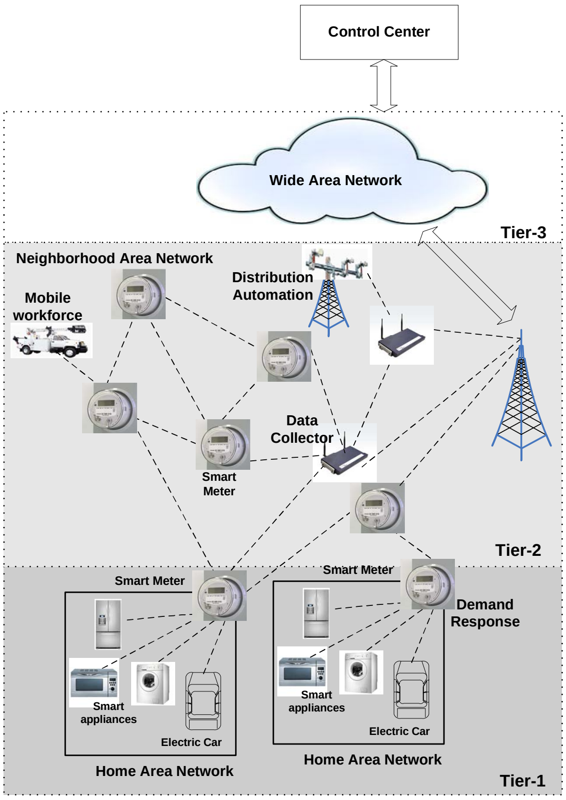

Figure 4: Multi-tier Smart Grid Communications Network with HANs, NANs and WANs.

AMI data is the most fundamental and crucial part of the SG traversing every portion of the SG communications network in two-ways. Thus, AMI is one of the most challenging applications in terms of establishing the routes from appliances to the utility.

4.2.2. Demand Response

Demand Response (DR) is introduced in response to the seasonal variations of electricity demand in an effort to smoothen the traffic. DR programs that are bundled with price options give customers incentives to reduce their electric consumption in response to system overloads. In this way, both utility and customer get the benefits. The utility company can control the peak power conditions on the grid by shifting consumption time and hence reducing the probability of system failure and lowering the cost. The customers, on the other hand, may get price incentives for their power consumption. DR uses the AMI infrastructure to implement its functionalities, such as to per-

Table 1: SG Application and Network Requirements [13].

	Network Requirements	
Application	*Bandwidth*	*Latency*
AMI	10-100 kbps/ node, 500 kbps backhaul	2-15 sec
Demand Response	14-100 kbps per node/device	500 ms - several minutes
Wide Area Situation Awareness	600-1500 kbps	20 - 200 ms
Distributed Energy Resources and Storage	9.6 - 56 kbps	20 ms - 15 s
Electric Transportation	9.6 - 56 kbps, 100 kbps is a good target	2s - 5 min
Distribution Grid Management	9.6 - 100 kbps	100 ms - 2 sec

suade customers to be more energy conscious. Thereby, utility companies will be able to control customers' non-essential load by turning on/off/up/down appliances. Obviously, this will be based on a prior agreement between the customer and utility company. Similar to AMI, DR also utilizes HAN, NAN and WAN in both ways and thus adds more traffic to the SG communications.

4.2.3. Wide Area Situational Awareness

Wide Area Situational Awareness (WASA) uses various technologies that support near real-time monitoring of the power grid across large geographic areas. Very high frequency of massive amount of information in the order of milliseconds about the current state of the power grid are collected from the transmission networks and electric substations. The gathered information are used to optimize the performance of the grid components as well as to provide a more timely prevention when problems are detected to avoid power grid disruption. Based on the purpose of the information usage, WASA can be divided further into Wide Area Monitoring Systems (WAMS), Wide Area Control Systems (WACS), and Wide Area Protection Systems (WAPS). WACS and WAPS require high bandwidth to meet the timing requirements. The data typically travels through the NAN and WAN.

4.2.4. Distributed Energy Resources (DERs) and Storage

In the SG, the electricity supplier will not only comprise of Bulk Generation, but also miscellaneous Distributed Energy Resources (DERs) which reside at the Transmission, Distribution, or even at the end-user systems. These DERs will be integrated into power systems and complement the centralized Bulk Generation. In addition, the presence of DERs is expected to enable many new features. The need for energy storage arises in order to store the surplus of electricity at a given time for distribution thereafter or to compensate the energy generation fluctuations from renewable sources such as wind and solar. In turn, both energy storage and DERs at end-users systems enable active participation of the end-users in making power supply-demand decisions. Excessive electricity supply can be used as backup sources at the time of power disturbances or to support the Demand Response changes, or sell them to the electricity market. To coordinate such DER activities, an effective communications infrastructure is needed at the NAN and, quite possibly, HAN levels.

4.2.5. Electric Transportation

Electric transportation, via either fully Plug-in Electric Vehicles (PEV) or Plug-in Hybrid Electric Vehicles (PHEV), are expected to enhance or even replace the traditional transportation that uses fossil fuels. Instead of using fossil fuels, an Electric Vehicle (EV) uses one or more electric motors which are powered by a rechargeable electric storage. To recharge the electric storage of an EV, the electric storage is connected to the SG and the electric power flows from the SG to the electric storage of the EV. This is known as Grid-to-Vehicle (G2V) flow and may occur at home or in public charging facilities. It is envisaged that most charging processes take place at the public charging facilities rather than at homes and almost simultaneously (e.g., in the morning after the owners arrive at their offices) [14]. Hence, the aggregate load of G2V at a given time may create a new peak power demand in addition to the existing peak power demand. On the other hand, EVs also introduce a new functionality as a power storage that can be used to reduce the peak demand when needed. This is known as Vehicle-to-Grid (V2G) flow. In V2G, an EV connects to the SG and feeds the electric power back from its power storage to the SG. Hence two-way flow of electric power occurs between EVs and the SG. In order to make such an exchange possible, intensive data communications between EVs and the SG is required (e.g., for charging the user and for assessing the peak demands). Since the communications occur when EVs are parked and connected to the SG, this connection point can be HAN or NAN.

4.2.6. Distributed Grid Management

Distribution Grid Management consists of various SG automation technologies for real-time information and remotely control devices in the grid. Some examples are Distribution automation, substation automation, fleet management by automatic vehicle location (AVL), and video surveillance. Distribution Automation (DA) operates on the distribution substation and utilizes an automated decision-making to provide more effective fault detection, isolation, and restoration. Substation automation is achieved through SCADA to control and monitor the grid. AVL is used for tracking and directing the mobile workforce to the location that needs to be repaired. Video surveillance is used to monitor the critical SG assets. The collected data in these applications will be directly connected to the WAN through a LAN or Fiber optics communications.

4.3. Routing Design Issues for Smart Grid

In this subsection, we provide a summary of major issues that may affect the design of the routing protocols for SG based on the applications discussed above. For each issue, we discuss how it relates to routing in the context of SG applications.

4.3.1. Node Heterogeneity

SG is conceived as a blend of communications technologies interconnecting various devices of different types, from common networking technologies such as computers, routers, switches to smart meters, home appliances, sensors, synchrophasors, and EVs. The data generated from these nodes will have different requirements in terms of routing and thus this may lead to different type of service (ToS) requirements for each type of data. Furthermore, each of these devices will have different hardware restrictions in terms of CPU, memory, battery or storage and thus routing protocol should consider these resource requirements as well. In addition to common resource variations such as in computation capability, storage capacity, and energy supply; a node in SG could be equipped with multiple interfaces instead of a single interface in order to exploit heterogeneous communications technology environments (i.e., multiple radios, channels). Such additional interface will affect the design of the routing protocol by providing alternative routes. These issues can be addressed by clustering the similar devices under a network and using different standards/protocols based on the cluster's needs. This is also related to interoperability which is discussed next.

4.3.2. Interoperability

The nodes and networks in SG may be owned and managed by different entities. To prevent large-scale blackouts and cascading failures, these utilities need to be able to route information among each other. Therefore, interoperability, the capability among different systems to exchange and use information securely, efficiently, and easily, is very important in a complex system such as the SG. The components of each of these different systems will need a way to communicate with each other independent from the physical medium used, type of devices, and manufacturers. One of the solutions typically employed currently is to deploy gateway nodes at certain edges of the communications network which can communicate with different entities via multiple interfaces. Gateway nodes will be able to recognize different protocols to provide interoperability among different components. However, it may not be possible to deploy such gateway nodes in every part of the networks. In addition, with the increasing variety of application, interoperability requirements may force researchers to come up with standard protocols that can be deployed in HANs, NANs and maybe WANs without any bridge device such as a gateway. This leads the routing design to consider standardization for the used hardware as well as used addressing architectures (e.g., IPv6 can be used in all devices to provide interoperability).

4.3.3. Node Placement

The network topology in SG HANs, NANs and WANs is formed based on the nodes placement and their transmission range. Given that most of the nodes such as smart meters, sensors and gateways are fixed and deployed at specific locations across large geographic areas with varying density and transmission ranges, HANs, NANs or WANs will have a wide variety of possible network topologies. The decision for data collector or sensor location in a NAN may affect the routing performance based on the signal quality, dynamically created links or interference from within or outside the SG communications network. For instance, in a HAN used for AMI applications, some bottleneck nodes may exist due to poor links and no other nodes may be available as alternative routes [15]. Furthermore, the collisions can be high at the data collector and its nearest nodes since all packets are forwarded into the direction of the collector. Therefore, the additional relay nodes would be needed which may require significant updates to the routing protocol to be used. The issue of node deployment plays a significant role when sensors are deployed for monitoring the SG devices. Careful planning of node placement may help alleviate some problems of routing in terms of interference and reliability. The addition or removal of new nodes should also be considered by the routing protocols to update the existing routes.

4.3.4. Network Dynamics

Most of nodes in SG are static. However, electric vehicles, mobile workforce and some nodes in the Distribution Grid Management application are considered mobile. Mobile nodes introduce new challenges regarding the handling of mobility and tractability of the nodes which can affect the routing protocol.

A good example for mobility is the involvement of mobile workforce in the SG. While on the way, the mobile workforce may perform a machine-to-machine communications to the sensors at the faulty location for online diagnostics. Sensor could be part of a Wireless Sensor Network (WSN) and they can communicate with mobile workforce devices via another network. In this case, routing message from and to the mobile workforce vehicle is more challenging since route stability becomes an important issue. Efficient routing with relatively low latency, high reliability, high security and support for mobility is required for this application. In addition, the network topology may change over time due to link and node failures, intra-network interference, as well as interference from the SG.

Tracking the vehicles could be another application where the field vehicle is being tracked and directed to the faulty SG location. The tracking information for the vehicles needs to be routed via the communications network of the SG. For instance a fleet management approach as in [13] could be followed to route the tracking information.

4.3.5. Security and Privacy

Security as a major requirement covers all aspects of the SG, from physical devices to routing protocol operations to ensure the availability and reliability of the whole network. Many endpoint devices in power transmission and distribution networks, and power generation networks are located in an open, potentially insecure environment which makes them prone to malicious physical attacks. These devices must be protected properly against unauthorized access such as modifying the routing table or some network information stored in the compromised device. These actions as well as spoofing, altering or replaying routing information during information exchange between nodes are examples of attacks against routing protocols.

Another major concern in the routing would be the privacy of the power data. Many customers would be reluctant to expose their power usage data (as well as the electric vehicle locations) and thus confidentiality and anonymity should be provided at all times. This may require additional mechanisms other than confidentiality when routing the data. For instance, if the customers may not even trust the utility company, the usage data may need to be routed to a third-party escrow service to provide the billing service. Non-repudiation is also required in some electricity transaction applications such as in the future electricity trade-market, and electric vehicle's power usage in public or private charging stations.

As a result, routing protocols should be designed by taking into account the security and privacy requirements of the specific SG applications considered. Wherever needed, confidentiality, integrity, authentication, and data validation should be provided as part of the routing process.

4.3.6. Quality of Service (QoS)

QoS, a guarantee by the network to provide certain performance in terms of bandwidth, reliability, delay, and jitter, etc., is also important in the SG. SG applications require QoS to provide high reliability and availability, especially for system control and situational awareness. For instance, the information concerning power networks incidents or disturbances, pricing of electricity, electricity load balancing, and electricity generation failures need to be delivered in real-time or near real time. The video surveillance for securing critical assets requires a high bandwidth. The power consumption data from each household can be generated at different pace and size. Billing application requires low frequency data reporting (weekly/monthly) and an aggregation of appliance-level data while demand response and managing load applications require much higher frequency (seconds/minutes/hours) of power consumption data reporting for more accurate information.

Besides the application, there are challenges that arise from the underlying low level protocols. Due to the specific features of their access and physical layers, different wireless communications technologies usually provide diverse QoS which impact the performance of routing protocol [16]. For example, IEEE 802.11 wireless LAN offers relatively high bit rate but the service is best effort since the access to medium is based on carrier sensing and random access. On the other hand, cellular networks offer better coverage and stability but at the lower data rates.

To provide QoS at the network layer in the SG, all QoS requirements from the application as well as the heterogeneity of the network with various resource constraints and underlying communications technologies should be considered. This is sometimes referred to as cross-layer design where one takes into account the constraints from application, MAC and physical layers when designing the routing protocol. QoS routing will not only consider finding a path to the destination but also ensure certain characteristics on such a path.

4.3.7. Scalability

Routing scalability or the ability to provide an acceptable level of service even with a sheer number of nodes is very crucial for the SG. Millions of smart meters will be attached to communications network to deliver power usage data from each household to utility companies. Nonetheless, the number of nodes connected to the network at a certain location would vary depending on the population density in that area. For instance, while urban areas will have a high density of customers, rural areas will be sparsely distributed with low number of customers. Therefore, any proposed routing protocol for the SG should be able to scale under a variety of use cases with their distinct operational requirements. Route discovery, maintenance and key distribution in case of secure routing will grow rapidly with the network size. This design issue may significantly affect the way the routing protocols are designed depending on the application and underlying network and the link metrics used.

5. Routing Protocol Classification in SG Communications

As noted before, in this paper, we survey the existing routing protocols for SG communications based on the corresponding network, namely HANs, NANs and WANs under a separate section. Before moving into the details of the proposed routing protocols, we first provide a classification of these protocols based on some criteria.

Our criterion is the underlying communications used for routing. There are mainly two technologies used: wired and wireless communications. While wireless communications refers to several options such as IEEE 802.11-based Wireless Mesh Networks (WMN), RF Mesh, WiMAX, 3G, 4G or LTE, wired communications refers specifically to power line communications (PLC) which uses the existing powerline for data communications. Other wired technologies, such as Ethernet and Fiber, are not included since they are special technologies that are not introducing routing issues.

