Wireless Mesh Routing in Smart Utility Networks

by

Gopalakrishnan B. Iyer

A thesis submitted to the Graduate Faculty of
Auburn University
in partial fulfillment of the
requirements for the Degree of
Master of Science

Auburn, Alabama
Dec 12, 2011

Keywords: Wireless networks, Smart meters, Smart utility networks,
Directed acyclic graph

Approved by

Prathima Agrawal, Chair, Samuel Ginn Distinguished Professor, Electrical and Computer
Engineering
Shiwen Mao, Associate Professor, Electrical and Computer Engineering
Thaddeus Roppel, Associate Professor, Electrical and Computer Engineering

Abstract

Today's world is more dependent on electrical power than ever. This dependency will increase manifold in the near future with more systems being computerized and a plethora of new electronic devices emerging for household, commercial and industrial applications. The availability of reliable electric power is crucial to sustaining current development and economic growth trends. Integrating intermittent power generated from renewable sources of energy such as wind, solar, geothermal and other energy sources with the existing power grid is the single greatest challenge of the 21st century. In order to achieve this task, a highly granular measurement of power consumed is paramount to achieving optimal efficiency through demand-response programs. This is the Smart Grid initiative, aimed at installing a highly efficient communication infrastructure for consumption data acquisition to achieve optimal demand-response of resources.

Recent advances in wireless communication technology, has allowed for low cost, low power devices to be deployed in large scale. The Smart Utility network is one such widely deployed network which is inherently tied to the physical systems of electric power, water and gas. A network of such devices, performing critical tasks requires an efficient data routing protocol in order to function as designed. Data routing protocols such as AODV (Ad-hoc On-demand Distance Vector) and DSR (Dynamic Source Routing), developed for wireless sensor networks fail to address the requirements of these networks in terms of inter-operability, routing metrics, network topology and sheer

scale of the network size. NIST (National Institute of Standards and Technology) has developed a conceptual reference model for deployment of smart utility networks and has laid out the framework for interoperable systems for the smart grid.

This thesis provides an overview of the existing communication infrastructure for the legacy power grid while describing the rapidly growing smart grid initiative and analyzes the performance of the wireless mesh routing protocols of Geographical routing and RPL (Routing Protocol for Low power and lossy networks) as applied to smart utility networks. Various routing metrics of packet success probability, end-end delay, hop count and link quality have been considered for this performance analysis. Further, realistic network topologies, obtained from actual smart meter network deployments in North America have been modeled in simulations to derive at results pertinent to the applicability of these wireless mesh routing protocols to Advanced Metering Infrastructure comprising of smart utility networks. The core contribution in this thesis is the construction of a simulation model for routing in wireless mesh utility networks using the discrete event simulator OMNeT++ and subsequent analysis of the two mentioned routing protocols using real-world topologies. This work has been performed in collaboration with Landis+Gyr, who provided actual deployment data for smart utility networks.

Acknowledgements

Table of Contents

List of Figures

Chapter 1

Introduction

It is a popular notion that while Alexander Graham Bell would have no idea what to make of the modern internet and communication technologies like the smart phone, Thomas Edison would still recognize and be quite comfortable with our power grid. Unfortunately, while the means of supplying energy has stayed largely the same throughout the years, demand has drastically increased and continues to grow with each passing year. The electric power infrastructure in North America is among the most complex systems ever constructed. With over 3,500 utility organizations, supply and demand are kept in balance at all times, while obeying the loading constraints. This mind boggling operation is kept functional using a communication infrastructure which is archaic. Electricity generation and distribution in 2011 is like computing and communication in 1971 [1].

Efficient communication architecture is essential, so that stability problems that develop in the grid can be reported much faster than they develop. With the current systems that are in place, stability problems in the grid can develop much faster than they can be reported. The need for better communication architecture is answered by the Smart Utility Network, which is an integral part of the Smart Power Grid. Devices built

on the seven layer OSI internet model, using optimal data routing protocols, media access control and latest physical layer wireless technology, are key to achieving a highly efficient Smart power grid and can be extended to various utilities such as water and gas.

1.1 Smart Power Grids

The revolutionary concept being employed in the smart power grid is the two-way communication between the consumer and the utility at the appliance/meter level. This will enable the consumer to continuously monitor power usage and make instantaneous decisions related to power saving using applications developed based on IPv6. Also, embedded controllers running these applications in appliances can communicate with Smart utility networks to automatically control power consumption during peak and off-peak load times. This will ensure that power is not utilized by the appliance when the consumption of power is costliest. One such system employs a wireless communications network that collects data from consumers and feeds it to collection points that send it to the enterprise back end systems. This data is used for time-of-the day usage based billing, load management and outage control among other functions.

1.1.1 Existing Communication Architecture

Currently, a very outdated and archaic communication system is used to co-ordinate such a complex grid system. It has been developed several decades ago to meet the needs of a regulated power industry. Today, the de-regulation of the power sector has led to several thousand utility providers, pushing the existing transmission line infrastructure to its limits. Power generation stations, transmission and distribution

centers and utility providers manage the delicate balance between demand and supply and ensure that power generated thousands of miles away reaches the target consumers, just-in-time. This communication involves control centers, substations and Supervisory Control and Data Acquisition (SCADA) systems in a star topology. Existing power grid communication system shown in Figure 1.1 consists of RTUs (Remote Terminal Units) at power plants and transmission and distribution centers which are linked to SCADA systems and a fault detection and correction scheme called Remedial Action Scheme (RAS). The link carries control and status information between each unit, which in this case can be different utilities with a sampling period of a few seconds. The control center at the utility consists of a central database connected to operation and commercial units. Many such control centers of different utilities are linked to each other by regional control centers. This type of a communication system will result in slow automatic control to balance load and generation. If a power outage occurs, the available systems with fast controls like the RAS will protect short-circuits and regulate voltages on lines, but it can neither detect nor correct rapidly occurring cascading failures in the power grid. It is evident that the communication system needs massive overhaul and upgrade to cater to the needs of the ever growing power grid.
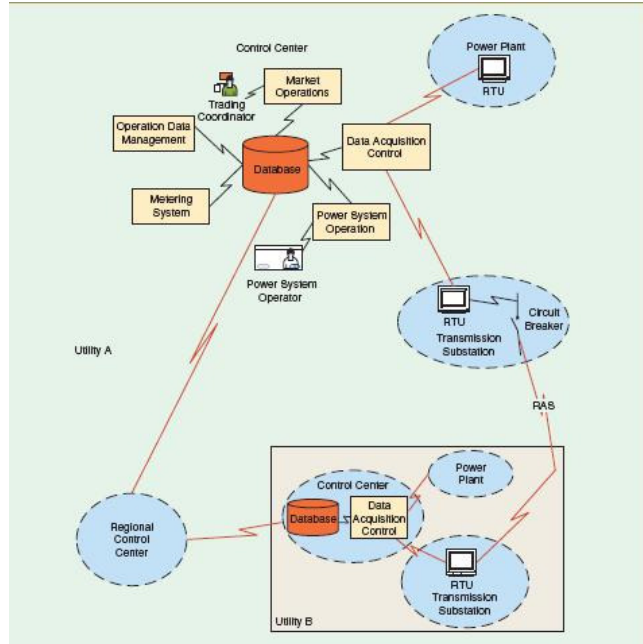
Figure 1.1: Existing Communication Architecture for the Power grid [1].

Devices like the IED (Intelligent electronic device) or Phasor measurement units (PMU's) which are available today to monitor power quality and have the ability to gather information several times in a single power cycle, are capable of allowing for planning and analysis of the power networks. These devices are limited to deployment only at the substation level and not grid wide due to the outdated communication infrastructure. The SCADA systems were developed with performance in focus rather than security. These components used for automating the power infrastructures used proprietary communication standards and operating systems which were designed primarily for functionality and performance rather than security. This is because security systems and automation systems are developed at different rates and are isolated from each other. This meant that the vendor providing the automation systems, did not bundle-

security and the consumer had to implement different systems to ensure security. Protection systems are applied locally to safeguard specific components and by central control through the supervisory control and data acquisition (SCADA) system. The central control system is too slow, and the protection systems are limited to protection of specific components only.

1.1.2 NIST Conceptual Model

The conceptual model outlined by National Institute of Standards and Technology (NIST) for Smart Grid interoperability supports planning and organization of the diverse, expanding collection of interconnected networks that will compose the Smart Grid. It divides the model into two domains as Actors and Applications. Actors include devices, systems, or programs that make decisions and exchange information necessary for performing applications. Smart meters, solar generators, and control systems represent examples of these devices and systems.

Applications, on the other hand, are tasks performed by one or more actors within a domain. Examples of these applications are home automation, solar energy generation and energy storage, and energy management.
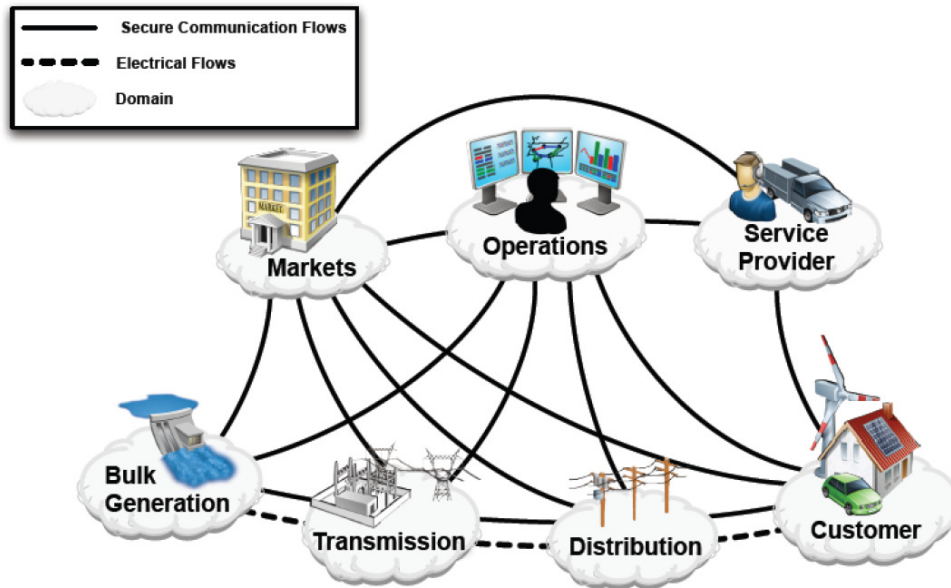
Figure 1.2: NIST Conceptual model for the Smart Power grid [2].

Figure 1.2 shows in concept, the communication flows and power flows between the seven domains of Consumer, Transmission, Distribution, Power Generation and Markets, Operations at the Enterprise back-end systems and Service providers.

As manual labor is being replaced by automated control, equipments are being networked for control from a single SCADA system. To avoid the cost of private lines which carry control data, the internet is an attractive option to network such devices. Wireless deployment is the most suitable option due to its low deployment costs in comparison to other physical layer technologies. NIST defines this overall system as a Cyber-physical infrastructure as:

- Electronic information and communications systems and services and the information contained in these systems and services.

- Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types.

- Communications include sharing and distribution of information. These include the following:

  - computer systems; control systems (SCADA);

  - Networks, such as the Internet.
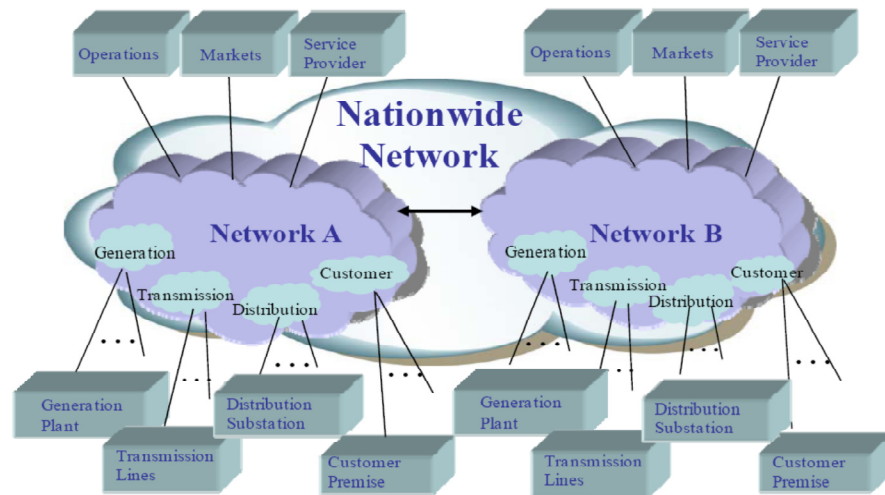
Figure 1.3: NIST model of network communication for the Smart Power grid [2].

Figure 1.3 represents the network communication model for the smart grid. This model can be compared to the current data networks and internetworking systems [2].

