Performance and Applicability of Candidate Routing Protocols for Smart Grid's Wireless Mesh Neighbor-Area Networks

Yue Gao

Department of Electrical & Computer Engineering
McGill University
Montreal, Canada

2014-04-15

A thesis submitted to McGill University
in partial fulfilment of the requirements of the degree of Master

Abstract

Neighbor-area network (NAN) is one of the most important segments of a smart grid communication network (SGCN) since it is responsible for information exchanges between utilities and a large number of smart meters (SMs) to enable various important smart grid (SG) applications. Greedy perimeter stateless routing (GPSR) and the routing protocol for low-power and lossy networks (RPL) have been considered for wireless mesh NANs. This thesis presents a study on performance and applicability of these two protocols in various NAN scenarios. Specifically, packet transmission reliability and delay of GPSR and RPL in an IEEE 802.11-based wireless mesh NAN are evaluated through extensive simulations. The effects of wireless channel characteristics, network offered load levels and cluster sizes are also investigated to assess feasibility of these two protocols with respect to different SG application requirements.

In addition to comparing the reliability and efficiency of GPSR and RPL, special attentions have been addressed to the system robustness in the presence of node failures. Node failures could hinder the network connectivity and degrade the reliability of the NAN segment of the SGCN. This thesis proposes a mechanism, namely proactive parent switching (PPS) that adaptively switches preferred parent nodes in order to help RPL quickly deflect network traffics from points of failures in the NAN scenario. Simulations with varying network availability and traffic load are carried out in order to understand the impact of node failures to the routing performance of GPSR and RPL with PPS and how the PPS can help RPL mitigate them.

The extensive simulation results first reveal that RPL has higher transmission reliability and lower delays than GPSR in all the three considered scenarios, i.e., different channel conditions, traffic loads and network sizes. Moreover, under the consideration of multiple node failures, RPL with PPS outperforms both conventional RPL and GPSR in transmission reliability since it can efficiently reroute packets over multiple alternative paths. Consequently, the results from this thesis indicate that RPL with PPS is a suitable routing protocol for NAN communications. However, RPL may impose extra requirements relating to its routing table management and maintenance. Therefore, there is still room for improving these two protocols for specific SG applications.

Résumé

Le réseau de région voisine (NAN: neighbor-area network) est l'un des plus importants composants du réseau de communication du smart grid puisqu'il est responsable de l'échange d'information entre les utilitaires et un large nombre de compteurs intelligents pour réaliser divers applications du smart grid (SG). Les deux protocoles de routage, GPSR (greedy perimeter stateless routing) et RPL (routing protocol for low-power and lossy networks), ont été considérés pour les NANs maillés sans fil. Cette thèse présente une étude sur la comparaison des performances et des applications de ces deux protocoles dans différents scénarios de NAN. Particulièrement, la fiabilité de la transmission de paquet et le délai du GPSR et du RPL dans les réseaux maillés IEEE 802.11 sont évalués par des simulations étendues. Les effets des caractéristiques du canal sans fil, des niveaux de charges de trafic et de la taille des groupes sont aussi examinés pour évaluer la faisabilité de ces deux protocoles par rapport aux différentes applications du SG.

En plus de comparer la fiabilité et l'efficacité du GPSR et du RPL, une attention particulière est adressée à la robustesse des systèmes en présence de nœuds défaillants. Les nœuds défaillants peuvent gêner la connectivité du réseau et dégrader la fiabilité du NAN. Cette thèse propose un mécanisme, nommé changement de parent proactif (PPS: proactive parent switching), qui change au nœud parent approprié afin d'aider le RPL à détourner rapidement le trafic des points de défaillance dans le NAN. Des simulations en variant la disponibilité du réseau et la charge de trafic sont performés afin de comprendre l'impacte des nœuds défaillants à la performance du routage du GPSR et du RPL avec le PPS, et comment le PPS peut aider le RPL à les éviter.

Les résultats de simulation révèlent que le RPL possède une fiabilité de transmission plus haute et un délai plus court que le GPSR dans les trois scénarios considérés, c'est-à-dire, différentes conditions de canal, charges de trafic et tailles du réseau. De plus, sous la condition de plusieurs nœuds défaillants, le RPL avec le PPS dépasse le RPL et le GPSR conventionnels en termes de fiabilité de transmission puisqu'il peut réacheminer efficacement les paquets à travers plusieurs trajets alternatifs. Par conséquent, les résultats de cette thèse indiquent que le RPL avec le PPS est un protocole de routage approprié pour les communications NAN. Cependant, le RPL peut imposer un traitement additionnel pour la gérance et la maintenance de sa table de routage. Donc, ces deux protocoles peuvent être améliorés pour des applications spécifiques du SG.

Acknowledgements

First of all, I would like to express the deepest appreciation to my supervisor, Prof. Tho Le-Ngoc, for his encouragement, guidance and support for my study. His profound knowledge, rigorous scientific attitude and patient guidance give me inspiration and motivation in my research process.

Next, I would like to thank all research group members for having interesting discussions and providing meticulous advices on my work. I would particularly like to thank Dr. Quang-Dung Ho and Gowdemy Rajalingham who kindly help me move on throughout my entire study and provide invaluable suggestions and comments on my papers and thesis. I am also particularly grateful for insightful comments and thorough suggestions given by Chonwang Chao on my thesis. I also would like to thank to Ishaan Singh and Rwan Ibrahim for their insightful and detailed discussions on my project.

In addition, I also take this opportunity to express my gratitude to my parents, relatives and friends who have encouraged me and provided continuous support to me. My best regards and blessings are given to all of those who supported me in any respect during the completion of my MEng studies.

Finally, I would like to thank the Natural Sciences and Engineering Research Council (NSERC) and industrial and government partners for their financial support.

Contents

List of Figures

List of Tables

List of Acronyms

ACK	Acknowledgment
AMC	Adaptive Modulation and Channel Coding
AMI	Advanced Metering Infrastructure
AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
CCK	Complementary Code Keying
CDF	Cumulative Distribution Function
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear-To-Send
DA	Distribution Automation
DAG	Directed Acyclic Graph
DAP	Data Aggregation Point
DBPSK	Differential Binary Phase Shift Keying
DIFS	Distributed Coordination Function Interframe Spacing
DIO	DODAG Information Object
DIS	DODAG Information Solicitation
DODAG	Direction-Oriented Directed Acyclic Graph
DQPSK	Differential Quaternary Phase Shift Keying
DSSS	Direct Sequence Spread Spectrum

EIFS	Extended Interframe Spacing
ETX	Expected Transmission Count
GF	Greedy Forwarding
GPSR	Greedy Perimeter Stateless Routing
HAN	Home-Area Network
IETF	Internet Engineering Task Force
MAC	Medium Access Control
MFR	Most Forwarding Progress within Radius
MP2P	MultiPoint-to-Point
MPDU	MAC Protocol Data Unit
NAN	Neighbor-Area Network
NFP	Nearest with Forwarding Progress
NIST	National Institute and Technology
NSERC	Natural Sciences and Engineering Research Council
OF	Objective Function
P2MP	Point-to-MultiPoint
PAP02	Smart Grid Priority Action Plan 2
PDR	Packet Delivery Ratio
PER	Packet Error Rate
PHY	Physical Layer
PIFS	Point Coordination Function Interframe Spacing
PLC	Power Line Communications
PLCP	PHY Layer Convergence Procedure
PPS	Proactive Parent Switching
PRR	Packet Reception Rate

QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
ROLL	Routing over Low Power and Lossy Network
RPL	Routing Protocol for Low Power and Lossy Networks
RTS	Request-To-Send
SG	Smart Grid
SGCN	Smart Grid Communication Network
SIFS	Short Interframe Spacing
SM	Smart Meter
SNR	Signal-to-Noise-Ratio
ST	Slot Time
WAN	Wide-Area Network
WMN	Wireless Mesh Network

Chapter 1

Introduction

1.1 Smart Grid

The power grid has not been innovated over the last century while there have been increasing demands on electrical energy, incidences of electricity shortages, power quality problems, rolling blackouts, electricity price spikes, and environmental issues. This has urged many countries to enhance the efficiency and reliability of their existing power grids as well as to seek alternative sources of reliable and high-quality electricity. As a result, "Smart Grid" (SG) has been introduced. There are many definitions of SG, some functional, some technological, and some benefits-oriented. According to [2], 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". It can monitor, protect and automatically optimize the operation of its interconnected elements including central and distributed power plants, energy storage stations, transmission and distribution networks, industrial and building automation systems, end-user thermostats, electric vehicles, appliances and other household devices. In essence, the primary objectives of SG are to allow utilities to generate and distribute electricity efficiently and to allow consumers to optimize their energy consumption.

Conceptually, the architecture of SG can be considered as the integration of power system layer and communication layer. The power system layer, as presented in Fig. 1.1, is comprised of four basic sub-systems that are bulk power generation, power transmission system, power distribution system, and power consumption. These sub-systems are explained as follows:

- The power generation combines conventional generation resources with renewable resources to generate electricity to supply consumers' demands. The utilization of distributed renewable energy sources becomes a powerful and indispensable complement to compensate the limitations of traditional power system.

- The power transmission is a high voltage transmission grid to deliver power from power generators to nearby power distribution systems. The transmission system must be expanded and upgraded and has capabilities to integrate renewable resources into the existing power system in an economically and operationally efficient way. It also requires appropriate long distance distribution with great quantities and qualities electricity, few losses and low cost.

- The power distribution delivers electrical power from power transmission system to consumers through low-voltage distribution cables and electrical substations. It has to be optimized such that the power loss and cost of transmissions are minimized given constraints such as power demand and transmission line capacity.

- The power consumption is composed of different types of power consumers (e.g., home, industry, and government consumers). Relied on different communications technologies, power consumption devices can be remotely controlled and switched the working modes.

The distinguishing feature of SG, compared to the existing electrical grid, is that the above-mentioned power sub-systems are integrated with the supporting communication layer, commonly referred to as Smart Grid Communication Network (SGCN), as shown in Fig. 1.2. SGCN plays the essential role to upgrade the existing power grid from unidirectional power flow with limited real-time control system to a bidirectional electricity system providing real-time and reliable communication to achieve self-regulation and management. It is primarily responsible for connecting the distributed electric devices to exchange real-time information in order to monitor, control, and automate the whole power grid. With such an

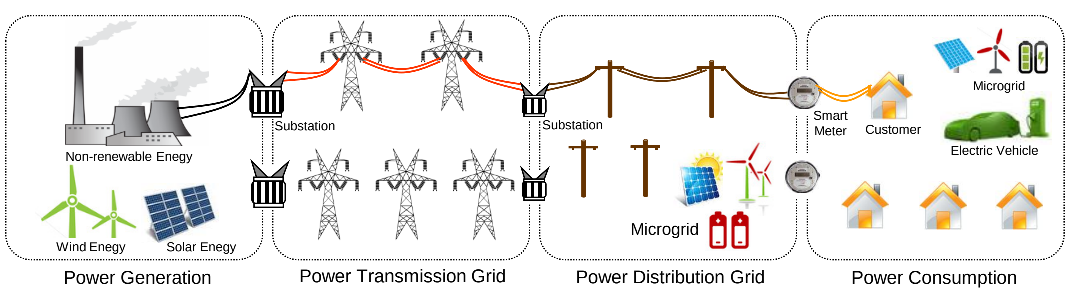

Figure 1.1: The power system layer of SG.

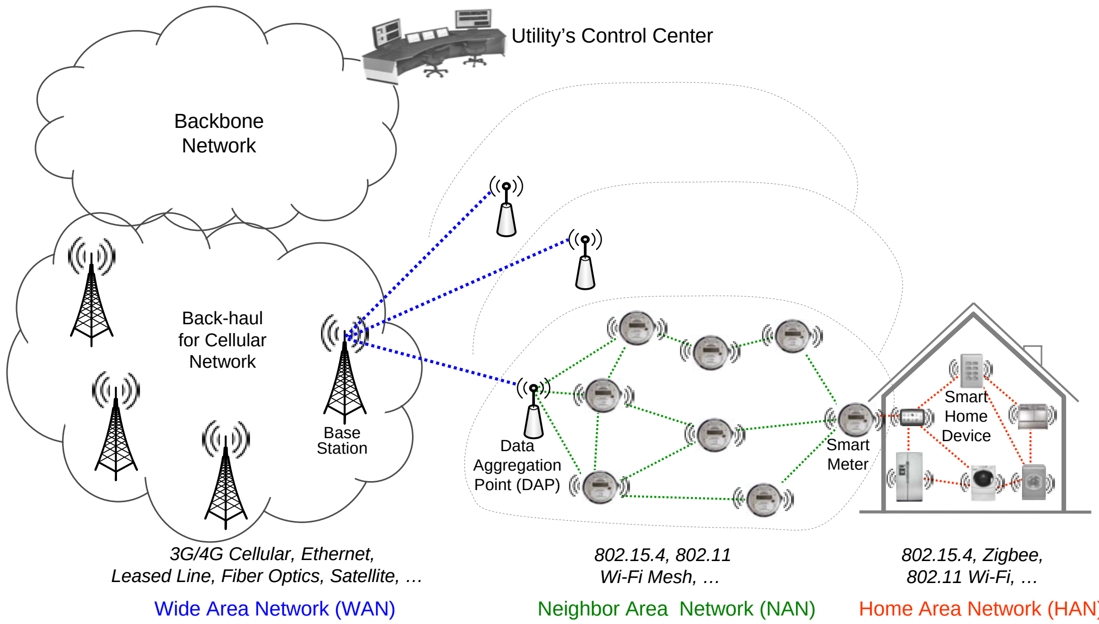

Figure 1.2: The communication system layer of SG.

energy management network, power flowing can be shared and distributed from diverse distributed generator and renewable energy sources to power consumers over a large-scale area. Also blackouts will be handled quicker when the utilities receive the alerts so that the huge cost on power disruptions and cascading failures will be minimized. The real-time bidirectional communications are the fundamental infrastructure required to accomplish the comprehensive power system management services with secure, intensive and time-sensitive information exchange. It helps both utilities and consumers better manage supply and demand loads so that they can save energy costs and reduce peak usages.

1.2 Smart Grid Communication Network

Communication reliability, robustness and efficiency are the major requirements addressed in SGCN. To meet these requirements, a hierarchical network architecture, as shown in Fig. 1.2, has been proposed for SGCN: home-area network (HAN) for communications among appliances and with smart meters (SMs) in residential and commercial buildings; neighbor-area network (NAN) for communications among SMs within a cluster of homes/buildings as the crucial intermediate network to connect consumers and utilities; wide-area network (WAN) for long-haul communications between NAN and utility's control centers. These segments of SGCN are interconnected through gateways: a data aggregation point (DAP) between WAN and NAN and a SM between NAN and HAN. DAP plays an important role to integrate the whole SG communication by exchanging information between HAN and WAN. For example, DAP forwards the periodic meter read up to the control centre in WAN and relays a command requesting consumption information to a SM in HAN if no packet received over a long time.

Each of these gateways communicates through the network with adjacent nodes. Technical details of each segment are summarized as follows:

1.2.1 Home-Area Network (HAN)

HAN is responsible for the communications among smart appliances and with a gateway (which is usually SM) at the consumer premise. Automated digital devices inside the building (e.g., air conditioner, dishwasher, dryer, refrigerator, kitchen stove, and washing machine) can be monitored and controlled by a control center or consumers to optimize the power supply and consumption. In addition, consumers can track the power consumption and perform optimization to reduce power costs. This network can support functions such as cycling air conditioners off during peak load conditions, sharing consumption data with in-home displays, or enabling a card-activated prepayment scheme. Many different technologies are considered to be used in HAN technologies to transfer data to the control center for analysis and optimization such as ZigBee, Wi-Fi, Ethernet, Z-Wave, HomePlug, Wireless M-Bus, Wavenis, etc. [3]. Wireless communications technologies are preferable choices due to their low cost and flexibility of infrastructure.

1.2.2 Neighbor-Area Network (NAN)

NAN is the communication network connecting HAN and WAN. It is usually divided into clusters where DAPs work as cluster heads relaying information between SMs and WAN. The number of SMs that each DAP communicates with varies from a few hundreds to thousands depending on grid topology and communication technologies and protocols. SMs are intermediate agents transporting information between HAN and WAN. DAPs may locally process received information (e.g., data aggregation, data filtering, etc.). They then forward processed information to utility's control centers over WAN. The networking communication protocols applied for NAN are required to be reliable, secure, power-efficient, and low-latency. They are also expected to be robust to link and/or device failures. There are quite a few technologies in contention to be used to implement NAN [3]. They include short-range and low-power IEEE 802.15.4/Zigbee wireless technology, broadband wireless standards like IEEE 802.11, IEEE 802.16 WiMAX, 3G/4G cellular, Power Line Communication (PLC), optical fiber communication, etc. Wireless mesh networking has appeared as a promising candidate due to its low installation and maintenance costs.

1.2.3 Wide-Area Network (WAN)

It covers the long-haul distances from DAPs to the control center throughout the distribution and transmission grid. The LAN enterprise network, core/metro network and backhaul network are integrated to be the WAN. It achieves the communications among different regions and systems including control center, substations, storage facilities, transformers and energy management systems. The utility's WAN also provides the two-way network needed for substation communication, distribution automation (DA), and power quality monitoring while also supporting aggregation and backhaul for AMI and any DR and demand-side management applications [4]. The data from home energy system is collected, processed and stored in the control centers and used to optimize communication capabilities for the power transmission and distribution and management on power outages and other failures. WAN can be implemented over fiber or wireless media using Ethernet or cellular protocols.

1.3 Wireless Routing in NANs: A Literature Review

Among the three representative segments of SGCN mentioned above, NAN has been attracting the most attentions from both academia and industry since it is responsible for gathering a huge volume of various types of data and exchanging important control signals between millions of SMs installed at customer premises and utility's control centers. It is the primary enabler for important SG applications such as AMI, DR, distributed energy resources and storage management, etc. Having the most crucial responsibility for the operating and coordinating the whole SG system, NAN serves as the medium to connect the HANs and WAN. Most traffics in NANs are exchanged in a periodic manner while some others might be transmitted by on-demand requests or event-based triggers. Different kinds of traffic induce various requirements that make NAN a very unique type of networking environment. Therefore, NAN has to be able to differentiate several types of input data and provide high quality of service (QoS) propriety to time-critical traffics. Besides, to ensure data confidentiality, integrity and privacy for commercial purposes, NAN is also expected to provide highly secure data transmission for electricity information, services queries and responses. Furthermore, since a huge volume of data transverses upward and downward through NAN, the capability to accommodate network congestions and performance degradation also needs to be concerned. All these requirements are needed to be coped with in order to guarantee the whole implementations and operations of SG system.