PLC has been used to control power distribution networks for more than a half century [17]. It offers several benefits due to the use of the existing powerline for data communications: PLC has low deployment cost, is able to reach a remote and isolated node as long as it is connected to the powerline, owned by the utility company itself and hence provides a certain level of security, and does not need redundant communications channel as in wireless communications. Due to these benefits, various proposed applications of PLC, specifically for home automation and SG, are found in the literature [18, 19, 20, 21, 22, 23]. Note that PLC also has specific behaviors that need to be addressed. Abrupt changes frequently occur during the normal operation when a node is turned on/off. The on/off of a node alters the impedance of the powerline and hence creates unbalance between transmitter, receiver and powerline. Such alterations not

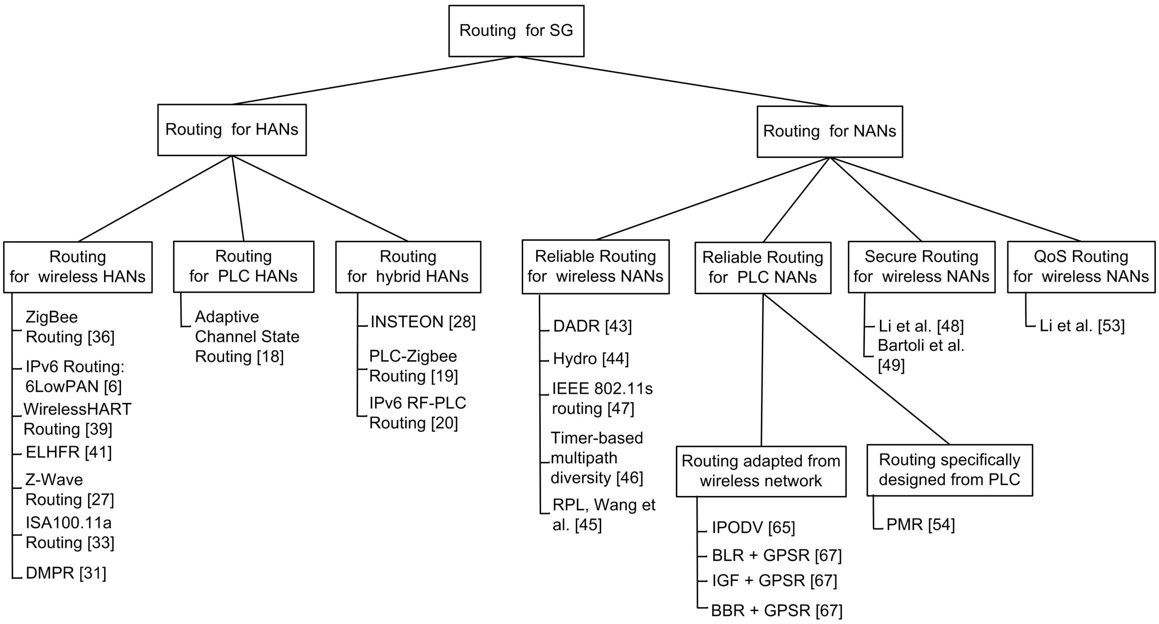

Figure 5: Routing protocol classification in SG Communications.

only influence the associated node but also affect the communications channel of the neighborhood around that node. And thus, asymmetric links between nodes occur. Therefore, reliability, connectivity, and response time are the main issues that need to be addressed in PLC networks.

Among the options for wireless communications, we focus on WMNs as for the others the communications is single-hop from the sources to the utility and thus routing is not an issue. WMNs are communications networks made up of radio nodes (e.g., home appliances, smart meters or gateways) organized in a mesh topology [24, 25]. The goal is to relay the data via this mesh network in multiple hops before it connects with the WAN or the utility. One nice issue here is to be able to utilize the existing smart meters as the relay nodes and thus provide a great coverage without depending on other network providers. There has been a great interest from the research community recently on mesh-based HAN and NAN implementations and thus many routing protocols have been proposed. In this respect, ZigBee [24] has been one of the widely used standards in HANs while IEEE 802.11s [26] has been the promoted standard in NANs.

We classify the protocols for HANs based on the underlying network using wireless communication, PLC or a combination of these. Specifically, three classes of routing protocols exist in HANs: 1) Routing in Wireless HANs; 2) Routing in PLC HANs; and 3) Routing on Hybrid HANs.

This criterion can also be applied to NANs. However, there is another criteria in NANs. This criterion is the goal of the routing protocol which considers reliability, security and QoS as the performance metrics. Thus, in addition to the underlying communication use for routing criteria, we have three classes of protocols. Nonetheless, PLC-based approaches focus solely on reliability metric and we currently do not have any security or QoS-based routing under PLC. Therefore, we will consider four classes: 1) Reliable Routing in Wireless NANs; 2) Reliable Routing in PLC NANs; 3) Secure Routing in Wireless NANs; and 4) QoS Routing in Wireless NANs. Fig. 5 represents these graphically.

6. Routing Protocols for HANs

There are several protocols that have been recommended for HAN communications. These are mainly based on wireless communications, some of which are open standards. Open standards are mostly built on IEEE 802.15.4 standard such as ZigBee, WirelessHART, and ISA100.11a. There are also a number of proprietary protocols such as Z-Wave [27], INSTEON [28] [29], and Wavenis [30]. On the wired side, HomePlug is the leading standard for PLC. Recently, a number of studies have targeted the design and implementation of these protocols along with their comparisons and analysis [6, 29, 31, 32, 19, 33, 34, 35].

In what follows, we provide a review of routing protocols under three categories in separate subsections: wireless HANs, PLC HANs and Heterogeneous HANs. At the end, we also provide a comparative summary of the major protocols.

6.1. Routing Protocol for Wireless HANs

6.1.1. ZigBee Routing Protocol

ZigBee is a standard developed by ZigBee Alliance and recommended as the common choice for HAN implementations [24]. ZigBee builds its network layer and application layer on top of the IEEE 802.15.4 standard. It has three types of devices: ZigBee coordinator, router, and end device. While both ZigBee coordinator and router are IEEE 802.15.4 Full Function Devices (FFDs) that have the ability to route packets, an end device is an IEEE 802.15.4 Reduced Function Device (RFD) that has a limited function and acts as a leaf node in the network. As shown in Fig. 6, ZigBee supports three types of network topology: star, tree, and mesh. Star topology is a one-hop topology from end devices to a router or a ZigBee coordinator while tree and mesh topology support multi-hop communications. Only one ZigBee coordinator is allowed in a tree topology or mesh topology to manage the whole network.

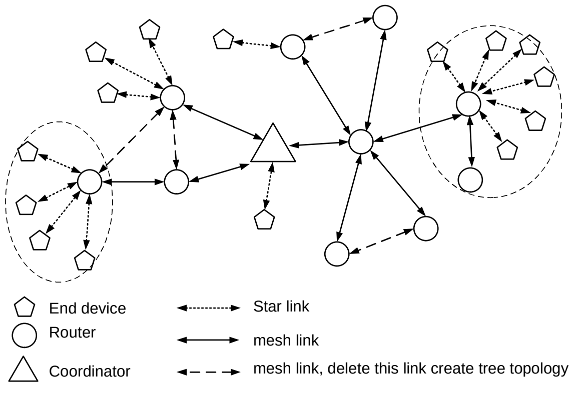

Figure 6: ZigBee network topology.

Routing in a ZigBee network depends on the network topology. ZigBee network layer provides three routing protocols [6]: (1) tree routing rooted at the ZigBee coordinator for data collection, (2) on demand mesh routing; and (3) source routing for the sink node to reply back to the end device in many-to-one communication. However, the supported number of hops for each routing is limited to 10, 30, and 5 hops, respectively.

Tree routing rooted at the ZigBee coordinator is a proactive routing based on the parent-child relationships established during the network formation phase. Firstly, the ZigBee coordinator defines the maximum number of routers and end devices per router, and the maximum depth of the network tree. Based on these three parameters, ZigBee network layer performs hierarchical distributed address assignment in which 16-bit network address space is divided by the ZigBee coordinator to its children using the following recurrence [36] :

$$A(d) = \begin{cases} 1 + D_m + R_m & if\ d = L_m - 1 \\ 1 + D_m + R_m \times A(d+1) & if\ 0 \leq \mathrm{d} < L_m - 1 \end{cases} \qquad (1)$$

where $A(d)$ is the number of addresses allocated at the tree depth d, R_m is the maximum number of routers connected to a router, D_m is the maximum number of end devices per router, and L_m is the maximum depth of the network tree. The coordinator and routers always take the first address of the address space while end devices take the last D_m addresses of the address space. For instance, Fig. 7 shows the address assignment for the tree topology from Fig. 6 with R_m = 5, D_m = 6, and L_m = 3. Based on the Equation 1, the total required addresses for these parameters is 242 addresses. As seen in Fig. 7 the address starts from 0 (taken by the coordinator) and the address space is represented in a square bracket (e.g.,[0-241]. A maximum of five routers and six end devices is allowed to connect to the coordinator and hence addresses [1-235] are allocated further for routers and addresses [236-241] are allocated for end devices. At the tree depth=1, the total number of required addresses is 67 addresses, and hence the three routers have the address spaces allocation of [1-67], [68-134] and [135-201] subsequently. At the tree-depth 2, the total number of required addresses is 12 addresses. The first address is always for the parent router, the next five addresses are for routers, and the last six addresses are for end devices.

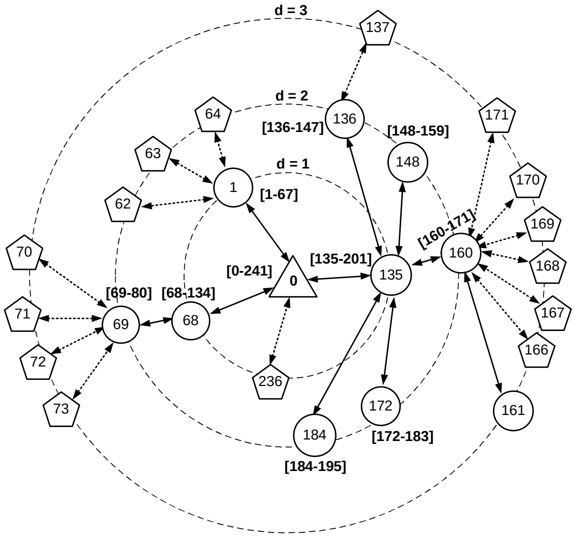

Figure 7: Address assignment for Fig. 6.

When a device (either a router or an end device) joins a parent node during the network formation, the parent node will provide an address to this node from its address pool. Since every router knows its address space, each router can easily determine whether the destination belongs to one of its children or not.

On the other hand, on-demand mesh routing is based on route discovery mechanism from Ad Hoc On Demand Distance Vector (AODV) [37]. Routes are established and stored in the routing tables through Path Request and Path Reply messages where the originating device broadcasts Path Request and the destination device replies with a Path Reply message. When the originating device is unable to find the route to destination in its routing table and also is unable to initiate route discovery, tree routing is used as a last resort.

However, these two routing protocols have scalability issues. Even though the address assignment can allow relatively simple routing algorithms, it may cause address exhaustion as the tree depth exceeds the pre-defined tree depth (e.g., for router with address 161 as in Fig. 7). Furthermore, changes to the tree topology may require re-addressing for most of the nodes if not for all the network. Another scalability issue is on many-to-one communications in which many end devices are communicating with a sink node. The routing table of routers near this sink node will have many route entries and may overflow due to the limited memory capacity of routers. To address these issues, the newer version of ZigBee called ZigBee Pro provides stochastic addressing mechanism and route aggregation. In the stochastic addressing mechanism, new end-devices are allowed to choose an address at random when they are joining the network. If there is a collision in which two end-devices pick the same address, ZigBee Pro has an address conflict resolution mechanism utilizing the unique MAC address of each node.

In source routing, instead of each end device broadcasting a route request to the same sink node, the sink node broadcasts a single route request and every router in the network records the sink node in its routing table as the destination. Then, when the end devices send data to the sink node, a reverse source route is built up in the packet. In this way, the sink node can immediately reply to the end device either saving or without saving the route to the routing table.

While ZigBee routing is envisioned for home automation applications, its use in apartments/multi-story office buildings maybe an issue regarding the addressing mechanism and interference. The need for gateways to provide relaying to the smart meters that are typically situated in the basements of such buildings is another issue.

6.1.2. IPv6 as the Routing Protocol: 6LowPAN

6LowPAN is an acronym of IPv6 over Low-power Wireless Personal Area Networks (WPANs). 6LowPAN builds an adaptation layer between MAC layer and network layer to enable the transmission of IPv6 packets over IEEE 802.15.4 [6] through: (1) fragmentation due to the different size of IPv6 packet (1280 bytes) and IEEE 802.15.4 frame size (127 bytes); (2) header compression from 40 bytes of IPv6 header to 2 bytes; (3) IPv6 address auto-configuration; and (4) IPv6 neighbor discovery for LowPANs. 6LowPAN has two categories of routing based on which layer the routing decision is done: (1) the mesh-under or layer 2 mesh where the routing decision is taken at the adaptation layer; and (2) the route-over or layer 3 routing where the routing decision is taken at the network layer. As shown in Fig. 8a, routing and forwarding in the mesh-under are performed at the link layer. A single IP hop will consist of multiple link layer hops. On the other hand, routing and forwarding in the route-over are performed at the network layer and each link layer hop is an IP hop as shown in Fig. 8b. For instance, Routing Protocol for Low power and lossy networks (RPL) [38] which will be discussed in the next section for NANs, is a candidate protocol for the route-over routing and can be used in HANs as well as NANs.

6LowPAN provides great advantages in terms of interoperability which have been mentioned in the previous subsection. For instance, in [32], 6LowPAN is used to provide end-to-end interoperability and QoS guarantees between ZigBee network (i.e., a HAN) and a BAN through a dual-stack gateway router. This gateway router performs QoS classification and packet aggregation on ZigBee application layer packets before tunneling them to the BAN server over 802.11 links.

Nonetheless, 6LowPAN has several issues to be addressed: Secure neighbor discovery (i.e., determining the IPv6 network prefix, local routers, and other network configuration parameters), service discovery (i.e., automatically locating other sensors/nodes and controllers and available higher layer services) and application of IPsec to the small home devices.