1.2 Advanced Metering Infrastructure (AMI)

As a part of the Smart Grid initiative, manually monitored utility meters for electricity, water and gas are being rapidly replaced by highly automated and networked smart meters. These networks may be connected to the Internet and provide two-way communication between the end user and the utility service provider. Smart utility networks comprising of wireless meters for electricity, water and gas can be considered as wireless sensor networks. The main function of such meters is to report data acquired from sensors periodically back to a collection point or a collector device. Together, these devices constitute the AMI. Legacy systems which are capable of Automated Meter Reading (AMR) cannot be considered as an AMI as the older systems are not capable of two-way communication with the metering devices.
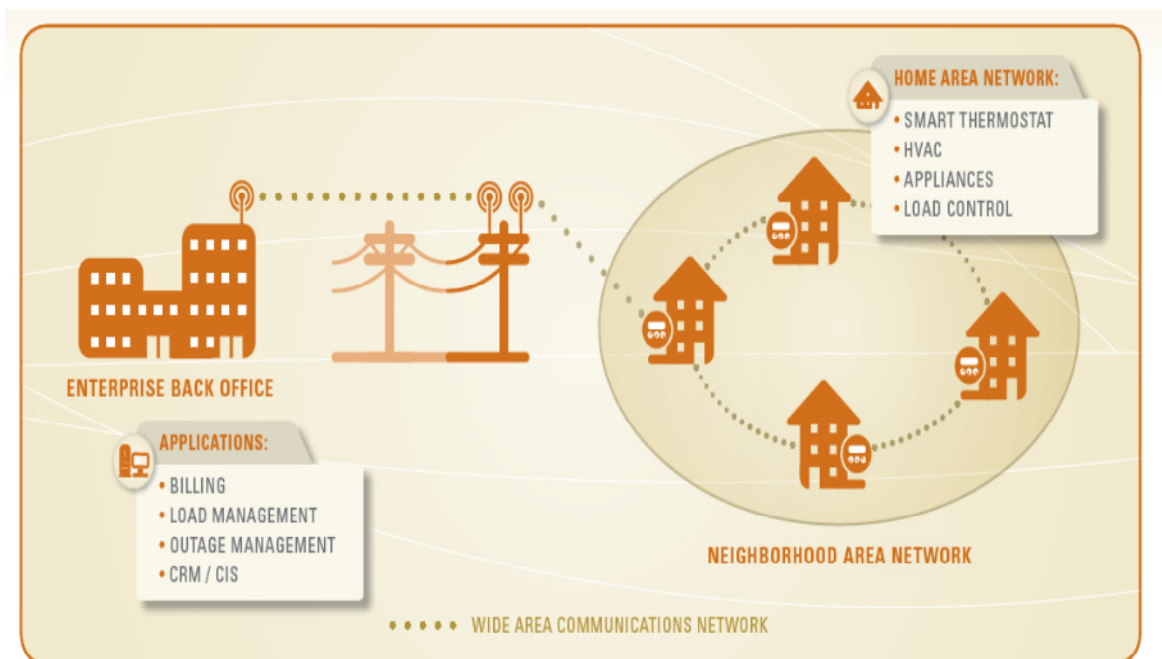
Figure 1.4: Advanced Metering Infrastructure (AMI) system [3].

Figure 1.4 shows one such AMI system comprised of home automation devices, transmission and distribution automation devices, connected to the back-end systems using wireless communications. The information collected by such an AMI can be used for improving the efficiency of generation and distribution of the monitored utility and prevent wastage of resources. A robust AMI can also quickly identify intrusions and security threats to such cyber physical systems, which are an integral part of our day-to-day lives. A data routing protocol is essential for forwarding collected information to an aggregation point. Thus, a fully functional protocol suite for networking of such smart metering devices is imperative to the success of the Smart Grid. These metering devices are small in size and are cost effective due to the enormous deployment volume. In such devices, wireless interfaces are provided for efficiently forwarding the acquired data to collection points. Use of wireless technology for communication has the well known shortcomings of lower reliability due to fading and interference, low data rates and susceptibility to intrusions and security threats. Moreover, low power consumption, limited computing power and storage restrictions are typical of such devices participating in the smart utility networks. In contrast to legacy network devices such as routers and switches which constitute the existing global internet, these metering devices are aware of the traffic characteristics based on pre-defined set of governing criteria. The approbation of such metering devices by the utility industry requires standardization of protocols employed in them. In addition to the AMI, industrial process monitoring, in-building automation, building energy management, home automation, health care, logistics etc. are target low-cost network end applications of these routing protocols [3], [4].

9

Chapter 2

Network Architecture

Smart utility networks can be deployed using various wireless network architectures. These networks can be implemented as wireless cellular networks or as a wireless mesh networks. The goal is to provide complete connectivity to all the metering nodes in the network. High reliability and low end to end latency combined with 100% packet success and delivery ratios are the requirements of an AMI network. In such networks, the quality of service is of utmost importance. Cellular network architectures in general are providers of greater quality of service as more often than not, they use licensed radio spectrum for their service and are fairly immune from the effects of interference. This type of deployment bears a significant infrastructure cost and complexity of deployment. The cellular deployment also requires extensive radio planning in order to optimize installation and use of infrastructure. On the other hand, a wireless mesh network does not involve use of complex infrastructure. In the case of an electric utility AMI network, it consists of the electric meters themselves, equipped with wireless communication capabilities and several collection points. In this mesh network, the electricity meters form an ad-hoc self organizing mesh and communicate with the collection points known as collectors, thus requiring minimal deployment effort and

network management. Wireless mesh network deployment is an optimal choice for deploying an AMI.

2.1 Smart Utility Wireless Mesh Network Hierarchy

Wireless Mesh Networks are formed by nodes which communicate directly with at least one other node. Each node in the networks performs the function of generating traffic and has the capability of forwarding data from other nodes toward a destination. The destination node may or may not be within their transmission range. The critical aspect of this network architecture is the ability of nodes to be self-organizing and periodically exchange messages to maintain network state such as connectivity, battery life and reliability.

In Smart utility networks, the wireless nodes are metering devices and distribution automation devices. In addition, there is a collector node, which serves as a destination for collection of periodic power consumption data. There may be many such collector devices, each representing a separate mesh network of metering nodes. Such collectors may have internet connectivity through a backhaul communication network, to send the collected data to enterprise back-end systems [5].

2.1.1 Home Area Network (HAN)

Home appliances and other electronic consumer devices are embedded with two-way communication capability using IEEE 802.15.4 based radio. There are a plethora of Bluetooth and Zigbee devices currently available for home automation applications.

Several such devices, communicating with one another or a central in-home energy monitor form the HAN. The ultimate goal is to report consumption data from these devices to the electric metering device, which then disseminates the data to the back-end system using the smart utility network mesh.

2.1.2 Neighborhood Area Network (NAN)

The wireless mesh network formed by thousands of metering end-points and the collector device is one Neighborhood Area Network. These networks typically represent a particular geographic location or a Neighborhood comprising of several thousand homes. The collector device in each NAN is connected via backhaul communication systems to the enterprise head end system.

2.1.3 Wide Area Network (WAN)

Several Neighborhood Area Networks are required to be networked, in order to collect the data generated by devices in the Home Are Network. A wide area network may span tens of miles and typically covers an entire city. The technology used to deploy a Wide Area Network may be wireless or wired and requires large bandwidth. WiMAX is a popular technology used to deploy WANs. The data acquired is ultimately used for demand-response applications and time of the day pricing based billing policies.
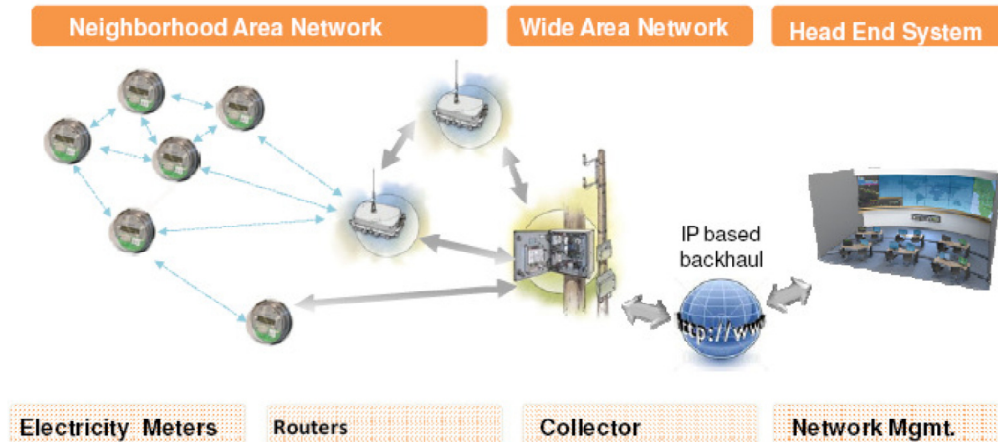
Figure 2.1: Smart Utility Mesh based Architecture [5].

Figure 2.1 shows the hierarchical architecture of Smart Utility Networks, in which several metering devices with routers and collectors in a mesh network form the Neighborhood area network and report to the head end systems though backhaul wide area networks.

Metering end points transmit and receive data at a speed of 9.6kbps whilst Router nodes and Collectors are able to transmit and receive at either 9.6kbps or at double this speed, namely 19.2kbps. Routers are typically mounted strategically on pole tops or on lamp posts and enjoy an improved high-speed line of sight communication to other Routers or ideally even the Collector itself. Metering end points typically transmit at power levels of 450mW which provides a few hundred meters of range whilst Routers transmit at higher power levels of 1W which provides up to 2km range between Routers. The Router mesh acts as a high speed communication highway for the meter traffic. Routers are also used as range extenders to bridge areas where there are no meters or only

scarce populations of meters which would otherwise lack mesh connectivity to a Collector. The Collector is equipped with 4 radio channels in order to handle the aggregated traffic of the whole network under its control. A Collector can typically handle up to 25,000 metering end points in a single network. Collectors are deployed throughout the Utility's service area to cover the entire population of meters. The number of Routers required in a network depends on the distribution of metering end points [5].

2.2 Real Network Topology

In the study of wireless mesh networks, a playground grid size is chosen for the simulation. In this playground, nodes are placed at random locations based on a chosen seed or they are distributed according to a uniform distribution with chosen mean and standard deviation. Although these distributions are good for simulations, they do not represent the way in which smart metering nodes are distributed in a real-world network.

In order to study routing protocols for smart utility networks, forming a wireless mesh, incorporating real world topologies are essential. Trace files containing geographical locations of real world deployed smart metering nodes were obtained and used in simulations to arrive at simulation results and conclusion herein.

Clusters of 500 and 1000 metering nodes with the collector located at the center of the deployed area derived from a large AMI deployment were used as network topologies for the simulation of data traffic in smart utility networks. In order to obtain real world comparable performance metrics from the routing protocols, it was necessary to use real deployed network topologies instead of a randomized topology. In general,

connectivity and performance are directly related to the network topology in which a routing protocol is used. Figures 2.2 and Figure 2.3 show the real topologies of 1000 and 500 nodes used for the performance analysis [6], [7].
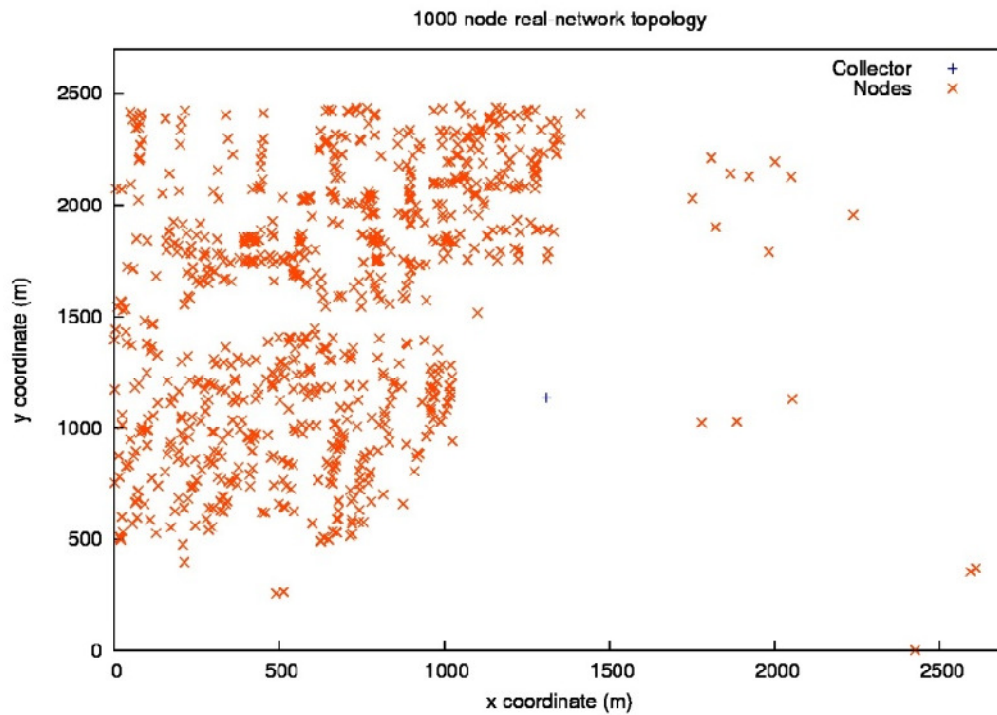
Figure 2.2: 1000 node real network topology
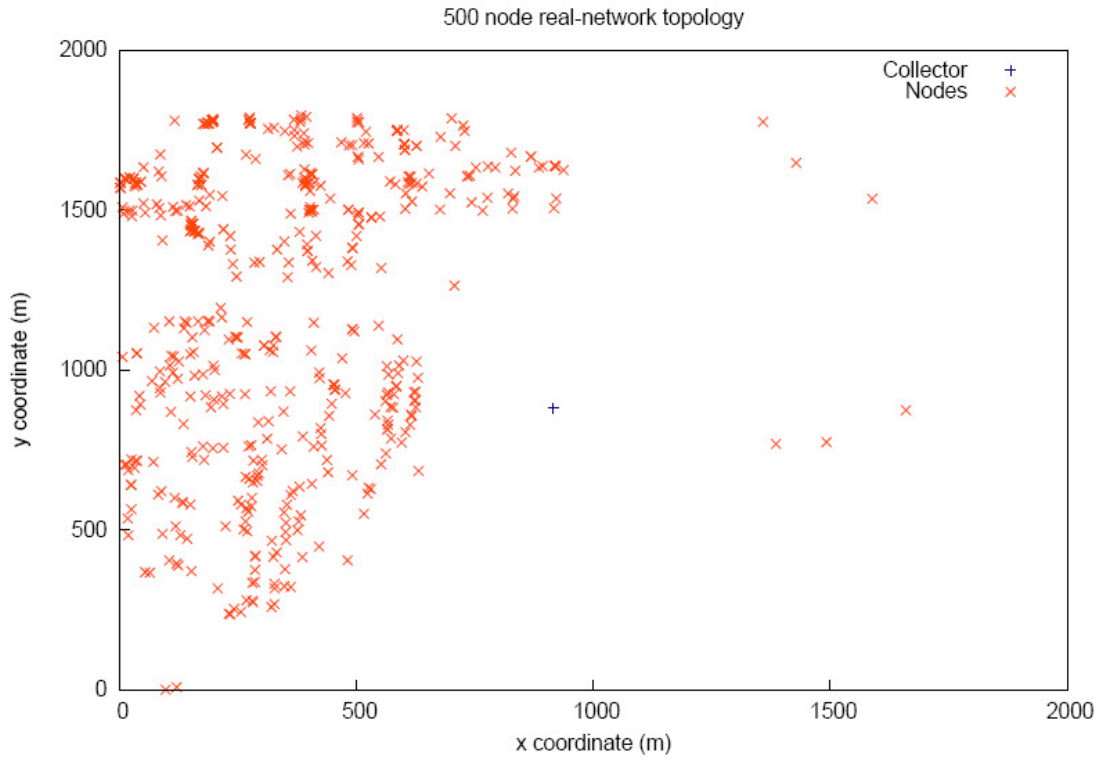
Figure 2.3: 500 node real network topology