There are various wired and wireless communication technologies that can be used to implement NANs such as broadband via the telephone lines or cable services, PLC, wireless cellular and wireless mesh networks (WMNs). Each technology has its own advantages and disadvantages in terms of costs (i.e. deployment, maintenance, and operation), coverage, communication reliability, latency and security, etc. Wireless technology is preferred in NAN over wired since it is expensive and impractical to deploy long copper or fiber-optic cables over sparse areas in NAN, such as suburban or rural areas. Adding or removing SMs and other components with wired connections are also costly and time consuming. In comparison with wired communications, the communication coverage of wireless can be easily expanded by simply adding routers and the installation and maintenance costs are relatively low. All these reasons drive the wireless technology to be a better option for communications in NAN. However, the wireless communication is relatively unreliable and easy to be affected by other wireless signals or surrounding obstacles. Therefore, a promising routing protocol to ensure efficient and reliable data transmission for SM applications is desired. Fig. 1.2 presents a widely-accepted two-tier configuration for NANs where WMNs are employed jointly with cellular networks. In the first tier, SMs are connected to each other using wireless mesh topology which is resilience to node failures and link fluctuations and requires low deployment/maintenance costs. Data from each cluster of SMs is collected at a DAP and relayed to the second tier over 3G/4G cellular networks that have very wide coverage while offering a high data rate and low latency. DAP plays an important role in NAN to support bi-directional traffics, which are gathering upward sensing measurement data traffics from SMs and sending downward instructions to control devices in HAN or reply queries from SMs.

Routing protocol is one of the key factors that determine the system performance of WMNs. As a result, wireless mesh routing protocols for NANs are the focus of large number of researches in the area of SG over the last few years. The study presented in [5] surveys various routing protocols selected for NAN scenarios. Geographic routing and RPL have been identified as the most promising routing protocol for NANs.

One of the compelling advantages of geographic routing protocols is that it can achieve network wide routing while maintaining only neighborhood information at each node. The simplicity of geographic routing leads to good scalability since it is no necessary to keep routing tables up-to-date and to have a global view of the network topology and its changes. Geographic routing protocols allow routers to be nearly stateless because forwarding decisions are based on location information of the destinations and the location information of one-hop neighbors. No routing table is needed to be constructed or maintained. 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 geographic routing can be kept at a considerably low level. In addition to these advantages, the fact that locations of NAN devices are fixed and accurately known promotes geographic routing protocols as one of the promising solutions for NANs.

The work in [6] presents the study of geographic routing in the wireless mesh based smart metering solution. SMs are provided with the geographical coordinates of the DAP which represents the destinations for their upward traffics whilst the DAP knows the coordinates of all SMs for downward control traffics. Performance of geographic routing in various realistic smart metering scenarios is presented by using simulations. Received packet ratios given by the protocol are measured against network scales, offered traffic rates and placements of routers and concentrators. For the small-scale scenario, the system performs with a received packet ratio of 100% for a low message frequency. However, success rate decreases with increasing message frequency due to collisions in some central nodes. For a large-scale scenario employing multiple routers and concentrators, a very high overall success rate of the system is still observed for low message frequency.

RPL is a representative protocol which captures most of the ideas introduced by self-organizing coordinate protocols [7]. RPL exhibits many advantages that are desirable in the NAN setting. First, the tree-like structure constructed by RPL matches well with the physical deployment and communication model of SMs (nodes) and DAPs (sinks or roots). Second, RPL is designed to be able to incorporate various types of routing metrics and constraints that can be addictive, multiplicative, inclusive/exclusive and so on. Therefore, both QoS-aware and constraint-based routing disciplines can be supported. Third, RPL allows multiple logical routing graphs to operate concurrently and independently to provide QoS differentiation for different classes of traffic in the NANs.

The work in [8] analyzes the stability of RPL whose DAG is built based on link layer delays. It is observed that the delay fluctuation introduced by the IEEE 802.15.4 medium access control (MAC) layer negatively influences RPL's stability. In order to dampen the link layer delay fluctuation, the author proposes the use of memory in delay calculation which can reduce the mean and variance of the end-to-end latency and thus improve the protocol stability. The authors in [9] provide a practical implementation of RPL with a number of proper modifications so as to fit into the AMI structure and meet stringent requirements enforced by the AMI. In particular, Expected Transmission Count (ETX) link metric and a novel ETX-based rank computation method are used to construct and maintain the DAG. Extensive simulation results in [9] 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 AODV, and produces satisfactory performances in terms of packet delivery ratio and transmission delay.

In [10], a simulation-based performance evaluation of RPL in real-life 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 with the help of periodic transmission of new DAG sequence number by the DAG root. For local repair, upon loosing parents, a node will try to quickly and locally find an alternate parent. Results in [10] show that when local repair mechanism is employed, the network fixes local connection outage to parent much quicker than if using global repair mechanism only. However, there are a few incidents where the outage time gets large to an order comparable with DAG sequence number period when DODAG information solicitation (DIS) or DODAG Information Object (DIO) is not heard for a long time. Self-organizing and self-healing solutions for RPL are proposed in [11]. SMs are able to automatically discover DAPs in their vicinity and setup a single or multi-hop link to a selected DAP. An overview on the weaknesses and strengths of RPL is provided in [12]. Multiple timers that assist the trickle algorithm used by RPL are also investigated using simulations and experiments. The authors in [13] presents an experimental analysis of RPL repair process using the Contiki RPL.

1.4 Motivations and Contributions

With the objective to provide efficient, reliable and robust communication for NANs, GPSR (a representative protocol of geographic routing class) and RPL (a state-of-the-art self-organizing coordinate protocol) are emerging as two of the most promising routing protocols. GPSR is very simple, truly distributed and can exploit the location information that is inherently available in NANs. However, it has not been extensively studied for communication in NAN except for the work in [6]. Some preliminary results are presented in [6] but there are three important limitations. First, an over-simplified free-space propagation channel model is assumed while in 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 limits the usefulness of the results presented in [6]. Second, only message transmission reliability is measured in that work. Transmission delay which is one of the decisive performance metrics to be investigated in smart metering scenarios is not taken into consideration. Third, only conventional smart metering data is assumed in [6]; it may not reflect the real needs of the future SG due to the emerging of many advanced SG applications (e.g., distribution automation, fault detection and restoration). As compared to

GPSR, RPL possesses many advanced features, such as dynamic routing graph, multiple instances routing, loop detection and avoidance. The performance of RPL in some aspects, namely, routing reliability, end-to-end latency and robustness, has been recently evaluated in [8] [9] [10]. However, the feasibility of RPL in respect to the routing requirements in NANs has not been thoroughly studied. Moreover, the superiority of RPL over GPSR under the constrains imposed by SG applications is still questionable due to the non-existence of work that gives in-depth evaluations and comparisons of GPSR and RPL.

This thesis fills the aforementioned gaps by first providing a detailed and quantitative evaluation comparing the performance of GPSR and RPL in different NAN scenarios. Various performance metrics are investigated, including packet delivery ratio, transmission delay and average transmission count. The effects of various NAN parameters on the performance of these two protocols are also investigated. Those parameters include wireless channel condition (i.e., channel shadowing variance), rate of data traffic generated by each SM and the NAN cluster size (i.e., total number of SMs per DAP). The results obtained can then determine the applicability, limitations, advantages/disadvantages of each algorithm in wireless mesh NANs with respect to the quality of services required by various SG applications.

Additionally, an important issue is that the robustness of GPSR and RPL in the case of node failures has not received sufficient attention in existing work. Therefore, this thesis also attempts to study the robustness of these two candidate routing protocols when a portion of network fails. An adaptive local repair mechanism is proposed to integrate with RPL in order to quickly recover from node failures. The proposed mechanism PPS can effectively help RPL reroute network traffic from points of failures. It proactively nominates another parent as the next hop once the preferred parent is unreachable after a predefined number of unsuccessful MAC layer transmissions/re-transmissions. Neighbor information supplied by the network layer is exploited to support the next hop switching procedure performed in the MAC layer. Extensive simulations are carried out to demonstrate the effectiveness of PPS.

1.5 Thesis Outline

The remainder of this thesis is organized as follows. Chapter 2 presents a number of key technical features of GPSR and RPL and the detailed implementation of these two protocols for NANs. The routing metrics for each algorithm are selected and the ideas and operations of the proposed PPS mechanism for RPL are also presented. Chapter 3 explains the simulation setup and parameters that are used to investigate the operations and performances of GPSR and RPL. Simulation results are then presented in Chapter 4. GPSR and RPL are compared in terms of transmission reliability and delay. The effects of various factors, such as channel shadowing levels, per-meter data rate, NAN cluster size and network availability, to the performance of these two protocols are investigated. Finally, Chapter 5 concludes this thesis.

Chapter 2

Implementation of GPSR and RPL[1]

2.1 GPSR

2.1.1 Protocol Description

GPSR is a representative implementation of the geographic routing family of routing protocols that route traffic based on the knowledge of a node's position along with those of its neighbors and the sink node. An extensive survey of existing work dealing with geographic routing protocols is presented in [16]. In its simplest form, Greedy forwarding (GF), when a node receives a message, it relays the message to its neighbor geographically closest to the sink, as illustrated in Fig. 2.1. Alternatively, one can consider another notion of progress, namely the projected distance on the source-destination-line, i.e., most forwarding progress within radius (MFR), the minimum angle between neighbor and destination, i.e., compass routing, or nearest with forwarding progress (NFP).

The dominant factor of GPSR's greedy forwarding is knowledge of the physical location of each participating node along the path. In the initial phase, the source node marks a packet with respect to a destination node and makes a locally optimal choice for the next hop. The packet's next hop is always the neighbor who is geographically closest to the destination, as illustrated by Fig. 2.1. The packet will be forwarded in this hop-by-hop and fully-distributed manner until the destination is reached. The success of greedy forwarding can be ensured if the

[1] Parts of chapter 2 have been presented in the "Challenges and Research Opportunities in Wireless Communications Networks for Smart Grid", in the IEEE Wireless Communications Magazine 2013 [14], and have been accepted for publication in the "Performance and Applicability of Candidate Routing Protocols for Smart Grid's Wireless Mesh Neighbor-Area Networks", in the IEEE International Conference on Communications 2014 [15].

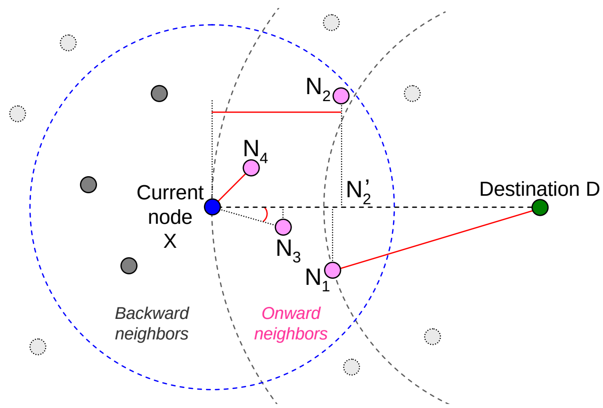

Figure 2.1: Examples of different GF strategies: (N_1) = shortest geographical distance, (N_2) = MFR, (N_3) = compass routing and (N_4) = NFP.

node density is high enough to allow for at least one neighbor allocated in a $2\pi/3$ angular sector of each intermediate node [17].

GPSR updates neighbor position information through a simple hello message protocol. Nodes periodically broadcast short hello messages advertising position information to all surrounding neighbors. Every node has a neighbor table for maintaining up-to-date geographic information of each neighbor. If a node does not receive an updated hello messages from one of its neighbors before the timeout timer T expires, that neighbor will be considered as lost and its corresponding entry will be removed from the neighbor table. In the worst case, a void region exists and there is no other neighbor closer to the destination, then the greedy forwarding strategy fails due to this local minimum problem. When this occurs, GPSR recovers by forwarding in perimeter mode and the packet traverses successively closer faces of a planar sub-graph of the radio network connectivity graph, until reaching a node closer to the destination, where greedy forwarding can resume. More detailed descriptions of GPSR can be found in [17]. Existing work shows that, compared to GF, GPSR can improve the packet delivery ratio [7].

2.1.2 Forwarding Schemes

2.1.2.1 Simple Greedy Forwarding

The original GPSR employs a GF scheme that is an efficient, low-overhead method of data delivery when used on a network with sufficient density, accurate location information and high link reliability independent of distance within the physical radio range. Nevertheless, such a forwarding scheme performs poorly in realistic conditions since it tends to forward packets on lossy links. Packets are delivered to neighbors that are closest to the final destination. However, such neighbors tend to be further away from the current node and thus are more likely to experience poor link quality which results in low supportable data rate or even high rate of packet loss. Obviously, this poor-link phenomenon must be taken into account when selecting next hops.

2.1.2.2 Greedy Forwarding with Blacklisting

GPSR takes advantage of knowing available information on the geographic locations of each node and simply forwards the packets through the shortest path to the destination. It eliminates the requirement of sharing and maintaining routing information. Nodes forward each packet by making hop-by-hop decision rather than following a pre-constructed end-to-end path. The simplicity of this forwarding decision, i.e., no requirements of route discovery and routing table maintenance, and its adaptivity to network changes are all considerable advantages of GPSR in the large-scale NAN. Moreover, in order to discover reliable paths and reduce the impact of channel variation over different links, the blacklisting scheme proposed in [18] and [19] is adopted.

In a nutshell, blacklisting attempts to exclude neighbors with low link quality. Neighbors are classified as favorable or not based on their distance and link quality with respect to the current node. This classification is done with the introduction of a predefined distance threshold, namely optimal distance. The simulation results in [18] demonstrate that GPSR with blacklisting based on optimal forwarding distance can achieve a higher packet delivery ratio and lower transmission delay as compared to the original GPSR. The detailed calculations and explanations of how the channel and radio affect the optimal distance given in [18] and [19] are presented in Appendix A.

2.1.3 Neighbor Connectivity and Failure Detection

Greedy forwarding in GPSR is associated with a simple periodic broadcast of hello messages. Besides keeping track of neighborhood topology, periodic hello messages help nodes be aware of their local link connectivity to other available neighbors. A better fault tolerance is achieved with higher hello message frequency. Especially in the highly dynamic network in which many nodes may randomly fail, the rate of sending hello messages should be sufficiently high so that nodes can quickly detect the loss of surrounding neighbors and then accurately route packets to an active one. However, higher frequency in exchanging hello messages will result in higher routing control overhead. The incurred overhead may lead to channel contention and waste network resources and thereby degrade network performance.

The precision of neighborhood status is also affected by the frequency at which the neighbor table is refreshed. Within a predefined interval, each neighbor entry is refreshed after receiving several up-to-date hello messages. If no hello message has been received from a neighbor during that period, that neighbor is deemed lost and the corresponding connection is broken. The refresh interval needs to be defined properly in order to reflect the dynamics of neighbor changes. If it is too large, the neighbor status reflects out-dated neighbor information and data packets can be sent to failed nodes. Based on suggestions from [20], the neighbor table refresh interval is defined to be twice that of the hello message broadcasts. Each node broadcasts two hello messages to notify its availability. It is tolerable if one hello message is lost due to link fluctuation or packet collision. Loss of two hello messages from a neighbor within the refresh interval indicates that either the neighbor failed or the connected link is really weak. The corresponding neighbor entry will be removed since it is undesirable to forward data packets via such a neighbor.

It is obvious that the frequency of hello messages also directly affects the awareness of neighborhood connectivity, and thus the transmission reliability of GPSR. In order to obtain the desired accuracy of the route/neighbor discovery, highly frequent flooding of hello messages is required and consequently the channel becomes susceptible to overloading. With the aim of efficiently using the bandwidth while still maintaining adequate accuracy of neighbor connectivity, the hello rate is set to be equal to the data rate. With the same rate, hello messages could also indicate the up-to-date link connectivity for data packets.

2.2 RPL

2.2.1 General Description

RPL belongs to the self-organizing coordinate routing class that builds a viable coordinate system based on communication distance rather than the geographic distance used in location-based routing. It is designed as the specific routing solution for LLNs, which consist of large number of highly constrained devices with limited communication capacity, small memory, and limited energy. These devices are interconnected by lossy (wireless or wired) links with low bandwidth, high loss rate and low link reliability. Other challenges such as large number of nodes and unattended devices in severe environment need to be considered in the development of the routing protocol for LLNs. The Routing over Low power and Lossy network (ROLL), which is a working group of the Internet Engineering Task Force (IETF), proposes RPL for different routing requirements in a wide variety of application areas of LLNs. There are four main application domains that attract the need for RPL specifications: urban, industrial, building automation and home automation scenarios. The smart grid application belongs to the urban application scenarios with the deployment of the AMI's advanced two-way communication. RPL with appropriate specifications is able to support the smart grid NAN communication network.

The motivation for specifying RPL is to optimize it for gathering sensing measurement data and forwarding it to the data collector (multipoint-to-point (MP2P) traffics) or sending instructions from the collector to control devices or querying replies (point-to-multipoint (P2MP) traffics). To support those types of routing traffics, the basic construction of RPL is a Directed Acyclic Graph (DAG) that is used to maintain the network state information. The key concept used in RPL is the destination oriented directed acyclic graph (DODAG) which is a tree structure specifying the routing paths between a root and the remaining nodes. The root is typically a gateway which acts as a common transit point that bridges every network node with a backbone network [21]. Each node in the DODAG is assigned a rank that represents the cost of reaching the root as per the objective function (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 [22]. The rank of a given node is calculated based on the ranks of its neighbors, the costs to reach each of these neighbors and other routing metrics. Initially, the root of DODAG starts sending out 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 the information about the identification of the DODAG, the rank of the broadcasting node, and parameters specifying the OF. DIO's are broadcasted from each node, triggered by the trickle timer. The interval of the trickle timer is exponentially increased when the network is stable. Thus, updating of DIOs is suppressed and accordingly redundant broadcasting is reduced.

When forming the DODAG topology, a node receiving a DIO message and ready to participate in the DODAG will add the DIO sender to its parent list, compute its own rank utilizing the rank information from this parent node driven by the DAG's OF. Then, its own updated rank information will be broadcast in a DIO message to allow the remaining nodes in the network to join the DODAG, discover the upward route to the sink and identify their set of neighbors and parents. The neighbor and parent set are also selected based on the OF indication received in the DIO message. Each node maintains the candidate neighbor set that contains all nodes that can be reached via link-local multicast. The candidate neighbor set is comprised of children set, sibling set and parent set. The selection of these three sets is dependent on the OF. In the severe shadowing scenario, when certain links disappear temporarily, the corresponding link cost over such a link may increases. When a node receives a DIO message with higher or equal rank to the current node, it retains the sender in its children set or sibling set, respectively.

The sender with lower rank is cached in the parent set. The preferred parent is selected from the parent set with the lowest rank so that it optimally meets the optimization objectives as the preferred next hop when routing the data packet towards the root.

