Quality-of-Service Differentiation for Smart Grid Neighbor Area Networks

Gowdemy Rajalingham

Department of Electrical & Computer Engineering
McGill University
Montreal, Canada

July 2015

Abstract

The intelligence of the Smart Grid (SG) relies heavily on a reliable and secure SG Communications Network (SGCN). In this thesis, the focus is on the SG Neighbor Area Network (NAN), a crucial segment of the SGCN, whose communications pose significant challenges, i.e., harsh communication medium, network size, uplink converge-cast traffic, etc. Now, as all generated uplink traffic must pass through the sink, it presents significant challenges with respect to routing through communications bottlenecks, i.e., node overloading, congestion, interference, packet collisions, etc. Therefore, this thesis aims to tackle these challenges. Specifically, previous works have explored the suitability of the Routing Protocol for Low Power and Lossy Networks (RPL) in the SG context. However, they only considered a single representative traffic class and failed to provide any Quality-of-Service (QoS) differentiation. Further, existing QoS solutions are inadequate as (i) SG application traffic will likely be quite different from that generated by traditional data applications and (ii) QoS requirements in the SG NAN context depend not only on traffic class requirements but also the current grid state. In addition, the number, type and proportion of traffic classes will affect the complexity and efficiency of any devised QoS scheme.

With that in mind, this thesis fills the aforementioned gaps by considering QoS requirements for different traffic classes and proposing QoS enabling extensions within the RPL framework in an attempt to achieve the desired QoS differentiation for SG applications. Specifically, correlating RPL routing metrics with different SG application traffic classes in an attempt to incorporate QoS differentiation at the network layer. Further, as most existing QoS differentiation approaches are MAC-based, a cross-layered approach is designed so as to allow for prioritized channel accesses. Therefore, three variants of RPL are studied, single instance RPL, multi-instance RPL (RPL-M) as well as multi-instance RPL with prioritized channel backoffs (RPL-M+). Extensive simulations were carried out to demonstrate the performance, in terms of latency and throughput, of standard RPL, RPL-M and RPL-M+. In particular, both traffic distribution as well as total data rate are varied for two traffic profiles, for a large-scale random deployment scenario. In addition, a real-life deployment scenario, a microgrid, was also considered to showcase the performance, achievable QoS differentiation as well as the usability (transferability) of the obtained results in a more general context.

Résumé

Les réseaux de distribution d'électricité possèdent un caractère intelligent grâce à l'utilisation des technologies d'informatiques et de communications. Au sein de ce réseau, le réseau de voisinage est essentiel mais pose de nombreux défis. En particulier, puisque la liaison montante se fait en diffusion convergente, le routage est susceptible à l'interférence, à l'encombrement et aux goulots d'étranglement. Donc, l'objectif de cette thèse est d'aborder et de résoudre ces défis. Plus précisément, la validité du protocole de routage « Routing Protocol for Low Power and Lossy Networks (RPL) » a été vérifiée auparavant pour le réseau sans fil à voisinage. Cependant, seule une classe de trafic a été considérée et la qualité de service (QoS) n'a pas été envisagée. De plus, comme les classes de trafic associées aux réseaux intelligents sont (i) plus diverses que celles des applications courantes et (ii) varient suivant les changements d'états du réseau électrique, les solutions existantes de QoS ne s'appliquent plus.

En conséquence, cette thèse fait face aux lacunes ci-dessus en proposant des solutions pour acquérir la QoS requise par les applications du réseau intelligent, adaptées au RPL. Notamment, en reliant les métrologiques informatiques de RPL aux exigences de QoS de différentes applications et ainsi inclure une solution de QoS à la couche réseau. De plus, comme la plupart des solutions de QoS s'appliquent à la sous-couche de contrôle d'accès au médium, un deuxième module a été conçu pour altérer et rendre l'accès au médium prioritaire. Donc, trois protocoles de routage ont été étudiés : RPL, RPL-M permettant la QoS au niveau réseau et finalement RPL-M+ qui inclue la QoS au niveau réseau et au niveau du contrôle d'accès au médium. Finalement, pour évaluer (en tant que délai de transmission et de débit) ces protocoles de routage, des simulations ont été effectuées en variant non seulement le débit mais, aussi la distribution des classes de trafic pour permettre un déploiement urbain à grande échelle. Étant donné que cette thèse est prévue pour les ingénieurs de réseaux et les concepteurs de systèmes de communications pour les réseaux intelligents, un deuxième déploiement réel a été aussi évalué correspondant à un micro-réseau. Cette dernière a été conçue pour estimer la transférabilité des résultats obtenus à grande échelle.

Acknowledgments

I would like to acknowledge my supervisor Professor Tho Le-Ngoc for his support, his guidance and encouragement without which this thesis could never have been completed. I am especially grateful for his sharp insights, his resourcefulness and his ability to quickly foresee solutions to potential pitfalls.

I take this opportunity to express recognition to all of the members of the Broadband Communications Research Lab for their help and support. In particular, I would like to express my thanks to Yue Gao who aided me in the early stages of this thesis. In addition, I am also grateful to our lab research associate, Dr. Quang-Dung Ho for his assistance, advice and never-ending invaluable help throughout the course of my studies.

I also like to express my gratitude for my family and my friends for their unceasing encouragement, support and attention that helped me complete this thesis. I also place on record, my sense of gratitude to one and all, who directly or indirectly, have lent their hand in this long and arduous venture.

Contents

List of Figures

List of Tables

Acronyms

1G, 2G, 3G, 4G	First, Second, Third, Fourth Generation
ACK	Acknowledgment
ADA	Advanced Distribution Automation
AMC	Adaptive Modulation and Channel Coding
AMI	Advanced Metering Infrastructure
AODV	Ad-Hoc On Demand Vector Routing
APP	Application
BLE	Bluetooth Low Energy
bps	bits per second
BS	Base Station
CDMA	Code-Division Multiple Access
CH	Cluster Head
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTP	Collection Tree Protocol
CTS	Clear To Send
DA	Distribution Automation

DAG	Directed Acyclic Graph
DAP	Data Aggregation Point
DER	Distributed Energy Resource
DG	Distributed Generation
DIFS	Distributed Coordination Function Interframe Spacing
DIO	DODAG Information Object
DODAG	Direction-Oriented Directed Acyclic Graph
DR	Demand Response
DS	Distributed Storage
DSSS	Direct Sequence Spread Spectrum
EIFS	Extended Interframe Spacing
EMI	Electro-Magnetic Interference
ETX	Expected Transmission Count
FIFO	First In First Out
FLIR	Fault Location, Isolation and Restoration
GEO	Geographic Routing
GF	Greedy Forwarding
GPSR	Greedy Perimeter Stateless Routing
GUI	Graphical User Interface
HAN	Home Area Network
HC	Hop Count
HEED	Hybrid Energy Efficient Distributed

IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
kbps	kilobits per second
LEACH	Low Energy Adaptive Clustering Hierarchy
LTE	Long-Term Evolution
M2M	Machine-to-Machine
MAC	Medium Access Control
Mbps	megabits per second
MiXiM	Mixed Simulator - Dependency Library
MP2P	Multi-Point-to-Point
NAN	Neighbor Area Network
NED	Network Description Language
NET	Network
NIST	National Institute of Standards and Technology
OF	Objective Function
OMS	Outage Management System
P2MP	Point-to-Multi-Point
P2P	Point-to-Point
PDR	Packet Delivery Ratio
PHY	Physical Layer
PIFS	Point Coordination Function Interframe Spacing
PMU	Phasor Measurement Unit

PPS	Proactive Parent Switching
QoS	Quality-of-Service
RPL	Routing Protocol for Low Power and Lossy Networks
RPL-M	Multi-instance RPL
RPL-M+	Multi-instance RPL with Prioritized Channel Backoffs
RR	Renewable Resource
RTS	Request To Send
SAS	Substation Automation System
SCADA	Supervisory Control and Data Acquisition
SG	Smart Grid
SGCN	Smart Grid Communications Network
SIFS	Short Interframe Spacing
SM	Smart Meter
ST	Slot Time
SUN	Smart Utility Network
TDMA	Time-Division Multiple Access
TOU	Time-Of-Use
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
WASA	Wide-Area Situational Awareness
WFQ	Weighted Fair Queuing
WiMAX	Worldwide Inter-operability for Microwave Access

WMN Wireless Mesh Network

WRR Weighted-Round-Robin

WSAN Wireless Sensor and Actuator Network

WSN Wireless Sensor Network

Chapter 1

Introduction

1.1 Wireless Sensor Networks (WSNs)

WSNs are typically composed of thousands of sensor nodes scattered in an area and capable of sensing environmental attributes, processing collected data and wirelessly communicating it to a base station (BS). Based on the application, these sensors can vary, i.e., temperature sensors, light sensors, medical sensors, humidity sensors and movement sensors. Thus, WSN can be used for a wide range of applications such as target field imaging, surveillance, environmental assessments, remote patient monitoring, smart homes, home automation, smart health, smart grid and many more. Depending on the application, these networks can be mobile or static, homogeneous or heterogeneous, and the nodes can be line-powered or battery-powered. Further, the implemented routing protocols can vary based on the network topology, components and the desired end goal. Thus, the challenge of designing routing protocols for WSNs lies with the properties of the nodes and the network itself. In particular, design criteria for WSN routing protocols should consider the challenges offered by differing node deployment or heterogeneity, desired fault tolerance, desired connectivity and coverage, desired level of energy consumption without loss of accuracy, desired network scalability, and finally the challenges offered by the wireless transmission media. However, the protocol implementation itself is application specific since different applications require different criteria of operation. With that in mind, for the remainder of this thesis, the focus will be on smart grid applications.

1.2 Smart Grid Evolution

Energy systems have evolved from small, localized plants to extraordinarily complex, widespread interconnected networks for the generation and delivery of electric energy to consumers, as shown in Fig. 1.1a. However, their fundamental operation, maintenance and management methods along with their physical infrastructure have not been sufficiently innovated despite the exponential growth of consumers and their demands. This lack of investment, combined with aging and un-computerized equipment, has resulted in an *inefficient* and increasingly *unstable* electric system [1]. The situation is further exacerbated by the lack of sufficient facilities and crisis handling procedures for fault detection, localization, isolation and service restoration. This implies that accidental break-downs or natural disasters could have a devastating impact [2–4], hurt the economy, and pose critical security and safety threats on national and international scales. Moreover, the current infrastructure is designed in an *inflexible* manner for conventional large fossil fuel burning power plants, whose non-renewable energy resources are scarce [5] and invite environmental pollution concerns due to (i) their toxic combustion by-products [1,6] and (ii) the devastating spills that can result from improper oil extraction and transportation. Thus, these issues and concerns drive the need for the *smart grid* (SG), as shown in Fig. 1.1b.

By definition, the SG "is an automated, widely distributed energy delivery network characterized by a two-way flow of electricity and information, capable of monitoring and responding to changes in everything from power plants to customer preferences to individual appliances" [7]. In a nutshell, it is a *modernized* and *computerized* electric utility grid whose primary objectives are (i) to allow utilities to generate and distribute electric power with enhanced quality, efficiency and reliability, (ii) to reduce the contribution of the power grid to climate change and (iii) to allow consumers to optimize their energy consumption. For example, reduction in power transmission losses and environmental pollution is achieved through extensive use of distributed energy resources (DER) and renewable resources (RR). Operable either in parallel or separately from the grid, DER encompass a wide range of small-scale distributed generation (DG) and distributed storage (DS) technologies that result in many benefits from both economical and operational points of view. For instance, assuming 10 percent penetration in the U.S. power grid, DER could save 10 billion dollars per year by 2020 as well as significantly reducing greenhouse gas emissions and enhancing power quality, reliability and independence [8].

As for efficiency and reliability, they are enhanced via real-time monitoring and control. Intelligent sensors and actuators, embedded with communications technologies, are integrated to autonomously collect data and enable remote control through data communication networks. As a result, the SG can optimize the operation of its interconnected elements (enable adaptive system configuration, operation and flexible management that allow for well-controlled energy injection from alternative sources at any point to help relieve heavy-load stress). DER, RR along with flexible facilities and mechanisms to incorporate them into the grid create microgrids, defined as smart small-scale distributed electricity systems. Microgrids, a distinguishing feature of the SG, can work either in grid-connected or island modes to achieve specific local goals such as reliability enhancement, carbon emission reduction, diversification of energy sources and cost reduction. Additionally, advanced distribution automation (ADA) enhances SG efficiency by offering an extension to utilities' control over small-scale systems. Specifically, local automation, remote control, and central decision making are brought together in ADA to deliver a cost-effective, flexible, and cohesive operating architecture [9, 10] whose benefits include improved utilization of system capacity, increased revenue due to quick restoration and higher customer loyalty.

Finally, data communications and remote control capability along with the deployment of smart meters (SM) enable various intelligent services and applications that help consumers customize their power consumption profile. A SM, a key SG element, is an electronic device that records electric energy consumption and communicates that information back to the utility for monitoring, management and billing purposes. It also supports two-way communication between the meter and the central system for other functions, referred to as advanced metering infrastructure (AMI). With real-time energy consumption information, electricity prices can vary during the day, i.e., time-of-use (TOU) pricing. Specifically, consumers can adjust the amount or timing of their energy consumption in response to real-time energy price. These actions, termed demand response (DR), can effectively help reduce energy consumption and cost, smooth out peak energy demand and thus prevent grid overload and cut the costs due to excessive backup power capacity. A recent Pacific Northwest National Laboratory study provided homeowners with SG technologies to monitor and adjust home energy consumption. The average household reduced its annual electric bill by 10 percent. If widely deployed, this translates to peak load reductions of up to 15 percent annually, or equivalently, more than 100 Gigawatts or the need to build 100 large coal-fired power plants over the next 20 years in the United States alone. This could
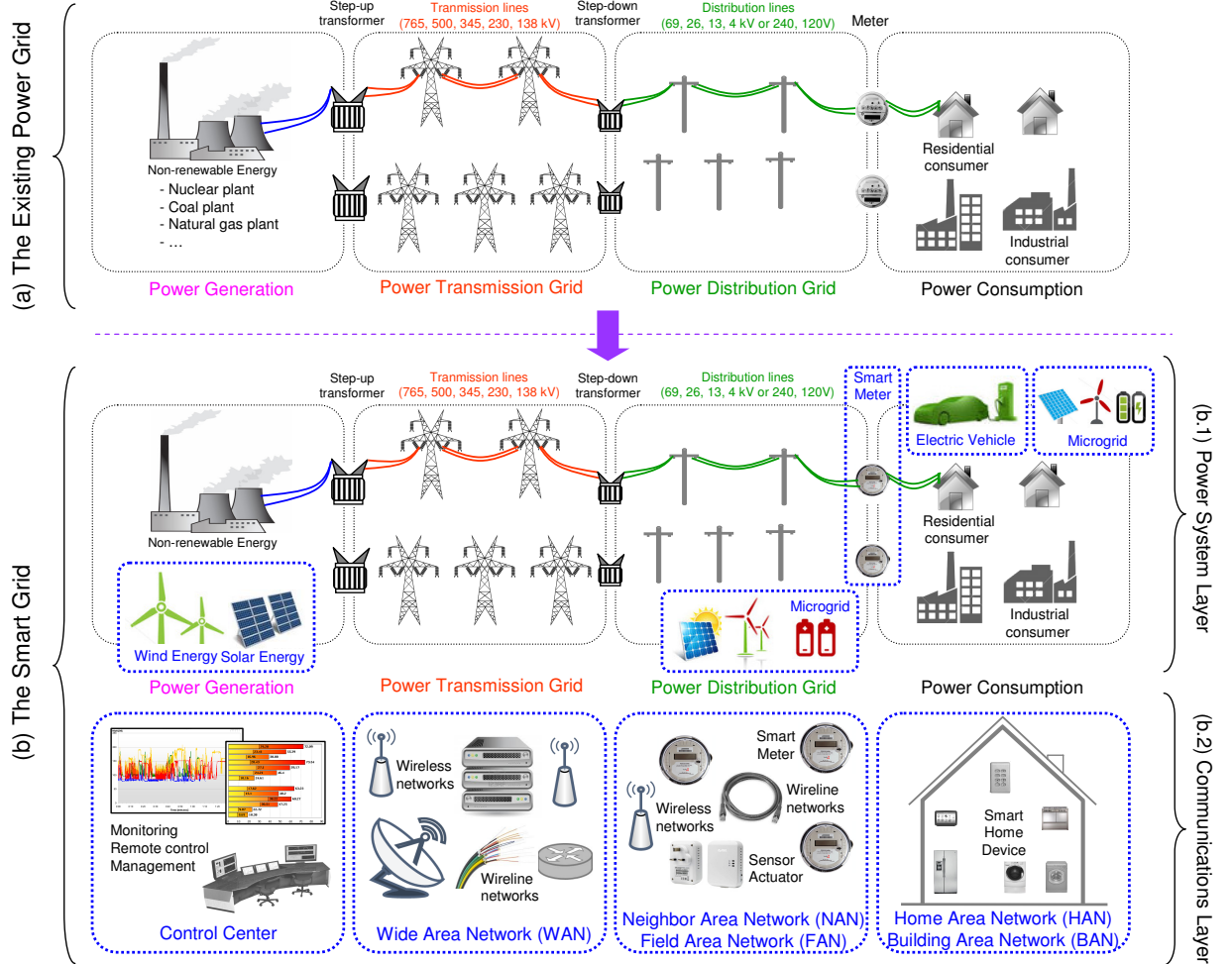
Figure 1.1   The existing power grid versus the smart grid

save up to 200 billion dollars in power grid capital expenditures, and take the equivalent of 30 million vehicles off the road [1].

1.3 Smart Grid Communication Networks (SGCN)

1.3.1 Characteristics, Requirements, and Challenges

The key to achieve the above-mentioned SG goals is embedding an advanced communications infrastructure into the power grid. The SG's overall architecture is therefore usually presented by the integration of the power system and the smart grid communications net-

work (SGCN), as shown in Fig. 1.1b.1 & b.2, respectively. This network transports sensor data and control signals that allow utilities to actively monitor and manage the entire electricity system in a harmonized manner. In other words, the SGCN is the SG's nervous system and it aims to support all identified SG functions. For example, the SGCN allows utilities to receive information from the grid to determine where power outages or system failures occur as well as their possible causes. It can also send instructions to related devices to prevent cascaded failures or even fix detected problems. Smart devices in residential/commercial buildings can inform consumers of the real-time energy price, main power grid status, operations of appliances and even allow consumers to dynamically control injection of power generated by local renewable DER in microgrids for stable operations and cost reductions. In essence, it is the SGCN that makes the power grid "smart" and allows for efficiency, reliability, integration of green and sustainable DG, and emerging SG applications. However, a successful implementation of a cost-effective, efficient, robust and secure SGCN is challenging since it has various characteristics, features, and requirements, different from those of existing residential and commercial communications networks.

As the SG is a complex system responsible for performing diversified functions from all power segments, the SGCN interconnects millions of devices [11] of different types in different topologies. Therefore, it must be scalable to network size and traffic volume as more advanced SG applications emerge. Moreover, most SGCN devices are required to operate in outdoor environments without regular maintenance for decades. Thus, the SGCN should support network upgrades and expansions with minimal human intervention. Next, despite the fact that most SGCN network elements are static, their communications links dynamically change over time. Given that many SGCN segments are implemented with wireless communications technologies, multi-path fading can introduce significant link condition variations. Surrounding environments and harsh weather conditions can also affect link quality. In cases of connectivity loss, in order to minimize packet loss and delay, the SGCN needs to have mechanisms to measure or estimate the instantaneous link quality and be able to adapt well to any link connectivity change (e.g., multiple link and/or node failures). For example, automatically re-route traffic around regions experiencing connectivity losses. Otherwise, the communications will be delayed or corrupted and the SGCN would fail to transport information necessary for detecting and troubleshooting power system faults. Therefore, the communications and networking protocols designed for the SGCN should be self-organizing, distributed, scalable, self-healing and robust.

Another SGCN challenge is the presence of various communications models. Multi-point-to-point (MP2P) is the primary model; data (i.e., energy consumption, metering profile, device status, power quality, etc.) collected by various types of intelligent devices flow towards data collectors or data aggregation points (DAP). The converge-cast nature of MP2P traffic requires data processing and communications/networking protocols that are specially developed to efficiently aggregate data and mitigate congestion at DAPs. Besides, point-to-multi-point (P2MP) is another important supported communications model. The information related to real-time pricing, commands for fault isolation or energy flow re-direction, instructions for DR functions, etc., are conveyed from utility control centers to field devices for optimizing user energy consumption, smoothing out power consumption peaks, optimizing the distribution grid and resolving various distribution level failures. Point-to-point (P2P) communications between two devices could be exploited to meet security, scalability, and hard real-time requirements in small-scale local SGCN segments.

Additionally, the SGCN is designed to enable a variety of industrial and residential applications whose constituent network elements greatly differ in terms of their Quality-of-Service (QoS) requirements. For example, home meters typically need to support low-data-rate and non-real-time communications for periodic meter readings and residential DR applications. Building or multi-building meters require much higher data rates and near-real-time communications for advanced commercial/industrial applications such as enterprise smart energy management, renewable energy integration, microgrid monitoring and coordination, etc. Devices for critical missions (e.g., fault detection and restoration) may only need to transmit short messages occasionally, however, these messages require very high reliability and stringent delay. Failures to deliver data or commands necessary for these missions within the allowed time frame can compromise power system operations with catastrophic consequences. Therefore, resource allocation and scheduling mechanisms for efficient provision of a wide range of QoS requirements is challenging. Furthermore, the SG is currently in its infancy, technical details related to communications traffic profiles and QoS requirements are still imprecise. However, given that most SG applications are for industrial monitoring and control, their characteristics and requirements are quite different from those of today's telecommunications applications such as file transfer, email exchange, web surfing, voice and video streaming.

Even though the SG offers many benefits, its strong dependence on the SGCN obviously makes it vulnerable to cyber threats. SGCN security breaches may result in not only

leakage of consumer information, but also serious consequences ranging from power blackouts, physical damage of equipment and infrastructure, and breakdowns of public safely and national security. As a result, security and privacy issues have been considered by governments, industries, and consumers as one of the highest priorities for design, deployment, and adoption of the SG. Given the vast scale and complex architecture of the SGCN as well as the presence of various traffic profiles and associated QoS requirements, existing security frameworks and protocols employed for public data communications networks are likely no longer adequate. They may need further enhancement or new/additional solutions need to be developed to properly address all security vulnerabilities in the SGCN.

1.3.2 SGCN Implementation

The SGCN is typically composed of various segments, each responsible for information and control message exchanges within a specific power grid region, as sketched in Fig. 1.1b.2. However, there is no one-size-fit-all communications technology due to the diversity in service coverage area, population density, financial budget, and performance requirements. Consequently, each segment's varying characteristics can be associated with a different communications network type whose communications characteristics are discussed below.

Home Area Network (HAN) corresponds to the consumer premise and is in charge of gathering sensor information from a variety of smart appliances and devices and delivering control information to them for better energy consumption management. For example, it can support functions such as cycling heaters, washers/dryers, or turning air conditioners off during peak load conditions. Typically, HANs need to cover areas of up to 200 square meters and support from 10 to 100 kilobits per second (kbps). Technologies include IEEE 802.15.4/ZigBee, Bluetooth Low Energy (BLE), etc.

Neighbor Area Network (NAN) handles smart metering communications that enable information exchange between customer premises and the utility company's wide area networks. NAN endpoints are SMs, considered to be the heart of the SG revolution. SMs support energy consumption recording and real-time or near real-time data acquisition and control for various SG applications including distribution automation (DA), power outage management, power quality monitoring, etc. A NAN cluster

usually covers an area of several square kilometers and forms a static network. The number of SMs in each cluster varies from a few hundreds to a few thousands depending on the power grid topology and the employed communications technology and protocol. The data rate required by each SM may vary widely depending on deployed applications. For example, for interval and on-demand meter reading, only around a few bits per second (bps) per meter is required. However, in order to support future applications, such as ADA, fault detection and restoration and so on, higher data rates, e.g., a few tens of kbps per meter, may be required. It is noted that the NAN is a critical segment of the SGCN since it is responsible for transporting a huge volume of different types of data and distributing control signals between utility companies and a large number of devices installed at customer premises. Technologies include IEEE 802.15.4g/SUN, IEEE 802.11 WiFi mesh, cellular networks, etc.

Wide Area Network (WAN) aggregates data from multiple NANs and conveys it to private utility company networks. It also enables long-haul communications among different DAPs of power generation plants, DER stations, substations, transmission and distribution grids, control centers, etc. Additionally, the utility company's WAN is responsible for providing the two-way network, needed for substation communications, distribution automation, power quality monitoring, etc., while also supporting data aggregation and back-haul for NANs. The WAN may cover a very large area, i.e., thousands of square kilometers and could aggregate a large number of supported devices and thus require hundreds of megabits per second (Mbps) of data transmission. Given its outdoor nature and need for long-haul communications, candidates technologies are WiMAX, 3G, 4G or Long Term Evolution (LTE).