Chapter 3

Radio and Wireless Environments

The choice of radio for any hardware mainly depends on the factors of power, data-rate and operating frequencies. Proprietary radios generally operate in a licensed spectrum for which the user is billed. On the other hand, IEEE standards based radios operate in the license free spectrum allocated for target applications by the FCC. Wireless Local Area Network (WLAN) and Worldwide Interoperability for Microwave Access (WiMAX) are the most popular examples operating on IEEE 802.11 and IEEE 802.16 standards, respectively.

Smart Utility Networks are comprised of low power devices communicating at a low data rate. The maximum allowed transmission power for such devices is 20dBm (100 mW) and can communicate at a maximum data rate of 250 kbps. Typically, devices in Smart Utility Network operate at 0dBm and a variable data rate between 25 kbps and 250 kbps. The IEEE 802.15.4 specifications for MAC and PHY are built for such target devices, operating at low power, low data rates and in highly lossy environments. The Zigbee alliance has adopted these standards for all Zigbee enabled devices. The IETF working group 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks) has adopted this standard for building a wireless embedded internet [8], [9], [10].

3.1 IEEE 802.15.4 PHY layer

The IEEE 802.15.4 physical layer has been designed to support low data rate wireless communication networks with restricted power. It has been developed for rapid deployment of low cost communication networks based on a standard. The radio operates on two unlicensed spectral frequencies of 868/915 MHz and 2.4 GHz and is chosen according to the target application. In the 868/915 MHz band, there are 11 (0 at 868.3 MHz and 1-10 up to 928 MHz) channels available, each 2 MHz wide. In the 2.4 GHz band, there are 15 (11-26) channels of 5 MHz each.

In the 2.4 GHz spectrum, the date rate is 250 kbps. The data modulation scheme is 16-ary orthogonal modulation with 4 bits/symbol and 62.5k symbols/sec. The data rate is 20 kbps at 868 MHz and 40 kbps at 915 MHz. Data modulation is Binary Phase Shift Keying (BPSK) with differential encoding in the lower frequency spectrum. The radio is capable of transmitting at a minimum of power of -3dBm (501 µW) and has a receiver sensitivity of -85dBm at 2.4 GHz and -92dBm at 915 MHz. It has additional features such as Packet strength indication for location and routing, clear channel assessment for CSMA dynamic channel selection for co-existence [11], [12].

3.2 IEEE 802.15.4 MAC layer

The driving factors behind the development of the IEEE 802.15.4 Medium Access Control standard were the requirements of extremely low cost devices, ease of installation, reliable data transfer, short range operation and multi-year battery life. Target devices which are low power and low data rate have quickly adopted this standard for

medium access functions, as we see in the plethora of Zigbee devices that are available today.

The devices using this protocol have been classified into two broad categories of Fully Functional Device (FFD) and Reduced Functional Device (RFD). FFDs can form the network in any topology, can function as Personal Area Network (PAN) coordinators and typically implement the complete protocol set. RFDs can be a part of a star topology or join as an end-device or a leaf node in a peer to peer mesh network. They cannot function as PAN coordinators and typically implement a reduced protocol set. Figure 3.1 illustrates FFDs and RFDs in typical IEEE 802.15.4 personal area networks [13].
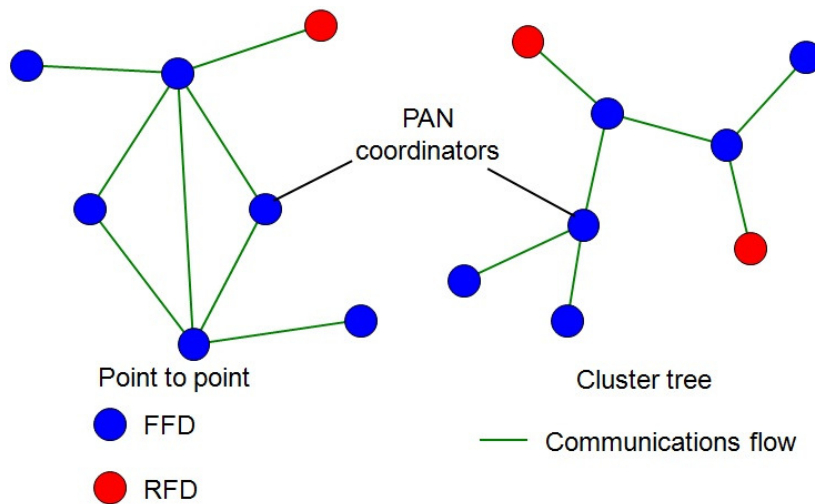
Figure 3.1: FFDs and RFDs in a PAN

The data services specified in the protocol, have acknowledged as well as unacknowledged messages. The maximum size of each MAC frame in this standard is 102 bytes. In addition, the standard provides management services for the upper network

19

layer by providing node notifications, network scanning and network synchronization [14].

3.3 Wireless Environment for Smart Utility Networks

The wireless environment places fundamental limitations on the performance of communication networks based on radio frequencies. The path between a pair of transmitter and receiver can vary between plain line of sight to tall buildings, forest area and mountainous terrain. These variations in geographical topology have given rise to the challenging problems of signal fading due to path loss and fitting of complex signal propagation models based on statistical data. In addition, the wireless channel is plagued by the ubiquitous problem of interference from a variety of sources ranging from cosmic background noise, to the electromagnetic noise generated by the household microwave. Even though there is a big corpus of theoretical results and experimental measurements for wireless communication in general, they tend to practically affect areas with more commercial impact such as cellular communication. The wireless mesh networks and wireless sensor networks have not gained as much from the modeling advances of wireless communication [15].

In Smart utility networks and the AMI, the wireless environment varies from indoor for home automation application to outdoor and industrial, highly noisy conditions. One important aspect of this wireless channel modeling is to estimate the average path loss between two nodes, or in general, two points in space. For smart utility networks, where the separation of nodes is from a couple of meters to a hundred meters,

the lognormal shadowing model has been shown to give accurate estimates for average path loss. Equation 3.1 returns path loss in dB as a function of the distance between two nodes and a few adjustable parameters.

$$PL(d) = PL(d_0) + 10.\eta.\log\left(\frac{d}{d_0}\right) + X_\sigma \qquad (3.1)$$

PL (d) is the path loss at distance **d**, *PL (d0)* is the known path loss at a reference distance *d0*, *η* is the path loss exponent, and $\mathbf{X_\sigma}$ is a Gaussian zero-mean random variable with standard deviation *σ.*

Another very important aspect of the wireless channel is the temporal variation of channel quality. This is especially pronounced in rapidly changing environments as those experienced in a smart utility network. Figure 3.2 shows a typical profile of channel variation. Notice the sharp drops (measured up to -50dB) and that most of the time the channel is below the average path loss (0dB). There are several theoretical models to describe temporal variation, taking their names from corresponding complex distributions (e.g., Rayleigh, Weibull, Nakagami, Gamma and lognormal) [15].
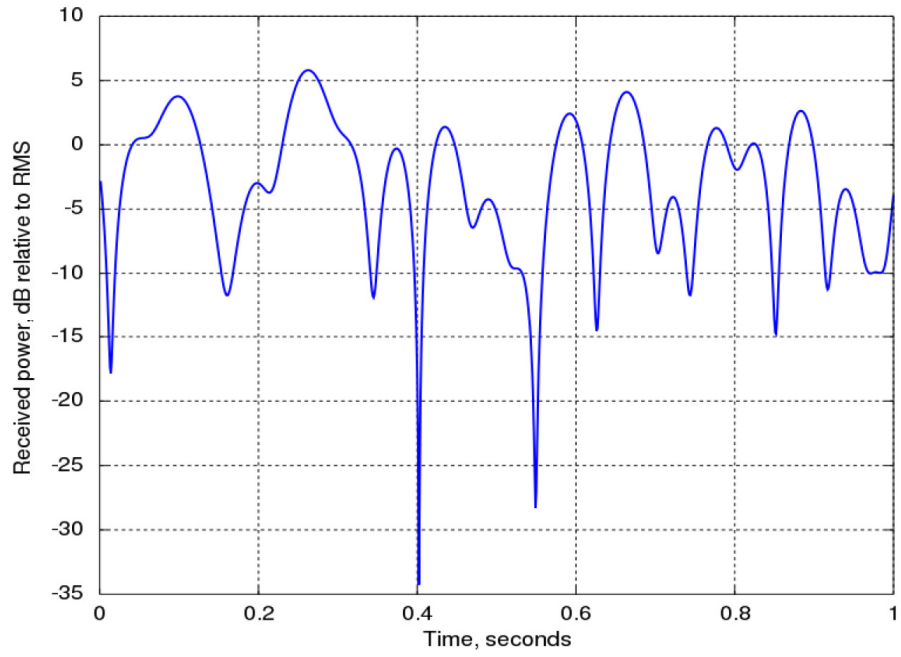
Figure 3.2: Temporal fading in a wireless channel

Chapter 4

Routing Protocols

Smart utility networks comprising of wireless meters for electricity, water and gas can be considered as wireless sensor networks. Routing in wireless sensor networks has been extensively studied in the literature. Several protocols have been proposed among which AODV and DSR are some of the widely used ones for wireless sensor networks. Routing protocols are broadly classified into Distance-Vector routing and Link-state routing based on the network information used in their algorithm to find the next hop node or communication link for routing the data packet to the destination in the most efficient manner. Distance vector routing protocols use weights to represent communication links, whereas link state routing considers the network state of each communication link for its routing algorithm.

These protocols rely on formation of a directed graph based on the network topology. The nodes in the network are represented by vertices and the communication link between two or more nodes as edges on a graph. They may or may not consider the condition of cyclic edges, which translates to a loop in the communication link. The edges are assigned weights which generally represent the distance from one node to another. The weights may also represent network conditions such as delay, hop count, link quality and congestion. These weights are used by the routing protocols to make

packet routing decisions based on an optimization algorithm, specific to the protocol. Thus specific routing protocols are designed to optimize specific weights. This translates to a routing protocol that functions optimally for one target application and does not for the other. In a smart utility network and AMI systems, the criteria for performing routing decisions vary considerably. It is a heterogeneous, hierarchical network architecture in which devices can vary from high power, high capacity to severely constrained nodes. In such a network, in which all devices run the same routing protocol, several metrics must be used for optimizing the routing algorithm [16], [17].

4.1 Routing Requirements

In order for the smart utility network to function as designed for its application, an efficient routing protocol is imperative. A single routing protocol is designed with target applications, according to which the routing algorithm optimizes routes and controls network functions. The requirements for routing in a smart utility network are diverse, as it has to be compatible for a wide range of devices, from home appliances to metering devices to collectors. Routing Protocols designed for the smart utility networks have to adhere to the requirements spelled out in [RFC5826], [RFC5673], [RFC5548] and [RFC5867] which are home automation routing, industrial routing, urban routing environments and in-building routing requirements respectively.