In the severe shadowing scenario, when certain links disappear temporarily, the corresponding cost over such a link may increases. The RPL graph could be changed only if the link changes result in nodes re-selecting their preferred parents and consequently resetting the interval of broadcasting DIO messages. Otherwise, the temporary link disappearance and following updates of the parents, siblings and children sets might not lead to any changes to the RPL graph. Hence the stability of the RPL graph is maintained. In addition to link fluctuation from channel shadowing, node failures can occur as well. With the presence of node failure, the frequency of detecting failures and updating the RPL graph significantly affects network performance.

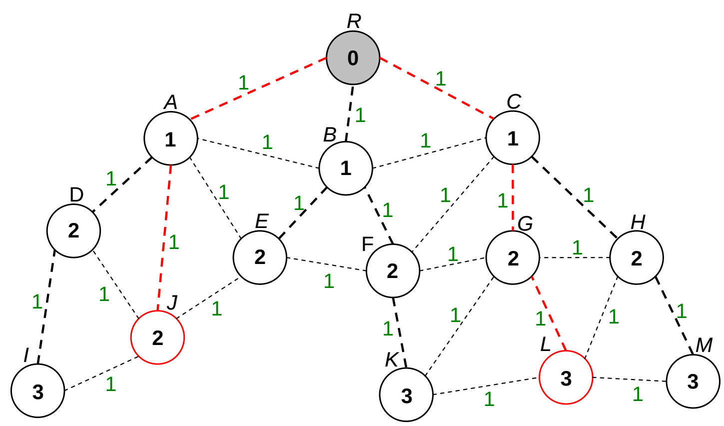

Figure 2.2: An example of DODAG using the hop count routing metric.

2.2.2 Routing Metrics

2.2.2.1 Hop Count

Hop count is the simplest and most commonly-used routing metric. Traditional wireless ad-hoc networks focus on finding paths with minimum hop count. This metric finds the routes quickly by simply computing the minimal number of hops between source and destination. The primary advantage of using this metric is its simplicity and ease of implementation. Any one hop transmission has equally one unit value and nodes only need to look for the next neighbor having minimum hop counts to the destination. Fewer hops on a path may lead to lower delay and energy consumption. Fig. 2.2 shows a DODAG constructed over a physical wireless network with hop count as the routing metric. All nodes receive DIO messages, join the DODAG and select parent sets based on the rank computation of minimizing hop count. The preferred parent of each node is randomly selected from those parents having same minimum rank values. Upward traffics are enabled by forwarding packets to their preferred parent hop-by-hop until the root node is reached. As shown in Fig. 2.2, 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: $L \to G \to C \to R$.

An important observation is that the hop count metric is only applicable with the assumption of relatively error-free links, which is sufficient in wired networks. In contrast, in wireless networks, this minimum hop count might not be always an efficient solution to find optimum paths for overall network performance. It does not consider any other characteristics of a link such as packet loss probability, fading, interference and other issues that have serious impact on wireless network link quality [23]. As a result, minimizing the hop count may lead to maximizing the distance traveled for each hop along a path, which is likely to minimize signal strength received at each receiver. Selected paths may therefore include lossy links that suffer from multiple packet losses and re-transmissions. Additionally, there could be many paths with the same minimum hop count in a dense network and each of them has widely varying link quality. Hence the random selection made by the minimum hop-count metrics is rarely able to pick optimal paths. Based on all above reasons and since the NAN is a wireless mesh network with time-varying links, this thesis proposes to employ link-quality-based routing metric for the implementation of RPL for NANs.

2.2.2.2 Expected Transmission Count (ETX)

ETX [24] is a widely-used link-quality-based routing metric that measures the expected (or average) number of transmissions, including re-transmissions, needed to successfully deliver a unicast packet across a link. An ETX of one indicates a perfect transmission medium, and an ETX of infinity represents a completely non-functional link. Due to varying characteristics of the transmission medium, ETX may vary widely from one link to another.

ETX is computed based on packet delivery ratio between the sender and the receiver in both forward and backward directions. The forward packet delivery ratio that measures the probability that a data packet sent from sender i successfully arrives at the receiver j is denoted as $p_{i,j}$. The backward packet deliver ratio that measures the probability that the acknowledgment (ACK) message sent from receiver j is successfully received at sender i is denoted as $p_{j,i}$. As a result,

$p_{i,j}p_{j,i}$ represents the probability that a packet is successfully received and acknowledged. The probability that a packet will be successfully delivered from i to j after k transmissions [25] can be expressed as $Pr_{i,j}(k)$:

$$Pr_{i,j}(k) = (1 - p_{i,j}p_{j,i})^{k-1}(p_{i,j}p_{j,i}). \tag{2.1}$$

Each transmission can be considered as a Bernoulli trial, and the number of transmissions till a packet is successfully received is a geometric variable. Therefore, the expected number of transmissions required to successfully deliver a packet from node i to node j is calculated as follows,

$$\omega_{i,j} = \sum_{k=1}^{\infty} kPr_{i,j}(k) = \frac{1}{p_{i,j}p_{j,i}} >= 1 \tag{2.2}$$

The routing protocols need to find the path with the minimum ETX value to have the least number of transmissions to deliver each data packet to its destination. To calculate $p_{i,j}$ and $p_{j,i}$, this thesis adopts the low-cost ETX measurement scheme proposed in [9], using the information of successful/failed MAC transmissions that can be obtained via a MAC layer feedback mechanism. The sender sends a data packet to a dedicated receiver and waits for the ACK. After successfully receiving the packet at the MAC layer, the receiver will reply with an ACK packet immediately and hence the sender will know the transmission was successful. If the receiver does not receive the ACK, it schedules the packet re-transmission. Once the number of re-transmission of the current packet reaches the maximum retry limit specified by the IEEE 802.11 MAC layer protocol, the packet will be deleted and the failure reported up to the network layer. Then the packet is considered lost. The ETX measurement of a link is based on the number of m packets transmitted to make the number of s successful network-layer transmissions of packets on the link between node i to node j in the past τ seconds. The Eq. (2.2) can be expressed as,

$$\omega_{i,j} = \frac{1}{\frac{s_{data}}{m_{data}}\frac{s_{ACK}}{m_{ACK}}} = \frac{m_{data}}{s_{ACK}} \tag{2.3}$$

where s_{data} equals to m_{ACK} since the receiver sends an equivalent amount of ACK messages back to the sender to exclusively reply each data packet that it has received.

This ETX estimation mechanism eliminates the heavy overhead caused by the periodic broadcast of probe messages. It also provides a more accurate link quality estimation than broadcast probing since statistics on the transmission of data packets and ACK messages are used rather those of probe messages that generally have different specifications in terms of packet/message length and rate [26]. However, since this mechanism replaces frequent probe messages by data packets and ACK messages, the frequency of data packet transmission may have an impact on the accuracy of ETX measurement.

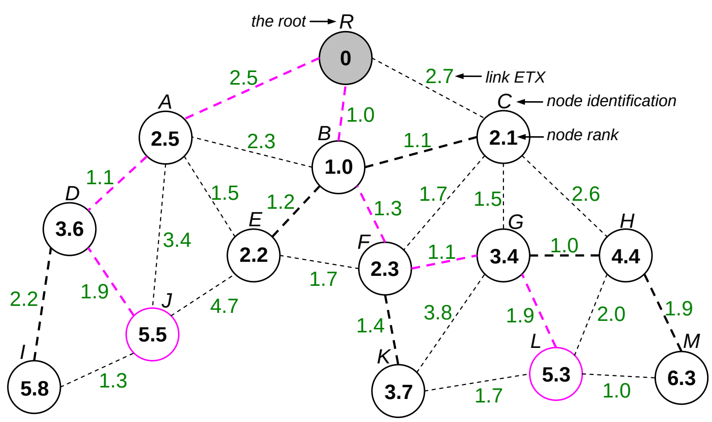

Figure 2.3: An example of DODAG using the ETX routing metric.

For the implementation of RPL in this thesis, accumulative OF based on ETX routing metric is used for calculating the rank of each node and constructing the DODAG. As a result, the optimal path selected by the protocol is the one with the minimum accumulative ETX value from possible paths to the destination. As an illustrative example, Fig. 2.3 shows a DODAG constructed over a wireless network by using the ETX routing metric. As can be seen, selected paths for traffic originated 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.

2.2.3 Global and Local Repairs in RPL

In addition to the trickle timer and DIO messages to support DODAG formation, local and global graph repair mechanisms are utilized with the aim of repairing the network topology in case of link fluctuations or node failures. Local repair only causes partial DODAG changes while global repair affects all DODAG nodes [21].

A DODAG root governs the global repair operation by periodically incrementing the DODAG version number. This initiates the DODAG reconstruction. Nodes in the new DODAG version can choose a new position whose rank is not constrained by their rank within the old DODAG version. Global repair attempts to eliminate node rank inconsistencies, loops, and floating sub-graphs that may be present in the DODAG after a long period of operation in order to re-optimize the entire routing hierarchy.

Local repair can be activated by any node that detects link fluctuations or node failures. It aims to find an alternate local path instead of globally re-optimizing the entire DODAG. RPL has two prominent local repair methods. The first one allows routing through alternate parents or siblings once the preferred parent is found to be lost. The second method, known as "poisoning", is used in the situation of a node running out of parents and siblings. The node sends out a "poison" message to its children to detach them from itself. Then, it broadcasts a DIS message soliciting DIO messages from all surrounding nodes in order to search for nodes that can serve as its parents.

2.2.4 Proposed Proactive Parent Switching (PPS)

Robustness is one of the key requirements when developing routing protocols for NANs. As the network topology changes due to network element (meters or wireless links) failures, it is imperative to dynamically update the routing decision. The reaction should be sufficiently fast to capture these changes. However, over-reacting could potentially compromise routing stability. Even though the robustness of RPL is addressed and studied in [10, 13, 21], the employed global and local repair mechanisms are quite simple and preliminary. Global repair is simply driven by a timer and it is mainly used to refresh the whole DAG to remove inconsistencies or loops that may appear over a long period of operation (minutes or hours) rather than dealing with small-scale variations. The local repair is triggered only after a node loses its parents and siblings. It can help to fix local issues introduced by node failures or link fluctuations, however, due to the fact that the repair operates at the network layer (with the involvements of control message exchanges, node rank re-computations, parent-child relationship reforming, etc.), there could be a significant delay and many packets may be dropped during the outage period. Therefore, this thesis proposes the PPS mechanism, which can effectively help RPL deflect network traffic from points of failures before local repair is activated. Instead of waiting until a node either detects the loss of its preferred parent (after exhausting all transmission/re-transmission attempts allowed by the MAC layer protocol) or runs out of all of its parents and siblings, PPS proactively nominates another parent as the next hop once the preferred parent is unreachable. Neighbor information supplied by the network layer is exploited to support the next-hop switching procedure performed at the MAC layer. Extensive simulations are carried out to demonstrate the effectiveness of PPS.

Neighbor information supplied by the network layer is exploited to support the next-hop switching procedure performed at the MAC layer. The operation principles of PPS imply that the reaction is triggered quickly to mitigate the delay and waste of channel capacity due to useless back-off stages and re-transmissions during the outage period. Meanwhile, over-reaction to transient fluctuations of network elements is avoided by observing over a window of multiple MAC-layer transmission attempts. It is noted that the "poisoning" local repair and global repair specified in [10, 13, 21] can be used jointly with PPS for local DODAG

Algorithm 1 Proactive parent switching (PPS)

Require: Data unit D from the network layer, $\mathbf{P}_i$, $\mathbf{K}$

```
Encapsulate D into MPDU
for (j ← 1; j ≤ n; j ← j + 1) do
  Update MPDU: MPDU.receiver ← P_{i,j}, ...
  for (k ← 1; k ≤ k_j; k ← k + 1) do
    Transmit MPDU to P_{i,j}
    while (ACK timer not expired) do
      if ACK for MPDU is received from P_{i,j} then
        Send confirmation to the network layer
        return [successful]
    Perform back-off procedure
Send failure notification to the network layer
return [failed]
```

re-construction and global DODAG re-optimization, respectively.

The operation of PPS is described as follows. At node i, upon receiving a data unit from the network layer, the MAC protocol first attempts to deliver the respective MAC protocol data unit (MPDU) to the preferred parent $P_{i,1}$. If this MPDU cannot be successfully delivered to $P_{i,1}$ after k_1 transmissions, an alternate parent, denoted by $P_{i,2}$, is attempted with k_2 transmissions. This procedure is iterated with maximum n parents (including the preferred parent) of node i. If all attempts fail, a failure notification will be sent to the network layer and the packet will be dropped. The maximum total number of transmissions that n parents attempt, denoted as K is,

$$\sum_{j=1}^{n} k_j = K. \tag{2.4}$$

Since, according to the routing rules specified by RPL, forwarding packets to a parent with a lower relative rank tends to result in a routing path that can reach the root at a lower cost, PPS should give the highest priority to the preferred parent $P_{i,1}$, then the first alternate parent $P_{i,2}$, then the second alternate parent $P_{i,3}$ and so forth. Note that the relative rank of parent $P_{i,j}$ is the sum of the rank of $P_{i,j}$ and ETX of the link from sender i to $P_{i,j}$. In order to enforce this priority, this thesis proposes that

$$k_u \geq k_v, \ \forall u < v; \ u, v \in \{1, 2, \ldots, n\}. \tag{2.5}$$

The pseudo-code of PPS is presented in Algorithm 1 where $\mathbf{P}_i$ and $\mathbf{K}$ are the set of parents of node i and the set of the maximum numbers of attempts

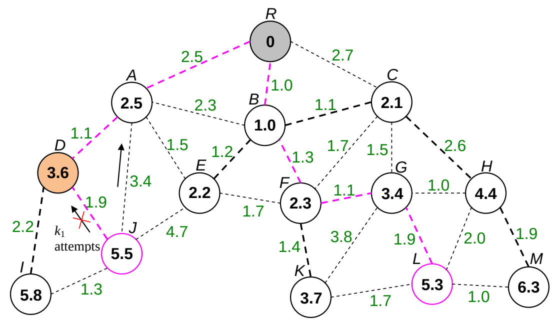

Figure 2.4: RPL with PPS in the scenario of a single node failure.

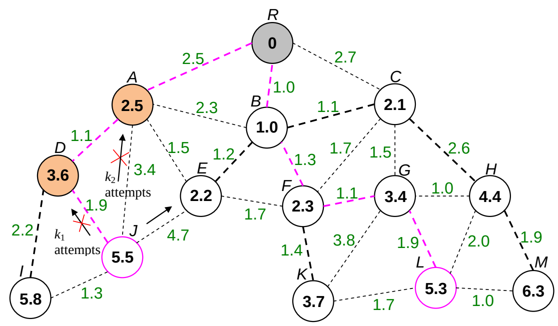

Figure 2.5: RPL with PPS in the scenario of two node failures.

for each corresponding parent, respectively, i.e., $\mathbf{P}_i = \{P_{i,1}, P_{i,2}, \ldots, P_{i,n}\}$ and $\mathbf{K} = \{k_1, k_2, \ldots, k_n\}$. It is noted that, for simplicity, not all operations carried out by the IEEE 802.11 MAC protocol are presented in Algorithm 1. The examples of RPL in cooperation with PPS are represented in Figs. 2.4 and 2.5. A scenario of single node failure is illustrated in Fig. 2.4, based on the constructed DODAG, node J intends to send data packets to its preferred parent node D. However, since node D has failed, all transmissions will not be acknowledged. Once the limitation of k_1 transmissions of a data packet is reached, node J has to switch its next hop to an alternative parent. If node J selects node A, its ETX value calculated from node A is $2.5 + 3.4 = 5.9$ transmissions. While if node J selects node E, its ETX value calculated from node E is $2.2 + 4.7 = 6.9$ transmissions. Therefore, by resulting in lower ETX value for node J, node A is selected to provide an alternative path for node J, which is $J \to A \to R$. If, unfortunately, node A has also failed as shown in Fig. 2.5, after trying k_2 transmissions, node E becomes the last candidate parent for node J to recover from the failures of node D and A. The updated alternative path is $J \to E \to B \to R$.

Chapter 3

NAN Simulation Models and Performance Metrics

3.1 Network Scenarios and Assumptions

A discrete event network simulation platform OMNET++ [27] is used to simulate a NAN cluster that consists of one DAP and n SMs (i.e., network nodes). The cluster is illustrated in Fig. 3.1, where the DAP is represented by a red square located in the center of the cluster while SMs are represented by black dots uniformly distributed in the circular area. The cluster size n is varied starting from 1000 nodes (a typical size that gives a reasonable trade-off between network performance and cost [1]). Each node is implemented with a radio communication module and works as an end-device and a router as well. In order to ensure that the results obtained in this thesis are meaningful and applicable to real-life scenarios, parameters related to meter deployment specified in the Smart Grid Priority Action Plan 2 (PAP02) published by the National Institute of Standards and Technology (NIST) [1] are applied, as summarized in Table 3.1.

The wireless channel is modeled with path-loss (with path-loss exponent α) and log-normal shadowing X_σ (with standard deviation σ) at independent intervals of 1 ms. In other words, $P_{R_x}[dBm] = P_{T_x}[dBm] - PL(d_0) - 10\alpha \log_{10}\left(\frac{d}{d_0}\right) - X_\sigma$, where P_{T_x} and P_{R_x} are the transmitted and received radio power, respectively; $PL(d_0)$ is the path loss at the reference distance d_0; λ and d are the wavelength and the transmitter-receiver distance, respectively. The radio transmission power P_{T_x} is selected to provide roughly 50 m of range. The values for path-loss and shadowing parameters are taken from NIST's PAP02. Radio communication modules in each node are built with IEEE 802.11b physical (PHY) and MAC layers. Simulation parameters related to these two layers are summarized in Table 3.1. GPSR and RPL are implemented in the network layer.

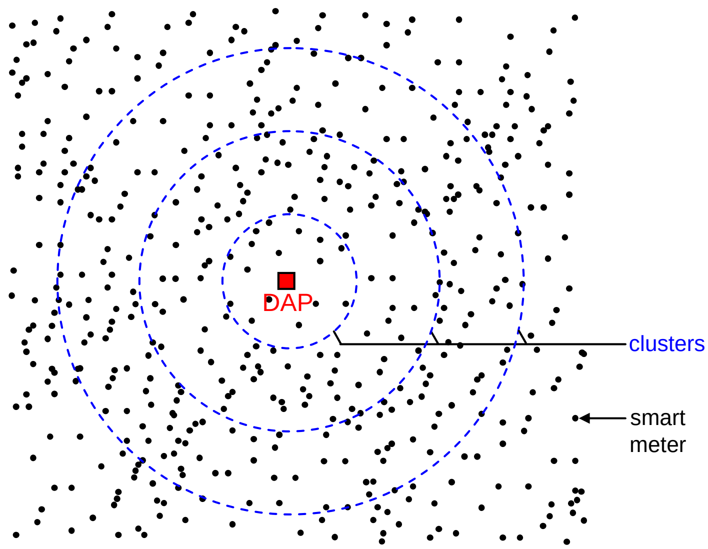

Figure 3.1: The illustration of simulated NAN cluster.

