Enabling Communication and Networking Technologies for Smart Grid

Shravan Garlapati

Dissertation submitted to the Faculty of the

Virginia Polytechnic Institute and State University

in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Computer Engineering

Jeffrey H. Reed

Sandeep K. Shukla

R. Michael Buehrer

Virgilio Centeno

Christian Wernz

February 20, 2014

Blacksburg, Virginia

Keywords: Distance Relays, Hidden Failures, Blackouts, Agents, DFS, IEEE C37.118, Multiple Facility Location, AMI, Spread Spectrum, Markov Chain Analysis, Backward Recursive Dynamic Programming

Enabling Communication and Networking Technologies for Smart Grid

Shravan Garlapati

(ABSTRACT)

Transforming the aging electric grid to a smart grid is an active area of research in industry and the government. One of the main objectives of the smart grid is to improve the efficiency of power generation, transmission and distribution and also to improve the stability and the reliability of the grid. In order to achieve this, various processes involved in power generation, transmission, and distribution should be armed with advanced sensor technologies, computing, communication and networking capabilities to an unprecedented level. These high speed data transfer and computational abilities aid power system engineers to obtain wide area measurements, achieve better control of power system operations and improve the reliability of power supply and the efficiency of different power grid operations.

In the process of making the grid smarter, problems existing in traditional grid applications can be identified and solutions have to be developed to fix the identified issues. In this dissertation, two problems that aid power system engineers to meet the above mentioned smart grid's objective are researched. One problem is related to the distribution-side smart grid and the other one is a part of the transmission-side smart grid. Advanced Metering Infrastructure (AMI) is one of the important distribution-side smart grid applications. AMI is a technology where smart meters are installed at customer site which gives the utilities the ability to monitor and collect information related to the amount of electricity, water, and gas consumed by the user.

Many recent research studies suggested the use of 3G cellular CDMA2000 for AMI network as it provides an advanced and cost effective solution for smart grid communications. Taking into account both technical and non-technical factors such as extended lifetime, security, availability and control of the solution, Alliander, an electric utility in Netherlands deployed a private 3G CDMA2000 network for smart metering. Although 3G CDMA2000 satisfies the requirements of smart grid applications, an analysis on the use of the current state of the art 3G CDMA2000 for smart grid applications indicates that its usage results in high percentage of control overhead, high latency and high power consumption for data transfer. As a part of this dissertation, we proposed FLEX-MAC - a new Medium Access Control (MAC) protocol that reduces the latency and overhead in smart meter data collection when compared to 3G CDMA2000 MAC.

As mentioned above the second problem studied in this dissertation is related to the transmission-side grid. Power grid transmission and sub-transmission lines are generally protected by distance relays. After a thorough analysis of U.S. historical blackouts, North American Electric Reliability Council (NERC) has concluded that the hidden failure induced tripping of distance relays is responsible for 70% of the U.S. blackouts. As a part of this dissertation, agent based distance relaying protection scheme is proposed to improve the robustness of distance relays to hidden failures and thus reduce the probability of blackouts.

This dissertation has two major contributions. First, a hierarchically distributed non-intrusive Agent Aided Distance Relaying Protection Scheme (AADRPS) is proposed to improve the robustness of distance relays to hidden failures. The problem of adapting the

proposed AADRPS to a larger power system network consisting of thousands of buses is modeled as an integer linear programming multiple facility location optimization problem. Distance relaying protection scheme is a real time system and has stringent timing requirements. Therefore, in order to verify if the proposed AADRPS meets the timing requirements or not and also to check for deadlocks, verification models based on UPPAAL real time model checker are provided in this dissertation. So, the entire framework consisting of AADRPS that aids in increasing the robustness of distance relays and reducing the possibility of blackouts, the multiple facility location optimization models and the UPPAAL real time model checker verification models form one of the major contributions of this dissertation.

The second contribution is related to the MAC layer of AMI networks. In this dissertation, FLEX-MAC - a novel and flexible MAC protocol is proposed to reduce the overhead and latency in smart meter data collection. The novelty of the FLEX-MAC lies in its ability to change the mode of operation based on the type of the data being collected in a smart meter network. FLEX-MAC employs Frame and Channel Reserved (FCR) MAC or Frame Reserved and Random Channel (FRRC) MAC for scheduled data collection. Power outage data in an AMI network is considered as a random data . In a densely populated area, during an outage, a large number of smart meters attempt to report the outage, which significantly increases the Random Access CHannel (RACH) load. In order to reduce the RACH traffic during an outage, this dissertation proposes a Time Hierarchical Scheme (THS). Also, in order to minimize the total time to collect the power outage data, a Backward Recursive Dynamic Programming (BRDP) approach is proposed to adapt the transmission rate of smart meters

reporting an outage. Both the Optimal Transmission Rate Adaption and Time Hierarchical Scheme form the basis of OTRA-THS MAC which is employed by FLEX-MAC for random data collection. Additionally, in this work, Markov chain models are presented for evaluating the performance of FCR and FRRC MACs in terms of average throughput and delay. Also, another Markov model is presented to find the mean time to absorption or mean time to collect power outage data of OTRA-TH MAC during an outage.

This work is partially funded by Oak Ridge National Laboratory (ORNL).

Acknowledgments

First of all I am grateful to my advisors Dr.Jeffrey Reed and Dr.Sandeep Shukla for guiding me with constant discussions and encouragement throughout my Ph.D study. I thank Dr.Michael Buehrer for helping me in taking important design decisions in my research work. His advise at various stages of my research was priceless.

I would like to thank Dr.Virgilio Centeno and Dr.Christian Wernz for serving on my committee. A special thanks to Dr.James Thorp for funding my research work during the first 15 months of my Ph.D. I would also like to thank all my teachers at Virginia Tech and Florida International University for teaching me the fundamental concepts which have greatly helped me in my research.

I also thank my lab members Munawwar Bangla, Sai Dhiraj, Hua Lin, Joseph Gaeddert, Santosh Kumar Sambamoorthy, Andrew Heier and Avik Sengupta for their productive discussions, collaborations and great help in my research. A special thanks to Yeashfi Hasan for proof reading my research papers for both technical and grammatical errors. I am also thankful to Oak Ridge National Labs (ORNL) for partly funding this research work.

I would like to thank the Bradley Department of Electrical and Computer Engineering and graduate school for providing me with the opportunity to pursue my PhD studies here at Virginia Tech. Finally, I would also like to thank Nancy Goad, Hilda Reynolds, Cindy Hopkins, Rebecca Semones and Ruth Athanson for all their help over the last four years.

This dissertation is based on the following published papers. Parts of these papers are included in the chapters of thesis.

1. Garlapati, S.; Hua Lin; Sambamoorthy, S.; Shukla, S.K.; Thorp, J.S.,"Agent Based Supervision of Zone 3 Relays to Prevent Hidden Failure Based Tripping," First IEEE International Conference on Smart Grid Communications (SmartGridComm), 4-6 Oct. 2010, Gaithersburg, Maryland, USA.

2. Garlapati, S.; Shukla, S.K.; Thorp, J.S.,"An algorithm for inferring master agent rules in an agent based robust Zone 3 relay architecture," North American Power Symposium (NAPS), 26-28 Sept. 2010, Arlington, Texas, USA.

3. Garlapati, S.; Shukla, S.K.,"Optimum location of master agents in an agent based zone 3 protection scheme designed for robustness against hidden failure induced trips," IEEE Power and Energy Society (PES) General Meeting, 22-26 July 2012, San Diego, California, USA.

4. Garlapati, S.; Shukla, S.K.,"Formal Verification of Agent based zone-3 backup supervision for transmission line protection," 19th International SPIN Workshop on Model Checking of Software, 23-24 July 2012, Oxford, U.K.

5. Garlapati, S.; Lin H.; Heier A.;Shukla, S.K. and Thorp J.S.,"A Hierarchically Distributed non-intrusive agent aided distance relaying protection scheme to supervise zone-3" published in International Journal on Energy and Power Systems, Sept 2013.

6. Garlapati, S.; Volos H.I.; Kuruganti T.; Buehrer M.R; Reed J.H.,"Performance evaluation of hybrid spread spectrum based advanced smart metering infrastructure with multi-user detection techniques ," International Conference on Wireless Technology and Systems (ICWITS), 11-16 Nov 2012, Maui, USA.

7. Garlapati, S.; Vaghefi R.M.; Buehrer M.R.; Reed J.H.,"PHY and MAC layer design of hybrid spread spectrum based smart meter network," poster presented at International Performance Computing and Communications Conference (IPCCC), 1-3 Dec 2012, Houston, Texas, USA.

8. Garlapati, S.; Vaghefi R.M.; Buehrer M.R.; Reed J.H.,"Performance evaluation of hybrid spread spectrum based advanced smart metering infrastructure with multi-user detection techniques in jamming Channel," Radio and Wireless Symposium (RWS), 20-23 Jan 2013, San Diego, California, USA.

9. Garlapati, S.; Kuruganti T.; Buehrer M.R; Reed J.H.,"OTRA-THS MAC to Reduce Power Outage Data Collection Latency in a Smart Meter Network," International Conference on Computing, Networking and Communications (ICNC), 3 -4 Feb 2014, Honolulu, Hawaii, USA.

10. Garlapati, S.; Kuruganti T.; Buehrer M.R; Reed J.H.,"FLEX-MAC : A Flexible MAC Protocol to Reduce LOEC in Cellular Smart Meter Network," to be submitted to ACM Transactions on Networking.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

This chapter introduces the basic components of the electric power system, i.e., generation, transmission and distribution systems. Also, it briefly describes what is smart grid and what are the main objectives of smart grid. Next, the basic concepts of distance relays and hidden failures are explained, followed by Advanced Metering Infrastructure (AMI).

1.1 Electric Power System

An electric power system is an interconnected network of various electrical components that are used for generation, transmission and distribution of power [48]. The three different components, i.e., generation, transmission and distribution along with their operating voltage ranges are as shown in Figure 1.1. A generation unit comprises of generators feeding into a power grid, protection and control equipment, step up voltage transformers. Generally the

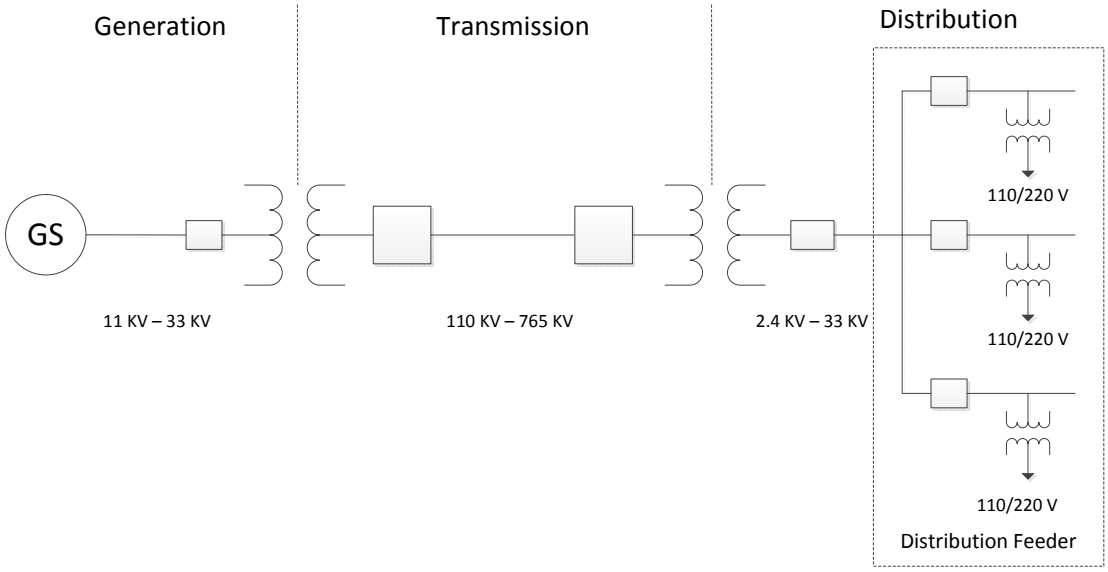

Figure 1.1: A high level view of a power system

power generation occurs at low voltages, i.e., in the range of 11 KV to 33 KV [11]. The transmission unit operates at high voltages (110 KV to 765 KV) and carries power from one region to an other region. A distribution substation transfers power from transmission system to the distribution system. A step-down voltage transformer at the distribution substation reduces the high transmission voltage to a level that is suitable for distribution. The output voltage from distribution substation is in the range of 2.4 KV to 33 KV [79]. Before the electricity is supplied to the customers, with the help of pole mount or drum transformers the voltage is further stepped down to 110 V or 220 V.

1.2 Smart Grid

The U.S. power grid, which is considered to be the world's largest machine is more than 100 years old. Aging infrastructure of the traditional grid, combined with the perennial increase in electricity consumption has forced the experts in the power industry to evaluate the status of the grid. It was concluded that the current electrical grid system is dilapidated and is not upto the mark of powering America's future, which resulted in the smart grid initiative [30]. The main objective of the smart grid is to improve the efficiency of electric power generation, transmission and distribution and thus improve the reliability in power supply to the customers. When the U.S. power grid was originally built the communication and networking engineering disciplines were not very well developed. Undoubtedly over the last 100 years there have been significant improvements in the area of communication and networking. Therefore, most of the researchers in power engineering believe that one of the ways to meet the above mentioned smart grid's objective is to leverage the advances in communication and networking and make the grid smarter. This statement is the main motivation behind this research work. During the process of making the grid smarter, new applications can be introduced and problems in existing grid applications can be fixed. As a part of this research work both these bases are covered, i.e., a new application (AMI) is introduced on the distribution side of the smart grid and a possible solution is provided to a well known and long standing problem of transmission line distance relaying protection scheme.

1.3 Hidden Failures and Distance Relays

Power grid transmission and sub-transmission lines are generally protected by distance relays [42]. Distance relaying protection schemes operate with the main objective of segregating a faulted line from the power grid as quickly as possible (less than a second) to reduce adverse effects of the fault on the grid. Also fault isolation is done with the objective of minimizing the amount of load shed as a result of the relay induced disconnection of lines. Distance relays are categorized as local primary (Zone 1) relays, secondary relays (Zone 2) and remote backup (Zone 3) relays. In distance relaying protection schemes, remote backup relays are preferred to local backup relays as the latter relies on the same electrical and communication equipment used by the primary relays and thus may be susceptible to *Common Mode Failure* [60] [82]. Although the remote backup relay and the primary relay are monitoring and protecting the same transmission line, physically they are located in different substations and thus are less susceptible to *Common Mode Failures*. Compared with the primary relays, the remote backup relays acting upon to clear a fault results in a larger amount of load shed. Therefore, distance relaying protection schemes are designed in such a way that the remote back relays operate with the longer fault clearing times, i.e., it operates when both the Zone 1 and Zone 2 relays fail or their associated sensors or breakers simultaneously fail to clear the fault. After a comprehensive analysis of historical blackouts such as 1965 Great North-East Blackout, 1977 New York Blackout and the 1996 Western Blackout, North American Electric Reliability Council (NERC) has arrived at a conclusion that the mis-operation of distance relays is one of the major causes of cascading outages

leading to blackout events [22][90]. Horowitz and Phadke re-examined the distance relaying protection scheme to eliminate the remote backup relays but concluded that the Zone 3 relays cannot be excised as its omission will put the power system at risk.

As mentioned above, a relay can mis-operate and erroneously trip a line out of service due to hidden failures [67] [74]. A hidden failure is a rare event, which is a permanent (software or hardware) or temporary (relay setting) error in a relay that may go unidentified for a long duration of time and gets excited by another event (e.g. line trips) leading to incorrect removal of circuit elements [74]. Because of the hidden failures, a Zone 3 relay may be over-sensitive to the temporary line loadings occurred due to the transients and misinterpret it as a fault even though the Zone 1 and Zone 2 relays do not classify the condition as faulty. Under these conditions, if the power system is operating in stressed state, the hidden failure induced mistrip may initiate other line trips, leading to cascading failures which may result in catastrophic events like blackouts. In [90], based on these temporary line loadings and Zone 3 relay hidden failures, an algorithm for simulation of cascading outages is proposed. A test simulation on NYPP 3000 bus model revealed 41,053 (24.4%) reasonable blackout scenarios out of 1,67,752 simulated events.

In protection relay engineering jargon, the mistrips are known as *over-trips*. In California and neighboring utilities, the average industry standard *over-trip* rate of extremely high voltage relays (distance relays) is approximately 10%. In the last decade, the relay mis-operation rate on 500 KV transmission lines in the northern utility of California, Pacific Gas and Electric (PG& E) is well above the industry standard [61]. In 2003 USA/Canada

Table 1.1: Comparison of different technologies [72]

No	Use Cases	3G/4G	GPRS	RF Mesh	PLC
1	Distribution Automation	Yes	Does not meet latency requirements	Does not meet latency requirements	Yes
2	Multi-Interval Meter Reading	Yes	Yes	Yes	Yes
3	On-Demand Metering Reading	Yes	Yes	Depends on network configuration	Yes
4	Firmware/Program Updates	Yes	Limited Capacity	Limited Capacity	Limited Capacity
5	Outage Management	Yes	Depends on network configuration	Depends on network configuration	Does not support outage reporting in some scenarios
6	Service Switch	Yes	Yes		Yes
7	Demand Response - Direct Load Control	Yes	Yes		Yes
8	Real-Time Pricing	Yes	Yes		Yes

blackout, 14 relay over-trips were observed [62]. The above mentioned theoretical studies and practical experiences exposed the vulnerability of a power grid to the relay hidden failures and urges the need for a mechanism to nullify the adverse effects of the hidden failures on the power grid. In this dissertation, agent aided distance relaying protection scheme is proposed to improve the robustness of distance relays to hidden failures and thus reduce the probability of blackouts.

1.4 Advanced Metering Infrastructure

The Advanced Metering Infrastructure (AMI) is a technology where smart meters installed at the customer's site give the utilities the ability to monitor and collect information related to the amount of electricity consumed by the customer. AMI is one of the important applications of the smart grid and is supposed to play a key role on the distribution side of the smart grid. A network set up for AMI is not only expected to carry smart meter data traffic but also it should handle the data generated by other smart grid applications such as Distribution Automation (DA) and Demand Response Management Systems (DRMS). In the recent past, the selection of the appropriate choice of communication technology for different smart grid applications has been debated a lot. After comparing different possible technologies, a recent research study has arrived at a conclusion that the 3G cellular technology is the right choice for distribution side smart grid applications like AMI, DA and DRMS [72]. The comparison of different communication technologies like Power Line Carrier (PLC), Global Packet Radio Service (GPRS), RF mesh and 3G cellular are as shown in Table 1.1. It is obvious from Table 1.1 that the 3G cellular technology seems to be a good choice for smart grid applications. Even though 3G cellular meets the requirements of distribution side smart grid applications, a simple analysis on the state of the art cellular network gives an indication that their usage results in a high percentage of control overhead (transport and MAC layer) and higher latency for smart grid data transfers. Hence, in order to reduce the control overhead and smart grid data collection latency, this dissertation proposes, a new network architecture and FLEX-MAC, a flexible MAC protocol with spread spectrum as the

PHY layer technology.

1.5 Contributions

This dissertation has two major contributions. First, a hierarchically distributed non-intrusive Agent Aided Distance Relaying Protection Scheme (AADRPS) is proposed to improve the robustness of distance relays to hidden failures. The problem of adapting the proposed AADRPS to a larger power system network consisting of thousands of buses is modeled as an integer linear programming multiple facility location optimization problem. Distance relaying protection scheme is a real time system and has stringent timing requirements. Therefore, in order to verify if the proposed AADRPS meets the timing requirements or not and also to check for deadlocks, verification models based on UPPAAL real time model checker are provided in this dissertation. So, the entire framework consisting of AADRPS that aids in increasing the robustness of distance relays and reducing the possibility of blackouts, the multiple facility location optimization models and the UPPAAL real time model checker verification models form one of the major contributions of this dissertation.

The second contribution is related to the MAC layer of AMI networks. In this dissertation, FLEX-MAC - a novel and flexible MAC protocol is proposed to reduce the overhead and latency in smart meter data collection. The novelty of the FLEX-MAC lies in its ability to change the mode of operation based on the type of the data being collected in a smart meter network. FLEX-MAC employs Frame and Channel Reserved (FCR) MAC or Frame Reserved

and Random Channel (FRRC) MAC for scheduled data collection. Power outage data in an AMI network is considered as a random data . In a densely populated area, during an outage, a large number of smart meters attempt to report the outage, which significantly increases the Random Access CHannel (RACH) load. In order to reduce the RACH traffic during an outage, this dissertation proposes a Time Hierarchical Scheme (THS). Also, in order to minimize the total time to collect the power outage data, a Backward Recursive Dynamic Programming (BRDP) approach is proposed to adapt the transmission rate of smart meters reporting an outage. Both the Optimal Transmission Rate Adaption and Time Hierarchical Scheme form the basis of OTRA-THS MAC which is employed by FLEX-MAC for random data collection. Additionally, in this work, Markov chain models are presented for evaluating the performance of FCR and FRRC MACs in terms of average throughput and delay. Also, another Markov model is presented to find the mean time to absorption or mean time to collect power outage data of OTRA-TH MAC during an outage.

1.6 Outline of the Text

As mentioned earlier, this dissertation involves work related to two different smart grid applications. Chapters 4, 5 and 6 discuss the first part, i.e., the work related to agent based distance relaying protection scheme and the chapters 7 and 8 explain the second problem, i.e., new architecture and Frame and Channel Reserved (FCR), Frame Random and Reserved Channel (FRRC) and Optimum Transmission Rate Adaptive-Time Hierarchical (OTRA-

TH) MAC layer schemes that significantly reduce the latency and control overhead in smart grid data collection when compared to 3G CDMA2000. Remainder of this dissertation is organized as follows: Chapter 2 briefly explains the basic concepts required to understand the following chapters. Related work is discussed in chapter 3. Chapter 4 discusses the long standing problem of distance relaying protection scheme that is responsible for 70% of the historical U.S. blackouts. Chapter 4 also explains the proposed Agent Based Distance Relaying Protection Scheme (ABDRPS) to reduce the probability of blackouts. In Chapter 5, the problem of adapting ABDRPS to a geographically wide spread larger power systems is modelled as an Integer Linear Programming (ILP) multiple facility location problem. ABDRPS depends on the real time communication between agents. Therefore, in chapter 6 the communication mechanism between different components of ABDRPS is modelled and formally verified using UPPAAL - a real time model checker.

Chapter 7 gives a detailed description of the proposed Non-TCP/IP based architecture, FCR and FRRC MAC layer schemes for power consumption data collection. In chapter 7, markov chain steady-state analysis is used to derive analytical expressions for average throughput and average latency of FCR and FRRC MAC. In chapter 8, OTRA-TH MAC is explained in detail for power outage collection and markov chain transient analysis is used to derive the average number power outage reportings and average Power Outage Data Collection Latency (PODCL).

Chapter 2

Background

The main aim of this chapter is to introduce the basic concepts required to understand advanced metering infrastructure and transmission line distance relaying protection scheme. This chapter is organized as follows: In section 2.1, basics concepts related to power system relaying are explained. Section 2.2 provides a brief summary of spread spectrum and it's different forms.

2.1 Basics of Power System Relaying

2.1.1 Relay

According to the Institute of Electrical and Electronic Engineers (IEEE) a relay can be defined as " *an electric device designed to respond to input conditions in a prescribed manner*

and after specified conditions are met, to cause contact operation or similar abrupt change in associated electric control circuits" [3]. In other words, relays detect abnormal power system conditions and respond as quickly as possible with a necessary corrective action in order to bring power system back to normal or safe state. There exists many different classes of relays. They are electric relays, electromechanical relays, electromagnetic relays, solid state relays, hybrid relays and computer relays. In power system engineering relays are mostly employed for protecting different circuit elements like transformers, generators and transmission lines. Therefore *relays* are also called as *protection relays*.

2.1.2 Relaying

Relaying is a sub-discipline of electric power engineering that deals with the principles of design and operation of protective relays. In the earliest relaying system designs, electromechanical relays and solid state relays were mostly used but in the recent past computer relays have surrogated the electromechanical and solid state relays. This research work is related to computer relaying schemes.