A Typical Implementation of a SGCN

In order to illustrate the use of multiple technologies in the SGCN, Fig. 1.2 presents a widely-accepted network architecture [12,13]. In particular, a low-power and low-data-rate radio technology provides the connectivity for devices in HANs and broadband wireless mesh networks (WMN) connect SMs in NANs and relay information to DAPs that are back-hauled by cellular and wireline networks. The wireless mesh has been considered as the most promising solution for NANs as it has low deployment and maintenance costs
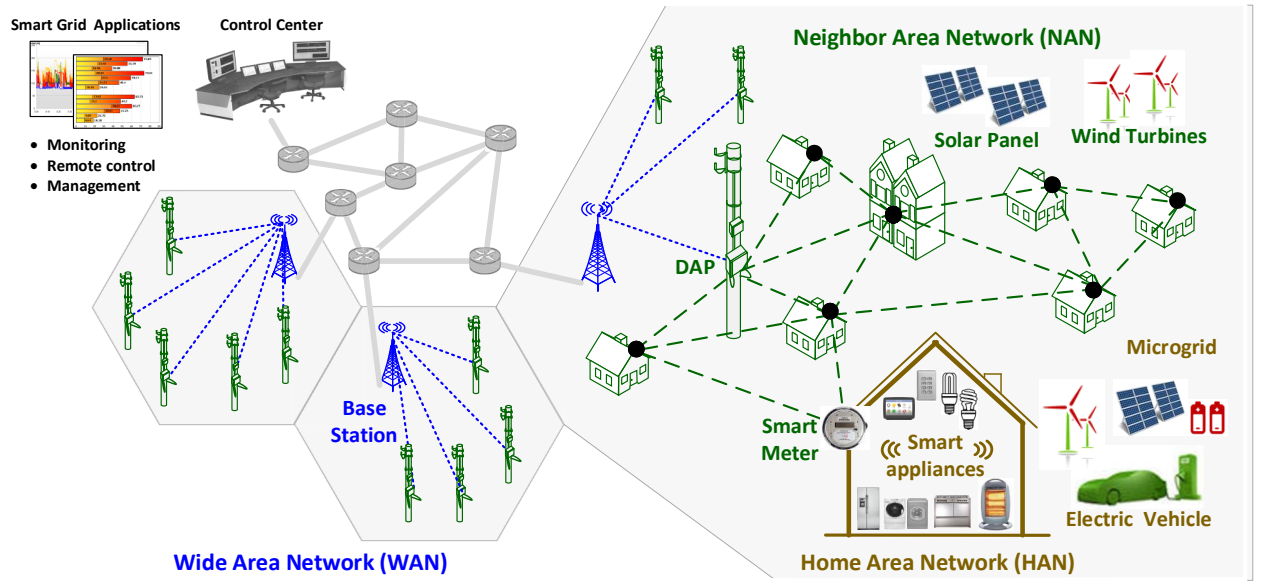
Figure 1.2   The SGCN as an integration of many communications technologies

as well as excellent resilience to node/link failures. A WMN can be established almost anywhere without the cost and disruption of running cabling or fiber. It provides a multi-path, multi-hop connectivity that is absolutely necessary for outdoor deployment. IEEE 802.11 WiFi radio is employed in this segment due to its maturity and low-cost while providing high-speed broadband communications (up to a few tens or even hundreds of Mbps) that emerging advanced SG applications are likely to require (as opposed to IEEE 802.15.4-based technologies that can only support up to a few hundreds of kbps). Cellular networks have a very wide coverage while offering high data rate and low latency. Especially, LTE technology can deliver low cost per bit, advanced radio resource management and scheduling, and high-performance connectivity needed to address the challenges of SG machine-to-machine (M2M) communications. This technology has been considered as a future-proof solution for DAPs and many other SG devices that need to remain in the field for decades. The wireline backbone in Fig. 1.2 can be implemented by various broadband technologies (leased lines or fiber optics) that can provide gigabit-per-second and sub-millisecond connectivity. For the remainder of this thesis, this network architecture is assumed.

1.4 Motivation

The intelligence of the SG relies heavily on wide-scale monitoring and control applications for which the intended form of communications is M2M. Specifically, M2M communications is characterized by short bursty traffic profiles within a network of various heterogeneous electronic devices, communications and software technologies [14, 15]. Furthermore, given the segmented nature of the SGCN, technology inter-operability is essential to maintain latency and reliability requirements imposed by SG M2M applications. Focusing on the SG, different environments translate into differing challenges and M2M requirements. At the home and smart building level, wireless networks are the norm and applications such as lighting control, heating, ventilation, etc., require SG monitoring applications. Therefore, the main M2M requirements are very low power consumption and inter-operability, coordination and resource allocation between the various different interconnected devices. At the power distribution level, the SG offers cost-effective communications for monitoring, control and diagnostic purposes. At this level, the main requirements are high scalability, high reliability and robustness to harsh power system environments. Moreover, when considering communication technologies, promising candidate system architectures incorporate cellular networks at the WAN level. This in turn raises further challenges associated with resource scheduling and allocation at the cellular level.

In this thesis, the focus lies solely on SG NAN communications. In particular, the NAN is singled-out for further study due to its unique yet challenging characteristics; (i) resiliency to harsh outdoors communication environment in the proximity of power systems, (ii) endurance for decades with minimal maintenance to match that of associated power systems, (iii) allowance for expansion to cover larger areas or additional endpoints and finally (iv) support for multiple traffic flows. Further, as it is composed of interconnected sensing nodes (SMs), the most promising form of communications for the SG NAN is a WMN [12, 13]. Given this choice, M2M traffic profiles within the NAN can be classified as unicast or multicast in the downlink direction and converge-cast in the uplink direction. Now, as all generated uplink traffic must pass through the DAP, it poses significant challenges with respect to routing through communications bottlenecks, i.e., overloading nodes close to the DAP, congestion at the DAP, increased interference, higher likelihood of packet collisions, etc. Therefore, this thesis aims to tackle the challenges of the SG NAN converge-cast uplink and achieve the required application requirements.

Specifically, previous works have explored in-depth the suitability of the Routing Protocol for Low Power and Lossy Networks (RPL) in the SG context [12, 13, 16, 17]. However, they only considered a single representative traffic class and failed to provide any means of securing the communications link. With that in mind, this thesis intends to expand on previous RPL-based research by considering QoS requirements for different traffic classes and proposing QoS enabling extensions within the RPL framework in an attempt to achieve the desired QoS differentiation for SG applications such as AMI.

1.5 Contributions

In the SG NAN converge-cast context, RPL is a promising routing protocol. However, as the NAN is not only responsible for providing connectivity for a vast number of devices but also meeting the varying QoS requirements of different types of SG applications, characterizing the performance requirements of various SG applications is important in order to understand which communications technologies and applications can be successfully paired [18]. Besides, in order to enable efficient prioritization of certain applications that have critical requirements, the communications network must be able to differentiate and provision different QoS requirements. Existing solutions related to QoS differentiation need to be revisited to cater for SG traffic because SG applications traffic will likely be quite different from that generated by traditional data applications in use today. In particular, the NAN is expected to carry a mix of both periodic and critical traffic. In addition, the number, type and proportion of traffic classes will affect the complexity and efficiency of any devised resource allocation scheme. Further, QoS requirements in the SG NAN context depend not only on traffic class requirements but also the current grid stability (e.g., stable, cascading faults, etc.) [19, 20]. Thus, research is needed to allow for a more seamless administration of all anticipated SG traffic types [18, 19].

With that in mind, this thesis fills the aforementioned gaps by expanding on the concept of QoS differentiation for different traffic classes through multiple RPL instances. Specifically, correlating RPL routing metrics or Objective Functions (OFs) with different SG application traffic classes in an attempt to incorporate QoS differentiation at the network layer. Further, as most QoS differentiation approaches are MAC-based, a cross-layered approach is designed so as to allow for prioritized channel accesses. Therefore, three variants of RPL are studied, single instance RPL, multi-instance RPL (RPL-M) as well as

multi-instance RPL with prioritized channel backoffs (RPL-M+). A simulation-centric performance evaluation is performed for (i) two traffic classes, to model periodic and critical AMI data, (ii) two relative traffic compositions to symbolize different grid conditions, (iii) three data rates to represent increasing data traffic load and (iv) two deployment scenarios to portray a large-scale random urban scenario as well as a real rural scenario. As this thesis is intended to be of use for SG communications system designers and network engineers, the real-life deployment scenario, a microgrid, was considered to showcase the performance and achievable QoS differentiation of the aforementioned RPL-based protocols as well as the usability (transferability) of the obtained results in a more general context. Extensive simulations are carried out to demonstrate the performance, in terms of latency and throughput, of standard RPL, RPL-M and RPL-M+.

1.6 Thesis Organization

This thesis is divided into five chapters. This chapter introduced the SG along with its benefits. Then, a communications infrastructure, the SGCN, as well as its associated crucial requirements have been highlighted. More detailed understanding of the SGCN and further work in converge-cast based QoS communications for this network will be presented in subsequent chapters as follows.

Chapter 2 surveys various existing routing protocols designed for wireless mesh networks that could be used for the NAN. Based on this survey, suitable families of routing protocols are determined. Then, promising candidate protocols for each selected routing families are compared and RPL is chosen for further study.

Chapter 3 investigates the QoS requirements of various current and emerging SG applications. Focusing on the AMI application, a key feature of the NAN, two representative traffic classes are chosen, namely critical and periodic AMI traffic. Based on these two chosen converge-cast traffic profiles, QoS enabling extensions are presented for RPL at not only the network layer, but also the MAC layer. Then, based on these extensions, two QoS specific variants of RPL, namely RPL-M and RPL-M+, are presented for further study.

Chapter 4 explores network performance, in terms of packet delivery ratio and latency, for RPL, RPL-M and RPL-M+. In particular, to determine the achievable QoS

differentiation in the NAN setting, the data rate along with the relative composition of the representative traffic classes (critical and periodic) are varied to model increasing data offered load and varying grid conditions, respectively. In addition, two separate deployment scenarios are chosen, a random large-scale urban setting as well as a *real* small-scale rural deployment scenario corresponding to the community of Burwash Landing, Yukon, Canada.

Chapter 5 concludes this thesis by providing a summary of the key observations and trends ascertained through the six devised study cases. Then, potential future research directions are presented to highlight suggested next steps to expand and improve upon the obtained results.

Chapter 2

Wireless Network Routing Protocols for NANs

In order to determine suitable routing protocols for the SGCN, this chapter surveys various existing routing protocols designed for wireless mesh networks. The focus is given to protocols that could be used for the NAN, arguably the most important segment of the SGCN. Based on this survey, suitable families of routing protocols, location-based protocols and self-organizing coordinate system protocols, are determined. Then, promising candidate protocols for each selected routing families are compared and a promising self-organizing coordinate system protocol is chosen for further study. Specifically, the main operating principles along with weaknesses and strengths of RPL are presented.

2.1 Routing in Wireless Networks

Network routing is the process of establishing paths for packet transmission from source to destination. This is done with packet-switching, i.e., breaking a message down into packets (with headers to guide message reassembly at the destination), and designing a routing protocol to select the best path to travel through the network in order to achieve some specific goal. For example, optimizing path selection for shortest paths, load balancing, reduced energy consumption, reduced overhead, enhanced robustness and reliability, etc.

In the context of wireless ad-hoc and sensor networks, over the last few decades, several routing protocols have been proposed and studied [21–26]. They can be classified into different protocol families depending on underlying network structure (i.e., flat, hierarchical,

Routing protocols for wireless networks
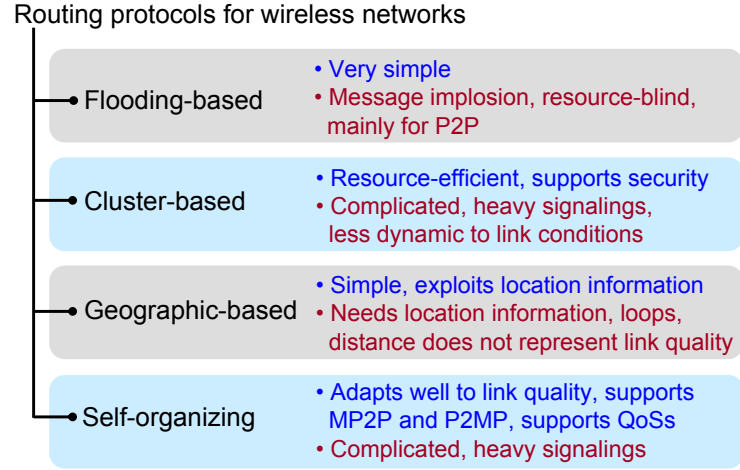
Figure 2.1   Routing protocol classification

and location-based routing) and protocol operation (i.e., multipath-based, query-based, negotiation-based, QoS-based, and coherent-based). Routing protocols can be proactive (i.e., each node actively collects current network status and maintains one or more tables containing routing information to every other nodes in the network) or reactive (i.e., routes are created when required by performing route discovery and selection procedures on-demand). In the following subsections, key features, advantages and disadvantages of a number of representative routing protocols (in Fig. 2.1) are investigated in order to facilitate the selection of candidate protocols for SG NANs.

2.1.1 Flooding-based Protocols

Flooding-based protocols enable P2P traffic patterns and rely on broadcasting data and control packets by each node into the entire network. In its conventional implementation, a source node sends a packet to all of its neighbors, each of which relays the packet to their neighbors, until all the nodes in the network (including the destination) have received the packet. Despite its simplicity, pure flooding suffers from many disadvantages including implosion, i.e., redundant copies of messages are sent to the same node by different neighbors or through different paths, and resource blindness, i.e., flooding lacks consideration for energy constraints of nodes when transmitting packets [27]. Flooding protocols are only particularly useful for P2P communications among a small number of mobile nodes without the need for any routing algorithm and topology maintenance.

2.1.2 Cluster-based Protocols

Cluster-based protocols are based on a hierarchical network organization. Nodes are grouped into clusters, with a cluster head (CH) elected for each one. Data transmission typically goes from cluster members to CH, and then from CH to sink node. Since CHs are responsible for relaying and processing high volume data, they typically have higher energy and computation capability. This kind of routing can support MP2P, P2MP and P2P traffic. Clusters are built and maintained as a function of various node and system parameters, such as node energy, link quality, traffic pattern, data correlations between nodes, etc. [28–34]. This class' drawbacks are that (i) link dynamics cannot be captured, and (ii) head selection, cluster formation and maintenance introduce significant signaling overhead. Besides, protocols like LEACH [33] and HEED [31] assume that TDMA and CDMA are used for intra-cluster and inter-cluster communications, respectively, and that nodes can tune their communication range through transmission power. These assumptions make them impractical for real deployment. Fortunately, splitting the network into smaller clusters efficiently limits the data flooding area. This offers benefits in scalability, lifetime, and energy consumption. Additionally, since nodes in physical proximity are more likely to sense correlated events, data can be efficiently aggregated at the CH to reduce network load. Implementation of security is also easier since CHs can act as trusted network entities.

2.1.3 Geographic or Location-based Protocols

Geographic protocols (GEO) route the traffic based on the location knowledge of a node, its neighbors and the sink node. Greedy forwarding (GF) is the simplest form of GEO. When a node receives a message, it relays the message to its neighbor geographically closest to the sink [35]. Since geographic distance is not necessarily radio communication distance, the drawback of GF is that the selection of next hop merely based on geographic distance may lead to void areas where the traffic cannot advance further towards the destination. More advanced location-based routing protocols that attempt to improve the delivery rate are proposed in [36–40]. The advantage of GEO is that it can achieve network wide routing while maintaining only neighborhood information at each node, hence significantly reducing signaling overheads and the complexity of the routing solution. However, node geographical locations must be known in advance. Otherwise, some mechanism to determine node locations with sufficient accuracy is necessary.

2.1.4 Self-organizing Coordinate Protocols

Self-organizing coordinate protocols counteract the biggest drawback of GEO by building a viable coordinate system based on communication distance rather than geographic distance. The aim of such coordinate systems, in the context of routing protocols, is not to mimic geographic location but rather to be of use for feasible routing solutions [22]. In particular, the cost of determining nodal geographic locations is eliminated via the generation of *virtual* coordinates upon which GEO style routing can operate. For example, *virtual* coordinates can be inferred based on their position relative to anchor nodes whose location is known. On the other hand, they can also be estimated based on some routing metric such as hop count, link-quality, bandwidth, etc. However, as with GEO protocols, the drawbacks of this class of protocol are related to how accurately the chosen coordinate system can model the real physical network characteristics.

2.2 Routing in NANs

2.2.1 SG NAN: Characteristics, Requirements, and Challenges

The NAN is an important constitutive segment of the SGCN since it provides the necessary connectivity between SMs and the utilities in order to enable various key SG applications. On one hand, it can be considered as an outdoor wireless sensor and actuator network (WSAN). On the other hand, it exhibits many characteristics and challenges that are not found in a general outdoor WSAN. Most NAN devices are installed in a close proximity to power lines and equipment. For example, SMs are typically in distribution feeders before the electricity is delivered into the apartments or buildings while smart sensors and controllers are along power lines, on utility poles, or in substation areas. Therefore, the communications of these devices can be affected by ambient electro-magnetic interference (EMI) produced by power lines and power switching equipment. Such EMI results in impulsive noise that is distinguished from the thermal Gaussian noise produced in the receivers of the devices themselves. Further, NAN devices are usually powered by the grid itself; however, in cases of power outages in the grid, they still have to stay operational by switching to their battery power supplies. Additionally, the NAN connects millions of SMs, routers, and gateways that are distributed over a vast geographical area. These devices are mostly installed outdoor and operate in harsh environments (low/high temperatures, obstacles, rain,

snow and so on). This network therefore needs to be scalable, self-organizing, and robust. Cyber security requirements are also critical since the NAN conveys a huge volume of private information of residential/commercial consumers (e.g., identities, power consumption profiles and habits, real-time residential/business activities, etc.) as well as vital sensor and control signals necessary to harmonize/optimize the operations of the power grid and to reduce energy consumption. Besides, traffic patterns and QoS requirements for NANs are different from those of conventional applications. For example, periodic meter reading requires high reliability but can tolerate latency and jitter. However, emergency messages (e.g., in case of power grid failures) are generated randomly in bursts but require very stringent latency. Therefore, developing routing protocols for NANs is a challenging task. The authors in [41–43] give a survey of routing protocols selected for NAN scenarios using various communications technologies and networking. This thesis, as previously discussed, focuses on wireless mesh networks due to their advantages in deployment, operation and maintenance costs.

2.2.2 Candidate Protocols

Given the routing protocol classifications presented, the feasibility of flooding-based protocols in the SG NAN context is hindered by their disadvantages. As for cluster-based protocols, their advantages seem very attractive for the NAN. As each node in the WAN serves multiple NANs, their interconnection is naturally organized into multiple clusters. Each cluster, a NAN, serves a few thousands of SMs and data is managed by the DAP acting as the CH. Then, SMs that have some underlying correlation can be placed within the same cluster. For example, SMs located in the same distribution feeder may send similar notification messages at the same time when their feeder fails. If those messages are gathered by their CH, redundancy can be detected and resolved efficiently to minimize network traffic volume while still assuring that no important information is lost throughout the network. Additionally, CHs can offer important security features required by the NAN. As for inter-cluster communications, as it corresponds to the WAN, as described in Section 1.3.2, it should be cellular. However, for intra-cluster communications, given the network size and the need for scalability, multi-hop communications is necessary. Further, in order to overcome the drawbacks of cluster-based protocols, intra-cluster communications should be protocols from either the location-based or self organizing coordinate system families.

Conversely, foregoing the natural organization of the NAN/WAN interconnection, clustering protocols could be implemented *within* the NAN. In particular, dividing the number of SMs associated with the same DAP into clusters. However, since CHs require higher energy and computation capability, this would necessitate the deployment of DAP-like SMs that can operate as CHs. Specifically, this creates a trade-off in terms of clustering benefits (e.g., limiting data flooding area, scalability, aggregation, etc.) versus the overheard associated with cluster formation, maintenance and operation. Additionally, most clustering protocols require some mechanism for multiple access, (e.g., TDMA, CDMA, etc.) whose successful implementation requires consistent state coordination between network nodes, which is difficult to maintain with wireless lossy links. Given these challenges, clustering protocols are rarely used in real-world deployment or commercial WSNs [22]. Therefore, even though clustering protocols seem advantageous for the NAN, research focus and standardization efforts have veered towards large converge-cast. With that in mind, the remainder of this chapter will focus on two promising candidate protocols, namely, greedy perimeter stateless routing (GPSR), a representative implementation of location-based routing class, and RPL, the state-of-the-art self-organizing coordinate protocol.

Routing Protocol for Low Power and Lossy Networks (RPL)

RPL is a representative protocol that captures most of the ideas introduced by self-organizing coordinate system protocols [23]. In terms of advantages, first, RPL constructs a directed acyclic graph (DAG) whose structure matches the physical structure of the NAN. Root nodes represent DAPs, leaf nodes represent SMs, and other nodes inside the DAG represent routers that maintain connectivity between root and leaf nodes. Second, MP2P and P2MP, typically required by the NAN, are the primary communications supported by RPL. Third, by employing different routing metrics and cost functions, RPL can construct multiple DAG instances over a given physical network. Each instance can be dedicated for a specific routing objective or constraint that can be addictive, multiplicative, inclusive/exclusive and so on. This facilitates QoS differentiation and provisioning for different NAN traffic types. Moreover, with the trickle timer that governs the network state update, RPL requires less signaling overhead and thus is more energy-efficient. Finally, the roots of DAGs can act as trusted entities that enable security in the network.

In [44], the performance of RPL implemented in an experimental platform using TinyOS is presented. The results in [44] indicate that RPL performs similarly to the Collection Tree Protocol (CTP), the de-facto standard data collection protocol for TinyOS 2.x [45], in terms of packet delivery and protocol overhead. Compared to CTP, RPL can provide additional functions, i.e., it is able to establish bi-directional routes and support various types of traffic patterns including MP2P, P2MP and P2P. Therefore, the authors in [44] conclude that RPL is more attractive for practical wireless sensing systems.

The work in [46] analyzes the stability of RPL whose DAG is built based on link layer delays. It is observed that delay fluctuations introduced by the IEEE 802.15.4 MAC layer negatively influences RPL's stability as it forces nodes to change their best parent so frequently that it results in significant end-to-end delay jitters. In order to dampen the link layer delay fluctuation, the author proposes the use of memory in delay calculation. Simulations of a small network demonstrate that the proposed solution can reduce the mean and variance of the end-to-end latency and thus improve the protocol stability.

The authors in [47] provide a practical implementation of RPL with modifications so as to fit into the AMI structure and meet its stringent requirements. In particular, expected transmission time (ETX) link metric and a novel ETX-based rank computation method are used to construct and maintain the DAG. ETX is measured by a low-cost scheme based on a MAC layer feedback mechanism. A reverse path recording mechanism to establish the routes for downlink communications (i.e., from gateways to end-devices) is also proposed. This mechanism is purely based on the processing of uplink unicast data traffic (i.e., from end-devices to gateways), and thus does not produce extra protocol overhead. Extensive simulation results in [47] show that, in a typical NAN with 1000 SMs, and in the presence of shadow fading, the proposed RPL-based routing protocol outperforms some existing routing protocols like ad-hoc on demand vector routing (AODV), and produces satisfactory performances in terms of packet delivery ratio and end-to-end delay.

Self-organizing and self-healing solutions for RPL are proposed in [48]. A distinguishing feature in [48] is that DAPs may choose to operate at different frequencies in order to accommodate a scalable large network consisting of multiple trees. SMs perform channel scanning to detect DAPs and select the best one. Also, SMs can detect connectivity loss arising from failed nodes/links/concentrator and automatically recover from such failures by dynamically connecting to an alternative concentrator in their vicinity. Numerous performance parameters of the proposed RPL are studied by simulations. They include DAP

discovery latency and effects of DAP failures to packet delivery rate and recovery latency. The results in [48] have demonstrated that the proposed solution exhibits self-organizing properties and therefore is appealing from a deployment perspective.

In [49], a simulation-based performance evaluation of RPL, in a real-life deployment topology with empirical link quality data, is presented. This study focuses on the mechanisms that RPL employs to repair link or node failures. Global repair is implemented by the DAG root with the help of periodic transmission of new DAG sequence number. As for local repair, a node will try to quickly and locally find an alternate parent upon the loss of the original parent. Results in [49] show that the network fixes local connection outage much quicker when local repair is jointly used with global repair then when only global repair is used. However, there are a few incidents, mainly in cases where packet delivery ratio is low or when control messages are not heard for a long time, where the outage time becomes comparable to the DAG sequence number period. The behavior and performance of these two mechanisms thus need further study and improvement for outdoor and large-scale networks like NANs.

Greedy Perimeter Stateless Routing (GPSR)

GPSR, a GEO protocol, uses GF to forward packets to nodes that are always progressively closer to the destination. However, unlike most GEO protocols that are vulnerable to local minimums, i.e., when there is no one-hop neighbor closer to the destination than the forwarding node itself, GPSR recovers by forwarding in perimeter mode. Whenever a node closer to the destination is found, GPSR switches back to greedy mode. Therefore, GPSR can achieve network wide routing while maintaining only neighborhood information at each node. In particular, it allows routers to be nearly stateless because forwarding decisions are based on location information of destinations and one-hop neighbors. Further, its simplicity leads to good scalability as it is not necessary to keep routing tables up-to-date and to have a global view of the network topology and its changes. A new node can join the network easily by locally exchanging information with existing nodes in its vicinity. Since establishment and maintenance of routes are not required, signaling overhead and computational complexity of GPSR can be kept at a considerably low level. In addition to these advantages, the fact that NAN device locations are fixed and accurately known promotes GPSR as a promising solution for NANs.

Performance of a geographic routing protocol in realistic smart metering scenarios is presented in [50]. Using simulations, received packet ratios given by the protocol are measured against network scales, offered traffic rates, and placements of routers and DAPs. For the small-scale scenario (350 SMs, 2 routers and 1 DAP), the simulations show that the system performs with a received packet ratio of 100% for a message frequency of 1 message per 4 hours. However, success rate decreases with increasing message frequency due to collisions in some central nodes. For a large-scale scenario (17181 SMs, multiple routers and DAPs), an overall success rate of 99.99% for a message frequency of 1 message per 4 hours is observed. In this case, it is noted that there are some isolated zones due to coverage gaps. Geographical distributions of packet success rate and hop-count are analyzed in order to determine the suitable number and placement of routers and DAPs that would result in an improved performance. However, there are three important limitations. First, an over-simplified free-space propagation channel model is assumed while real-life NANs are always deployed in a challenging outdoor environment with many factors that complicate the radio signal transmission. As a result, this assumption hinders the usefulness of results presented in [50]. Second, only message transmission reliability is measured. Transmission latency, which is one of the decisive performance metrics to be investigated in smart metering scenarios, is unfortunately not taken into consideration. Third, only conventional smart metering data is assumed in [50]. In fact, many advanced SG applications (e.g., DA, ADA, fault detection and restoration and so on) are emerging.

The works of [12, 51, 52] complement the work in [50] by investigating the performance of geographic routing protocols in practical NAN scenarios through extensive study on transmission reliability and latency of GPSR against channel conditions, network scales, and per-meter traffic in practical NAN scenarios specified by SG standards. The results demonstrate the effects of realistic channel models and increasing network loads introduced by emerging SG applications to the system performance of NANs. However, since geographic distance cannot capture wireless channel conditions, the major flaw of GEO protocols is that the selection of next hop merely based on geographic distance may lead to void areas. Even though GPSR attempts to resolve this issue by having alternative forwarding mechanisms to go around the voids, e.g., the perimeter mode, lengthened routing paths may waste channel resource and thus degrade system performance. Therefore, in the NAN context, the performance of location-based versus self-organizing coordinate system protocols is needed.

RPL versus GPSR

When comparing between RPL and GPSR, RPL possesses many advanced features (OF to capture channel dynamics, self-organizing coordinate to route traffic and so on). Further it requires heavy signaling to gauge link/network conditions and to propagate information that is necessary to construct and maintain the routing tree properly. Unless there is a mechanism that can efficiently control the signaling message broadcast procedure, significant overheads required by RPL could potentially degrade network performance. Routing fluctuation due to frequent changes in estimated link/path quality could be another issue with RPL. GEO, on the other hand, is very simple and truly distributed. It fully exploits the location information that is naturally available in NANs. However, to ensure routing around void areas, GPSR's perimeter mode can also lengthen routing paths, waste channel resource and thus degrade system performance.