Data packets are periodically generated at a rate of r packets/s/node. Following the estimation given in Table 3.2, which is obtained from table 7 of NIST's PAP02, the total traffic load offered to the network by interval/on-demand meter reading, demand response and remote connect/disconnect applications is approximately 16808 bytes/day/meter. Since it is assumed in this thesis that each packet carries 100 data bytes, the equivalent data packet rate is $r = \frac{16808}{24\times60\times60\times100} \approx 0.00195$ packets/s/node, namely the base data rate.

It is noted that, in this thesis, 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. The performance of the network is mainly evaluated based on data packet delivery ratio P_{D} and the transmission delay which is statistically represented by its 95th percentile value D_{95}.

3.2 Performance Metrics

3.2.1 Packet Delivery Ratio

Packet delivery ratio (PDR), P_{D}, is defined as the ratio of packets successfully received by the destination compared to the total number of packets sent out by the source. It is calculated by $P_{\mathrm{D}} = \frac{|\mathbf{N}_{\mathrm{rx}}|}{|\mathbf{N}_{\mathrm{tx}}|}$, where $\mathbf{N}_{\mathrm{tx}}$ and $\mathbf{N}_{\mathrm{rx}}$ are the set of data packets generated and sent by network nodes and the set of packets that are received and successfully decoded by the DAP, respectively; $|S|$ is the cardinality of

Table 3.1: Simulation parameters

Smart Meter Deployment	
Node density (urban)	$\rho = 2000$ nodes/km^2
Node placement	uniformly random
Num. of nodes per cluster	n (varying)
Wireless Channel	
Path-loss	$\alpha = 3.6$
Shadowing	Log-normal, σ (varying)
PHY Layer	
Standard	IEEE 802.11b
Frequency band	2.4 GHz
Transmission rates	{1.0, 2.0, 5.5, 11.0} Mbps
MAC Layer	
Standard	IEEE 802.11b
Operation mode	Mesh
RTS/CTS	Disabled
ACK	Enabled
Max. retransmissions	7
Back-off procedure	Binary exponential
Min. contention window	$CW_{\min} = 31$
Max. contention window	$CW_{\max} = 1023$
ST, SIFS, PIFS, DIFS, EIFS	20, 10, 30, 50, 364 μs
Application Layer	
Data length	$L_0 = 100$ bytes per packet
Packet rate	r packets/s/node (varying)

(ST: slot time; SIFS: short interframe spacing; PIFS: point coordination function interframe spacing; DIFS: distributed coordination function interframe spacing; EIFS: extended interframe spacing)

set S. In each simulation, $|\mathbf{N}_{\mathrm{tx}}|$ is chosen to be 100000 for statistical measurement of P_{D}.

3.2.2 Transmission Delay

Timing is critical in SGCN, especially for time-sensitive NAN traffic. Therefore, interests in examining how the transmission delay affects SG communication performance have emerged. The transmission delay is generally defined as the total time required for a packet to be transmitted along the path from source to destination as perceived by the application layer. It includes all possible delay caused by forwarding a data packet such as processing delay during the route discovery phase, propagation delay, re-transmission delay and etc. It is an important factor to analyze the delay resulting from route discovery caused by different routing protocols.

Table 3.2: Data traffic from SM to DAP [1].

Event	**How Often (events /meter /day)**	**proportion**	**Size (bytes /event)**	**Average Traffic Load (bytes /meter/day)**
Multiple interval meter read data (Commercial /industrial electric meters)	24	0.10	2400	3840
Multiple interval meter read data (Residential electric meters)	6	0.90	1600	12960
Subtotal	Frequency *proportion=	7.8 events /meter/day	Frequency *size *proportion=	16800 bytes /meter/day
On-demand read request application errors	$25/1000 * 1/1000$		50	0.000025
On-demand meter read data	25/1000		100	2.5
Send service switch operate acknowledgment	2/1000		25	0.05
Send service switch operate failure	$1/1000 * 50/1000$		50	0.0025
Send metrology information after a successful service switch operate	2/1000		100	0.2
Send service switch state data	50/1000		100	5
Subtotal	0.079		N/A	7.75375
Total	7.879		N/A	16808 bytes /meter/day

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 packet transmission time (T_p^{DATA}), acknowledgement transmission time (T_p^{ACK}), back-off time (T_{BO}) and interframe spacings (T_{IFS}). Its calculation is shown in Appendix B. Note that these components represent total values since for a successful delivery of a data packet there might be multiple back-off stages and re-transmissions.

Note that statistics of reliability and delay can be obtained for the entire simulation or per node. In addition to these two primary performance metrics, parameters related to next hop selection and path determination are analyzed for an in-depth understanding of GPSR and RPL.

Chapter 4

Performance Evaluation of GPSR and RPL[2]

Existing studies show that the performance of WMNs varies with network scale, wireless channel characteristics, deployment settings, traffic loading levels and equipment availability. Therefore, in order to assess the feasibility of GPSR and RPL routing protocols in wireless mesh NANs, this chapter provides a comprehensive study on the performance of these two protocols in various practical NAN scenarios.

GPSR and RPL are investigated in two sections. In the first section, a detailed comparison of GPSR and RPL is provided with the assumption that all nodes are active and operate during the entire simulation time. The performance metrics PDR and transmission delay are studied to demonstrate the performance patterns and trends of GPSR and RPL when the variance of channel shadowing σ, per-node data rate r and cluster size n are swept. When the channel shadowing σ is more severe, packet corruption is more likely due to higher level of channel randomness. This results in high packet loss, re-transmissions and in turn performance degradation. When r increases, packets are generated and sent out more often to induce a higher chance for channel contentions, back-offs and packet re-transmissions. Even though routing paths are not lengthened, longer delays and lower transmission reliability levels are expected. Cluster size n is an important parameter in system design since the larger it is, the lower the required costs related to installation, operation and maintenance of DAPs. However, an increase in the cluster size has a dual effect. First, a large number of nodes in the

[2]Parts of chapter 4 have been presented in the "Challenges and Research Opportunities in Wireless Communications Networks for Smart Grid", in the IEEE Wireless Communications Magazine 2013 [14], and have been accepted for publication in the "Performance and Applicability of Candidate Routing Protocols for Smart Grid's Wireless Mesh Neighbor-Area Networks", in the IEEE International Conference on Communications 2014 [15].

cluster inject more traffic towards the DAP. Second, since node density is fixed ($\rho = 2000$ nodes/km^2) and $n = \pi R^2 \rho$, a larger number of nodes also implies that the geographic area of the cluster, i.e., πR^2, expands. Packets from nodes further away need to traverse longer distances (or more hops) to reach the DAP. This effectively increases the network load and average hop count at the same time. As a result, this dual effect will significantly increase transmission delay while decrease PDR.

For the detailed implementation of GPSR, hello messages are sent out at the same rate of data messages. The neighbor table is refreshed after broadcasting every two hello messages, which is pre-specified in section 2.1.3. RPL is implemented based on the design principle of the original protocol along with the default parameters specified in [7] without the PPS mechanism. The DIO generation and transmission are controlled by a unique trickle timer at each node whose parameters are specified in [7] as well. If the routing topology is not consistent such as a node changes its preferred routing path or a new node joins the DODAG, the trickle timer resolves the inconsistency by resetting its interval to the minimum value; this is done to generate more frequent DIOs to disseminate updated information within the DODAG. Simulation results presented in this section will investigate their operations as well as pinpoint other important features such as reliability and efficiency of the protocols with severe environment, the corresponding expected traffic load and large network size. The study cases carried out in this section are briefly described as follows: Study case I is to investigate the operations of GPSR and RPL under an ideal channel condition, with base data rate, and with a typical network size. The purposes of Study case II, III and IV are to investigate the different effects of channel shadowing variance, data traffic load and cluster size on the system performance of GPSR and RPL, respectively. Possible differences between their network performances will be attributed to the presence of the swept parameters in different study cases. The detailed information are summarized in Table 4.1.

Table 4.1: Simulation parameters of study cases I, II, III and IV

Parameter	**Study Case**			
	I	II	III	IV
Shadowing σ (dB)	0	**0,4,8,12**	8	8
Packet rate r (packet/s/node)	0.00195	0.00195	**0.001**, **0.00195**, **0.01**, **0.1**	0.00195
Cluster size n (nodes)	1000	1000	1000	**1000**, **3000**, **6000**
Network availability a (%)	100	100	100	100

In the second section, the robustness of GPSR and RPL in NANs is evaluated by taking into account the effects of node failures. Failures of network nodes is represented by f ($f \in [0, 1]$) which is the fraction of nodes that randomly fail during simulation time. Failed nodes and arrival time of their failures are uniformly distributed. A node remains silent (i.e., incapable of transmitting and receiving any packet) after it fails. Availability of the network is thus given by $a = 1 - f$. In order to address the impact of node failures, the robustness of GPSR, conventional RPL and RPL with the proposed PPS mechanism is compared in scenarios with different levels of network availability. The decrease of network availability a results in an increasing number of network disconnections and communication truncations between nodes. Larger number of re-transmissions and control packets are imposed on the network to reduce packet loss by detecting and recovering from node failures. The related results and observations will be presented. Furthermore, with the aim of understanding the impact of growing traffic load in the occurrence of node failures, the per-node data rate r is swept. To support high data rate applications and provide fault-tolerant routing, PPS's ability to re-route packets to different next hops could be a promising mechanism. The performance of GPSR and RPL with PPS in response to high probability of node failures and heavy traffic loads is illustrated and discussed in the following study cases: Study case V compares the robustness of GPSR and RPL with PPS under the scenarios with different portions of network failures. Per-node data rate is swept in Study case VI to investigate the effects of both node failure and traffic load on the system performance of GPSR and RPL with PPS. The details of these two study cases are summarized in Table 4.2:

Table 4.2: Simulation parameters of study cases V and VI

Parameter	**Study Case**	
	V	VI
Shadowing σ (dB)	8	8
Packet rate r (packet/s/node)	0.00195	**0.001, 0.00195, 0.01, 0.1**
Cluster size n (nodes)	1000	1000
Network availability a (%)	**100, 95, 90**	90

4.1 Network Performance without Node Failure

4.1.1 Study Case I: Routing Protocol Operation with Ideal Wireless Channel

This thesis compares the network performance of GPSR and RPL step by step from ideal to realistic scenarios. In the first study case, the ideal channel condition is assumed. The performance of GPSR and RPL is expected to be similar since ETX measure used by RPL might not provide any advantages in case there is no channel randomness. The following figures and discussions in this study case will illustrate this assumption. The simulation parameters are set as follows, channel shadowing $\sigma = 0.0$ dB, $r = 0.00195$ packets/s/node and $n = 1000$ nodes ($R = 398.9$ m).

First, Figs. 4.1 and 4.2 present details of packet delays and routing path lengths (in terms of hop count) of 50 sampled packets received at the DAP for GPSR and RPL, respectively. It can be seen that packets routed over longer paths (traversing a large number of hops) to reach the DAP generally experience higher delay for both GPSR and RPL. However, the correlation between the hop count and the delay does not always hold since different transmission may experience different channel conditions and thus different number of collisions, back-off stages and re-transmissions. The cumulative distribution function (CDF) of delays is then given in Fig. 4.3. It can be seen that the delay statistics of all successfully transmitted packets are similar for GPSR and RPL. 95% of the received data packets experience no more than 11.41 ms and 11.26 ms of transmission delay for GPSR and RPL, respectively. For packet transmission reliability, over the entire simulation time, there is no packet loss for both GPSR and RPL, i.e., $P_{\mathrm{D}} = 100\%$.

Further detailed investigations of the correlation between source-destination distance and PDR, average transmission delay and routing path length per node are plotted in Figs. 4.4, 4.5 and 4.6, respectively, where their horizontal axis represent distances from nodes to the DAP. As can be seen in Fig. 4.4, every node can successfully deliver all of their packets to the DAP. Even for nodes that are far away from the DAP (i.e., beyond roughly 400 m to the DAP), their P_{D}'s are still 100%. The dependency of average transmission delay of GPSR and RPL on the geographical distance from the source to the packet destination is illustrated in Fig. 4.5. For nodes that are located no more than 50 m away from the DAP, almost all packets for GPSR and RPL have a delay of around 0.3526 ms, which is equivalent to the analytical minimum delay $D_{\min}$ given in Eq. (B.3). This can be explained by two facts: (i) these packets are transmitted directly to the DAP since source-destination distances are shorter than 50 m transmission range; and (ii) no re-transmission is required since communication links over short distance are reliable. When source-destination distance is larger than the transmission range,

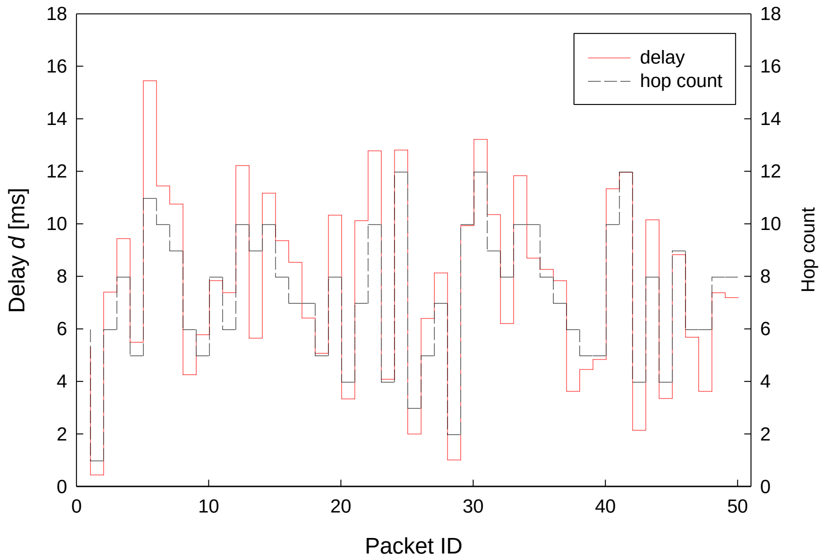

Figure 4.1: Delay and hop count for 50 sampled GPSR packet transmissions.

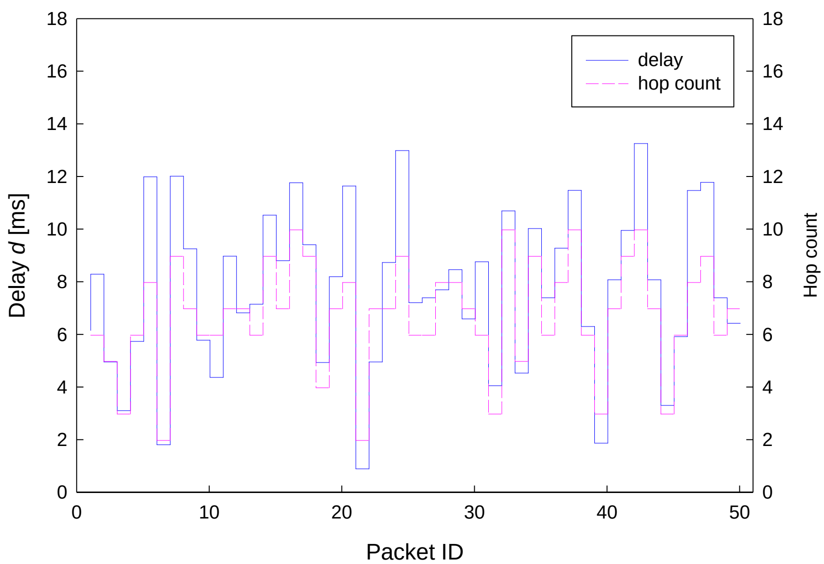

Figure 4.2: Delay and hop count of 50 sampled RPL packet transmissions.

multi-hop paths have to be employed to deliver packets to the DAP. Obviously, multi-hop transmissions result in longer delays. Moreover, most packets routed by GPSR and RPL experience quite similar average delays when they traverse the same number of hops to the DAP, as shown in Figs. 4.5 and 4.6. In the case where there is no channel shadowing, our results indicate that GPSR and RPL

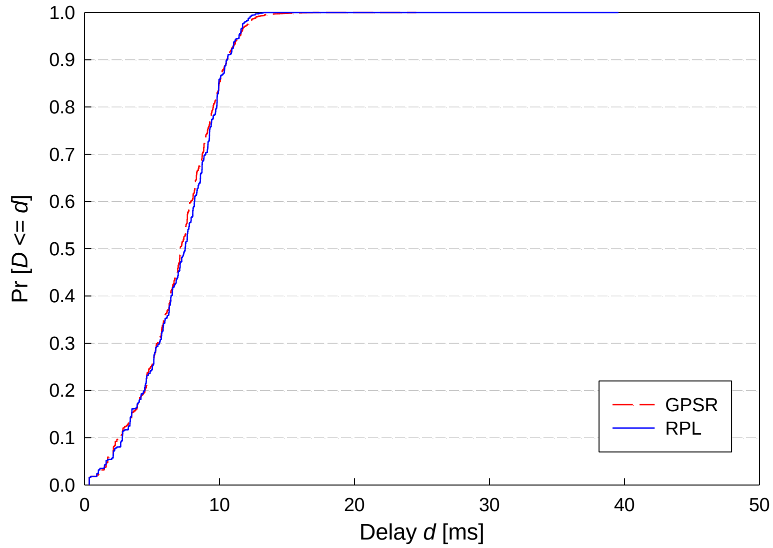

Figure 4.3: CDF of packet transmission delays.

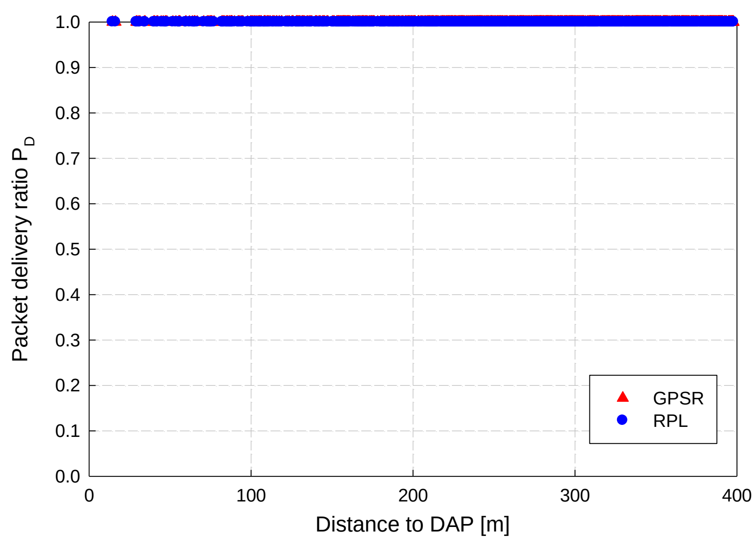

Figure 4.4: Average transmission reliability versus node-DAP distances.

perform similarly by achieving the same 100% of P_{D}, maximum 13 ms of average transmission delay and maximum 12 hops of path length.