The nodes participating in these networks are low power devices and have severe constraints in terms of CPU power, memory, battery and operating environments. Utility meters are designed to last for approximately 20 years on battery. Due to these constraints, restrictions are placed on routing requirements. For Home automation

applications, the duty cycle of devices is less than 1% and the convergence time for the protocol is 500 milliseconds [18], [19], [20], [21].

The routing protocol has to perform device aware routing, and must avoid battery constrained devices or devices under strain for frequent routing of packets. For industrial automation applications, more focus is on the reliability which has to be as close to 100% as possible. Reliability is measured by the number of successful transmissions over number of attempts in a given period of time. Also, a zero configuration network is necessary when new devices enter or leave the network.

The most important requirement for routing protocols in a smart utility network is inter-operability. The entire smart grid and hence the smart utility network must adhere to inter-operability standards specified by NIST in its Smart grid inter-operability model document [2].

4.2 Non-standard routing protocols

Routing protocols developed for wireless sensor networks such as DSR and AODV have specific applications as target and use a highly customized algorithm for routing based on routing metrics for that application. In a wide area, large scale network like the smart utility network, there are heterogeneous devices, manufactured by different vendors for a variety of clients such as utility companies and consumers. In this section, non-standard routing protocols and their mechanisms have been discussed in brief.

4.2.1 AODV

Ad-hoc On-demand Distance Vector Routing (AODV) protocol was developed primarily for an ad-hoc network which is the cooperative engagement of a collection of mobile nodes without the required intervention of any centralized access point or existing infrastructure. Networks using AODV have the property of dynamic self-start and do not require any network management for communication.

Although AODV does not depend specially on particular aspects of the physical medium across which packets are disseminated, its development has been largely motivated by limited range broadcast media such as those utilized by infrared or radio frequency wireless communications adapters. AODV over IEEE 802.11 standards is very popular and has been widely studied in the literature. The AODV algorithms primary objectives are:

- To broadcast route discovery packets only when necessary

- To distinguish between local connectivity management , neighborhood detection and general topology maintenance

- To disseminate information about changes in local connectivity to those neighboring mobile nodes that are likely to need the information

AODV uses a broadcast route discovery mechanism. It relies on dynamically establishing route table entries at intermediate nodes. The Path Discovery process is initiated whenever a source node needs to communicate with another node for which it has no routing information in its table. Every node maintains two separate counters, a node sequence number and a broadcast id. The source node initiates a path discovery by broad-

casting a route request (RREQ) packet to all of its neighbors. The RREQ contains the path traversed until it reaches the destination. Eventually, a reverse route stack is entered and sent back to the source. This is done using a route reply (RREP) message. As the RREP travels back to the source, each node along the path sets up a forward pointer to the node from which the RREP came and updates its timeout information for route entries to the source and destination and records the latest destination sequence number for the requested destination [22].

Figure 4.1 represents the reverse path setup and forward path setup as the RREQ and RREP travel from the source S to destination D and vice-versa respectively.
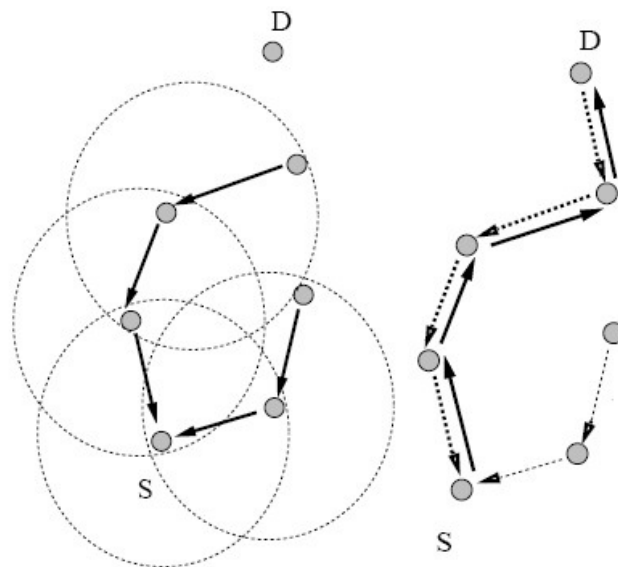

Figure 4.1: Reverse and Forward route formation in AODV

4.2.2 DSR

The Dynamic Source Routing protocol (DSR) is a routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for

any existing network infrastructure or administration. The protocol is composed of the two mechanisms of Route Discovery and Route Maintenance, which work together to allow nodes to discover and maintain source routes to arbitrary destinations in the ad hoc network. The use of source routing allows packet routing to be loop-free, avoids the need for up-to-date routing information in the intermediate nodes through which packets are forwarded, and allows nodes forwarding or overhearing packets to cache the routing information in them for their own future use. All aspects of the protocol operate entirely on-demand, allowing the routing packet overhead to scale automatically to only that needed to react to changes in the routes currently in use. DSR can support very rapid rates of arbitrary node mobility under the assumption that nodes do not continuously move so rapidly as to make the flooding of every individual data packet the only possible routing protocol.

The DSR protocol is composed of two mechanisms that work together to allow the discovery and maintenance of source routes in the ad hoc network:

- Route Discovery is the mechanism by which a node S wishing to send a packet to a destination node D obtains a source route to D. Route Discovery is used only when S attempts to send a packet to D and does not already know a route to D.

- Route Maintenance is the mechanism by which node S is able to detect, while using a source route to D, if the network topology has changed such that it can no longer use its route to D because a link along the route no longer works. When Route Maintenance indicates a source route is broken, S can attempt to use any other route it happens to know to D, or can invoke Route Discovery again to find

28

a new route. Route Maintenance is used only when S is actually sending packets to D.

Route Discovery and Route Maintenance each operate entirely on demand. In particular, unlike other protocols, DSR requires no periodic packets of any kind at any level within the network. For example, DSR does not use any periodic routing advertisement, link status sensing, or neighbor detection packets, and does not rely on these functions from any underlying protocols in the network. This entirely on-demand behavior and lack of periodic activity allows the number of overhead packets caused by DSR to scale all the way down to zero, when all nodes are approximately stationary with respect to each other and all routes needed for current communication have already been discovered. As nodes begin to move more or as communication patterns change, the routing packet overhead of DSR automatically scales to only that needed to track the routes currently in use. Similar to AODV, DSR also uses RREQ and RREP as route discovery packets [23]. Figure 4.2 shows the route discovery mechanism from source A to destination E with the route discovery id as 2.
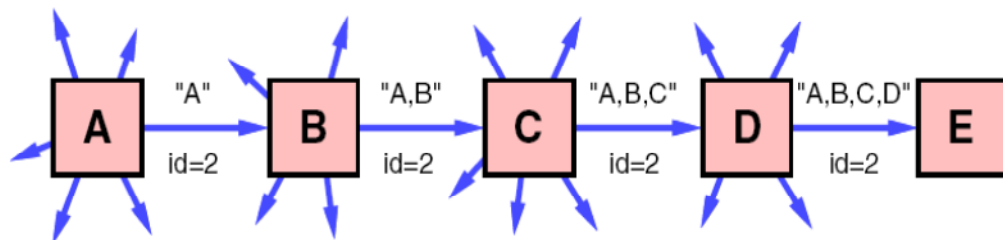

Figure 4.2: Route discovery in DSR protocol

4.2.3 Geographical Routing

Geographical Routing is a distance vector routing protocol which adopts a combination of weighted link metrics and geographical proximity to route data packets. Geographical routing has a multitude of implementation flavors and mechanisms to build routes in the network. This protocol supports peer to peer communication by employing a routing scheme which utilizes the geographical coordinates (latitude and longitude) of the communicating nodes.

During commissioning, nodes are automatically provided with the geographical coordinates of the target or destination for their upstream communication whilst the collector knows the coordinates of target meters for downstream communications. In each case the transmitting node discovers the geographical coordinates of its neighboring nodes and is therefore able to select a neighbor which is geographically closest to the final destination node. Thus the communication path will have the minimum number of hops ensuring the lowest latency. Should a node be identified as a neighbor during upstream communication, it will be chosen regardless of any other nodes due to the router's ability to transmit data at a higher speed directly towards the destination via the communication highway. The typical latency achieved using this approach is approx. 5–8 seconds for a round trip from destination node to any other node, depending on the number of hops. The maximum number of hops a packet is allowed to survive is configurable. In addition a time to live mechanism is incorporated so packets are not repeatedly retried. This routing scheme needs to compute the next hop based on a pre-determined algorithm from a list of nodes designated as neighbors [24].

The computation is based on geographical distance, i.e. the node closest to the destination among the neighbor list. Packets are routed from source S to destination D as shown in Figure 4.3. In the figure 4.3, nodes are placed on a grid with x and y axis representing their geographic coordinates in two dimensions. Figure 4.4 shows the greedy method used by geographical routing to forward packets to the destination based on geographical distance alone.
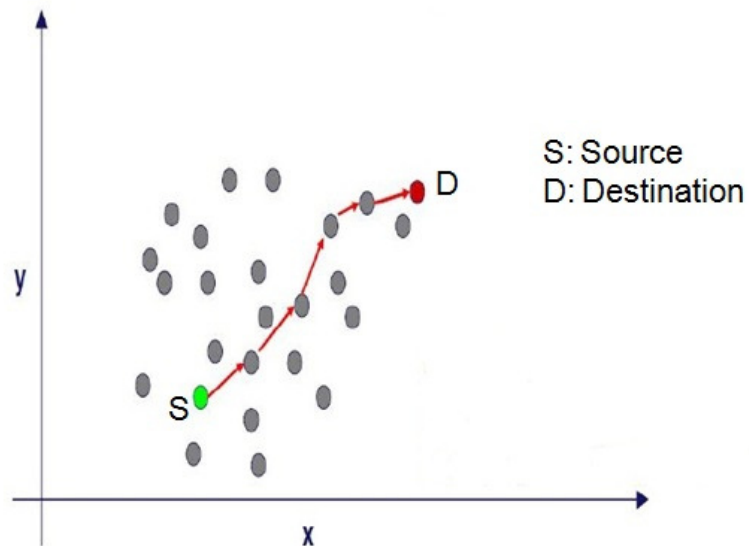
Figure 4.3: Forwarding in geographical routing

While geographic routing performs well in most cases where the route is available and has high reliability, there are several cases in which geographical routing tends to fail at a local minimum. In such cases where the route hits dead-end, remedial schemes like face routing or following a right-hand rule to re-route the packets is necessary. Figure 4.5 illustrates one such case in which the geographical routing protocol encounters a local

minimum and is unable to find the next hop node.
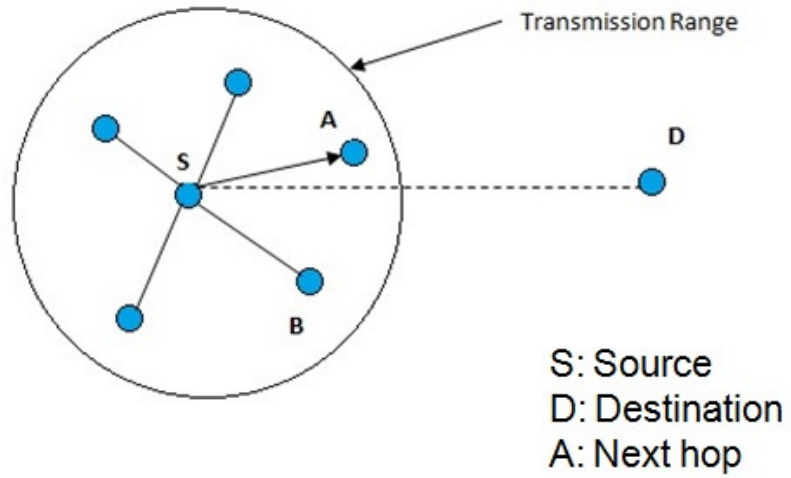
Figure 4.4: Greedy forwarding in geographical routing
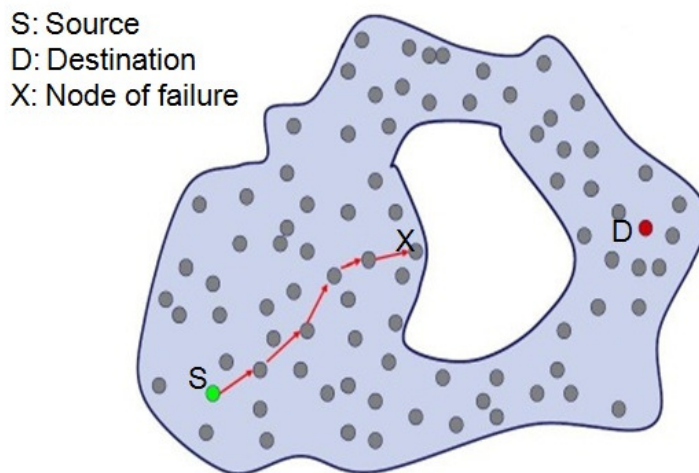
Figure 4.5: Forwarding failure in geographical routing

4.3 Routing Protocols for Smart Utility Networks

It can be seen that AODV, DSR and Geographical routing protocols described in sections above are routing protocols designed for wireless mesh networks are highly specific in optimizing metrics, in route discovery mechanism and forwarding algorithms. None of these protocols are standards and are implemented for target applications by customizing aspects of each protocol. In order for these protocols to work for smart utility networks, in which devices are heterogeneous and vary in capacity and constraints, they have to inter-operable. Over the last decade, Internet Protocol (IP) based routing protocols have proven to be fairly interoperable and similar protocols are used in practice in the core internet as well as the perimeter internet devices such as commercial routers developed by a large number of vendors.