In [16], the operation and performance of GPSR and RPL in NAN scenarios are compared. Extensive simulations are carried out to identify the advantages and disadvantages of each algorithm. Preliminary results in [16] demonstrate that RPL performs better than GPSR, however, the former requires a signaling mechanism and extra overhead for link quality estimation and a higher computation complexity for graph maintenance and path determination. An extension of this work is presented in [13, 17, 53]. Specifically, RPL is extended with the Proactive Parent Switching (PPS) algorithm that allows for preemptive parent switching based on link reliability. Extensive simulation results reveal that RPL offers higher transmission reliability and lower delays than GPSR in all scenarios of interest that are characterized by different channel conditions, traffic loads and network sizes. Moreover, under the consideration of multiple node failures, PPS can effectively improve network resilience since it can adaptively reroute packets over multiple alternative paths. Consequently, the results indicate that RPL with PPS is a very promising routing protocol for NAN communications. However, RPL does impose extra requirements on network signaling overheads, memory and computation capability of network devices since it needs to estimate link quality, maintain neighbor information and the routing tree structure. Given these results, the remainder of this thesis will focus on RPL as the chosen routing protocol for the SG NAN. In particular, examining network performance with many advanced features in an attempt to ensure not only reliability and throughput but also QoS differentiation for the numerous NAN traffic classes.

2.3 RPL

2.3.1 Detailed Description

RPL belongs to the self-organizing coordinate system routing class that constructs a viable coordinate system based on communication distance rather than the geographic distance used in location-based routing. RPL's key concept is the destination oriented directed acyclic graph (DODAG), a tree structure that specifies the routing paths between the root and the remaining nodes. The root is typically a gateway that acts as a common transit point that bridges every node and a backbone network [54].

Then, each node in the DODAG is assigned a rank that represents the cost of reaching the root as per the OF. The OF is designed to guide traffic to the root over paths that minimize a particular routing metric, such as hop count or ETX. A list of possible metrics that could be used for the OF in RPL is presented in [55]. The rank of a given node is calculated based on the ranks of its neighbors, the cost to reach each of these neighbors and other routing metrics. Initially, the DODAG root starts sending out DAG information option (DIO) messages with a predefined lowest rank indicating that it is the traffic sink. Upon receiving a DIO, each node calculates its own rank based on information carried in the message and its local state. Each DIO contains information about the DODAG identification, the rank of the broadcasting node, parameters specifying the OF and so on. DIO messages are periodically broadcasted from each node, triggered by the trickle timer. In this way, DIO messages are gradually propagated from the root down to the most distant nodes and thereby help create a DODAG representing the physical network. For a given node, any neighbor with a lower rank is considered as a parent. When a node receives a packet destined to the root, it forwards the packet to its preferred parent. This results in the most cost-effective path to the root for the selected OF. In case no parent is available, the node can forward the packet to a sibling (a neighboring node equally ranked as the node itself).

In order to control and limit signaling overhead, the duration of DIO broadcasts is doubled after each trickle timer expiration. The smallest interval between two consecutive DIOs is denoted by $I_{\min}$, and the number of times $I_{\min}$ can be doubled before maintaining a constant rate is denoted by I_{doubling}, so $I_{\max} = I_{\min} \times 2^{I_{\text{doubling}}}$. After any event that causes a change in the DODAG structure (parent node unreachable, new parent selection, new DAG sequence number, etc.), the timer is reset to $I_{\min}$.
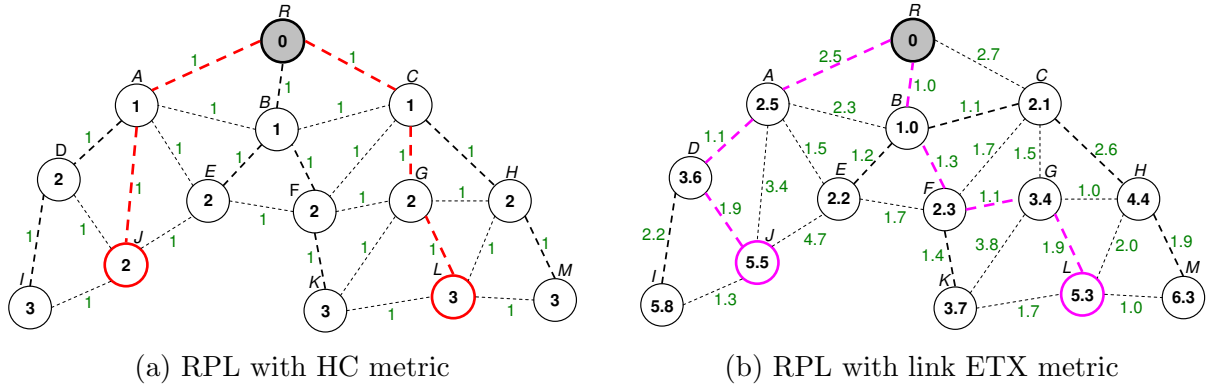
(a) RPL with HC metric   (b) RPL with link ETX metric

Figure 2.2   RPL DODAGs with different OFs

For illustrative purposes, Figs. 2.2a and 2.2b show DODAGs constructed over the sample physical wireless network with hop count and ETX as routing metrics, respectively. In the first case, Fig. 2.2a, every wireless link connecting two neighboring nodes (denoted by a dashed line) is simply assigned with equal cost of "1" (hop) and the rank of each node is equal to the total number of hops required to reach the root starting from the node itself. Paths from each node to the root are denoted by thick dashed lines. For example, traffic from node J may follow different paths to root node R as can be seen in Fig. 2.2a. However, using the DODAG and the aforementioned forwarding rule, J sends its packets to A which in turn forwards to R. This is the lowest-cost (i.e., 2-hop) path from A to R. Another example is the 3-hop path from L: $L \rightarrow G \rightarrow C \rightarrow R$.

In the second case, Fig. 2.2b, hop count is replaced by ETX, a measure of the quality of the wireless link between two nodes. By definition, ETX is the number of expected packet transmissions necessary for error-less reception at the intended receiver. An ETX of one indicates a perfect transmission medium, whereas an ETX of infinity represents a completely non-functional link. For example, if it took n transmissions to successfully deliver m packets, the ETX of the link is $\frac{n}{m}$ ($n \geq m$). Due to varying characteristics of the transmission medium, ETX may vary widely from one link to another. As illustrated in Fig. 2.2b, selected paths for traffic originating from J and L are $J \rightarrow D \rightarrow A \rightarrow R$ (5.5 transmissions) and $L \rightarrow G \rightarrow F \rightarrow B \rightarrow R$ (5.3 transmissions), respectively. By using ETX to reflect radio communication cost rather than simple hop count, this DODAG is expected to result in better system performance.

2.3.2 Areas of Interest

As explored in Section 2.2.2, RPL is a promising routing protocol for the NAN. However, the NAN is not only responsible for providing connectivity for a vast number of devices but also meeting the varying QoS requirements of different types of SG applications. Alarm notifications and control signals for critical missions (e.g, fault detection, distribution grid protection and restoration, etc.) require the latency measured in milliseconds and the consequence of failing to deliver such information on time can be catastrophic. Periodic and regular activities (e.g., energy metering, scheduled software/firmware updating, etc.), on the other hand, require reliable communications and can tolerate the latency of a few seconds or minutes [19, 20].

With that in mind, characterizing the performance requirements of various SG applications is important in order to understand which communications technologies and applications can be successfully paired [18]. Besides, in order to enable efficient prioritization of certain applications that have critical requirements, the communications network must be able to differentiate and provision different QoS requirements. Furthermore, existing solutions related to QoS differentiation may need to be revisited to cater for SG traffic because the traffic generated by SG applications will likely be quite different from that generated by traditional web browsing, downloading, or streaming applications in use today. In particular, the SGCN is expected to carry a mix of both periodic and critical traffic generated and distributed across different network segments. Further, the number, type and proportion of traffic classes will affect the complexity and efficiency of any devised resource allocation scheme. Thus, research is needed to allow for a more seamless administration of all anticipated SG traffic types [18, 19]. One potential solution could be RPL [54] using multiple network graphs constructed with different OFs corresponding to different traffic classes. Therefore, Chapter 3 will focus on RPL extensions that enable QoS differentiation through not only multiple instances of RPL, but also a cross-layered RPL extension that allows for channel access prioritization.

Chapter 3

Quality-of-Service (QoS) Supports for NANs

This chapter investigates the QoS requirements of various current and emerging SG applications. Focusing on the AMI application, a key feature of the NAN, two representative traffic classes are chosen, namely critical and periodic AMI traffic. Based on these two chosen converge-cast traffic profiles, QoS enabling extensions are presented for RPL at not only the network layer, but also the MAC layer. Then, based on these extensions, two QoS specific variants of RPL are presented for further study.

3.1 QoS Requirements in the SGCN

The SGCN is designed for large-scale emerging SG industrial applications. Thus, its anticipated traffic is likely quite different from that generated by commercial and enterprise communications networks in use today. Specifically, the SGCN has to be robust and secure. High network availability is critical along with predictable sub-second convergence for any failures. The network should possess a degree of fault tolerance for increased resiliency and have the ability to self-recover. Further, the network should support a secure end-to-end transport layer ensuring confidentiality, integrity and data privacy in order to meet the North American Electric Reliability Corporation-Critical Infrastructure Protection regulatory requirements [19, 56]. However, specific requirements vary based on the nature and objectives of the deployed SG application. For example, critical information required for stable and reliable grid operation will be time sensitive and have stringent latency require-

ments. Moreover, even specific SG applications may require multiple priority settings based on grid operation context. For instance, the desired QoS differentiation for periodic meter reads will vary based on whether the grid is operating in a conventional manner, during an outage or with other active applications that need real-time information. Therefore, the SGCN is faced with two important QoS factors: (i) a wide range of latency, bandwidth, security and reliability requirements and (ii) the need for dynamic flow priority associations based on grid condition and operation [57]. In light of this, an in-depth description of anticipated SG applications, extracted from [19, 41, 42, 56–60], where applications are classified based on their network association, is presented below. Then, Table 3.1 summarizes SGCN traffic types and their respective bandwidth and latency requirements.

3.1.1 Home and AMI Networks

For Home and AMI networks, (i) uplink applications (consumer to control center) can range from periodic meter reads to failure notifications and (ii) downlink applications (control center to consumer) can allow for optimization of electricity usage. Examples include:

Smart Metering & Advanced Metering Infrastructure (AMI) applications monitor electricity usage. In the HAN, home device electricity usage, typically a few kbps per device, is instantaneously transferred to the SM with a delay of about 2 to 15 seconds [41, 42, 58]. Consequently, home electricity usage can be optimized and overall home power consumption reduced. In the NAN, aggregate energy consumption information is transmitted by each home's SM periodically. The associated traffic is predictable and has long latency requirements. For conventional meter readings, only basic power use information is considered and thus the required data rate is a few bps per SM, with latency of about 2 to 15 seconds. Further, only medium reliability is required but high security is still necessary [57]. However, for advanced applications (e.g., power quality monitoring, ADA, etc.), many other parameters (e.g., active and reactive power, phase and frequency) are collected at much higher frequencies. Therefore, each meter will require higher data transmission rate and more stringent delay [56, 58]. For instance, for critical and priority AMI data, based on grid operating conditions, the delay allowance drops to 250 milliseconds and 300 milliseconds, respectively [41, 42, 60].

Outage Management Systems (OMSs) enable the required fast outage (e.g., short circuits, failures at power stations and damage in transmission and/or distribution lines [61]) detection and recovery, by predicting outage location, providing outage analysis and allowing for service restoration [62]. Moreover, the OMS can be enhanced with the inclusion of near real-time data exchanged between SMs and control centers. With this integration, SMs can act as a trip wire to indicate loss of power at an endpoint. Thus, they can be programmed to automatically give a "last gasp" message to indicate their power loss, thereby providing valuable information for pin-pointing the origins of the outage [63]. Additionally, with this notification system, utilities can forego the extra manpower required for accurate outage reports and analysis. As outage management is a critical SG function, it falls under the critical AMI setting and requires latency within the 250-millisecond range to ensure grid reliability.

Demand Response (DR) allows utilities to communicate with home devices (e.g., load controllers, smart thermostats and home energy consoles) in an attempt to reduce or shift power use during peak demand periods and thereby mitigate the need for rolling blackouts. With direct load control, this power usage shift can be triggered by a simple switch-off command to an appliance and thus its bandwidth requirement is a few tens of kbps [58]. Its latency ranges from as little as 500 milliseconds (e.g., for mission-critical control messages) up to several minutes (e.g., for load balancing management) [56, 58]. Furthermore, customers can participate with demand pricing by opting for dynamic power pricing (e.g., nodal market's power price will vary every few minutes). For example, a water heater could use current market conditions to decide when to run or remain idle. The exact format of this information exchange (i.e., centralized or selective data exchange) is currently unknown, but it is expected that individual nodal price updates will be small, perhaps 1400 bytes in size.

3.1.2 Distribution Network

Distribution network applications are mainly employed for failure detection or to optimize electricity distribution, utility assets and even workforce access. Examples include:

Fault Location, Isolation and Restoration (FLIR) restores the grid in the event of failures (e.g., lightning strike, circuit breakers trips, etc.). High speed protection information requires 8 to 10 milliseconds of delay. Breaker reclosures, lockout functions

and many transformer protection and control applications need 16 milliseconds. Finally, some lower priority protection and control applications can tolerate latencies of up to 500 milliseconds and 1 second [60]. Further, the primary factors for FLIR's bandwidth usage include the circuit complexity and number of communication steps involved before the fault can be isolated. This translates to a bandwidth requirement typically ranging from 10 kbps to 30 kbps [64].

Distribution Automation (DA) deals with volt/var and power quality optimization on the distribution grid. Electricity flow from utilities to consumers is optimized in order to enhance power delivery's efficiency and reliability. Generally, wide-spread inclusion of DA is expensive but it becomes more important in scenarios with DER. This service may generate from 2 to 5 Mbps of traffic and require 25 to 100 milliseconds of delay bound [65]. Further, high security and reliability are necessary [41, 42, 57].

Asset Management predictably and pro-actively gathers and analyzes non-operational data for potential asset failures. It offers management, automation, tracking, and optimization of the work order process, field crew scheduling and field assets [61]. With "smart" sensors and monitoring equipment that allow for communications, asset management systems can balance system performance, avert risk of failure and enhance reliability. Thus, primary bandwidth drivers are asset numbers along with the amount of non-operational monitoring data needed to predict asset health.

Workforce Access provides expert video, local device access and voice communications with field workers. It typically requires 250 kbps of bandwidth and 150 milliseconds of latency [19, 41, 42, 56]. Specifically, when considering the mobile workforce, latency requirement for enterprise data is around 250 milliseconds, while those for real-time video and push-to-talk Voice over Internet Protocol (VoIP) bearers/signaling are around 200 milliseconds and 175 to 200 milliseconds, respectively [60].

3.1.3 Substation Networks

In substation networks, substation automation systems (SAS) are designed for monitoring, control and protection of substation devices. These applications perform actions based on collected real time data. Therefore, communications is critical and should be highly reliable, scalable, secure and cost-effective [61]. As for inter-substation communications,

emerging applications such as DER and DA rely on communications with strict latency requirements from 12 to 20 milliseconds [41, 42, 56]. Examples are presented below.

Wide area situational awareness (WASA) refers to a set of technologies designed to improve power system monitoring across vast geographic areas and thereby efficiently respond to power system disturbances and cascading blackouts. One primary measurement technology, synchrophasors, have varying levels of latency requirements as well as stringent reliability of approximately 99.99995% [58]. For real-time monitoring and control, latency requirements range from 20 to 200 milliseconds. Specifically, estimates range from 60 milliseconds for measurements, 100 milliseconds for phasor measurement units (PMUs) clock synchronization and 500 milliseconds for PMU data. For post-event, historical data, low latency is nonessential [41, 42, 58, 66]. The required bandwidth is between 600 kbps and 1500 kbps and its main factors are the number of PMUs, word length, number of samples and frequency [41, 42, 56, 58]. Additionally, transmission lines monitoring is crucial for detecting icing, overheating and lightning strikes. In this case, the monitoring scheme includes deploying WSNs to gather line condition information. However, communications requirement specifics vary based on the network model, size and preferred communication technology [61]. Furthermore, substation surveillance applications are proposed for enhanced security. These applications can tolerate latencies of a few seconds [56] but require high bandwidths of up to a few Mbps, especially for video surveillance, and the primary factors for bandwidth usage are the number of cameras and the video's resolution.

Substation Supervisory Control & Data Acquisition (SCADA) considers traffic generated when a master periodically polls substation IEDs. The required bandwidth depends on the number of polled devices and is forecasted to be around 10 to 30 kbps. The latency requirement is typically from 2 to 4 seconds [19, 56]. However, under certain grid conditions, latency requirements are more stringent. For instance, load shedding for underfrequency has a delay allowance of only 10 milliseconds, SCADA critical measurements for poll response require 100 milliseconds, most distribution applications require 250 milliseconds. In the second range, SCADA applications include image files, fault recorders, medium speed monitoring and control information, low speed observation and measurement information, text strings, audio and video data streams [60]. Additionally, high security and reliability are required [57].

Traffic Type	Traffic Regularity & Data Rate	Latency
HOME AND AMI		
In-home Communications	Regular/on-demand, A few kbps/device	$2 \sim 15$ s
Meter Reads	Regular/on-demand, A few bps $\sim$ kbps/meter	$2 \sim 15$ s, 100's of ms[*]
Connects & Disconnections	Occasional, Very low rate	100's ms[†], Long[‡]
Outage Management	Occasional, Low rate	Near real-time (10's of ms)
Demand Response (DR)	Occasional/on-demand, 10's of kbps	500 ms[II], several minutes[♮]
Power Trading Information	Periodical, Low rate	10's of seconds
DISTRIBUTION		
FLIR	Event-triggered, $10 \sim 30$ kbps	Real-time
Distribution Automation	Periodical, A few Mbps	$25 \sim 100$ ms
Event Notification Signals	Occasional/event-triggered, Burst of data	Near real-time
Asset Management	Periodical/on-demand, Variable rates	Variable latencies
Workforce Access	Occasional, 250 kbps or higher	150 ms or lower
SUBSTATION		
Synchrophasor	Occasional/on-demand, $600 \sim 1500$ kbps	$20 \sim 200$ ms[§], Long[♭]
SCADA	Polling, $10 \sim 30$ kbps	$2 \sim 4$ s
Inter-substation	Regular, Variable rate	$12 \sim 20$ ms
Site Surveillance	Periodical/event-triggered, A few Mbps	A few seconds

[*]advanced applications, [†]fast responses to grid conditions, [‡]customer moving,
[II]mission-critical, [♮]load balancing, [§]monitoring and control, [♭]historical data

Table 3.1   SGCN traffic types and their required QoSs.

3.2 Representative AMI Traffic Classes

Given the various types of SGCN traffic and their respective bandwidth and latency require-
ments, as shown in Table 3.1, and the importance of the NAN, as described in Section 2.2.1,
this work focuses on the SG NAN traffic associated with AMI applications. In particular,
the converge-cast nature of NAN traffic is emphasized due to its challenging communica-
tions requirements with regards to reliability, latency, scalability, and security. Specifically,
as shown in [57] and Section 3.1.1, the application traffic associated with smart metering
belongs to two distinct traffic classes:

Critical AMI traffic Higher priority alert messages with smaller packet sizes, high reli-
ability, high security and stringent latency requirements of at most 200 milliseconds.

Periodic AMI traffic Lower priority periodic meter reads with larger packet sizes, high
security, and medium reliability but can tolerate latency (up to a few seconds of
delay) and jitter.

Therefore, for the remainder of this thesis, only the above mentioned two traffic classes are considered. Further, the traffic classes are considered only in the uplink direction, and thereby correspond to converge-cast traffic profiles. Finally, as RPL has been selected as the most promising network routing protocol in the context of the SG NAN, the remainder of this chapter will focus on methods of incorporating QoS differentiation into the RPL framework.

3.3 RPL QoS Differentiation

Generally, application-based QoS and traffic priority requirements are addressed through queue scheduling mechanisms at the MAC layer. For instance, based on traffic class requirements, the queuing algorithm would no longer be a simple First In First Out (FIFO) queue but a more complex structure where processing favors higher priority packets. For example, fair queuing scheduling mechanisms include Weighted-Round-Robin (WRR) and Weighted Fair Queuing (WFQ) [67]. Additionally, priority can be incorporated at the MAC layer through alterations to the Carrier Sense Multiple Access Collision Avoidance (CSMA/CA) backoff mechanism for channel contention. Specifically, instead of allowing all packets equiprobable channel access, the contention window can be reduced for higher priority packets thereby increasing their channel access probability [68]. However, these aforementioned methods only consider QoS at the wireless channel access level.

With RPL, QoS can be incorporated at the network layer through multiple instances of the DODAG network graph. Since the DODAG is built based on an OF, traffic differentiation can be incorporated through correlation with differing OFs. Thus, each traffic type would be associated with a different OFs and consequently will be routed along a different RPL network graph instance. In particular, [69, 70] proposes a cross layer QoS mechanism that incorporates a priority queue with multiple instances of RPL. However, the focus is on the MAC level QoS differentiation. Moreover, the RPL instances are both based on the same OF but generate distinct DODAGs due to partitioning of the actual physical network (i.e., nodes are classified as regular or alarm, regular nodes are sources and routers but alarm nodes are only sources). With that in mind, this work expands on the concept of QoS through multiple RPL instances by also considering the effect of traffic differentiation at the *network* layer. Specifically, the OF chosen by each traffic class must be correlated with a given desired application traffic goal. Then, to ensure distinct network

graphs per OF, the cross-correlation between OFs must be minimized. This applies mainly to OFs based on similar estimation characteristics. For example, if channel links are estimated through probing messages, any OF derived from the statistics of probing messages will be correlated and thus the generated network graphs may not be sufficiently distinct. Additionally, since each RPL instance generates packets independently and can differ in next hop choice, this creates an implicit priority queue within each node (i.e., each node has limited resources and their usage is weighted by each DODAG's operations). Thus, to ensure that the effect of only multiple RPL instances is considered in simulations, any MAC level prioritization should focus of channel access and not queue scheduling. Given these concerns, the proposed RPL QoS mechanisms consist of (i) MAC layer QoS and (ii) Network-layer QoS as discussed next.

3.3.1 Medium Access Control (MAC) Layer QoS

Given the typical implementation of the SGCN (as chosen in [12, 13]), for the communications modules built into each SM, IEEE 802.11b physical (PHY) and MAC layers are selected. The PHY layer operates in the 2.4 GHz frequency band and uses direct sequence spread spectrum (DSSS) technology. Adaptive modulation and channel coding (AMC) can support multiple data transmission rates, i.e., 1.0, 2.0, 5.5, or 11.0 Mbps, depending on channel conditions. The MAC layer employs the CSMA/CA mechanism. A node with a new packet to transmit will continuously sense the channel in the hope that it remains idle for a time interval equal to a distributed coordination function interframe spacing (DIFS). When the channel is measured idle for a DIFS, the node backs off for a random period of time. After expiry of the back-off timer, the node transmits if the channel is still idle. This back-off mechanism attempts to minimize the probability of transmission collision. In addition, to avoid channel capture, a node must wait a random back-off time between two consecutive new packet transmissions, even if the medium is sensed idle in the DIFS time.

For each packet transmission, the back-off time is X times the contention window slot time (ST) where X is picked uniformly in $\{0, 1, \ldots, CW_n\}$ where CW_n represents the contention window which is a function of the number of failed packet transmissions. At the first transmission attempt, CW_0 is set to equal the minimum contention window $CW_{\min}$. Binary exponential back-off is assumed: after each unsuccessful transmission, the contention window is doubled, up to a maximum value $CW_{\max}$. In other words, the
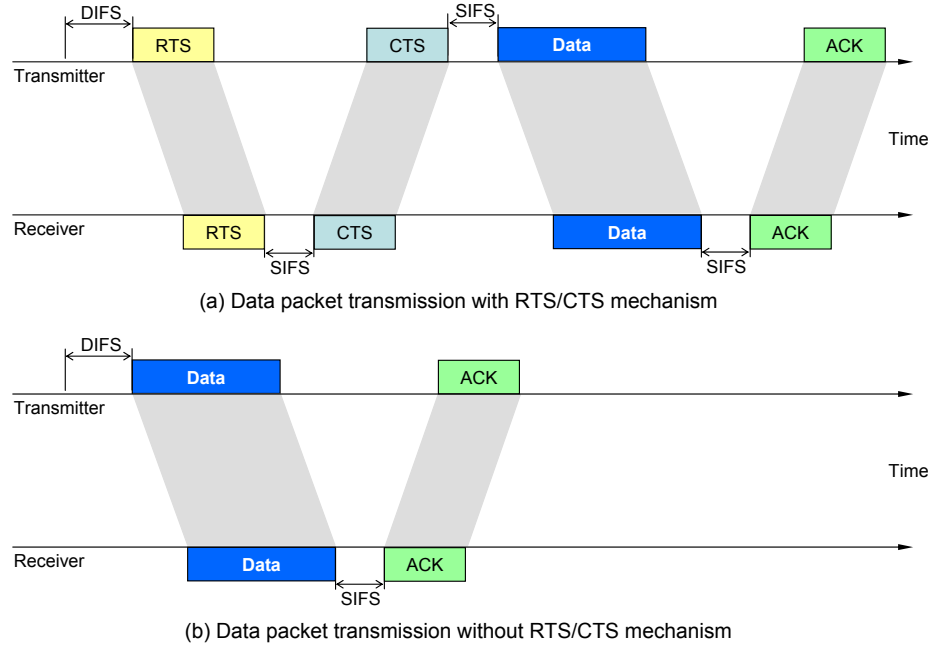
(a) Data packet transmission with RTS/CTS mechanism

(b) Data packet transmission without RTS/CTS mechanism

Figure 3.1   The timing diagram showing basic operations of IEEE 802.11 CSMA/CA with and without RTS/CTS

contention window for the n-th trial and $X(n)$ are,

$$CW_n = \min\{(CW_{\min} + 1) \times 2^n - 1, CW_{\max}\},$$
$$X(n) \sim \mathcal{U}(0, CW_n)$$

(3.1)

respectively. The back-off time counter is decremented and a node only transmits when the back-off time reaches zero. The receiver sends an ACK signal, after a period of time called the short interframe spacing (SIFS), to signal successful packet reception. If the transmitting node does not receive the ACK, it reschedules packet transmission according to the given back-off rules. Request-to-send (RTS)/Clear-to-send(CTS) mechanism is optional. A timing diagram illustrating the transmission of a data packet using IEEE 802.11 CSMA/CA with RTS/CTS is given in Fig. 3.1. More details on IEEE 802.11 PHY and MAC layers can be found in [71].