The similarity of GPSR and RPL also can be explained as follows. When most packets could be successfully delivered by greedy forwarding, GPSR approximates the shortest path routing with the optimal number of hops and each hop distance is maximized, as also demonstrated in [17]. While RPL pays more attention to

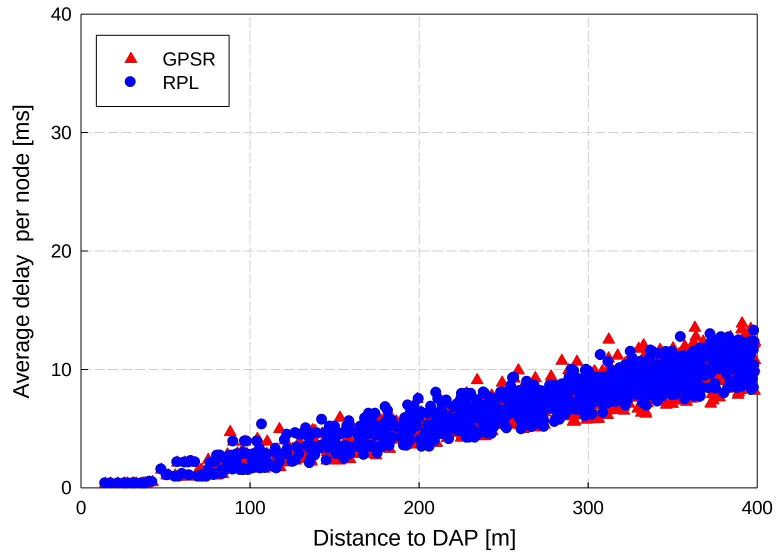

Figure 4.5: Average transmission delay versus node-DAP distances.

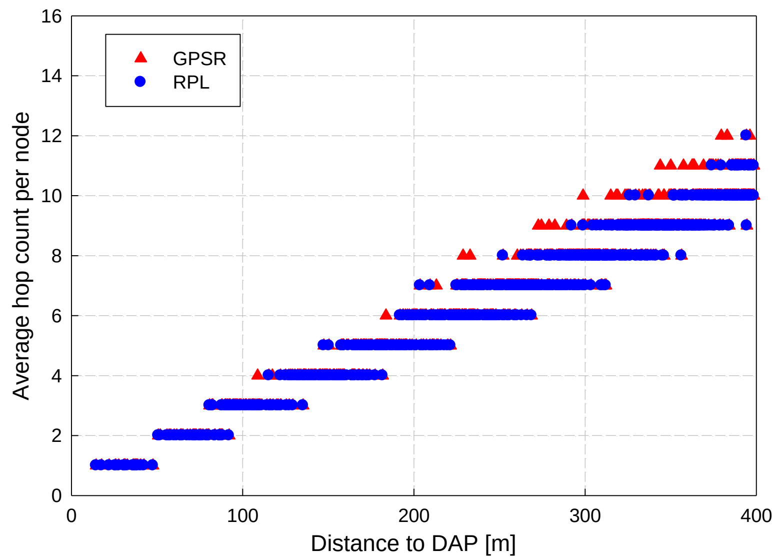

Figure 4.6: Average hop count versus node-DAP distances.

minimizing the total path cost ETX in order to ensure high reliability of packet delivery. Thus RPL may lead to relatively longer but more reliable routing paths than GPSR. However, in the case with no shadowing, wireless communication between each pair of nodes is always reliable within the communication range. ETX metric turns to reflect the hop count and alternative parents are not much different from each other. The purpose of RPL with ETX becomes to minimize

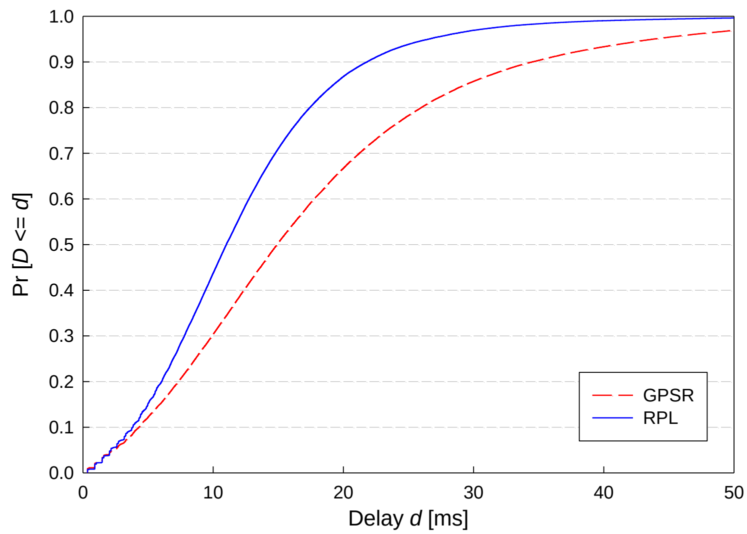

Figure 4.7: CDF of packet transmission delays.

the total hop count for each packet. Therefore, when no shadowing is present, GPSR and RPL perform well and similarly.

4.1.2 Study Case II: Effects of Channel Condition

It should be noted that many packets will loss due to the dynamic variance of wireless channels, especially in NANs. Therefore, system performance when $\sigma =$ 8.0 dB is first measured to represent a realistic communication environment of NAN [1]. Other parameters related to cluster and application data rate are the same as those of the Study Case I, i.e., $r = 0.00195$ packets/s/node and $n = 1000$ nodes ($R = 398.9m$). RPL as quality-aware routing protocol based on ETX metrics is expected to perform better than GPSR under channel variations. The observation from Figs. 4.7 and 4.8 is that, compared to the case of no shadowing, communication is less reliable and experiences higher delay for both RPL and GPSR in severe shadowing environment. However, when $\sigma = 8.0$ dB and the difference between the channel quality of alternative paths is high, the gain of RPL selecting path by ETX metric becomes visible. RPL successfully delivers more than 99.82% of packets to the DAP while GPSR only guarantees around 98.37%. D_{95} for GPSR shown in Fig. 4.7 is around 43.83 ms which is much higher than that of RPL (26.57 ms).

The detailed comparisons between GPSR and RPL in terms of average transmission reliability, per node delay and routing path lengths are plotted in Figs. 4.8, 4.9 and 4.10, respectively. As can be seen in Fig. 4.8, with GPSR, packets originated at nodes further away from the DAP generally suffer from lower relia-

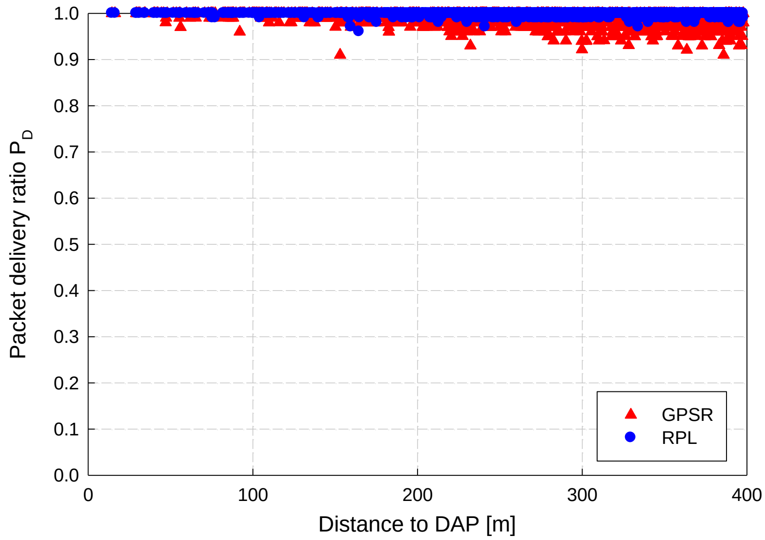

Figure 4.8: Average transmission reliability versus node-DAP distances.

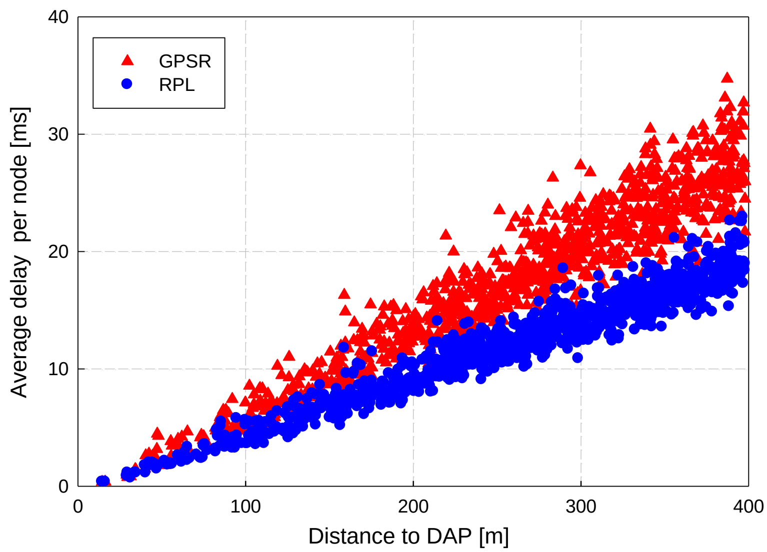

Figure 4.9: Average transmission delay versus node-DAP distances.

bility. With RPL, every node can still successfully deliver nearly all of its packets to the DAP. Even for nodes that are quite far away from the DAP (i.e., beyond 300 m from the DAP), their P_{D}'s are still higher than 96.50%. However, with GPSR, nodes that are beyond 200 m from the DAP have suffered from noticeable packet loss. For example, for nodes that are located around 300 m from the DAP, only 92.45% of their packets can reach the DAP. Additionally, as shown in

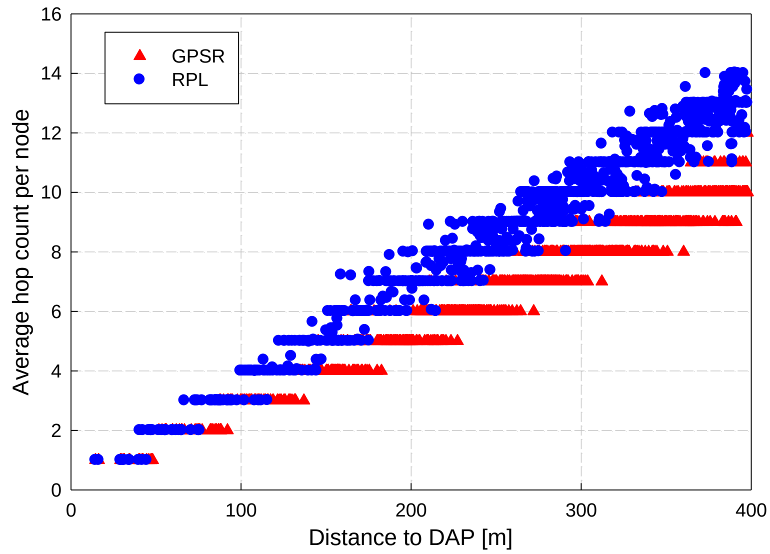

Figure 4.10: Average hop count versus node-DAP distances.

Fig. 4.9, average transmission delay per node given by RPL never exceeds 22.0 ms while it can be as high as 35.0 ms for GPSR. Fig. 4.10 demonstrates that packets traverse over multi-hop routing paths. Packets routed by RPL at the same source-destination distance have longer path lengths in terms of hop count as compared to GPSR. The long-distance hop is employed by GPSR to offer the greatest potential forward distance in the direction of the destination but the link could be unreliable. For RPL, instead of selecting a further hop that gets packet closer to its destination, a hop with shorter distance but higher transmission reliability is preferred. These observations indicate that there is a tradeoff between forward distance and transmission reliability.

Re-transmissions are rarely required over short reliable links selected by RPL while in greedy mode of GPSR, more re-transmissions are likely to occur and this can lead to additional delay. In order to verify this view, average transmission time that GPSR and RPL require for a successful packet delivery in each node are plotted in Fig. 4.11. As expected, RPL in fact requires fewer transmissions than GPSR. This, however, does not hold at a few nodes where GPSR results in smaller number of transmissions, as can be seen in the bottom of Fig. 4.11 where the curves are zoomed in for 200 nodes whose identifications range are from 400 to 600. This is due to the fact that RPL nominates preferred parents for traffic forwarding by considering the estimated total cost to reach the DAP from the current node (which is the sum of the link ETX from the node to the candidate parent and the rank of that parent), not merely on ETX of the link. This selection rule is applied to ensure that the traffic will finally reach the DAP with the lowest

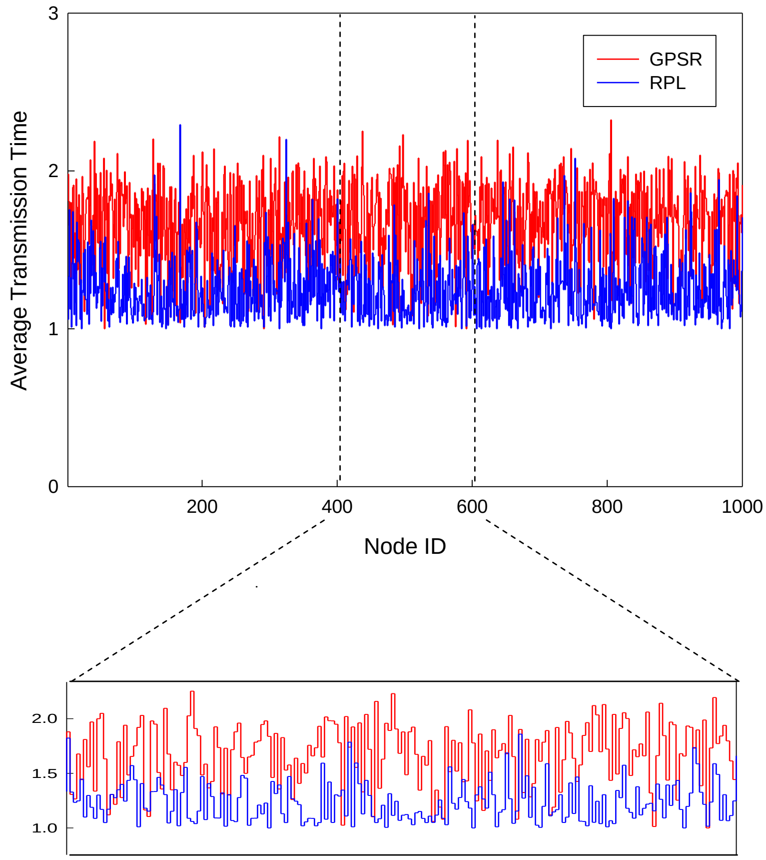

Figure 4.11: Average transmission time per successful delivery for each node.

total cost.

Low PHY data rates selected by GPSR for long range communications may also contribute to longer delays than RPL. Fig. 4.12 shows that RPL transmits the majority of packets (64.46%) with the highest PHY data rate 11.0 Mbps. However, GPSR has only 46.03% packets transmitted at 11.0 Mbps. Another 40.37% of the packets are transmitted by GPSR at the lowest data rate (1 Mbps), which is much higher than 24.72% of RPL. It indicates that the maximum PHY data rate (11.0 Mbps) is likely to be selected by RPL for communications over short distances while the minimum PHY data rate (1.0 Mbps) is likely to be selected by GPSR for communications over long distances.

Next, in order to study the rate at which the system performance is degraded due to the increasing level of channel shadowing, P_{D} and the D_{95} when shadowing variance σ is swept from 0.0 (no shadowing) to 12.0 dB (severe shadowing) are plotted in Figs. 4.13 and 4.14, respectively. When shadowing increases, the channel randomness increases accordingly and thus links are less reliable and the

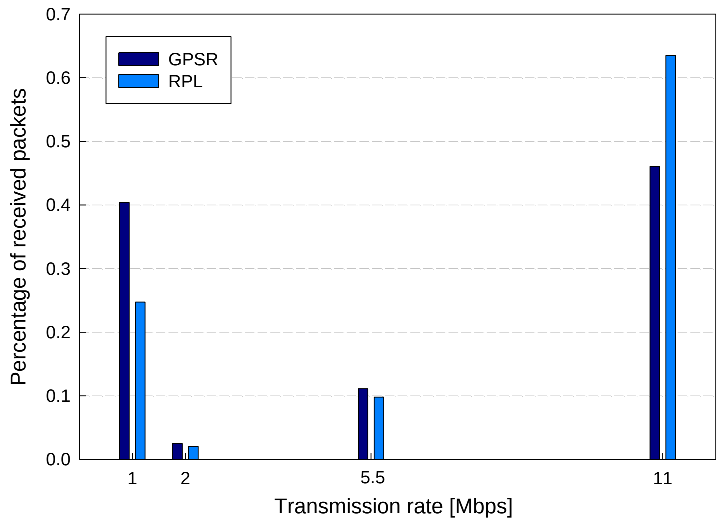

Figure 4.12: Packet transmission rate distribution.

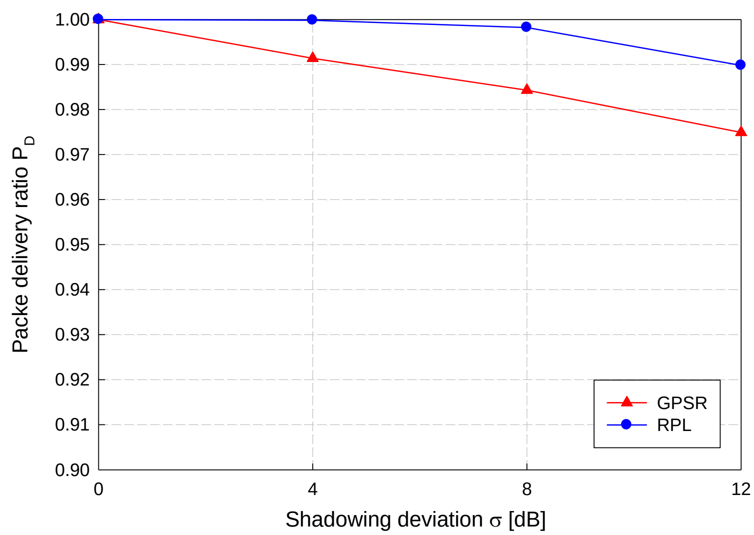

Figure 4.13: Average packet delivery ratio versus channel shadowing.

network performance degrades for both GPSR and RPL. For example, when σ doubles from 4.0 to 8.0 dB, for GPSR, the reliability is reduced from 99.10% to 98.37% while D_{95} is increased from 34.5 ms to 43.83 ms. The significant increase in delay is the result of a higher rate of channel contention, back-off and re-transmissions. Acknowledgment and re-transmission mechanisms of IEEE 802.11b MAC layer in this situation help to maintain sufficiently high PDR. Similar effects are also observed with RPL. When there is no shadowing (σ = 0.0 dB), as also

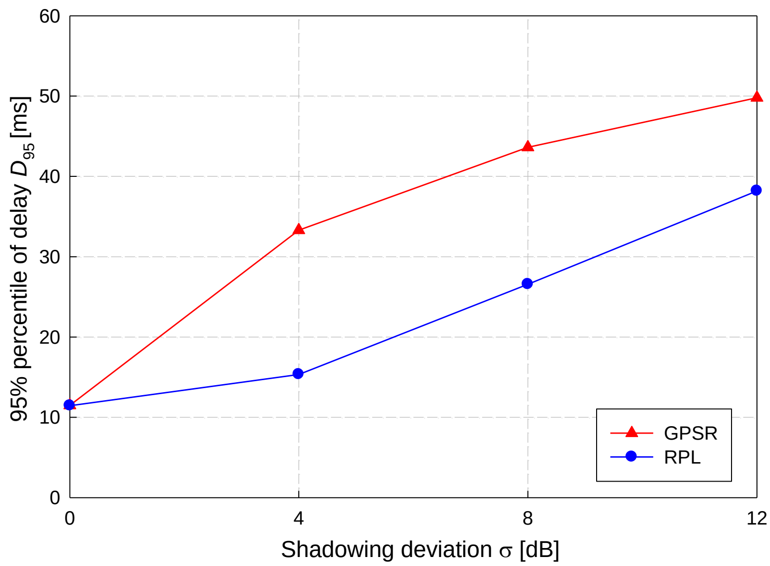

Figure 4.14: 95th percentile of transmission delay versus channel shadowing.

shown in Study Case I, GPSR and RPL perform similarly. For all non-zero values of σ, RPL outperforms GPSR in terms of both transmission delay and PDRs: for example, in a high link dynamic environment ($\sigma = 12.0$ dB), RPL outperforms GPSR by having 1.49% more of P_D and 11.61 ms less of D_{95}.