### 4.3.1 Need for an IPv6 based Standard Routing Protocol

Current internet routing standards are based on IP version 4 (IPv4) which allows a maximum of 2^{32} unique addresses for nodes, of which a large block are reserved for special uses and are unavailable for public domain addressing. Even with classful network addressing and subnet addressing, the address space is quickly running out and is believed to have already run out in some parts of the world. The Smart Utility network can potentially add over 2 billion new devices to the network. In order to support addressing each of these devices, migration of smart utility routing protocols to IP version 6 (IPv6), which allows a maximum of 2^{128} unique addresses. Since the mainstream internet will migrate to IPv6, it will be fully interoperable with all networked

systems, globally. The Internet Engineering Task Force (IETF) has a working group called IETF-ROLL (Routing Over Low power and Lossy networks) for this very purpose and is tasked with developing a new routing protocol for target networks such as the smart utility network [25].

4.3.2 RPL

Routing Protocol for LLNs (Low power and Lossy Networks) or RPL is an IPv6 distance vector routing protocol designed by the IETF-ROLL group considering the requirements spelled out in [RFC5826], [RFC5673], [RFC5548] and [RFC5867] which are home automation routing, industrial routing, urban LLNs and in-building routing requirements respectively. In concept, RPL is a form of gradient routing, which has shown to be robust and relatively immune to topological changes.

The routing protocols that exist for wireless sensor networks do not find applicability in smart utility networks as the routing metrics used by these protocols are highly application specific. RPL, an IPv6 routing protocol has been developed for a variety of applications and is on its way to becoming a routing standard for smart utility networks. RPL is a graph building based routing protocol and specifies the mechanisms for construction of a Destination Oriented Directed Acyclic Graph (DODAG) using an objective-function. The objective function operates on a combination of metrics and constraints to compute the best path for routing data packets to the destination [26].

4.3.3 RPL mechanisms and metrics

The core of RPL is the mechanism to maintain the network state information such as connectivity and degree of connectivity of each node using multiple DODAGs, each having unique objective functions which optimize paths based on multiple metrics and constraints. The root of a DODAG in RPL is characterized by zero outgoing edges and is typically called an LBR (LLN Border Router).

The root is a gateway device in smart utility network connecting the mesh network to head-end systems. All edges in the DODAG are contained in paths oriented toward and terminating at one root node. The DODAG root initiates the construction of the directed acyclic graph by transmitting a DODAG Information object.

This control message is propagated down the network in order to build the graph. Some of the multiple functions performed by DIO messages are:

- Identify the DAG as originating from a particular DAG root.

- Propagate rank information of the node initiating it and a parameter called minimum rank increase, used for the recipient of the DIO in order to compute its own rank.

- Define the Objective Function (OF) which specifies the metric or a combination of metrics used to compute rank at each node.

After receiving multiple DIO messages, a node will compute its own rank and determine its position in the DAG with respect to other nodes.
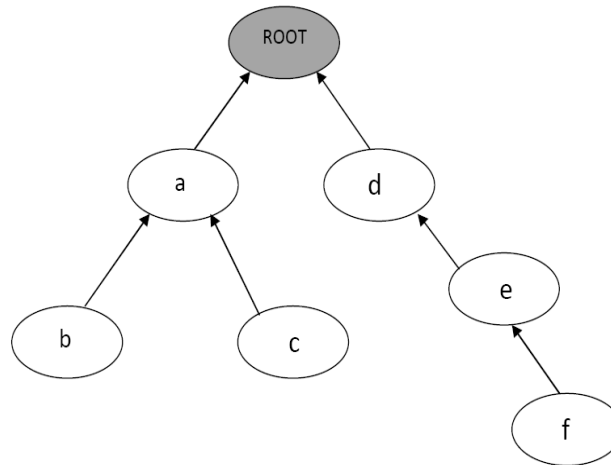
Figure 4.6: RPL instance containing a DODAG

Figure 4.6 illustrates an RPL instance after formation of the DODAG. The objective function dictates some rules to form the DODAG. Besides providing flows from the leaf towards the root, RPL also creates routes in the opposite or down direction. This requires a routing state to be built at every node and a mechanism to populate these routes. This is accomplished by the DAO (Destination Advertisement Object) message. DAO messages are used to advertise prefix reach-ability towards the leaf nodes in support of the down traffic.

RPL also supports point-to-point (P2P) communication from any node to any other node in the graph. When a node sends a packet to another node within the LLN network, the packet travels up to a common ancestor at which point it is forwarded in the down direction to the destination. A majority of routing protocols use periodic messages on the control plane in order to maintain adjacency and keep routing tables updated. This

mechanism would particularly be costly in LLNs where resources are scarce and nodes are highly constrained. An adaptive timer mechanism called the trickle timer is at the core of the RPL control plane. This mechanism controls the sending rate of DIO messages in order to avoid frequent topology changes due to re-structuring of the graph. As the network becomes stable, the number of RPL control messages decrease. When an inconsistency is detected (such as a loop or a change in the DODAG parameters) a local repair is issued by the node detecting the inconsistency and the trickle timer is reset to quickly fix the issue. In the worst case, a global repair is issued where the graph is built all over, starting with the root. A new version of the DODAG is created whenever a global repair process is initiated.

A brief description of the implementation of RPL used for the performance analysis of the routing protocol specific to smart utility networks is provided herein. In this case, an electric metering network is considered where an electricity meter constitutes a node in the AMI. A multi-hop wireless AMI network is considered for the analysis that comprises of 500 nodes that make up metering devices and one collection device that serves as the root. The routing protocol builds and maintains one DAG structure rooted at the collection device. Since RPL is designed to optimally perform for multipoint-to-point traffic flows, the implementation omits DAO objects used for point-to-multipoint traffic flows.

The DIO implementation is essential for the construction of the DAG and is sufficient for the performance analysis of RPL. Every node in the AMI network is assigned a node ID, which for example can be the IPv6 address of the node. The root of

the network is given an ID of 0 to mark it as the sink. Minimum values indicative of network state are stored at each node. The node may be subject to various constraints, memory availability being one of them. The following information is stored at each meter node:

- Current rank of the node

- Ordered list of parents' node ID

- Node ID of preferred parent

- Destination ID of sink (0 in this case).

Each entry of the parent list includes:

- Node ID of the parent,

- Rank of the parent node, and

- Link metric ETX from itself to each parent.

The default parent is in the parent list of the node and has the lowest rank among all the nodes in the parent list. There is no network information stored at the root node or the sink, since there is no traffic originating from it. RPL specifies forwarding rules that are similar to any other routing protocol. Once the routing table, consisting of the parent list and the preferred parent has been established through the construction of the DAG, the forwarding rules govern the flow of packets from the nodes to the root. A meter node that generates or receives a data packet destined for the root should forward this packet to its default parent. The packet should be dropped if the node does not have a default parent. The ETX statistic can be considered for switching to another parent from the parent list after sufficient number of attempts. Building of the DAG is the foremost step in RPL and

rank computation is one of the key mechanisms in RPL for building the DAG. The rank of the root is a constant and is assumed to be 1.0 in this implementation. The packet success probability of each link k, denoted p_k is randomly assigned for each link to a parent. The metric ETX of link k, X (k) , is computed as the inverse of the packet success probability of each link.

$$X(k) = \frac{1}{p_k} \qquad (4.1)$$

The initial value of ETX of any link k is set to be 1.0. The ETX is updated and calculated from Equation 4.1 from a randomized set of packet success probability values when a DIO is received by a node from a parent. Hence, the ETX value of each link keeps changing over time. This introduces the temporal nature of link characteristics observed in LLNs. The rank is computed based on the updated ETX count and is transmitted in the DIO. The receiving node calculates its own rank from the rank contained in the DIO according to equation 4.2. Here, R_i is the rank of the node receiving the DIO and R_k is the rank of the node transmitting the DIO.

$$R_i = floor\left(\frac{R_k}{\beta}\right) \qquad (4.2)$$

β is a constant which is specific to each DAG and represents the minimum rank increase parameter and *floor(α)* is the function that evaluates to the greatest integer less than or equal to α.

The computation of rank maintains the following relationship between any 2 nodes i and j:

- $R_i < R_j$ indicates i is closer to the root than j in the DAG and j can safely add i in its parent list.

- $R_j = R_i$ indicates both nodes i and j are in the same position in the DAG. In this case either of them assigning each other in the parent list can create loops, requiring reconstruction of the DAG.

- $R_i > R_j$ indicates that node i may be in the sub-DAG of j and if j adds i in its parent list, it can create loops. However, node i can safely add node j in its parent list.
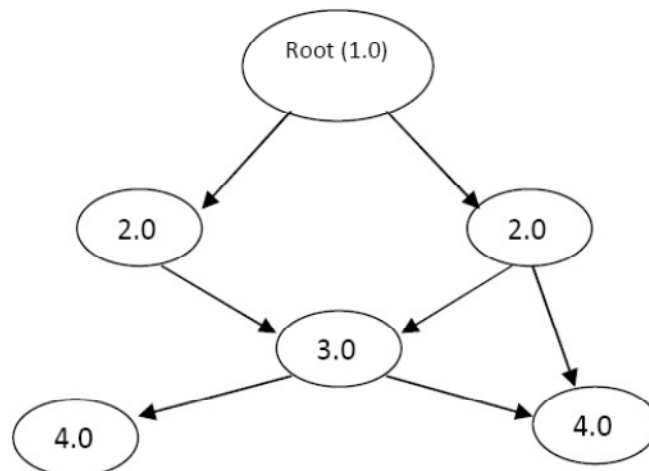

Figure 4.7: Illustration of rank computation using DIO

Figure 4.7 shows a possible DAG configuration with ranks of each node indicating their relative position in the DAG. The construction of the DAG, maintenance and node table population mechanisms in RPL can be summarized as follows. The root institutes DAG

construction by emitting a DIO message. The DIO includes information such as root node ID and its rank value. Any node that receives this initial DIO message adds the root to its parent list and computes its own rank by the rank computation equation (4.2) using link metric ETX calculated from equation (4.1). This node then originates a DIO and emits it further with its own rank. A node j already in the DAG, upon receiving a DIO message from a node i, should either discard the DIO, or modify and forward the DIO according to the following rules. A node will thus, always keep a position in the DAG by maintaining a parent list and adapting its rank value according to DIO messages from other nodes. The node will also notify other nodes with its own rank via DIO messages when needed and hence nodes will maintain a consistent and efficient DAG structure that provides routing support for any traffic generated from the nodes to the root [27].

4.4 Comparing RPL and Geographical Routing protocols

Two routing protocols designed for smart utility networks have been implemented in a discrete event simulator and their performance for a specific scenario of electricity meters forming a wireless mesh network as a part of an AMI and sending multi-point to point traffic sequentially has been evaluated herein.

RPL is a routing protocol under development by the IETF-ROLL group and is well on its way to becoming a standard. It constructs routing paths from the nodes to the central collection points based on the deployed architecture. It utilizes packet success probability and subsequently derives ETX as a metric to construct the routing paths. A multipoint-to-point RPL network for the specific scenario of electricity metering devices has been implemented and analyzed for performance of this routing protocol.

Geographical routing, also a distance vector routing protocol is based on computation of geographical distance between source, destination and nearest next hop node. Although proprietary, this protocol has proven to be scalable as it has been deployed in large scale networks comprising of more than 2 million metering end-points and network devices with collectors reporting data to utility head-end systems.

Chapter 5

Performance Analysis

In order to compare the performance of the wireless mesh routing protocols a simulation setup was developed using the discrete event simulator OMNeT++ and the wireless sensor network framework Castalia. The 802.15.4 MAC/PHY modules provided with the Castalia framework were used as lower layers under the routing layers of RPL and Geographical routing developed at a conceptual level for this performance analysis. As Castalia was developed for BANs (Body Area Networks) it included temporal channel variation and fading models which were close to real world low power and lossy networks. These models made Castalia a right choice over other frameworks available for wireless sensor network simulations. Geographical routing protocol, although proprietary, has been widely deployed in smart utility networks and AMI systems and is currently the protocol running in over 2 million metering end-points. Hence, this was chosen for comparison of performance over RPL, which is still in developmental stage and has no known large scale deployments in North America.

5.1 Modeling with OMNeT++

OMNeT++ is an object-oriented modular discrete event network simulation framework. It has a generic architecture, so it can be used in various problem domains:

- Modeling of wired and wireless communication networks

- Protocol modeling

- Modeling of queuing networks

OMNeT++ itself is not a simulator of anything concrete, but rather provides a framework and tools for writing simulations. One of the fundamental ingredients of this infrastructure is component architecture for simulation models. Models are assembled from reusable components termed modules. OMNeT++ simulations can be run under various user interfaces. Graphical, animating user interfaces are highly useful for demonstration and debugging purposes, and command-line user interfaces are best for batch execution [28].