2.1.3 Protection System

A protection system protects the power system from pernicious effects of a sustained fault. A fault can be defined as a short circuit or an abnormal system condition. A fault is generally considered as a random event. Any power system component, i.e., line, bus, transformer,

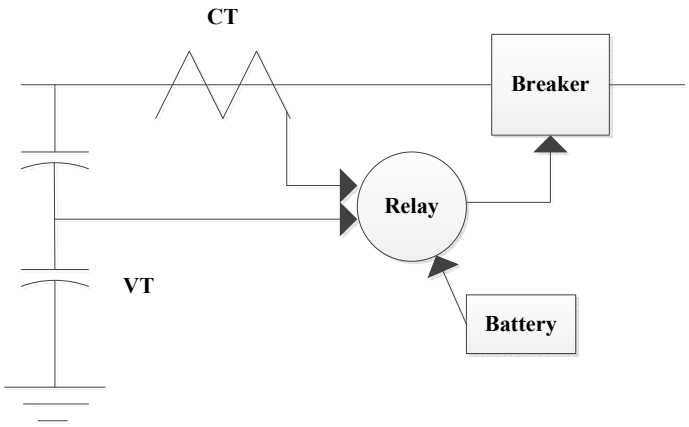

Figure 2.1: Elements of a protection system [68]

generator can experience a fault. The main objective of a protective system is to isolate a faulted equipment as soon as possible from the power system, otherwise the fault may spread to the other parts of the system and lead to power system instability which is undesirable. The basic elements of a protection system are as shown in Figure 2.1. It consists of sensors (i.e. Current Transformers (CT) and Voltage Transformers (VT)), protective relays, circuit breakers and battery. Current and voltage transformers respectively sense current and voltage values and pass it to the relay. The protective relay executes the relaying algorithm and decides if a fault exists or not. If a fault exists then the relay sends a signal to the circuit breaker to disconnect the faulted element from the power system. A portion of this research work is related to transmission line distance protection scheme which is discussed in next subsection.

2.1.4 Distance Relaying Protection Scheme

Power grid transmission line system is generally protected by distance relaying protection scheme. Distance relays operate based on the principle of impedance ratio, which is the ratio of the magnitude of the measured voltage to that of the magnitude of current. In order to account for the inaccuracies in sensing equipment, uncertainty in distance setting of relay and to make sure that there is no blind spot, multiple zones of protection (Zone 1, Zone 2) are employed for each transmission line. In the presence of a fault if the breaker associated with the zone 1 or zone 2 relay doesn't trip (due to a failure in current transformer, voltage transformer, relay or breaker), the faulted line cannot be isolated from the system. To overcome this situation a backup relay or Zone 3 relay is placed in the remote substation. Thus there exist three different zones of protection, i.e., Zone 1, Zone 2 or Zone 3 relays. It is already explained earlier that the remote back up relay is preferred to local backup relay as the latter can be a victim of "common mode failure" along with the primary relay (Zone 1). Zone 1, Zone 2 and Zone 3 relays are located in different substations and each of them has their own associated CT, VT and breaker. Zone 1, Zone 2 and Zone 3 settings of relay R_{12} are as given below

$$R_{12}(Zone1) = 0.85 * (Z_{12}) \tag{2.1}$$

$$R_{12}(Zone2) = 1.2 * (Z_{12}) \tag{2.2}$$

$$R_{12}(Zone3) = Z_{12} + (1.2 * Z_{25}) \tag{2.3}$$

Similarly for R_{21}

$$R_{21}(Zone1) = 0.85 * (Z_{21}) \quad (2.4)$$

$$R_{21}(Zone2) = 1.2 * (Z_{21}) \quad (2.5)$$

$$R_{21}(Zone3) = Z_{21} + (1.2 * Z_{13}) \quad (2.6)$$

Here Z_{xy} is the impedance of the transmission line connected between bus x and bus y. Zone 1 relay operates instantaneously, i.e., within 1 to 2 cycles (16 to 32 msec). A coordination delay of 20 to 30 cycles (300 to 500 msec) is allowed before Zone 2 relay operates. Zone 3 relay or remote back up relay is allowed to operate with a coordination delay of 1 sec (1000 msec). Coordination delays not only provide selectivity in isolating a faulted section but also ensure reliability of operation of the distance protection scheme [43]. Detailed explanation of zones of protection is out of the scope of this dissertation. Interested readers are referred to [68].

2.1.5 Phasor Measurement Unit

A phasor is a complex number which represents both the magnitude and phase angle of the sine waves found in electricity. A Phasor Measurement Unit (PMU) is a device that measures the voltage and current phase angles and magnitude on an electricity grid, using a time source of synchronization. PMU is invented by Dr.James S. Thorp and Dr.Arun G. Phadke at Virginia Tech. With the help of PMU's, synchronized real-time measurements are

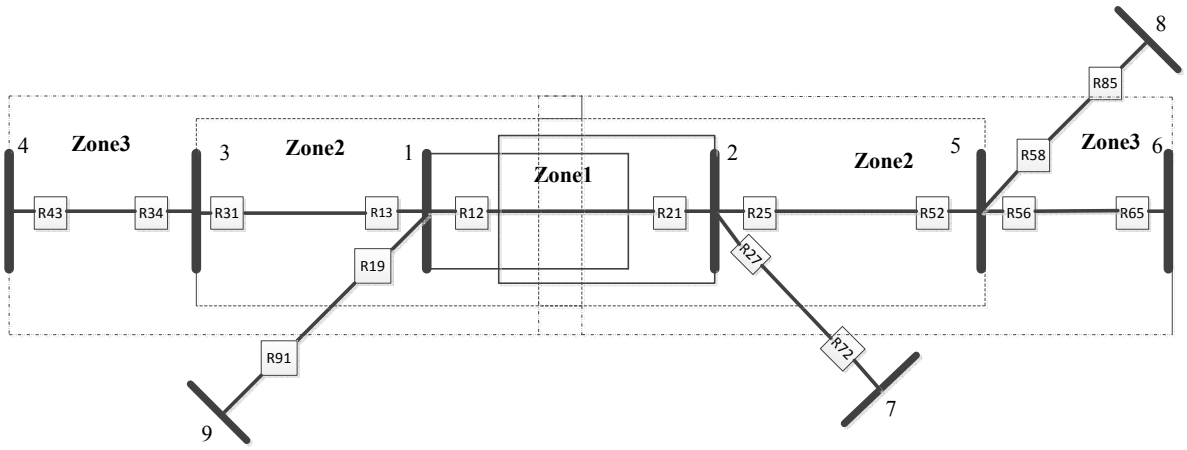

Figure 2.2: Zones of protection

obtained from various remote measurement points (covering wide area) on the grid. PMU's use Global Positioning System (GPS) for the purpose of time synchronization. The time synchronization PMU measurements are also known as *synchrophasors*. A PMU can be a dedicated device or the PMU functionality can be a part of protective relay, the latter is mostly preferred [2][76][55] . The synchrophasor measurements aid power system operators to achieve faster and improved power system state estimation and thus obtain better control of electric power transmission line system. PMU measurements and communication of these measurements to control center follow IEEE C37.118 standard. At present different utilities in U.S. are in the process of installing wide area measurement systems consisting of phasor measurement units.

2.2 Spread Spectrum Communication

This section explains the basic concepts required to understand the second problem studied in this dissertation, i.e., MAC Layer design for AMI networks.

2.2.1 Spread Spectrum

Spread spectrum can be defined as any modulation technique which

(a) utilizes substantially more bandwidth than required for the data rate being transmitted and

(b) the increase in bandwidth is achieved by using a pseudorandom signal that is independent of the data. The receiver uses the same pseudorandom signal to recover the transmitted spread signal.

In spread spectrum, the process of increasing the signal bandwidth is known as *spreading* and the opposite of spreading, i.e., the process of decreasing the signal bandwidth is known as *despreading*. There are many advantages of spreading a signal to a bandwidth greatly beyond the information rate in a pseudorandom manner. A few of them include resistance to interference (intentional or otherwise), the potential to hide the signal from unintended reception (i.e., low probability of intercept or LPI), low probability of detection or LPD, resistance to multipath fading, improved multiple access capability, and ranging [69]. Initially spread spectrum radios were used for military applications but in the recent past (starting from 1990's) spread spectrum technology has been used in the commercial sector. The most

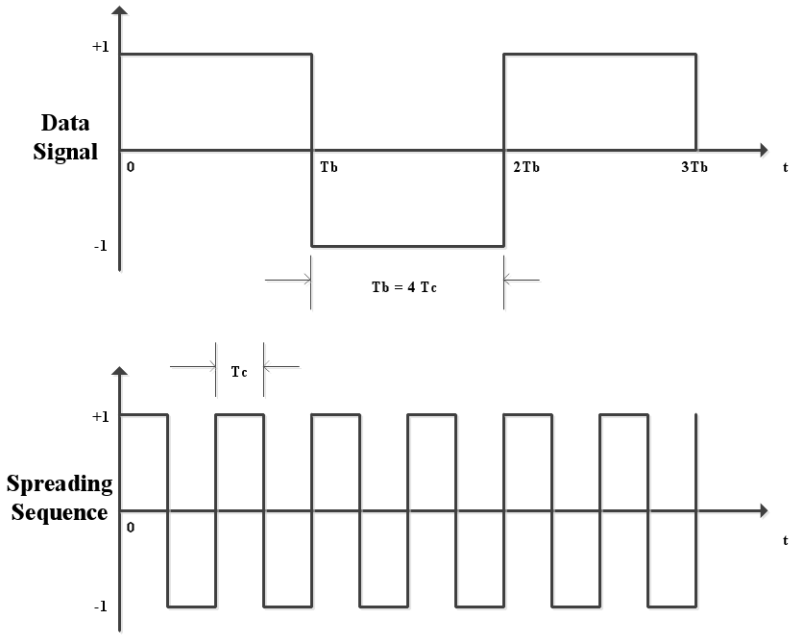

Figure 2.3: Sample data signal and spreading sequence

commonly used spread spectrum systems are Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), Time Hopping Spread Spectrum (THSS) and different combinations of these systems known as Hybrid Spread Spectrum (HSS) systems. The following subsections briefly discuss these systems.

2.2.2 Direct Sequence Spread Spectrum

A DSSS generates a spread-spectrum signal by directly multiplying the data signal stream by a high rate spreading waveform before the carrier modulation [88]. The spreading waveform consists of pseudorandom symbols and is generated using a pseudorandom noise (PN) sequence. Linear Feedback Shift Register (LFSR) is generally used for generating psuedo-

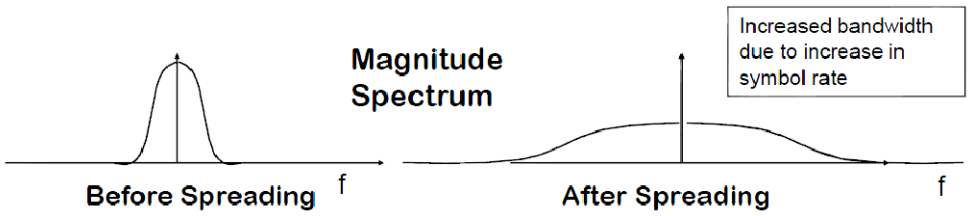

Figure 2.4: Direct sequence spread spectrum

random sequence. A sample data signal and spreading sequence is as shown in Figure 2.3. The dual of the convolution theorem of Fourier Transform says that the multiplication of two signals in the time-domain is equivalent to the convolution of their spectra. Thus, the bandwidth of the resulting signal is approximately equal to the largest among the spreading sequence and data signal. Spreading sequence is also known as spreading code, code sequence and chipping sequence. The benefit provided by spread spectrum is measured by *processing gain* or *spreading gain*. The *processing gain* of DSSS can be defined in the following two different ways

a) the ratio of the symbol rate of the spreading waveform to the symbol rate of the information signal.

b) the ratio of the spread bandwidth to the information rate [57].

Figure 2.4 shows the signal before spreading and after spreading. DSSS performs well in multipath environments and it is mostly used in commercial applications like 3GPP WCDMA and 3GPP2 CDMA2000.

2.2.3 Frequency Hopping Spread Spectrum

In this form of spread spectrum the frequency of the transmitted signal is varied in a pseudo-random fashion. This is as shown in Figure 2.5. Similar to DSSS, FHSS uses pseudorandom noise sequence to change the center frequency of the carrier to one of the q different non-overlapping frequency channels every chip period T_c [84]. The number of different hopping frequencies (q) is known as the spreading gain. FHSS excels in jamming and fading channels. Based on the value of chip period (T_c), Frequency hopping is categorized as slow frequency hopping (SFH) and fast frequency hopping (FFH) [71]. In FFH, the chipping period (T_c) is less than the data symbol period (T_s) whereas in SFH the chipping period (T_c) is greater than the data symbol period (T_s). FFH provides frequency diversity at the symbol level, which provides a substantial benefit in fading channels. SFH performs well in Gaussian channel. In the case of SFH, coherent demodulation is easier because frequency hopping rate is much slower than the data rate.

2.2.4 Time Hopping Spread Spectrum

THSS is the least popular among the different forms of spread spectrum. THSS is a form of pulse-based system in which transmissions occur based on a series of low duty cycles similar to that of the impulse-radio systems [92] [12]. In THSS systems, the period and duty cycle of pulsed RF carrier are varied in a pseudorandom manner under the control of a code sequence. Figure 2.6 gives a pictorial view of time hopping spread spectrum. A data burst

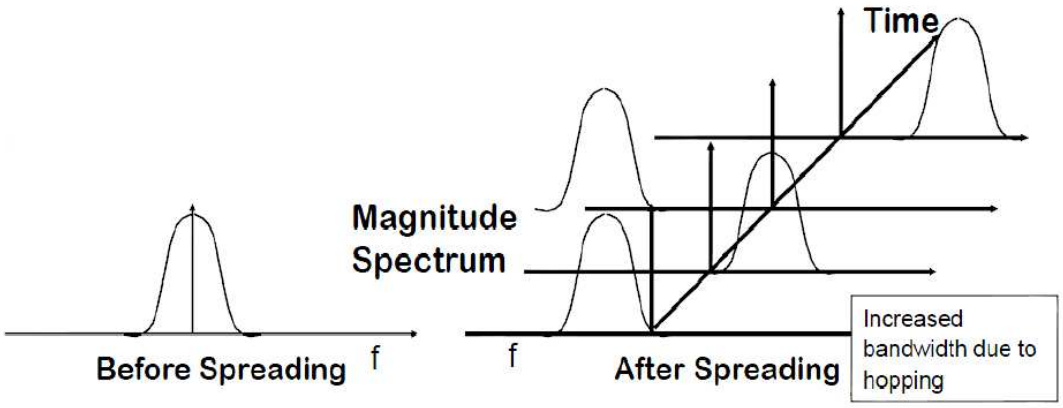

Figure 2.5: Frequency hopping spread spectrum

may consist of b bits of data. As shown in Figure 2.6, the time instance at which a burst is transmitted is determined by a pseudorandom sequence. THSS is used in Ultra Wide Band (UWB) communication systems but UWB didn't succeed commercially.

2.2.5 Hybrid DS/FH/SS

HSS(Hyrbid Spread Spectrum System) combines direct sequence and frequency hopping techniques. The data signal is first spread using a direct sequence of length N and then further spread by hopping the center frequency to one of q hop frequencies. This technique is useful for obtaining extremely high spreading factors since it can spread the bandwidth more than either DSSS or FHSS alone. HSS is attractive because it can combine the good features of both DSSS and FHSS systems while avoiding some of their shortcomings. For example, a hybrid system can combine the anti-multipath effectiveness of DSSS systems

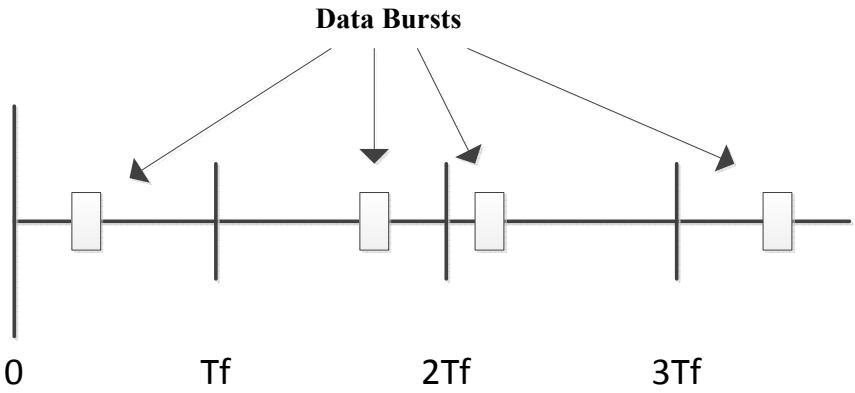

Figure 2.6: Time hopping spread spectrum

with the good antipartial-band-jamming features of FHSS systems [33]. Hybrid systems may also use shorter psuedorandom sequences and hopping patterns, thus reducing the overall acquisition time. A disadvantage of hybrid systems is the increased complexity of their transmitters and receivers. The total spreading gain of HSS system is $q * N$.

Chapter 3

Related Work

This chapter discusses the prior related work done by other researchers in the analysis of hidden failures in distance relays, blackouts, combined power and communication simulations and advanced metering network design. As the two problems studied in this dissertation are disjoint, there exists two different sections on related studies.

3.1 Prior Work on Distance Relays

This section briefly summarizes the work done by other researchers in analysing cascading outages, performing combined power and communication simulations. Thorp *et al.* studied the anatomy of cascading outages in a system due to hidden failures and proposed few preventive strategies [82] [83] [80]. Wang *et al.* have simulated a large number of cascading outages and proposed an idea for optimal location of relays for protection system enhance-

ment [90]. Nedic *et al.* developed an AC blackout model, examined and verified criticality of a 1000 bus network by creating cascading failures [59]. Carreras *et al.* developed a dynamic model to study the complex global system dynamics of blackouts in power transmission system [14]. Chen *et al.* developed a hidden failure embedded DC model for power transmission systems and studied the power law distributions in North American blackout. They also evaluated possible mitigation measures after investigating global system dynamics [18]. Dobson *et al.* developed a loading-dependent analytical solvable model for general probabilistic cascading failure analysis [23]. Phadke examined the mechanisms of hidden failures of the protection system and their role in power system disturbances [67]. Chowdhury *et al.* developed methods to create cascading failures in large interconnected power systems under different credible contingency conditions and using a 118 bus system, they proved that their methods can be used to report several cases of cascading outages [20]. In [41], an agent based backup protection system is developed for transmission networks. They used EPOCHS, a federation of power and network simulators to study the protection scheme.

3.2 Prior Work on AMI

Advanced metering infrastructure is one of the important distribution side applications of the smart grid. In the recent past a lot of research has been devoted to AMI network design. After a detailed analysis of AMI networks, Liu *et al.* suggested that a well planned and organized AMI network has many advantages in various aspects of electric grid operations

like distribution automation, faster service restoration and network condition monitoring [53]. The pros and cons of different possible technologies for AMI communication are as follows.

3.2.1 RF Mesh

Yan *et al.* studied the security vulnerabilities of AMI and proposed a wireless multi hop architecture based in-network collaborative scheme to provide secure and reliable AMI communications in smart grid [94]. Moreover, the multi-hop architecture requires two different networks, i.e., a Local Area Network (LAN) and a Wide Area Network (WAN) for data collection. Smart meters use LAN for transmitting data to the intermediate Data Aggregator Point (DAP) and WAN to send data from DAP to the utility control center. Generally IEEE 802.11 Wi-Fi or IEEE 802.15.4 Zigbee based networks are considered for LAN and IEEE 802.16 WiMAX or 3G/4G cellular networks are used as WAN. The main issue of RF mesh networks is that the multi-hop architecture increases the delay in data transfer from smart meter to the utility control center. Also, in rural areas, the long distance between the smart meters (houses) decreases the reliability in transmission and increases the number of DAPs.

3.2.2 Power Line Carrier Communication

Power Line Carrier Communication (PLCC) is another possible technology for AMI network data collection. The power lines are not designed to carry data signals and hence PLC

presents many difficulties for data communication. The PLC channel noise may be excessive and also has very abnormal characteristics. The PLC exhibits high attenuation at frequencies of interest to communications and hence repeaters may be required to compensate for cable losses [39]. PLCC also involves handling electromagnetic compatibility issues when interfacing electronic circuits with power lines. To make it worse, the channel properties like impedance and attenuation, noise fluctuate with load and time in an unpredictable way, i.e., when ever a device is plugged-in or out and switched in or out, channel properties change. Thus, PLC channel can be characterized as a very harsh and noisy transmission medium, frequency-selective, time varying, and is impaired by colored background noise and impulsive noise [39]. Hence, modelling the PLC channel is not an easy task.

In USA, a pad/pole mount transformer supplies power to 7-8 houses [9] [73]. A transformer attenuates PLC data signals by around 55 to 75 dB [66]. Hence, apart from installing smart meters, utilities should also install repeaters at every transformer, which significantly increases costs. On the other hand, in Europe, a single secondary transformer serves upto 100 households and hence the number of repeaters required are lower when compared to USA. Therefore, PLCC is a preferred means of communication for smart grid applications in Europe but not in USA. Another important issue of PLCC is that the power lines can be easily tapped into and hence questions are being raised about the security of the information conveyed over the PLC.

3.2.3 Cellular Networks

It was aforementioned in chapter 1, a reliable source compared the key characteristics of different communication and networking technologies like RF mesh, PLC and 3G cellular and concluded that 3G Commercial Cellular Technologies (3GCCT) provide an advanced and cost effective solution for smart grid communications [72]. The comparison results are as shown in Tables 1.1 and 3.1. The main reason for this is that the 3G cellular gives ubiquitous coverage, high reliability, high capacity and data rates, robust security, low cost of ownership, high performance and high scalability. Also, there exists other research studies that support this argument [63] [36]. Grayson-Collin Electric Cooperative in Texas and Duck River Electric Membership Corp in Tennessee have promulgated that they have decided to use cellular communications for Advanced Metering Infrastructure (AMI) [26] [45]. But it is unclear if they are using 3GCCT or LTE based communication. All the above mentioned research studies and practical implementations considered commercial cellular networks and specifically [63] [36] and [72] support the use of commercial 3GCCT for smart metering application.

On the other hand Alliander, a utility in the Netherlands built a private CDMA2000 (1xEV-DO) based wireless network in 450 MHz band to address its communication needs for smart metering and other smart grid applications [16]. Alliander studied the economics of 450 MHz band for AMI and concluded that building a private network in the 450 MHz or other lower frequency bands not only offers gain in terms of coverage, service quality and control but also economical compared to using a commercially offered cellular service from GSM, GPRS,

Table 3.1: Summary of technologies and capabilities

	3G/4G	**RF Mesh**	**PLC**
Network Type	Operator managed WAN	Utility deployed and operated	Utility deployed and operated
Topology	Cellular	star	Power line
Spectrum Type	Licensed	Unlicensed	Power-line
Typical Data Rate	1 Mbps	9.6-100+ Kbps	Several to 100+ Kbps
Message Delivery Latency	$<$ 1 sec	$<$ 1 - 60 sec	$<$ 1 sec
Coverage	10s of meters to 10s of Km's per cell site	Up to 50m	up to multiple Km's
Reliability/Availability	Rate of successful link establishment $>$ 99%	Deployment and product specific	Dependent on the underlying power line

CDMA or LTE [17]. In their study, along with economic feasibility, Alliander considered other factors such as extended life time (more than 15 years), security, availability and control. According to Ericsson, the choice of public (3G/4G) or private cellular network for smart meter data collection is non-technical and it depends on whether the utility can recover the cost of investment or not [28]. This dissertation doesn't argue the use of public or private network for smart metering. In this research work, we assume that the utilities are employing a private 3G CDMA 2000 network for smart metering.

Although 3G cellular technologies satisfy the requirements of smart grid applications, an analysis on the use of the current state of the art 3G cellular technologies for smart grid applications gives an indication that their usage results in a high percentage of control

overhead and high latency for data transfer. The detailed discussion of overhead and latency of 3G cellular networks is provided in chapter 7. In order to reduce the overhead and latency in AMI network data collection, we proposed a new network architecture and FLEX MAC - a novel MAC layer protocol as a part of this dissertation.