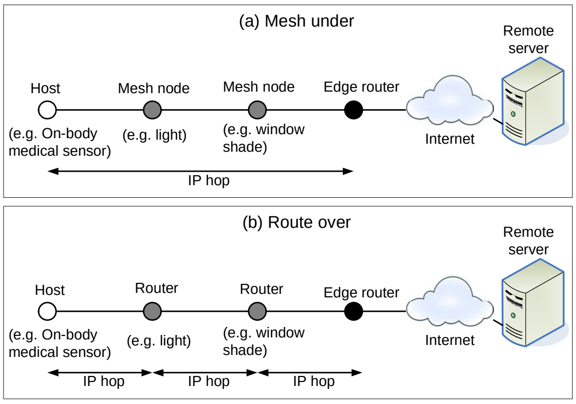

Figure 8: Mesh-under and route-over comparison [6].

6.1.3. WirelessHART Routing Protocol

WirelessHART is a technology which is commonly used for industrial real-time applications [39] [40] and is suitable for applications in the electric power system such as in a substation or a generation plant [24]. It is in fact a centralized wireless network that uses a central network manager to provide static routing and communications schedules. It uses graph routing (explained below) to route messages and source routing for network diagnostics. WirelessHART builds its physical layer based on IEEE 802.15.4-2006 and specifies the Data Link, Network, Transport and Application layers.

The network manager in WirelessHART maintains a complete list of all devices and has full knowledge of the network topology. It gets this information from each network device by pulling the neighbor tables from each network device. This neighbor table contains a list of all devices that a network device can connect to. Based on this information, the network manager has a collection of non-unique graph routes that might overlap. Each graph route is associated with a unique graph ID. Fig. 9 shows an example of a network topology that has two graph IDs: graph ID 1 and graph ID 2. Node 1 sends packets to node 3 using graph ID 2, either through node 2 (i.e., graph route 1-2-3) or directly to node 3 (i.e, graph route 1-3). Similarly, node 1 sends packets to node 5 using graph ID 1 which has several routes to node 5 (e.g., graph route 1-3-4-5, graph route 1-2-5, or graph route 1-2-3-4-5). These pre-determined paths are then distributed to each network device. To send a packet, the source device writes a specific graph ID (determined by the destination) in the network header. All network devices on the way to the destination must be pre-configured with graph information that specifies the neighbors to which the packets may be forwarded.

6.1.4. Enhanced Least-Hop First Routing

[41] proposes a routing mechanism which is the implementation of graph routing of WirelessHART called Enhanced Least-Hop First Routing (ELHFR). ELHFR provides multipath to the gateway. Based on the graph topology built by the network manager, ELHFR uses Breadth First Search (BFS) algorithm to build the spanning tree of the graph topology rooted at the gateway. In this way, every node in the spanning tree has a

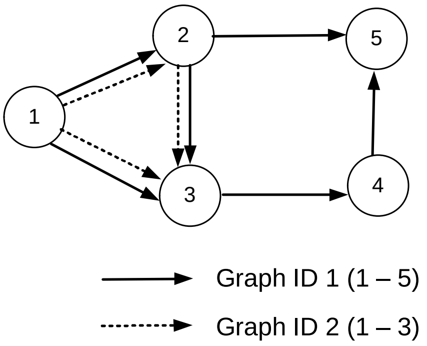

Figure 9: An example of graph routing.

single-path route with the least-hops to the gateway. To provide multipath, ELHFR generates the sub-graph of each leaf node on the spanning tree and use it as the redundant path. All the paths in the sub-graph are given the same graph ID.

The network manager re-generates all the leaf nodes periodically to maintain the routing information. However, periodic route maintenance does not take into account the irregular activities such as a node joining or leaving the network. For these cases, the network manager provides a temporary solution (e.g., provides a single path for the new node) and informs the affected nodes. Later, the periodic route maintenance will provide the ultimate solution. On receiving data, intermediate nodes examine the destination address and perform the following forwarding action: They use source routing if the destination is not gateway and select the next hop neighbor from its graph table. The simulation results show that the packet loss ratio and throughput of ELHFR outperforms AODV [37] when the number of nodes is greater than 30 nodes. However, the end-to-end delay of both protocols does not differ significantly.

6.1.5. ISA 100.11a Routing Protocol

Similar to WirelessHART, ISA 100.11a is suitable for applications in the electric power system such as a substation or a generation plant [24]. It builds the Data Link Layer, Network Layer, Transport Layer, and Application layer; on top of the Physical layer of IEEE 802.15.4-2006. ISA100.11a supports two types of network topology: star and mesh. ISA100.11a has routing mechanism at two different levels: (1) subnet-level mesh routing, and (2) backbone-level routing. While subnet-level mesh routing is performed at the data link layer, backbone-level routing is performed at the network layer. At the subnet-level, graph routing and source routing are used. However, the details of backbone-level routing are not specified [33].

6.1.6. Disjoint Multi Path Routing Protocol

[31] proposes on-demand Disjoint Multi Path Routing Protocol (DMPR) for ZigBee-based home network control system that uses Infrared (IR) and relay modules as the actuators. IR is used to control TV, DVD and AC; while relay modules are used to switch power on/off in electronic devices and control a motor. DMPR is based on Kruskal's algorithm, a greedy algorithm that finds a minimum spanning tree of a connected weighted graph by selecting a node which has the minimum energy so that the total energy level of all the nodes is minimized. Source routing is employed during data forwarding so that the sink can use the routing path list in the packet header to reply to the sender. This protocol is geared to home automation in WPANs and its applicability to SG has not been discussed. One possible application for this protocol could be in Demand Response systems for the utility company to turn on/off a device for energy saving purposes.

6.1.7. Z-Wave Routing Protocol

Z-Wave is a proprietary technology developed by ZenSys and intended for home control and automation [6] [27]. It consists of a protocol stack with five layers: Physical, MAC, transfer, routing, and application layer. Z-Wave has two basic types of devices: Controller and Slave. Controller device can issue control commands while slave is an end device that executes commands from the controller. Controllers are differentiated further based on their functions in the network. A primary controller is the only controller in Z-Wave mesh network that has the ability to include or exclude devices in the network and hence it has the latest network topology in its routing table. Other controllers copy their information from the primary controller when they join the network. Typical primary controllers are portable (e.g., a battery-operated remote control) while secondary controllers are typically static and connected to a power source. Slave devices may also forward a message if the received command message requested them to do so. A special slave, called *routing slave*, is allowed to send messages to other nodes without being requested to do so. This slave has predefined static routes to some nodes when it joins the network.

Z-Wave employs source routing mechanism at the routing layer. The controller that initiates the message stores a complete route of up to four hops to destination in the frame. Every intermediate node forwards the message according to this route. In case of portable controller, it will try to reach the destination directly first (i.e., no routing) before trying to determine its position and finding a node that can be used as a starting point for repeating a frame. Based on this starting node, it calculates the shortest route to the destination, and puts a complete route in the frame.

6.2. Routing Protocol for PLC HANs

PLC has two different classes based on their operating frequency and data rate: Broadband (BB) PLC and Narrowband (NB) PLC. While BB PLC, standardized as IEEE 1901, was approved in 2010, NB PLC standard is currently under development by the IEEE P1901.2 working group. Our focus is NB PLC since BB PLC does not need to employ routing.

An example of NB PLC routing is given in [18]. The authors propose an Adaptive Channel State Routing (ACSR) algorithm that tracks the variation of the PLC network topology to find a reliable path. ACSR is based on shortest path routing. It uses Channel State Indicator (CSI) metric to measure the channel stability between two nodes and distance metric to check node reachability. Every node periodically sends a routing information packet with a sequence number to their neighboring nodes.

The CSI value is incremented whenever a node sequentially receives a routing information packet from a neighboring node and otherwise decremented whenever the routing information packet is not sequential due to a packet loss. A channel state is stable if the CSI value is higher than a given threshold value and unstable otherwise. When the path between two nodes is symmetric and both nodes can perform direct exchange, the distance metric value is 1. Repeater nodes are required for packet exchange when the distance value is greater than 1. An infinite value of the distance metric shows asymmetric path or unknown path between two nodes.

Due to the fact that every node may have a different size of neighboring nodes, a probabilistic flooding is used when the path between two nodes is unstable or unknown. The flooding probability is determined by the node's density around the relaying node. A high probability is given for a light area.

The proposed routing protocol is compared with DSDV (Destination Sequenced Distance Vector) [42], a shortest path routing which is used for Mobile Ad-hoc Networks (MANETs), in a high Packet Error Rate (PER) testbed. In DSDV, each route tagged with a sequence number to indicate the age of the route. This sequence number is generated by the destination. A route with higher sequence number is preferred for forwarding decision. If different routes have the same sequence number, the route with a better metric is selected. In addition, DSDV guarantees loop-free routes for each destination. However as a distance vector routing, DSDV requires a periodic update of its routing tables in addition to the trigger update due to topology changes.

The experiments show that ACSR, compared to DSDV, has a better throughput and shorter end-to-end delay. Furthermore, ACSR also creates less network traffic than DSDV that uses a simple flooding mechanism. However, the path set-up time of ACSR is longer than DSDV since ACSR should wait until the CSI value is above the threshold value before establishing the path between two nodes.

6.3. Routing Protocol for Hybrid HANs

Hybrid approaches that combine wireless and PLC are preferred in home automation to provide path diversity and to increase reliability. This section discusses these approaches.

6.3.1. INSTEON

INSTEON [28] [29] is a proprietary standard that provides a hybrid mesh of RF and PLC for home automation. Every INSTEON device can be an RF-only device, a powerline-only device, or a hybrid RF-powerline device. Each type of device can generate, receive and forward message. A mechanism called "simulcast" is used to deliver a message from a sender to a receiver. When a sender generates a message, every neighbor node within the range of the sender that receives the message, simultaneously retransmits the message within a given timeslot to enhance the signal strength. When a hybrid device receives a message and needs to transmit it again, the hybrid device retransmits the message via the alternate medium first before retransmiting it via the same medium. For instance, when a hybrid device receives a message via powerline, it will first retransmit it via RF and then retransmit the same message via powerline in the next timeslot. In this way, path diversity can be achieved. INSTEON uses two fields in its message to avoid broadcast storms. The *max hops* field is used to configure the maximum hop of the message. The maximum allowable hops is 4 hops. The *hop-left* field is used for forwarding decision. This hop-left field is similar to Time To Live (TTL) field of Internet Protocol (IP). The message is retransmitted as long as the hop-left value is greater than zero. Before, a node retransmits a message, it decreases the hop-left value.

INSTEON is a proprietary technology which makes it difficult for academic community to engage in further research on it.

6.3.2. Routing in PLC-ZigBee Network

In [19] a combined PLC and wireless communications for home automation, specifically a backbone network of HomePlug Command and Control (HomePlug C&C) and ZigBee, is proposed. Flooding and AODV routing protocols are integrated to this network with some adaptations in the forwarding mechanism. For flooding approach, each node forwards data packets with a given sequence number only once, regardless of the number of interfaces and underlying links. For AODV, instead of broadcasting, nodes sequentially forward Route Request (RREQ) to destination nodes. Three routing strategies are used to exploit the combined network: (1) Joint-path, (2) Backbone-based, and (3) Dual-path.

Joint-path is the basic strategy and establishes joint routes that may traverse both networks to reach destination nodes. Backbone-based is built on joint-path but firstly selects powerline to forward packets. Dual-path allows nodes to receive packets either from a wireless path or a backbone-based path. Packet Delivery Ratio (PDR), average end-to-end latency, energy cost, and network overhead are used to evaluate the performance of the combined network. Simulation results show that the PDR of dual-path and backbone-based strategy are better than joint-path while flooding is better than AODV in term of network energy cost, network overhead, and average latency. The combined network also shows a lower network overhead and higher PDR than a single wireless or wired network.

6.3.3. Routing in IPv6 RF-PLC Network

The work in [20] proposes hybrid IPv6 RF-PLC network architecture in smart buildings. This architecture composed of battery-operated RF-only nodes, PLC-only nodes, and RF-PLC gateways. The RF-PLC gateway uses 6LowPAN route-over protocol to provide interoperability between RF and PLC. The routing protocol in 6LowPAN route-over is RPL and the routing metric is a node's energy estimation. The protocol selects the less energy wasting path while Expected Transmission Count (ETX) routing metric is used for a tie-breaker. RF-PLC gateways are placed in such a way that every RF-only node could reach a gateway in one hop to optimize the network lifetime of the RF nodes. RF-only nodes send their packets to the nearest RF-PLC gateway which then relays them to the PLC backbone. PLC backbone is responsible for forwarding them to the base

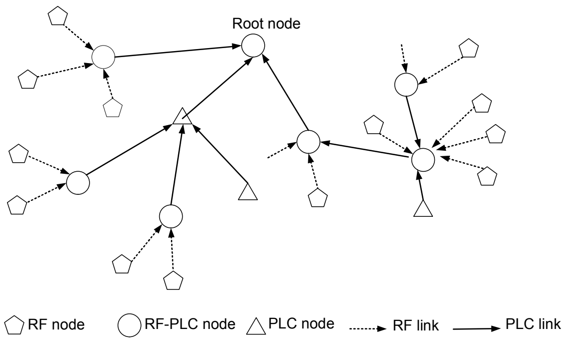

Figure 10: Example of RF-PLC network with one-hop to a gateway.

station as shown in Fig 10. Simulation results show that an increase in the number of RF-PLC gateways improves the network lifetime, decreases latency, and reduces packet loss.

6.4. Summary of Routing Protocols for HANs

In Table 2, we provide a summary of routing protocols for HANs by specifying the associated MAC and adaptation layer protocols. In particular, the used underlying MAC protocol affects the design, cost and performance of routing protocols.

7. Routing Protocols for NANs

As previously discussed in Section 4.2, many applications of SG utilize NAN. In particular AMI applications have received the most attention from the research community so far. In such applications, the routing protocols focus on data reporting from the access point tier (i.e., Smart Meter) to the backhaul distribution tier (data collector) as shown in Fig. 4. However, depending on the used underlying communication, routing challenges may differ. As previously mentioned in Section 5, we focus on two network types that introduce routing issues: 1) WMN and; 2) PLC. Further, we classify the WMN-based routing protocols into 3 categories based on the SG requirements: Reliable Routing [43] [44] [45] [46] [47], Secure Routing [48] [49] [50] [51] [52], and QoS Routing protocols [53]. These classifications and comparison of each routing protocol can be seen in Table 3. We now look at each category in detail.