5.2 Castalia Framework

Castalia is the framework used with OMNeT++ in building and simulating the routing layers of RPL and Geographical routing with IEEE 802.15.4 MAC/PHY as lower layers [29]. Some of the features of Castalia used for building the simulation model are:

- Advanced channel model based on empirically measured data.

  – Model defines a map of path loss, not simply connections between nodes

  – Complex model for temporal variation of path loss

- Fully supports mobility of the nodes

- Interference is handled as received signal strength, not as a separate feature

- Advanced radio model based on real radios for low-power communication.

- Probability of reception based on Signal to Interference Noise Ratio (SINR), packet size, modulation type. PSK, FSK supported, custom modulation allowed by defining SNR-BER curve.

- Multiple TX power levels with individual node variations allowed

- States with different power consumption and delays switching between them

- Realistic modeling of RSSI and carrier sensing

Figure 5.1 shows the node composite module built with Castalia for use in simulations. In this module, the MAC and PHY is the IEEE 802.15.4 radio sub-module and the routing sub-module is built from RPL and Geographical routing.
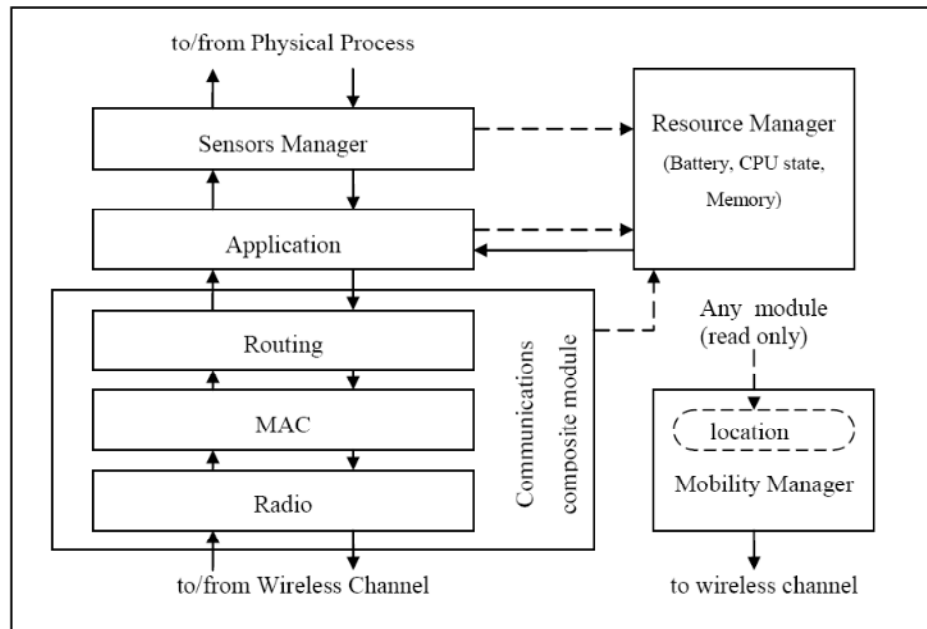

Figure 5.1: Composite node module in Castalia

5.3 Simulation Parameters

In this section, parameters used for simulation at each of the modules of PHY, MAC, Routing have been listed. The MAC/PHY parameters chosen herein are according to an RF chip based on IEEE 802.15.4 standards developed by Texas Instruments, CC2420 which is widely deployed in Zigbee enabled devices. These parameters try to mimic real world wireless conditions as closely as possible. Also, an application layer has been used in the simulations, which generates traffic to simulate a smart metering network. Typically, in legacy systems, packets are generated once every 30 days for electric billing systems. In the smart utility metering and AMI systems, the data thus generated is highly granular and is at the rate of a packet every few seconds [29].

5.3.1 PHY layer parameters

Physical layer parameters used for simulating each node in the smart utility network is given in table 5.1. These parameters are specified as options in the IEEE 802.15.4 standard and are modeled by Castalia.

Table 5.1: IEEE 802.15.4 PHY parameters

Parameter	Value
Radio Data Rate	250 kbps
Modulation Scheme	Frequency Shift Keying (FSK)
Bandwidth	2 MHz
Receiver Sensitivity	-95dBm
Transmission Power	20dBm
Operating Frequency	900 MHz

5.3.2 MAC layer parameters

A standard 802.15.4 MAC layer model was used for this simulation. The data rate to match the radio was set at 250 kbps. The MAC layer used slotted Carrier Sense Multiple Access (CSMA) as a method for channel access and Collision Avoidance (CA) as a method to minimize collision of packets. In addition, the MAC layer of each module contains a parameter isFFD. It indicates if a node is a Fully Functional Device (FFD) or a Reduced Functional Device (RFD). This parameter is set true for only 1 node in the entire network which is the Collector node in the network. For all other nodes, this parameter is set to False and by default others are RFDs.

5.3.3 Wireless Medium parameters

The wireless module has configurable parameters for the lognormal shadowing module and a parameter to turn the temporal fading model on or off. In all simulations of RPL and Geographical routing, the temporal fading model is on. The temporal fading model is provided by Castalia according to statistical data gathered from wireless channel experiments. The parameters used for modeling the wireless channel for smart utility networks have been listed in table 5.2.

Table 5.2: Wireless environment parameters

Parameter	Value
Path loss at distance of d_0	60dB
Reference distance d_0	1m
Path Loss Exponent (β)	2.7
Standard Deviation of Gaussian distribution (σ)	4.0

5.4 Validation of Simulation Models

In order to analyze multiple routing protocols, the underlying link layer, physical layer and the channel conditions have to be optimized according to the network topology in use and the environment in which such networks are deployed. The choice of IEEE 802.15.4 MAC/PHY standards for such networks is optimal as it is similar to the future standard 802.15.4g for Neighborhood Area Networks. This standard is a likely candidate for deployment in smart utility networks and has been adopted by the Zigbee Alliance for home automation networks.

With the aim of quickly validating the link layer model for analysis of the routing protocols, packet success probability rates were gathered from a 400 node real network comprising of smart meters and network devices. The packet success probability distribution in the network was obtained as shown in Figure 5.2. These values represent the real world channel characteristics reflected in the packet success probabilities at the link layer.
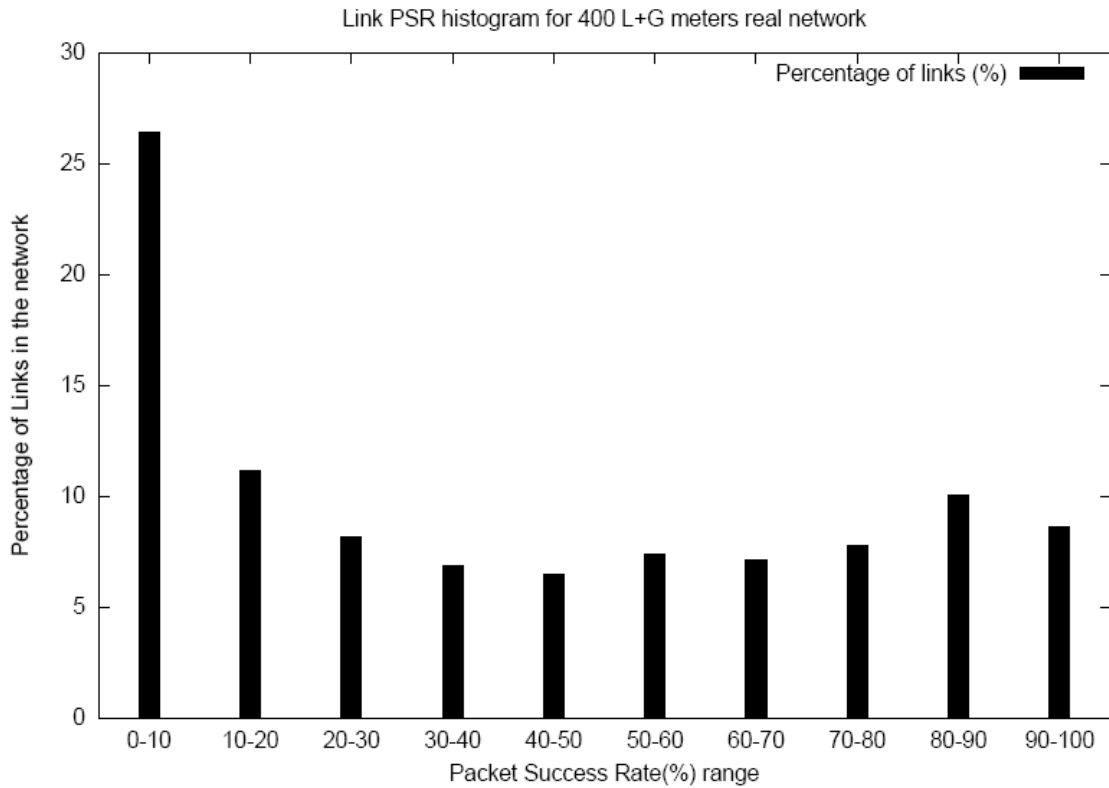
Figure 5.2: Packet Success Rate Histogram for Validation

After having computed the packet success probability distribution for a 400 node real network for comparison, a simulation experiment was conducted to determine the packet success probability yielded by the simulator's link, physical and channel models. This was done for a 100 node subset derived from a large rurally deployed real network. This experiment set each node to broadcast a total of 100 packets in a sequential order. The received packets were counted and the source was recorded. The computed ratio of total transmitted packets to those received by each node was collected as the link packet success probability. The packet success probability values obtained from the experiment were used to plot the connectivity map of the nodes with the collector.

Figure 5.3 shows the topology of the 100 node network used for the experiment and all the possible links between nodes. The nodes with links to the collector in figure 5.3, have a packet success rate of more than 60%. The values obtained from the experiment with the 100 node network and the on-field data from the 400 node network showed a fair correlation in packet success probability. This experiment quickly validated the simulation model for IEEE 802.15.4 MAC/PHY to be yielding link characteristics similar to those obtained from field measurements. This validation allowed the use of the IEEE 802.15.4 MAC/PHY simulation models to be used under the two routing layers of RPL and Geographical routing for performance analysis.
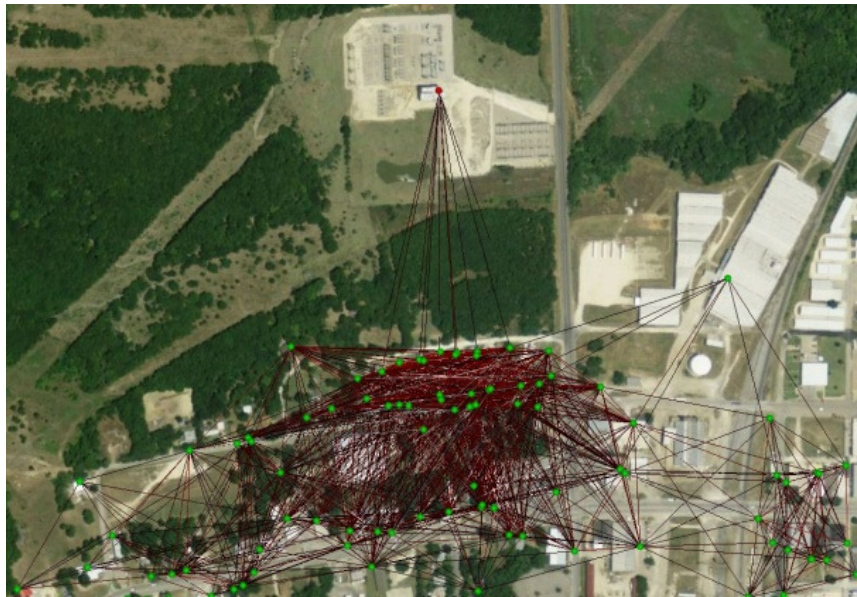

Figure 5.3: Plot of links with PSR greater than 60% in the network

Chapter 6

Results

RPL was implemented to build the DODAG (Destination Oriented Directed Acyclic Graph) using ETX (Expected Transmission count) as the metric for rank computation. The packet success probability matrix was constructed for all the 500 nodes in the network and all possible links between every other node. This was done by collecting packet success probability values through the link layer tests for each link described in Chapter 4, section 4.3.3. The ETX value for the ith link was computed using the packet success probability p_i for that link using equation 4.1.

Geographical routing was modeled using a combination of ETX and geographical proximity to compute routes. Links with a packet success probability of more than 60% were selected as potential neighbor nodes for each node. The distance between each neighbor node and the destination (collector) were computed using the distance formula in equation (6.1). The node at (x', y') with the least distance (d) to the collector at (x, y) was used as the next hop node.

$$d = \sqrt{(x' - x)^2 + (y' - y)^2} \qquad (6.1)$$

Simulations of RPL and Geographical routing algorithms were run for the 500 node real network with the application layer running a test case for gathering the statistics of hop count and end to end delay.