Chapter 4

Agent Aided Distance Relaying Protection Scheme

It was discussed earlier in chapter 1 that the distance relays are susceptible to hidden failures and can lead to cascading outages like blackout. A blackout is a scenario where a region/area is out of power temporarily for some duration of time. One of the main objectives of the smart grid is to improve the reliability of the grid and thus provide uninterrupted power supply to the customers. Thus, one of the main constituents of the smart grid vision is to obtain the wide area measurements and control to improve the robustness of power system applications to an unprecedented level. In order to obtain the wide area measurements, power system network has to be endowed with the communication and networking infrastructure.

In this research work, in order to increase the robustness of the Zone 3 relays to hidden

failures, we propose a hierarchically distinguished non-intrusive agent based Zone 3 relay supervision scheme. The communication between agents aid the distance relaying scheme to reduce the possibility of hidden failures leading to blackout events. In this research work the problem we intend to study is briefly stated as follows:

"How can a communication network and fast computing abilities enhance the functionality of Zone 3 relays so that they can be robust to hidden failures, and over active undesired tripping can be prevented?"

We attempt to answer this question by first developing a distributed hierarchical agent based scheme and then demonstrating a few simulations based experimental data to backup the possible validity of our scheme. However, the problem at hand is as much a problem in the domain of distributed fault-tolerant computing with networked communication, as it is a power system protection problem. The solution we provide here is based on certain idealization and our scheme will work under those idealizations, explicitly stated in the next subsection. However, we believe to solve this problem we need to proceed incrementally, first by devising a scheme that works under a few ideal assumptions, and then carefully enhancing the scheme as the assumptions are gradually removed.

4.1 Assumptions

To simplify the first order solution, we assume that the communication network is robust and no computing node or the communication links can fail. So we are making an important

assumption that even though a Zone 3 relay's relaying functionality (may be hardware or software or mechanical) may be susceptible to hidden failure, the agent functionality we impart is somehow special, and cannot be subject to hidden failure. This can be achieved by redundancy and autonomous monitoring. However, we do not assume anything special about packet losses in the network and we also do not make any special assumptions about network delays. Our simulations actually simulate various TCP/IP based protocols for communication, for various physical media, and various traffic scenarios. We also assume that we can run an agent on each protection relays as they are usually intelligent electronic devices (IED) capable of running specific application software. It is also possible to design an agent as a dedicated hardware device and connect it to the relay. One important distinction of the proposed solution in this work with other agent based relaying schemes (e.g. [91] [41]) is that our agents are non-intrusive in the sense that they do not take over any relaying functions, but just monitor and provide information to the relays.

In this work, we do a trace driven simulation approach to experimentally validate our scheme. We simulate a power system model dynamics separately and create cascading outages due to a sequence of Zone 3 relay trips following a real fault event. We then use the timed traces from the power system simulator and simulate the corresponding network with NS-2, to estimate the delays in communicating between various agents running on the various relays. This allows us to refrain from combination simulators which are time consuming to build, but it serves our purpose of demonstrating the validity of our scheme.

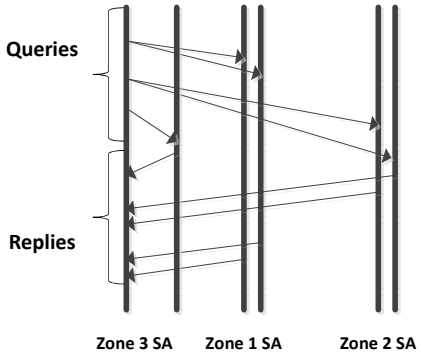

Figure 4.1: Non-hierarchical agent communication

4.2 Proposed Scheme

This section describes the agent based Zone 3 relay supervision scheme in detail. The main distinction between our scheme and other agent based relaying schemes (e.g. [82] [22]) is that our agents are non-intrusive, i.e., they do not take over the relaying functionality, but just monitor and aid relays in decision making to trip or not to trip. Relay protection engineers do not like the idea of intrusive agents therefore we preferred to use non-intrusive agents in our Zone 3 supervision scheme.

A fault in a single transmission line is sensed by multiple relays under different zones of protection (Zone 1, Zone 2 and Zone 3). For example in Figure 2.2, a fault in the transmission line connected between bus 1 and bus 2 can be sensed by relays R_{12},R_{21},R_{43},R_{31},R_{52},R_{65},R_{72}, R_{91} and R_{85}. The proposed scheme exploits this redundancy in the transmission line protection to distinguish a fault as a true fault or hidden failure induced fault. In our scheme,

each relay is associated with an agent that has the ability to communicate with the other agents in the network. Whenever a relay senses a fault in the transmission line protected by it, its associated agent records it and communicates with the other agents protecting the same transmission line in the network to find out if the perceived fault is a true fault or a hidden failure induced fault. If the majority of the other relays protecting the same transmission line also sense a fault, classifying it as a faulty condition, agent can advise its associated relay to trip. On the other hand if the majority of the other relays do not sense a fault, categorizing it as a fault-free condition, agent can advise the relay not to trip. This is because the relay might have sensed a fault due to hidden failure and it is not required for the relay to trip. It is possible that a fault in a single transmission line can be at least sensed by six relays, i.e., Zone 1, Zone 2 and Zone 3 from both ends of the transmission line. Therefore in order to classify a sensed fault as a true fault or a hidden failure induced fault, agent has to communicate with at least five other agents. This is as shown in Figure 4.1.

In Figure 4.1, a Zone 3 slave agent is shown to be communicating only with five slave agents but depending on the power system network topology it is possible that a slave agent may end up communicating with more than upto 10 to 15 relays. Therefore the communication scheme shown in Figure 4.1 can result in longer response times which is not desirable for distance relaying protection scheme. As mentioned in section 2.1.4, distance relaying protection scheme is a time critical application, i.e., Zone 1, Zone 2 and Zone 3 relay has to trip a line within 32 msec, 300 msec and 1 sec respectively. If the total response time is longer than these times, agent supervision scheme does not serve the intended purpose.

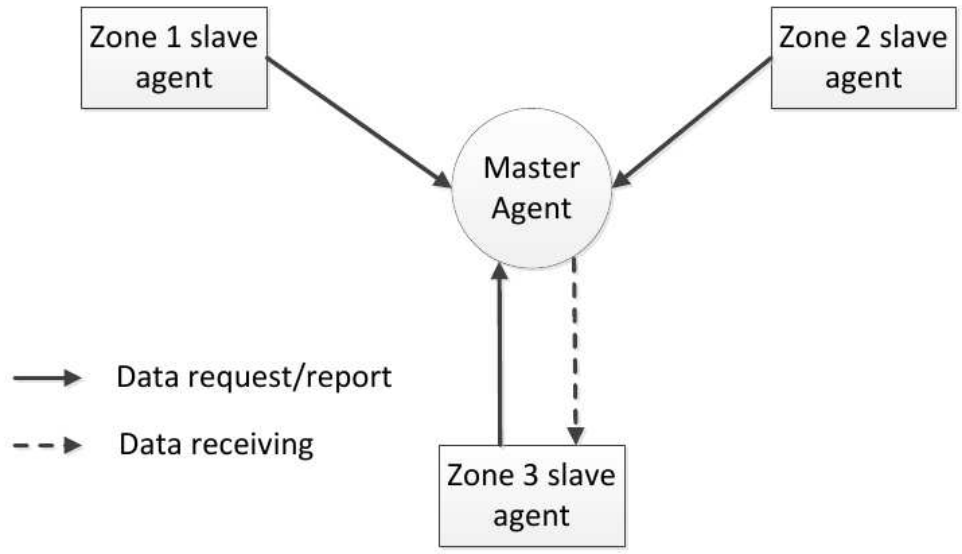

Figure 4.2: Communication mechanism between master agent and slave agents

Therefore, in order to reduce the response times, agents are hierarchically distinguished as slave agents and master agents. A slave agent associated with a relay is called as *slave relay agent* and a master agent associated with a relay is called as *master relay agent*. Therefore the terms *slave relay agent*, *slave agent relay* and *slave agent* are used interchangeably. Similarly terms *master relay agent*, *master agent relay* and *master agent* are identical.

The communication mechanism between the master and different (Zone 1, Zone 2 and Zone 3) slave agents is as shown in Figure 4.2. Slave agents exhibit the normal behaviour of agents, i.e., they can record a fault and communicate with the master agent. More importantly slave agents report the fault status 30 times per sec to the master agent. The master agent has a different set of responsibilities compared to the slave agent. At any given instance master agent has the most recent fault status information of all the slave agent relays reporting to it. When ever a relay senses a fault, its associated slave agent records it and queries the master

agent to find out if the relay associated with it can trip or not. Master agent compares the querying slave agent relay's fault status with the fault statuses of the other slave agent relays protecting the same transmission line as that of the querying slave agent relay. In order to compare the fault statuses, the master agent must know ahead of time which set of relays are protecting the same transmission line. Section 4.3 provides an algorithm explaining how a master agent finds the set of relays (relay-set) protecting a transmission line under different zones of protection. Based on the result of comparison, the master agent suggests the querying slave agent relay to trip or not to trip the transmission line out of service. The entire process of a relay sensing a fault, its associated slave agent recording the fault and querying the master agent to classify (true or hidden failure induced) a fault, the master agent performing fault statuses comparisons and sending an acknowledgement to the queried slave agent has to be finished with in the fault clearing time of the respective relay, i.e., 1 sec for Zone 3 relay, 300 msec for Zone 2 relay and 32 msec (almost instantaneous) for Zone 1 relay. With the current state of the art networking and communication equipment the timing requirements for Zone 1 and Zone 2 relay may be difficult to meet but Zone 3 relay timing requirements may be met. Therefore the agent based distance relaying supervision scheme proposed in this work restricts its analysis only to Zone 3 relay supervision, i.e., only to improve the robustness of the Zone 3 relays to hidden failures but not Zone 1 and Zone 2 relays. But we still need agents at all the relays, i.e., Zone 1, Zone 2 and Zone 3 because we need all the other relays (Zone 1 and Zone 2) fault status information to categorize a Zone 3 relay fault as a true or falsely perceived fault. One other foreseeable benefit of this scheme

is the identification of hidden failures in these relays. For example, in the above scenario if any of the listed relay pick-ups is not observed or other relays respond, it is an indication of a hidden failure in the relay that has not responded or responded wrongly, in sensing the fault. This scheme can be further extended to supervise Zone 2 protection also, provided reasonable communication delays are present.

4.3 Algorithm

When queried by a Zone 3 slave relay agent, in order to compare the fault status of different relays protecting a transmission line, a master agent must know ahead of time which set of relays are protecting a transmission line. The algorithm for creating master agent comparison rules is as follows:

a) Read power system network data file. We have used IEEE standard data files.

b) Store all the bus numbers from bus data. Also store transmission lines, transformers connected between buses, resistance and reactance of the transmission lines from line data. As explained above calculate the Zone 1, Zone 2 and Zone 3 settings of each relay located at both ends of a transmission line.

c) Convert the given power system network into a graph *G(V,E,R)*. Where v is the set of n vertices and each vertex is denoted *v[i]*. i = 1,2,..n. Where E is the set of m edges and each edge is denoted as *E[j]* where j=1,2,..m, R is the set of 2m relays. Each vertex represents a power system bus and each edge represents a transmission line or a transmission line

connected between buses. E_v is the set of edges connected to a vertex v. Where each edge connected to a vertex is denoted as $E_v[l]$ where l=1,2,..k. R_{xy} represents a relay positioned at vertex x and is monitoring the edge (transmission line) connected between vertices x and y.

d) Depth first search (DFS) is a well known and commonly used searching algorithm in graph theory. From Figure 2.2 it is obvious that the DFS can be applied to find the set of relays protecting a transmission line. For a relay R_{xy}:

i) Store R_{xy} as Zone 1 and Zone 2 relay of edge (transmission line) connected between vertex x and y.

ii) Starting from vertex x by traversing in the direction of vertex y perform a two stage DFS. For all the edges at the end of stage 2, store R_{xy} as the relay offering protection under Zone 3. Two stage DFS for relay R_{12} in Figure 2.2 is shown in Figure 4.3. At the end of stage 2 of DFS, relay R_{12} can be considered as a Zone 3 relay for transmission lines connected between buses 2 and 5, 2 and 7.

Repeat step d) for all the relays in the network. The end result gives the set of Zone 1, Zone 2 and Zone 3 relays protecting all the transmission lines in a given power system network.

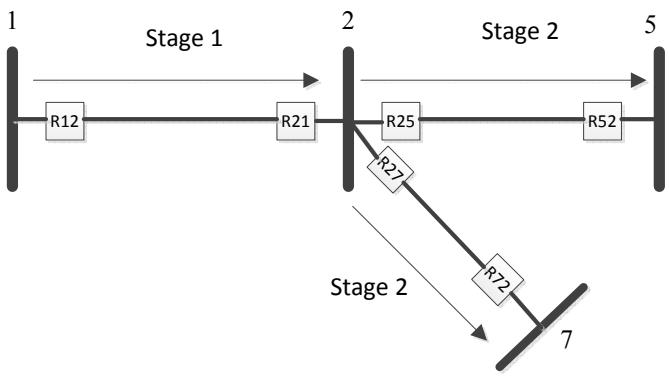

Figure 4.3: Illustration of DFS for relay

4.4 Simulations

The proposed Zone 3 relay supervision scheme is a time-critical application. When faults are observed in Zone 3 relays, relay status checking and breaker cooperation need to be done within a short time slot to prevent failure to propagate and expand. Hence the end-to-end latencies between relays and the master agent become crucial to implement this scheme. Therefore to gain better evaluation of communication latencies, several network infrastructures for the Zone 3 supervision scheme are simulated in network simulator OPNET. In order to evaluate the end-to-end latencies between the master agent and Zone 3 slave agent relays, OPNET modeller networking simulations are performed. As a part of our simulations we explored different network topologies, physical media of communication, network protocols, link bandwidths to find out the best possible combination.

We performed experiments with three different communication network topologies for the

IEEE-39 bus system. In the Type I network, the network topology is assumed to be same as that of the power system topology. In this model, each bus in the power system has a corresponding communication node (router or host) and parallel to each transmission line there is a communication link. We allocate slave agents to buses which monitor the status of relays in their vicinity. In the Type II network, we consider an alternative topology (star topology) in which each bus agent has a dedicated communication link to the master agent. In the Type III network, we examine a more practical network configuration which is shown in Figure 4.4. We assume that a distance protection relay has an agent associated with it that can communicate directly with the master agent. Slave agent relays near a bus/substation are connected in a local area network (LAN) which uses Ethernet as a link layer protocol. Slave agent relays can send messages from one LAN to the other LAN or master agent via routers. The communication links are similar to the Type I network. LAN at a bus connecting multiple relays is as shown in Figure 4.5 [2]. Similar LANs are maintained at all the other buses in the network.

We assume that the communication between a master agent and a slave agent occurs as per the PMU's synchrophasor measurement and communication standard IEEE C37.118 specifications. At present both the PMU and the relay are sold together as a single unit [2] and currently PMU's are being installed in different parts of the US grid. Therefore the main reason for the selection of IEEE C37.118 is that, if Zone 3 relay supervision scheme is officially accepted to be put into practice in real systems, the use of IEEE C37.118 will ease the process of integration of the Zone 3 supervision scheme with traditional distance relaying

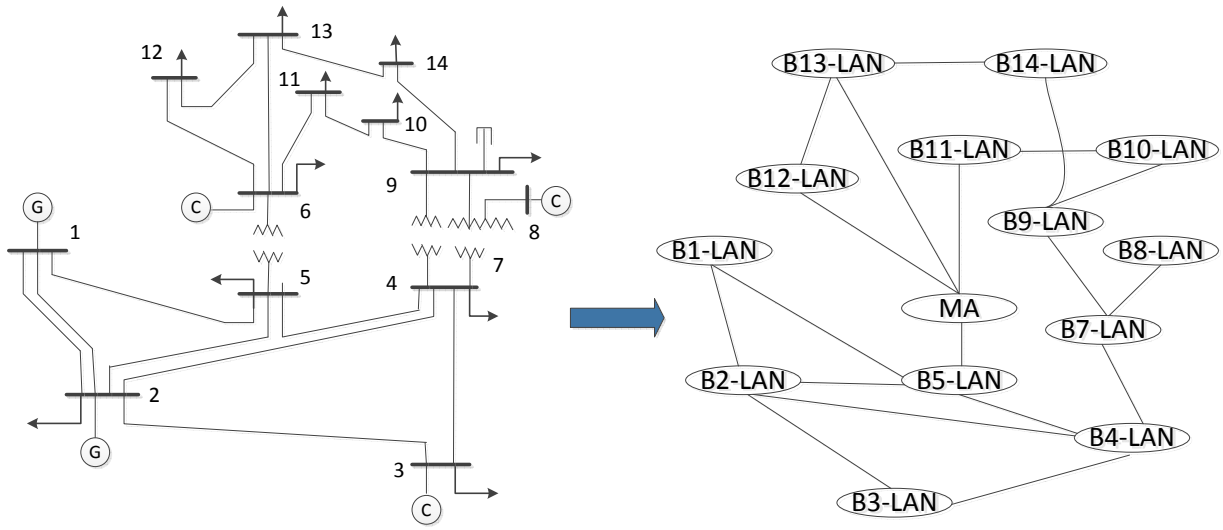

Figure 4.4: Communication architecture (Ethernet WAN) similar to power system network topology connecting LAN's at different substations

scheme. Along with the PMU installation, the communication and networking equipment required to transfer the synchrophasor data from the transmission substation to the control center is also currently being set up. Therefore if properly designed, the Zone 3 supervision scheme can use the same communication and networking infrastructure used for the PMU data transfer which results in financial savings.

UDP and TCP are the widely used protocols for networking simulations. UDP is an unreliable transport protocol but it is a best effort, fast and has less overhead and it is always feasible to add reliability to it at the application layer. TCP is a reliable transport protocol with flow control and congestion control functionality. Both of these two are used in Internet

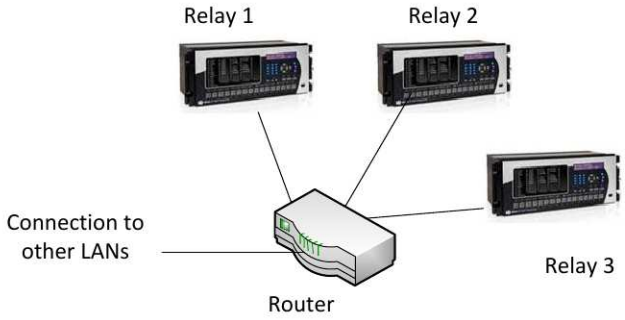

Figure 4.5: Communication mechanism between master agent and slave agents

Table 4.1: Simulation parameters of interest

Parameter	**Value**
Packet Size	52
Packet Arrival Rate	30 times/sec
Average Fiber Length	500 miles
Propagation Speed of Fiber	$2 * 10^8$ m/sec
Fiber Propagation delay	0.0040233(sec)
Fiber Capacity	100 Mbps

at present and are believed to play an important role in smart grid applications. We considered TCP in our simulations as it provides a reliable data transfer. Moreover the database models in OPNET by default use TCP. Three physical media are used to model the communication links in the system including power line carrier, copper line and optical fibre which represent low(1 Mbps), medium (10 Mbps) and high (100 Mbps) bandwidth respectively.

As mentioned in section 4.3, at any given time the master agent has the fault status information of all the slave agent relays reporting to it. In order to store the fault status information, the master agent maintains a database at its location. Whenever a master agent receives a query from a Zone 3 slave agent relay, the total round trip communication

delay between the queried slave agent and the master agent can be split into multiple delays as given by Equation 5.1.

$$t = t_c + t_d + 33 \tag{4.1}$$

where t_c is the round trip delay (msec) just for the purpose of communication between the slave agent and the master agent. t_d is the database access time. Database at the master agent can contain millions of records. One of the major bottle necks for the Zone 3 supervision scheme to be put into practice is the master agent database access time. Accessing a huge database consumes a long time of the order of few hundreds of msec. If performance tuning techniques are used effectively in database design then its access time can be reduced. We assume a database access time of 100 msec. Master agent requires most recent fault status values. Therefore instead of querying the entire database (which stores data collected over months), a separate smaller size database can be maintained to store the most recent fault status values, which relatively requires lesser access time compared to the larger database. Therefore the selected value of 100 msec appears reasonable for the mini database access time. It is aforementioned that a slave relay agent reports fault status to the master agent at 30 times per sec, i.e., new fault status data arrives at the database every 33 msec. Therefore before querying the database, the master agent waits for 33 msec in order to use the most recent fault status information from other slave agent relays. Therefore in OPNET simulations total database access time is set to 133 msec.

Table 4.2: OPNET simulation results - maximum response time from Zone 3 slave agent to master agent

Network Configuration	**Copper**	**Power Line**	**Optical Fiber**
Type I	186	205	175
Type II	160	138	166
Type III	186	187	182

The simulations parameters of interest are as shown in Table 4.1. The propagation speed of copper is same as optical fiber is $2 * 10^8$ m/s. The value of propagation delay used for copper and fiber optic network based simulations is obtained from dividing communication wire length by propagation speed. As per [90], the propagation delay of the power line carrier (PLC) is 0.33 milliseconds per 1000 km. Remaining parameters shown in Table 4.1 are same for all the network configurations. In Table 4.2, the maximum response time from a Zone 3 slave agent to the master agent is given for each of the earlier described three different network configurations. The simulation results are as shown in Table 4.2. All the network configurations satisfy the Zone 3 relay fault clearing time of 1 sec. But for the simulation of large power system networks, we consider Type III network configuration as it appears to be practical for the relays at a substation (bus) to be connected in a LAN and communicate via a router with the external world. It is well known that PLC is a harsh medium and data transfer through it can create a lot of problems [97]. Compared to copper wires, optical fibers are less expensive, experience lower signal degradation and require lower number of repeaters [35]. Therefore we prefer to use optical fiber for the remainder of the OPNET simulations.

Chapter 5

Agent Based Zone 3 Protection Scheme For Larger Power Systems

The post-mortem analysis of few blackouts in U.S. and Europe concluded that the hidden failure induced tripping of distance relays is one of the primary causes of blackouts. In order to provide the distance relays with situational awareness and improve their robustness to hidden failures, a non-intrusive agent based relay supervised distance protection scheme is proposed in the previous chapter and the simulation results seemed satisfactory. The methodology presented in chapter 4 is limited to single master agent and multiple slave agents communication therefore it can only be applied to smaller power system networks. In order to adapt the relay supervision scheme to a geographically widely distributed larger bus system, more than one master agent is required because the use of a single master agent may result in slave agent to master agent round trip communication delays greater than the relay

fault clearing times which defeats the purpose of the relay supervision scheme. Therefore for a larger power grid that needs multiple master agents, finding the number of master agents required and the location of the master agents is an issue that has to be addressed. In this chapter, the problem of minimizing the number of master agents required to serve the slave agent queries and finding an optimum location for the master agents is modelled as a multiple facility location problem. Networking simulations are performed using *OPNET* and optimization models are developed and simulated using *IBM ILOG CPLEX*.