4.1.3 Study Case III: Effects of Data Traffic Load

Since SMs are deployed to support not only conventional SG applications (e.g., meter reading, demand response, and so on as mentioned in [1]) but also those are expected in the future (e.g., advanced distribution automation, fault detection and restoration, etc.), they are responsible for exchanging an increasing volume of information. As a result, the scenario presented in this study case investigates how the network performance scales with network offered load. The system performance is studied when each node offers a higher level of load to the network. Per-node data rate r is swept and shadowing variance σ and cluster size n are held constant at 8.0 dB and 1000 node, respectively. When data packets are sent more often, 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 cluster size is unchanged), lower transmission reliability and longer delays are observed for both GPSR and RPL. Figs. 4.15 and 4.16 show the results that the performance of both GPSR and RPL degrade when data rate increases, while RPL can still achieve higher PDR and lower transmission delay than GPSR. For example, it can be seen from Fig. 4.15 that when traffic rate

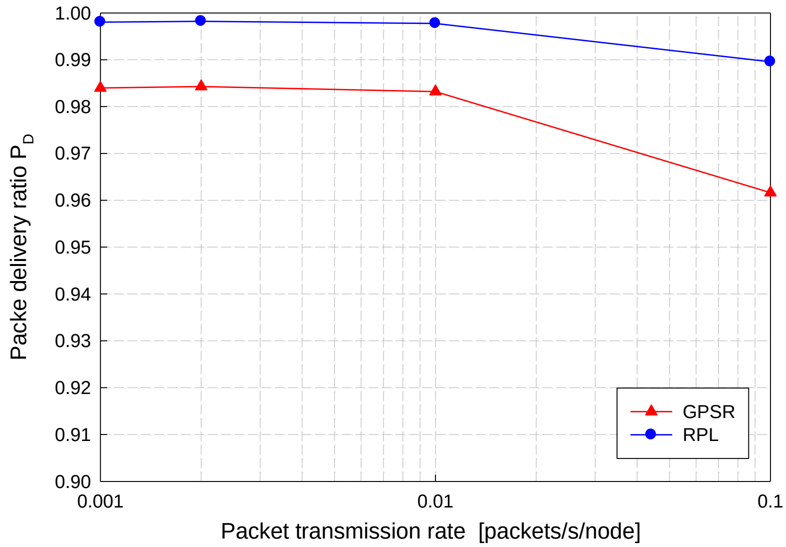

Figure 4.15: Average packet delivery ratio versus per-meter data rate.

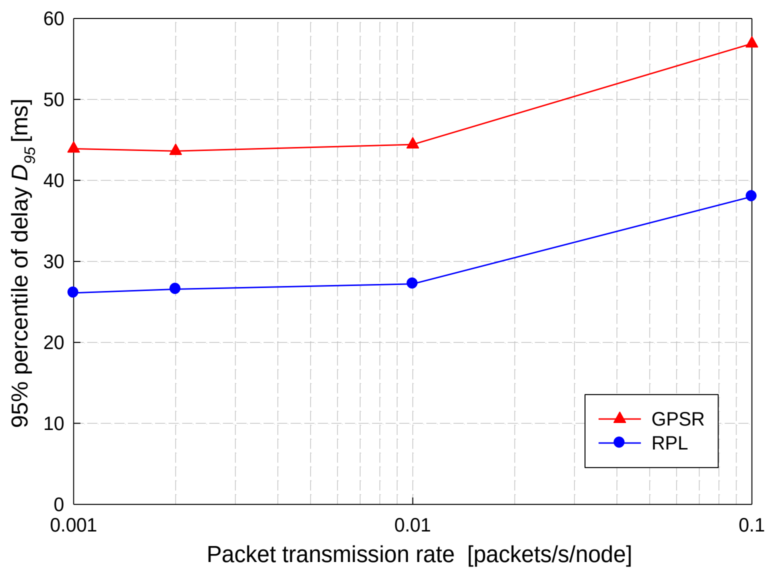

Figure 4.16: 95 percentile of transmission delay versus per-meter data rate.

r increases from 0.01 to 0.1 packets/s/node, P_{D} given by GPSR is reduced from 98.32% to 96.16%, as compared to the decrease from 99.78% to 98.96% of RPL. D_{95} of GPSR increases from 44.42 ms to 56.9 ms while that of RPL increases from 27.22 ms to 38 ms, as shown in Fig. 4.16. Furthermore, with heavier traffic loads, unreliable routing path selected by GPSR and its higher hello message frequency both lead to a significant increase in channel contentions thus more packet losses. Therefore, the gaps between RPL and GPSR in terms of PDR and transmission reliability are observed to be widened when per-meter data rate r is increased from 0.001 to 0.1 packets/s/node.

4.1.4 Study Case IV: Effects of Cluster Size

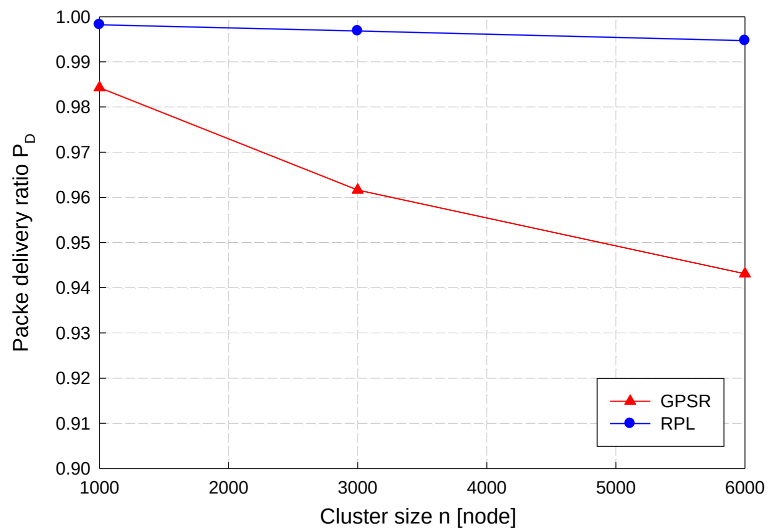

Figure 4.17: Average packet delivery ratio versus cluster size.

The scalability is one of the most important issues of NAN communication. With SG being implemented step by step, the number of SMs will increase dramatically. Consequently, there is a great challenge for candidate routing protocols to provide an acceptable level of communication with a large number of nodes. This study case investigates the effects of cluster size on system performance of GPSR and RPL. Shadowing variance σ and per-node data rate r remains constant at 8.0 dB and $r = 0.00195$ packets/s/node. Figs. 4.17 and 4.18 show the scalability of the two routing protocols. With the same node density, increasing the number of nodes leads to expanding the coverage area for each cluster. As the cluster size increases, network offered traffic load and average traffic path length are both increased. Since packets routed over a longer path are more likely to be lost, packet loss increases. When varying the number of nodes from 1000 to 6000, P_{D} of GPSR drops from 98.43% to 94.31%, but RPL still maintains its P_{D} with negligible loss, i.e., from 99.82% to 99.47%. The reliability benefits of employing RPL are enhanced in a larger network. The transmission delays are significantly higher with increasing network size for both RPL and GPSR. Packets

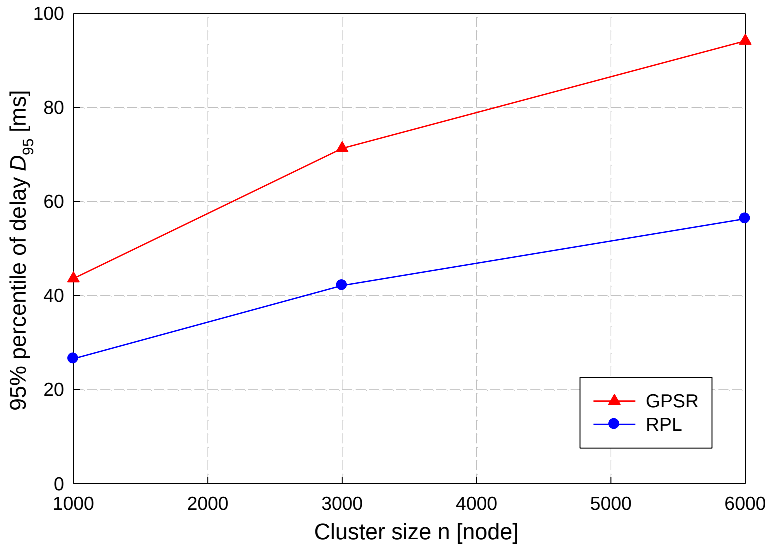

Figure 4.18: 95th percentile of transmission delay versus cluster size.

with GPSR generally require fewer hops to reach the destination. However, each long-distance hop provides unreliable transmission and requires a larger number of re-transmissions for successful packet reception. D_{95} of GPSR dramatically grows from 43.62 ms to 94.16 ms, whereas RPL still performs better with relatively lower D_{95}, e.g. 23.56 ms to 56.33 ms. It can be concluded that RPL provides lower delay as compared to GPSR, even with longer traversed path in a larger network. This can be explained through the fact that a higher proportion of the transmission delay is due to exponential back-offs as opposed to propagation time on multiple hops. Therefore, RPL is a more efficient and reliable routing protocol in a large-scale network.

4.2 Network Performance with Node Failures

This section focuses on investigating the effects of node failures to network performance and how the PPS can help RPL mitigate them. For PPS, $K = 7$ (commonly used for short IEEE 802.11 MAC frames) and $n = 3$ are assumed. To meet the constraint specified by (2.5), the simple well-known binary exponential rule is applied, i.e.,

$$\frac{k_j}{k_{j+1}} = 2, \ \forall j \in \{1, 2, \ldots, n-1\}. \tag{4.1}$$

Then, from Eqs. (2.4) and (4.1), the maximum numbers of transmissions for each of the 3 candidate parents are $\mathbf{K} = \{k_1, k_2, k_3\} = \{4, 2, 1\}$.

In the following study cases, the performance of RPL with $\mathbf{K} = \{4, 2, 1\}$, namely, RPL-PPS(4,2,1), is evaluated. In order to verify the parent switching principle proposed by PPS and demonstrate its advantages, GPSR and other three schemes of RPL as references are also studied: RPL-PPS(1,2,4) with $\mathbf{K} = \{1, 2, 4\}$ (i.e., parents with higher relative ranks are given greater numbers of transmission attempts, as opposed to the proposed principle), RPL-PPS(1,1,...,1) with $\mathbf{K} = \{1, 1, 1, 1, 1, 1, 1\}$ (i.e., the packet is switched to another parent once a single transmission attempt fails), and the conventional RPL (without using PPS), namely RPL-non-PPS.

4.2.1 Study Case V: Effects of Node Failure

Communication in NAN requires the routing protocol to be adaptive and reliable even when some nodes undergo failures. The robustness of GPSR and RPL with PPS to against node failures is demonstrated in Figs. 4.19 and 4.20 when network availability a is swept. Note that in this study, each node is assumed to generate data at the base rate of $r = 0.00195$ packets/s/node and shadowing variance σ and cluster size n are constant at 8.0 dB and 1000 nodes, respectively. The network becomes unstable with the presence of increasing random node failures. Therefore, the transmission reliability is decreased for both GPSR and RPL with PPS. When a decreases from 100% to 90%, P_{D} of GPSR slightly decreases from 98.43% to 97.07%. The accurate neighbor information is maintained when neighborhoods change by an adequate hello rate of GPSR. Nodes could promptly correct routing paths and thus losing packets to unreachable nodes is mitigated. For RPL-non-PPS, although it achieves P_{D} of 99.82% when a is 100%, its P_{D} drops to 85.84% when a is 90%. All transmissions to a primary preferred parent that has already failed are useless, the performance therefore degrades. In comparison with GPSR and RPL-non-PPS, RPL with PPS experiences the same decreasing trend of P_{D} with decreasing a. However, P_{D} drops at a much lower rate. This can be explained due to the fact that PPS helps to deflect traffic from failed nodes by switching the next hop to another parent. For example, RPL-PPS(4,2,1) gives the best performance when a is high (i.e, a is 100% or 95%). RPL-PPS(1,2,4) gives more retries to parents with higher relative ranks and thus results in higher-cost paths. RPL-PPS(1,1,...,1) is over-reacting (i.e., it reacts too fast to transient network condition changes and results in unnecessary path fluctuations) and at the same time tends to push next hops to parents with higher costs then primary preferred parents. As a result, RPL-PPS(1,2,4) and RPL-PPS(1,1,...,1) both experience lower PDRs as compared to RPL-PPS(4,2,1). However, when more nodes become unavailable, packets should be deviated quickly to have a higher chance to reach any active parents. Therefore, when a decreases to 90%, RPL-PPS(1,2,4) begins to give a higher P_{D}, i.e.,99.69%, than that of RPL-PPS(4,2,1), i.e. 99.03%.

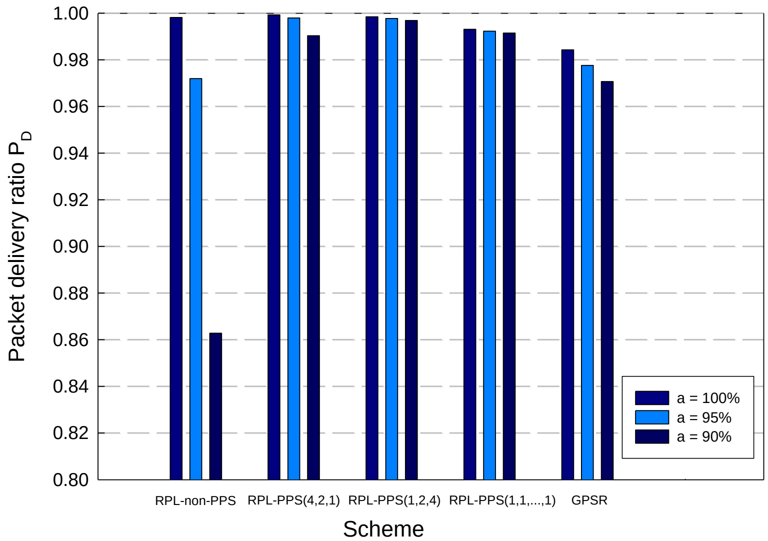

Figure 4.19: PDR of GPSR and RPL with parent switching schemes versus network availabilities.

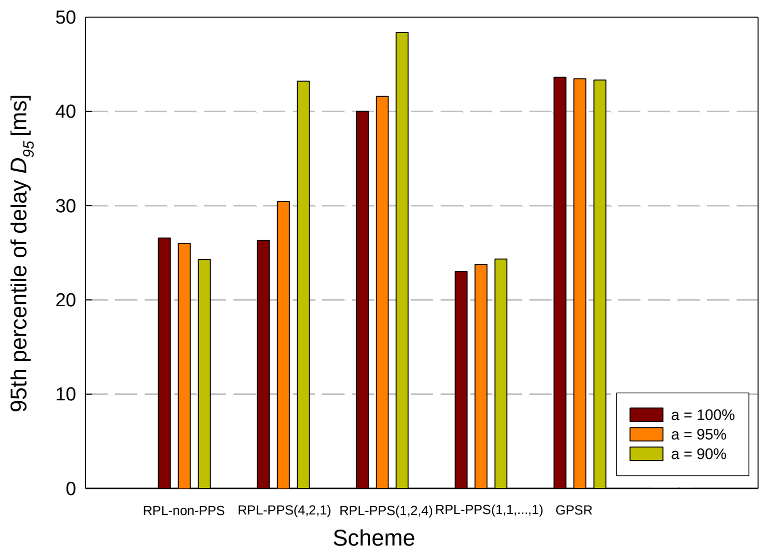

Figure 4.20: 95th percentile of transmission delay of GPSR and RPL versus network availabilities.

The transmission delays, D_{95} of GPSR and RPL-non-PPS, are slightly reduced when network availability decreases. More packets experiencing high delays due to traverse over long path will highly likely to be lost if there are more node failures along paths. Note that the columns in Fig. 4.20 only count delays for successfully delivered packets. Therefore, the decreasing network availability decreases both transmission reliability and delays of GPSR and RPL-non-PPS. On the contrary, RPL with PPS improves reliability but induces higher delays. With low network availability, both RPL-PPS(4,2,1) and RPL-PPS(1,2,4) might give too many wasteful attempts to primary or secondary parents that have likely already failed. Therefore, when a is 90%, D_{95} of RPL-PPS(4,2,1) and PPS(1,2,4) are increased to 43.20 ms and 48.38 ms, respectively. While RPL-PPS(1,1,...1) has the lowest D_{95}, i.e., 24.34 ms, since it does not have the exponential back-off procedures for packet re-transmission. Once a transmission failure is detected, nodes will simply re-transmit the packet to another candidate without exponentially increasing the contention window.