Further, traffic prioritization can be achieved by altering the conventional backoff mechanism. Specifically, the random backoff exponent ranges, i.e., $CW_{\min}$ and $CW_{\max}$, in CSMA/CA are altered based on the traffic class. Therefore, given a priority class p, the priority backoff for the n-th transmission is $X(n, p)$ times the contention window ST. Specif-

ically, the contention window for the n-th trial, $CW(n, p)$, and $X(n)$ are,

$$CW(n, p) = \min\{(CW_{\min}(p) + 1) \times 2^n - 1, CW_{\max}(p)\},$$
$$X(n, p) \sim \mathcal{U}(0, CW(n, p))$$

$$(3.2)$$

respectively, where the choice of $CW_{\min}(p)$ and $CW_{\max}(p)$ alters the channel access probability. In particular, a small contention window size implies shorter random backoff times and thereby increases channel access probability. Therefore, higher priority traffic is associated with shorter backoff periods and vice versa.

3.3.2 Network-Layer QoS

At the network layer, routing over different DODAGs allows for traffic differentiation. For instance, to achieve high reliability, the chosen OF should incorporate accurate network state information and reliable links. To achieve better end-to-end latency, shortest paths might be optimal. However, in a wireless network with channel attenuation and shadowing, this might not necessarily be the case. Furthermore, one-to-one relationships between OFs and traffic classes are unlikely since OFs are based upon some network resource and traffic classes are generally based upon multiple requirements. In this case, since no additional probing control signaling is employed, all estimated metrics would be based upon successful data message transmissions and thus correlated. Therefore, the choice of Hop Count (HC) and link ETX helps ensure minimal overlap between the two DODAG instances. As for the association between OF and traffic class, HC and link ETX are considered, as discussed below.

HC

HC poses low overhead and is simple to implement. As an example, Fig. 3.2a illustrates a DODAG created based upon a HC routing metric. Specifically, since the metric is HC, all graph edges have a weight of 1, i.e., 1 hop, and the rank of the nodes is depicted in the node. All nodes receive DIO messages, join the DODAG and select parent sets based on their relative ranks. Each node's preferred parent is chosen randomly from its parent set with minimal rank values. Uplink traffic is forwarded hop-by-hop through preferred parents until the root is reached. For instance, traffic from node J may follow different

paths to root node R. However, using the DODAG and the mentioned forwarding rule, J sends its packets to A which then finally forwards them to R. This is the smallest-cost (i.e., 2-hop) path from A to R. Another example is the 3-hop path from $L : L \rightarrow G \rightarrow C \rightarrow R$ [3 hops]. Further, with reliable links, this metric will lead to shortest paths, lower delay and energy consumption. However, with poor links, the choice of the next hop as the neighbor closest to the destination will lead to higher channel attenuation (longer links) and thereby degrade performance. In such a case, latency will increase due to increased re-transmissions. Therefore, HC as a metric should be considered for delay tolerant, medium reliability and low priority traffic.
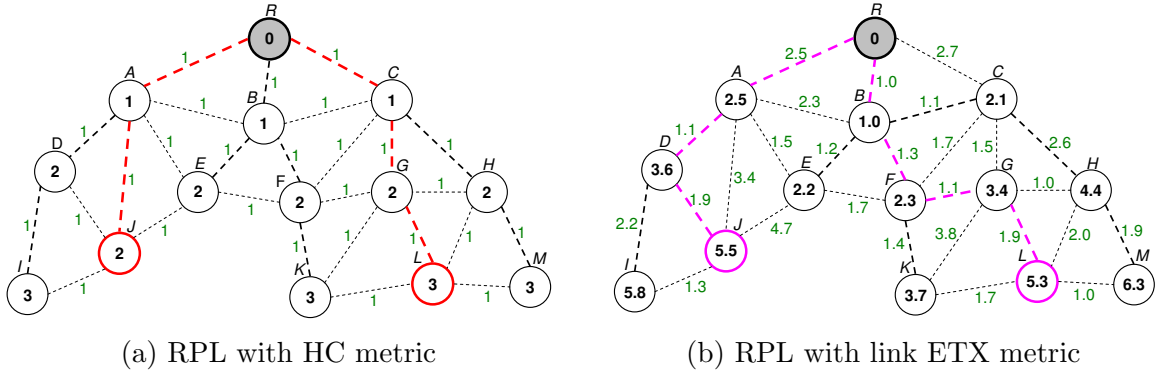

(a) RPL with HC metric (b) RPL with link ETX metric

Figure 3.2 RPL network graphs

Link ETX

Link ETX, a link-quality-based routing metric, requires overhead for link quality measurements but can accurately translate the physical network into the logical network graph. In particular, to reduce overhead, this implementation of link ETX considers the two-way packet flow over a single link $\mathcal{L}_{i,j}$ as data transmissions over link $\mathcal{L}_{i \rightarrow j}$ and the corresponding acknowledgment messages over link $\mathcal{L}_{j \rightarrow i}$. Specifically, link ETX is calculated as,

$$\mathbf{ETX_{i,j}} = \frac{|\mathbf{N_{tx_{data}}}|}{|\mathbf{N_{rx_{data}}}|} \cdot \frac{|\mathbf{N_{tx_{ACK}}}|}{|\mathbf{N_{rx_{ACK}}}|} = \frac{|\mathbf{N_{tx_{data}}}|}{|\mathbf{N_{rx_{ACK}}}|}. \tag{3.3}$$

where $|\mathbf{N_{tx_{data}}}|$, $|\mathbf{N_{rx_{data}}}|$, $|\mathbf{N_{tx_{ACK}}}|$, and $|\mathbf{N_{rx_{ACK}}}|$ are the number of transmitted data, received data, transmitted acknowledgment and received acknowledgment messages, respectively. As an illustrative example, Fig. 3.2b shows a DODAG constructed over a wireless

network using the link ETX metric. Since this OF does not pose additional overhead but does accurately represent the physical network link states, it should be considered for high priority traffic with stringent latency requirements and high reliability. Additionally, it is noted that link ETX is computed from data messages generated within its associated DODAG. For instance, for one RPL instance with multiple traffic profiles, link ETX will be calculated based on all data messages. However, for multiple RPL instances, link ETX will be calculated based only on data transmissions generated within the link ETX DODAG.

3.4 Proposed RPL Variants

To reiterate, RPL centers on the formation of a tree-based routing hierarchy, namely a DODAG. The nodes are ranked based upon an OF that represents some network criterion (latency, bandwidth, packet delivery ratio, etc.) which is then used for DODAG generation. Different ranking schemes can be used to generate *multiple separate logical* DODAGs for the *same physical* network. Since the OFs that rank the nodes are generally resource-oriented, they can be associated with application traffic goals. In this work, the focus is given to QoS through multiple RPL instances. In particular, how distinct OFs over the same physical network can provide QoS traffic differentiation for multiple traffic classes. Therefore, for all subsequent QoS analysis, the protocols being compared are link-ETX based single instance RPL as well as RPL-M and RPL-M+, as described below.

3.4.1 RPL-M

For RPL-M, only *network* layer QoS differentiation is considered. As this thesis considered only two distinct traffic classes for smart metering applications, two separate DODAG instances are generated per traffic class. Then, given the characteristics of each class, the OF to traffic class associations are, (i) HC as the routing metric for periodic traffic, and (ii) link ETX as the routing metric for critical traffic.

3.4.2 RPL-M+

For RPL-M+, a cross-layered QoS mechanism is devised in which (i) RPL-M is employed to achieve network level QoS differentiation and, (ii) CSMA/CA based channel access prioritization is used to obtain MAC level QoS differentiation as well. As for the priority

settings for the MAC level CSMA/CA alterations, lower contention window bound values are used for critical traffic so as to allow for higher priority channel access. For simplicity, the default contention window minimum and maximum values were halved for the high priority traffic class. Additionally, for the network level, the same settings as RPL-M are used for the OF to traffic class associations.

3.4.3 Research Direction

As explored in Section 3.1, QoS requirements in the SG NAN context depend not only on traffic class requirements but also the current grid state (e.g., stable, cascading faults, etc.). With that in mind, any QoS investigations should consider study cases with varying grid state conditions. In particular, as this thesis focuses on the communications layer of the SG, distinct grid state conditions can be modeled by altering the distribution of traffic classes. For example, when power system faults occur, their associated critical messages will be sent. Thus, with higher concentration of critical messages, one can infer that the grid is experiencing increased faults. Additionally, as new SG applications emerge, the bandwidth requirements will inevitably increase. Therefore, subsequent QoS examinations will consider study cases where traffic distribution as well as total data rate are varied. Finally, as this thesis is intended to be of use for SG communications system designers and network engineers, a real-life deployment scenario, a microgrid, is considered to showcase the performance and achievable QoS differentiation of the aforementioned RPL-based protocols. Further details are presented in Chapter 4.

Chapter 4

Performance and Feasibility of QoS Differentiation in NANs

In order to obtain an in-depth understanding of protocol operation and to study the feasibility of standard RPL, RPL-M and RPL-M+ presented in Chapter 3, this chapter investigates network performance, in terms of packet delivery ratio and latency, for the three RPL variants. In particular, to determine the achievable QoS differentiation in the NAN setting, the data rate along with the relative composition of the representative traffic classes (critical and periodic) are varied to model increasing data offered load and varying grid conditions, respectively. In addition, two separate deployment scenarios are chosen, namely a random large-scale urban setting as well as a *real* small-scale rural deployment scenario corresponding to the community of Burwash Landing, Yukon, Canada.

4.1 Simulation Platform

Given the numerous available network simulators (e.g., OPNET, NS2, NS3, etc.), OM-NeT++ [72], a modularly designed discrete-event simulator, was chosen as it possesses many key features that make it a promising simulation platform for this work. In particular, it (i) is fully open-sourced, (ii) possesses a large number of protocols and models that are continually increasing, (iii) is built upon a C++ back-end that allows for easier class declarations and polymorphism, (iv) is bundled with debugging tools for ease of programming, (v) can run in either GUI or command line mode and finally (vi) allows for custom or parametrized network topologies through the NED language.
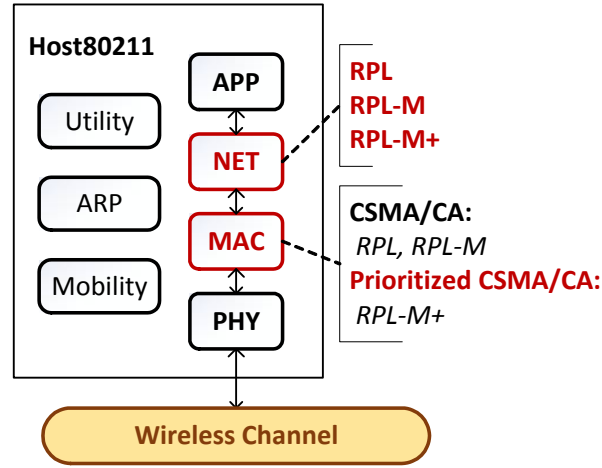
Figure 4.1 Communications module model for the host protocol stack (customized elements in red)

As the typical SG implementation described in Section 1.3.2 implies a IEEE 802.11 WiFi radio as the communications technology for the SG NAN, the MiXiM (mixed simulator) dependency library was chosen. Specifically, the MiXiM network node model for IEEE 802.11 is as shown in Fig. 4.1, where each sub-module represents layers of the protocol stack (APP, NET, MAC, PHY) as well as additional modules for mobility, address resolution and utility functions. It is important to note that even though MiXiM and OMNeT++ provide the underlying communication models (channel, radio, node, network, etc.) and event scheduling structures, in terms of routing protocols, only basic protocols such as flooding are provided. Thus, they lack the models for state-of-the-art network routing protocols such as RPL and its proposed variants. Therefore, custom implementations, inherited from the available open-source framework, were developed and tested in this thesis to model and simulate the chosen promising routing protocols for the SG NAN. Specifically, a new network layer sub-module was designed for each routing protocol. As C++ allows for inheritance, each custom layer is derived from the base layers provided by MiXiM. Additionally, modular programming was employed so as to reduce complexity. In particular, (i) RPL's message structure, (ii) message handling functions, (iii) network graph sub-modules along with their creation and maintenance functions, (iv) algorithmic functions to determine and update chosen routing metrics, as well as (v) some additional utility functions were developed. Additionally, as RPL-M+ is a cross-layered protocol with MAC alterations, the MAC layer of the host model was updated to reflect the changes to
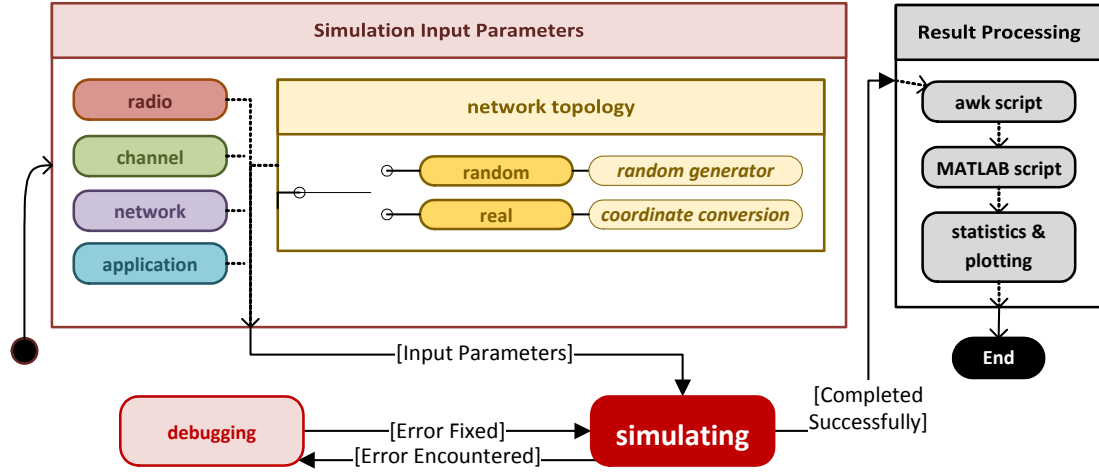
Figure 4.2 Simulation workflow

the CSMA/CA protocol. Finally, additional integration features were devised so as to allow for ease of switching between different protocols from the simulation initialization interface (i.e., alter the models with a simulation parameter and not through code re-compilation).

Then, for the workflow, as shown in Fig. 4.2, once the custom simulation implementation is operational, simulation input parameters have to be calculated and set based on not only the network deployment scenario but also the simulation study cases. In particular, (i) network and application level parameters are related to the devised simulation study case as they set the data rate as well as the routing protocol, and (ii) radio, channel and network topology are based on the deployment scenario. Specifically, as this thesis considers not only a random topology but also a real one, there are two topology generation options. The first builds a random deployment given the desired number of nodes and the node density via a separate c program developed specifically for this purpose. The second translates latitude and longitude coordinates into Cartesian coordinates to model the real node geographical distribution, i.e., latitude/longitude coordinates were manually determined and converted to Cartesian coordinates through a conversion program. Once the input parameters are set, the simulation is run till successful completion with the potential to debug on errors. To process the raw results, custom developed awk and MATLAB script files designed to cater to the generated simulation output files are employed to produce datasets which can then be statistically evaluated and processed to generate the final results. Further details on the simulation setup are described in the following section.

General Lower Layer Characteristics		
PHY	Standard	IEEE 802.11b
	Frequency band	2.4 GHz
	Transmission rates	$\{1.0, 2.0, 5.5, 11.0\}$ Mbps
MAC	Standard	IEEE 802.11b
	RTS/CTS	Disabled
	ACK	Enabled (14 Bytes)
	Max. re-transmissions	7
	Back-off procedure	Binary exponential
	ST[*], SIFS[†], PIFS[‡], DIFS[Ⅱ], EIFS[§]	$20, 10, 30, 50, 364$ μs

[*]slot time , [†]short interframe spacing, [‡]point coordination function interframe spacing,
[Ⅱ]distributed coordination function interframe spacing $= 2 \times ST + SIFS$,
[§]extended interframe spacing $= SIFS + DIFS + $ Total ACK length/PHY header rate

Table 4.1   MAC and PHY layer specifications

4.2 Simulation Setup

4.2.1 Node Model

All nodes are assumed to be homogeneous except for the DAP which has an additional interface to communicate with the upper tier network (e.g., LTE backhaul). In this chapter, network node and SM are synonymous and refer to a digital power electric meter with communications capability and other smart features (e.g., data processing, computing, etc.). Each node has a radio communications module responsible for relaying sensor data (e.g., voltage, current, phase, energy consumption and so on) to the DAP (either directly or via other SMs using multi-hop paths). This means that each SM acts not only as a network end-device but also as a router to relay traffic for other SMs and form a mesh network. In order to ensure that the results obtained in this work are meaningful and applicable to real-life scenarios, parameters related to SM deployment scenarios and wireless channel characteristics specified by the National Institute of Standards and Technology (NIST) SG Priority Action Plan 2 [73] are taken into consideration.

4.2.2 PHY and MAC Layer Specifications

For the communications modules built into each SM, IEEE 802.11b PHY and MAC layers are selected. Simulation parameters related to these two layers are summarized in Table 4.1.

4.2.3 Wireless Channel Model

Following the specifications in [73], the wireless channel is modeled by path-loss (with path-loss exponent α) and log-normal shadowing X_σ (with standard deviation σ) as shown below:

$$P_\text{R}[\text{dBm}] = P_\text{T}[\text{dBm}] + 10\log_{10}\left[\frac{\lambda^2}{16\pi^2 d^\alpha}\right] - X_\sigma, \tag{4.1}$$

where P_T and P_R are the transmitted and received radio power, respectively; λ and d are the wavelength and the transmitter-receiver distance, respectively. Specifically, [73] recommends different values for α and σ based on the nature of the deployment scenario, i.e., rural, suburban, urban. Additionally, the density of SMs to DAP along with the average distance between SMs varies based on the chosen deployment scenario. Therefore, the values for the transmission range, network density and channel characteristics are chosen in accordance with [73] for each deployment scenario.

4.2.4 Traffic Model

Since SMs are deployed to support not only conventional SG applications (e.g., meter reading, power outage detection, DR and so on) but also emerging future applications (e.g., ADA, fault detection and restoration, electric vehicles and so forth), they are expected to handle an increasing volume of information exchanges. As a result, in this chapter, application (APP) data traffic generated by each node in the simulated NAN is swept over a wide range to gauge the performance of the NAN under different levels of offered load. In particular, APP data is generated periodically for each node at rate R_B [Bytes/s]. It is noted that, in this chapter, only uplink traffic (i.e., from nodes to the DAP) is considered since the communications in this direction is *converge-cast* in nature and more challenging in the NAN scenario, as compared to that of the downlink direction. Further, as described in Section 3.2, this chapter considers the application traffic associated with smart metering that belongs to two distinct traffic classes, namely critical (c) and periodic (p) AMI traffic, as described in Table 4.2.

Traffic Generation

Given that distinct traffic classes have varying characteristics and QoS requirements, their relative composition can alter overall network performance. Therefore, to model this be-

Traffic Characteristics	Critical Traffic	Periodic Traffic
Message Type	Alert messages	Periodic meter reads
Packet Size	Small packets 25 Bytes	Large packets 100 Bytes
Latency requirement	Delay sensitive $\mathcal{O}(10^2)$ ms	Delay tolerant $\geq \mathcal{O}(10^3)$ ms
Reliability requirement	High Reliability	Medium Reliability

Table 4.2   Representative AMI traffic classes

havior, the devised traffic model allows for not only the generation of multiple distinct traffic classes but can also vary their relative compositions. Specifically, the *total* node rate in Bytes/s, i.e., R_B [Bytes/s], is assumed *constant* for each simulated data rate (for ease of comparison between scenarios). Then, given $N_C = 2$ traffic classes, node rates $R_B(i)$ [Bytes/s] and $R_p(i)$ [packets/s] and finally $L(i)$ [Bytes] for traffic class i ($i = $ c, p), the node rates for each traffic class are determined as a fraction, p_i, of the total data generated at each node. Namely, for traffic class i,

$$R_B(i) = R_B \times p_i \quad [\text{Bytes/s}] \tag{4.2a}$$

$$R_p(i) = R_B(i) \times \frac{1}{L(i)} \quad [\text{packets/s}] \tag{4.2b}$$

where in order for (4.2a) and (4.2b) to hold, $\sum p_i$ must be equal to one. Thus, N_C controls the number of distinct traffic classes present and the p_i distribution controls their relative composition.

Traffic Composition

Given that QoS requirements depend not only on (i) a wide range of latency, bandwidth, security and reliability requirements but also (ii) the need for dynamic flow priority associations based on grid condition and operation [57], distinct grid conditions are considered. In particular, as the transmission of critical messages imply the occurrence of a critical event such as faults/errors, varying relative traffic compositions can model distinct grid conditions, as described below.

Traffic Distribution I examines the case where the node rate in *packets/s* for the two traffic classes are equivalent, i.e., $R_p(\text{c}) = R_p(\text{p})$. Further, as critical messages are shorter and occur at lower R_B frequency, this scenario is meant to model a moderate grid state where some alert messages are present. However, the grid is mainly

operating in a stable condition and the majority of traffic is associated with periodic meter reads.

Traffic Distribution II models the case where the node rate in *Bytes/s* for the two traffic classes are equivalent, i.e., $R_B(\text{c}) = R_B(\text{p})$. As critical messages are shorter, this scenario aims to model an extreme grid condition where critical messages are flooding the network, namely in the case of cascading failures that trigger the transmission of critical messages throughout a large segment of the network.

Effective Node Transmission Rate

For ease of discussion in the case of multiple traffic classes, (i.e., critical, c, and periodic, p, traffic classes), the effective node transmission rate is defined based on an equivalent, combined rate whose characteristics are,

$$L = L(\text{c}) + L(\text{p}) \quad [\text{Bytes}] \tag{4.3a}$$

$$R_B = R_B(\text{c}) + R_B(\text{p}) \quad [\text{Bytes/s}] \tag{4.3b}$$

$$R_p = \frac{R_B}{L} \quad [\text{packets/s}] \tag{4.3c}$$

where (4.3a) implies that the *combined* packet length, L, is the sum of the packet lengths of each traffic class. Therefore, all subsequent discussions will consider the effective node transmission rate such that the above mentioned characteristics are met. Further, as the equivalency is done at the byte level, for any number of traffic classes and any relative composition, all scenarios with the same node rate, R_B [Bytes/s], are directly comparable.

4.2.5 Routing Protocols of Interest

Three network routing protocols, namely RPL, RPL-M and RPL-M+ are considered for QoS based scenarios and are studied for the purpose of determining achievable QoS differentiation through multiple RPL instances. In particular, how distinct OFs over the same physical network can provide QoS traffic differentiation for multiple traffic classes in the SG NAN context. Protocol details are presented below.

RPL considers a single-instance built upon the link-ETX OF, as defined in Section 3.3.2, for the two traffic classes, i.e., routing is done over the same network graph.

Protocol	Traffic Class	Objective Function	CW_{min}	CW_{max}
RPL	Critical	Link ETX	31	1023
	Periodic		31	1023
RPL-M	Critical	Link ETX	31	1023
	Periodic	Hop Count	31	1023
RPL-M+	Critical	Link ETX	15	511
	Periodic	Hop Count	31	1023

Table 4.3   Routing protocol specifications

RPL-M generates two separate RPL instances for each traffic class, as discussed in Section 3.4, in order to investigate *network* layer QoS differentiation. Further, the OF to traffic class associations are, (i) HC as the routing metric for periodic traffic, and (ii) link ETX as the routing metric for critical traffic, as shown in Table 4.3.

RPL-M+ employs a cross-layered QoS mechanism such that RPL-M is extended with a CSMA/CA based channel access prioritization scheme at the MAC level, as discussed in Section 3.4. For simplicity, the default contention window minimum and maximum values were halved for the high priority traffic class. However, the same settings as RPL-M are used for the OF to traffic class associations, as shown in Table 4.3.

4.2.6 Network Deployment scenarios

Given that the SG NAN represents the distribution network of the SG, its specific deployment characteristics will vary based on the nature of its associated distribution grid. In particular, the disparity is mainly related to population density. For example, the number of nodes, the average distance between nodes, and even channel characteristics will differ between rural and urban settings. With that in mind, this chapter considers two deployment scenarios, as discussed below.