5.1 Problem Description

As shown in Figure 4.4, a single master agent at bus 6 can handle the queries from the Zone 3 slave agents located at all the buses in the network. This is because the power system network shown in Figure 4.4 is small (14 bus system), therefore the round trip communication delay between the master agent and any Zone 3 slave agent in the network is less than one sec, which is the Zone 3 fault clearing time. Practical power system networks consists of a large number of buses (> 1000) and they are geographically spread around long distances (1000's of miles). If a single master agent is employed to serve all the Zone 3 slave agents in a large power grid, the round trip communication delay between the slave agents and the master agent over such long distances can be greater than 1 sec which renders the Zone 3 supervised scheme described in section II to be ineffective in aiding Zone 3 relays to distinguish between a true fault or a hidden failure based fault and respectively to trip or not to trip. Therefore

for the larger bus systems, in order to effectively utilize the Zone 3 distance relay supervisory scheme, the power system network has to be populated with multiple master agents such that the round trip communication delay between any Zone 3 relay slave agent and at least one master agent has to be below one second. If a larger bus system requires multiple master agents, then the problem is to find the minimum number of master agents required and the optimal location for these master agents. The major constraint to minimize the number of master agents is to maintain the round trip communication delay between any Zone 3 slave relay agent in the network and at least one of the master agents to be below 1 sec. Therefore the problem at hand is stated as follows:

"*Given a wide area power system network populated with slave agents at different buses, select a minimum number of slave agents as master agents such that the round trip communication delay between any Zone 3 slave agent relay and at least one master agent is less than one sec.*"

Once a slave agent is selected to be a master agent, it is assigned the extra responsibilities of a master agent as described in chapter 4. A single relay can sense fault in more than one transmission line under different zones of protection. Therefore a relay can be a part of two different relay-sets. A relay-set is defined as the set of relays protecting the same transmission line under different zones of protection. It is possible that all the relays in one relay-set may be reporting to a master agent and relays in second relay-set may be reporting to another master agent. As a result of this single relay which is a part of two relay-sets may end up reporting to two different master agents. This is as shown in Figure 5.1. Slave

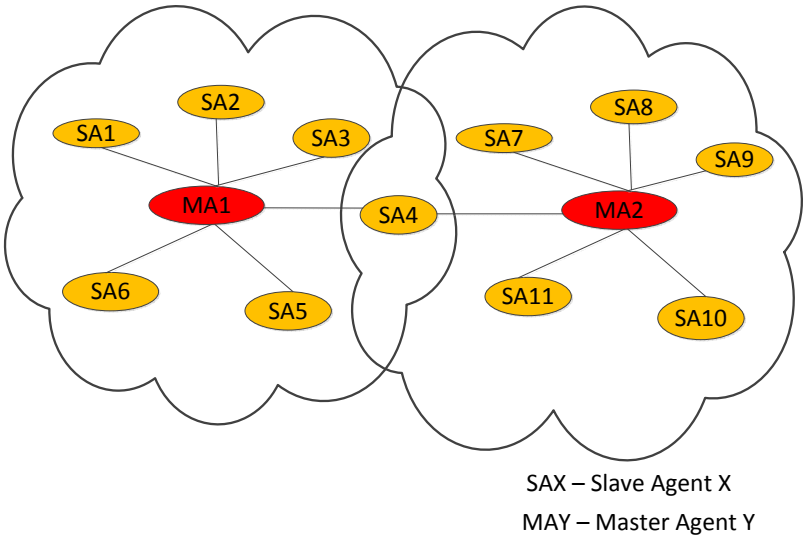

Figure 5.1: Slave agent communicating with multiple master agents

agent 4 is reporting its fault status to both the master agent MA1 and the master agent MA2. In Figure 5.1, just for the purpose of illustration, a single slave agent is shown to be reporting to multiple master agents. But in larger bus systems it is possible that few tens to hundreds of slave agents can be found to be reporting their fault status to more than one master agent. As each slave agent is expected to be reporting fault status at the rate of 30 times per sec, this can result in huge data traffic overhead. Therefore in order to reduce the data traffic, the second objective is to find the optimum location for the master agents such that the number of slave agents reporting to the multiple master agents is minimized while the total number of master agents is maintained same as that obtained by solving the problem formulated above. Therefore the second problem can be stated as follows:

"*Given a wide area power system network populated with slave agents at different buses; find an optimum location for N number of master agents such that the total number of slave agents reporting to the multiple master agents is minimized and the round trip delay between any slave agent and the master agent that the slave agent is communicating with is less than the Zone 3 tripping time of one sec.*"

5.2 Optimization Models

The problem described in section 5.1 is modelled as *multiple facility location* problem which is described in detail in this section. Let N be the number of buses in the power system network. As master agent has to be placed in a LAN at a bus, the number of possible facility (master agent) locations is also N. Let M be the number of relay-sets. The number of relay sets is equal to the number of the transmission lines. The problem is solved in three different phases.

5.2.1 Phase I

Minimize

$$\alpha = \sum_{i=1}^{N} Y_j \tag{5.1}$$

Subject to :

$$\sum_{i=1}^{N} X_{ij} = 1, \forall i \in M \tag{5.2}$$

$$X_{ij} \leq Y_j, \forall i \in M, j \in N \tag{5.3}$$

$$X_{ij} * t_{ij} \leq t_m, \forall i \in M, j \in N \tag{5.4}$$

In phase I, the objective is to minimize the number of master agents (facilities) required to serve all the slave agents (customers) such that the round trip communication delay between any Zone 3 slave agent and atleast one master agent is less than 1 sec. This is given by the Equation 5.1. The constraint in the Equation 5.2 restricts the assignment of a relay-set to one possible master agent. Intuitively Equation 5.2 puts a restriction that all the slave agent relays protecting the same transmission line has to report to a single master agent. If different slave agent relays in a relay-set report to different master agents, in order to acknowledge a query from a Zone 3 slave agent, the master agent may not have enough fault status information from the other slave agents protecting the same transmission line. For example consider a relay-set A,B,C,D,E,F and assume that the slave agent relays A,D are reporting to the master agent MA1 and the remaining slave agent relays B,C,E,F are reporting to MA2. If MA1 receives a query from the slave agent relay A, the response sent by MA1 may not be correct because it doesn't have fault statuses of all the other slave agent relays (except D) from the relay set. In order to obtain the fault statuses of slave agent relays B,C,E,F, master agent MA1 can communicate with MA2. This results in traffic overhead

and higher round trip communication delays (> 1 sec) between the master agent MA1 and the querying slave agent relay A. Moreover this can be considered as a bad communication network design. In order to avoid these complications, Equation 5.2 restricts the slave agent relays in a relay-set to report their fault statuses to the same master agent. The constraint in Equation 5.3 says that a relay-set can only be assigned to one of the N possible locations if that particular location is selected for the placement of the master agent. Equation 5.4 is a very important constraint in the assignment of a relay-set to a master agent which says that a relay-set can only be assigned to a master agent if the round trip communication delay (t_{ij}) between the master agent and all the slave agent relays in a relay-set is less than the Zone 3 relay fault clearing time (t_m).

5.2.2 Phase II

Minimize

$$\beta \tag{5.5}$$

Subject to :

$$\sum_{i=1}^{N} X_{ij} = 1, \forall i \in M \tag{5.6}$$

$$X_{ij} \leq Y_j, \forall i \in M, j \in N \tag{5.7}$$

$$X_{ij} * t_{ij} \leq t_m, \forall i \in M, j \in N \tag{5.8}$$

$$\sum_{i=1}^{N} Y_j = \alpha \tag{5.9}$$

$$\beta \geq \sum_{i=1}^{N} SA_{ij}, \forall j \in N \tag{5.10}$$

$$SA_{ij} \leq Y_j, \forall i, j \in N \tag{5.11}$$

$$NS_{ij} * X_{jk} \leq SA_i k, \forall i, k \in N, j \in M \tag{5.12}$$

In phase I, each relay-set is assigned to a master agent. Relay-set assignment doesn't provide a final solution because in reality slave agent relays in a relay-set report to the master agent but not relay-sets. Therefore in phase II we assign each slave agent relay to a master agent with the objective of minimizing the maximum number of assignments over all the slave agent relays, i.e., the maximum number of master agents that a slave agent relay has to report to is minimized. Equation 5.6, Equation 5.7 and Equation 5.8 are same as Equation 5.2, Equation 5.3 and Equation 5.4 respectively. Equation 5.9 restricts the total number of master agents to be α, i.e., the output of phase I. Equation 5.10 says that a slave agent relay cannot report its fault status to more than β master agents. Equation 5.11 puts a restriction that a slave agent can be set to report to an agent at a bus/substation if and only if that particular location(bus/substation) is selected as a master agent location (facility location). The constraint in Equation 5.12 indicates that if a relay-set (X_{jk}) is assigned to a master agent (Y_k), a slave agent (NS_{ij}) is in that relay-set, assign that slave agent to report to the same master agent (Y_k).

5.2.3 Phase III

Minimize

$$\sum_{i=1}^{N}\sum_{j=1}^{N} NA_{ij} \tag{5.13}$$

Subject to :

$$\sum_{i=1}^{N} X_{ij} = 1, \forall i \in M \tag{5.14}$$

$$X_{ij} \leq Y_j, \forall i \in M, j \in N \tag{5.15}$$

$$X_{ij} * t_{ij} \leq t_m, \forall i \in M, j \in N \tag{5.16}$$

$$\sum_{i=1}^{N} Y_j = \alpha \tag{5.17}$$

$$\alpha \geq \sum_{i=1}^{N} SA_{ij}, \forall j \in N \tag{5.18}$$

$$SA_{ij} \leq Y_j, \forall i, j \in N \tag{5.19}$$

$$NS_{ij} * X_{jk} \leq SA_{ik}, \forall i, k \in N, j \in M \tag{5.20}$$

At the end of phase II, the number of master agents and their location is known and we also know that a slave agent relay X is reporting to the master agent Y. Moreover at this stage, as shown in Figure 5.1 the number of slave agent relays reporting to the multiple master agents can also be found. As a next step in phase III we minimize the total number of slave agents communicating with the multiple master agents while the total number of master agents is

maintained same as in phase II. In simple terms the difference between phase II and phase III is that, at the end of phase II the placement of master agents (facilities) can be such that slave agents (customers) A, B, C and D are reporting to 1, 2, 3 and 4 number of master agents respectively, i.e., total slave agent to master agent fault status data transfers is 10 whereas the phase III may find a location for the master agents such that the slave agents A, B, C and D could be reporting to 2, 1, 3, 2 number of master agents respectively, i.e., total slave agent to master agent fault status data transfers is 8. It is aforementioned that each slave agent reports fault status 30 times/sec to a master agent. Therefore decreasing the number of data transfers from 10 to 8, i.e., 2 can result in a reduction of 60 (2 * 30) data packet transfers/sec. For larger bus systems if the number of such reduced data transfers from phase II to phase III is of the order of hundreds then a significant reduction in packet data transfer can be achieved. Thus phase III attempts to minimize the total number of slave agent to master agent packet data transfers and aids in efficient communication network design. All constraints in phase III are similar to phase II except the constraint in Equation 5.18, which indicates that the maximum number of master agents that a slave agent is assigned to cannot be greater than α.

5.3 IBM ILOG CPLEX Simulations

The end-to-end communication delays between the master agent and the Zone 3 relay slave agents are obtained by performing OPNET simulations similar to those discussed in chapter

Table 5.1: Format of the data collected from OPNET simulations

MAL	t_{i1}	t_{i2}	t_{i3}	t_{i4}	.	.	.	t_{iN-1}	t_{iN}
1	t_{11}	t_{12}	t_{13}	t_{14}	.	.	.	t_{1N-1}	t_{1N}
2	t_{21}	t_{22}	t_{23}	t_{24}	.	.	.	t_{2N-1}	t_{2N}
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.		.
N	t_{N1}	t_{N2}	t_{N3}	t_{N4}	.	.	.	t_{NN-1}	t_{NN}

4. IEEE 9 bus, IEEE 14 bus, IEEE 30 bus and IEEE 57 bus system are considered as test inputs for OPNET simulations. An Ethernet wide area network (WAN) as shown in Figure 4.4 is designed for each of the above mentioned IEEE bus systems and networking simulations are performed. Similar to the chapter 4 simulations, the communication between a master agent and a slave agent occurs as per the PMU's synchrophasor measurement and communication standard IEEE C37.118 specifications. Also the simulation parameters are same as that of Table 4.1 in chapter 4. For a given test input, at the end of networking simulations the data collected from OPNET is as shown in Table 5.3. The data is in the form of $N * N$ matrix, where N is the number of buses in the power system network. MAL is the master agent location. t_{ij} is the round trip communication delay between the slave agent at location j and the master agent at location i.

IBM ILOG CPLEX is a tool for modelling and simulating optimization based analytical decision support applications [65]. The data collected from the OPNET simulations is modified in order to generate a suitable input for the CPLEX simulations. Using the DFS algorithm described in chapter 4, relay-sets are generated for all the transmission lines in a given power

Table 5.2: IBM ILOG CPLEX simulation results

No	**Bus Systems**	**NMA**	**Slave Agent Assignments**	
			Phase II	Phase III
1	9	1(5)	54(5)	54(5)
2	14	1(14)	120(1)	120(1)
3	30	1(30)	246(1)	246(1)
4	57	2(38,49)	678(31,38)	462(28,38)
5	118	4(17,32,65,94)	2424(17,44,70,100)	1914(17,38,69,96)

system network. Actually a relay-set is a set of sets. The number of individual sub-sets in a relay-set is equal to the number of transmission lines. Each sub-set indicates the set of relays protecting a transmission line under different zones. Also the size of the each sub-set depends on the power grid topology, i.e., depending on the power system network topology different transmission lines may be protected by different number of relays. The relay-set information and the communication round trip delays are given as input to CPLEX. Optimization models described in section 5.2 are created in CPLEX using the OPL modelling language. The OPNET networking simulation files and CPLEX optimization models can be found at www.filebox.vt.edu/users/gshra09/facility.zip.

The results obtained from CPLEX simulation are as shown in Table 5.3. The optimization models presented in section 5.2 are tested using IEEE 9, IEEE 14, IEEE 30, IEEE 57 and IEEE 118 bus systems as inputs. In the distance relaying protection scheme, the Zone 3 fault clearing time is 1 sec, i.e., during CPLEX simulations the parameter t_m used in phase I, II and III optimization models has to be set to 1 sec. We have used smaller bus systems as test inputs. The maximum round trip communication delay for IEEE 118 bus sytem

(largest test input) is 279 msec which is less than 1 sec. If we set $t_m = 1sec$, for all the test inputs the simulation results indicate that the number of master agents (NMA) required is one. Therefore just for the purpose of illustration the value of t_m is reduced from 1000 msec to 200 msec. Off course, if you have access to larger power system network containing thousands of buses t_m can be to 1 sec. As shown in Table 2, with $t_m = 200msec$ IEEE 118 bus system requires 4 master agents, IEEE 57 bus system requires 2 master agents whereas a single master agent can meet the timing requirement for IEEE 9, 14 and 30 bus systems. At the end of phase I, the location of master agents for IEEE 57 bus system is at buses 38 and 49. The total number of slave agent to master agent communications at the end of phase II is 678 with master agent locations 31 and 38 whereas at the end of phase III the number of slave agent to master agent communications is reduced to 426 and the master agent locations are shifted to 28 and 38. Therefore the advantage of using the phase III is obvious, which resulted in a significant (252 i.e. 30%) reduction of slave agent to master agent communications while the number of master agents is maintained same as that of the phase II. The optimized locations for the master agents are Local Area Network(LAN) at buses/substations 28 and 38. Similarly for IEEE 118 bus system the reduction in the number of slave agent to master agent data transfers from phase II to phase III is 510 which is around 20%.

Chapter 6

Formal Verification of Agent Based Distance Relaying Protection Scheme

In previous chapters hierarchically distributed non-intrusive agent aided transmission line distance relaying protection scheme has been proposed. This scheme is meant to provide the distance relays with situational awareness and improve their robustness against hidden failures. Distance relaying protection scheme is a part of safety critical cyber physical system (in particular, power system) and it operates with stringent timing requirements to remove the faulted line out of service. Before putting into practice, it is better to formally verify that the agent based relay supervisory scheme meets the specifications and its usage gives intended results and doesn't carry any negative side effects. Therefore, in this chapter agent based relay supervision scheme is formally modelled, validated and its properties are verified using UPPAAL - a timed automata based formal verification tool.

6.1 Model Checking of Real Time Systems

This section provides a brief overview of real time systems, model checking and UPPAAL software.

6.1.1 Real Time Systems

A real time system can be defined as a system in which certain tasks or operations have guaranteed minimum and/or maximum response times [47]. In other words correct functioning of the system depends not only on the results produced but also on the time instance at which the result is obtained [44]. Examples of real time systems are nuclear power plant, aeronautic controllers, pacemakers, video games, distance relaying protection scheme and multimedia streaming applications etc. In a real time system, state of the system progresses with time and needs to be sensed and controlled with computing systems. Quality of Service (QoS) and end-to-end timing constraint are the two parameters that play a significant role in successful functioning of a real time system. Tasks in a real time system can be categorized as hard real time tasks and soft real time tasks. Hard real time tasks must strictly meet timing constraint. A failure to meet timing constraint in a hard real-time task may lead to a fatal error. For example, in the presence of a fault distance relaying protection scheme must trip the line out of service within 1 sec, otherwise fault may spread to other parts of the system and lead to irreparable damage of the expensive equipment such as generator and transformer blow out etc. Therefore the task of the distance relaying protection scheme to

trip a faulted line out of service is considered as a hard real time task. Hard real time task is also known as critical task. On the other hand soft real time task can be completed at any time. Soft real time task can be considered as non-critical task. For example assuming that the fault is cleared automatically by the protection equipment, providing the time of occurrence of a fault and fault related information to the operator present at the control center may be delayed by few seconds or minutes as it is a non-critical task.

6.1.2 Model Checking

Model checking is a technique for verifying properties (deadlock free, safety etc.) of a system. In model checking system behaviour is modelled as a state machine (automaton) and its properties are verified. Here system can be a software system, hardware system, real time system and electro-mechanical system etc. Clarke and Emerson pioneered the model checking of hardware and software systems using temporal logic formula [27] [21]. Clarke and Emerson research work is mostly applied for finite state systems. Alur and Dill proposed the theory of timed automata to model and verify real time systems [8] [7]. Henzinger et al proposed a simplified version of timed automata known as timed safety automata [40].

6.1.3 UPPAAL

Based on the theory of timed automata and timed safety automata, Larsen et al developed UPPAAL a tool for modelling, simulation and verification of real time systems modelled

as networks of timed automata [10]. Properties of the system to be verified are specified in timed computation tree logic (TCTL). UPPAAL has been used in verification of wide variety of real time systems such as Gearbox controller, multimedia systems, web services business activity protocol, QoS management in wireless systems, mutual exclusion protocol, Philips audio control protocol etc [10]. For a detailed tutorial and explanation of UPPAAL refer to [50].

6.2 Modelling Behaviour

Because of strict timing requirements for the proper functioning of distance relays, time based formal models are needed, and UPPAAL allows us to model these in the form of timed automata, and allows model checking of timed properties on the models. To the best of our knowledge this is the first instance of applying formal verification to the protection scheme in a power system.

In UPPAAL the model of system's behaviour is expressed as the composition of the behaviour models of its individual components. The main components of the agent aided distance relaying protection scheme are sensors (CT and VT), Zone 1 relay, Zone 2 relay, Zone 3 relay, breakers, slave and master agents. There exist two different models for both the sensor and the breaker. The reason for this is as follows: Zone 3 relay operates when both Zone 1 and Zone 2 relay fail and/or their associated both breakers or sensors fail simultaneously. Practically it is possible that the Zone 3 relay and its sensor and breaker equipment

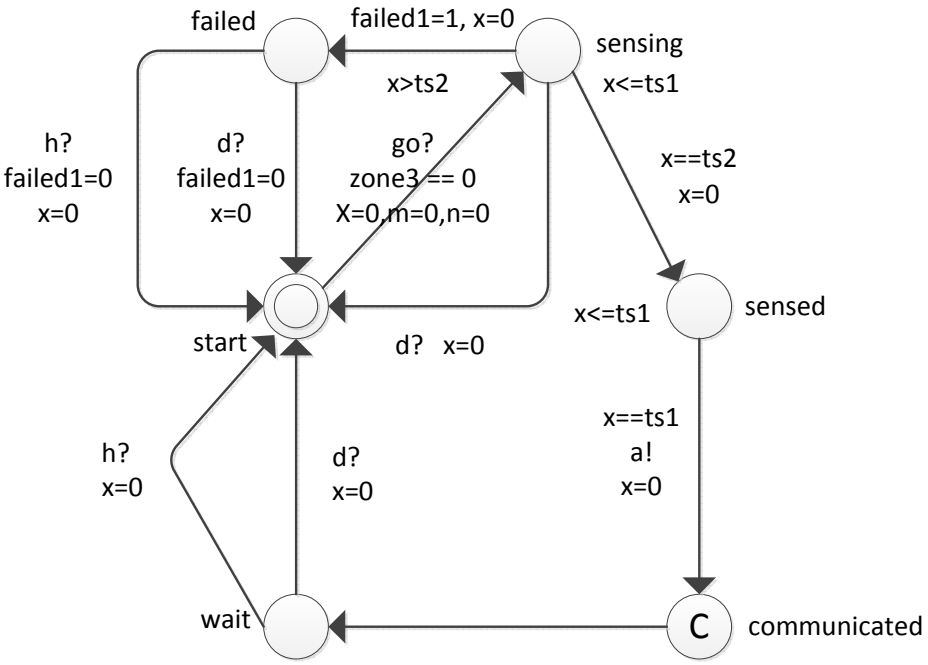

Figure 6.1: Sensor1 automaton

can fail but we didn't consider this scenario in our model. The main reason being the probability of Zone 1, Zone 2 and Zone 3 relays failing simultaneously is very low. Moreover Zone 3 is the only backup available. If we consider the case where Zone 3 relay also fails along with Zone 1 and Zone 2 relay we cannot successfully verify the distance relaying scheme. Hence the case of either Zone 3 relay or its sensor or breaker failure is not considered. Therefore the Sensor 1 and the Breaker 1 models have *failed* state whereas the Sensor 2 and the Breaker 2 models do not have *failed* state. Sensor 1 and Breaker 1 model the behavior of the sensor and the breaker associated with Zone 1 and Zone 2 relays. Whereas the behavior of the sensor and the breaker of the Zone 3 relay are respectively presented in the Sensor 2 and the Breaker 2 models.

A reset transition moves an automaton from any state to the *start* state. The following two

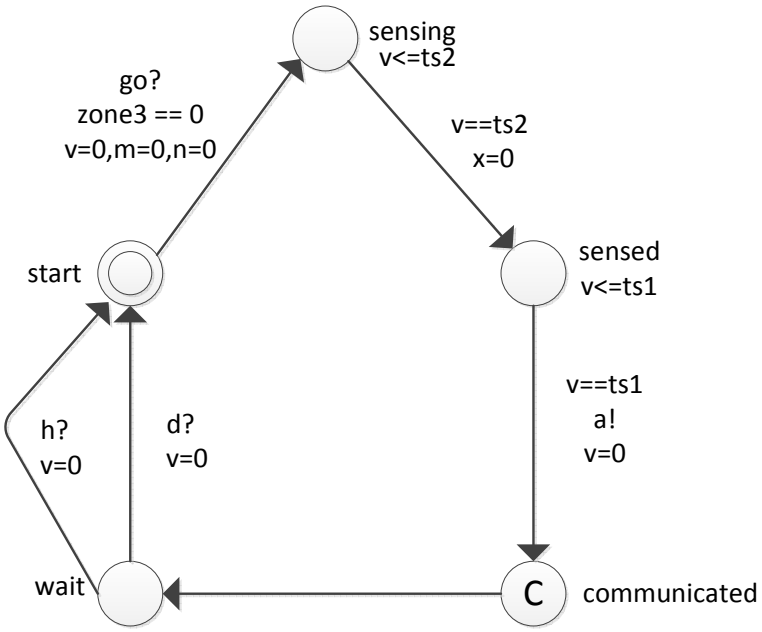

Figure 6.2: Sensor2 automaton

reset transitions are used by all the automatons described in this section. These two reset transitions are used multiple times to explain the behaviour of all the automata. Instead of rewriting these transitions many times they are just explained once here. At this point they may or may not be clearly understood but by the end of this section their relevance should become apparent.

1. *Reset I*: In our system model, when breakers at both ends of the line trip, a reset signal is sent via the broadcast channel d to all automatons to move to the *start* state. As shown in Figure 2.2 a transmission line is protected by Zone 1, Zone 2 and Zone 3 relays in both the directions. At least two relays, i.e., one relay per direction have to trip in order to remove a faulted line out of service. In total there are at least six relays protecting a transmission line. Depending on which relay out of these six relays trip's

last, any of the six breakers can send a reset signal via the urgent broadcast channel *d* to reset the whole system.