The test case used for the performance analysis was constructed based on the scenario that each of the 500 nodes sends multi-point to point traffic directed towards the collector. The application packet rate was set at 1 packet/second. This was done sequentially to measure individual statistics. The sequential transmission of packets also ensured low number of collisions and minimal interference. All other nodes in the network simply participated in the routing and were not allowed to transmit when one of the nodes was transmitting. Each node transmitted 100 packets with the collector as the destination. The statistics were gathered at the collector, which kept a record of packet count, delay suffered by each packet, number of hops taken by each packet for every source that transmitted in the network. Figure 6.2 shows the hop count distribution in the 500 node real network for RPL versus Geographical routing protocol. A maximum of 7 hops was recorded for each of the routing protocols in the 500 node network. The plot shows that the distribution of hop count varies with the routing protocol as route selection varied based on the metrics used. RPL places a significant number of nodes at 1 hop distance from the collector while Geographical routing has the maximum number of nodes 3 hops away. Overall, RPL has an average hop-count of 2.3 hops while Geographical routing has an average of 2.6 hops. Figure 6.3 shows the delay histogram for the 500 node real network for RPL versus Geographical routing protocols. Overall, the packets recorded less delay with RPL as compared to Geographical routing. The plot

shows that on an average the packets suffered 160ms and 173ms of delay with RPL and Geographical routing.

Reliability statistics were also obtained for the 500 node network. Reliability is measured by computing the packet delivery ratio. Packet delivery ratio is Total number of received packets at the collector over Total number of packets transmitted by each node. On an average RPL showed a constant packet delivery ratio between 98% and 100% for each packet and an average of 99.98% while Geographical routing showed similar performance with an average of 99.30% as shown in Figure 6.1. Dead-ends in the route taken by packets routed using geographical routing is one of the causes for a drop in packet delivery ratio in certain nodes in the 500 node real network. Packet drops using RPL are caused due to unreliable links and subsequent inability of a node to re-join the graph by parent selection through a local repair mechanism.

In order to visualize the hop-count distribution in the network and understand how spatial distribution affects performance, a coded hop count map was generated for both Geographical routing and RPL as shown in Figure 6.4 and Figure 6.5 respectively. It verifies that for exactly the same geographic topology, RPL and Geographical routing produce a completely different network topology as is shown by the number of nodes n hops away from the collector, which is located at the center of the grid. Although RPL produces a topology with higher maximum rank, it optimizes ETX (Expected Transmission Count), while Geographic routing optimizes a combination of geographical distance and link quality. This affects the performance of both the routing protocols in terms of delay.
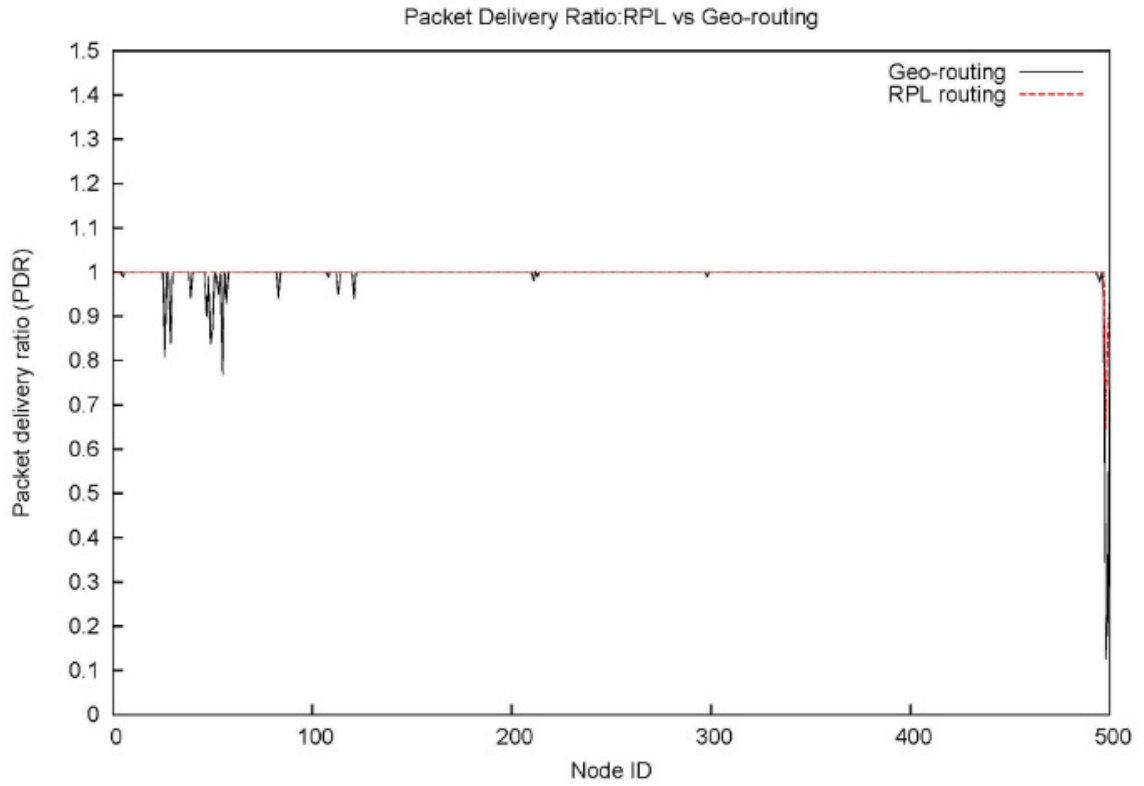
Figure 6.1: Packet delivery ratio: RPL vs. Geographical routing
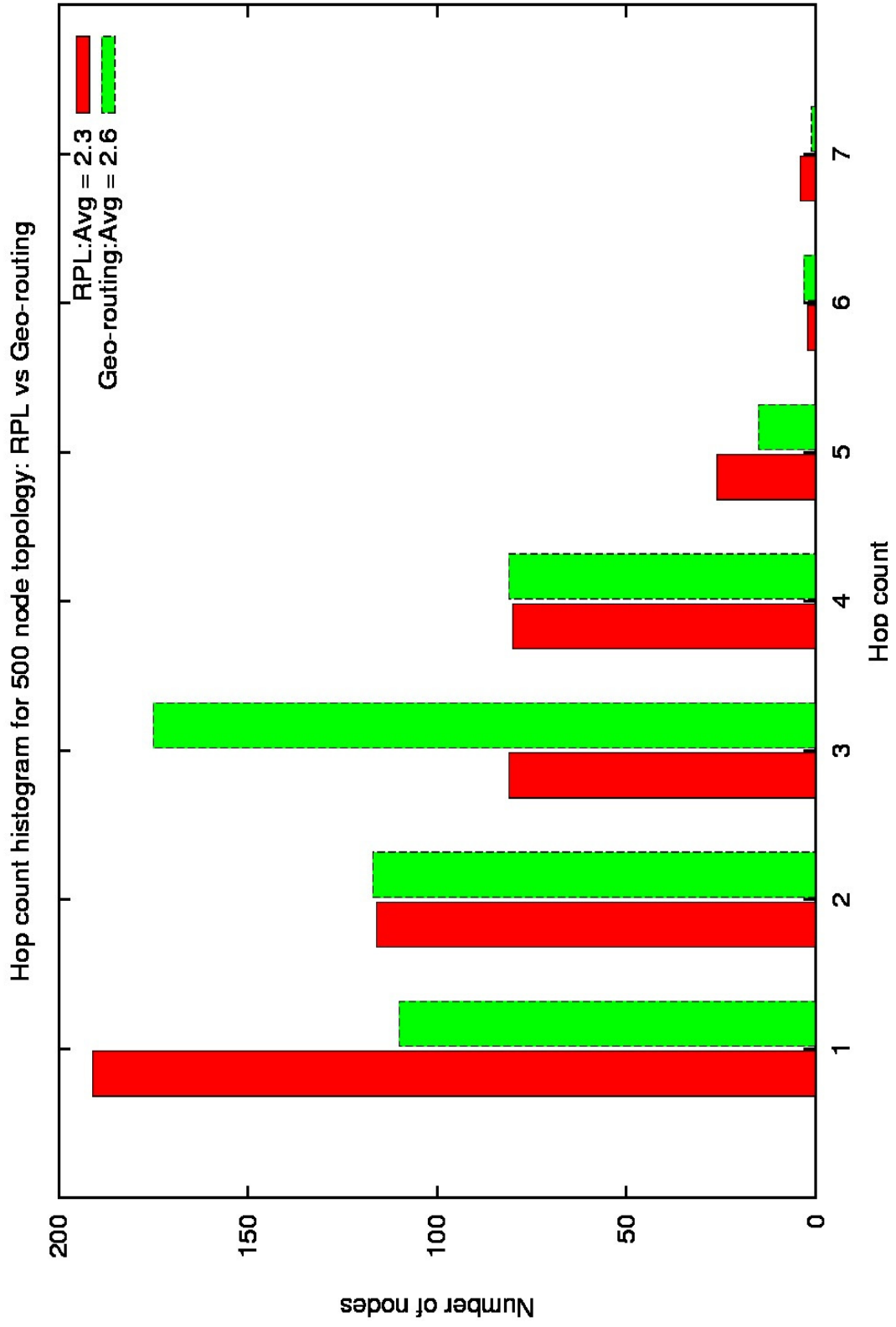
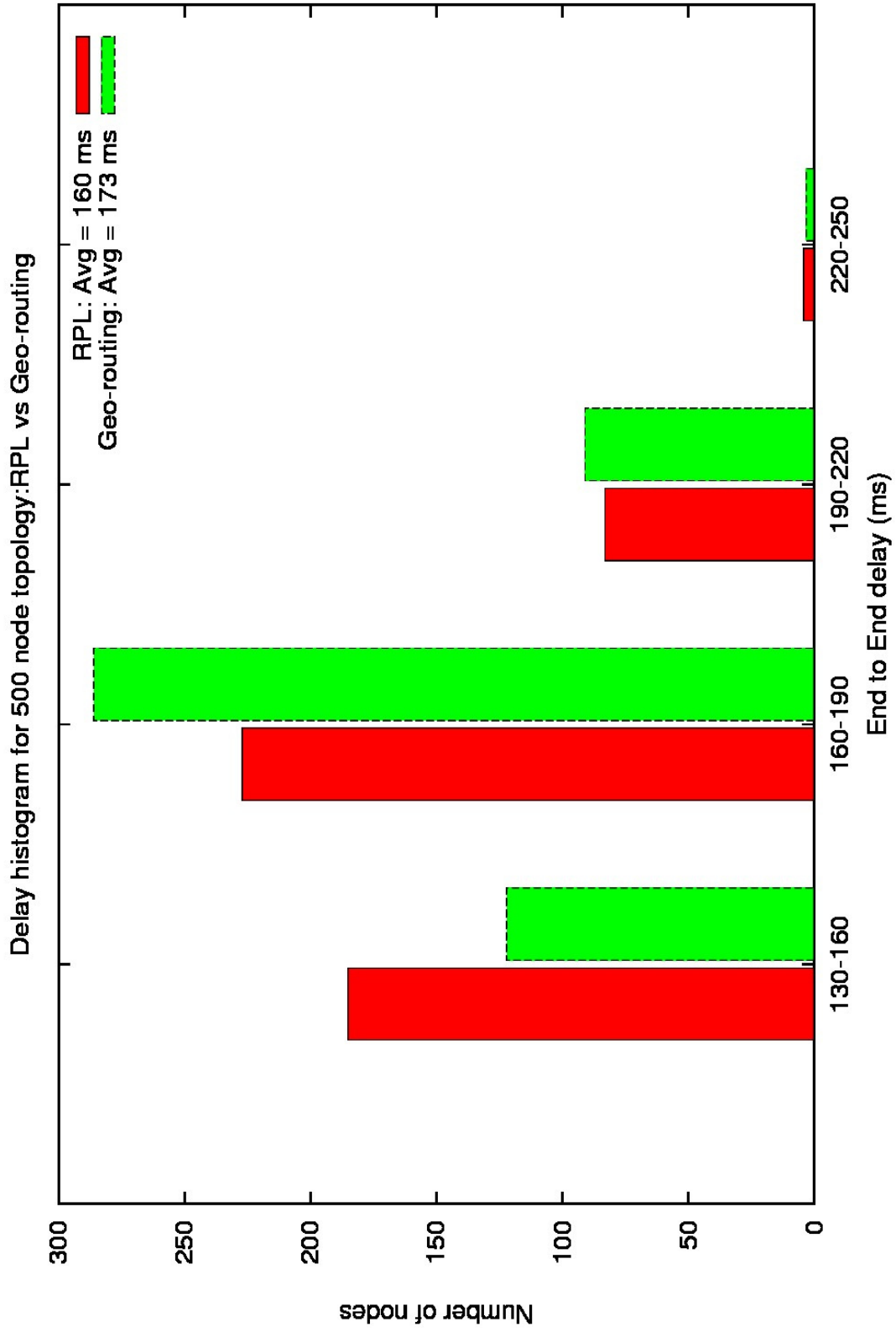Figure 6.2: Hop-count histogram for RPL vs. Geographical Routing