7.1. Reliable Routing in Wireless NANs

Frequent route breaks occur in a wireless mesh network because of fading effects and signal interference that make the quality of wireless links unstable and time-variant. This is especially true for SG applications which are deployed in harsh environments. To tackle this problem and improve the reliability, three approaches were proposed for SG: 1) Utilizing multiple paths [43] [44] [46]; 2) Providing fast and effective path repair mechanism while minimizing the control overhead using ETX-based rank computation and reverse path recording mechanism [45]; and 3) The modification of cost metric calculation and the use of route fluctuation prevention algorithm [47]. Note that these techniques have already been used in several ad hoc networks such as Wireless Sensor Networks (WSNs) and now their applicability to a large-scale SG network are investigated as detailed next.

7.1.1. Distributed Autonomous Depth-First Routing

Distributed Autonomous Depth-First Routing (DADR) [43] is a proactive distance vector routing protocol without control messages for path maintenance or path repair. It uses a lightweight control mechanism to provide at most k (when available) possible paths for each destination and a Depth First Search (DFS) guided by the routing table and backtracking mechanism for path recovery after link failures. The routing table is updated based on the information learned during data forwarding, during periodic HELLO message exchanges among neighboring nodes, or when the node receives a route poisoning message. A unique Frame ID (FID) is added to the packet for loop detection. Each time a node forwards a packet, it stores FID, previous sender and the next hop in the FID table. When the node finds the FID of the received packet in its FID table, i.e., loop is detected, then it generates a route poisoning message to inform others that loop occurs and the path should be removed from their routing tables. The FID table entry is deleted when the FID_{timer} related to that entry expires, assuming that the packet has been delivered correctly. The link cost, i.e., data forward ratio metric, is incremented when an acknowledgment for each packet sent is received to reflect a more reliable link and decremented otherwise.

The real deployment of DADR in a large-scale flat mesh network of up to 1500 nodes in Japan as well as the software simulation of large-scale flat mesh network that consists of 2107 smart meters and 500 relay nodes show its scalability [43]. DADR reliability is also shown in a small-scale deployment in either indoor or outdoor environment experiments. The indoor experiment uses twelve nodes with IEEE 802.15.4 standard. The outdoor experiment uses twenty nodes. In both environments, even when a central node where most of the routes to the gateway pass through is taken out, the reliability slightly declines before it goes back to 100% again. This shows the capability of data forwarding mechanism in learning a new route. In addition, the guided DFS creates less control overhead than AODV [37] and Optimized Link State Routing (OLSR) [55] for path recovery after link failures in a large-scale unreliable network. For a 500-node network, AODV that uses Breadth First Search (BFS) requires 250,000 control packets, OLSR that uses a Modified BFS requires 25,000 control packets, and the guided DFS requires only 5,000 control packets.

This approach provides several advantages in unreliable wireless environments. It adapts quickly to the frequently changing topology by using an alternate route while carrying the information about the failed link in the data packet. Hence, routes are updated dynamically with low control overhead. Furthermore, since the bit error rates of links depend on the packet size, it provides a more reliable topology compared to the traditional route discovery approach in which the control packet is smaller than the data packet. It also avoids the discrepancy of the link's reliability since there is no time difference between route discovery and data forwarding as in the traditional routing. Typical traditional routing has two independent steps:(1)

Table 2: Summary of Routing Protocols for HANs.

Routing Protocol	*Data Link*	*Adaptation Layer*	*Network Layer*
ZigBee	CSMA/CA	n/a	Tree routing, on-demand mesh routing, source routing
6LowPAN			
- Mesh Under	CSMA/CA	layer 2 mesh routing	n/a
- Route Over	CSMA/CA	n/a	RPL routing
Wireless-HART	TDMA	n/a	graph and source routing
ISA100.11a	TDMA, CSMA/CA, graph routing and source routing	n/a	backbone routing
Z-Wave	CSMA/CA	n/a	Source routing
INSTEON	TDMA	n/a	Simulcast

Table 3: Routing Protocol Classification for NANs.

Routing Protocol	*Reliable*	*Secure*	*QoS*	*Point-to-point routing*	*One-to-many routing*	*Many-to-one routing*	*Multi-path*	*Low Latency*	*Scalable*	*Energy Efficient*	*Load Balancing*	*Application*
DADR [43]	✓				✓	✓	✓		✓			wireless AMI
Hydro [44]	✓			✓	✓	✓	✓		✓		✓	wireless AMI
Timer based multipath diversity routing [46]	✓				✓	✓	✓				✓	wireless AMI
Jung et al. [47]	✓			✓		✓	✓					wireless AMI, status management and monitoring
Wang et al. [45]	✓				✓	✓		✓	✓			wireless AMI
Li et al. [48]		✓			✓	✓			✓			wireless AMI
Bartoli et al. [49]	✓	✓				✓				✓		wireless AMI
Li et al. [53]			✓	✓					✓			DR
PMR [54]	✓				✓		✓					AMI-PLC

route discovery and maintenance, and (2) data forwarding. Another advantage is, instead of initiating a new route discovery when all possible next hops fail, it returns the packet back to its previous sender so that the previous sender can try an alternate route. As shown in Fig. 11, node **a** returns the packet back to **Src** and then **Src** tries an alternate route through node **f**.

However, as the authors also mentioned in [43], this approach has several disadvantages even though they have not seen the degradation of performance due to these disadvantages. First, it has additional state in the data forwarding phase which increase the CPU and memory overhead of intermediate nodes. Second, loop detection false positives might occur when the acknowledgments are lost since there can be multiple packets with the same FID traveling across the network. Loop detection false negatives might also occur in which some data forwarding loops are undetected when the FID table is deleted to early, i.e., FID_{timer} is too short. Another disadvantage is the packet latency in the flat mesh topology since the data packet needs to travel in several hops to reach the destination.

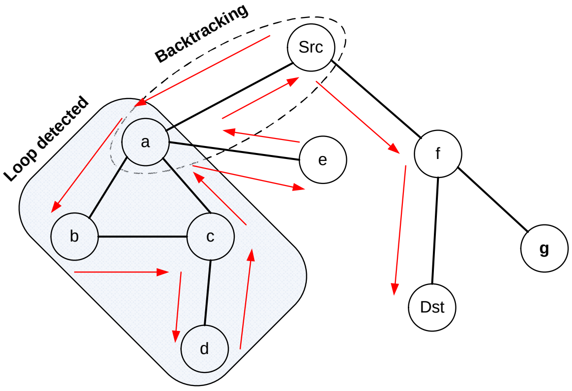

Figure 11: Backtracking mechanism and loop detection.

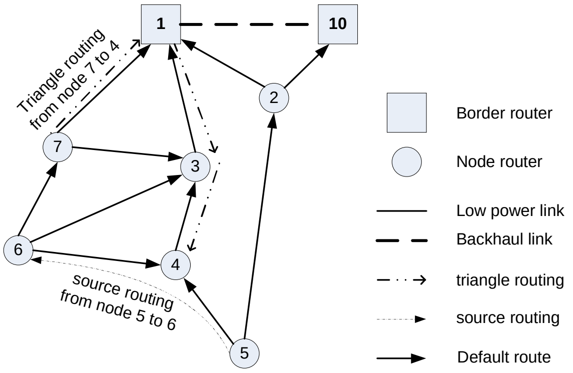

Figure 12: A network with multiple border routers.

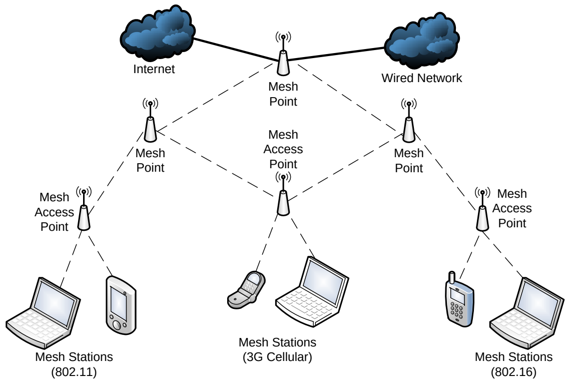

Figure 13: A sample WMN using 802.11s notation [57].

7.1.2. Hybrid Routing Protocol

Hybrid Routing Protocol (Hydro) [44] is a link-state routing protocol for Low-power and Lossy Networks (L2N). It uses a distributed algorithm for Directed Acyclic Graph (DAG) formation that provides multiple paths to a border router. To provide a reliable default route to a border router, each node builds its default route table by adding its neighbor nodes towards a border router. Then, each node will maintain statistics about the link-layer packet success rate of the nodes in its default route table. The entries in the default route table are ordered based on this data-driven link estimation, i.e., ETX metric.

Each node periodically creates a topology report based on its several top ranked entries of its default route table and opportunistically piggybacks it on frequent data traffic to a border router using a default route. The border router then aggregates the received topology reports to create a global view of the network topology, i.e. the Link State Database. In this way, point-to-point routing through a triangle routing occurs, i.e., source node sends a packet to a border router using the default route and then the border router sends it to the destination node using source routing.

Based on the Link State Database, the border router optimizes an active point-to-point routing between nodes and then uses a *route install* message to update a node's flow table. This *route install* message consists of flow match and flow path. Flow match is the criteria used to determine whether a given packet matches a flow table entry while flow path is a complete path to a destination node. Thus, each node takes the following order of actions to forward a packet to a destination. Firstly, it uses source routing if the packet has source routing information in its header and forwards the packet to the next node in the sequence. Then, point-to-point source routing based on its flow table if the destination is found in the flow table. Finally, it uses the default route to forward packet to a border router, i.e., it uses triangle routing. For example, the communication between node 7 and node 4 in Fig. 12 uses triangle routing. Node 7 sends the message to the border router using its default route and then the border router uses source routing to send it to node 4.

Two testbeds and a real deployment with mesh nodes are used to measure the performance of Hydro. The first testbed consists of 48 nodes located at the same floor and the network diameter varies between 3-5 hops. The second testbed has 125 nodes spread across three floors and the real deployment consists of 57 nodes in which 49 nodes are spread across four floors and eight nodes located at a remote residential environment. Either a PC with a connected node for interfacing with the L2N or an embedded Linux device with an integrated IEEE 802.15.4 is used as border routers. Three days of observation of periodic reports from the network nodes to an external server in the real deployment network has shown that the PDR remains high even during weekdays. Furthermore, the default route to border routers provides the reliability and robustness of Hydro.

Hydro also supports multiple border routers which are connected through separate interfaces through a backhaul link. These border routers are the duplicates of the main border router and maintain the same global view of the network topology. In addition, to avoid single point of failure, proper placements of these border routers can reduce congestion and the network depth in a large network. However, the use of source routing creates significant overhead in large networks (e.g., NANs) that require many hops to reach the destination.

7.1.3. IEEE 802.11s Routing

IEEE 802.11s [26] [56] extends the single hop IEEE 802.11 WLAN to a multi-hop Wireless Mesh Networks (WMNs). Two important features of IEEE 802.11s are the mandatory Coordination Function (CF) called Enhance Distributed Channel Access (EDCA) that enables different medium access priorities and frame forwarding and routing at the data link layer. To differentiate between routing at the network layer that uses IP address and routing at the data link layer that uses MAC address, routing at the data link layer is called *path selection*. The nodes are given special names based on their roles in the mesh. An example is provided in Fig. 13. IEEE 802.11s is yet to be formally ratified.

The default multi-hop routing protocol in IEEE 802.11s is Hybrid Wireless Mesh Protocol (HWMP). HWMP is a hybrid tree routing. It is formed as a combination of on-demand reactive routing and tree-based proactive routing. The on-demand reactive routing is an adaptation of AODV protocol. It is used when there is no root node. It reduces the impact of frequent topology changes, and enables peer-to-peer communications between two nodes. A source node broadcasts Path Request (PREQ) message to initiate route discovery and a unicast Path Reply (PREP) message is sent back by the destination node or any intermediate node that knows a path to the destination.

The tree-based proactive routing is used when there is a root node. The root node initiates route discovery in two ways: (1) By periodically broadcasting a root announcement (RANN) message: Upon RANN message reception, each node sends a unicast PREQ to the root node, and then the root node replies to each PREQ message with PREP message, and (2) By proactively disseminates PREQ message to all nodes in the network: A node creates or updates its path to the root and then replies to this proactive PREQ message if and only if the PREQ message has a greater sequence number or offers a better metric.

The mandatory routing metric in HWMP is the *airtime link metric* that measures the channel resources consumed for transmitting a test frame over multihop routes. It is based on Equation 2,

$$c_a = \left[\mathbf{O} + \frac{B_t}{\mathbf{r}}\right] \frac{1}{1 - e_f} \tag{2}$$

where c_a is the airtime cost of a link, $\mathbf{O}$ is channel access overhead, B_t is the size of a test frame (in bits), $\mathbf{r}$ is the bit rate at which the frame can be transmitted (in Mbps) by a node, and e_f is the link error rate. This link error rate is measured based on the probability of retransmission.

While 802.11s standard is fully compatible with higher layer protocols, its default airtime link metric is reported to be very sensitive to changes in link usage during the data transmission [26] which causes route instability problem. This instability occurs among paths with similar metrics when the less loaded path momentarily offers a better link metric. Shortly after this path is selected for data transmission, its link metric drops and the newly less loaded old path or any other paths will have a better link metric and therefore the routing path may constantly change. In the context of Border Gateway Protocol (BGP), this is called *route flap*. This may be a major issue when the protocol is deployed in very harsh dynamic environments where NANs are deployed.

7.1.4. Improved Reliable Routing via IEEE 802.11s

As mentioned in the previous protocol description, the airtime link metric may not be perfectly suitable for SG environments [47]. Therefore, Jung et al. [47] proposes a link error rate that takes into account the varying packet size and route fluctuation prevention algorithm to address these problems. The link error calculation is shown in Equation 3

$$e_f = \frac{\sum_i^{P_n} M_i \times \left(1 - \frac{B_i}{B_{max}+B_i}\right)}{P_n R_{max}} \tag{3}$$

where M_i is the total number of retransmissions at the MAC layer of node i, P_n is the total number of packets transmitted by node n, and $R_{max}$is the maximum retransmission count, B_i is the size of packet i (in bytes), and B_{max} is the biggest size of the packet respectively. This calculation takes into account the difference in the packet size. The frame retransmission at the MAC layer of smaller frame size has a higher penalty than large frame size since smaller frames are less prone to bit errors.

To handle the route instability, the route selection method in HWMP is modified by taking into account the airtime link cost variation. To support the proposed route fluctuation prevention algorithm, instead of maintaining only one optimal route in the routing table as in the default HWMP, multiple route information from the current RANN messages and from the previous RANN messages are stored in the routing table. Therefore, the routing table stores the optimal route and multiple reserve-paths from the previous RANN messages as well as from the current RANN messages. The optimal route will change if only if the variation of the airtime cost in the current optimal route is higher than the variation of the reserve-path.