Next, in order to have a more detailed understanding of the above results, mean hop count and communication cost of routing paths for various schemes are compared in Figs. 4.21 and 4.22, respectively. Since GPSR takes effort in forwarding packets to the node closest to the destination, it pursues the goal of minimizing hops traversed between the source and the destination. As can be seen in Fig.4.21 (with an assumed network availability of 90%), GPSR forwards most packets over short paths to reach the destination, that is demonstrated by having higher fraction of paths with less than 10 hops and no path longer than 16 hops. For RPL-non-PPS, packet transmissions always choose primary preferred parents having the lowest relative ranks, the traffic flow therefore also follows short paths to the root, where the maximum path length is 16 hops. However, in order to maximize the transmission reliability, RPL-non-PPS chooses parents with better link qualities. More reliable links (lower ETX value) with shorter distance are chosen for each hop so that RPL has a higher proportion of longer paths than GPSR, i.e., higher fraction of packets with path length of 12 to 16 hops. When PPS is employed, routing paths are lengthened since the traffic flow can be redirected towards alternate parents having higher relative ranks in cases where preferred parent failures are detected. In the extreme case, i.e., RPL-PPS(1,1,...,1), there are noticeable fraction of paths that require 17, 18, and 19 hops due to the fact that, at each node, packets can be spread to 6 different alternate parents (in addition to the preferred parent) that significantly diverge paths from the root. This illustrates the over-reacting behavior and in consequence longer path lengths emerge. RPL-PPS(4,2,1) also selects longer paths (as compared to RPL-non-PPS) to deflect traffic from points of failures, however, over-reaction is prevented by allowing only 2 possible alternate parents. RPL-PPS(1,2,4) has slightly higher fraction of longer paths. Recall that RPL-PPS(4,2,1) prefers the default parents while RPL-PPS(1,2,4) allows more trials with alternate parents. For example, if a node requires 5 re-transmissions for packet delivery, the former only attempts with 2 parents whereas the latter will likely involve all 3 parents. To sum up, by considering more candidate parents when switching, a higher level of path diversity can be obtained. However, increasing path diversity may result in longer paths that may in turn require more network resources and thus degrade network performance.

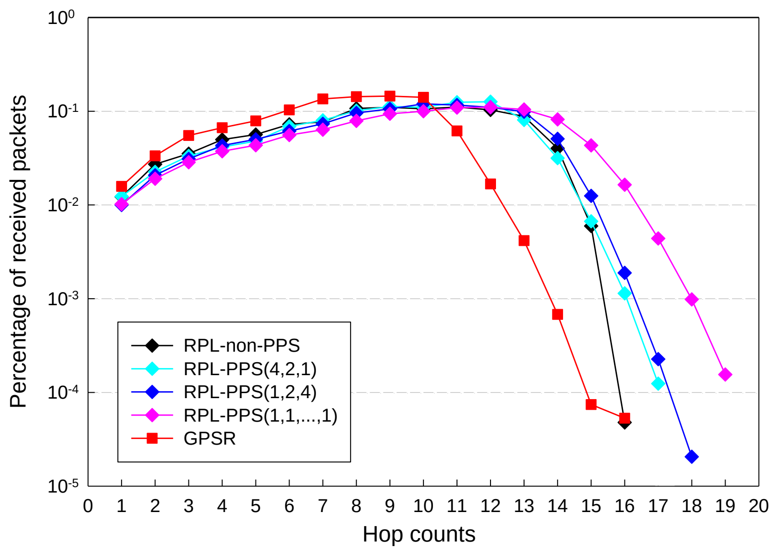

Figure 4.21: Distribution of routing path lengths versus parent switching schemes ($a = 90\%$).

Mean communication cost of routing paths is plotted in Fig. 4.22. It is measured by the ratio of the total number of frame transmissions in the whole network against the number of packets successfully delivered to the DAP. When the network availability a is 100%, GPSR has higher path costs than RPL since it has to try several re-transmissions over those long but unreliable links in order to achieve successful deliveries. However, when a decreases, the impact of node failures on the path cost is negligible. Accurate neighbor connectivity information is maintained and all failed nodes are excluded promptly by frequent hello messages. For a given RPL scheme, as expected, when the network availability (i.e., the number of working nodes) decreases, increasing path costs are observed in Fig. 4.22. This can be explained as follows: A decrease in the number of working nodes might enforce more senders to replace their lower-rank failed parent by higher-rank alternate parents as their next hops. These alternate parents are more likely to require additional transmissions and/or subsequently lead to higher-cost paths to the root. The next observation is that, when there is no node failure, non-PPS works well and results in quite low path cost by sending packets over high quality links connecting the sender to its default parent. However, when nodes failures occur, it may blindly keep sending packets to failed default parents until the DODAG is corrected by conventional local and/or global repairs. Thus, it requires a greater number of transmissions. Compared to RPL-PPS(4,2,1), RPL-PPS(1,2,4) and RPL-PPS(1,1,...,1) require higher routing costs since they tend to deviate traffic to alternate parents that are more likely farther away from the senders and hence lead to links with lower quality and/or longer paths. Note that when network availability a is 90%, the path cost of RPL-PPS(1,2,4) is slightly lower than that of RPL-PPS(4,2,1). This indicates that when there are significant number of node failures, RPL-PPS(4,2,1) might give too many wasteful attempts to primary parents that have likely already failed. Although RPL-PPS(1,2,4) has the lower path cost than all other RPL schemes, GPSR has the lowest path cost as shown in Fig. 4.22. Nodes update their neighbor status with frequent hello messages. The overall GPSR path cost is relatively lower than that of the PPS mechanism since almost none of the GPSR transmissions are wasted on failed nodes.

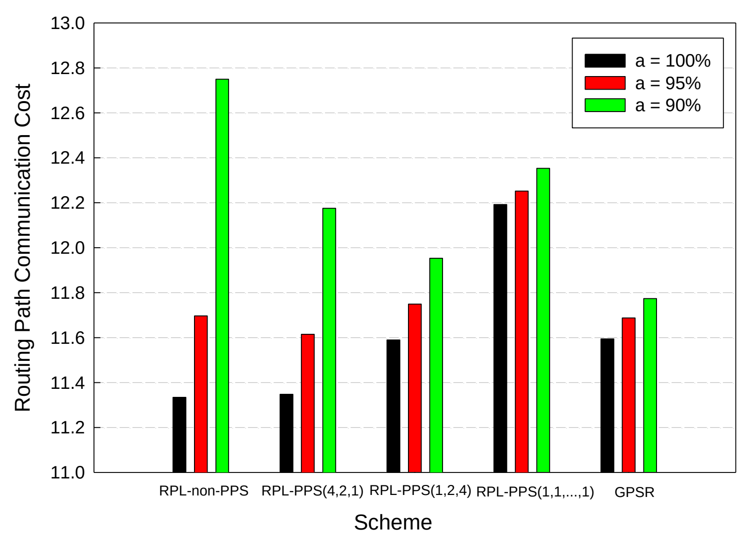

Figure 4.22: Communication cost versus parent switching schemes and network availabilities.

All of the above results in Study Case V give information regarding the ability of GPSR and RPL to operate in networks with different levels of network failures. When network availability a decreases, the robustness of RPL in providing reliable communications is enhanced by the PPS mechanism which notifies different candidates regarding re-transmissions. However, along with path diversity, transmission delay is increased with the increasing number of re-transmissions via non-optimal and longer paths. Generally speaking, for all considered network availabilities, RPL with PPS significantly improves transmission reliability and still produces tolerable transmission delays.

4.2.2 Study Case VI: Effects of Data Traffic Load

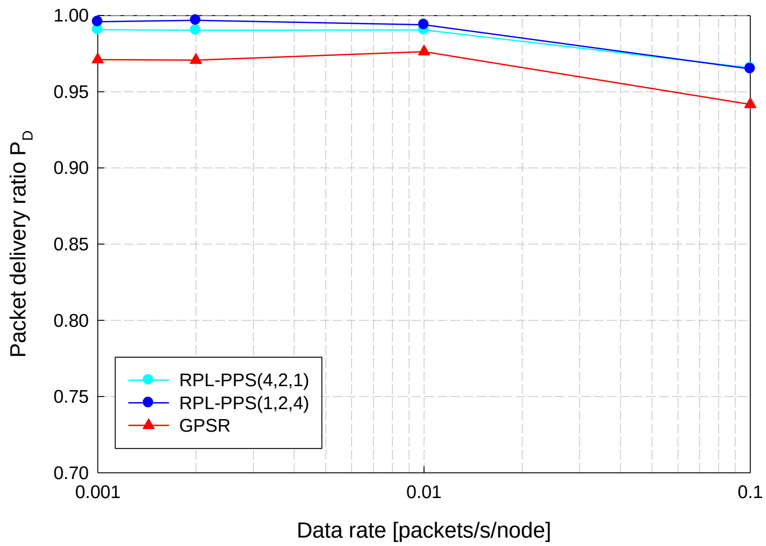

Figure 4.23: PDR of GPSR and RPL with PPS versus per-meter data rates ($a = 90\%$).

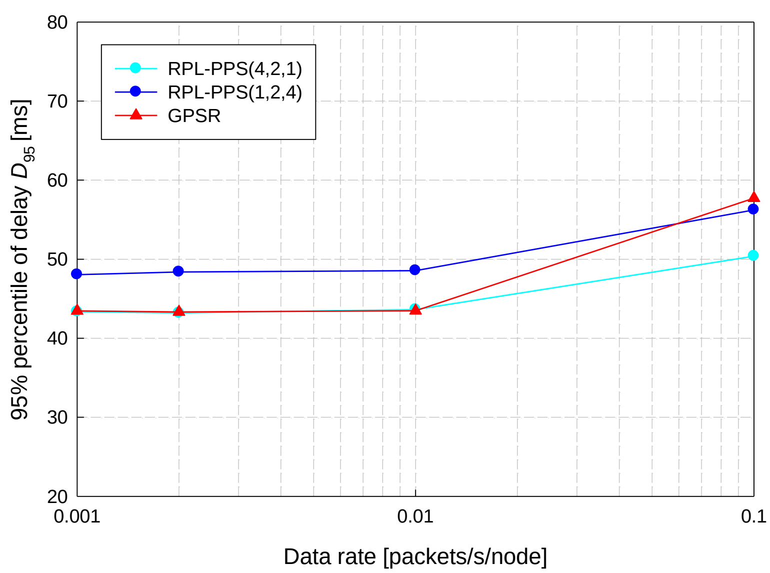

Figure 4.24: 95th percentile of transmission delay of GPSR and RPL with PPS versus per-meter data rates ($a = 90\%$).

To study the effects of increasing traffic load in the presence of node failures, the per-node data rate r is swept in this study case. The comparisons of RPL with PPS to GPSR are plotted in Figs. 4.23 and 4.24. Network availability, channel shadowing variance and cluster size are fixed to 90%, 8.0 dB and 1000 nodes, respectively. It can be observed that there is a decrease in PDR and an increase in transmission delay for both GPSR and RPL when the traffic load becomes heavy. GPSR achieves lower PDR than RPL with PPS in all cases of different traffic loads. When $r = 0.1$ packets/s/node (more than 50 times of the base rate), P_{D} of GPSR drops to 94.17% and D_{95} is increased to 57.72 ms. It can be explained that data traffics intensely compete for channel resources and consequently network collisions occur. At where traffic load is high, GPSR's inability to adapt will degrade performance further. While this problem can be mitigated by PPS's dynamic rerouting to alternative neighbors, as indicated in Fig. 4.23. Comparing between GPSR and RPL with PPS, the latter has improved the transmission reliability over the entire range of data rates of interest. To give some illustrative examples, compared to GPSR, RPL-PPS(1,2,4) can boost P_{D} from 97.07% to 99.69% at the base data rate. However, as can be seen in Fig. 4.24, RPL-PPS(4,2,1) and RPL-PPS(1,2,4) achieve higher PDRs but experience higher delays than GPSR when r is less than 0.1 packets/s/node. Although the packet is redirected to other parents and finally received at the destination, the transmission delay significantly increases due to the cumulative exponential back-off time before each re-transmission. Another interesting observation is that both RPL-PPS(4,2,1) and RPL-PPS(1,2,4) are able to achieve a reliability of higher than 96% even when the network with 90% availability is heavily loaded with 0.1 packets/s/node. In this case, the superiority of RPL with PPS is clearly demonstrated where both RPL-PPS(1,2,4) and RPL-PPS(4,2,1) provide lower D_{95}, i.e., 50.39 ms and 56.23 ms, than that of GPSR, i.e., 57.72 ms. Overall, in comparison with GPSR, RPL with PPS is more efficient to handle node failures and heavy traffic loads.

Chapter 5

Conclusions

This thesis compares the performance of GPSR and RPL, two promising routing protocols used in wireless mesh NANs. Extensive simulations have been carried out with IEEE 802.11-based radio and the practical system parameters related to NAN's characteristics and deployment scenarios specified in NIST's PAP02. In the severe shadowing environment, the results conclude that RPL outperforms GPSR in terms of both packet transmission reliability and delay since it can effectively exploit the link-quality-based metrics (i.e., ETX), to direct traffic over reliable wireless links and finally results in efficient end-to-end paths. Besides, for a cluster of 1000 SMs using RPL in a typical NAN environment, a variety of applications such as smart metering, real-time pricing, demand response, etc., can indeed be supported with packet transmission reliability higher than 99.82% and the 95th percentile of delay less than 26.57 ms. Higher per-meter data rates (up to 50 times of the base rate) or larger network sizes (up to 6000 nodes) can also be supported to accommodate emerging SG applications.

This study also highlights the robustness of considered protocols against network element failures as a critically important feature of SG NANs. For RPL, PPS is proposed to effectively reroute traffic around non-connected network regions caused by SM malfunctions. Extensive simulations have demonstrated that, with properly selected parameters, PPS can significantly improve the packet transmission reliability by adaptively forwarding traffic to alternate next hops once default next hops are detected to be unreachable. Over-reaction to transient network condition fluctuations is prevented by observing over a window of multiple transmission attempts. The results have indicated that PPS can help RPL maintain a higher reliability (higher than 96.5%) in NANs with 90% of network availability under heavy loads (0.1 packets/s/node). As compared to RPL with PPS, the transmission reliability and delay supported by GPSR is only 94.17% and 57.72 ms, respectively. The network performance of GPSR is further degraded by heavier traffic load in the presence of node failures.

By observing the results of all these performed simulations, acceptable efficiency of the proposed PPS and importance of using RPL with construction of routing graph are demonstrated. In comparison with GPSR, RPL is more applicable in NAN communications by having higher system performance (transmission reliability and lower delays) in different channel conditions, traffic loads, and network sizes. Furthermore, with the support of PPS, RPL can successfully reroute packets from failures using alternative paths, and thus improves the performance of the conventional RPL, especially in its robustness. For future work, a number of features/advantages of RPL could be explored, including the capability of QoS differentiation (by routing different types of traffic on different RPL graphs constructed with different routing metrics on the same physical networks) and DAO mechanism with storing or non-storing mode to support downward traffics, etc. Other widely used wireless technologies such as IEEE 802.11g or IEEE 802.15.4 could also be evaluated on their ability to meet the requirements of SG applications.

Appendix A

Geographic Routing with Blacklisting

The geographic routing protocols commonly employ the blacklisting scheme to forward packets on lossy links. Nodes take advantage of excluding unreliable neighbors connected with high-variance links. The determination of optimal forwarding distance for blacklisting strategy proposed in [18] is summarized as follows. In order to obtain the relationship between packet reception rate (PRR) and sender-receiver distance, the authors in [18] follow three steps that gradually find the correlation of distance to received signal strength, received signal strength to signal-to-noise-ratio (SNR) and the SNR to PRR. The realistic channel model presented in [28] is employed. Based on this analytical link loss model, the optimal forwarding distance can be estimated via mathematical analysis. The strength of propagated signal is exponentially decayed with respect to the distance d between sender and receiver. Besides, for a given d, the signal strength is fluctuated randomly by shadowing effect which typically follows log-normal distribution. In other words, the received signal strength $P_{R_x}[dBm]$ at distance d is derived as follows:

$$P_{R_x}[dBm] = P_{T_x}[dBm] - PL(d_0) - 10\alpha \log_{10}\left(\frac{d}{d_0}\right) - X_\sigma. \tag{A.1}$$

where P_{T_x} and P_{R_x} are the transmitted and received radio power, respectively; $PL(d_0)$ is the path loss at the reference distance d_0; d is the distance between transmitter T_x and receiver R_x; λ is wavelength and α is the path-loss exponent; $X_\sigma \sim (0, \sigma^2)$ represents path loss due to shadowing effect and it is a Gaussian random variable with zero mean and standard deviation σ. Given the transmission power P_{T_x}, SNR at distance d is:

$$SNR(d) = P_{R_x}(d) - P_{noise} \tag{A.2}$$

Once SNR is known, corresponding bit error rate (BER) and packet error rate (PER) can be computed. Consequently, the start of unreliable communication range where PER begins to be lower than a predefined threshold can be found. For Eq. (A.2), P_{R_x} is derived from Eq. (A.1) and P_{noise} is the thermal noise which depends on radio characteristics and environment. $P_{noise} = KTB$ where $K = 1.38 \times 10^{-23}$[J/K/Hz] is the Boltzmann's constant; T is an ambient temperature of 300[K](27[°C]); B is the receiver radio bandwidth. Therefore, SNR as a function of d can be expressed as:

$$SNR(d) = P_{T_x} - PL(d_0) - 10\sigma \log_{10}\left(\frac{d}{d_0}\right) - X_\sigma - P_{noise}. \tag{A.3}$$

Eq. (A.3) shows that $SNR(d)$ follows normal random distribution $N(\mu, \sigma^2)$ with mean μ which is $P_{T_x} - PL(d_0) - 10\alpha \log_{10}\left(\frac{d}{d_0}\right) - P_{noise}$. The probability density function of $SNR(d)$ is presented as follows:

$$Pr_{SNR(d)} = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right). \tag{A.4}$$

In this thesis, IEEE 802.11b radio standard is assumed for NAN communications. It offers four different data rates, i.e., 1, 2, 5.5, and 11 Mbps, and each of which corresponds to a given combination of modulation and coding on the PHY layer. When SNR and modulation method are known, BER can be derived. Then PER of different modulation techniques associated with each IEEE 802.11b data rate can be described by their corresponding BER. First, the relationship between BER and PER of an L-byte long data packet [29], denoted by $P_{data_m}(L)$, can be expressed as :

$$P_{data_m}(L) = 1 - (1 - P_{e_1}(24))(1 - P_{e_m}(28 + L)), \tag{A.5}$$

Where $P_{e_1}(24)$ is the probability of error of a 24-byte PHY layer convergence procedure (PLCP) preamble/header transmitted using PHY mode; $P_{e_m}(28 + L)$ is the probability of error of MPDU including 28-byte MAC overhead; $P_{e_m}(x)$ can be expressed in terms of BER as:

$$P_{e_m}(x) = 1 - (1 - BER_m)^{8L}, \tag{A.6}$$

Where BER_m depends on modulation schemes and is estimated for each PHY mode m. Since MAC and PHY layers correspond to IEEE 802.11b, an L-byte long frame will be transmitted using PHY mode m, where m=1, 2, 3, and 4 represents for 1, 2, 5.5, and 11 Mbps PHY rates, respectively. The BER can be expressed by $\frac{E_b}{N_0}$, which is the ratio of energy per bit E_b to noise power N_0. However, instead

Table A.1: Modulation dependent parameters.