2. *Reset II*: If any of the Zone 3 relay senses no fault, then it moves from the location *calculate* to *nofault* transmitting a *nofault* signal via the broadcast channel *nf*. The remaining Zone 1, Zone 2 and Zone 3 relays receive the signal via the broadcast channel *nf* and move to *nofault* state. Zone 3 relay moves from *nofault* to *start* state by transmitting a reset signal on the broadcast channel *h*. All the automata move from their current location to *start* state after receiving a reset signal on the broadcast channel *h*.

In the following description of timed automata words *state* and *location* are used interchangeably and they both mean the state of an automaton.

a) Sensor 1: Both the current and the voltage transformer are modelled as a single sensor. Timed automaton model of Sensor 1 is as shown in Figure 6.1. It uses the clock x to measure time. Sensor 1 moves from initial state *start* to the *sensing* state via the urgent channel *go* if the boolean variable *zone3==0*. If *zone3==0* it is an indication that all automatons are in start state. Also during this transition integer variables m and n are set to zero. These two variables are used by the master agent. If Sensor 1 is functioning correctly, it senses the current and the voltage values within *ts2* msec and moves from the state *sensing* to *sensed*. On the other hand if Sensor 1 is malfunctioned it will make a transition from the *sensing* state to the *failed* state in the time interval *(ts2, ts1)*. Automaton can move from *failed* to

start state via *Reset I* or *Reset II*. If Sensor 1 makes transition from the location *sensing* to *sensed*, within *ts2* msec it sends the voltage and the current values to the respective relay via the synchronization channel *a* and moves to the committed location *communicated*. In networks of timed automata describing a system if any automaton is in a committed location next transition is from that location. Committed location is used in the execution of atomic sequence. From the committed location *communicated*, Sensor1 makes a transition to the *wait* state via the urgent channel *go*. Automaton can move from the *wait* to *start* state via *Reset I* or *Reset II*.

b) Sensor 2: The behavior of the Sensor 2 is similar to that of the Sensor 1 except that the former doesn't have the *failed* state. Timed automaton of the Sensor 2 is as shown in Figure 6.2.

c) Zone 1 Relay: Timed automaton of Zone 1 Relay is as shown in Figure 6.3. It uses the clock *z* to measure time. It receives the current and the voltage values from the Sensor 1 via the synchronization channel *a* and moves to the *calculate* state from the *start* state. Relay consumes *tz2* to *tz3* msec of processing time to find out if the transmission line protected by it is faulty or not. If there is a fault in the transmission line, Zone 1 relay moves from the state *calculate* to *faulty* within the time interval *(tz2, tz3)*. During this transition boolean variables *fault1, fault2* are set and a fault signal is sent to the slave agent associated with the relay via the communication channel *e*. It is aforementioned that in order to remove a faulted line out of service relays at both ends of the line have to sense and respective breakers have to trip. The Boolean variables *fault1* and *fault2* provide the fault status of the relays

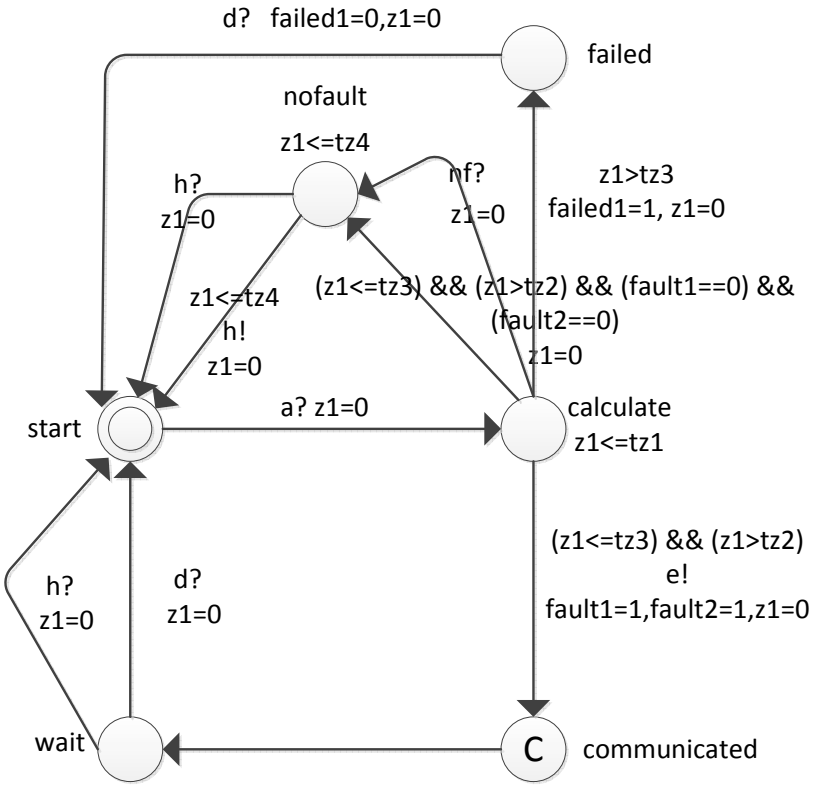

Figure 6.3: Zone 1 Relay automaton

at both ends of the line. Initially both *fault1* and *fault2* are set to zero indicating a no fault condition. Whenever system (relay) senses a fault both *fault1* and *fault2* are set to one. The breaker trip at one end of the line resets *fault1* while the breaker trip at the other end of the line sets *fault2* to zero which removes the fault from the system.

On the flip side if there is no fault then relay makes a transition from the state *calculate* to *nofault* via *Reset II* if the Boolean variable *fault1* is not set. If *fault1* is already set, it is an indication that the system has already detected the fault via Zone 2 or Zone 3 relay and Zone 1 relay cannot move to *nofault* state. Zone 1, Zone 2 and Zone 3 relays all operate simultaneously until fault detection stage and detect the fault within the time interval *(tz2,*

tz3). The main difference in Zone 1, Zone 2 and Zone 3 relay models is the time instance at which they send tripping signal to their respective breakers. So, in the presence of a transmission line fault it is hard to predict which relay can first detect that fault and set the *fault1* variable. Thus it is necessary to check if *fault1* is set before moving from the state *calculate* to the state *nofault*. If Zone 1 Relay is malfunctioned, it does not respond in the time interval *(tz2, tz3)* and makes a transition to the *failed* state in time interval *(tz3, tz1)* and sets the Boolean variable *failed1* giving an indication that the relay has failed. Relay makes transition from the *failed* state to the *start* state when it receives a reset signal on the broadcast channel d via *Reset I*. During this transition it resets the Boolean variable *failed1*. A communication delay of $tz4$ msec is involved in sending a trip signal from a relay to the breaker. So, with a delay of $tz4$ msec Zone 1 Relay automaton moves from the state *faulty* to *communicated* sending a trip signal to its breaker via the synchronization channel b, then moves to the *wait* state via the urgent channel *go*. Automaton then makes a transition from the *wait* to the *start* state via *Reset I*.

d) Zone 2 Relay: Timed automaton of Zone 2 Relay is as shown in Figure 6.4. It uses the clock z_2 to measure time. Transitions from the state *start* to *faulty* are similar to that of Zone 1 Relay with few changes. First, the Boolean variable *failed1* is replaced with the Boolean variable *failed2*. Second, the *faulty* state is a committed location. From the *faulty* state automaton makes a transition to the *wait1* state. If the breaker of Zone 1 Relay trips and resets the *fault1* variable, it is an indication that the system is fault free and Zone 2 relay moves to *start* state in time interval $[0, t2)$ msec by transmitting a signal via the urgent

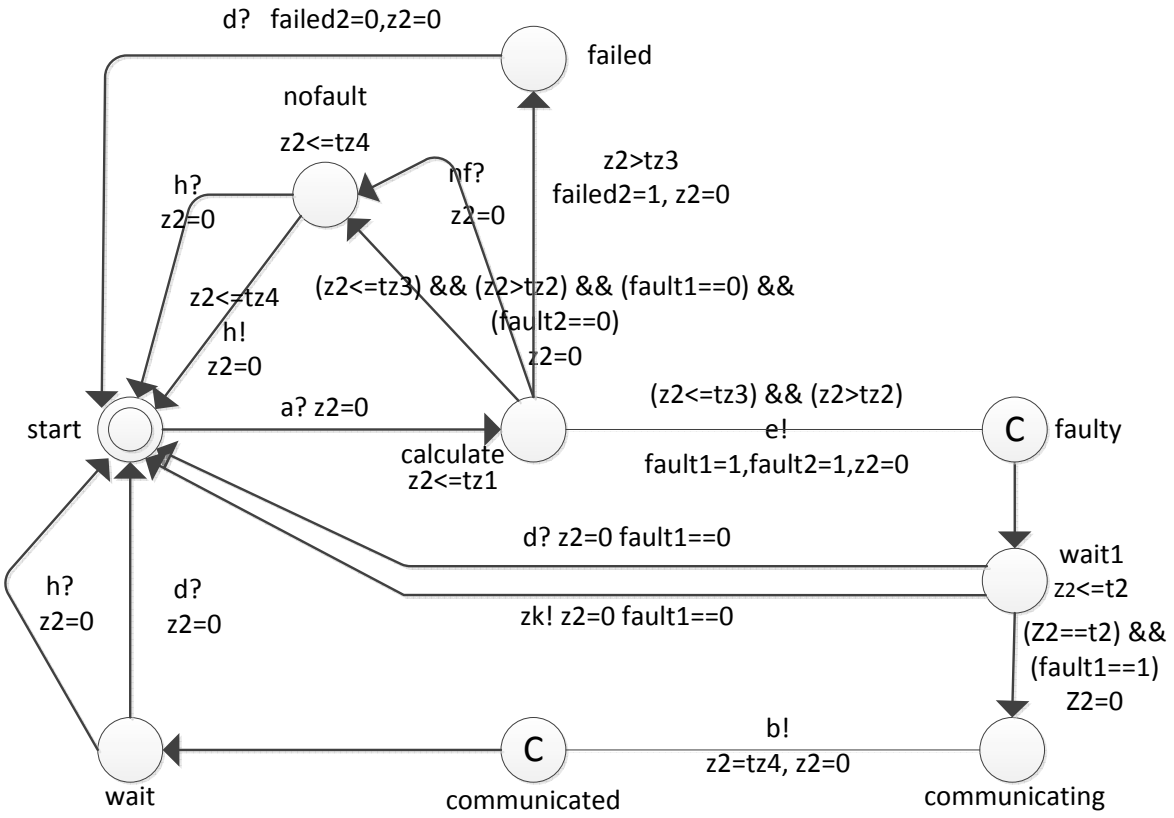

Figure 6.4: Zone 2 Relay automaton

channel *zk* or by receiving a *Reset I*. If the breaker associated with Zone 1 relay doesn't trip within a communication delay of t_2 Zone 2 Relay moves to the *communicating* state from the *wait1* state to send a trip signal to its breaker. Zone 2 Relay automaton makes a transition from the *communicating* to the *communicated* state with a delay of tz4 msec. During this transition Zone 2 Relay sends a trip signal to its breaker via the synchronization channel *b*, and then moves to the *wait2* state via the urgent channel *go*. Automaton then makes a transition from *wait* to the *start* state via *Reset I*.

e) Zone 3 Relay: Timed automaton of Zone 3 Relay is as shown in Figure 6.5. It uses the clock z_3 to measure time. Zone 3 relay automaton behavior is almost similar to that of Zone

2 Relay, except that it doesn't have *failed* state. The other change is that the variable $t2$ is replaced with the variable $t3$. When Zone 3 relay is in *wait1* state, within the coordination delay $[0, t3)$ if the breaker associated with either the Zone 1 or Zone 2 relay doesn't trip, Zone 3 relay moves to the *communicating* state and sends a signal to its breaker to trip the line out of service.

f) Breaker 1: Timed automaton of Breaker 1 is as shown in Figure 6.6. Automaton uses the clock y to measure time. Breaker 1 is initially in the *start* location. Automaton receives a trip signal from its associated relay via the channel b and makes a transition from the location *start* to *received*. After receiving the trip signal from the relay, breaker and its associated electromechanical machinery trips a line out of service with a delay of tb1 msec. So, assuming that the breaker is functioning correctly automaton moves from the state *received* to the committed location *intermediate* in tb1 msec and resets the *fault1* variable, indicating that the line is tripped. If a transmission line is faulty then breakers at both ends of the line have to trip to remove the line out of service. So, to make a transition from the state *intermediate* to *tripped*, automaton performs a check to find out if the breaker on the other end of the line has tripped or not. If it is tripped *fault2* is reset otherwise *fault2* is set. Irrespective of whether *fault2* is set or reset automaton makes a transition from location *intermediate* to *tripped*. But if *fault2* is reset, automaton while making a move from the state *intermediate* to *tripped* transmits a faultfree signal via the channel c to the observer automata, giving an indication that the system is free of fault. When automaton is in *received* state, if the breaker doesn't respond for more than $tb2$ msec then it moves to

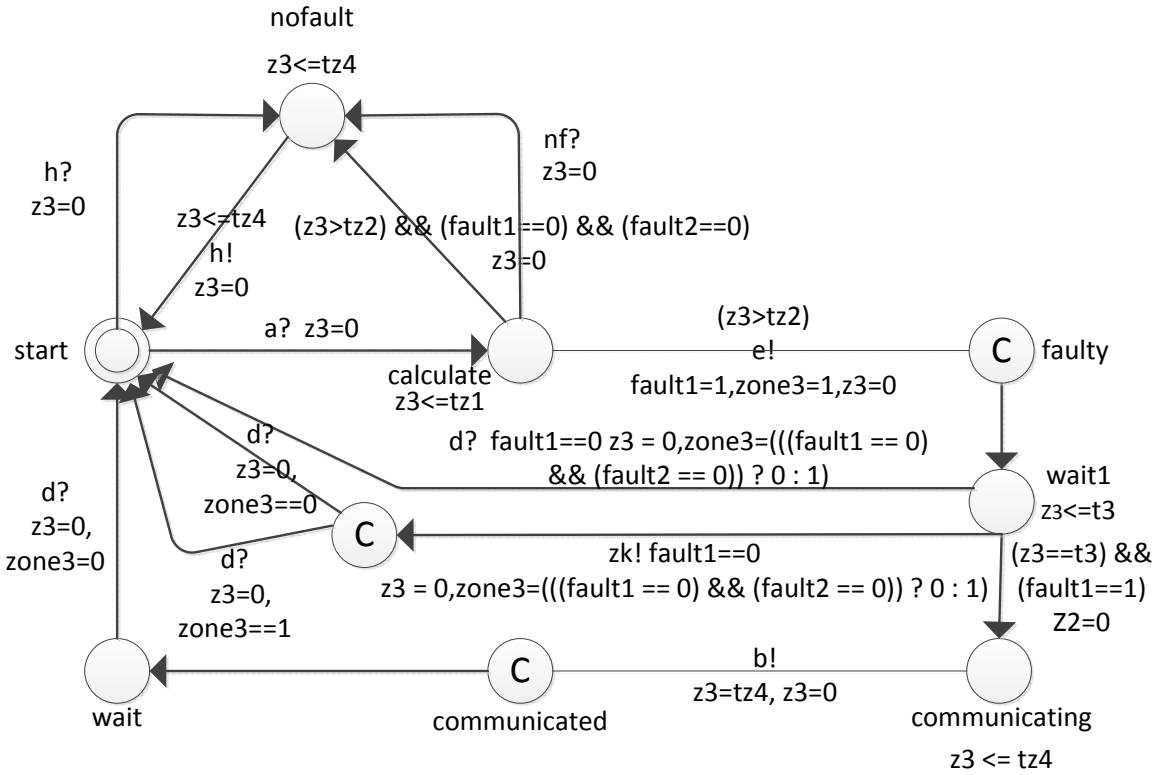

Figure 6.5: Zone 2 Relay automaton

failed state in time interval $[tb2, tb1)$. From the *failed* state breaker can make transition to the *start* state via *Reset I*. Transition from the location *tripped* to *start* occurs when both the Boolean variables *fault1* and *fault2* are reset. Also during this transition automaton sends a reset signal via *Reset I*.

g) Breaker 2: Timed automaton of Breaker 2 is approximately similar to that of Breaker 1 with the only change being Breaker 2 doesn't have a *failed* state. It is as shown in Figure 6.7.

h) Observer automaton (OA): Observer automata captures the high level behaviour of the

distance relaying protection scheme, i.e., whether the system is *faultfree* or *faulty*. As shown in Figure 6.8 observer automata has only 2 states, i.e., *faultfree* and *faulty*. Automaton is initially in *faultfree* location. When Zone 1 or Zone 2 or Zone 3 Relay senses fault, they transmit fault signal n channel *e*. OA listen's it and moves to the *faulty* location. Transition from the state *faulty* to *faultfree* occurs when the automaton receives a reset signal via *Reset I*.

i) Helper automaton: As shown in Figure 6.9 helper automaton has two transitions and one state. Whenever any automata has to make an urgent transition, helper automata sends a signal via the urgent channel *go* and other automata listens and makes a transition. Similarly Zone 2 and Zone 3 Relay make an urgent transition from the state *wait1* to the *start* state via the urgent channel *zk*.

j) Slave agent: Similar to the sensor and the breaker models there exist two different models for the slave agent. Slave agent 1 is used to model the behaviour of the agent located at Zone 1 and Zone 2 relay. Timed automaton of the slave agent 1 is as shown in Figure 6.10. Slave agent 1 records the outcome of the relay execution algorithm, records it and reports it to the master agent so that the latter's database is up to date. The current state of the art relays can communicate at 30 times/sec, i.e., they can transmit new fault status every 33 msec. Therefore the master agent receives a new fault status from a slave agent 1 every $delay1 = 33$ msec. In our model we declared a global variable *afault* for each slave agent and it is updated with a delay of 33 msec. As slave agent's *afault* variable is declared as global, master agent also has access to it. By declaring *afault* variable as global, model is simplified

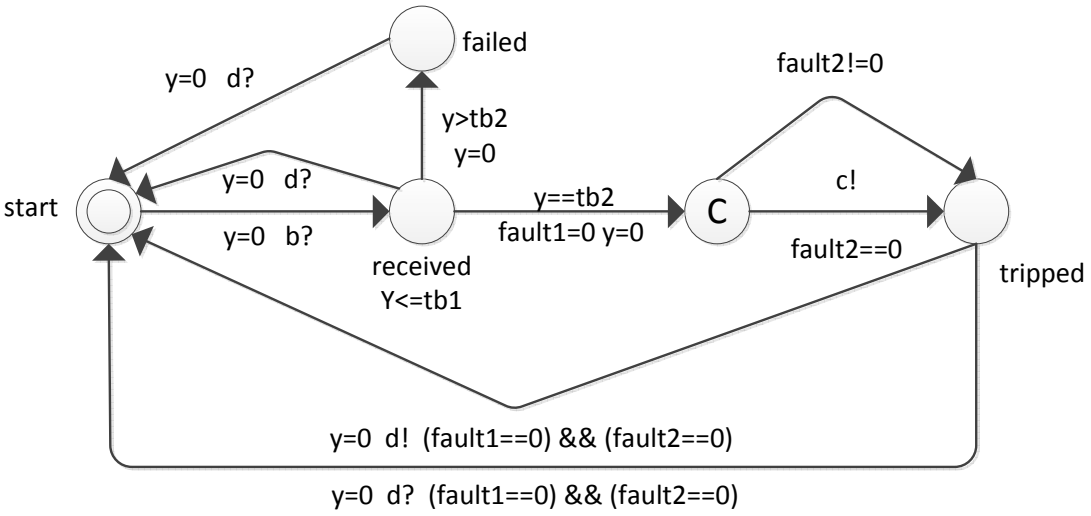

Figure 6.6: Breaker1 automaton

as fault status value passing is avoided between the master agent and the slave agent.

Timed automaton of Slave agent 2 is as shown in Figure 6.11. The behaviour of the agent associated with Zone 3 relay is modelled by the Slave agent 2. Slave agent 2 makes a transition from the state *start* to *received1* after receiving a fault signal from the Zone 3 relay. Similar to the Slave agent 1 fault variable *afault* of the Slave agent 2 is updated with a delay of $delay1 = 33$ msec. Automaton moves from the location *received1* to the committed location *sent* with a delay of 33 msec and sends a fault status update signal via the synchronization channel f to master agent. Then Slave agent 2 makes a transition from the committed location *sent* to the normal location *wait*. In the *wait* state automaton waits for the reply from master agent to confirm if the fault sensed by the Zone 3 relay associated with the Slave agent 2 is a true fault or a hidden failure induced fault. When automaton is

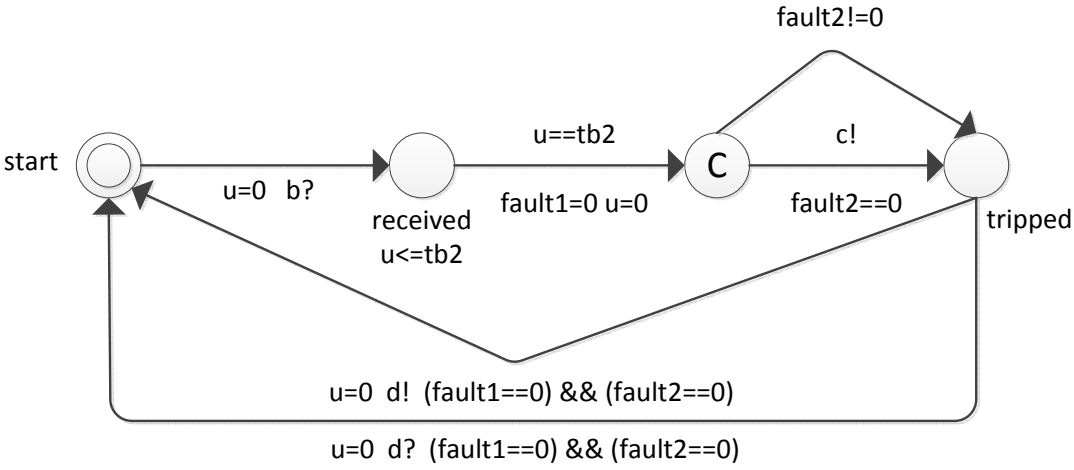

Figure 6.7: Breaker2 automaton

in the *wait1* state, there is a possibility of three different transitions.

1. If either the Zone 1 or Zone 2 relay clears fault, Slave agent 2 makes a transition to the *start* state. When the master agent sends a signal to the Slave agent 2 via the synchronization channel g about whether the fault is a true fault or a hidden failure based fault, Slave agent 2 listens and moves from the location *wait* to the committed location *received 2*. Slave agent 2 then moves from the committed location *received2* to *start*. During the transition from the state *wait* to *received2* boolean variable *fault1* is updated by *function1()*. If the fault is a hidden failure induced fault, *function1()* resets *fault1* variable and if the fault is a true fault, *fault1* variable is set. It is aforementioned that a fault in a transmission line can be sensed by atleast six different relays. As each relay has a slave agent associated with it, atleast six slave agents report to the master

agent about the fault status in a line. In *function1()* boolean variable *afault* of Slave agent 2 is compared with *afault* variables of five other slave agents. If at least half (3 out of 6) *afault* variables are set to 1, it is an indication that the transmission line is faulty and the boolean variable *fault1* is set to 1 and the breaker associated with the Zone 3 Relay can trip if both the Zone 1 and the Zone 2 relay breakers fail to trip. On the other hand if more than half (>3 out of 6) of the *afault* variables are set to zero, it is an indication that there is no fault in the line then the Boolean variable *fault1* is set to zero and it is not required for the Zone 3 relay's breaker to trip. If the sensor or the relay fails the respective slave agent's *afault* variable is not taken into consideration in the above decision making which is implemented by *function1()*.