Random Urban Deployment

In an urban region, population density is high and by consequence, node (or SM) density is high. According to [73], urban SM density is approximately $\rho = 2000$ [nodes/km^2]. Further, channel parameters are higher so as to account for higher probabilities of obstructions and interference. In particular, the path-loss exponent and the shadowing variance are
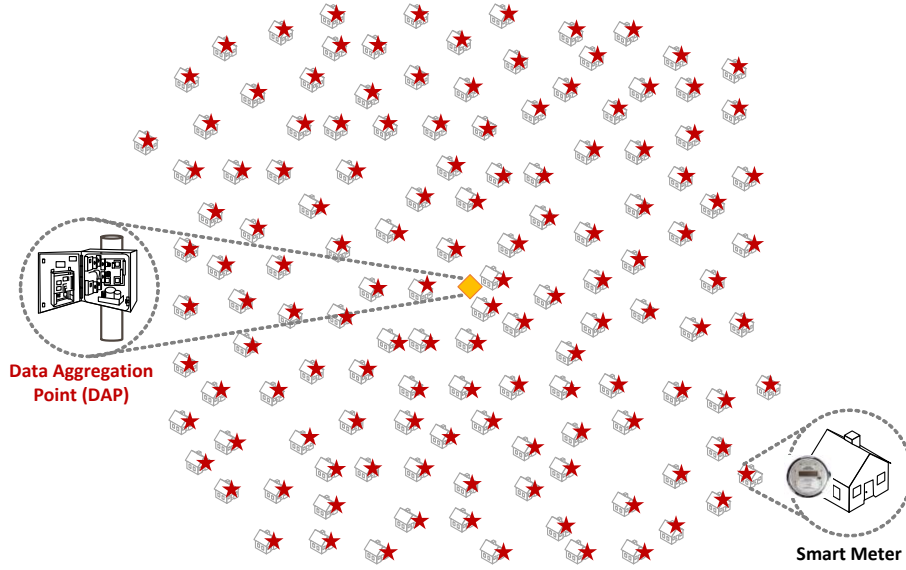
**Figure 4.3** Random urban deployment scenario (red stars are SMs, yellow rhombus is the DAP)

Deployment	Quality of Service	
Environment	Urban	Rural
Node density	$\rho = 2000$ nodes/km^2	$\rho = 40$ nodes/km^2
Transmission range	50 m	450 m
Node placement	uniformly random	Burwash Landing
Network size	1000 SMs and 1 DAP	80 SMs and 1 DAP
Path loss	$\alpha = 3.6$	$\alpha = 2.1$
Shadowing, lognormal	$\sigma = 7.4$ dB	$\sigma = 2.2$ dB

Table 4.4 Deployment scenarios

estimated to be 3.6 and 7.4 dB, respectively. Additionally, transmitted radio power P_T is chosen to have the communication range of approximately 50 m (suitable for urban density). Given these parameters, a large-scale random deployment scenarios was devised for QoS investigations such that the DAP is located at the network center, as shown in Fig. 4.3 and described in Table 4.4.
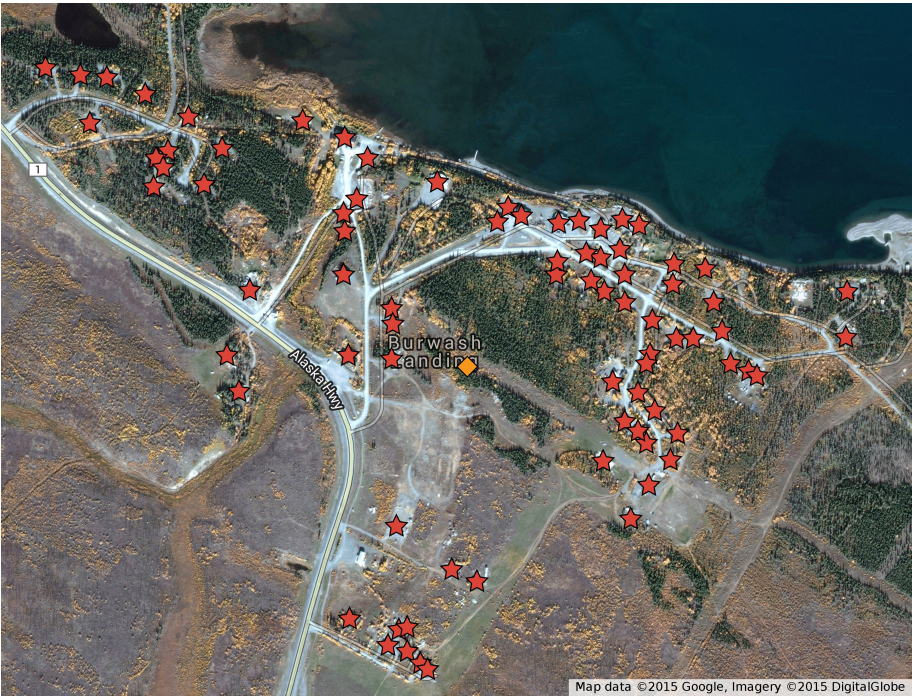
Rural Deployment - Burwash Landing, YK, CA

As one of the greatest challenge of the SG is providing its advantages to the grid at large as well as allowing for the incorporation of smaller smart distributed electricity systems
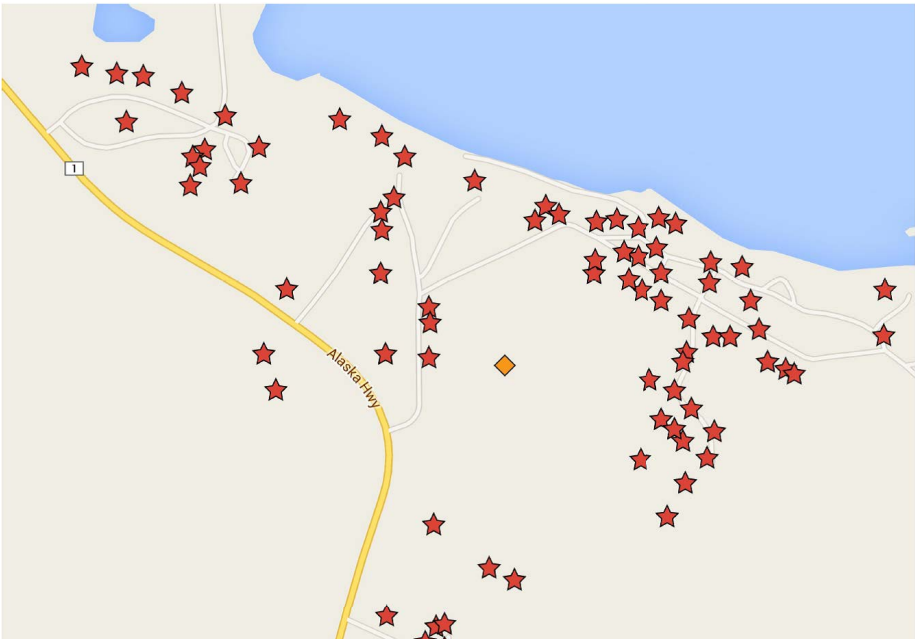
BurwashLanding

BurwashLanding.xlsx

◆ DAP
★ origin
★ 1
★ 2
★ 3
★ 4
★ 5
★ 6
★ 7
★ 8
★ 9
★ 10
★ 11
★ 12
★ 13
★ 14
★ 15
★ 16
★ 17
★ 18
★ 19
★ 20
★ 21
★ 22
★ 23

(b) Satellite view (red stars are SMs, yellow rhombus is the DAP)

Figure 4.4 Burwash Landing, Yukon, Canada - Rural deployment scenario

or microgrids, this chapter considers a realistic potential microgrid, namely the remote community of Burwash Landing, in the Yukon territory of Canada. In particular, node placement is modeled based on satellite map images of buildings within this town, as shown in Fig. 4.4. The DAP is assumed to be placed at the center to reduce the transmission range which is roughly estimated to be around 450 m. Even though this range is large, as the town is remote, channel conditions are much more favorable than in the urban scenario. In particular, the path-loss exponent and the shadowing variation, as estimated by [73], are 2.1 and 2.2 dB, respectively. Further, as the town encompasses only 80 buildings within a 2 km^2 region, SM density is roughly $\rho = 40$ [nodes/km^2]. Additionally, simulations consider only converge-cast communications *within* the microgrid. Further details are presented in Table 4.4.

4.3 Network Performance Metrics

The performance of the network is mainly examined via packet delivery ratio and packet transmission delay, as described below. Additionally, in order to have an in-depth understanding of each algorithm, some other parameters are also investigated, i.e., hop count, average transmission delay per node, etc.

4.3.1 Packet Delivery Ratio (PDR)

PDR is the percentage of data packets that are received and decoded successfully by the DAP. It is calculated by the following equation:

$$\text{PDR} = \frac{|\mathbf{N}_{\text{rx}}|}{|\mathbf{N}_{\text{tx}}|}, \tag{4.4}$$

where $\mathbf{N}_{\text{tx}}$ is the set of data packets generated and sent by network nodes. In each simulation setting, $|\mathbf{N}_{\text{tx}}|$ is chosen to be 100000 for statistical measurement of PDR. Further, end-to-end PDR is calculated for the entire simulation as well as per node for more detailed investigations.

4.3.2 Packet Transmission Delay

Transmission delay D_p of data packet p accounts for the duration from the time when p is ready for the transmission at the original source until p is received and decoded correctly at its final destination. D_p includes various components: the time for sending and receiving control messages (T_p^{RTS}, T_p^{CTS}, T_p^{ACK}) and packet p itself (T_p^{DATA}), back-off time (T_{BO}) and interframe spacings (T_{IFS}). In other words, its calculation is as follows:

$$D_p = T_p^{\text{RTS}} + T_p^{\text{CTS}} + T_p^{\text{ACK}} + T_p^{\text{DATA}} + T_p^{\text{BO}} + T_p^{\text{IFS}}. \tag{4.5}$$

Further, these components represent accumulated values since for one successful data packet delivery there might be multiple back-off stages and packet re-transmissions. For ease of discussion, overall simulation delay characteristics are mainly presented through the 95th percentile of delay. Additionally, average transmission delay per node is considered for more detailed investigations.

4.4 QoS in Urban Scenario

For achievable QoS differentiation, three investigation cases were devised for the random urban deployment scenario, as shown in Table 4.5. The first study case considers achievable QoS based on the RPL variants for the base data rate as specified by [73]. The second case considers how protocols operate and perform with increased traffic load. The third case examines how QoS differentiation is affected by varying grid conditions, modeled as varying traffic composition.

4.4.1 Study Case I: Achievable QoS Differentiation at the Base Data Rate

Due to the varying nature and number of applications (monitoring, control, automation, etc.) used to collect, process and relay the gathered SG data, QoS requirements such as bandwidth, latency, reliability and security will vary. For example, basic periodic metering data requires medium reliability but can tolerate latency and jitter. However, alert or emergency messages for grid failures are random, occur in bursts and require very stringent latency. Thus, QoS in terms of latency and reliability differ for different classes of SG traffic. Further, network routing should possess the ability to dynamically route packets

| Parameter	Urban QoS Study Cases		
	I	II	III
Pathloss α	3.6	3.6	3.6
Shadowing σ (dB)	7.4	7.4	7.4
Node rate r (packets/s)	$r_b^\dagger$	$\{r_b, 0.01, 0.1\}$	$\{r_b, 0.01, 0.1\}$
Network size n (nodes)	1000	1000	1000
Traffic Distribution	II	II	III

$^\dagger r_b = 1.556 \times 10^{-3}$ as calculated from NIST estimates for 125-byte packet

Table 4.5 Simulation parameters of study cases I-III

based on their QoS requirements in order to meet application level criteria.

With that in mind, this case study considers the achievable QoS differentiation for the three protocols of interest, RPL, RPL-M and RPL-M+, at the base data rate. Specifically, following the estimation given in [73] for conventional SG applications (including interval/on-demand meter reading, DR and remote connect/disconnect applications), the total traffic load offered to the network by each SM is approximately 16808 [Bytes/day]. Therefore, the smart metering base data rate estimated in [73] of 16808 [Bytes/day] = $\frac{16808}{24 \times 60 \times 60}$ [Bytes/s] corresponds to $r_b = \frac{16808}{24 \times 60 \times 60 \times 125} = 1.556 \times 10^{-3}$ [packets/s] for a 125-byte packet. Further, to model a grid condition where some critical messages are present, Traffic Distribution I is chosen such that the node rates, in packets/s, for both traffic classes are equivalent (however given their relative packet lengths, critical traffic only represents 20% of the network's offered load). Then, traffic class performance is evaluated based on PDR, delay and hop count in order to gauge protocol performance differences. Further details are in Table 4.5.

In order to investigate the operations of the three chosen routing protocols, the correlation between source-DAP distance and PDR, average transmission delay and routing path length per node are plotted in Figs. 4.5, 4.6 and 4.7, respectively. In these figures, the horizontal axis represents the geographic distance from source nodes to the DAP. Further, to determine achievable QoS differentiation, RPL is employed as the benchmark to determine baseline network performance. Thus, it is not expected to achieve the desired QoS differentiation. For RPL-M and RPL-M+, as the two traffic classes are routed differently, a noticeable segregation in traffic class performance is anticipated. However, as this study case examines performance with the base data rate, significant relative performance differences between RPL-M and RPL-M+ are not foreseen.
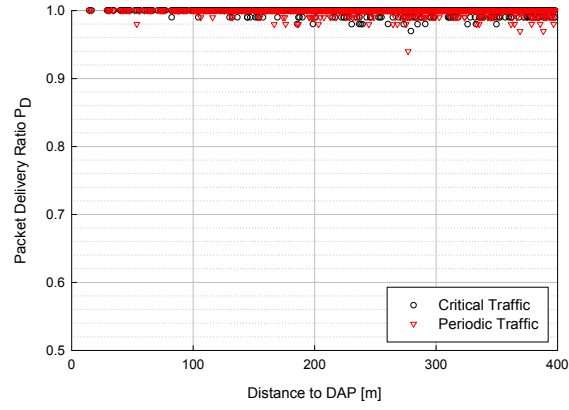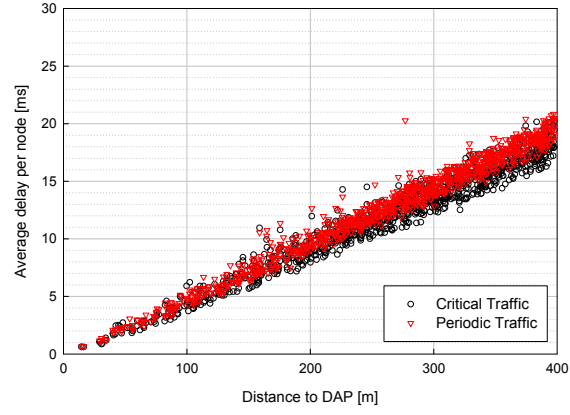
(a) RPL
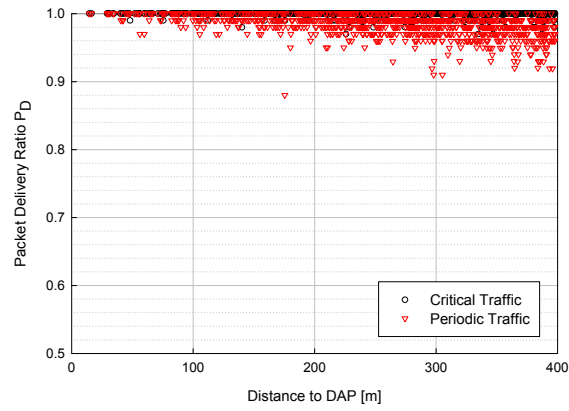
(b) RPL-M
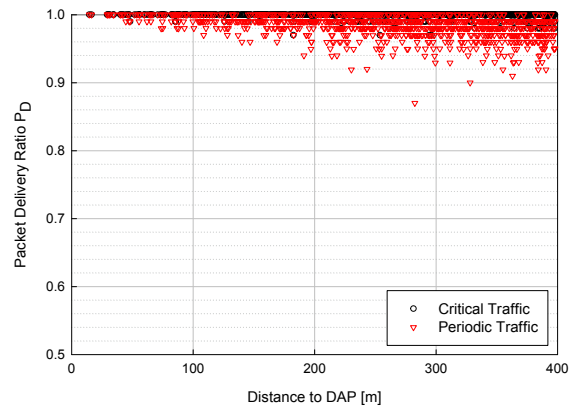
(c) RPL-M+

Figure 4.5   Average transmission reliability vs. source-DAP distance (case I)

For RPL, as shown in Fig. 4.5a, the PDR is approximately 100% for the two traffic classes, regardless of source-DAP distance. Given that the base data rate, r_b, is quite low (as compared to the theoretical IEEE 802.11b link capacity) the network is underloaded and PDR is high, as anticipated. As for the delay, Fig. 4.6a, critical and periodic traffic overlap significantly. For instance, at 100 m from the DAP, all packets are delivered within $4 \sim 6$ ms with no clear separation between the two traffic classes. However, nodes farther from the DAP (beyond 200 m) experience a negligible advantage of 1 ms for critical over periodic traffic. As this delay advantage is minimal, its main contributing factor is most likely packet length. In particular, as larger packets necessitate longer transmission times (T_p^{DATA}), this excess accumulates over the multiple hops on the way to the destination. Thus, the gap between traffic classes should increase slightly with source-DAP distance, as observed. Next, for the hop count, Fig. 4.7a, there is an almost exact overlap between the average hop count of the two traffic classes. As RPL routes all traffic classes over the same network graph, this overlap is reasonable. Therefore, achievable QoS differentiation with RPL alone is quite limited, as there are no significant differences for PDR, delay or even path characteristics between the two traffic classes. Further, as the network graph is built upon packet reception statistics, it fails to take into account packet characteristics. Thus, distinct QoS requirements cannot be met as there is no significant distinction between traffic classes.

For RPL-M, the PDR difference between the two traffic classes grows with increasing source-DAP distance, as shown in Fig. 4.5b. Further, not only does the magnitude of the difference increase with source-DAP distance, so does the number of nodes that experience this widening gap between the PDRs of critical and periodic traffic (always favoring critical traffic). Nonetheless, the PDR of both traffic classes fall within SG targets as defined in Table 4.2, i.e., PDR is still greater than $88 \sim 90\%$ and thus reliability requirements are met. In terms of delay, Fig. 4.6b, the delay difference between the two traffic classes also grows with increasing source-DAP distance. For example, at roughly 50 m from the DAP, the two traffic classes have similar delays of $2 \sim 5$ ms whereas beyond 100 m from the DAP, there is a clear distinction between the delay of periodic and critical traffic, with periodic-traffic packets requiring up to 5 ms extra to reach the destination. From another perspective, with increasing distance to the DAP, the relative difference in hop count between the two traffic classes also increases, as shown in Fig. 4.7b. For example, at 200 m from the DAP, most critical-traffic packets require 1 hop more than periodic traffic. At 300 m
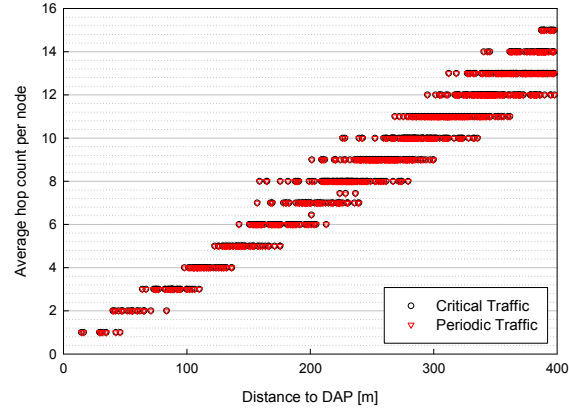
(a) RPL
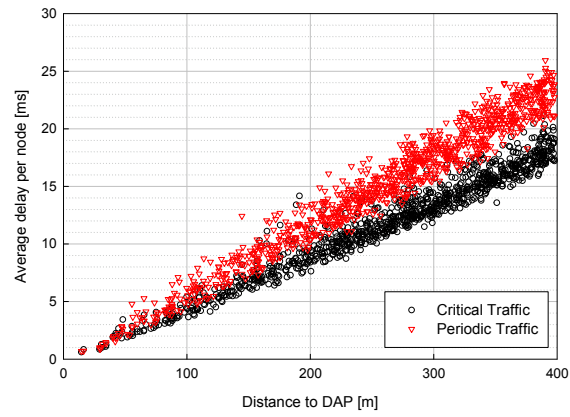
(b) RPL-M
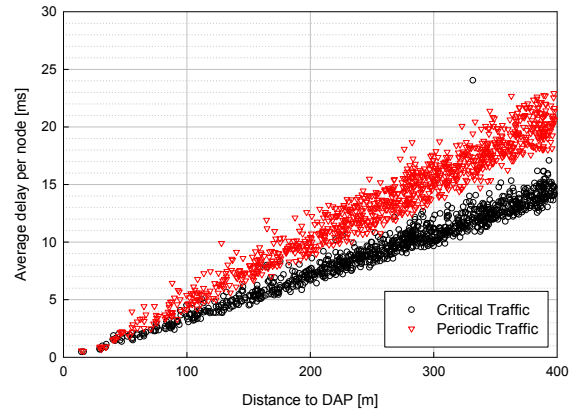
(c) RPL-M+

Figure 4.6   Average transmission delay vs. source-DAP distance (case I)

from the DAP, this increases to 2 hops and further at 400 m from the DAP, it grows to 4 hops. Thus, it is interesting to note that for nodes at the same distance to the DAP, critical-traffic packets traverse a larger number of hops as compared to periodic traffic. As the HC metric attempts to select the next-hop neighbors that result in the greatest geographical progression towards the final destination (shortest path), those neighbors are usually far away from the current node and have relatively low link quality. Link ETX, on the other hand, selects neighbors with shorter distance but higher transmission reliability. In other words, critical traffic trades off longer forwarding progress for higher transmission reliability. Therefore, it results in longer but more reliable paths and thus better overall performance, as compared to periodic traffic. Besides, if less reliable next-hop links are chosen, there is a higher likelihood of packet re-transmissions and drops which lengthen average packet transmission delay, as observed for periodic traffic. Therefore, with RPL-M, QoS differentiation as defined in Table 4.2 is achievable and is more pronounced with increasing source-DAP distance.

For RPL-M+, the PDR difference between the two traffic classes grows with increasing source-DAP distance, as can be seen in Fig. 4.5c. For periodic traffic, nodes farther away from the DAP generally suffer from lower reliability, as compared to critical traffic. Additionally, PDR performance between RPL-M and RPL-M+ is analogous. This is to be expected as channel access prioritization affects PDR through MAC resource allocation and scheduling. Specifically, should network load increase, a more pronounced effect should be observable. However, at the base data rate, the network is underloaded and thus RPL-M and RPL-M+ perform similarly. Next, when considering the delay, Fig. 4.6c, the delay difference between the two traffic classes also grows with increasing source-DAP distance. In addition, the spread of critical traffic delay for nodes at the same source-DAP distance is minor, i.e., $1 \sim 2$ ms. This implies that source-DAP distance plays a crucial role in critical-traffic packet delay and allowing for prioritized channel access reduces the delay inducing effects of channel congestion. Nonetheless, even though the spread of periodic traffic delay for nodes at the same source-DAP distance remains at roughly 5 ms, the overall delay itself has been shifted down by about 2 ms when compared to RPL-M, i.e., all periodic-traffic packets reach the destination within 23 ms with RPL-M+ compared to the $25 \sim 26$ ms necessary for RPL-M. This implies that channel access prioritization favoring critical-traffic packets not only has a beneficial effect on critical-traffic packets but also periodic-traffic packets as it reduces network congestion. As for the hop count, as shown in Fig. 4.7c,

(a) RPL
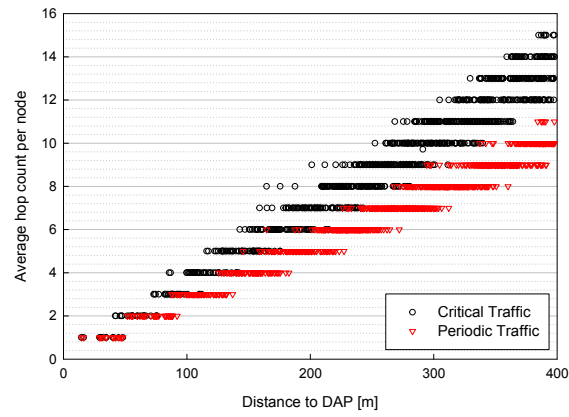
(b) RPL-M
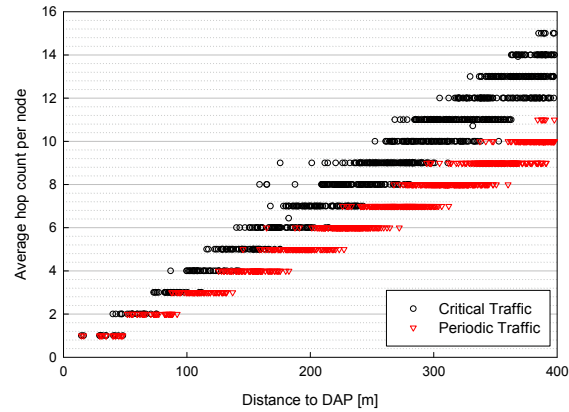
(c) RPL-M+

Figure 4.7   Average hop count vs. source-DAP distance (case I)

there is little difference between RPL-M and RPL-M+ as their network graphs are formed in a similar manner. Therefore, with RPL-M+, altering the channel access probability allows for decreased delay for both traffic classes (reduction in back-off times and network congestion for critical and periodic traffic, respectively). However, a significant difference in PDR should be observable at higher data rates as channel access prioritization alters MAC resource allocation. This is further explored in study case II. Regardless, RPL-M+ does achieve the desired QoS differentiation targets specified in Table 4.2.

Finally, comparing the overall performance between the three protocols, Fig. 4.8 illustrates the average difference between critical and periodic traffic. Specifically, given a network size of N, the average differences in PDR, delay and hop count are as follows,

$$\overline{\Delta_{\text{PDR}}} = \frac{1}{N} \sum_{i=1}^{N} [\text{PDR}(i)_{\text{critical}} - \text{PDR}(i)_{\text{periodic}}] \tag{4.6a}$$

$$\overline{\Delta_{\text{D}_{\text{p}}}} = \frac{1}{N} \sum_{i=1}^{N} [\text{D}_{\text{p}}(i)_{\text{critical}} - \text{D}_{\text{p}}(i)_{\text{periodic}}] \tag{4.6b}$$

$$\overline{\Delta_{\text{HC}}} = \frac{1}{N} \sum_{i=1}^{N} [\text{HC}(i)_{\text{critical}} - \text{HC}(i)_{\text{periodic}}] \tag{4.6c}$$

For example, (4.6a) represents the average PDR difference between traffic classes, i.e., it is the mean of the difference between (i) the average per node PDR for critical traffic and (ii) the average per node PDR for periodic traffic. Equations (4.6b) and (4.6c) are the corresponding average differences for delay and hop count, respectively. In addition, as the mean holds no information about the spread of the difference between the two traffic classes, Fig. 4.8 also includes errors bars of one standard deviation to show the variability of the reported means.