The simulation that uses periodic data and on-demand data generated randomly with different packet size in small grid mesh networks show that the proposed method provides better throughput and delivery ratio. Compared to the traditional HWMP, the proposed method has a higher PDR, lower end-to-end delay, and less retransmission at the MAC layer. However, there will be significant extra overhead in the routing table since it stores both previous and current routes.

7.1.5. Timer-based Multipath Diversity Routing

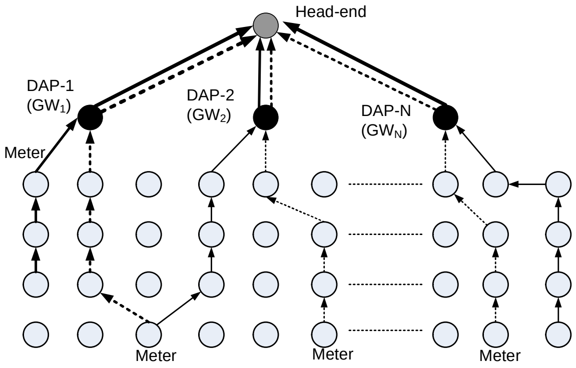

Figure 14: Multiple routes in multigate wireless mesh network [46].

Timer-based multipath diversity routing [46][58] is based on hybrid tree routing of IEEE 802.11s [56]. It uses proactive routing to establish multiple routes to multiple-gateways in advance by periodically broadcasting Root ANNouncement (RANN) message from each Data Aggregator Point (DAP) station at random to avoid collision while on-demand routing mainly deals with the path failures. Each smart meter has multiple routes in its tree table as shown in Fig. 14. If the received RANN is not found in the tree table, a new routing tree is inserted into the table. Otherwise only in case of newer or better path information, the corresponding routing tree is updated.

This routing protocol is modified from the standard HWMP protocol as shown in Fig. 15. Specifically, a backup HWMP buffer stores a self-generated packet (data packet from upper layer) when this packet is sent. If a node receives link failure notification, it will search this buffer for all the affected packets by using the source and destination address information from

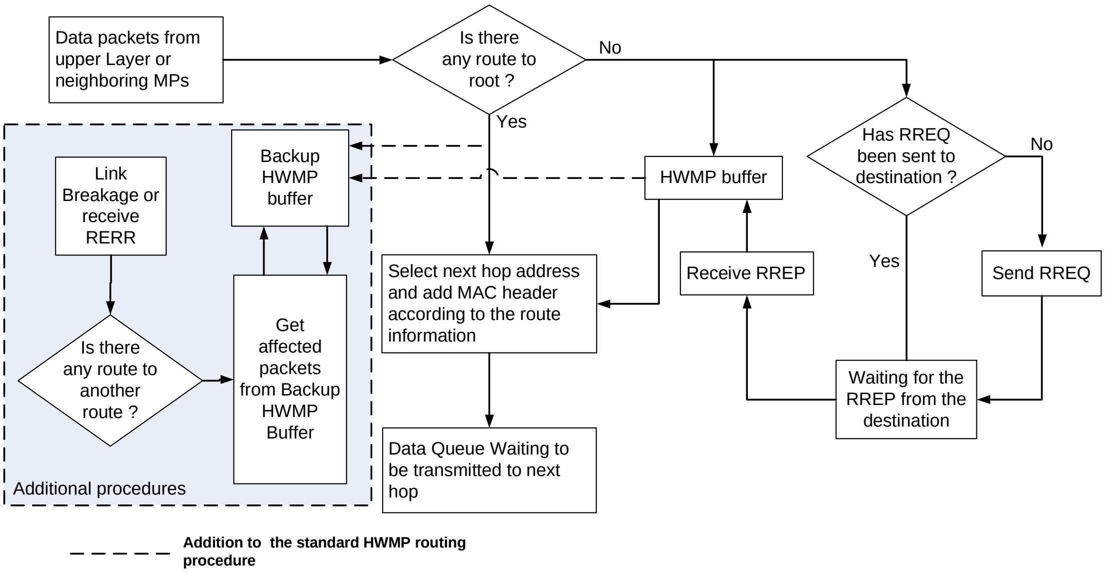
Data packets from upper Layer or neighboring MPs
Is there any route to root ?
No
Yes
Backup HWMP buffer
Link Breakage or receive RERR
Is there any route to another route ?
Get affected packets from Backup HWMP Buffer
Additional procedures
HWMP buffer
Has RREQ been sent to destination ?
No
Yes
Select next hop address and add MAC header according to the route information
Receive RREP
Send RREQ
Waiting for the RREP from the destination
Data Queue Waiting to be transmitted to next hop
Addition to the standard HWMP routing procedure

Figure 15: Timer-based multipath diversity routing operation, recreated from [46].

the notification. The node will then send those packets using the backup route if any. If this backup route has also failed or is unavailable, the on-demand routing starts working to find a new route. The buffer uses a timer to clean-up its content periodically to reduce the possibility of retransmitting packets that have already been successfully transmitted. Nonetheless, the performance of the approach needs to be tested with respect to its tree table insertion overhead when the topology is very dynamic.

7.1.6. IPv6 Routing Protocol for Low Power and Lossy Networks (RPL)

RPL is currently under development by the Internet Engineering Task Force (IETF) [38] to support various applications for Low Power and Lossy Networks (LLNs) such as in urban environment [59], home automation [60], building automation [61], and industrial applications [62]. Thus RPL framework has a flexible design and supports a variety of objective functions in order to build the routing topology based on various link/node metrics and constraints. RPL is a distance vector routing protocol that organizes a topology as a Directed Acyclic Graph (DAG) that could support multiple sink nodes. This DAG is partitioned into one or more Destination Oriented DAGs (DODAGs), one DODAG per sink node. In case of multiple sink nodes, it is expected that the roots are federated by a common backbone. Each node has a certain rank property to maintain its position in the DODAG.

RPL uses two control messages: DODAG Information Object (DIO) and DODAG Destination Advertisement Object (DAO) to construct DODAG, inward path, and outward path. The sink node of a DODAG starts broadcasting DIO message that contains information such as DODAG-ID, rank information of the broadcasting node, and the objective function that specifies the metrics and method for computing DAG rank. Based on rank information and objective function from the received DIO, a node that wants to join the DODAG calculates its rank and the cost of reaching the node from itself. Then it adds the sender of the received DIO to the parent list, updates rank information on the DIO message, and then broadcasts it. In this way, each client node knows its parent and able to forward any inward traffic to the sink by using its parent as the next-hop node. On the other hand, DAO is issued by a node to build an outward path from the sink to the node. It follows the inward path and contains the originator node rank information and reverse route information to record the node visited along the way to the sink. In this way, the root node knows the outward path from the root to the client nodes.

RPL proposes two mechanisms for DAG repairs, a global repair and a local repair. A root node issues DIO with a new sequence number periodically for global repair. However, it poses time overhead for repairing broken link or finding new parent. Hence a local repair mechanism has been designed to fill the gap. First a node starts a 'poison' message to notify its children to find alternate parents. Then it broadcasts DODAG Information Solicitation (DIS) message to trigger the other nodes that hear DIS message to starts sending DIOs. In this way, the problem is fixed locally and only the node with the broken link and a part of its subgraph need to modify its parent list. The work in [63] evaluates this local repair performance in a SG Substation Network based of the real topology and link failure information of 86 electric substations with a single root node. ETX metric is used to build the DODAG. Several routing metrics such as path quality, control plane overhead, ability to cope with unstable situations, and end-to-end delay between nodes are evaluated.

A modified version of RPL [45] was designed to satisfy the reliability and low-latency requirements of large-scale AMI network by using the ETX link metric. The periodic measurement of ETX based on a MAC layer feedback mechanism enables each node to monitor the ETX of links to any of its parent nodes, adjust its default parent and current rank, and inform

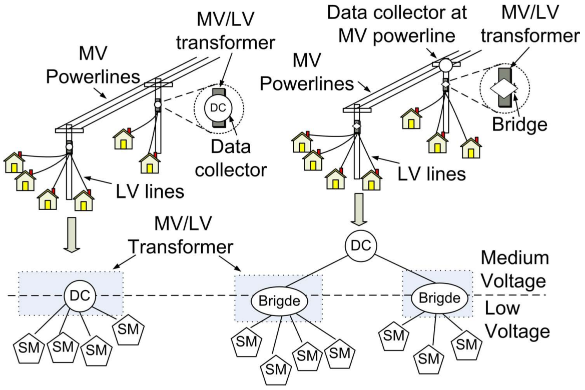

Figure 16: Typical network topology of PLC networks.

others by issuing a DIO message if its current rank is changed. In this way, each node will pick the link with low ETX and hence provide good end-to-end reliability.

To reduce the overhead, instead of using DAO message, the reverse path recording mechanism is used to form outward paths from the inward data traffic. Each time a node receives an inward data packet, the node records the source and the last-hop node in its destination list. Based on its destination list, a node can reach its descendant node by using the last-hop node recorded previously as the next-hop node.

Using a network topology of 1000 nodes and one gateway node located in the center, the overall PDR and average end-to-end delay performance of the proposed routing protocol has been shown to outperform AODV. In contrast to AODV, per-node PDR and per-node average end-to-end delay are not sensitive to the distance of a node to the gateway. A satisfactory performance in both metrics can still be achieved even in the presence of shadow fading.

7.2. Reliable Routing in PLC NANs

By following the structure of the electric power grids, a PLC network can be created. The typical structure of electric power grids is bus or tree topology [64]. In the tree topology, Medium Voltage/Low Voltage (MV/LV) transformer is located at the root of the tree. This tree topology is suitable for AMI applications. Fig. 16 shows the typical network topology of PLC network based on the data collector location. A hierarchical topology can be built based on these two basics topologies. A single data collector can be placed on the MV/LV transformer to collect data from smart meters. A wider coverage of the collector can be achieved by placing the collector on the MV side as shown in Fig. 16. However, this approach may require additional equipment. MV transformer has a different effect on BB PLC and NB PLC. While NB PLC is able to penetrate a transformer even with a significant Signal to Noise Ratio (SNR), BB PLC requires additional equipment, called a coupler, to get through the transformer [22].

To reach the collector, smart meter needs a multi-hop route due to the different distance of smart meter to the collector and the hostility of the medium for data transmission (e.g., varying impedance, noise, high attenuation). However, performing multi-hop in PLC network is very challenging. Due to dynamic topology changes, finding a next hop node would require permanent monitoring of PLC communications channel and frequently updating the routing table. These efforts create a significant signaling overhead. Thus, since the fast changing topology of PLC network is considered similar to ad-hoc/wireless networks [23] [65] [66] [54], various routing protocols from wireless network are proposed to be adapted for PLC networks [65] [67]. However, care must be taken when using routing algorithms from wireless communications to PLC since the network characteristics (i.e., interference) of PLC are different. In addition, in PLC networks, nodes are static and have no power limitation. In this section, we first look at the adapted protocols from wireless networks and then review the protocols that are specifically designed for PLC routing.

7.2.1. Routing Protocols Adapted from Wireless Networks

The work in [65] proposes an Improved On-demand Distance Vector (IPODV) routing protocol to cope with the fast changing topology of PLC networks. Two improvements from AODV are: 1) an improvement in the neighbor table management so that stable neighbors are selected during the route discovery, and 2) an improvement in the route maintenance mechanism to reduce the overhead. In AODV, an entry of the neighbor table is deleted when a node does not receive any packets within the next HELLO message period. However, since the physical topology of PLC network remains unchanged in the long run and only momentarily changes, IPODV takes into account this fact and uses an aging algorithm to record the link quality based on the number of HELLO messages received recently. The link quality is lower when fewer HELLO messages are received from a neighbor node. A threshold value is used for the deletion of the neighbor table entry. If the link quality of the neighboring node is lower than the threshold, the entry is deleted. However, if the link quality is higher than the threshold, the entry is marked as valid. Instead of sending periodic HELLO messages to maintain the routing table and neighbor table as in AODV, IPODV also uses data packets for that purpose and hence reduces the frequency of sending HELLO message as shown in Fig. 17. A detection window is defined and when a node receives a data packet and HELLO message within the detection window, the data packet is marked and sent while the HELLO message is discarded. Other nodes that receive the marked data packet update their tables. The simulation result shows that IPODV produces more robust routes than in AODV. The experiments in a small testbed also show that IPODV sends fewer hello packets and route error packets while transmitting more data packets than AODV.

The work in [67] proposes geographic routing protocols from WSNs as the routing protocol for PLC networks due to the fact that the network nodes in PLC network are static and their location is known a priori. Beacon-less Routing (BLR) [68], Beacon Based Routing (BBR) [69], and Implicit Geographic Forwarding (IGF) [70] are examined. The Greedy Perimeter Stateless Routing (GPSR) [71] recovery strategy is adopted in those geographic routing protocols when a route is broken. Two routing algorithms Shortest Path Routing (SPR) and sim-

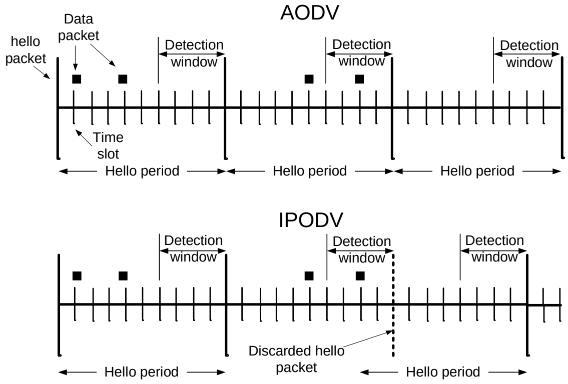

Figure 17: Comparison of hello message mechanism in AODV and IPODV, recreated from [65]

ple flooding mechanisms are used as the benchmark. SPR is assumed to have the knowledge about the node connections that have a quality link metric exceeding the minimum requirement and selects the best path between two nodes by minimizing a cost function. Two different baseline SPRs, namely SPR1 and SPR2, are defined based on two cost functions. In SPR1, the cost function is the delay in terms of the number of hops whereas in SPR2 the cost function is the total energy required to deliver the packet. In a simple flooding, every node which overhears a message also retransmits it if this message is not intended to it. The initial results for a certain distribution network topology have shown that geographic protocols are suitable for energy and delay efficient transport of unicast messages. Their performances are close to the SPR1 benchmark. When some nodes are switched off and lead to broken routes, GPSR keeps packet loss rate low. In addition, SPR2 showed lower energy consumption than SPR1 at the expense of an increased delay. Simple flooding is able to find the shortest route and hence provides the lowest delay at the expense of higher energy consumption.