2. If Slave agent 2 is waiting for an acknowledgement from the master agent, it is possible that a breaker associated with the Zone 1 or Zone 2 relay to trip. Therefore it is not required by the slave agent 2 to wait for the fault classification signal from master agent. In this case the transition from *wait* to *start* can occur in two different ways. If Zone 3 relay interprets that either the Zone 1 or Zone 2 relay has tripped and *fault1==0*, slave agent 2 receives a reset signal on the urgent broadcast channel *zk* and it moves from *wait* to *start* state. This is known as *Zone 3 Reset*. item The transition from *wait* to *start* state can occur via *Reset I*.

k) Master Agent: The behaviour of the master agent is modeled using two timed automatons. The master agent stores the requests in a queue as they are received and processes them based on the First in First Out (FIFO) order. As shown in Figure 6.12 the master

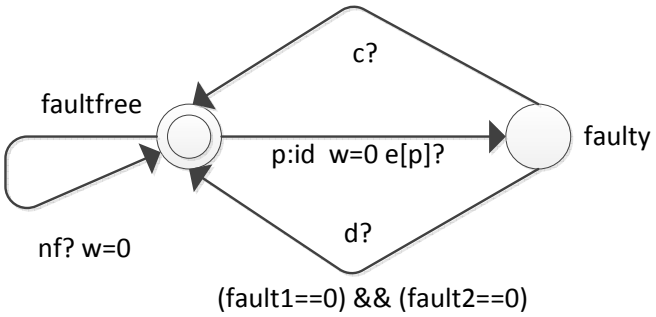

Figure 6.8: Observer automaton

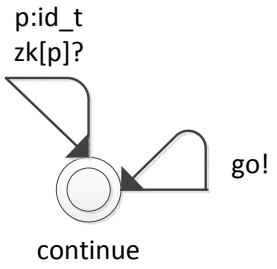

Figure 6.9: Helper automaton

agent receives requests from Slave agent 2 via the synchronization channel f and appends it to queue using the *enqueue()* function. The received request is processed by the master agent task execution timed automaton shown in Figure 6.13. Whenever a request is received, length of the queue *len* is greater than zero and automaton moves from the initial location start to evaluate. There are three possible transitions from *evaluate* state:

1. While Slave agent 2 of Zone 3 relay is waiting to receive a trip/no trip signal from the

master agent, breakers associated with either the Zone 1 relay or Zone 2 relay at both ends of the line may trip and reset *fault1* and *fault2* variables. In this case the master agent deletes from its queue the Zone 3 relay Slave agent 2 queries at both ends of the line and moves from the *send* to *start* state.

2. A slave agent is capable of transmitting new fault variable every 33 msec. Therefore a maximum delay of 33 msec is allowed for master agent to process a request. Also, a database query time of 100 msec is assumed in OPNET simulations. A detailed justification is provided in [83] for the selection of database query and master agent service time. Hence the total master agent delay in processing a single query is 133 msec. Therefore the master agent automaton moves from *evaluate* to *send* state approximately in 133 msec.

3. The third possible transition is from *evaluate* to *start* state via the *Zone 3 Reset*.

Automaton can move from the *send* state to *start* state via four different transitions.

1. Within *delay1* msec, master agent processes the next query in queue and sends a reset signal on the channel *g*.

2. The second possible transitions is via *Reset I*.

3. The other two possible transitions are due to *Zone 3 Reset*.

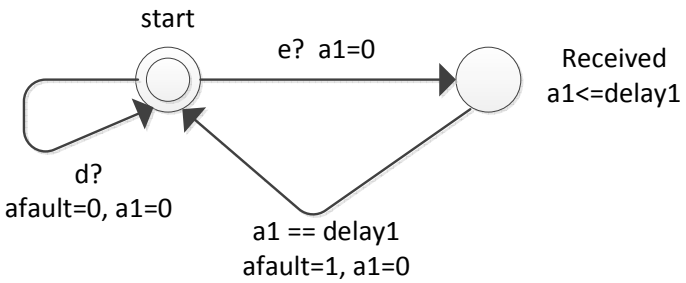

Figure 6.10: Slave agent 1 automaton

Table 6.1: Timing values

Parameter	**Before Scaling**	**After Scaling**
ts1	2	-
ts2	1	-
tb1	21	-
tb2	20	-
tz1	8	-
tz2	2	-
tz3	6	-
tz4	4	-
t2	268	33
t3	968	121
delay	133	17
delay1	75	10

6.3 Verification

The description of the complete model can be downloaded from www.filebox.vt.edu/users /gshra09/agents.zip. This section explains the properties of the agent based Zone 3 relay supervision scheme that are verified. In UPPAAL Timed Computation Tree Logic (TCTL) is used to specify system properties. Sensor1t(2t,3t) and Breaker1t(2t,3t) are the sensor and the breaker associated with the Zone1t (Zone2t,Zone3t) relay protecting the line at one end

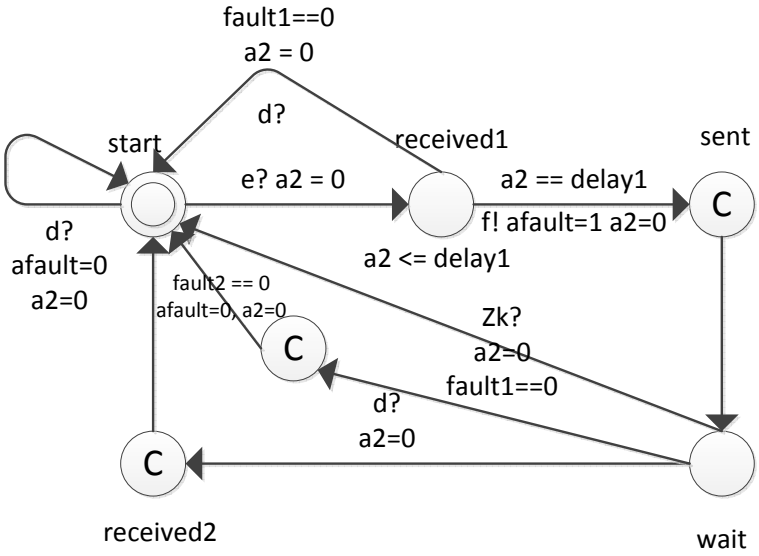

Figure 6.11: Slave agent 2 automaton

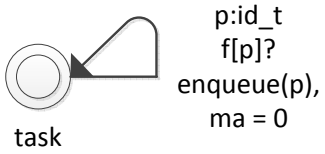

Figure 6.12: Master agent task receive automaton

whereas Sensor1f(2f,3f) and Breaker1f (2f,3f) are the sensor and the breaker associated with the Zone1f(Zone 2f,Zone3f) relay protecting the line at the other end. afault[0], afault[1], afault[2], afault[3], afault[4] and afault[5] are fault status recorded by slave agents of Zone1t, Zone1f, Zone2t, Zone2f, Zone3t and Zone3f respectively. The following properties are verified.

Safety Property:

a) *A [] no deadlock*, i.e., system is deadlock free.

Bounded Liveness Property:

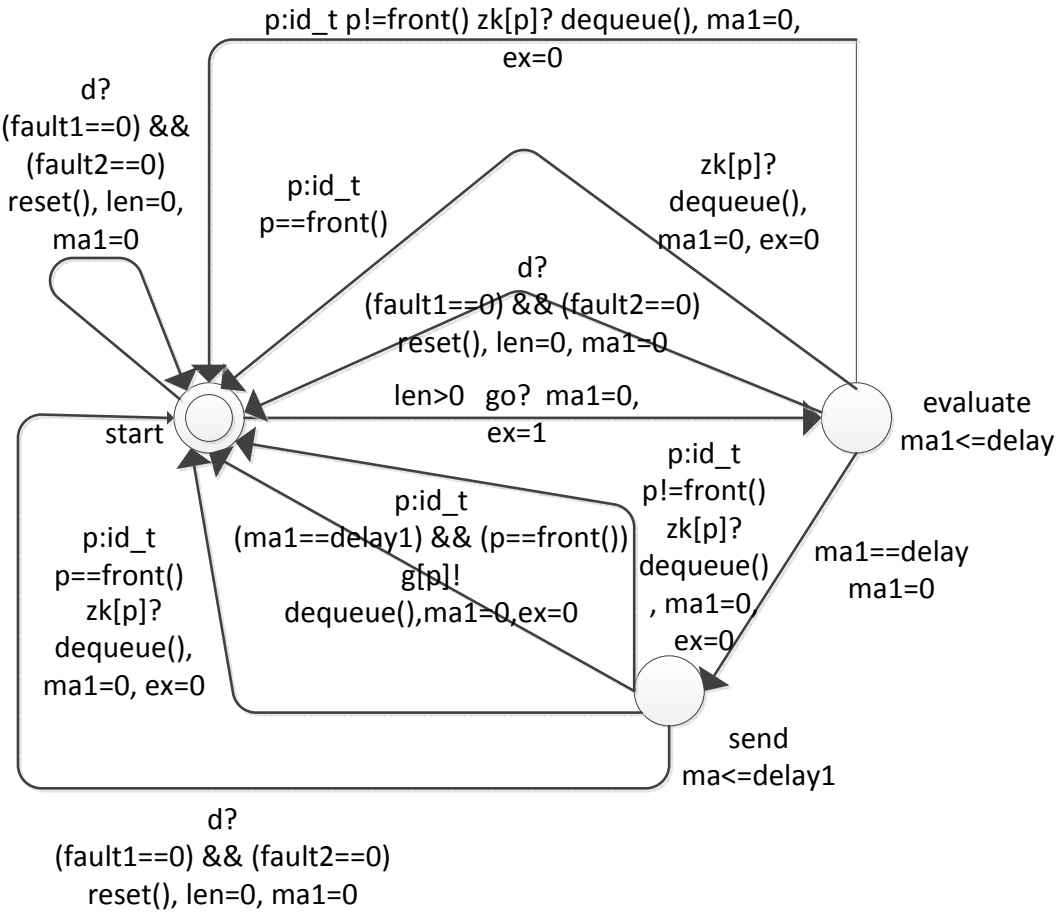

Figure 6.13: Master agent task execute automaton

b) *System.faulty* $\longrightarrow$ *((System.faultfree) and (System.w* $\leq$ *153))*, i.e., System is fault free within 153 msec. If there is a large range in timing, UPPAAL leads to state space explosion. Therefore timing values in slave agent to master agent communication, Zone 2 and Zone 3 waiting times are scaled by a factor of 8. Actually the system should be fault free within the Zone 3 fault clearing time of 1 sec. A Zone 3 slave agent should receive a response from master agent within 968 msec, scaling this by 8 results in 121 msec. Remaining time of around 32 msec is lost in communication delays between sensor and relay, relay and breaker.

These values are not scaled as they are low. Not scaling these values doesn't have any effect on the scaled agent communication delays. Hence the total time available for the system to be fault free is ($121 + 32 = 153$ $msec$). The timing values before and after scaling are as shown in Table 6.1.

Model Correctness Properties:

c) *((Sensor1t.failed or Z1t.failed or Breaker1t.failed) and (Sensor2t.failed or Z2t.failed or Breaker2t.failed) and (afault[4] == 1) and ($n < m$)) $\longrightarrow$* (not (Breaker3f.tripped)). Here 'n' is the number of slave agents with *afault = 1* and 'm' is the number of slave agents with *afault = 0*. If Sensor1t or Zone1t relay or Breaker1t failed and Sensor2t or Zone2t or Breaker2t failed and Zone3t relay slave agent's Boolean variable *afault[4]* is set to 1 then Zone 3 breaker cannot trip if $n < m$.

d) *((Sensor1f.failed or Z1f.failed or Breaker1f.failed) and (Sensor2f.failed or Z2f.failed or Breaker2t.failed) and ($n < m$) and (afault[5] == 1)) $\longrightarrow$ (not (Breaker3t.tripped)).*

This property is similar to property c) but this is verified at the other end of the line.

e) *((Sensor1t.failed or Z1t.failed or Breaker1t.failed) and (Sensor2t.failed or Z2t.failed or Breaker2t.failed) and (afault[4] == 1) and ($n \geq m$)) $\longrightarrow$ Breaker3t.tripped.*

If Sensor1t or Zone1t relay or Breaker t1 failed and Sensor2t or Zone2t or Breaker2t failed and Zone3t relay slave agent's Boolean variable afault[4] is set to 1 then Zone 3 breaker can trip if $n \geq m$ and both n is greater than one. ($n > 1$) indicates that atleast one relay (Zone1 or Zone2 or Zone3) from both ends of line sense that there is a fault.

f) *((Sensor1f.failed or Z1f.failed or Breaker1f.failed) and (Sensor2f.failed or Z2f.failed or*

Breaker2f.failed) and (afault[5] == 1) and $(n \geq m)$ *and* $(n > 1)$ *)* $\longrightarrow$ *Breaker3f.tripped.* This property is similar to e) but this is verified at the other end of the line.

The main aim of the agent based distance relaying scheme is to aid Zone 3 relays to prevent hidden failure induced trips. Properties *c, d, e, f* prove that the model presented in section 6.2 satisfies this criteria. Also the addition of agents should not disturb the actual operation of distance relaying scheme, i.e., it should be deadlock free and be able to isolate faulted line within 1 sec. Properties *a, b* verify that these two requirements are met. Therefore the above described six logical properties are sufficient to guarantee the correctness of our model.

6.4 Observations

In the above two sections agent based Zone 3 relay supervision scheme is formally modelled and verified for the simplest scenario of a single transmission line being protected by two Zone 3 relays. Depending on the power system network topology, it is possible that more than two Zone 3 relays may be protecting a transmission line. The following observations discusses how to handle this scenario.

1. Observation 1: The number N of Zone 3 slave agent requests a master agent with an average service time of t_s can handle at any given time is upper bounded by $N \leq (1000 - t_r)/(t_s)$. Where t_r is the maximum round trip communication delay between any slave agent and master agent in the network. It is possible that a Zone 3 slave

agent may not receive acknowledgement from the master agent with in its fault clearing time of 1 sec. The two main reasons for this are network congestion and length of the queue at the master agent. In order to mitigate the network congestion problem, in chapter 4 we designed the network with sufficient bandwidth for OPNET simulations. Therefore the problem of network congestion can be neglected. As mentioned earlier, from OPNET simulations the average t_s is assumed to be 133 msec and t_r is 150 msec which results in $N \leq 6.4$.

It is well known that the transmission line fault occurrence is a rare event. Further the probability of a fault occurring simultaneously in more than one transmission line is very low. Therefore we restrict this analysis to a single transmission line fault. Also it is mentioned earlier that we restrict our analysis to Zone 3 relay supervision scheme. As discussed above, with $t_s = 133\ msec$ the maximum number of slave agent queries answered by a master agent in 1 sec is 6. Table 6.2 shows the percentage of transmission lines in a given power system network protected by more than six Zone 3 relays. The percentage is around 18 for a 30 bus system and for remaining bus systems the percentage is less than 8. As the percentage of transmission lines with more than six Zone 3 relays is high, the master agent should be capable of handling more than 6 queries in a second. This can be achieved by doubling the query processing capacity of the server or arranging an extra server for query processing at the master agent. Either of these can result in the maximum number of slave agent queries answered by a master agent to be 12. It can be observed from Table 6.2 that the percentage

Table 6.2: Percentage of Zone 3 relays protecting a transmission line

Bus System	**% of lines with $N > 6$**	**% of lines with $N > 12$**
14	0	0
30	17.7	0
57	5.75	0
118	7	0.0025
127	3.25	0

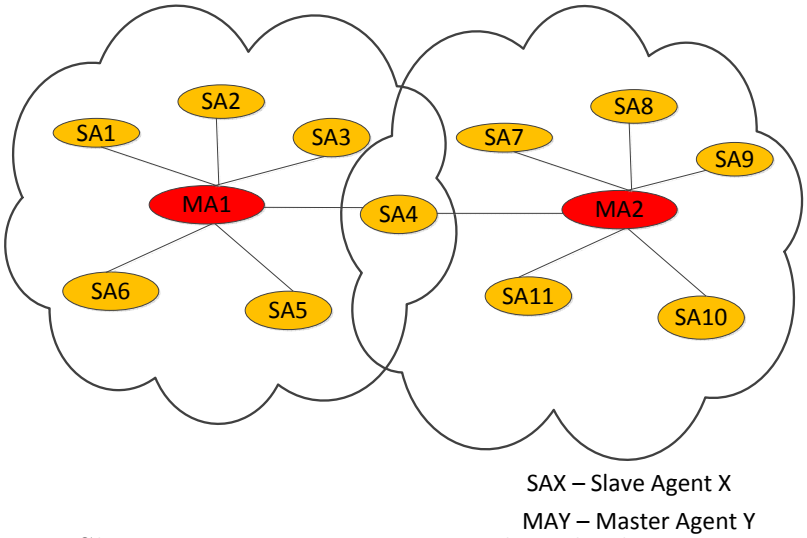

Figure 6.14: Slave agent communication with multiple master agents

of transmission lines in a given power system network protected by more than twelve Zone 3 relays is zero. Therefore for the power system networks shown in Table 6.2, a master agent capable of answering 12 queries per sec should be sufficient to meet the stringent timing requirements of Zone 3 relays. If the above discussed issues are taken into consideration, the formal models can be easily extended to a power system network of any size.

2. Observation 2: It is aforementioned in chapter 5 that a larger bus system requires

more than one master agent to answer queries from Zone 3 slave agents. Therefore a power system network is divided into sub-networks and a master agent is assigned to each sub-network to acknowledge queries from Zone 3 slave agents in that sub-network. It is possible that a network partitioned into sub-networks can be as shown in Figure 6.14. If we can prove that both the sub-networks are disjoint, then the above described formal models and observation I can be applied to them to prove that both the sub-networks independently satisfy the properties verified in section 6.3. Therefore the entire power system network consisting of both these sub-networks can be assumed to satisfy the properties mentioned in section 6.3. The only connection between the two sub-networks shown in Figure 6.14 is that there exists some slave agent relays that are considered as a part of both these sub-networks. If these relays sense a fault, they can send queries to the master agents in both the sub-networks and fault classification depends upon the response from both the master agents. Thus, there exists some interconnection between both the sub-networks. The interconnection can be avoided by using directional relays at the buses that are common to both the sub-networks. The directional relays can distinguish the fault, i.e., in which sub-network the fault exists and based on that it can communicate with the corresponding master agent. Thus, the two sub-networks can be proved to be disjoint. If there are more than two sub-networks in a network, the same approach can be used to negotiate the interconnection between different sub-networks. As the sub-networks in a network are proved to be disjoint, each sub-network can satisfy the verification properties discussed in section

VI and observation I. Therefore the entire network can satisfy the properties discussed in section 6.3.

Chapter 7

FLEX-MAC : A Flexible MAC Protocol to Reduce Overhead and Latency in AMI Networks

Advanced Metering Infrastructure (AMI) is a technology where smart meters installed at the customer's site give the utilities the ability to monitor and collect information related to the amount of electricity consumed by the customer. AMI is one of the important applications of the smart grid and is supposed to play a key role on the distribution-side of the smart grid. As mentioned in chapter 1, [72] compared the key characteristics of different communication and networking technologies like RF mesh, PLC and 3G cellular and concluded that 3G cellular technologies provide an advanced and cost effective solution for smart grid communications

[72]. The comparison results are as shown in Tables 3.1 and 9.3. The main reason for this is that the 3G cellular gives ubiquitous coverage, high reliability, high capacity and data rates, robust security, low cost of ownership, high performance and high scalability. Although 3G/4G cellular technologies satisfy the requirements of smart grid applications, an analysis on the use of the current state of the art 3G/4G cellular technologies for smart grid applications indicates that their usage results in a high percentage of control overhead, high latency and high power consumption for data transfer (section 7.2).

A wireless device (smart meter, mobile phone etc.) using 3G/4G cellular technologies has to go through the random access procedure to acquire resources (4G LTE - Physical resource blocks, 3G CDMA - spreading code) for communication. It is well known that the Random Access CHannel (RACH) transmissions in cellular networks are vulnerable to collisions, retransmissions and hence the RACH has lower throughput and higher packet delays when compared to the data channels [89] [95]. In addition, 3G/4G cellular technologies use TCP/IP based communication for data services, which incurs more overhead. The overhead associated with the TCP/IP and RACH of 3G/4G cellular technologies are discussed in detail in section 7.2. Therefore, instead of using the existing 3G/4G cellular technologies, we propose a non-TCP/IP based stand alone system and FLEX-MAC, a novel and flexible MAC layer protocol to reduce the latency and overhead in data collection. The novelty of the FLEX-MAC lies in its ability to change the mode of operation based on the type of the data being collected, i.e., it uses a different MAC protocol for scheduled and random data collection. This chapter proposes two new MAC layer schemes that the FLEX-MAC

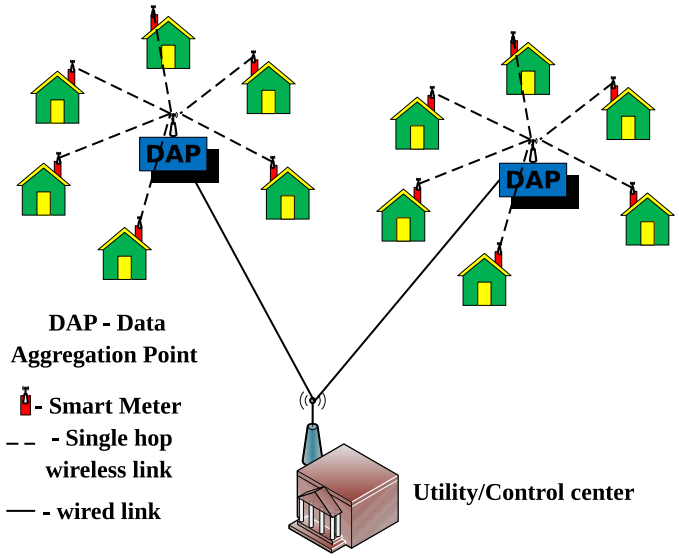

Figure 7.1: Advanced Metering Infrastructure

can employ for scheduled data collection. Chapter 8 explains the FLEX-MAC operation for random data collection. FLEX-MAC protocol reduces the mean power consumption data collection latency by 1/3rd and mean power outage data collection latency by 1/8th when compared to the average data collection latency of 3G CDMA2000.

The remainder of this chapter is organized as follows: Section 7.1 gives a brief description of the AMI architecture and the types of data handled by the AMI network. The control overhead and latency issues associated with the use of 3G/4G technologies for distribution-side smart grid data collection are discussed in Section 7.2. The proposed MAC layer schemes are explained in Section 7.3. Section 7.4 describes the system model. In Section 7.5, average throughput and average packet delay expressions are derived using markov chain analysis. Simulation results and discussions are provided in Section 7.6. Section 7.7 concludes the chapter.

7.1 Preliminaries

7.1.1 Advanced Metering Infrastructure

AMI is a technology where the traditional electricity meters are going to be replaced by smart meters at the customer's site, which give the utilities the ability to monitor and collect information related to the amount of electricity consumed by the customer. In addition to customer power consumption data collection, the communication network set up for AMI can also be used for the other distribution-side smart grid applications such as Advanced Distribution Automation (ADA), Demand Response Management System (DRMS) and Outage Management System (OMS). As shown in Figure 7.1, we assume a two-layered communication architecture for the AMI network. The control center collects the data from the smart meters and the Data Aggregation Point (DAP) acts as a relay between the smart meter and the utility. The control center hosts a database server which stores the data collected from smart meters. We assume that the AMI employs wireless communication network between the smart meters and the DAP and a wired/wireless network between the DAP and the utility. In the process of data collection, smart meters send the consumer's load consumption data to the utility at a preselected time interval. The time interval could be 15 minutes or 30 minutes or 1 hour. The number of smart meters that a DAP handles can vary from as few as 500 to as many as 30000 [1] [4] [34].

7.1.2 Data Types

Taking into account all the distribution-side smart grid applications, the data handled by the AMI network can be divided into two categories:

Scheduled Data

If the time instance at which the data needs to be collected from or sent to the smart meter is known in advance, those data are categorized as scheduled data. Examples of scheduled data are customer power consumption data and DRMS data. Scheduled data frame format is as shown in Figure 7.2.

Random data

If the time of arrival of the data to the DAP or the smart meter is unknown and occurs at a random time instance, that data are categorized as random data. Power outage data is an example of random data. Random data frame is as shown in Figure 7.3.

Power outage is considered as a rare event in most of the developed countries in North America and Europe. According to the North American Electric Reliability Council (NERC), the average number of large scale power outages occurred in U.S. during 1984 - 2006 are 3.3 per month. According to U.S. census bureau the total number of households during this period is 95 Million [86]. Assuming a smart meter per household, the average number of power outage reportings per smart meter would have been 0.00177 between 1984 and 2006.