Based on Fig. 4.8, for RPL, the average difference is approximately zero for the three performance metrics. For RPL-M, the average difference in PDR, delay and hop count are 1.6%, −3.3990 ms and 2.2187 hops, respectively. For RPL-M+, the average difference in PDR, delay and hop count are 1.6%, −4.0445 ms and 2.2331 hops, respectively. It is interesting to note that in this case, the negative values for the average delay difference imply that critical traffic reaches the destination faster than periodic traffic. Therefore, both RPL-M and RPL-M+ allow for QoS differentiation in such a manner that critical-traffic packets experience reduced delay with increased path lengths. As the network is
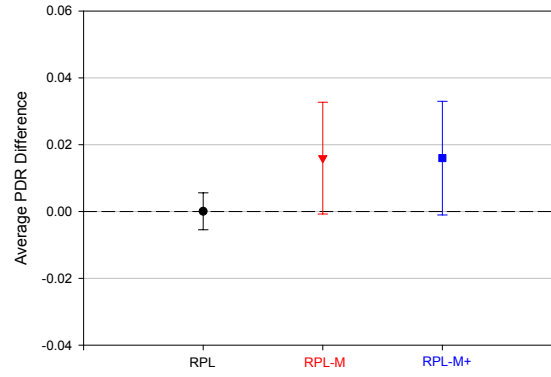
(a) Average PDR difference
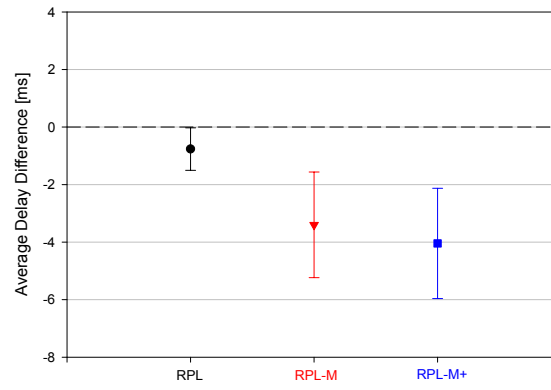
(b) Average delay difference
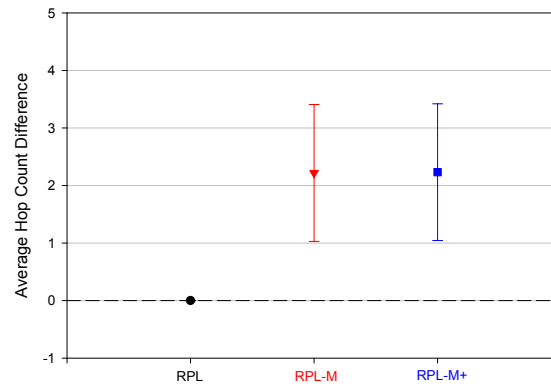
(c) Average hop count difference

Figure 4.8 Average performance difference between critical and periodic traffic (case I)

underloaded, average PDR difference is minimal (even though this difference is quite large with increasing source-DAP distance, a greater proportion of network nodes are closer to the DAP and thus the average difference is quite small). Thus, RPL-M and RPL-M+ do achieve the desired QoS differentiation as outlined in Table 4.2. However, their relative performance differences, between RPL-M and RPL-M+, are not significant at the base data rate. Further, as their relative performance difference is expected to grow with increased data rate, the subsequent case study will explore the effects of increased data traffic load.

4.4.2 Study Case II: Effects of Data Traffic Load

Since SMs are deployed to support not only conventional SG applications (e.g., meter reading, DR, and so on as mentioned in [73]) but also those expected in the future (e.g., ADA, fault detection and restoration, etc.), they are responsible for exchanging an increasing volume of information. As a result, the simulation presented in this study case investigates how network performance scales with increasing level of network offered load. Specifically, for the simulation's data rate sweep, R_p[packets/s] is the variable being swept for an *effective* combined 125-byte packet (composed of a 100-byte periodic class packet and a 25-byte critical class packet). The sweep begins at the base data rate of $r_b = 1.556 \times 10^{-3}$ [packets/s] [73]. Then, two additional data rates are considered such that $R_p = \{0.01, 0.1\}$[packets/s]. These rates were chosen so as to ascertain network performance as data rate increases by orders of magnitude. Additionally, to model a grid condition where some critical messages are present, Traffic Distribution I is chosen such that the node rates, in packets/s, for both traffic classes are equivalent (however given their relative packet lengths, critical traffic only represents 20% of the network's offered load). Further details are in Table 4.5.

With increasing data traffic load, channel contentions take place with a higher probability. This results in a large number of back-off stages per packet. Even though routing paths are not lengthened (since network size is unchanged), lower transmission reliability and longer delays are observed for RPL, RPL-M and RPL-M+. Further, with increasing data rates, network congestion becomes more significant and can lead to multiple re-transmissions before the packet is successfully received. Additionally, smaller packets have a higher probability of being successfully transmitted since they require less transmission time (i.e., lower probability of being affected by channel shadowing or burst fading events). Therefore, it is expected that critical traffic will outperform periodic traffic for

Node Rate [packets/s]	RPL		RPL-M		RPL-M+	
	Critical	Periodic	Critical	Periodic	Critical	Periodic
0.001556	0.998766	0.998715	0.998725	0.982747	0.998675	0.982707
0.01	0.998201	0.995959	0.997830	0.977655	0.997393	0.975983
0.1	0.961111	0.880427	0.973620	0.861172	0.963593	0.858943

Table 4.6   Packet delivery ratio values for study case II
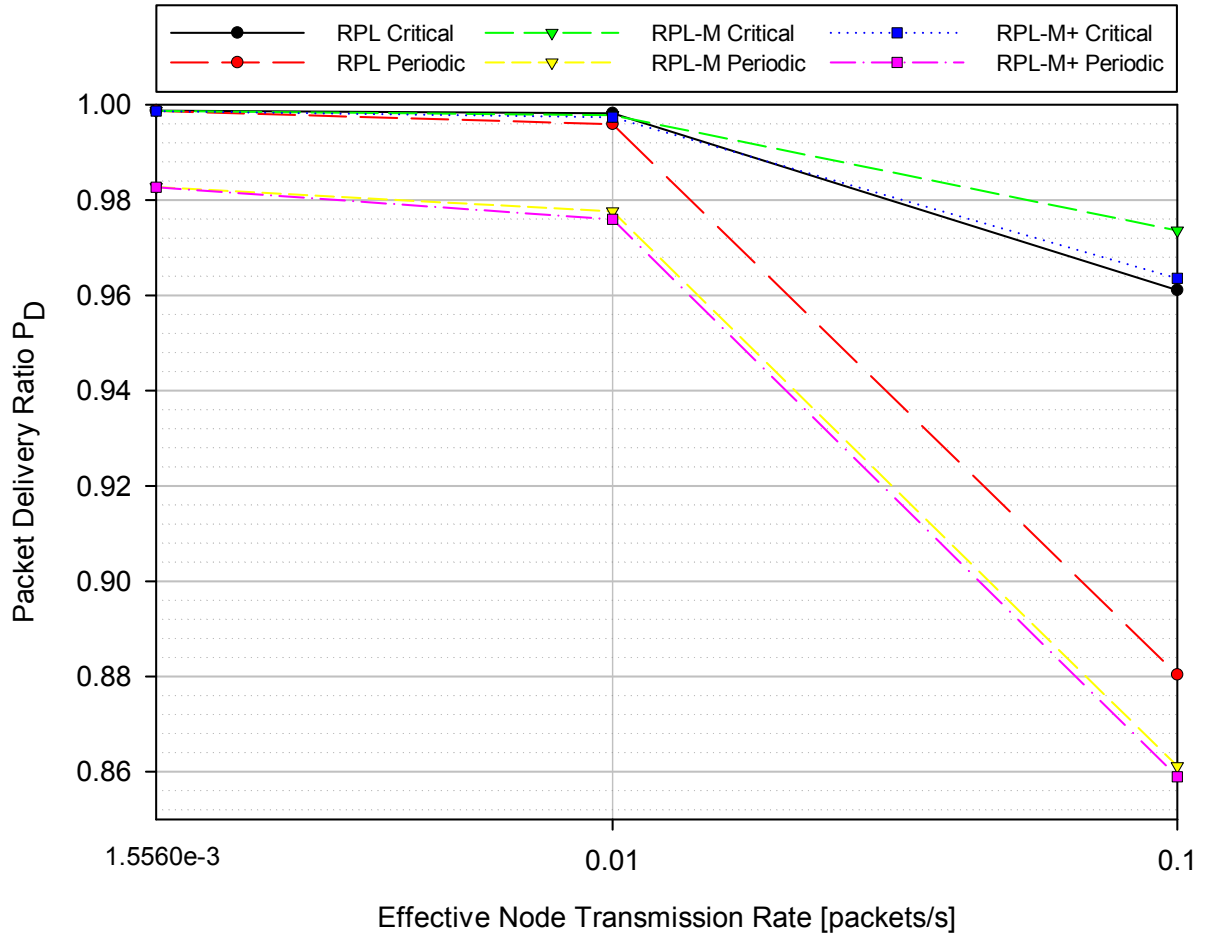
Figure 4.9   Packet delivery ratio for traffic distribution I (case II)

all cases. Further, Figs. 4.9 and 4.10 and Table 4.6 show that, as data rate increases, the performance, in terms of PDR and 95th percentile of delay, of all three protocol degrades. Fortunately, desired QoS requirements are still met in all cases for this traffic distribution.

For RPL, depicted in Fig. 4.9 via circular symbols (in black for critical traffic and red for periodic traffic), there is minimal PDR difference ($0.01 \sim 0.22\%$) observed between the traffic classes at low data rates. However, at higher data rates such as 0.1 packets/s, a significant difference, 8.07%, between the PDRs of the two traffic classes, favoring critical traffic, can be seen. In this case, since the traffic classes are routed over the same ETX network graph, the disparity in their reliability stems from the interaction of the different packets and the channel, i.e., their data rates and packet lengths. Now, since the node rates, in packets/s, of the traffic classes are equivalent in Traffic Distribution I, i.e., $R_p(\text{c})$ = $R_p(\text{p})$, the higher PDR of critical traffic, as shown in Fig. 4.9, can be attributed to how its packets interact with the channel. Specifically, shorter transmission times interspersed over time thereby achieving better temporal diversity. Further, this effect is more pronounced at higher data rates due to the increase in interference, packet collisions and corruptions. Thus, with shorter packets, there is a lower likelihood for collisions and less exposure to interference effects thereby achieving higher PDR as compared to periodic traffic. As for the delay, as shown by the red bars in Fig. 4.10, the relative difference between critical and periodic traffic delay is insignificant (less than 1 ms) at low data rates. However, a noticeable difference of roughly 18.91 ms more for critical traffic can only be seen for high data traffic, i.e., 0.1 packets/s. In this case, since the node rates (in packets/s) are the same, even though critical-traffic packets are shorter, they are more likely to sense a busy channel (especially if the channel is given to a periodic-traffic packet that takes four times as long to transmit). Therefore, the need to back-off increases with increasing traffic congestion and thus the delay gap between the traffic classes increases. Moreover, as data rate increases, the actual delay also increases. Fortunately, even with the increase, QoS latency requirements are still achieved as all communications occur within $\mathcal{O}(10^2)$ ms, the stricter of the two bounds.

For RPL-M, depicted in Fig. 4.9 via triangle symbols (in green for critical traffic and yellow for periodic traffic), there is an increasing PDR difference between critical and periodic traffic. In particular, critical traffic achieves roughly 1.60%, 2.02% and 11.24% higher PDR than its periodic counterpart for the three successive data rates. Since RPL-M routes the traffic classes over separate network graphs, namely link ETX and HC network graphs for critical and periodic traffic, respectively, this widening PDR gap between the traffic classes is due to (i) the fact that the ETX graph is not only able to adapt to changing network conditions but (ii) is also built solely upon the reliability statistics of
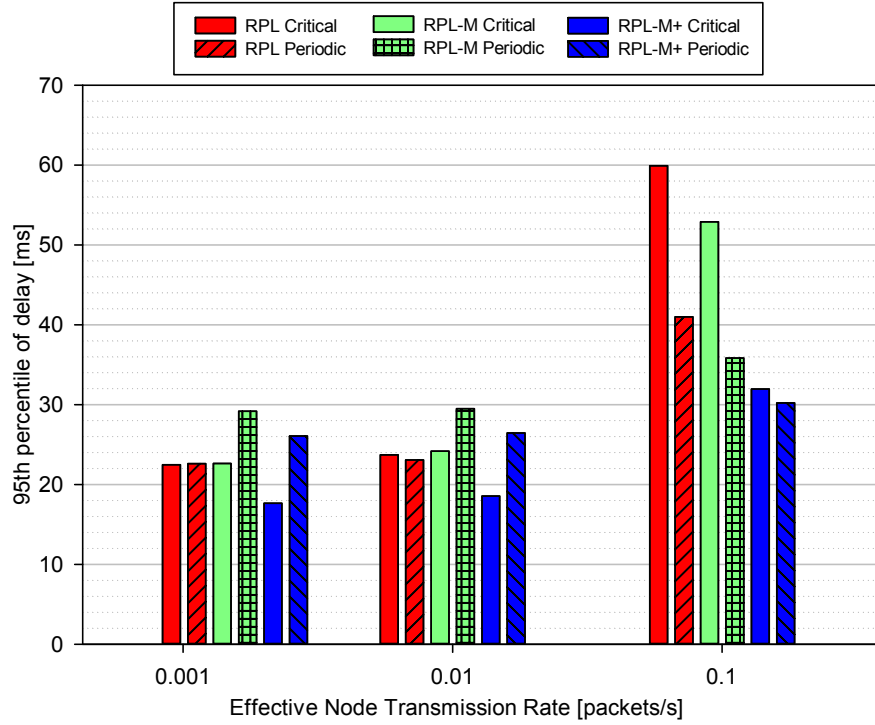
Figure 4.10 95th percentile of delay for traffic distribution I (case II)

critical-traffic packets and employed only for critical-traffic packets. Therefore, the ETX graph is more representative and thus more reliable and leads to higher PDR for critical over periodic-traffic packets. However, as HC is less reliable than ETX, the PDR of periodic traffic degrades faster with increased traffic load. It is also interesting to note that periodic traffic with RPL-M is roughly $1.60 \sim 1.93\%$ lower than its RPL equivalent (the equivalent comparison for critical traffic is negligible). This observation can also be explained through the reduced reliability of the HC metric as opposed to the link ETX metric. However, as the lowest achievable PDR with RPL-M is 86.12%, medium reliability is still achieved, as desired. Further, for the delay, as shown by the green bars in Fig. 4.10, at the two lower data rates, periodic traffic delay is higher by roughly $6.54 \sim 5.33$ ms than that of critical traffic. This increase in periodic traffic delay can be explained by the reduced reliability of the HC metric, (as compared to the ETX metric) thereby increasing the likelihood for packet re-transmissions. However, as data rate increases, this delay gap closes and eventually reverses (lower periodic traffic delay than critical traffic delay at 0.1 packets/s). This reversal is explained through packet delay recording. Specifically, end-to-end packet

delay is only recorded for successfully received packets. Therefore, as data rate increases and PDR favors critical-traffic packets, the received packets from the periodic traffic class are those received with minimal interference or congestion and thus lower overall delay. Next, comparing between the delays of RPL-M and RPL, for the two lower data rates, (i) critical traffic delay is analogous and (ii) periodic traffic delay is higher for RPL-M as explained by the reduced reliability of the HC metric. However, it is interesting to note that at 0.1 packets/s, the delay of the two traffic classes is lower with RPL-M than with its RPL counterpart. As RPL-M operates with two distinct network graphs that more reliably represent the two traffic classes, the latter observation implies that traffic segregation at the network layer alone can translate into improved delay characteristics. Therefore, RPL-M also achieves the desired QoS requirements as defined in Table 4.2.

For RPL-M+, depicted in Fig. 4.9 via square symbols (in blue for critical traffic and magenta for periodic traffic), the relative PDR performance between the two traffic classes is analogous to that of RPL-M, i.e., up to 1% difference between the corresponding PDRs for RPL-M and RPL-M+. Nonetheless, as RPL-M+ differs from RPL-M in terms of the additional prioritized channel access at the MAC level, its effect of PDR should be mainly related to MAC queue management. For instance, favoring one class of packets over another will be more significant when queue resources are scarce. Thus, PDR differences between RPL-M and RPL-M+ should grow with increasing data rate. However, as Traffic Distribution I implies equivalent node rates in packets/s, these differences are negligible due to the smaller offered load associated with critical traffic, i.e., 20% of total offered load is critical and thus favoring critical-traffic packets is only favoring a small percentage of the total network offered load. Furthermore, the delay characteristics and trends also behave similarly to that of RPL-M, as shown by the blue bars in Fig. 4.10. However, as critical traffic profits from increased channel access probability, its delay with RPL-M+ is significantly lower than that of RPL-M for all data rates. In addition, as the back-off ranges associated with critical traffic are half of those of periodic traffic, the swifter processing of critical traffic frees the channel at a faster rate and thus ameliorates network congestion. This in turn improves the delay of periodic traffic as well. For example, when comparing RPL-M+ with RPL-M for each successive data rate, (i) critical traffic is 4.98, 5.61 and 20.94 ms lower and (ii) periodic traffic is 3.11, 3.04 and 5.61 ms lower. Thus, even though RPL-M and RPL-M+ perform similarly in terms of PDR and meet the SG QoS requirements, RPL-M+ poses a clear delay advantage.

Finally, in order to consider the overall performance difference between the two traffic classes, the average of the three chosen protocols was taken. In particular, the average PDR difference between critical and periodic traffic widens from 1.07% to 1.46% and up to 9.93% for each successive data rate. As a significant difference in PDR is only observed for 0.1 packets/s and this rate corresponds to the lowest achievable PDR of 86%, increasing the data rate further would reduce the PDR beyond the required SG targets. Thus, based on reliability requirements for periodic traffic, for a large urban NAN, the effective combined data rate should at most be of the order of 0.1 packets/s. As for the delay, the overall trend favors critical traffic at low data rates, but eventually reverses with lower periodic traffic delays. In particular, the average delay difference between critical and periodic traffic are -5.03, -4.20 and 12.57 ms for each successive data rate. However, as all these values are in the ms range and the critical traffic latency requirements of $\mathcal{O}(10^2)$ ms are met, latency requirements are fully met for both traffic classes. Further, as critical traffic comprises only 20% of the network offered load, the full impact of channel access prioritization is not yet seen. With that in mind, the subsequent case study will consider the effect of traffic distribution.

4.4.3 Study Case III: Effects of Traffic Distribution

As SMs operate within the SG, their QoS requirements depend not only on their desired application requirements (e.g., reliability, bandwidth, security, latency, etc.) but also their dynamic flow priority association based on current grid condition and operation [57]. With that in mind, the simulation presented in this study case investigates how network performance scales when distinct grid conditions are considered. In particular, as the representative traffic classes depict critical and periodic traffic, varying relative traffic compositions alters the current grid condition. Thus, this sweep extends study case II by now modeling the grid condition where critical messages are flooding the network, namely Traffic Distribution II. Specifically, now critical messages comprise half of the total network offered load, i.e., $R_B(c) = R_B(p)$[Bytes/s]. Then, for this new distribution, the same data rate sweep as study case II is performed. The aim of this study is therefore to determine how traffic distribution, i.e., grid condition, affects the observations of study case II. Further details are in Table 4.5.
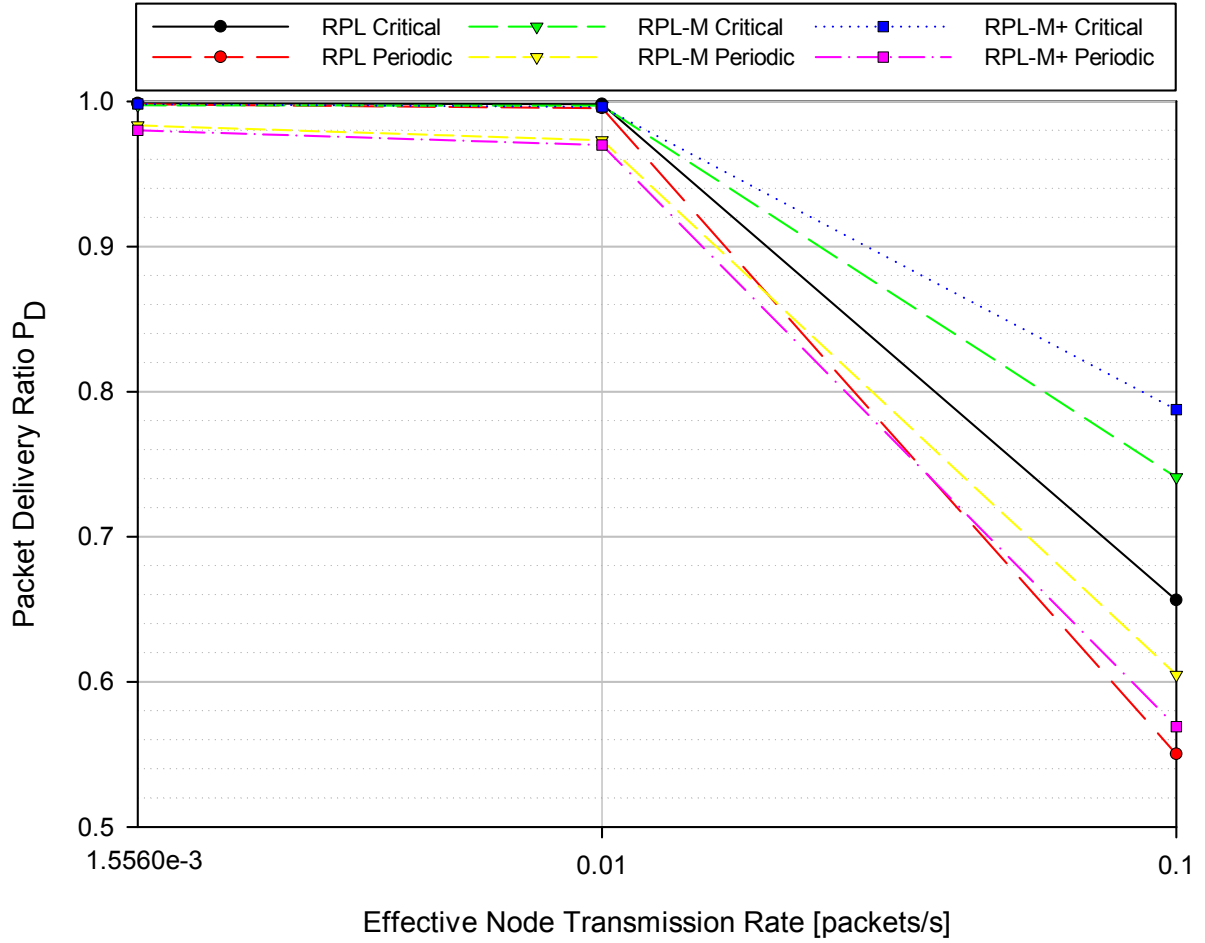
Figure 4.11   Packet delivery ratio for traffic distribution II (case III)

Node Rate [packets/s]	RPL		RPL-M		RPL-M+	
	Critical	Periodic	Critical	Periodic	Critical	Periodic
0.001556	0.998660	0.998040	0.997423	0.983500	0.998243	0.980020
0.01	0.998133	0.995307	0.997116	0.973165	0.996203	0.969975
0.1	0.656193	0.550211	0.741055	0.604839	0.787612	0.569090

Table 4.7   Packet delivery ratio values for study case III

In this case, in order to achieve the equivalent node rate, in Bytes/s, of Traffic Distribution II, as critical-traffic packets are four times shorter, their node rate (in packets/s) must be four times higher than that of periodic traffic. However, for each data rate, the total network load is equivalent to that of the study case II, i.e., the total volume per node in bytes
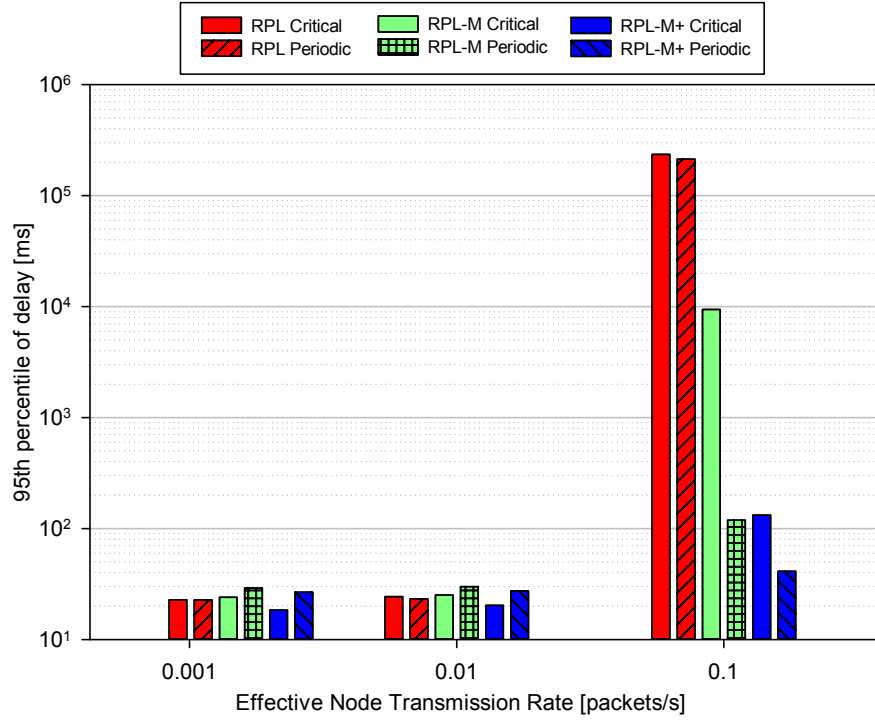
Figure 4.12   95th percentile of delay for traffic distribution II (case III)

is the same but its relative traffic composition is altered. Thus, even though the network is bound to experience elevated levels of congestion and increased likelihood of contentions, back-offs and re-transmissions, it is directly comparable to study case II. Additionally, as critical-traffic packets are shorter, the expectation that they will outperform periodic traffic remains. Further, one can infer that the observable reduction in performance with respect to study case II is a consequence of the rising grid instability. To that effect, Figs. 4.11 and 4.12 as well as Table 4.7 showcase that as the data rate increases, achievable performance sharply decreases to the point of no longer satisfying the desired QoS requirements.

For RPL, depicted in Fig. 4.11 via circular symbols (in black for critical traffic and red for periodic traffic), there is minimal PDR difference ($0.06 \sim 0.28\%$) observed between the traffic classes at the two lower data rates. However, a significant difference of 10.60% can be observed for 0.1 packets/s. As for the absolute PDR values, at the two lower data rates, the traffic classes maintain a PDR above 99%. At 0.1 packets/s, the PDR drops sharply down to 65.62% and 55.02% for critical and periodic traffic, respectively. Thus, with Traffic Distribution II, a node rate of 0.1 packets/s is no longer achievable based

on the QoS targets outlined in Table 4.2. Further, the overall behavior and observable trends are analogous to study case II, i.e., the shorter length of critical-traffic packets allow for better temporal diversity and thus outperform periodic traffic. Additionally, the magnitude of the relative difference between the two traffic classes is similar, namely 8.07% and 10.60% for Traffic Distribution I and II, respectively. However, as there is no longer an equivalency between critical and periodic node rates (the equivalency is at the byte level for Traffic Distribution II), the drop in performance is much sharper, i.e., $30.49 \sim 33.02\%$ lower PDR for 0.1 packets/s per node with Traffic Distribution II than with Traffic Distribution I. Therefore, the increased critical-traffic node rate in packets/s substantially increases network congestion, interference, contention and thus increases the likelihood of packet drops and re-transmissions. This phenomenon can also be observed through the delay, as shown by the red bars in Fig. 4.12. In particular, for 0.1 packets/s, the 95th percentile of delay surges by orders of magnitude, having increased to $\mathcal{O}(10^5)$ ms from $\mathcal{O}(10^1)$ ms. This exponential growth is due in large part to increased network congestion. Specifically, with each back-off, the contention window doubles. Thus packets that travel to the destination via multiple back-offs and re-transmissions will inevitably do so at a high latency cost. Moreover, as this increase far exceeds the increased delay observed for 0.1 packets/s with Traffic Distribution I, it highlights how regardless of the effective combined data rate, individual traffic class node rates affect network performance in a more meaningful way. Finally, as the desired QoS requirement is for latency in the order of $\mathcal{O}(10^2)$ and $\mathcal{O}(10^3)$ ms for critical and periodic traffic, respectively, RPL cannot meet the latency or PDR requirement for Traffic Distribution II when the data rate is high.