7.2.2. Routing Protocols Specifically Designed for PLC

Powerline Multi-path Routing (PMR) [54] is an on-demand source routing protocol that builds multiple routes of maximally disjoint routes through request/reply cycle and is specifically designed for Narrowband PLC. PMR performs broadcasting control to reduce the broadcasting overhead. When the master node needs a route to a slave node and there is no available route information, the master node floods the RREQ message to the entire network. This RREQ messages reach the destination slave through different routes. The destination node picks up multiple disjoint routes from the arrived RREQ packets and sends RREP packets back to the source node via the chosen path. A user-defined positive integer **k** and an average-hops value are used for broadcasting control. The average-hops value is the topological distance from Master node to a given node. This distance is almost constant. An intermediate node forwards duplicate RREQ packets whose incoming node is different from the first received RREQ packet if the hop count in the duplicate RREQ packets are not greater than the hop count of the first received RREQ packet plus average-hops/**k**. Otherwise, the duplicate RREQ packets are dropped. Fig. 18 shows an example of forwarding decisions of node **a** and node **b**. For k=4, node **a** forwards the received RREQ packet from node **c** and node **d**. The first received RREQ packet in node **a** is from node **c** and since the hop count of the received RREQ packet from node **d** is not greater than 5, node **a** forwards this packet. Node **b** also forwards these two packets further, while the received RREQ packet from node **e** is dropped.

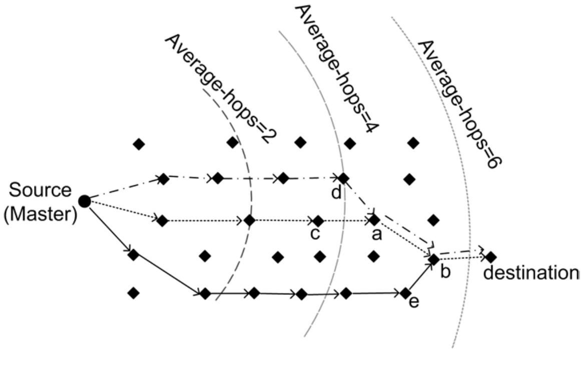

Figure 18: Forwarding decision in PMR.

PMR also uses extra back-off time for the first received RREQ packet and random packet forwarding mechanism to provide fairness in routing discovery. Broadcasting conflict occurs when an RREQ packet which takes the fastest path occupies too many network resources and prevents other RREQ packet to reach their destinations. Therefore, an intermediate node that first receives an RREQ packet will wait until the random back-off time expires before re-broadcasting the RREQ packet. In this way, other RREQ packet that propagates later than the fastest RREQ will have a chance to reach the destination. Instead of first-in-first out strategy, the selection of packet for re-broadcasting from the queue buffer is performed at random. A newly received RREQ packet is discarded when the buffer length is exceeded the pre-defined buffer limit or when it has high similarity with any RREQ packet in the packet buffer. The performance comparison with Split Multipath Routing (SMR) [72] through simulation in a large-scale environment with 1024 nodes shows that PMR has greater success ratio of finding disjoint routes and less average overhead than SMR.

7.3. Secure Routing for Wireless NANs

As previously mentioned, security should cover all aspects of SG including routing protocols and the data passing through the network. While there are some papers that discuss the data security and privacy for SG as discussed in [48] [49], there is no specific work on routing security for the SG. However, since most of the proposed routing protocols for NANs are based on WMN, there are many work for security in WMN that may be suitable for SG with some adaptations. Hence in this subsection, we will look at these two categories separately.

Table 4: Attack on routing, summarized from [77].

Routing Phase	*Security Attack*
Route Discovery	Routing table overflow attack, Routing cache positioning attack, Flooding (PREQ, HELLO, acknowledgment), Routing loop, Routing message modification
Route Maintenance	broadcasting false control message (e.g., link-broken error message)
Advanced/ sophisticated attacks	Wormhole attack, Blackhole/sinkhole attack, Byzantine attack, Rushing attack, Resource Consumption attack, PHEV location disclosure attack

7.3.1. Security for WMNs

Security for WMNs has been an active research area in recent years. Due to inherent security problems of wireless environments that are prone to passive and active attacks, ensuring security in WMNs is crucial for the realization of many WMN-based applications including SG. Security threats for WMNs are present at each level of the protocol stack.A more comprehensive discussion about securing WMNs can be found in [73] [74] [75] [76].

In this section, we focus our discussion on security threats on routing that may occur at the network and data link layers. Link layer is also considered since a lot of routing protocols follow a cross-layer approach where link layer information is utilized for routing decisions. Since WMN routing strategies follow two major steps of *Route Discovery* and *Route Maintenance*, similar attacks on MANET/WSN routing can also occur at different phases of WMN routing as summarized in Table 4 and these may come from internal or external attackers. Since most of the proposed routing protocols for NANs discussed in the paper are based on HWMP of IEEE 802.11s standard, we specifically discuss the security attacks and secure routing under HWMP [50] [51]. We also discuss differentiated security approach [52] that in our view is suitable for the SG.

IEEE 802.11s does not specify security in routing and hence HWMP is vulnerable to routing attacks such as PREQ flooding, route redirection and routing loop formation [50]. PREQ flooding is a Denial-of-Service (DoS) attack that makes every intermediate node keep forwarding the PREQ message since it is destined to an address that does not exist in the network. In a short time, the bandwidth becomes saturated. The other two attacks are performed by modifying the mutable fields of the control packet. Basically, HWMP has mutable and non-mutable fields in the control packet. Non-mutable fields remain unchanged while mutable fields (i.e., hop count, TTL and metric) are modified at each hop by the intermediate nodes before forwarding control packet to the next hop. Route re-direction happens when the malicious node divert traffic to itself by either advertising a route to a destination that has a greater Destination Sequence Number than the original destination or modifying the metric field of PREQ message to zero to announce a better path to a destination. Routing loop formation is also performed by modifying the metric field and spoofing MAC addresses.

In [50], a Secure Hybrid Wireless Mesh Protocol (SHWMP) is used to tackle these attacks. The approach assumes the availability of keys via IEEE 802.11s Mesh Security Architecture and utilizes IEEE 802.1X for initial authentication. SHWMP provides hop-by-hop authentication on the mutable fields using a Merkle tree. This is a binary tree which concatenates the hash values of mutable elements in a hierarchical manner. Eventually at the root, one hash-value is obtained for all the mutable fields. Non-mutable fields of the routing packet are protected using symmetric encryption. Simulation results show that compared to HWMP, SHWMP provides higher PDR and incurs little computational and storage overhead. Through analysis, SHWMP is shown to be robust against flooding, routing loops and routing message modification attacks. Since 802.11s has not been approved yet, depending on the key generation mechanisms of Mesh Security Architecture is a strong assumption in this work. Moreover, there has been some claims on the collision resistance of Merkle trees in the past [51].

As another approach, Identity Based Cryptography (IBC) is used to authenticate HWMP control messages, i.e. route request (PREQ) and route reply (PREP) messages by creating digital signature of the mutable fields [51]. In IBC, given an identity of a node, public and private keys are generated using a hash function. Before sending control messages, the digital signature of the mutable fields is calculated using the private key. This signature is included in the control packet. When a node receives a control message, it verifies the digital signature using the transmitter's public key. If it is not correct, the packet is dropped. Simulation results show that compared to HWMP, the digital signature does not affect the end-to-end delay. Furthermore, the additional overhead does not increase significantly. However, this approach only addresses the attacks from external nodes.

Obviously, even if these approaches make HWMP secure to use in real-life, the question of how to deploy it in a large-scale NAN is yet to be addressed. In particular, the key management issues with respect to their locations and how different portions of the SG Network communicates with different keys are the main issues that need to be dealt with in a typical AMI application. The routing performance in terms of delay, bandwidth, etc. should also be assessed under a variety of key sizes and security approaches.

Meanwhile, Gamer et al. [52] proposed differentiated security in which data and routing traffic are separated into different traffic classes based on the traffic's protection requirement. This approach is similar to Virtual LAN (VLAN) approach. Every node that participates in the mesh network is assigned to at least one protection level called Type of Protection (ToP). This ToP represents the ability of the node to forward and read the frame contents of certain traffic within the same protection level. Each TOP has a group key to secure data and routing traffic as well as multicast and broadcast messages. To get ToPs and the associated group keys, each node must communicate with an authentication server. In this way, only eligible nodes may take part in the mesh network to prevent external malicious nodes to join the network. However, this approach only prevents attacks from the internal malicious nodes from different protection levels since they do not have the TOP group key and does not eliminate attacks from the internal malicious nodes within the same protection level. And again, the issue of deployment on SG, especially with respect to authentication server, multicast groups etc., raises challenges about the applicability of the approach.

7.3.2. Secure Data Aggregation

Within the AMI network, the data size is expected to be fairly large as a result of the large-scale monitoring, sensing and measurement. In order to reduce the communications burden, aggregating the data is one possible solution. At an intermediate node, the received packets from its leaf nodes are aggregated prior to forwarding the aggregated packets to its parent node. Two different secure data aggregation approaches were proposed for AMI multihop networks as shown in Table 5. These are based on the application of the aggregation function. The aggregation can be done either by applying a function such as sum, count, average, etc. to the received data or by concatenating multiple packets under the same header.

Using the first approach, Li et al. [48] proposed an end-to-end encryption based on Paillier cryptosystem [78] to secure the information aggregation. At the intermediate node and the sink node, the aggregation operation is performed by multiplication of all incoming encrypted packets. After the aggregation operation, the sink node decrypts the aggregation result to obtain the final result. Hence, the end-to-end confidentiality of the information is maintained.

The second approach, Bartoli et al. [49], proposed both end-to-end and hop-by-hop security protection for the information aggregation using two different symmetric keys: a shared key between the smart meter and the gateway and pairwise keys between every node and its one-hop neighbors. At the aggregator node, the aggregation operation is performed by first eliminating unnecessary overhead from each packet and then concatenating those packets into a single packet. To secure the packet, AES block cipher was used for end-to-end security and hop-by-hop security. Performance evaluations of the proposed routing in a variety of lossy channels showed that a high number of packet losses occurred only in very noisy channels. Furthermore, the lossless aggregation reduces unnecessary overhead transmission (headers and Message Integrity Code (MICs)) by concatenating several packets into a single packet, and thus maximizes the link usage and minimizes the network traffic and saves energy. In a multihop network, the energy savings increase along with the increased number of hops.

7.4. QoS Routing

There is not much work on QoS routing in the SG. However, given that NANs may use a WMN based architecture, some of the prior QoS works in WMNs may apply with some adaptations. We first provide an overview of these approaches and then focus on specific QoS for the SG.

7.4.1. QoS Routing in WMNs

QoS provisioning in WMN has started to receive attention from the research community recently and initially some work has been done with single-channel assumption [79, 80]. Basic QoS extensions to 802.11 have also been developed under 802.11e by means of Hybrid Controlled Channel Access and EDCA (Enhanced Distributed Channel Access), but only aimed at the MAC layer. A framework to provide IEEE 802.11e-based parameterized QoS in terms of admission control algorithms and scheduling algorithms is presented in [81]. A distributed bandwidth-constrained routing is proposed in [82] considering intra-flow interferences.

There are also some works with the assumption of a TDMA-based MAC layer to provide bandwidth guarantees [83]. The work [84] considered service differentiation and packet aggregation in WMNs to provide statistical QoS guarantees for VoIP applications. They define four different data classes and perform packet aggregation at each node to minimize the packet handling overhead. The work in [85] studies the performance of multimedia traffic in WMNs. The mesh-based testbed is used to transmit video and voice data with different network configurations and network cards. MPLS-based [86] cross-layer routing framework is presented in [87] to enable a good application delivery. A good survey of QoS extensions to IEEE 802.11-compliant networks at the MAC layer is reported in [88].

7.4.2. QoS Routing in Wireless NANs

As far as the SG applications are concerned, the protocol proposed in [53] is one of the few approaches to multi-constrained QoS routing in wireless NANs. The proposed protocol, namely Optimized Multi-Constrained Routing (OMCR), is a simple greedy algorithm that can be implemented in a distributed manner based on two QoS requirements: delay and outage probability. The authors assume that a home appliance can communicate with the control center by sending a QoS requirement and then the control center assigns one or more routes for the home appliance to guarantee the QoS requirement. The performance comparison with an approximation algorithm called Fully Polynomial Time Approximation Scheme (FPTAS) using path-length metric showed that both have similar performance in terms of path-length while the running time of OMCR is shorter and it is more scalable than FPTAS. The network size does not have significant impact on the running time of OMCR.

Another QoS routing approach is part of the IEEE 802.11s standard. Since SG provides services to various applications that may vary in packet size, EDCA mechanism of IEEE 802.11s supports SG to differentiate data traffic by priority and provide QoS for time-critical data [47]. EDCA is originally defined in IEEE 802.11e standard [89]. It is a contention based distributed medium access mechanism that provides prioritized QoS support by delivering traffic based on their priorities. It has four different priority categories (highest priority first) : voice, video, best effort, and background. Each priority class has its own queue for data transmission.

Since EDCA only provides service differentiation and not QoS guarantees, the work in [90] extends EDCA with distributed resource reservation (EDCA/RR) to provide QoS guar-

Table 5: Secure Routing Comparison.

Characteristics	*Li et al. [48]*	*Bartoli et al. [49]*
Type of secure aggregation	End-to-End Security	End-to-End and Hop-by-Hop Security
Type of Aggregation	Encrypted Data Aggregation	Encrypted Data Aggregation
Aggregation function	additive homomorphic encryption	concatenation
Final result	single aggregate value	multiple original values from source
Crypto System	Paillier	AES CCM 128 bit for end-to-end, AES-CBC-MAC 128 bit for hop-by-hop
Security requirement covered :		
- Confidentiality	Yes	Yes
- Integrity	No	Yes
- Authentication	No	Yes
- Data freshness	Yes	Yes

antees and proposes to combine it with HWMP. EDCR/RR operates like EDCA for the first two low-priority classes and offers resource reservation for high-priority classes. The idea is that instead of two separate processes (i.e., route discovery and then resource reservation), both processes are combined into a route and reservation request (RRQ). In this way, route discovery will be performed with less message overhead and shorter delays compared to EDCA. The receiving node is only allowed to reply if it supports the requested QoS requirements.