Data rate(Mbps)	Modulation	Bits/symbol m	Minimum SNRs (dB)
1	BPSK	1	0.866
2	QPSK	2	1.773
5.5	16-QAM	4	2.312
11	256-QAM	8	4.684

of providing the $\frac{E_b}{N_0}$ metric, the 802.11b presents the signal by SNR, which can be converted to $\frac{E_b}{N_0}$ by Eq. (A.7):

$$\frac{E_b}{N_0} = \frac{SNR \times B}{R}, \tag{A.7}$$

Where R is the respective data rate which can be any of the four IEEE 802.11b data rates; B is the channel bandwidth of 22 MHz. The system based on the IEEE 802.11b technology implements various modulation modes for every transmission rate, which are differential binary phase shift keying (DBPSK) for 1 Mbps, differential quaternary phase shift keying (DQPSK) for 2 Mbps, and complementary code keying (CCK) for 5.5Mbps and 11 Mbp, as described in Table A.1. The M-ary quadrature amplitude modulation (QAM) is used for simplicity and it was proved to yield similar results compared to CCK [30]. BER can be computed for an additive white Gaussian noise (AWGN) channel using equation A.8 for DBPSK and DQPSK modulation [31], and Eq. (A.9) for 16-QAM and 256-QAM:

$$BER = \frac{1}{2}\exp(\frac{E_b}{N_0}) \tag{A.8}$$

$$BER = 2(1 - \frac{1}{\sqrt{M}})erfc(\sqrt{\frac{2E_b}{N_0}}) \tag{A.9}$$

Where $M = 2^m$ is 16 and 256 for the 16-QAM and 256-QAM, respectively; m is the number of bits encoded in one symbol which can contain one of M values; and erfc is the complementary error function. With the assumption of the required BER to be lower than i.e. 10^{-8} for all four modulation schemes, the corresponding minimum SNRs are shown in Table A.1. To calculate the probability that the received SNR is higher than these thresholds, the CDF of $P_{SNR(d)}(x)$ is required and can be computed from Eq. (A.10):

$$F_Y(y) = \frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^{x} \mathrm{e}^{-\frac{(t-u)^2}{2\sigma^2}}\, \mathrm{d}t = 1 - Q(\frac{(y-\mu)}{\sigma}) \tag{A.10}$$

The probability that received signal $SNR(d)$ is higher than $SNR_{threshold}$ is:

$$
\begin{aligned}
&\Pr(d)\left[P_{SNR(d)}(x) > P_{SNR_{threshold}}\right] \\
=&1 - \Pr(d)\left[P_{SNR(d)}(x) < P_{SNR_{threshold}}\right] \\
=&1 - \left[1 - Q(\frac{y-\mu}{\sigma})\right] = Q\left(\frac{SNR_{threshold} - \mu}{\sigma}\right) \qquad \text{(A.11)} \\
=&\frac{1}{2} - \frac{1}{2} erf\left[\frac{SNR_{threshold} - (P_{T_x} - PL(d_0) - 10nlog_{10}(\frac{d}{d_0}) - P_{noise})}{\sigma\sqrt{2}}\right]
\end{aligned}
$$

Where Q-function can also be expressed in terms of the error function erf. The $SNR_{threshold}$ is defined to be 0.886dB, which is the minimum required SNR to demodulate a packet for the lowest data rate 1Mbps. With the channel bandwidth of 802.11b is 22MHz, the corresponding thermal noise P_{noise} is $-101dBm$. At different distance d, the mean of SNR varies as a function of d. In addition, different shadowing deviations also have the corresponding effect on the probability of the PRR, which both can be observed from Fig. A.1 below.

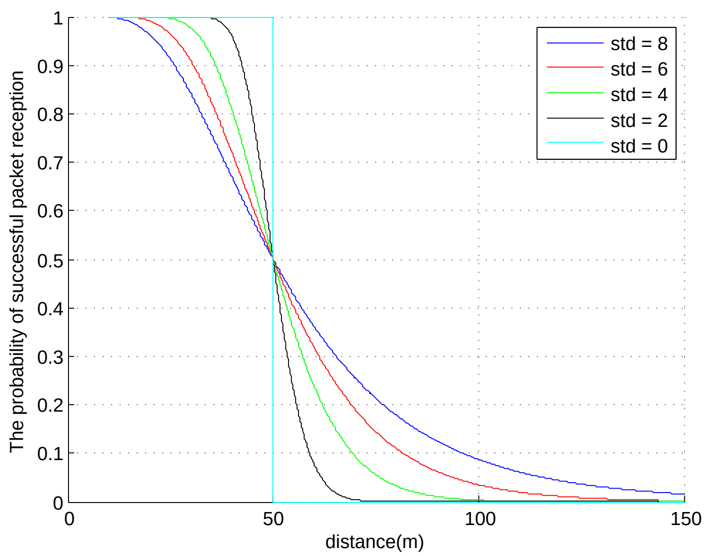

Figure A.1: Packet reception rate to distance per transmission.

The wireless link can be classified into three reception regions based on PRRs: connected, transitional and disconnected [32]. The connected region is defined to be the range of the distance in which a link has the PRR higher than 95%; the transitional region is where the PRR is bounded between 95% and 5%; the disconnected region is where the PRR is lower than 5%. Major concern is given to the transitional region since it significantly affects the network robustness.

Any pair of nodes within that range has the probabilistic connection, so called a lossy wireless link such that link dynamics vary with link fluctuations. The transitional region is often large and influenced by the channel variance. When $\sigma = 0.0$ dB, there is no log-normal shadowing and thus SNR decays monotonically with distance. The PRR is about 100% within the connected region while it instantly drops to 0% when SNR falls below $SNR_{threshold}$. The distance 50 m is the boundary to distinguish the connected region and the disconnected region. In this case, there is no transition region. When $\sigma = 4.0$ dB, the transitional region spans from 43m to 75m. A higher shadowing standard deviation implies a larger transitional region, which increases the number of unreliable and asymmetric links. When $\sigma = 8.0$ dB, the width of the transitional region increases, which starts from 15m to 135m.

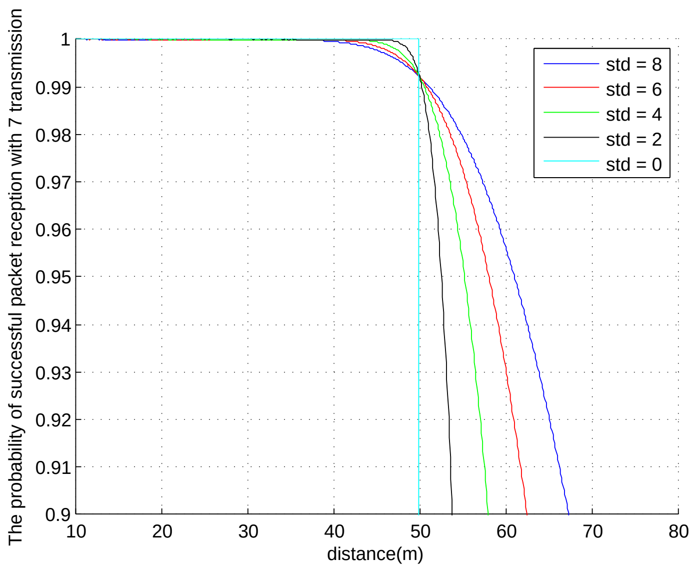

Figure A.2: Packet reception rate to distance per 7 retries.

The MAC level re-transmission is a necessary technique that should be combined with blacklisting to promise high reliability of packet transmission. Blacklisting filters out those paths with moderate reliability and re-transmissions further improves the transmission reliability along them. It can be observed in Fig. A.2 that the PRR is greatly improved with the combination of blacklisting and max 7 re-transmissions at the IEEE 802.11 MAC. This distance-PRR curve will be used as the reference to determine the connected, transitional and disconnected regions for GPSR with blacklisting. Those links with long distances and resulting in PRR lower than 95% will be considered as highly unreliable links and ignored. For example with $\sigma = 8.0$ dB, GPSR blacklists those neighbors in the transitional region, nodes that are further than 50 m away, and then selects the closest one to the destination among the remaining reliable neighbors. Setting such a high threshold for blacklisting could ultimately guarantee links with relatively high quality, but it may also cause greedy forwarding failure when a node has no neighbor in its connected region. Fortunately, this problem can be solved in GPSR by switching the greedy forward routing to the perimeter routing as in the case where there is no potential forwarder.

Appendix B

PHY and MAC Layer Specifications and Operations of IEEE 802.11b

For the communication modules built in each SM, IEEE 802.11b PHY and MAC layers are selected. The PHY layer operates at 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 carrier sense multiple access with collision avoidance (CSMA/CA) mechanism. A node with a new packet to transmit senses the channel. If the channel is sensed idle for a time interval equal to a DIFS, the node transmits. Otherwise, if the node senses a transmission either immediately or during the DIFS, it continues monitoring the channel. 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 time, the node transmits if the channel is idle. The 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. At each packet transmission, the back-off time is X times the contention window 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 transmissions failed for the packet. At the first transmission attempt, CW_0 is set equal to the minimum contention window $CW_{\min}$. Binary exponential back-off is assumed: after each unsuccessful transmission, contention window is doubled, up to a maximum value $CW_{\max}$. In other words, the contention window for the n-th trial is $CW_n = \min\{(CW_{\min}+1)\times 2^n - 1, CW_{\max}\}$. The back-off time counter is decremented and a node transmits when the back-off time reaches zero. Once the data packet is received successfully,

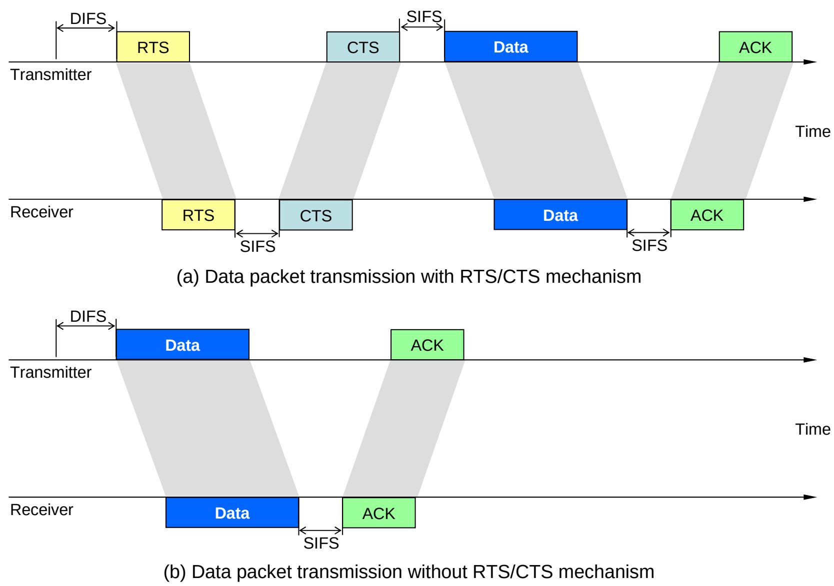

Figure B.1: The timing diagram showing basic operations of IEEE 802.11 CSMA/CA with and without RTS/CTS.

the receiver sends an ACK to signal successful reception. ACK is transmitted at the end of the packet, after a period of SIFS. If the transmitting node does not receive the ACK, it reschedules the 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. B.1. More details on IEEE 802.11 PHY and MAC layers can be found in [33].

Packet Transmission delay D_p of data packet p is significantly affected by the above-mentioned PHY and MAC operations. Its calculation is shown in the following:

$$D_p = T_p^{\mathrm{RTS}} + T_p^{\mathrm{CTS}} + T_p^{\mathrm{ACK}} + T_p^{\mathrm{DATA}} + T_p^{\mathrm{BO}} + T_p^{\mathrm{IFS}}. \tag{B.1}$$

Note that these components represent accumulated values since for a successful delivery of a data packet there might be multiple back-off stages and packet re-transmissions. It can be seen from Fig. B.1 and Eq. (B.1) that, for a packet of 100 bytes of data, when RTS/CTS mechanism is enabled, transmission delay for the best-case (i.e., when there is no collision, back-off, re-transmission and the highest AMC mode with data rate of 11.0 Mbps is selected), denoted by $D_{\mathrm{min}}^{\mathrm{RTS/CTS}}$, can be calculated as follows:

$$
\begin{aligned}
T_{\text{RTS}} &= \frac{\text{PHYheader} \times 8}{10^6} + \frac{\text{RTSpayload} \times 8}{11 \times 10^6} = \frac{24 \times 8}{10^6} + \frac{20 \times 8}{11 \times 10^6} \approx 206.6\ \mu\text{s} \\
T_{\text{CTS}} &= \frac{\text{PHYheader} \times 8}{10^6} + \frac{\text{CTSpayload} \times 8}{11 \times 10^6} = \frac{24 \times 8}{10^6} + \frac{14 \times 8}{11 \times 10^6} \approx 202.2\ \mu\text{s} \\
T_{\text{DATA}} &= \frac{\text{PHYheader} \times 8}{10^6} + \frac{(\text{PHYheader} + \text{NETheader} + \text{AppData}) \times 8}{11 \times 10^6} \\
&= \frac{24 \times 8}{10^6} + \frac{(34 + 18 + 100) \times 8}{11 \times 10^6} \approx 302.6\ \mu\text{s} \\
T_{\text{BO}} &= 0 \\
T_{\text{IFS}} &= \text{DIFS} + \text{SIFS} \times 2 = 50 + 10 \times 2 = 70\ \mu\text{s}
\end{aligned}
$$

$$
\Rightarrow D_{\min}^{\text{RTS/CTS}} \approx 781.3\ \mu\text{s}. \tag{B.2}
$$

In the case when RTS/CTS mechanism is disable, transmission delay for the best-case, denoted by $D_{\min}$, can be calculated as follows:

$$
\begin{aligned}
T_{\text{RTS}} &= 0 \\
T_{\text{CTS}} &= 0 \\
T_{\text{DATA}} &\approx 302.6\ \mu\text{s} \\
T_{\text{BO}} &= 0 \\
T_{\text{IFS}} &= \text{DIFS} = 50\ \mu\text{s}
\end{aligned}
$$

$$
\Rightarrow D_{\min} \approx 352.6\ \mu\text{s}. \tag{B.3}
$$

However, since collisions, back-offs and re-transmissions are expected, packet transmissions may experience higher delays compared to the best-case values.

Statistics of transmission delay are represented by the average value $\overline{D}$ or CDF, namely $F_D(d)$. $\overline{D}$ and $F_D(d)$ are calculated as follows:

$$
\overline{D} = \frac{1}{|\mathbf{N}_{\text{rx}}|} \sum_{p \in \mathbf{N}_{\text{rx}}} D_p, \tag{B.4}
$$

$$
F_D(d) = \Pr[D < d] = \frac{|\mathbf{N}_{\text{rx}}(D \leq d)|}{|\mathbf{N}_{\text{rx}}|}, \tag{B.5}
$$

where $\mathbf{N}_{\text{rx}}$ and $\mathbf{N}_{\text{rx}}(D \leq d)$ are set of data packets that are received and decoded successfully by the DAP and a subset of $\mathbf{N}_{\text{rx}}$ whose transmission delay is equal to or lower than d, respectively;

Bibliography

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

[2] *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.

[3] M. S. Obaidat, A. Anpalagan, and I. Woungang, *Handbook of green information and communication systems.* Academic Press, Nov. 2012.

[4] G. Privat *et al.*, "Smart building functional architecture," Finseny, Tech. Rep., Mar. 2013.

[5] 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.

[6] 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.

[7] 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.

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

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

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

[11] 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.

[12] T. Clausen *et al.*, "A critical evaluation of the ipv6 routing protocol for low power and lossy networks (rpl)," in *in Proc. of the 2011 IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications*, 2011, pp. 365–372.

[13] K. D. Korte, A. Sehgal, and J. Schonwalder, "A study of the rpl repair process using contikirpl," in *in Proc. the 7th International Conference on Autonomous Infrastucture, Management and Security (AIMS)*, 2012, pp. 50–61.

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

[15] 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*, 2014.

[16] F. Cadger, K. Curran, J. Santos, and S. Moffett, "A survey of geographical routing in wireless ad-hoc networks," *IEEE Communications Surveys Tutorials*, vol. 15, no. 2, pp. 621–653, 2013.

[17] 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.

[18] K. Seada, M. Zuniga, A. Helmy, and Bhaskar, "Energy efficient forwarding strategies for geographic routing in lossy wireless sensor networks," in *ACM 2nd Conference on Embedded Networked Sensor Systems*, 2004.

[19] O. Gnawali *et al.*, "Interaction of retransmission, blacklisting, and routing metrics for reliability in sensor network routing," in *IEEE SECON 2004*, 2004, pp. 34–43.

[20] I. D. Chakeres and E. M. Belding-Royerl, "The utility of hello messages for determining link connectivity," in *Excellent Paper Award Proceedings of the 5th International Symposium on Wireless Personal Multimedia Communications (WPMC) 2002*, Oct. 2002.

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

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

[23] I. Bhakta *et al.*, "Incorporating qos awareness in routing metrics for wireless mesh networks," *International Association of Engineers*, vol. 1, Jul. 2010.

[24] D. S.J.DeCouto, D. Aguayo, J. Bicket, and R. Morrisi, "A high-throughput path metric for multi-hop wireless routing," in *ACM Mobicom*, May 2003.

[25] R. Draves, J. Padhye, and B. Zill, "Routing in multi-radio, multi-hop wireless mesh networks," in *In ACM MobiCom*, Sep. 2004.

[26] K. han Kim and K. G. Shin, "On accurate measurement of link quality in multi-hop wireless mesh networks," in *ACM MobiCom*, 2006, pp. 38–49.

[27] 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.

[28] A. Goldsmith, *Wireless Communication*. Cambridge University Press, Aug. 2005.

[29] S. C. Javier del Prado Pavon, "Link adaptation strategy for ieee 802.11 wlan via received signal strength measurement," in *IEEE ICC*, May 2003, pp. 1141–1145.

[30] G. D. Holland, N. H. Vaidya, and P. Bahl, "A rate-adaptive mac protocol for multihop wireless networks," in *In Proc. ACM/IEEE MobiCom*, Jul. 2001, p. 236–251.

[31] H. K. Jean-Pierre Ebert, Dániel Hollós and M. Löbbers, "Does multi-hop communication reduce electromagnetic exposure?" *The Computer Journal*, vol. 48, no. 1, pp. 72–83, 2005.

[32] C. Yin and T. Andreas, "On the implications of the log-normal path loss model: an efficient method to deploy and move sensor motes," in *SenSys*, 2011, pp. 26–39.

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