For RPL-M, depicted in Fig. 4.11 via triangle symbols (in green for critical traffic and yellow for periodic traffic), the magnitude of the PDR difference between the two traffic classes starts at roughly 1.39% and grows with higher data rates (up to 2.40% and 13.62% for high data rates), always favoring critical traffic. As for the absolute PDR values, a PDR above 97% can be maintained for the two lower data rates. At 0.1 packets/s, the PDR drops to 74.11% and 60.48% for critical and periodic traffic, respectively. Therefore, RPL-M, like RPL, cannot achieve the desired QoS targets for a node rate of 0.1 packets/s. Further, as altering traffic composition does not directly affect the representativeness of the ETX network graph (ETX graph is still built solely upon the reliability statistics of critical-traffic packets), once again the relative performance of the two traffic classes is similar to that observed in study case II (at 0.1 packets/s, the PDR difference between the traffic classes

is 11.24% and 13.62% for Traffic Distribution I and II, respectively). However, increased individual traffic class node rates still translates into a sharp PDR drop at high data rates. Specifically, the PDR drop between Traffic Distribution I and II for 0.1 packets/s is roughly 23.26% and 25.63% for critical and periodic traffic, respectively. It is interesting to note that compared to the $30.49 \sim 33.02\%$ drop experienced by RPL, RPL-M's separate network graphs are able to more reliably, by roughly 7%, weather the increased network congestion associated with Traffic Distribution II. As for the delay, as shown by the green bars in Fig. 4.12, at low data rates, critical traffic delay is lower than that of periodic traffic by roughly $5.00 \sim 4.82$ ms. However, at 0.1 packets/s, critical traffic delay is about 9.44 seconds but periodic traffic delay is only about 118.84 ms. Compared to RPL, periodic traffic delay has been reduced by three orders of magnitude simply by segregating the network graphs. However, critical traffic delay was only decimated and thus is still two orders of magnitude above the desired range. This unevenness in delay reduction between the traffic classes can be explained by the fact that only the critical traffic data rate has been increased in this study case. Therefore, even though separating routing decisions between the traffic classes can help alleviate network congestion, it is not enough by itself. Next, comparing between the two traffic distributions, differences in delay are negligible until 0.1 packets/s where the sudden increase in delay is due to network congestion. Therefore, once again, as the QoS requirement for critical traffic is in the order of $\mathcal{O}(10^2)$, the desired targets cannot be reached for 0.1 packets/s.

For RPL-M+, depicted in Fig. 4.11 via square symbols (in blue for critical traffic and magenta for periodic traffic), the PDR difference between the two traffic classes starts at roughly 1.82% and grows with higher data rates (up to 2.62% and 21.85% for high data rates), always favoring critical traffic. Since the effect of channel access prioritization on PDR is mainly related to MAC queue management, favoring one class of packets over another will be more significant when queue resources are scarce. Thus, there is a shift as data rate increases where the PDR difference between RPL-M and RPL-M+ for a given traffic class is recouped by the other. Specifically, for RPL-M, the PDR of critical and periodic traffic at 0.1 packets/s are 74.11% and 60.48%, respectively. As for RPL-M+, the corresponding PDRs are 78.76% and 56.91% where the $\sim 4\%$ lost for periodic traffic is recouped as an increase for critical traffic. This shifting procedure is then responsible for the observed widening gap. Further, when comparing between Traffic Distribution I and II, unlike RPL and RPL-M, for high data rates, there is a significant difference between

the relative performance of the two traffic classes. In particular, at 0.1 packets/s, the PDR difference doubles for Traffic Distribution II as compared to Traffic Distribution I, i.e., the relative difference between critical and periodic traffic is 10.47% and 21.85% for Traffic Distribution I and II, respectively. Additionally, when comparing the PDR drop between Traffic Distribution I and II, for 0.1 packets/s, the drop is roughly 17.60% and 28.99% for critical and periodic traffic, respectively. This is roughly the same overall drop as that experienced by RPL-M with the difference accounted for by the observed shifting. Next, when examining the delay, as shown by the blue bars in Fig. 4.12, at low data rates, critical traffic delay is lower than that of periodic traffic by roughly $8.29 \sim 7.12$ ms. However, at 0.1 packets/s, critical traffic delay is about 132.05 ms but periodic traffic delay is only about 41.17 ms. Compared to RPL-M, the delay of the two traffic classes has been reduced, especially at 0.1 packets/s, where RPL-M+ poses a clearly striking improvement. First, latency targets outlined by SG application requirements are met, i.e., latency is in the order of $\mathcal{O}(10^2)$ and $\mathcal{O}(10^3)$ ms for critical and periodic traffic, respectively. Second, channel access prioritization clearly alleviates the effect of network congestion on packet transmission delay. Finally, compared to study case II, there is still an increase in delay (about 100.07 ms and 10.93 ms for critical and periodic traffic, respectively). However, an increase is inevitable. Thus, the fact that latency targets are still met is enough to render RPL-M+ a promising protocol for the SG NAN, even as grid instability increases and routing critical-traffic packets becomes of paramount importance.

Finally, when considering the overall performance variation between the two traffic distributions, a significant decrease in PDR can be observed with Traffic Distribution II, i.e., the lowest achievable PDR for Traffic Distribution II is 55.02% as opposed to the 86.12% of Traffic Distribution I. This decrease is mainly due to increased network congestion and illustrates that even though the total network offered load is the same, individual node rates in packets/s play an important role in determining achievable network throughput. In particular, for Traffic Distribution I, the drop in PDR experienced at 0.1 packets/s was still acceptable. However, for Traffic Distribution II, beyond 0.01 packets/s, the sharp drop in PDR falls below desired levels. Further, it is interesting to note that the relative performance between the traffic classes remains similar (network congestion affected both traffic classes equivalently), with slight PDR shift in the case of RPL-M+ due to its favoring of critical traffic. As for the delay, once again, at 0.1 packets/s, the delay difference between the traffic distributions is orders of magnitude apart. In this case, the channel access

prioritization of RPL-M+ is a necessary factor in order to meet latency requirements for both traffic classes. Without it, multiple rounds of back-offs and re-transmissions imply that even the critical-traffic packets that successfully arrive at the DAP would in effect be unusable as they would comprise obsolete information. Thus, in cases with increasing grid instability, there should be enhanced prioritization of critical-traffic packets, as was the case with RPL-M+. Therefore, even though QoS targets are not met for 0.1 packets/s (especially in terms of critical-traffic packet delay), RPL-M+ is the protocol that realizes the best overall results.

4.5 QoS in Rural Scenario

As smaller smart distributed electricity systems or microgrids form an integral part of the SG framework, the three previous urban investigation cases were repeated for the Burwash Landing rural deployment scenario in order to determine how the results and observations of study cases I to III translate into a real-life deployment scenario. With that in mind, the first study case considers the achievable QoS differentiation for the three protocols of interest, RPL, RPL-M and RPL-M+, for the base data rate estimated from [73] in a realistic SG microgrid, as specified in Table 4.4. The second case considers how protocol operation and performance varies with increased traffic load. Then, as microgrids operate within the SG, their QoS requirements will also vary based on grid operation conditions. Therefore, the third case examines how QoS differentiation is affected by varying grid conditions, modeled as varying traffic composition. Further details are in Table 4.8.

4.5.1 Study Case IV: Achievable QoS Differentiation at the Base Data Rate

This case study mirrors study case I, i.e. Traffic Distribution I for the base data rate. However, the notable exception is the choice of network deployment, namely the remote community of Burwash Landing. Therefore, this study case aims to not only determine achievable QoS differentiation for the three chosen protocols but also considers the effect of network deployment. Specifically, it showcases QoS differentiation achievable through RPL-based routing protocols for AMI traffic classes in a *real-life* deployment scenario as compared to a random generic deployment scenario.
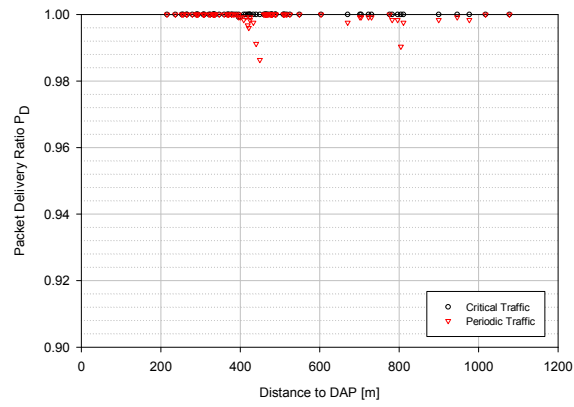
For all three protocols, the correlation between the source-destination geographic distance and PDR, average transmission delay and routing path length per node are plotted
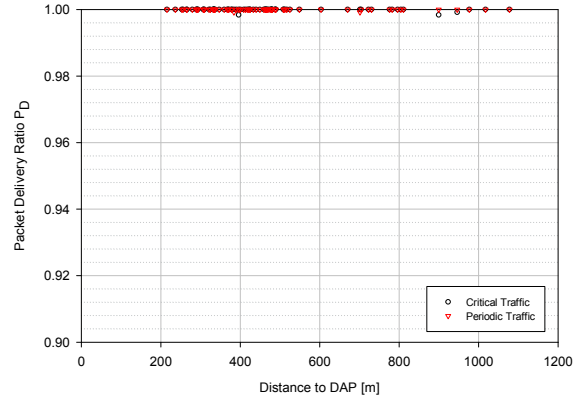
(a) RPL
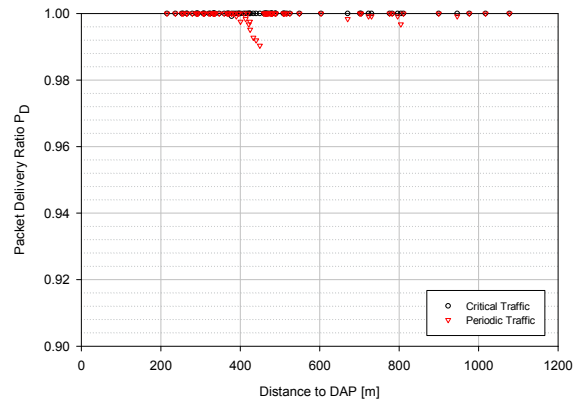
(b) RPL-M

(c) RPL-M+

Figure 4.13 Average transmission reliability vs. source-DAP distance (Burwash Landing, case IV)

Parameter	Rural QoS Study Cases		
	IV	V	VI
Pathloss α	2.1	2.1	2.1
Shadowing σ (dB)	2.2	2.2	2.2
Node rate r (packets/s)	r_b	$\{r_b, 0.01, 0.1, 1\}$	$\{r_b, 0.01, 0.1, 1\}$
Network size n (nodes)	80	80	80
Traffic Distribution	II	II	III

$^\dagger r_b = 1.556 \times 10^{-3}$ as calculated from NIST estimates for 125-byte packet

Table 4.8   Simulation parameters of study cases IV-VI

for the two traffic classes in Figs. 4.13, 4.14 and 4.15, respectively. As can be seen in Fig. 4.13, every node can successfully deliver the majority of its packets to the DAP. Even for nodes that are far away from the DAP (i.e., beyond roughly 400 m to the DAP), a PDR greater than 98% can be attained. Next, for nodes that are located no more than 400 m away from the DAP, almost all packets for periodic and critical traffic have a delay of less than 2 ms and the two traffic classes behave similarly. Beyond that, the sparse and non-uniform geographic node distribution of the network leads to a sporadic, sparse scattered delay distribution, as shown in Fig. 4.14. Further, the average hop count versus source-DAP distance is depicted in Fig. 4.15. In this case, the maximal path length is only 4 hops which is consistent with the small-scale of the Burwash Landing deployment scenario. Again, as there are small sections of the network that are more isolated than others, the higher path lengths correspond to those regions and thus only represent a small, less dense portion of the network. Based on these observations, the QoS requirements for both traffic classes outlined in Table 4.2 are met. However, there is only negligible differences between the two traffic classes, especially for RPL. Therefore, QoS differentiation is minimal for RPL-M and RPL-M+ and negligible for RPL.

For the relative performance of the three protocols, the general trends follow those described in study case I. In particular, (i) periodic traffic PDR drops are only seen for RPL-M and RPL-M+ as HC is a less reliable routing metric, (ii) critical traffic requires less transmission time and experiences more favorable channel conditions and thus its delay is slightly lower than that of its corresponding periodic traffic counterpart, and finally (iii) critical traffic requires longer path lengths (RPL-M and RPL-M+) as link ETX trades off the longer forwarding progress for the higher transmission reliability (in contrast, RPL path characteristics are identical between the two traffic classes as they are routed over
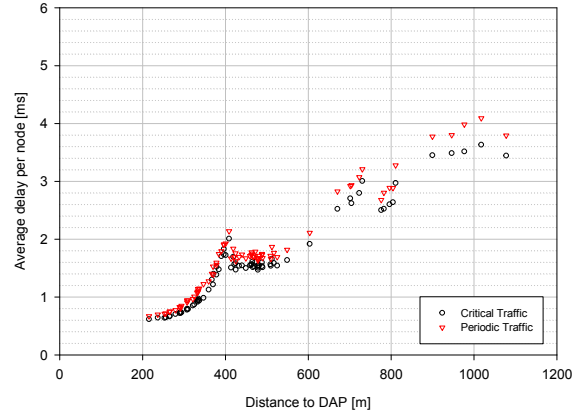
(a) RPL
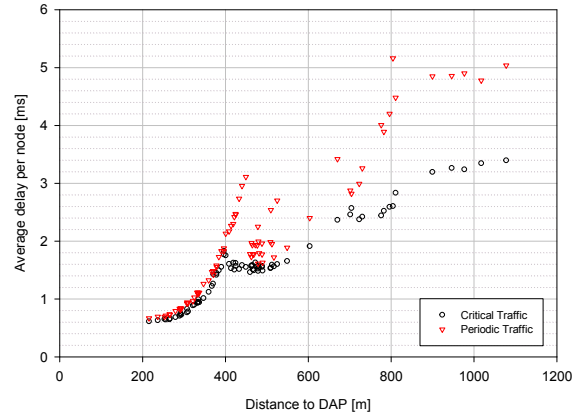
(b) RPL-M
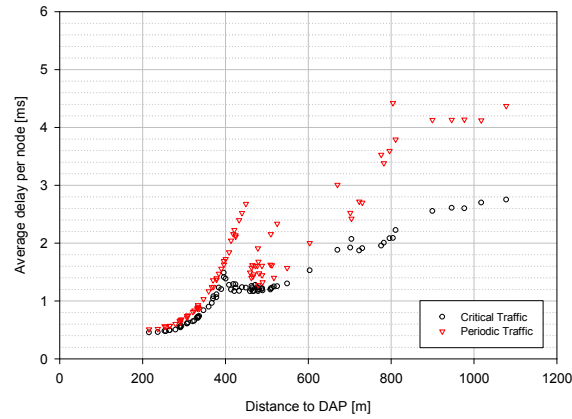
(c) RPL-M+

Figure 4.14   Average transmission delay vs. source-DAP distance (Burwash Landing, case IV)

the same network graph). However, the realistic nature of the network implies that these trends do not monotonically vary with increasing source-DAP distance, i.e., the large-scale random deployment leads to more uniform network performance characteristics whereas the realistic case's behavior will vary based on non-uniform network segments.

Further, as this network is small and operates at a low data rate, the main performance differences are related to delay and path characteristics. A significant difference in PDR should be observable at higher data rates as channel access prioritization alters MAC resource allocation. This is explored in the subsequent study case. Additionally, even though the deployment scenarios for study cases I and IV are vastly different, the general observable trends are similar, i.e., the relative performance differences between critical and periodic traffic as well as between the three routing protocols are comparable. It is the absolute performance that differs, i.e., the actual PDR and delay measured for the study cases. Therefore, results such as those obtained in study cases I, II and III do properly generalize the relative achievable network performance.

4.5.2 Study Case V: Effects of Data Traffic Load

This study case reproduces study case II but once again the remote community of Burwash Landing, in the Yukon, is considered rather than a random network. Nonetheless, the data rate sweep itself is exactly as defined in study case II. Despite the similarities, the study case not only considers microgrid network performance but highlights the transferability and usability of the generic results obtained in study case II for a random network. Further details are in Table 4.8.

For the PDR, as shown in Fig. 4.16, the overall behavior of all three routing protocols is comparable to the results presented in study case II. In particular, a significant difference in PDR between the two traffic classes is only observed for 0.1 and 1 packets/s, where all three protocols differ on average by roughly 1.04% and 6.28%, respectively. Further, the PDR difference between traffic classes widens for each successive data rate. However, unlike study case II, the magnitude of the PDR decrease is significantly less, i.e., even at 1 packets/s, the lowest achievable PDR is 92.53% (periodic traffic). As this is a rural scenario with a small network and favorable channel conditions, packet loss would most likely only become significant when the network is close to saturation, which is not yet reached. Therefore, even at 1 packets/s, PDR requirements are met for all three protocols.
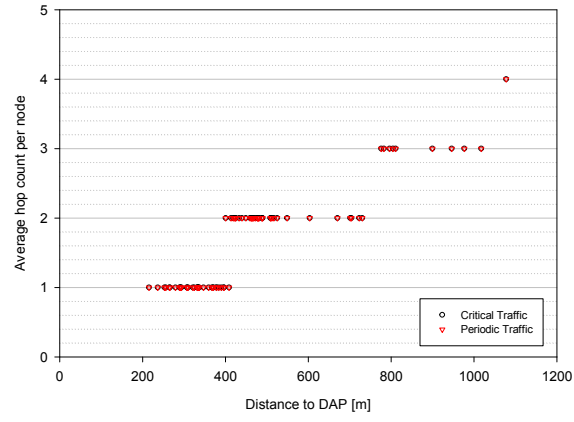
(a) RPL
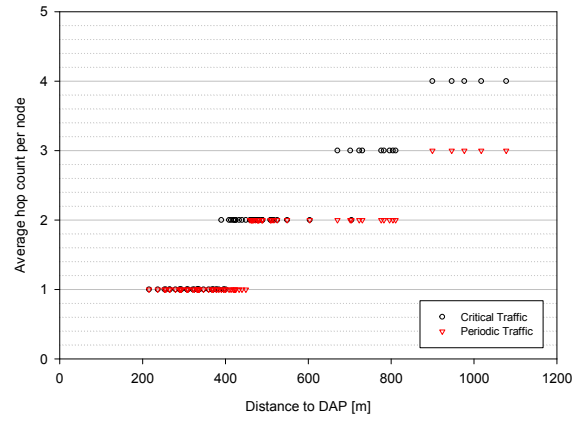
(b) RPL-M
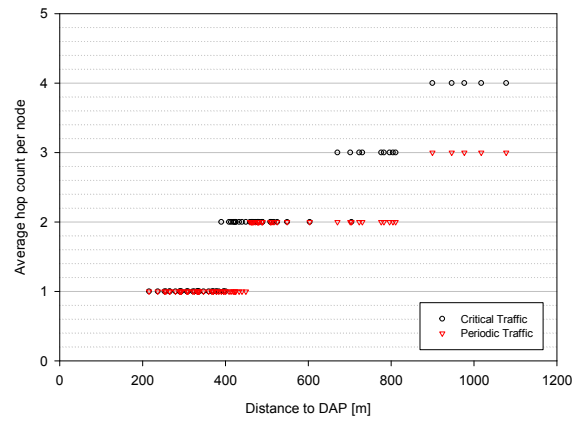
(c) RPL-M+

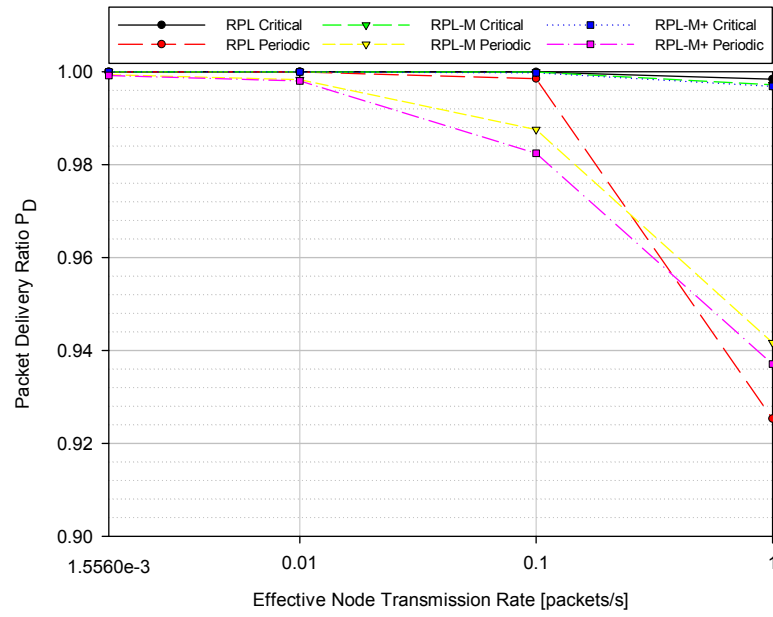**Figure 4.15** Average hop count vs. source-DAP distance (Burwash Landing, case IV)

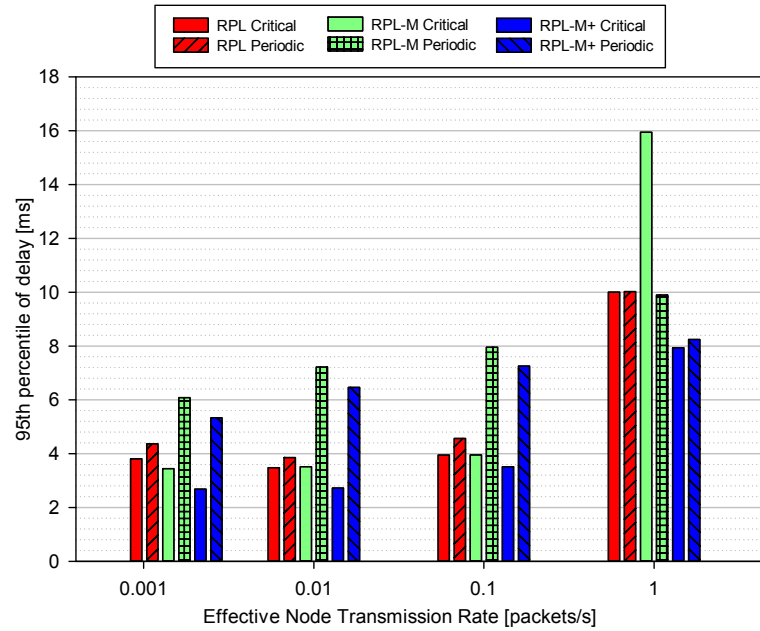**Figure 4.16** Packet delivery ratio for traffic distribution I (Burwash Landing, case V)

Figure 4.17 95th percentile of delay for traffic distribution I (Burwash Landing, case V)
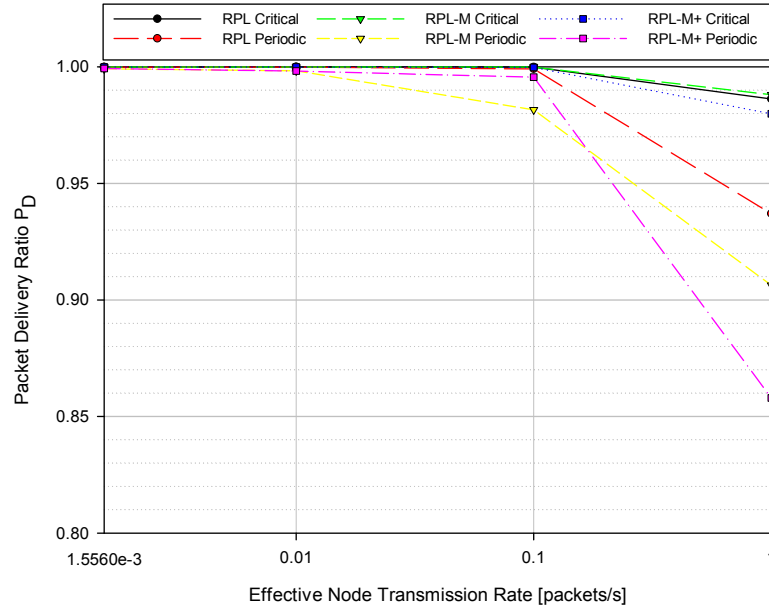
Figure 4.18   Packet delivery ratio for traffic distribution II (Burwash Landing, case VI)

As for the delay, as shown in Fig. 4.17, the overall trend favors critical traffic at low data rates, but eventually reverses with lower periodic traffic delays. Once again, the main characteristics described in study case II still hold. However, as this network is small and sparsely populated, delay requirements are always met, i.e., the delay never exceeds 16 ms and thus the stricter bound of $\mathcal{O}(10^2)$ is met by all traffic classes. Therefore, the relative response of the three protocols to increased data rates is comparable between the two deployment scenarios and the observable trends discussed in study case II are in fact still applicable.

4.5.3 Study Case VI: Effects of Traffic Distribution

This case study mirrors that of case III for the Burwash Landing deployment. Grid conditions are modeled through varying relative traffic compositions and the data rate sweep of study case III is repeated for Traffic Distribution II. Thus, this case study aims to determine how network performance is affected by grid conditions as well as how comparable the results are, to those of study case III. Further details are in Table 4.8.