The work in [91] proposes another enhancement to HWMP, specifically in the reactive phase of HWMP. This improvement makes the on-demand routing of HWMP a QoS-aware routing protocol. To find a path between source and destination that satisfies the end-to-end delay requirement, the route discovery and route maintenance are modified. PREQ message has some additional fields that are used to store some QoS information such as the delay constraint. When a node receives PREQ message and the PREQ message contains QoS information, the node compares its one-hop delay with the delay constraint stored in the message. If its one-hop delay is greater, then PREQ message is dropped. The simulation results show that the proposed solution increases the performance of HWMP by reducing the end-to-end delay at the expense of insignificant additional overhead.

8. Routing Protocols for WANs

The WAN is the network which consists of different components such as core network or backhaul network to support SG applications. In most cases, the used technology is wired/optical and routing is handled by means of a public network such as the Internet or private lines [92]. This is especially true for the core network where Fiber optics, IP/Multi-Protocol Label Switching (MPLS) and Metro Ethernet are employed [93]. The issues regarding routing in these networks are not within the scope of this paper as they do not arise as a result of employing SG applications. For instance, the issues of security, QoS, reliability, etc. that are specific to SG applications have long been studied within the Internet [94][95].

In case of wireless infrastructure (i.e., wireless WAN), most of the time routing is not an issue since the data can be transmitted in one hop to the destination (e.g., WiMAX, 4G, GPRS). The issues in these wireless technologies are mostly related to physical layer, channels, radio, handoff, etc. [96]. As a result, it can be concluded that the technology in WANs utilizes the existing IP protocols and thus there are no new routing challenges raised as a result of deploying SG applications.

The only case where routing can come into picture is in the deployment of a multi-hop wireless WAN which can be a proprietary/private network belonging to a particular company. Specifically, the company can deploy mesh routers or towers in all of its substations to create a mesh among these substations and some gateways situated at several residence locations to collect metering data [97]. In such a case, multi-hopping among base-stations as well as mesh routers can introduce some routing challenges which are similar to the challenges in NANs that were discussed in the previous section.

9. Future Research Directions

Given the routing design issues and the state of the current routing research, several requirements of SG routing are yet to be addressed, especially with the increasing number of applications envisioned for SG. In this section, we provide a list of open issues to be studied in the future as part of SG routing challenges that may be related to any of the HANs, NANs or WANs.

9.1. QoS Architecture

The SG communications network shares all types of information generated by end-point devices which have diverse end-to-end latency requirements. This indicates the need for a comprehensive QoS architecture as in the case of Internet's Differentiated Services (DiffServ) [98] or Integrated Services (IntServ) [94]. Different types of time-critical data may be prioritized differently based on the applications. Therefore, application and flow-based prioritization can better fit to the requirements of SG just like IntServ. For this purpose, it will not be enough to propose QoS routing approaches at the HAN, NAN, or WAN side. A comprehensive QoS understanding of gateways at different network components may be needed. The implementation of message prioritization should be done based on the number of priority levels, resource allocation at each level, priority mapping to each communications class, priority transition between different networks, admission control criteria when there is a congestion in the network, and dynamic control adjustments.

9.2. Secure Routing

As far as the security is concerned, the previously discussed routing protocols deal with two different data requirements of the SG: SG is expected to have an aggregate data for statistical analysis for operation management and individual power consumption for billing purposes. The former raises concerns regarding privacy and thus requires different efforts in addition to securing the routing. The latter, however, is an issue that needs to be addressed along with routing. While the existing secure routing approaches for MANETs and WSNs could be employed in most of the applications, the problem of interoperability among different network components and the diversity of attacks that can be started on these networks make it challenging to have a comprehensive secure routing approach. In addition, depending on the applications, the security goals will differ making it a more complex issue. Adaptation of the existing approaches to the SG based on its needs and requirements is a future challenge. One of the major parts of the adaptation effort should address the issue of key management whether it be a symmetric or asymmetric key cryptographic approach. Key management may re-shape the design of some of the routing protocols to realize their applicability.

9.3. Secure and QoS-aware Routing

Given the security and QoS requirements above, an interesting future direction would be to provide both in a wireless environment. Traditionally, in wired networks this may not be a top concern since there will be enough resources. However, in wireless networks such as WMN, WSN or WPAN, providing security might hurt some of the QoS. For instance, some of the metrics such as reliability and delay should be guaranteed under security protection. This puts additional burden on the network and requires approaches with less overhead in terms of both security and QoS. In addition, new studies which will evaluate the current performance of QoS routing along with security approaches are needed. Among the other metrics that need to be included in assessment is the mobility handling when mobile workforce is involved as clients of the NANs. This even creates a more challenging problem in the intersection of security, QoS and mobility which has not been studied before.

9.4. Hybrid Routing using PLC and Wireless Communication

Hybrid routing refers to routing in hybrid SG communications networks where both PLC and wireless communications are utilized. Such routing may provide some benefits in terms of path diversity and energy consumption (if this is an issue). However, the design of these types of routing protocols is challenging due to different characteristics of PLC and wireless communications. In addition, standardization is needed to guarantee the interoperability among different network components. Current approaches target HANs and typically adapt existing routing protocols from wireless networks. It is an important challenge to design similar protocols for NANs where the network includes medium voltage powerline (i.e., more interference will be there).

9.5. Cross Layer Routing via Multi-channels and MIMO

Even though a hybrid SG communications architecture that utilizes different communications technologies provide some benefits, the performance in terms of bandwidth, packet loss, delay and interference is still below the expectations and hence there is a need for the development of novel communications protocols for improved performance. To tackle the harsh environmental conditions and limit radio interferences, advanced physical layer/radio technologies such as Multiple Input Multiple Output (MIMO), multiple radio interfaces and smart antennas should be exploited while developing cross-layer routing protocols. In particular, multi-radio multi-channel WMNs have a lot of potential to be used in SG NANs. However, the assignment of channels and use of radios dynamically based on the traffic requirements need to be tackled. This raises the problem of cross-layer QoS routing support under a dynamic channel assignment and security protection which has not been studied before.

9.6. Scalable Routing

Given that the current state of the art routing protocols for MANETs or WMNs only work on networks with smaller network diameters (i.e., the number of hops is limited), the applicability of these approaches to large-scale NANs may not be possible. In particular, the performance of multi-hop routing degrades significantly as reported in [99]. This indicates the need for scalable routing approaches which can maintain the performance throughout the network. The major focus for this purpose will be the routing metrics used. The metrics that reveals link layer or physical layer information are highly desirable. In fact, there has been a lot of research on WMN routing metrics [100] but these have not specifically focused on the needs of SG applications. For instance, how these metrics will behave under QoS requirements of NANs is yet to be explored.

9.7. Simulation Tools and Testbeds for Routing

The design of new routing protocols also raise the issue of testing for SG networks which is not an easy task. Current routing research heavily relies on simulators which may fail to capture the characteristics of wireless environments [57]. While there has been a big interest on the testbeds for implementing WMN routing, the tests so far remain in building setups with smaller networks. On the other hand, SG network environments will be different and introduce interference especially from the devices which are part of the SG. Considering the large-scale NANs, deployment of testbeds for SG requires significant academia-industry cooperation and investment. Nonetheless, in the mean time, researchers will need simulation tools or remotely accessible testbeds where they can test the performance of routing protocols. This indicates a need for special network simulators/emulators which can imitate the characteristics of SG environments and provide easy access to researchers. In particular, virtualization can be exploited in conjunction with these simulators for more realistic tests. There are some initial efforts (e.g., SG Communications Assessment Tool (SG-CAT) [101], TCIPG testbed from the University of Illinois [102]) but more efforts are needed for quality simulators as well as testbeds. Such availability will significantly enhance the routing research in the SG.

9.8. Standardization and Interoperability in Routing

Although there are some standardization efforts within HAN in terms of the use of ZigBee, for NANs there is no similar common standard. The use of 802.11s standard for NAN routing can be an example of the standardization efforts but due to availability of several communications options, several standards will be needed. The other issue related to standardization is the interoperability of the networks as they may be using different routing protocols. While this is addressed with the deployment of gateways, using the same standard could be advantageous in terms of deployment convenience and flexibility. For instance, 6LowPAN is based on IPv6 which can also be employed in a NAN and thus HAN and NAN will be interoperable in terms of communications. In addition, when dealing with fault-tolerance, different utilities may need to communicate with each other in order to prevent the spread of the blackouts. In such cases, if the used routing protocols are different and the Smart Grid devices which sit at different utility networks cannot communicate with each other, power restoration can be delayed. As a result, the use of standards will force routing research to comply with the standard requirements and consider meeting those standards rather than coming up with new designs from scratch.

9.9. Multicast Routing

The use of multicast in SG applications is expected to be a common need in the future given that DR applications may deal with a group of residents in a neighborhood. The multicast message may also be subject to some QoS requirements. Therefore, there will be a need for multicast routing in NANs. Currently, there is no work dealing with multicast routing in SG applications. HAN applications can also use multicast to communicate with a set of devices at home. Therefore, routing protocols for HANs/NANs should be adapted to support multicasting in SG applications.

10. Conclusion

There is an increasing interest towards the development of routing protocols to satisfy the requirements of the SG applications. However, the development of routing protocols for SG is still in its infancy given that there are a lot of challenges yet to be addressed. In this paper, we have summarized and classified these routing protocols under three SG network components, namely HANs, NANs and WANs. For the former two, we have presented a routing classification by using the underlying communications medium and several key metrics such as reliability, security and QoS. We have also identified pros and cons of these protocols to point out the need for further research. In addition, we have described and discussed several major routing-related issues, such as QoS, security, testing and multicasting that need to be addressed in the future routing protocols.

References

[1] N. I. of Standards, T. (NIST), NIST framework and roadmap for smart grid interoperability standards, Release 1.0, 2010.

[2] T. N. E. T. L. (NETL), Understanding the benefits of smart grid (2010).

[3] W. Wang, Y. Xu, M. Khanna, Survey paper: A survey on the communication architectures in smart grid, Comput. Netw. 55 (2011) 3604–3629.

[4] X. Fang, S. Misra, G. Xue, D. Yang, Smart grid - the new and improved power grid: A survey, Communications Surveys Tutorials, IEEE (2011).

[5] R. H. Katz, D. E. Culler, S. Sanders, S. Alspaugh, Y. Chen, S. Dawson-Haggerty, P. Dutta, M. He, X. Jiang, L. Keys, A. Krioukov, K. Lutz, J. Ortiz, P. Mohan, E. Reutzel, J. Taneja, J. Hsu, S. Shankar, An information-centric energy infrastructure: The berkeley view, Sustainable Computing: Informatics and Systems 1 (2011) 7 – 22.

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

[7] J. Gao, Y. Xiao, J. Liu, W. Liang, C. P. Chen, A survey of communication/networking in smart grids, Future Gener. Comput. Syst. 28 (2012) 391–404.

[8] Z. Fan, P. Kulkarni, S. Gormus, C. Efthymiou, G. Kalogridis, M. Sooriyabandara, Z. Zhu, S. Lambotharan, W. Chin, Smart grid communications: Overview of research challenges, solutions, and standardization activities, Communications Surveys Tutorials, IEEE PP (2012) 1 –18.

[9] C. Hauser, D. Bakken, A. Bose, A failure to communicate: next generation communication requirements, technologies, and architecture for the electric power grid, Power and Energy Magazine, IEEE 3 (2005) 47 – 55.

[10] A. Ghassemi, S. Bavarian, L. Lampe, Cognitive radio for smart grid communications, in: Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, pp. 297 –302.

[11] V. Aravinthan, V. Namboodiri, S. Sunku, W. Jewell, Wireless ami application and security for controlled home area networks, in: Power and Energy Society General Meeting, 2011 IEEE, pp. 1 –8.

[12] B. Lichtensteiger, B. Bjelajac, C. Mu andller, C. Wietfeld, Rf mesh systems for smart metering: System architecture and performance, in: Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, pp. 379 –384.

[13] D. of Energy, Communications requirements of smart grid technologies, 2010.

[14] W. Su, H. Rahimi Eichi, W. Zeng, M. Chow, A survey on the electrification of transportation in a smart grid environment, Industrial Informatics, IEEE Transactions on PP (2011) 1.

[15] C. Muller, S. Subik, A. Wolff, C. Wietfeld, A system design framework for scalability analysis of geographic routing algorithms in large-scale mesh networks, in: Proceedings of the 3rd International ICST Conference on Simulation Tools and Techniques, SIMUTools '10, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), ICST, Brussels, Belgium, Belgium, 2010, pp. 23:1–23:7.

[16] L. Badia, M. Miozzo, M. Rossi, M. Zorzi, Routing schemes in heterogeneous wireless networks based on access advertisement and backward utilities for qos support [quality of service based routing algorithms for heterogeneous networks], Communications Magazine, IEEE 45 (2007) 67 –73.

[17] D. Dzung, I. Berganza, A. Sendin, Evolution of powerline communications for smart distribution: From ripple control to ofdm, in: Power Line Communications and Its Applications (ISPLC), 2011 IEEE International Symposium on, pp. 474 –478.

[18] J. Heo, K. Lee, H. K. Kang, D.-S. Kim, W. H. Kwon, Adaptive channel state routing for home network systems using power line communications, Consumer Electronics, IEEE Transactions on 53 (2007) 1410 –1418.

[19] C. Jin, T. Kunz, Smart home networking: Combining wireless and powerline networking, in: Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International, pp. 1276 –1281.

[20] L. Ben Saad, C. Chauvenet, B. Tourancheau, Heterogeneous IPv6 Infrastructure for Smart Energy Efficient Building, in: SDEWES, Dubrovnik, Croatie.

[21] R. Benato, R. Caldon, Application of plc for the control and the protection of future distribution networks, in: Power Line Communications and Its Applications, 2007. ISPLC '07. IEEE International Symposium on, pp. 499 –504.

[22] S. Galli, A. Scaglione, Z. Wang, Power line communications and the smart grid, in: Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, pp. 303 –308.

[23] G. Bumiller, H. Hrasnica, L. Lampe, M. Lobashov, T. Stockhammer, Protocols for PLC Systems, John Wiley & Sons, Ltd, pp. 311–362.

[24] B. Akyol, H. Kirkham, S. Clements, M. Hadley, A survey of wireless communications for the electric power system, Prepared for the U.S. Department of Energy, 2010.

[25] V. C. Gungor, F. C. Lambert, A survey on communication networks for electric system automation, Comput. Netw. 50 (2006) 877–897.