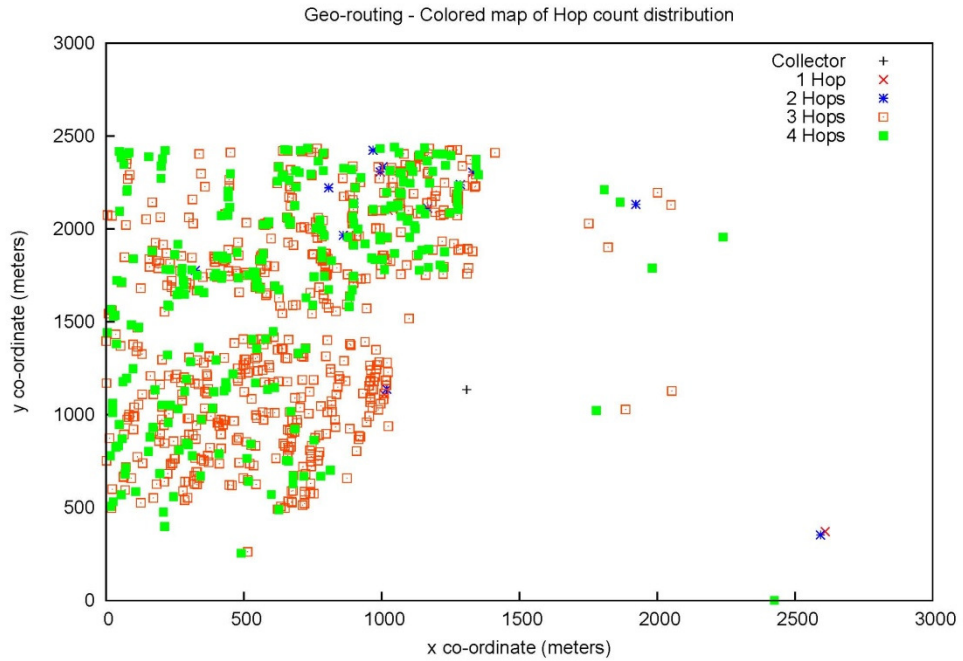Figure 6.3: Delay histogram for RPL vs. Geographical Routing

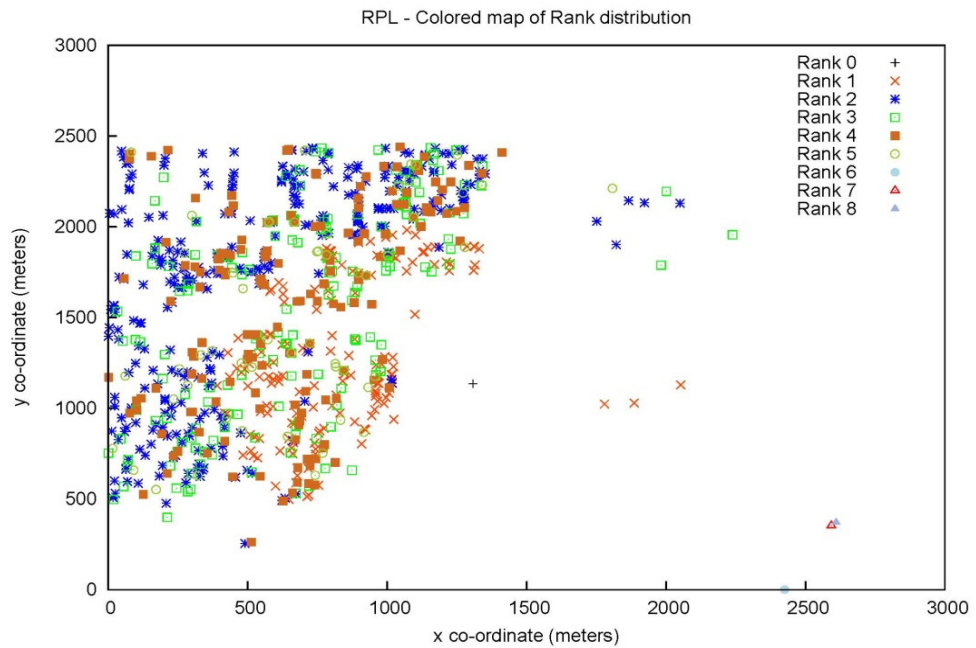**Figure 6.4: Hop-count map for Geographical routing**

Figure 6.5: Hop-count map for Geographical routing

57

Chapter 7

Conclusion

In this thesis, we gave a brief introduction to the existing archaic communication infrastructure for the power grid and described the Smart Grid initiative and the benefits that it will bring with an upgraded state-of-the-art communication infrastructure. Emphasis was laid on the success of the Smart Utility Network and the AMI systems, which are at the core of the smart grid. The type of radios that were used, based on IEEE 802.15.4 standards for MAC/PHY were described in brief. In further sections, the type of wireless environment, fading characteristics and temporal nature in which these radios operate was elucidated.

The hierarchical nature of the smart utility network architecture was studied and the formation of wireless mesh networks by smart metering end-points was illustrated. Three non-standard routing protocols for wireless mesh networks; AODV, DSR and Geographical routing were described and the need for an IPv6 based standard routing protocol was justified. The design criteria for such an over-arching routing protocol based on the requirements spelled in various RFCs which took into account home, industrial, in-building and outdoor routing conditions and metrics. The role of IETF in the development of a standard routing protocol and the routing protocol RPL was described. It's working mechanism and metric optimization was compared with Geographical

routing protocol. Further, two routing protocols, RPL and Geographical routing that are designed for smart utility networks have been modeled using a discrete event simulator OMNeT++ and Castalia framework. Their performance for a specific scenario of electricity meters forming a wireless mesh network as a part of an AMI and sending multi-point to point traffic sequentially was evaluated.

The statistics obtained from the simulation of the routing protocols yielded results which show that both wireless mesh routing protocols show similar performance for the given network size and traffic scenario. Thus, a clear conclusion on one protocol having advantages over the other in terms of network performance did not emerge out of the analysis of these results. Both RPL and Geographical routing are so far good contenders as efficient routing protocols for smart utility networks. RPL is most likely to emerge as the favored protocol as it is well on its way to becoming a standard. It constructs routing paths from the nodes to the central collection point based on the deployed architecture. We utilized packet success probability and subsequently derived ETX as a metric to construct the routing paths. We implemented a multipoint-to-point RPL network for the specific scenario of electricity metering devices and analyzed the performance of this routing protocol.

Geographical routing, although proprietary, has proven to be scalable as it has been deployed in large scale networks comprising of more than 2 million metering end-points and network devices with collectors reporting data to utility head-end systems.

Chapter 8

Future Work

RPL is an IPv6 based routing protocol designed for inter-operability as a requirement for smart-grid deployments. The choice of IPv6 is ideal for integration of such network with legacy computer networks ("Internet") for a variety of applications ranging from home-automation to grid-wide automation and data acquisition. Scalability in RPL has yet to be shown through analytical methods, simulations or on-field deployments as it is a protocol in development and has not been widely implemented. It still remains in the realms of research, development and open to improvements as actual results from field-tests emerge. Scalability in RPL according to the view of the author is strictly implementation specific. It depends on a multitude of factors ranging from the trickle timer [RFC 6206] parameters to the operating mode (storing or non-storing) in which nodes are deployed. Storing mode of RPL does involve each node to keep a record of the child nodes for downward traffic and a list of the ordered pair (destination prefix, preferred parent). In addition, the rank computation frequency is strictly dependent on the trickle timer mechanism. As control messages (DIO) are periodically generated governed by the trickle timer, the parameters of I_{min}, $I_{doubling}$ which determine the frequency of DIO messages will establish the rate at which the topology changes in relation to changes in the wireless network environment. It also remains to be seen how RPL will scale in terms

of storage requirements at the leaf nodes, which may need to store a large set of parents as a result of the tree span [30].

The storing mode of RPL may present a scaling complexity of $O\left(N\sqrt{N}\right)$ for a network of size N nodes. Geographical routing is shown to be scalable to N nodes in terms of storage complexity as $O(N)$ and $O(1)$ per node [31]. The issue of scalability remains to be addressed for RPL as there is no known wide scale smart utility network deployment using this routing protocol to measure performance. The future work will be to simulate RPL and Geographical routing for wireless mesh networks of size larger than 5000 nodes, a 10 fold increase in network size over the one used for this performance analysis, to measure performance and determine scalability of these two routing protocols for smart utility networks. In addition to increasing the scale of the network for simulations, rural, sub-urban and urban deployment scenarios showing variation in network density between sparse and highly dense will be used for performance analysis. In future, these results need to be compared with performance statistics gathered from on-field real networks to compare simulated results and actual results.

Bibliography

[1] Carl H. Hauser; David E. Bakken; Anjan Bose, "A Failure to Communicate," *Power and Energy Magazine, IEEE*, pp. 47-55, Mar-Apr, 2005.

[2] National Institute of Standards and Technology, "NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0," *U.S. Department of Commerce*, September 2009.

[3] Solution Brief, Motorola Inc."AMI and Beyond: How Wireless Broadband enables the Smart Grid Today and Tomorrow," 2009.

[4] Karnouskos S.; Terzidiz O.; Karnouskos P., "An Advanced Metering Infrastructure for Future Energy Networks," IEEE NTMS Conference, Paris, May 2007.

[5] B. Lichtensteiger; B. Bjelajac; C. Müller and C. Wietfeld, "RF Mesh Systems for Smart Metering: System Architecture and Performance," IEEE SmartGridComm, Maryland, October 2010.

[6] Iyer G.; Agrawal P.; Monnerie E.; Salazar R., "Performance Analysis of Wireless Mesh Routing Protocols for Smart Utility Networks," IEEE SmartGridComm, Brussels, October 2011.

[7] Iyer G.; Agrawal P., "Routing based on RPL for Smart Utility Networks," IEEE 12th ICDCN-SIPS, Workshop, Bangalore, January 2011.

[8] Zigbee Alliance, "Zigbee Specification,", October. 2010 https://docs.zigbee.org/zigbee-ocs/dcn/07-5299.pdf

[9] Zigbee Alliance, "Understanding Zigbee Gateway,", September 2010 http://www.zigbee.org/LearnMore/WhitePapers.aspx

[10] McGranaghan, M.; Von Dollen, D.; Myrda, P.; Gunther, E., "Utility experience with developing a smart grid roadmap," *IEEE Power and Energy Society General Meeting* - Conversion and Delivery of Electrical Energy in the 21st Century, 2008

[11] IEEE Task Group 4, "IEEE Std. 802.15.4-2003: Wireless PAN Physical Layer (PHY) Specifications," IEEE Press, Piscataway, NJ, 2003.

[12]   IEEE Task Group 4, "IEEE 802.15.4 Physical Layer (PHY) overview," https://mentor.ieee.org/802.15/file/04/15-04-0227-04-004a-ieee-802-15-4-phy-layer-and-implementation.ppt

[13]   IEEE Task Group 4, "IEEE Std. 802.15.4-2003: Wireless PAN Medium Access Control (MAC) Specifications," IEEE Press, Piscataway, NJ, 2003.

[14]   IEEE Task Group 4, "IEEE 802.15.4 Medium Access Control (MAC) overview," https://mentor.ieee.org/802.15/file/04/15-04-0218-01-004a-ieee802-15-4-mac-overview.ppt

[15]   Theodore S. Rappaport, "Wireless Communications: Principles and Practice," IEEE Press, Piscataway, NJ, 1996.

[16]   Ian. F. Akyildiz and Xudong Wang, "A Survey on Wireless Mesh Networks," *IEEE Communications Magazine*, vol. 43, Sept. 2005.

[17]   T. Watteyne; K.Pister; D. Barthel; M. Dohler; I. Auge-Blum, "Implementation of Gradient Routing in Wireless Sensor Networks," IEEE GLOBECOM, Hawaii, December 2009.

[18]   IETF document, "Home Automation Routing Requirements in Low power and Lossy Networks," [RFC 5826].

[19]   IETF document, "Industrial Routing Requirements in Low power and Lossy Networks," [RFC 5673].

[20]   IETF document, "Routing Requirements for Urban Low power and Lossy Networks," [RFC 5548].

[21]   IETF document, "Building Automation Routing Requirements in Low power and Lossy Networks," [RFC 5867].

[22]   C. E. Perkins; E. M. Royer; S. R. Das, "Ad Hoc On-Demand Distance Vector (AODV) Routing," IETF Mobile Ad Hoc Networks Working Group, IETF [RFC 3561].

[23]   D. B. Johnson; D. A. Maltz; Y-C Hu, "The Dynamic Source Routing Protocol for Mobile Ad hoc Networks (DSR)," IETF Mobile Ad Hoc Networks Working Group, Internet Draft, work in progress, 24 February 2003.

[24] Jain, R.; Puri, A.; Sengupta, R., "Geographical Routing Using Partial Information for Wireless Ad Hoc Networks," *IEEE Personal Communications*, vol.8, pp 48-57, Feb. 2001.

[25] D. Popa; N. Dejean; R. Salazar, "Applicability Statement for the Routing Protocol for Low power and Lossy Networks in AMI networks," Draft, IETF ROLL working group, 2011.

[26] P. Thubert, "RPL Objective Function Zero," Draft, IETF ROLL working group, 2011

[27] T.Winter; P. Thubert, "RPL: IPv6 Routing Protocol for Low Power and Lossy Networks," draft-ietf-roll-rpl-11, July 2010.

[28] A. Varga and R. Hornig, "An overview of the OMNeT++ simulation environment," Simutools 2008: 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops, ICST, Brussels, Belgium, 2008.

[29] Castalia Framework for OMNEST simulator, http://castalia.npc.nicta.com.au/

[30] P. Levis; T. Clausen; J. Hui, "The Trickle Algorithm," IETF ROLL working group, [RFC 6206]

[31] Young J. Kim; Ramesh G.; Brad K.; Scott S.; "Geographic Routing Made Practical," NSDI 2005, Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation, Vol. 2.