In particular, the PDR and the 95th percentile of delay are shown in Figs. 4.18 and 4.19, respectively. Specifically, similarly to study case III, (i) a significant decrease in PDR can be
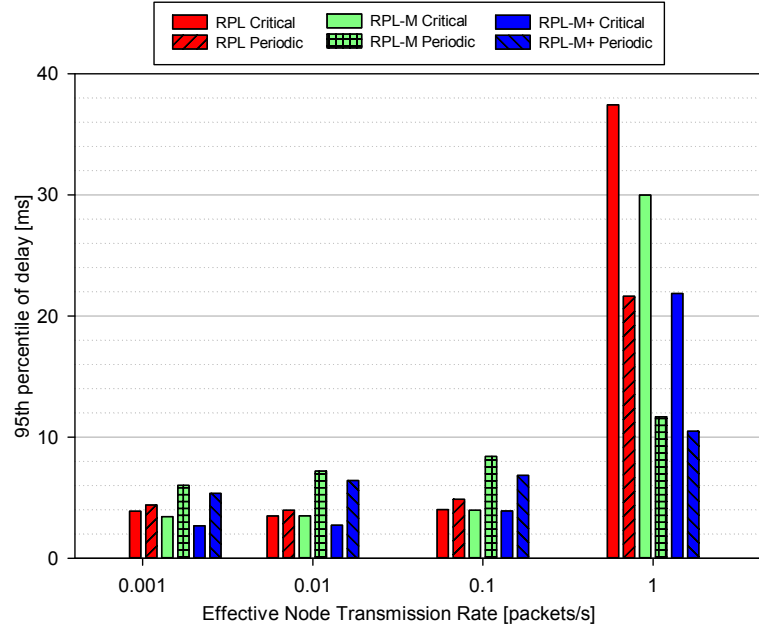
Figure 4.19 95th percentile of delay for traffic distribution II (Burwash Landing, case VI)

observed for higher data rates and illustrates that individual node rates play an important role in determining achievable network throughput, (ii) at low data rates, critical traffic achieves lower delay but this trend reserves with increased data rate. However, unlike study case III, both PDR and delay are always within the required QoS performance targets as specified by SG applications. Next, compared to the results of study case III, the relative performances between the two traffic classes as well as the routing protocols are analogous, i.e., RPL-M+ does achieve the best delay performance even with increased data rates, RPL-M+ does tradeoff periodic traffic load for critical traffic load with increased network congestion, etc. Therefore, the results of study case III are generalizable and can indeed be of use as a blueprint of achievable relative network performance. Of course, to determine the actual performance, each devised deployment scenario would have to be studied separately. However, these results can aid in understanding the underlying behavior and expectations as protocol, data rates and traffic composition vary for critical and periodic traffic.

Chapter 5

Conclusion

This chapter concludes this thesis by providing a summary of the key observations and trends ascertained through the six devised study cases. Then, potential future research directions are suggested to expand and improve upon the obtained results.

5.1 Summary

The SG optimizes the existing power electric grid with the introduction of a reliable and secure SGCN whose NAN poses communications challenges due to its converge-cast nature and differing QoS requirements for uplink data traffic. Focusing on the NAN, RPL has been shown to be a promising routing protocol. However, as the NAN is not only responsible for providing connectivity for a vast number of devices but also meeting the varying QoS requirements of different types of SG applications, characterizing the performance requirements of various SG applications is important in order to understand which communications technologies and applications can be successfully paired [18]. Further, existing solutions related to QoS differentiation need to be revisited to cater for SG traffic because SG applications traffic will likely be quite different from that generated by traditional data applications in use today. In particular, the NAN is expected to carry a mix of both periodic and critical traffic. In addition, the number, type and proportion of traffic classes will affect the complexity and efficiency of any devised resource allocation scheme. Moreover, QoS requirements in the SG NAN context depend not only on traffic class requirements but also the current grid state (e.g., stable, cascading faults, etc.).

With that in mind, this thesis expands on the concept of QoS through multiple RPL instances by considering the effect of traffic differentiation at the network layer, i.e., using multiple distinct network graphs constructed with different OFs to represent the QoS requirements of different traffic classes. In particular, three variants of RPL were studied, single instance RPL, multi-instance RPL (RPL-M) as well as multi-instance RPL with prioritized channel backoffs (RPL-M+). Simulations were conducted for (i) two traffic classes, to model periodic and critical AMI data, (ii) two relative traffic compositions to symbolize different grid conditions, (iii) three data rates to represent increasing data traffic load and (iv) two deployment scenarios to portray a large-scale random urban scenario as well as a real rural scenario. Specifically, as this thesis is intended to be of use for SG communications system designers and network engineers, the real-life deployment scenario, a microgrid, was considered to showcase the performance and achievable QoS differentiation of the aforementioned RPL-based protocols. Then, performance in terms of latency and throughput of standard RPL, RPL-M and RPL-M+ was compared.

From the results, first, for the base data rate in the urban scenario, achievable QoS differentiation with RPL alone is quite limited, as there are no significant differences for PDR, delay or even path characteristics between the two traffic classes. For RPL-M, critical traffic trades off longer forwarding progress for higher transmission reliability. Thus, with RPL-M, QoS differentiation is achievable and is more pronounced with increasing source-DAP distance. For RPL-M+, channel access prioritization favoring critical-traffic packets not only has a beneficial effect on critical-traffic packets but also periodic-traffic packets as it reduces network congestion. As such, both traffic classes experience a reduction in packet delay and RPL-M+ does achieve the desired QoS differentiation targets. However, as the network is underloaded at the base data rate, average PDR difference is minimal and thus the relative performance differences between RPL-M and RPL-M+ are not significant at the base data rate. Next, for the base data rate in the rural setting, QoS differentiation is minimal for RPL-M and RPL-M+ and negligible for RPL, as was the case in the urban scenario. However, the realistic nature of the network implies that these trends do not monotonically vary with increasing source-DAP distance, i.e., the large-scale random deployment leads to more uniform network performance characteristics whereas the realistic case's behavior will vary based on non-uniform network segments. Thus, even though the deployment scenarios for study cases I and IV are vastly different, the general observable trends are similar and do properly generalize the relative achievable network performance.

Second, for the effects of data traffic load in the urban scenario, traffic segregation at the network layer alone can translate into improved PDR and delay characteristics, i.e., the ETX graph is more representative and thus more reliable and leads to higher PDR for critical over periodic-traffic packets for RPL-M and RPL-M+. In particular, a significant PDR difference between the two traffic classes is mainly seen at high data rates. In addition, even though RPL-M and RPL-M+ perform similarly in terms of PDR, RPL-M+ poses a clear delay advantage. Regardless, SG QoS requirements are met for all three protocols. However, overall, based on reliability requirements for periodic traffic, for a large urban NAN, the effective combined data rate should at most be of the order of 0.1 packets/s. Next, for the effects of data traffic load in the rural scenario, the overall behavior of all three routing protocols is comparable to the results of the urban scenario. However, unlike the urban scenario, the magnitude of the PDR decrease is significantly less as (i) the smaller network's saturation level is higher than that of the large urban counterpart and thus not reached yet for the data rates considered and (ii) the rural channel conditions are more favorable. Therefore, even at 1 packets/s, PDR requirements are met for all three protocols. In any case, the relative response of the three protocols to increased data rates is comparable between the two deployment scenarios and the observable trends discussed in the urban scenario are in fact still applicable and transferable.

Third, for the effects of traffic distribution in the urban scenario, the increased critical traffic node rate, in packets/s, substantially increases network congestion, interference, contention and thus increases the likelihood of packet drops and re-transmissions. In fact, all but RPL-M+ experience an exponential growth in delay due to increased network congestion. Further, the channel access prioritization of RPL-M+ is a necessary factor in order to meet latency requirements for both traffic classes. Without it, multiple rounds of back-offs and re-transmissions imply that even the critical-traffic packets that successfully arrive at the DAP would in effect be unusable as they would comprise obsolete information. Thus, in cases with increasing grid instability, there should be enhanced prioritization of critical-traffic packets, as was the case with RPL-M+. In addition, regardless of the effective combined data rate, individual traffic class node rates, in packets/s, affect network performance in a more meaningful way. In particular, the relative performance between the two traffic classes is similar between the two traffic distribution. However, given the increased critical traffic data rate, a node rate of 0.1 packets/s is no longer achievable based on the QoS targets. Nonetheless, RPL-M+ is the protocol that realizes the best overall results.

Next, for the effects of traffic distribution in the rural scenario, the *relative* performances between the two traffic classes as well as between the routing protocols are analogous to the urban scenario. However, unlike the urban scenario, both PDR and delay are always within the required QoS performance targets as specified by SG applications. Therefore, the results of the urban scenario are generalizable and can indeed be of use as a blueprint of achievable relative network performance. Of course, to determine the *actual* performance, each devised deployment scenario would have to be studied separately. Regardless, these results can aid in understanding the underlying behavior and expectations as protocol, data rates and traffic composition vary for critical and periodic traffic.

5.2 Further Aspects and Issues

In an attempt to identify possible future research trends in the SGCN, this chapter outlines a number of technical challenges and corresponding work directions in this network. Specifically, QoS differentiation & provisioning and network coding are addressed.

5.2.1 QoS Differentiation and Provisioning Extensions

As network level QoS differentiation has proven to be quite effective, future work should focus on furthering this concept. In particular, as distinct network graphs do provide a measure of QoS differentiation, achievable QoS may be more significant with a wider range of routing metrics and OFs. In addition, network level resources can be imbued with priority schemes, i.e., reserved links, prioritized neighbors, etc. Further, the existing RPL framework allows for multiple independent network graph instances. However, as each node's graph information is stored locally, a network level priority scheme could be devised so as to weigh the routing operations of the separate and distinct network graphs. Next, as the cross-layered RPL-M+ did realize the best overall performance. MAC level QoS differentiations, beyond channel access prioritization could be employed in conjunction to network level schemes. Specifically, as standard MAC QoS differentiation is accomplished through the use of prioritized queues or MAC resource allocation schemes, further work could focus on how to efficiently design and implement such protocols for the specific QoS requirements of SG applications.

Further, as SG application traffic is quite diverse, additional traffic classes along with more elaborate traffic distributions could be devised. Moreover, node failure could be incor-

porated into the simulations so as to ascertain protocol recovery in the face of disruptions and failures. In addition, as an extension to the microgrid deployment scenario, its communications link to the main grid could be explored further, i.e., how QoS differentiation should be defined and maintained in grid-connected mode as opposed to island mode.

5.2.2 Network Coding

Operations of the SG depend on complex systems of sensors and controllable devices, all of which are tied together through the SGCN. The efficacy and success of emerging SG applications depends on the capability of the SGCN to reliably and expediently gather and transmit sensor data to control centers and vice versa. Transportation of data from a huge number of sensors to a limited number of data collectors or centralized computing centers poses numerous communications challenges due to the bottlenecks associated with the converge-cast nature of this kind of traffic, harsh outdoor environments that lead to severe channel attenuation and shadowing as well as large network scales. With that in mind, conventional network routing can be designed such that the protocols are robust, reliable, self-healing, scalable and possess low overhead. However, there is a limit on what can be achieved through routing alone [74]. A potential solution to enhance reliability, increase throughput and possibly incorporate security would be network coding [74–76].

As a concept, network coding is a communications paradigm in which the flow of information instead of individual packets is considered. Specifically, intermediate nodes no longer simply store-and-forward packets but transmit a combination of their received packets. This combination, essentially an algebraic function of received packets, is designed such that network performance (i.e., capacity, reliability, security, scalability, data compression, etc.) is improved. With these potential advantages, network coding protocols have been successfully implemented to increase robustness and efficiency in distributed storage systems [77] as well as sensor networks [78]. For the SGCN, network coding's opportunistic use of the wireless broadcast medium and its ability to incorporate diversity in a seamless manner to increase robustness and efficiency of data transmission leads to potential advantages such as data aggregation through coding, data compression through packet correlation, enhanced security, improved reliability as well as scalability. In particular, future research direction is focused on a network coded extension to RPL [79] as well as tunable sparse network coding [80].

Bibliography

[1] C. Feisst, D. Schlesinger, and W. Frye, "Smart grid, the role of electricity infrastructure in reducing greenhouse gas emissions," Cisco internet business solution group, white paper, Oct. 2008.

[2] "What caused the power blackout to spread so widely and so fast?" Genscape, Aug. 2003.

[3] "Major power outage hits New York, other large cities," CNN, Aug. 2003.

[4] "The great 2003 North America blackout," CBC, Aug. 2003.

[5] H. L. Willis and W. G. Scott, "Distributed power generation - planning and evaluation," *Marcel Dekker, New York*, 2000.

[6] R. G. Pratt *et al.*, "The smart grid: An estimation of the energy and CO2 benefits," U.S. Department of Energy, Tech. Rep., Jan. 2010.

[7] *Draft Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation With the Electric Power System (EPS), and End-Use Applications and Loads*, IEEE P2030 Std., 2011.

[8] E. Incorporated, "Smart grid: Enabler of the new economy," The Electicity Advisory Committee, The Electricity Advisory Committee, Tech. Rep., Dec. 2008.

[9] E. Clarke, "Control and automation of electrical power distribution systems," *FL:CRC Press*, 2006.

[10] D. G. Hart, "How advanced metering can contribute to distribution automation," *IEEE Smart Grid*, Aug. 2012.

[11] T. Smith, "Utility-scale smart meter deployments, plans, & proposals," Institute for Electric Efficiency, Tech. Rep., May 2012.

[12] G. Rajalingham, Q.-D. Ho, and T. Le-Ngoc, "Evaluation of an efficient smart grid communication system at the neighbor area level," in *the 11th Annual IEEE Consumer Communications & Networking Conference (CCNC'2014)*, Las Vegas, Nevada, U.S., Jan. 2014.

[13] Q.-D. Ho, Y. Gao, G. Rajalingham, and T. Le-Ngoc, *Wireless Communications Networks for the Smart Grid.* Springer International Publishing, 2014.

[14] Z. Fadlullah, M. Fouda, N. Kato, A. Takeuchi, N. Iwasaki, and Y. Nozaki, "Toward intelligent machine-to-machine communications in smart grid," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 60–65, Apr. 2011.

[15] S. K. Tan, M. Sooriyabandara, and Z. Fan, "M2M communications in the smart grid: Applications, standards, enabling technologies, and research challenges," *International Journal of Digital Multimedia Broadcasting*, vol. 2011, 2011.

[16] Q.-D. Ho, Y. Gao, G. Rajalingham, and T. Le-Ngoc, "Performance and applicability of candidate routing protocols for smart grid's wireless mesh neighbor-area networks," in *IEEE International Conference on Communications (ICC'2014)*, Sydney, Australia, Jun. 2014.

[17] Y. Gao, "Performance and applicability of candidate routing protocols for smart grid's wireless mesh neighbor-area networks," Master's thesis, McGill University, 2014.

[18] G. W. Arnold, "Challenges and opportunities in smart grid: A position article," *Proceedings of the IEEE*, vol. 99, no. 6, pp. 922–927, Jun. 2011.

[19] K. Hopkinson *et al.*, "Quality-of-service considerations in utility communication networks," *IEEE Transactions on Power Delivery*, vol. 24, no. 3, pp. 1465–1474, Jul. 2009.

[20] S. K. Tan *et al.*, "M2M communications in the smart grid: Applications, standards, enabling technologies, and research challenges," *International Journal of Digital Multimedia Broadcasting*, pp. 1–8, 2011.

[21] E. Alotaibi and B. Mukherjee, "A survey on routing algorithms for wireless ad-hoc and mesh networks," *Computer Networks*, vol. 56, no. 2, Feb. 2012.

[22] T. Watteyne *et al.*, "From MANET to IETF ROLL standardization: A paradigm shift in WSN routing protocols," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 4, pp. 688–707, Jan. 2011.

[23] "Overview of existing routing protocols for low power and lossy networks," IETF ROLL, IETF draft, draft-ietf-roll-protocols-survey-07 (work in progress), Apr. 2009.

[24] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," *Ad Hoc Networks*, vol. 3, no. 3, pp. 325—-349, Nov. 2005.

[25] M. Abolhasan, T. A. Wysocki, and E. Dutkiewicz, "A review of routing protocols for mobile ad hoc networks," *Ad Hoc Networks*, vol. 2, no. 1, pp. 1–22, Jan. 2004.

[26] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: A survey," *IEEE Wireless Commun.*, vol. 11, no. 6, pp. 6–28, Dec. 2004.

[27] Y. C. Tseng, Y. S. C. S.-Y. Ni, and S. Jang-Ping, "The broadcast storm problem in a mobile ad hoc network," *Wireless Networks*, vol. 8, no. 2/3, pp. 153–167, Mar. 2002.

[28] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Trans. Wireless Commun.*, vol. 1, no. 4, pp. 660–670, Oct. 2002.

[29] Z. Zhou *et al.*, "Energy-efficient cooperative communication in a clustered wireless sensor network," *IEEE Trans. Veh. Technol.*, vol. 57, no. 6, pp. 3618–3628, Nov. 2008.

[30] O. Younis, M. Krunz, and S. Ramasubramanian, "Node clustering in wireless sensor networks: Recent developments and deployment challenges," *IEEE Network*, vol. 20, no. 3, pp. 20–25, May 2006.

[31] O. Younis and S. Fahmy, "HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," *IEEE Trans. Mobile Comput.*, vol. 3, no. 4, pp. 366–379, Oct. 2004.

[32] A. Manjeshwar and D. P. Agrawal, "TEEN: a routing protocol for enhanced efficiency in wireless sensor networks," in *Proc. Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing*, Apr. 2001, pp. 2009–2015.

[33] ——, "APTEEN: A hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks source," in *Proc. International on Parallel and Distributed Processing Symposium (IPDPS)*, Fort Lauderdale, FL, USA, Apr. 2002, pp. 195–202.

[34] A. Boukerche, R. W. Pazzi, and R. Araujo, "Fault-tolerant wireless sensor network routing protocols for the supervision of context-aware physical environments," *Journal of Parallel and Distributed Computing*, vol. 66, no. 4, pp. 586–599, Apr. 2006.

[35] I. Stojmenovic and S. Olariu, *Handbook of Sensor Networks: Algorithms and Architectures*. Hoboken, New Jersey: John Wiley & Sons Inc., Oct. 2005.

[36] P. Bose *et al.*, "Routing with guaranteed delivery in ad hoc wireless networks," in *Proc. 3rd ACM Int. Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications (DIAL)*, Seattle, WA, USA, Aug. 1999, pp. 48–55.

[37] B. Karp and H. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," in *Proc. Annual International Conference on Mobile Computing and Networking (MobiCom)*, Boston, MA, USA, Aug. 2000, pp. 243–254.

[38] H. Frey and I. Stojmenovic, "On delivery guarantees of face and combined greedy-face routing algorithms in ad hoc and sensor networks," in *Proc. 12th ACM Annual International Conference on Mobile Computing and Networking (MobiCom)*, Los Angeles, CA, USA, Sep. 2006, pp. 390–401.

[39] E. Elhafsi, N. Mitton, and D. Simplot-Ryl, "End-to-end energy efficient geographic path discovery with guaranteed delivery in ad hoc and sensor networks," in *Proc. 19th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Cannes, France, Sept 2008, pp. 1–5.

[40] H. Kalosha *et al.*, "Select-and-protest-based beaconless georouting with guaranteed delivery in wireless sensor networks," in *Proc. 27th Conference on Computer Communications (INFOCOM)*, Phoenix, AZ, USA, Apr 2008, pp. 346–350.

[41] Q.-D. Ho, Y. Gao, and T. Le-Ngoc, "Challenges and research opportunities in wireless communications networks for smart grid," *IEEE Wireless Communications*, pp. 89–95, Jun. 2013.

[42] Q.-D. Ho and T. Le-Ngoc, "Smart grid communications networks: Wireless technologies, protocols, issues and standards," in *Handbook on Green Information and Communication Systems*, S. O. Mohammad, A. Alagan, and W. Isaac, Eds. Elsevier, 2012.

[43] N. Saputro, K. Akkaya, and S. Uludag, "A survey of routing protocols for smart grid communications," *Computer Networks*, vol. 56, no. 11, pp. 2742 – 2771, 2012.

[44] J. Ko *et al.*, "Evaluating the performance of RPL and 6LoWPAN in TinyOS," in *Proc. the Workshop on Extending the Internet to Low power and Lossy Networks (IP+SN)*, Chicago, IL, USA, 2011.

[45] O. Gnawali *et al.*, "Collection tree protocol," in *Proc. the 7th ACM Conference on Embedded Networked Sensor Systems (SenSys)*, Nov. 2009, pp. 1–14.

[46] M. Nucolone, "Stability analysis of the delays of the routing protocol over low power and lossy networks," Master's thesis, KTH Electrical Engineering, 2010.

[47] D. Wang *et al.*, "RPL based routing for advanced metering infrastructure in smart grid," Mitsubishi Electric Research Laboratories, Tech. Rep. TR2010-053, Jul. 2010.

[48] P. Kulkarni *et al.*, "A self-organising mesh networking solution based on enhanced RPL for smart metering communications," in *Proc. IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Jun. 2011, pp. 1–6.

[49] J. Tripathi, J. C. de Oliveira, and J. P. Vasseur, "Applicability study of RPL with local repair in smart grid substation networks," in *Proc. the First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Oct. 2010, pp. 262–267.

[50] B. Lichtensteiger *et al.*, "RF mesh system for smart metering: System architecture and performance," in *Proc. IEEE Smart Grid Communication*, Mayland, USA, Oct. 2010, pp. 379–384.

[51] G. Rajalingham, Q.-D. Ho, and T. Le-Ngoc, "Attainable throughput, delay and scalability for geographic routing on smart grid neighbor area networks," in *IEEE Wireless Communications and Networking Conference (WCNC'2013)*, Shanghai, China, Apr. 2013.

[52] Q.-D. Ho, G. Rajalingham, and T. Le-Ngoc, "Performance and applicability of geographic-based routing in smart grid's neighbor area networks," in *Advanced Technologies for Communications (ATC), 2013 International Conference on*, Oct. 2013, pp. 215–219.

[53] Q.-D. Ho, Y. Gao, G. Rajalingham, and T. Le-Ngoc, "Robustness of the routing protocol for low-power and lossy networks (rpl) in smart grid's neighbor-area networks," in *IEEE International Conference on Communications (ICC'2014)*, London, UK, Jun. 2015.

[54] "RPL: IPv6 routing protocol for low-power and lossy networks," Internet Engineering Task Force (IETF), RFC 6550, March 2012.

[55] "Routing metrics used for path calculation in low-power and lossy networks," Internet Engineering Task Force (IETF), RFC 6551, March 2012.

[56] Y. Gobena *et al.*, "Practical architecture considerations for smart grid WAN network," in *Proc. Power Systems Conference and Exposition (IEEE/PES)*, 2011, pp. 1–6.

[57] K. C. Budka, J. G. Deshpande, T. L. Doumi, M. Madden, and T. Mew, "Communication network architecture and design principles for smart grids," Alcatel-Lucent, Tech. Rep., 2010.

[58] "Communications requirements of smart grid technologies," US's Department of Energy, Tech. Rep., Oct. 2010.

[59] *IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation*, IEEE 1646-2004 Std., 2011.

[60] J. G. Deshpande, E. Kim, , and M. Thottan, "Differentiated services QoS in smart grid communication networks," Alcatel-Lucent, Tech. Rep., 2011.

[61] V. Gungor *et al.*, "A survey on smart grid potential applications and communication requirements," *IEEE Transactions on Industrial Informatics,*, vol. 9, no. 1, pp. 28–42, Feb. 2013.

[62] "Distribution operations curtails customer load for grid management," SCE Internal, Jan. 2010.

[63] "Outage management: The electric utility's no.1 headache," TROPOS networks, Tech. Rep., Jul. 2007.

[64] G. Hataway, T. Warren, and C. Stephens, "Implementation of a high-speed distribution network reconfiguration scheme," in *Proc. Power Systems Conference: Advanced Metering, Protection, Control, Communication, and Distributed Resources*, Mar. 2006, pp. 440–446.

[65] "Voltage regulation and protection issues in distribution feeders with distributed generation," SCE, Jan. 2010.

[66] Z. Huang and J. Dagle, "Synchrophasor measurements: System architecture and performance evaluation in supporting wide-area applications," in *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*, July 2008, pp. 1–3.

[67] P. Thai, "Packet-level QoS over RPL: Routing protocol for low-power and lossy networks," Master's thesis, Drexel University, Philadelphia, PA, 2011.

[68] I. Al-Anbagi, "Quality of service for wireless sensor networks in smart grid applications," Master's thesis, University of Ottawa, Ottawa, Canada, 2013.

[69] N. T. Long, M.-P. Uwase, J. Tiberghien, and K. Steenhaut, "QoS-aware cross-layer mechanism for multiple instances RPL," in *2013 International Conference on Advanced Technologies for Communications (ATC'13)*, Ho Chi Minh City, Vietnam, October 2013.

[70] G. Rajalingham, Y. Gao, Q.-D. Ho, and T. Le-Ngoc, "Quality of service differentiation for smart grid neighbor area networks through multiple rpl instances," in *Proceedings of the 10th ACM Symposium on QoS and Security for Wireless and Mobile Networks*, ser. Q2SWinet '14. New York, NY, USA: ACM, 2014, pp. 17–24.

[71] *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*, IEEE Std 802.11b-1999 Std., 2001.

[72] V. András and H. Rudolf, "An overview of the OMNeT++ simulation environment," in *Simutools 08 Proceedings of the 1st international conference on Simulation tools and techniques for communications networks and systems and workshops*, 2008, pp. 1–10.

[73] *NIST Priority Action Plan 2 - Guidelines for Assessing Wireless Standards for Smart Grid Applications*, National Institude of Standards and Technology Std., 2011.

[74] A. S. M. Medard, *Network Coding: Fundamentals and Applications*. Academic Press, Oct. 2013.

[75] R. Bassoli, H. Marques, J. Rodriguez, K. Shum, and R. Tafazolli, "Network coding theory: A survey," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 1950–1978, Apr. 2013.

[76] G. Rajalingham, Q.-D. Ho, and T. Le-Ngoc, "Random linear network coding for converge-cast smart grid wireless networks," in *Communications (QBSC), 2014 27th Biennial Symposium on*, June 2014, pp. 208–212.

[77] A. Dimakis, P. Godfrey, Y. Wu, M. Wainwright, and K. Ramchandran, "Network coding for distributed storage systems," *IEEE Trans. Information Theory*, vol. 56, pp. 4539–4551, Sep. 2010.

[78] A. Kamra, V. Misra, J. Feldman, and D. Rubenstein, "Growth codes: maximizing sensor network data persistence," in *Proc. the 2006 conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM)*, Oct. 2006, pp. 255–266.

[79] G. Wang and G. Feng, "Network coding for enhancing data robustness in low-power and lossy networks," Network Working Group, Internet Draft, draft-wang-roll-data-robustness-00, Nov. 2013.

[80] R. Prior, D. E. Lucani, Y. Phulpin, M. Nistor, and J. Barros, "Network coding protocols for smart grid communications," *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1523–1531, May 2014.