[26] R. G. Garroppo, S. Giordano, L. Tavanti, Implementation frameworks for ieee 802.11s systems, Computer Communications 33 (2010) 336 – 349.

[27] G. Mikhail, Catching the z-wave, Electronic Engineering Times India (2006) 1–5.

[28] P. Darbee, Insteon:the details (2005).

[29] P. Darbee, Insteon:compared, White Paper (2006).

[30] Wavenis technology, http://www.coronis.com (last accessed : Feb 28, 2012).

[31] D.-M. Han, J.-H. Lim, Smart home energy management system using ieee 802.15.4 and zigbee, Consumer Electronics, IEEE Transactions on 56 (2010) 1403 –1410.

[32] P. Yi, A. Iwayemi, C. Zhou, Building automation networks for smart grids, in: International Journal of Digital Multimedia Broadcasting, volume 2011.

[33] S. Petersen, S. Carlsen, Wirelesshart versus isa100.11a: The format war hits the factory floor, Industrial Electronics Magazine, IEEE 5 (2011) 23 –34.

[34] T. Lennvall, S. Svensson, F. Hekland, A comparison of wirelesshart and zigbee for industrial applications, in: Factory Communication Systems, 2008. WFCS 2008. IEEE International Workshop on, pp. 85 –88.

[35] C. Alcaraz, J. Lopez, A security analysis for wireless sensor mesh networks in highly critical systems, Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on 40 (2010) 419 –428.

[36] P. Baronti, P. Pillai, V. W. C. Chook, S. Chessa, A. Gotta, Y. F. Hu, Wireless sensor networks: A survey on the state of the art and the 802.15.4 and zigbee standards, Comput. Commun. 30 (2007) 1655–1695.

[37] C. Perkins, E. Royer, Rfc 3561 - ad hoc on-demand distance vector (aodv) routing, 2003.

[38] T. Winter, P. Thubert, A. Brandt, T. Clausen, J. Hui, R. Kelsey, P. Levis, K. Pister, K. Struik, J. Vasseur, Rpl: Ipv6 routing protocol for low power and lossy networks, 2011.

[39] J. Song, S. Han, A. Mok, D. Chen, M. Lucas, M. Nixon, Wirelesshart: Applying wireless technology in real-time industrial process control, in: Real-Time and Embedded Technology and Applications Symposium, 2008. RTAS '08. IEEE, pp. 377 –386.

[40] D. Yang, Y. Xu, M. Gidlund, Coexistence of ieee802.15.4 based networks: A survey, in: IECON 2010 - 36th Annual Conference on IEEE Industrial Electronics Society, pp. 2107 –2113.

[41] Z. Jindong, L. Zhenjun, Z. Yaopei, Elhfr: A graph routing in industrial wireless mesh network, in: Information and Automation, 2009. ICIA '09. International Conference on, pp. 106 –110.

[42] C. E. Perkins, P. Bhagwat, Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers, in: Proceedings of the conference on Communications architectures, protocols and applications, SIGCOMM '94, ACM, New York, NY, USA, 1994, pp. 234–244.

[43] T. Iwao, K. Yamada, M. Yura, Y. Nakaya, A. Cardenas, S. Lee, R. Masuoka, Dynamic data forwarding in wireless mesh networks, in: Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, pp. 385 –390.

[44] S. Dawson-Haggerty, A. Tavakoli, D. Culler, Hydro: A hybrid routing protocol for low-power and lossy networks, in: Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, pp. 268 –273.

[45] D. Wang, Z. Tao, J. Zhang, A. Abouzeid, RPL based routing for advanced metering infrastructure in smart grid, in: Communications Workshops (ICC), 2010 IEEE International Conference on, pp. 1 –6.

[46] H. Gharavi, B. Hu, Multigate communication network for smart grid, Proceedings of the IEEE 99 (2011) 1028 –1045.

[47] J.-S. Jung, K.-W. Lim, J.-B. Kim, Y.-B. Ko, Y. Kim, S.-Y. Lee, Improving ieee 802.11s wireless mesh networks for reliable routing in the smart grid infrastructure, in: Communications Workshops (ICC), 2011 IEEE International Conference on, pp. 1 –5.

[48] F. Li, B. Luo, P. Liu, Secure information aggregation for smart grids using homomorphic encryption, in: Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, pp. 327 – 332.

[49] A. Bartoli, J. Hernandez-Serrano, M. Soriano, M. Dohler, A. Kountouris, D. Barthel, Secure lossless aggregation for smart grid m2m networks, in: Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, pp. 333 –338.

[50] M. S. Islam, Y. J. Yoon, M. A. Hamid, C. S. Hong, A secure hybrid wireless mesh protocol for 802.11s mesh network, in: Proceeding sof the international conference on Computational Science and Its Applications, Part I, ICCSA '08, Springer-Verlag, Berlin, Heidelberg, 2008, pp. 972– 985.

[51] J. Ben-Othman, Y. Benitez, On securing hwmp using ibc, in: Communications (ICC), 2011 IEEE International Conference on, pp. 1 –5.

[52] T. Gamer, L. Vlker, M. Zitterbart, Differentiated security in wireless mesh networks, Security and Communication Networks 4 (2011) 257– 266.

[53] H. Li, W. Zhang, QoS routing in smart grid, in: GLOBECOM 2010, 2010 IEEE Global Telecommunications Conference, pp. 1 –6.

[54] S. Liang, S. Chen, X. Ding, C. Zhang, Y. Xu, A broadcasting algorithm of multipath routing in narrowband power line communication networks, in: Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on, pp. 467 –471.

[55] T. Clausen, P. Jacquet, Rfc 3626 - optimized link state routing protocol (olsr), 2003.

[56] G. Hiertz, S. Max, R. Zhao, D. Denteneer, L. Berlemann, Principles of ieee 802.11s, in: Computer Communications and Networks, 2007. ICCCN 2007. Proceedings of 16th International Conference on, pp. 1002 –1007.

[57] S. Uludag, T. Imboden, K. Akkaya, A taxonomy and evaluation for developing 802.11-based wireless mesh network testbeds, Wiley International Journal of Communication Systems (2011).

[58] H. Gharavi, B. Hu, Multigate mesh routing for smart grid last mile communications, in: Wireless Communications and Networking Conference (WCNC), 2011 IEEE, pp. 275 –280.

[59] M. Dohler, T. Watteyne, T. Winter, T. Barthel, Rfc 5548 - routing requirements for urban low-power and lossy networks, 2009.

[60] A. Brandt, J. Buron, G. Porcu, Rfc 5826 - home automation routing requirements in low-power and lossy networks, 2010.

[61] J. Martocci, P. De Mil, N. Riou, W. Vermeylen, Rfc 5867 - building automation routing requirements in low-power and lossy networks, 2010.

[62] K. Pister, P. Thubert, S. Dwars, T. Phinney, Rfc 5673 - industrial routing requirements in low-power and lossy networks, 2009.

[63] J. Tripathi, J. de Oliveira, J. Vasseur, Applicability study of RPL with local repair in smart grid substation networks, in: Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, pp. 262 –267.

[64] N. Pavlidou, A. Han Vinck, J. Yazdani, B. Honary, Power line communications: state of the art and future trends, Communications Magazine, IEEE 41 (2003) 34 – 40.

[65] W. Gao, W. Jin, H. Li, An improved routing protocol for power-line network based on aodv, in: Communications and Information Technologies (ISCIT), 2011 11th International Symposium on, pp. 233 –237.

[66] F. Pacheco, L. Pinho, E. Tovar, Queuing and routing in a hierarchical powerline communication system, in: Emerging Technologies and Factory Automation, 2005. ETFA 2005. 10th IEEE Conference on, volume 2, pp. 8 pp. –66.

[67] M. Biagi, L. Lampe, Location assisted routing techniques for power

line communication in smart grids, in: Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, pp. 274 –278.

[68] M. Heissenbuttel, BLR: beacon-less routing algorithm for mobile ad hoc networks, Computer Communications 27 (2004) 1076–1086.

[69] L. Demoracski, Fault-tolerant beacon vector routing for mobile ad hoc networks, in: Parallel and Distributed Processing Symposium, 2005. Proceedings. 19th IEEE International, p. 8 pp.

[70] T. He, S. Son, S. Son, J. Stankovic, IGF: A state-free robust communication protocol for wireless sensor networks, Tech rep CS200311 (2003).

[71] B. Karp, H. T. Kung, GPSR: greedy perimeter stateless routing for wireless networks, in: Proceedings of the 6th annual international conference on Mobile computing and networking, MobiCom '00, ACM, New York, NY, USA, 2000, pp. 243–254.

[72] S.-J. Lee, M. Gerla, Split multipath routing with maximally disjoint paths in ad hoc networks, in: Communications, 2001. ICC 2001. IEEE International Conference on, volume 10, pp. 3201 –3205 vol.10.

[73] S. Glass, M. Portmann, V. Muthukkumarasamy, Securing wireless mesh networks, Internet Computing, IEEE 12 (2008) 30 –36.

[74] N. Ben Salem, J.-P. Hubaux, Securing wireless mesh networks, Wireless Communications, IEEE 13 (2006) 50 –55.

[75] M. S. Siddiqui, C. S. v, Security issues in wireless mesh networks, in: Proceedings of the 2007 International Conference on Multimedia and Ubiquitous Engineering, MUE '07, IEEE Computer Society, Washington, DC, USA, 2007, pp. 717–722.

[76] P. Yi, T. Tong, N. Liu, Y. Wu, J. Ma, Security in wireless mesh networks: Challenges and solutions, in: Information Technology: New Generations, 2009. ITNG '09. Sixth International Conference on, pp. 423 –428.

[77] B. Wu, J. Chen, J. Wu, M. Cardei, A survey of attacks and countermeasures in mobile ad hoc networks, in: Y. Xiao, X. S. Shen, D.-Z. Du (Eds.), Wireless Network Security, Signals and Communication Technology, Springer US, 2007, pp. 103–135. 10.1007/978-0-387-33112-6-5.

[78] D. Catalano, R. Gennaro, N. Howgrave-Graham, P. Q. Nguyen, Paillier's cryptosystem revisited, in: Proceedings of the 8th ACM conference on Computer and Communications Security, CCS '01, ACM, New York, NY, USA, 2001, pp. 206–214.

[79] Q. Xue, A. Ganz, Qos routing for mesh-based wireless lans, International Journal of Wireless Information Networks 9 (2002) 179–190. 10.1023/A:1016085627790.

[80] H. Jiang, W. Zhuang, X. Shen, A. Abdrabou, P. Wang, Differentiated services for wireless mesh backbone, Communications Magazine, IEEE 44 (2006) 113 – 119.

[81] X. Chu, Provisioning of parameterized quality of service in 802.11e based wireless mesh networks, Mob. Netw. Appl. 13 (2008) 6–18.

[82] R. Hou, K.-S. Lui, H.-S. Chiu, K. L. Yeung, F. Baker, Routing in multihop wireless mesh networks with bandwidth guarantees, in: Proceedings of the tenth ACM international symposium on Mobile ad hoc networking and computing, MobiHoc '09, ACM, New York, NY, USA, 2009, pp. 353–354.

[83] M. Leoncini, P. Santi, P. Valente, An stdma-based framework for qos provisioning in wireless mesh networks, in: Mobile Ad Hoc and Sensor Systems, 2008. MASS 2008. 5th IEEE International Conference on, pp. 223 –232.

[84] R. Riggio, D. Miorandi, F. De Pellegrini, F. Granelli, I. Chlamtac, A traffic aggregation and differentiation scheme for enhanced qos in ieee 802.11-based wireless mesh networks, Comput. Commun. 31 (2008) 1290–1300.

[85] X. Cheng, P. Mohapatra, S.-J. Lee, S. Banerjee, Performance evaluation of video streaming in multihop wireless mesh networks, in: Proceedings of the 18th International Workshop on Network and Operating Systems Support for Digital Audio and Video, NOSSDAV '08, ACM, New York, NY, USA, 2008, pp. 57–62.

[86] E. Rosen, A. Viswanathan, R. Callon, Rfc 3031 - multiprotocol label switching architecture), 2001.

[87] L. Romdhani, C. Bonnet, Cross-layer qos routing framework for wireless mesh networks, in: Proceedings of the 2008 The Fourth International Conference on Wireless and Mobile Communications, IEEE Computer Society, Washington, DC, USA, 2008, pp. 382–388.

[88] H. Kim, J. C. Hou, C. Hu, Y. Ge, Qos provisioning in ieee 802.11-compliant networks: Past, present, and future, Comput. Netw. 51 (2007) 1922–1941.

[89] Ieee standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements 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 (Amendment to IEEE Std 802.11, 1999 Edition (Reaff 2003) (2005) 1 –189.

[90] A. Hamidian, U. Krner, Extending edca with distributed resource reservation for qos guarantees, Telecommunication Systems 39 (2008) 187–194.

[91] J. Ben-Othman, L. Mokdad, M. Cheikh, Q-hwmp: Improving end-to-end qos for 802.11s based mesh networks, in: Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE, pp. 1 –6.

[92] P. Regan, Wide area networks, Pearson/Prentice Hall, 2004.

[93] C. Lima, Communications aspects of the smart grid, in: IEEE SCV ComSoc Monthly Meeting Presentations.

[94] Z. Wang, Internet QoS: architectures and mechanisms for quality of service, Morgan Kaufmann series in networking, Morgan Kaufmann, 2001.

[95] S. Convery, Network security architectures, Networking technology series, Cisco Press, 2004.

[96] V. Garg, Wireless communications and networking, The Morgan Kaufmann series in networking, Elsevier Morgan Kaufmann, 2007.

[97] W. Paper, Wireless wan for the smart grid, Trilliant Inc. (2010).

[98] K. Kilkki, Differentiated Services for the Internet, Macmillan Publishing Co., Inc., Indianapolis, IN, USA, 1999.

[99] T. Imboden, K. Akkaya, Z. Moore, Performance evaluation of wireless mesh networks using ieee 802.11s and ieee 802.11n, in: Proceedings of IEEE Workshop on Convergence among Heterogeneous Wireless Systems in Future Internet in conjunction with International Conference on Communications'12.

[100] H. Liu, W. Huang, X. Zhou, X. Wang, A comprehensive comparison of routing metrics for wireless mesh networks, in: Networking, Sensing and Control, 2008. ICNSC 2008. IEEE International Conference on, pp. 955 –960.

[101] A. Patel, J. Aparicio, N. Tas, M. Loiacono, J. Rosca, Assessing communications technology options for smart grid applications, in: Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on, pp. 126 –131.

[102] tcipg, Trustworthy cyber infrastructure for the power grid, 2012.