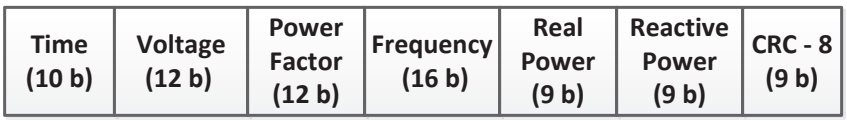

Figure 7.2: Scheduled data frame

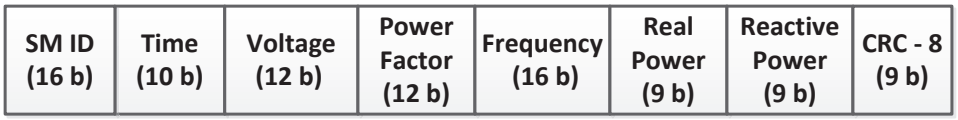

Figure 7.3: Random data frame

On the other hand, power consumption and DRMS data transfer occurs periodically with a time interval of 15 minutes [29] [51] [58]. Therefore, we can consider that the scheduled data contributes to a high percentage ($> 95\%$) of the traffic in the AMI network and the percentage of random traffic is relatively small ($< 5\%$). In this work, the proposed MAC layer schemes are suitable for scheduled data collection and hence this paper deals only with the collection of the scheduled data. However, the proposed non-TCP/IP based architecture can be used for both scheduled and random data collection. The procedure for random data collection is is explained in chapter 8.

7.2 3G/4G Issues

As mentioned earlier, according to [72] the current cellular technologies seem to be a good choice for smart grid applications. In this section, we argue that the 3G/4G technologies are not an appropriate choice for smart grid applications. The main issues of using the current

state of the art 3G/4G cellular technologies for smart grid applications are as follows:

7.2.1 TCP/IP Overhead and ROHC Compression

3G/4G cellular technologies, i.e., CDMA 2000, WCDMA and 4G LTE employ a Transmission Control Protocol/Internet Protocol (TCP/IP) based data protocol stack [46]. There are two versions of IP, i.e., IPV4 and IPV6. IPV6 is the successor of IPV4. The header overhead of TCP/IPV4 and TCP/IPV6 is 40 bytes and 60 bytes respectively. Depending on the payload size, the overhead contribution from TCP/IP protocol varies from negligible to significant. Nowadays, it is not uncommon to use smart phones to access internet applications like email, web and video streaming. The data transfers involving these applications is generally very high on the order of hundreds of KBytes to MBytes. As a result, the relative overhead (overhead with respect to payload) of TCP/IP packets is around 5% to 10% [15].

In 3G/4G cellular technologies, RObust Header Compresssion (ROHC) is used to reduce the overhead [31] [25]. ROHC reduces the overhead by a considerable amount when the data size is large. As the smart meter data size is around 10 Bytes, ROHC may not be applicable when collecting smart meter data using 3G/4G cellular network. The working principle of ROHC is as follows: after the TCP/IP connection is established between the source (smart meter, mobile etc) and destination (database server, web server etc.), ROHC observes the first few packets (1 to 2) and then applies the compression for the remaining packets. The data transfers involving distribution-side smart grid applications is very low, i.e., less than

100 Bytes [64]. Hence, the smart grid devices may not have the sufficient amount of data to send before the ROHC starts applying the compression algorithm on the smart grid data. So, the TCP/IP header of the smart grid data packets may not be compressed. Therefore, the overhead contribution from TCP/IP protocol is significant if 3G/4G cellular technologies are used for the smart grid data packets.

TCP uses a 3-way handshake for connection establishment (SYN,SYNC-ACK,ACK) and connection termination (FIN,FIN-ACK,ACK) between a source and a destination. In order to transfer 25 Bytes of customer power consumption data from smart meter to DAP and receive an ACK (68 Bytes) from database server at the control center, six additional packets have to be transferred.

Using the Wireshark network packet analyzer, it was observed that the TCP/IP connection establishment/termination packet sizes are 68 Bytes (60 Bytes TCP/IPV6 Header + 8 Bytes data) [75]. So, using 3G/4G technologies the total data transferred is 561 Bytes, resulting in an overhead of 536 Bytes, i.e., 2144%. This is as shown in Figure 7.4.

In this analysis, we considered only the transport layer overhead because the overhead associated with the lower layers like MAC and PHY is less and approximately the same for most of the technologies. It is obvious from this simple analysis that the use of TCP/IP results in very large control overhead for smart grid applications. Undoubtedly, TCP offers reliability in data transfer but the overhead associated with it has to be taken into account while adapting it for an application that involves small size data transfers. Irrespective of the type of the network being designed, i.e., wired or wireless network, reducing the data

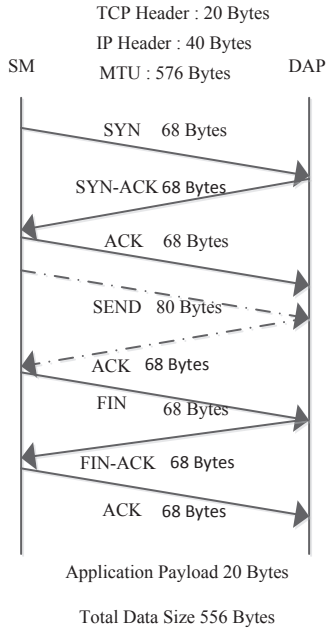

Figure 7.4: Data exchange between SM and DAP using TCP/IP based stack

overhead decreases the latency in data transfer from source to destination and it also results in bandwidth savings which further reduces the expenses in system design. Particularly for wireless networks, bandwidth reduction is of paramount importance as the wireless spectrum is very expensive.

TCP/IP based data transfer is appropriate for smart phones because the smart phone applications communicate with TCP/IP servers that are located in different parts of the world. On the other hand, the data collected from the smart meters is restricted to a local area. As shown in Figure 7.1, smart meters send data to or receive queries from a single source, i.e., database located at the control center. Therefore, IP based communication may not be required for smart meter data transfer. In Figure 7.1, assuming that there is a database at the DAP, the wireless portion of the network can be considered as a smart

metering sensor network. No wireless sensor networks use TCP/IP based stack as it results in data overhead and latency. In order to send the data collected at the DAP to the control center, TCP/IP based stack can be used for the wired portion of the network between DAP and the control center.

Taking the above factors into consideration, it appears that the TCP/IP based 3G/4G cellular technologies are not an appropriate choice for smart grid applications. One of the solutions to address the above discussed issues may be to design a custom network for distribution-side smart grid applications. Consider the AMI network shown in Figure 7.1. A high level view of the AMI network gives an impression that its architecture is similar to that of a cellular network. This aspect of AMI network is misleading communication and networking engineers to suggest the use of 3G/4G cellular network for smart meter data collection. It is more appropriate to consider AMI network as a long distance sensor network (single hop) rather than a cellular network. Therefore, designing an efficient (low overhead and low latency) custom long distance wireless sensor network would be more appropriate rather than using a 3G/4G cellular network.

Similar to any other network, once set up, AMI network is also expected to be used for several years. Therefore, from the utilities perspective, it is worth considering the idea of designing a custom AMI network rather than using an already existing 3G/4G network. Also, setting up their own network gives the utilities improved privacy and security in the data transfer.

In general, most wireless sensor network designs are limited to a small coverage area of 2 to

3 km. In recent years, a lot of research has been done in the area of long distance wireless sensor network design and experimental test beds were set up using off the shelf equipment to transmit and receive upto 13.2 km [88] [84]. The current state of the art radios that are used in wireless sensor network design can transmit up to 40 miles with a data rate of 115.2 kbps [71]. Motivation can be drawn from these research studies to design a long range AMI network that can exactly meet the demands of smart grid applications.

As mentioned above, with the current state of the art RF modems, designing a long range wireless sensor network is not a difficult task but the main issue is to reduce the data overhead. Unlike the TCP/IP based 3G/4G cellular stack, a data stack similar to the Zigbee sensor network can be used in the custom AMI network design to reduce the overhead. Zigbee protocol stack does not include a transport layer [81]. Therefore, it is up to the designer to ensure an end-to-end reliable data delivery in a Zigbee data transfer. We are not suggesting the use of Zigbee protocol stack for AMI radios because MAC and PHY layers of Zigbee are insecure [13]. But we are suggesting that a solution to reduce control data overhead is to design an AMI network protocol stack similar to Zigbee, i.e., without transport(TCP) layer and ensure end-to-end reliable data delivery at the application layer.

7.2.2 RACH Transmission Issues

As mentioned earlier, a wireless device using 3G/4G technologies for the purpose of communication acquires resources via random access procedure, which involves RACH transmissions,

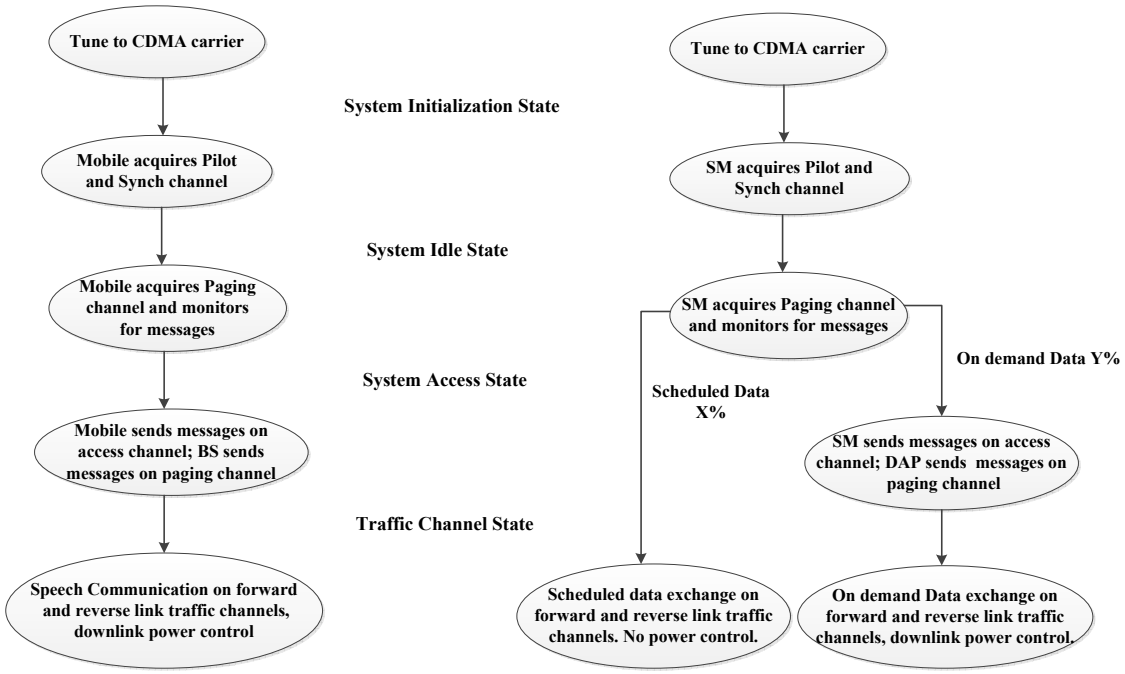

Figure 7.5: Differences between cellular MAC vs AMI MAC

possible collisions and retransmissions. In 3G WCDMA, RACH delay is of the order of few hundreds of msec [38] and in 4G LTE, depending on the traffic volume, the delay can vary from 10 msec to 30 msec [34] [5]. As discussed in section 7.1, a high percentage ($> 95\%$) of the data in smart grid applications is scheduled. In other words, the time of occurrence of data transfer is known ahead of time. The proposed MAC layer schemes (section 7.3) leverage the information related to the time of occurrence of the smart grid data transfer to avoid the RACH transmissions, overhead and delay. Specifically, the resources for the scheduled data are allocated ahead of the transmission time and hence it is not required by the smart grid devices to request for resource allocation during the transmission. Thus, by avoiding the RACH transmissions, smart grid devices reduce the RACH control overhead and RACH latency involved in data transfer.

7.3 FLEX-MAC Layer design

As discussed in Section 7.2, the use of 3G/4G cellular network for distribution-side smart grid applications results in high MAC layer control overhead and latency in data collection. This chapter proposes FLEX-MAC - a flexible MAC layer to reduce control overhead and latency in smart meter data collection. The main objective of the FLEX-MAC layer is to perform the mapping between the logical and the physical channels. We assume that the AMI network has pilot, synchronization, paging and traffic channels in the downlink and random access channel, traffic channel in the reverse link. The above mentioned channels exist in any cellular technology but the number and the type (Dedicated and Control) of these channels can differ from one technology to another. We assume spread spectrum as the PHY layer technology. Specifically, we use direct sequence spread spectrum (DSSS).

7.3.1 Cellular CDMA MAC vs FLEX-MAC

The proposed FLEX-MAC is a variant of the cellular CDMA MAC. Therefore, we explain the operation of the FLEX-MAC by comparing it with the operation of Cellular CDMA-MAC. The main differences between the cellular MAC and the FLEX-MAC are as shown in Figure 7.5. The system initialization, system idle and traffic channel states are the same whereas the behaviour of the system access state is different in the AMI network when compared to that of the cellular network. It is aforementioned that the AMI network carries both scheduled and random traffic and the percentage of scheduled data ($> 95\%$) is very

high compared to the random data ($< 5\%$). As the AMI network can schedule more than 95 % of the data to be collected from the smart meters, it is known in advance when a smart meter sends data to the DAP, whereas in cellular network the time of call origination or data transfer from mobile is not known ahead of time. Unlike the CDMA MAC which incurs RACH overhead and latency for data transfer, the proposed FLEX-MAC exploits the knowledge of the time of occurrence of the data transfer to reduce the RACH overhead and delay involved in scheduled data collection.

As shown in Figure 7.5, in 3G cellular networks (CDMA), a MS initiates a call by sending a request on the RACH to the BS to allocate (reserve) a traffic channel for the purpose of voice/data communication. While sending a RACH request, every MS competes with many other MSs in the cell that are requesting the BS to allocate the resources. If a MS's access request collides with the request from an other MS, it has to retransmit the request which results in longer connection delay. BS acknowledges the MS's request by sending a message on the paging channel. This is an indication that the system resources (spreading code) are reserved for the MS. MS uses the information sent by the BS for further voice/data communication.

As explained above the entire process of call set up incurs few seconds of delay and unnecessary data overhead due to the MS access request and message exchanged by the BS with a MS. As mentioned earlier a high percentage ($> 90\%$) of the data collected from the smart grid applications is scheduled and a small portion of the data is random. The time scheduling in smart grid data collection can be leveraged to obviate the data transfer/call

set up process. For example, if a smart meter with unique identification number x is scheduled to send data to the DAP in the frame number y. Both the variables x and y can be used as inputs to a hashing algorithm to select a spreading code from the available set of spreading codes for uplink transmission. Both the smart meter and a demodulator at the DAP can be tuned to the same spreading code for the purpose of spreading and despreading respectively. In 3G cellular the overhead and the latency associated with the call set up process cannot be avoided because of the randomness in call origination. Whereas in smart grid applications, as explained above, a MAC layer designed to take the advantage of time scheduled data collection can reduce the overhead and latency in data transfer. But in order to leverage the time scheduled data collection, DAP and smart meters have to be at least frame synchronized if not time synchronized.

A MS that is a part of a cell monitors the downlink paging channel every t time slots for any message (eg: notify call arrival) from the BS. Here t is a design parameter and is decided by the cellular network operator but it is of the order of few tens of slots. In 3GPP WCDMA, at the MS, the uplink frame transmission takes place approximately T_0 chips after the reception of the downlink frame [6]. Thus, 3GPP WCDMA maintains uplink coarse frame level synchronization. If a MS is scheduled to transmit its packet in m^{th} uplink frame, let us consider that the MS monitors the downlink paging channel close to $m-p$ uplink frame, i.e., next uplink frame after monitoring the downlink paging channel is $(m-p)th$ frame. In FLEX-MAC design, BS transmits the value of the $(m-p)$ as a part of the paging channel message. Based on the value of $m-p$, a MS can find out the uplink frame number m

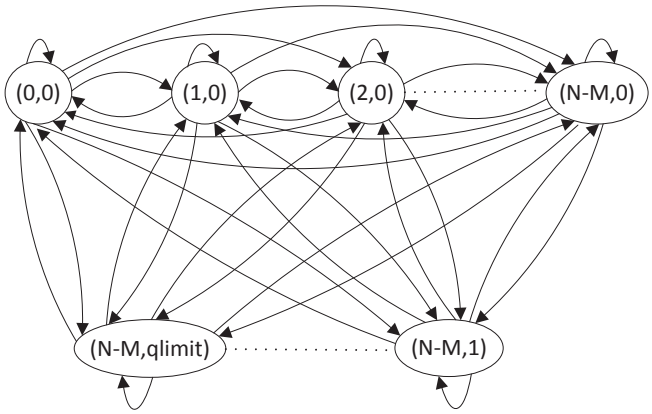

Figure 7.6: Markov chain

that it is scheduled to transmit the packet. Thus, in FLEX-MAC design both uplink coarse frame level synchronization and frame number synchronization between MS and BS has to be maintained. Based on the methodology used to select the spreading codes, we propose two different FLEX-MACs. They are *Frame and Channel Reserved (FCR) MAC* and *Frame Reserved and Random Channel (FRRC) MAC*. In FCR MAC, as described above a hashing algorithm is used for selecting the spreading code whereas as in FRRC MAC, a smart meter randomly selects a spreading code from N uplink spreading codes. The design of hashing algorithm is out of the scope of this research work. In both the MACs, an uplink frame is reserved for a smart meter for the transmission of scheduled data.

The main reason for selecting the spreading spectrum as the PHY layer technology is that the uplink transmissions in spread spectrum can be asynchronous whereas in OFDMA based systems like 4G LTE the uplink transmissions are synchronous. In 4G LTE, MS's use RACH transmissions for synchronizing the uplink transmissions and resource allocation.

$$N_s = \begin{cases} ((N-M+1)) * (qlimit+1) - ((N-M) * (qlimit)) \text{ if } N-M \neq 0 \\ ((N-M+1)) * (qlimit+1) - ((N-M) * (qlimit)) - qlimit \text{ if } N-M = 0 \end{cases} \tag{7.1}$$

Hence, RACH overhead and RACH delay are inevitable for 4G LTE uplink transmissions.

7.4 System Model

This system model is used for analyzing the proposed MAC layer for uplink transmissions. We consider a DS-CDMA based smart meter network consisting of a single base station network and a total of M smart meters. The main reason for selecting DS-CDMA is that, DS-CDMA performs better in jamming environments, its capacity is soft and it offers security at the PHY layer. We also assume that K out of M smart meters transmit at the same time with a spreading code of length N. Unlike the cellular network, where cell phones can be highly mobile, in smart meter network, smart meters are stationary. Hence, we assume a closed loop power control system that operates at a lower frequency of 100 Hz when compared to that of the 3G WCDMA that operates at 1500 Hz. We considered both AWGN and frequency selective multipath Rayleigh fading channel. We also consider the out-of-cell interference from six neighboring cells. We also assume that the base station employs rake receiver with perfect channel estimation. Maximal Ratio Combining (MRC) is used to combine the output signals from rake receiver. As the proposed MAC layer is for uplink transmissions, the downlink channel is assumed to be delay and error free. Urban

COST-Hata model is used for path loss calculations. Also, as the smart meters are stationary we ignore Doppler shift in our analysis.

7.5 Markov Chain Analysis

In this section, markov chain analysis is used to derive the average throughput and the average packet delay of FCR and FRRC MAC.

7.5.1 FCR MAC

As discussed in the above section, FCR MAC schedules the time slot for the packet transmission and the transmission channel (spreading code) for the packet. The markov chain of FCR MAC is as shown in Figure 7.6. A state n in a markov chain is defined by two parameters (n_r, n_q). Here n_r is the number of smart meters in retransmission state and n_q is the number of smart meters in the queue. As discussed in above section, in a given time slot, M smart meters are scheduled for transmission. If the number of channels are limited to N, then the maximum number of possible retransmissions are $N - M$. Hence, the range of n_r is $0 \leq n_r \leq N - M$. If there are more than $N - M$ smart meters are in retransmission state, they are stored in queue at the base station and are are allowed for retransmission when there are free channels available for transmission. Assuming that the queue size is $qlimit$, if the number of smart meters in retransmission state exceed $N - M + qlimit$, the remaining smart meters are dropped and are not scheduled in future. The range of N_q is

$0 \leq n_q \leq qlimit$. The total number of states in the markov chain is given by equation 7.1. In the first case, when $N - M \neq 0$, the markov chain states are $(0,0)$, $(1,0)$, $(2,0)$,....., $(N-M,0)$, ...,$(N-M, qlimit)$. In the second case, i.e., when $N - M = 0$, the markov chain has only one state, i.e., $(0,0)$.

The one step transition probabilities from state n to state m in Markov chain of Figure 7.6 is given by equation 7.2. In equation 7.2, $k = (M + n_r + n_q) - (m_r + m_q)$, p_s is the probability of packet success and is given by equations 7.3 and 7.4. The equation 7.3 assumes a stateless Bernoulli model, i.e., the BER p_b of each bit is i.i.d. There exists Frame Error Rate (FER) equations in the literature that capture temporal correlation based on Gilbert-Elliot recursive model [49] [54]. But those equations are derived for a multipath flat Rayleigh fading channel whereas we considered a frequency selective multipath fading channel in this work. Tralli and Zorzi investigated the possibility of Markov modeling for the physical layer block error process in a WCDMA cellular system in a frequency selective multipath fading channel and concluded that their WCDMA model may be used for matching run length distributions for either error or error-free runs but generally not both [70] [85].

$$P_{nm} = \begin{cases} \sum_{j=0}^{n_r} \binom{n_r}{j} pr^j (1-pr)^{n_r - j} \binom{M+j}{k} p_s^k (1-ps)^{M+j-k} \text{ if } ((k \geq 0) \,\&\&\, (M + j \geq k)) \\ 0 \text{ if } ((k < 0) \,||\, (M + j < k)) \\ 1 - \sum_{l=0}^{m-1} P_{nl} \text{ if } ((N - M > qlimit) \,\&\&\, (m_r = N - M) \,\&\&\, (m_q = qlimit) \,\&\&\, (m_r + m_q - n_q \geq qlimit)) \\ 1 - \sum_{l=0}^{m-1} P_{nl} \text{ if } ((N - M \leq qlimit) \,\&\&\, (n_r - m_r = 0) \,\&\&\, (m_q = qlimit) \,||\, (m_r + m_q - n_q > qlimit)) \end{cases} \tag{7.2}$$

To the best of our knowledge there do not exist FER equations in the literature that capture temporal correlation in a frequency selective multipath Rayleigh fading channel.

Markov chain modeling of frequency selective multipath Rayleigh fading channel, deriving FER equations, collecting real time data and validating the Markov model with the real time data is not only a time consuming process but that on its own can be a separate research topic. Therefore, we considered the simpler stateless Bernoulli model in deriving the equation 7.3.

In equation 7.2, $\binom{n_r}{j} pr^j (1-pr)^{n_r-j}$ is the probability that j packets are transmitted from n_r smart meters in retransmission state. $\binom{M+j}{k} p_s^k (1-ps)^{M+j-k}$ is the probability that k packets are successful when $M+j$ packets are transmitted with an average packet success rate of p_s given by equation 7.3.

$$p_s = \sum_{k=0}^{K} \binom{n}{k} p_b^k (1-p_b)^{n-k} \tag{7.3}$$

where p_b is the probability of bit error and is given as follows

$$p_b = Q\left(\frac{1}{\sqrt{(\frac{N_0}{2*E_{b,1}}) + (\frac{\sum_{k=2}^{K} R_k}{3*P_1*N})}} \right) \tag{7.4}$$

Where K = the number of smart meters

N = Processing gain

R_k = Power of kth smart meter

$E_{b,1}/N_0$ = SNR of desired smart meter

Let P be the state transition matrix and $\pi = \{\pi_1, \pi_2, \pi_3, ..., \pi_{N_s}\}$ denote the steady-state probability vector, which is obtained from

$$\pi = \pi P \tag{7.5}$$

$$\sum_{n=1}^{N_s} \pi_n = 1 \tag{7.6}$$

Average Throughput

Average Throughput ('S') is defined as the number of packet successfully transmitted in a slot. It is given by equation 7.7.

$$S = \sum_{n=1}^{N_s} \pi_n \sum_{j=0}^{n_r} \sum_{c_s=1}^{M+j} c_s * \binom{n_r}{j} pr^j \left(1-pr\right)^{n_r-j} \binom{M+j}{c_s} p_s^{c_s} \left(1-p_s\right)^{M+j-c_s} \tag{7.7}$$

In equation 7.7, π_n is the average probability of markov chain being in state n, $\binom{n_r}{j} pr^j (1-pr)^{n_r-j}$ is the probability that j packets are transmitted from n_r smart meters in retransmission state. $\binom{M+j}{c_s} p_s^{c_s} (1-ps)^{M+j-c_s}$ is the probability that c_s packets are successful when $M+j$ packets are transmitted with an average packet success rate of p_s given by equation 7.3. $\sum_{j=0}^{n_r} \sum_{c_s=1}^{M+j} c_s * \binom{n_r}{j} pr^j \left(1-pr\right)^{n_r-j} \binom{M+j}{c_s} p_s^{c_s} \left(1-p_s\right)^{M+j-c_s}$ is the average number of successful packets in state n.

Average Packet Delay

Average packet delay is the delay in the transmission of a packet from head of the line of the queue until the ACK is received at the smart meter. Average packet delay ('D') is given as follows

$$D = \frac{G}{S} \tag{7.8}$$

G is the offered load and it is given by equation 7.10.

$$G = \sum_{n=1}^{N_s} \pi_n \left(M + \sum_{j=0}^{n_r} j \binom{n_r}{j} pr^j \left(1-pr\right)^{n_r - j} \right) \tag{7.9}$$

$$= \sum_{n=1}^{N_s} \pi_n \left(M + (n_r * pr)\right) \tag{7.10}$$

In equation 7.10, $\sum_{j=0}^{n_r} j\binom{n_r}{j} pr^j \left(1-pr\right)^{n_r-j}$ is the average number of transmissions from smart meters in retransmission state. M is the number of smart meters scheduled to transmit packet in a slot. Hence, $\left(M + \sum_{j=0}^{n_r} j\binom{n_r}{j} pr^j \left(1-pr\right)^{n_r-j} \right)$ is the average number of total transmissions from a state n of the markov chain shown in Figure 7.6.

$$P_{nm} = \begin{cases} \sum_{j=0}^{n_r} \binom{n_r}{j} pr^j \left(1-pr\right)^{n_r-j} f\left(k|M+j,N,p_s\right) \text{ if } \left((k \geq 0) \,\&\&\, (M+j \geq k)\right) \\ 0 \text{ if } \left((k<0) \,||\, (M+j<k)\right) \\ 1 - \sum_{l=0}^{m-1} P_{nl} \text{ if } \left((N-M > qlimit) \,\&\&\, (m_r = N-M) \,\&\&\, (m_q = qlimit) \,\&\&\, (m_r + m_q - n_q \geq qlimit)\right) \\ 1 - \sum_{l=0}^{m-1} P_{nl} \text{ if } \left((N-M \leq qlimit) \,\&\&\, (n_r - m_r = 0) \,\&\&\, (m_q = qlimit) \,||\, (m_r + m_q - n_q > qlimit)\right) \end{cases} \tag{7.11}$$

7.5.2 FRRC MAC

In FRRC MAC, the time slot for packet transmission is scheduled but the spreading code (channel) is not allocated ahead of time. A smart meter randomly selects one of the available spreading codes and spreads the transmitting packet using that spreading code. Assuming that the received signal power at the BS from all the smart meters is same, if two smart meters transmit using the same spreading code, collision occurs. At the receiver, the received packet is correlated with all the available spreading codes for despreading. The Markov chain is same as that of the FCR MAC but the transition probabilities change. The one step transition probabilities from state n to state m in FRRC MAC is given in equation 7.11.

In equation 7.11, $k = (M + n_r + n_q) - (m_r + m_q)$. $f\left(k|M+j, N, p_s\right)$ is the conditional probability that the k packets are successfully transmitted if $M + j$ smart meters are transmitted and p_s is packet success probability and N is the total number of spreading codes (channels). $f\left(k|M+j, N, p_s\right)$ is evaluated by the following recursive expression. Similar equations can be found in [19].

$$f\left(k|n, N, p_s\right) = \sum_{i=0, i\neq 1}^{n} p_n^i f\left(k|n-i, N-1, p_s\right) + p_n^1 f\left(k-1|n-1, N-1, p_s\right) ps + p_n^1 f\left(k|n-1, N-1, p_s\right)(1-ps) \quad (7.12)$$

In equation 7.12, $p_n^i = \binom{n}{i}\left(1-\frac{1}{M}\right)^{n-i}\left(\frac{1}{M}\right)^i$ is the probability that i out of n smart meters

transmit over an arbitrary channel, such as the first channel, with the initial conditions

$$f\left(k|n,0,p_s\right)=\begin{cases}1 \text{ if } k=0 \text{ and any } n\\ \\ 0 \text{ if } k>0 \text{ and any n}\end{cases} \tag{7.13}$$

$$f\left(k|0,m,p_s\right)=\begin{cases}1 \text{ if } k=0 \text{ and any } m\\ \\ 0 \text{ if } k>0 \text{ and any } m\end{cases} \tag{7.14}$$

$$f\left(k|1,m,p_s\right)=\begin{cases}(1-p_s) \text{ if } k=0 \text{ and } m\geq 1\\ \\ (p_s) \text{ if } k=1 \text{ and } m\geq 1\\ \\ 0 \text{ if } k>1 \text{ and } m\geq 1\end{cases} \tag{7.15}$$

$$f\left(k|n,1,p_s\right)=\begin{cases}1 \text{ if } k=0 \text{ and } n>1\\ \\ 0 \text{ if } k>0 \text{ and } n>1\end{cases} \tag{7.16}$$

and

$$f\left(k|n,m,p_s\right)=0 \text{ if } k<0 \tag{7.17}$$

Like FCR MAC, equation 7.5 and equation 7.6 are used to find the steady-state probabilities. The average throughput of the FRRC MAC is given by equation 7.18.

$$S=\sum_{n=1}^{N_s}\pi_n\sum_{j=0}^{n_r}\sum_{c_s=1}^{M+j}c_s\binom{n_r}{j}pr^j\left(1-pr\right)^{n_r-j}f\left(c_s,M+j,N,p_s\right) \tag{7.18}$$

Table 7.1: Simulation parameters

Parameter	**Value**
Transmit power (R_t)	24 dBm
Smart meter antenna gain	2 dBi
Effective Isotropic Radiated Power (EIRP)	26 dBm
Base station noise figure	2 dB
Sinc pulse cut off factor	0.22
Transmission scheme	FDD
Uplink bandwidth	2.5 MHz
Downlink bandwidth	2.5 MHz
Chipping rate	2.0491 Mcps
Spreading code length	128
Data rate	16 Kbps
Frame size	10 msec
Cell radius	5 Km
Path loss model	COST 231 WI
Base station antenna gain	18 dBi
Cable loss in base station	2 dB
Max path loss	166.6 dBm
E_b/N_0	5.29 dB
Temperature	290 K

In equation 7.18, $\binom{n_r}{j} pr^j \left(1 - pr\right)^{n_r - j}$ is the probability of j transmissions given that the number of smart meters in retransmission state are n_r. $f\left(c_s, M + j, N, p_s\right)$ is given by equation 7.12.

The average packet delay of the FRRC MAC is obtained by substituting S from equation 7.18 in equation 7.8. The average offered load 'G' is given by equation 7.10.

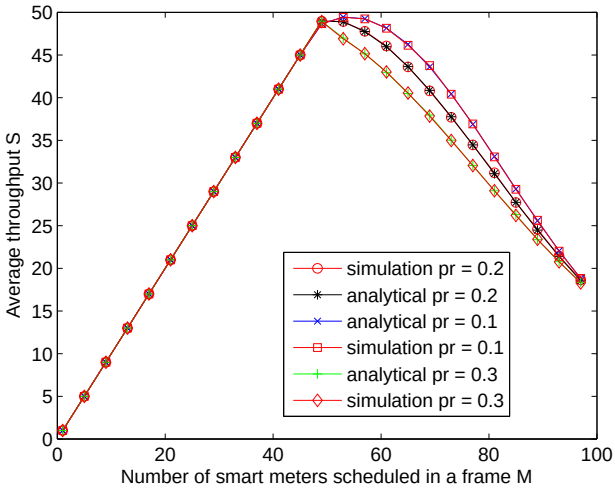

Figure 7.7: Throughput of FCR MAC

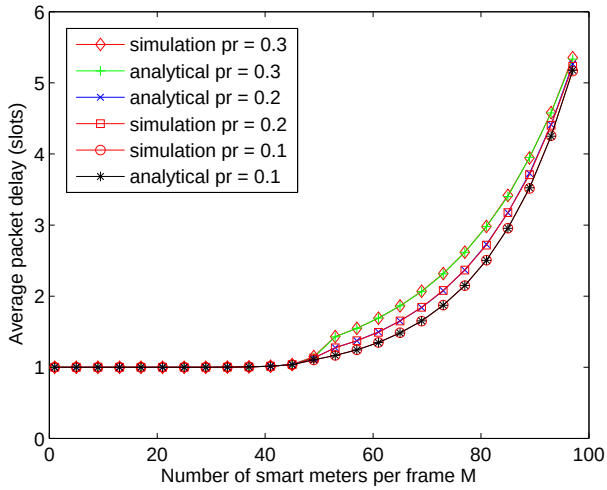

Figure 7.8: Average packet delay of FCR MAC

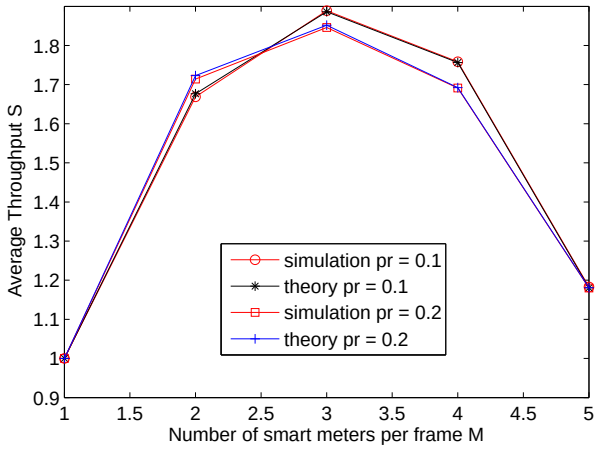

Figure 7.9: Throughput of FRRC MAC

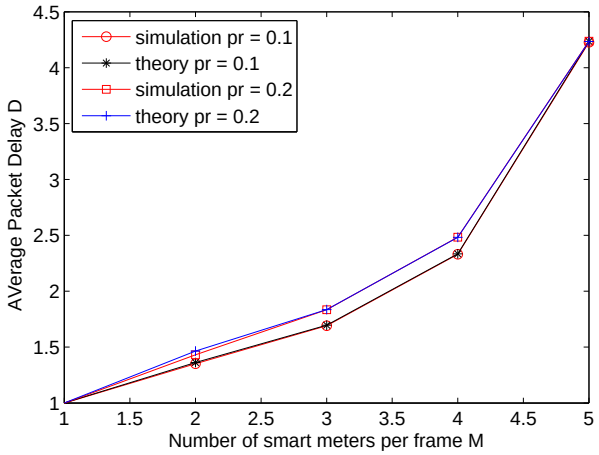

Figure 7.10: Average packet delay of FRRC MAC

7.6 Simulation and Results

In this section, we present the simulation results of the proposed MAC layer schemes. The simulation parameters are as shown in Table 7.1. Figure 7.7 gives the average throughput of the FCR MAC. It can be observed from Figure 7.7 and Figure 7.8 that the analytical expressions derived for the average throughput and average packet delay of FCR MAC match very well with the average throughput and average delay obtained using simulation. The conditional probability of equation 7.12 has exponential time complexity. For N = 127 and varying M from 1 to 50, it took more than 2 weeks to calculate the transition probabilities on a cluster. Therefore, we compare theory and simulation curves for average throughput and average packet delay of FRRC MAC for small values of N and M, i.e., for N = 7 and M is varied from 1 to 5. The average throughput and the average packet delay plots of FRRC MAC are given by Figure 7.9 and Figure 7.10 respectively. It can be observed from Figure 7.9 and Figure 7.10 that the simulated curves match the analytical curves. On the flip side, the simulation of FRRC MAC finishes quicker for large values of N when compared to analytical curves. Hence, when comparing the performance of FCR MAC and FRRC MAC, we use simulated average throughput and average packet delay of FRRC MAC rather than analytical expressions given in equation 7.8 and equation 7.18.

Figure 7.11 and Figure 7.12 compare respectively the average throughput and the average packet delay of the FCR MAC and FRRC MAC. It can be observed from Figure 7.11 that the FCR MAC has higher throughput when compared to FRRC MAC. For a given set

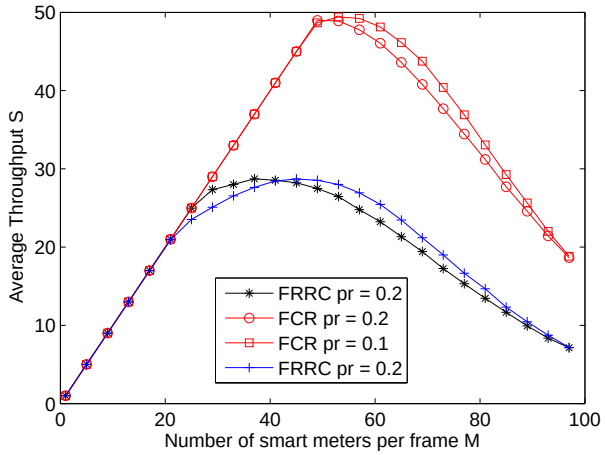

Figure 7.11: Comparison of average throughput of FCR and FRRC MAC

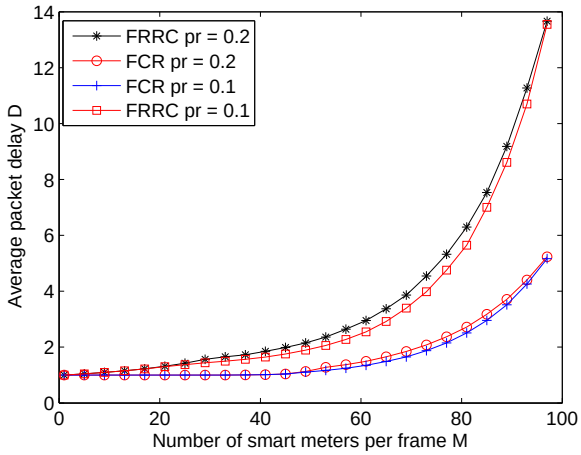

Figure 7.12: Comparison of average packet delay of FCR and FRRC MAC

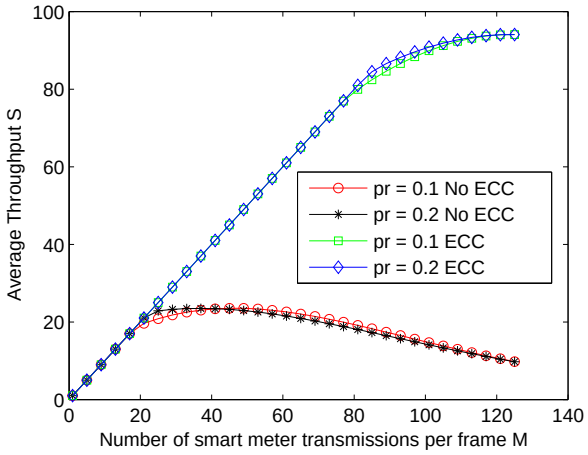

Figure 7.13: Average throughput of FCR MAC in multipath channel

of parameters, the throughput of FRRC MAC is 34 whereas the FCR MAC supports 50 simultaneous user transmissions. It can be inferred from Figure 7.12 that, when the number of smart meters per frame is greater than 10, the average packet delay of FCR MAC is significantly lower than that of the FRRC MAC. As the FCR MAC performs better than the FRRC MAC, the simulation results presented from now on are only related to the FCR MAC.

The simulation and analytical results discussed until now are for AWGN channel. The performance of FCR MAC is evaluated in multipath fading channel with and without coding. 3-bit error-correction convolution code is used. It can be observed from Figure 7.13 and Figure 7.14 that the FCR MAC has very good performance in multipath channel with error correction coding and it supports upto 80 simultaneous smart meter transmissions. The main reason for the improved performance of FCR MAC in multipath channel when compared to AWGN channel is due to the rake receiver diversity gain.

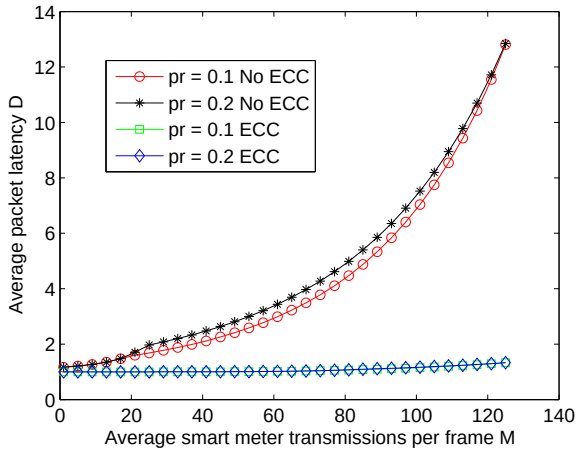

Figure 7.14: Average packet delay of FCR MAC in multipath channel

7.7 Conclusion

In conclusion, 3G/4G cellular technologies are not a good choice for distribution-side smart grid applications as its usage results in high overhead and latency in data transmission. In order to reduce the control overhead and latency in smart meter data collection, we proposed a new network architecture with two new MAC layer schemes. They are FRRC and FCR MAC. The analytical expressions for average throughput and average packet latency of FCR and FRRC MAC are derived using markov chain analysis. It was observed from the simulation results that the FCR MAC has superior performance in terms of both average throughput and average packet latency when compared to FRRC MAC. The performance of FCR and FRRC MAC is compared against 3G CDMA200 MAC in chapter 9.

Chapter 8

OTRA-THS MAC for Power Outage Data Collection

It was aforementioned in chapter 7 that the data traffic handled by AMI network can be categorized as scheduled data and random data. Customer power consumption data is an example of scheduled data and power outage data is an example of random data. As mentioned earlier, FLEX-MAC changes its mode of operation based on the type of the data being collected. In chapter 7, it was discussed that the FLEX-MAC employs FCR and FRRC MAC layer schemes for scheduled data collection. Also, chapter 7 provided a detailed analysis of the performance of FCR and FRRC MACs. In this chapter, we present Optimum Transmission Rate Adaptive - Time Hierarchical Scheme (OTRA-THS) MAC - a novel MAC layer scheme used by FLEX-MAC for power outage data collection.

The deployment of advanced metering infrastructure by electric utilities poses unique communication challenges, particularly as the number of meters per aggregator increases. When there is a power outage, a smart meter tries to report it instantaneously to the electric utility. In a densely populated residential/industrial locality, it is possible that a large number of smart meters simultaneously try to get access to the communication network to report the power outage. If the number of smart meters is very high on the order of tens of thousands (metropolitan areas), the power outage data flooding can lead to Random Access CHannel (RACH) congestion. Several utilities are considering the use of cellular network for smart meter communications. In 3G/4G cellular networks, RACH congestion not only leads to collisions, retransmissions and increased RACH delays, but also has the potential to disrupt the dedicated traffic flow by increasing the interference levels (3G CDMA). In order to overcome this problem, in this chapter we propose a Time Hierarchical Scheme (THS) that reduces the intensity of power outage data flooding and power outage reporting delay by 6/7th, and 17/18th when compared to their respective values without THS. Also, we propose an Optimum Transmission Rate Adaptive (OTRA) MAC to optimize the latency in power outage data collection.

The remainder of the chapter is organized as follows: THS is explained in section 8.1. OTRA MAC and markov chain analysis is provided in section 8.2. Simulation results are discussed in section 8.3. Section 8.4 concludes the chapter.

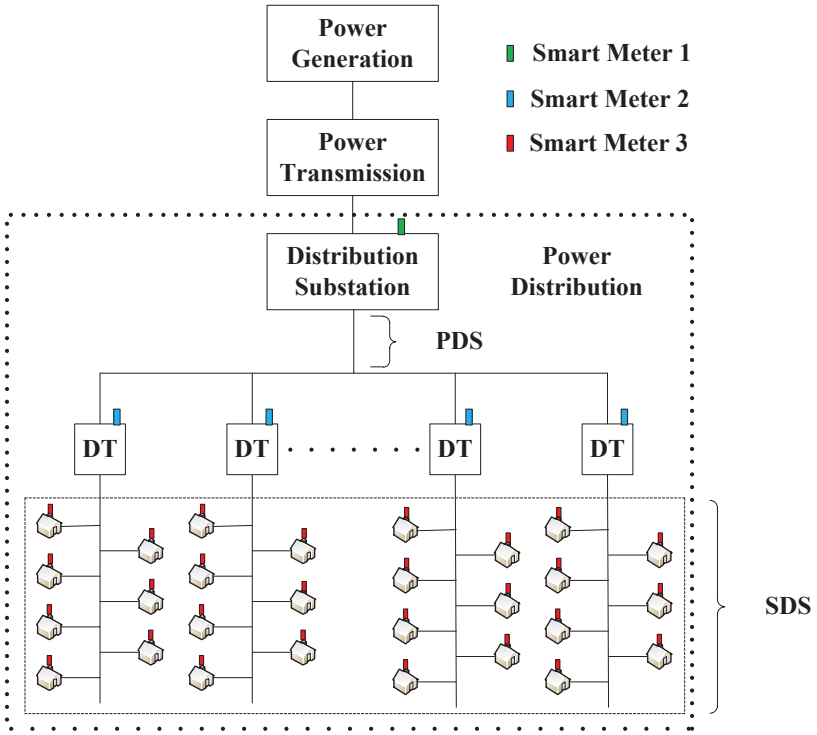

Figure 8.1: Power generation, transmission and distribution system

8.1 THS to Reduce Random Traffic Volume

A high level overview of electric power generation, transmission and distribution system is as shown in Figure 8.1. Based on the operating voltages, distribution system is divided into primary distribution system (2.4 KV to 69 KV) and secondary distribution system (120 V to 600 V). In general, Distribution Substation (DS) transformers step down the transmission system voltage to lower levels. The section of the power network connected between DS and Distribution Transformers (DT) is considered as Primary Distribution System (PDS). PDS consists of primary or distribution feeders that originate from DS. Secondary Distribution System (SDS) connects primary feeders with the industrial and residential customers. SDS

consists of step down transformers and secondary circuits at utilization voltage levels. It is obvious from the above description of power distribution system that there exists a hierarchy in its network. The proposed THS scheme leverages this hierarchy in power distribution system to reduce the amount of traffic generated during a blackout.

It is aforementioned in chapter 7, according to [72], 3G cellular CDMA is appropriate for smart meter data collection. However, some utilities are installing hierarchical RF mesh network operating in ISM band (902 - 928 MHz) for smart meter data collection [24] [52]. As the interference in ISM band is higher than cellular bands, RF mesh network data transmissions are limited to smaller distances when compared to cellular data transmissions and hence RF mesh employs repeaters, collectors in the communication path between the data aggregator (analogous to BS in cellular) and smart meter [52]. Irrespective of the type of the data collected, i.e., power consumption or power outage data, RF mesh network employs the same hierarchy (intermediate repeaters and collectors).

To the best of our knowledge, none of the previous research works proposed to use different approach for collecting power outage data and power consumption data. In this chapter, we propose THS to reduce the intensity of the outage data generated in a smart meter network during a blackout. The difference between the *hierarchy* in the proposed scheme and the *hierarchy* in RF mesh network is that, the proposed scheme exploits the hierarchy in the power distribution network to reduce the random data traffic volume while the RF mesh network uses a hierarchical communication network to collect the data. Once again, we assume that the smart meter network employs a single hop communication between the BS

and a smart meter for power consumption data collection and in this chapter, we propose to use the THS for power outage data collection.

In THS, we assume that there exists three types of smart meters, i.e., SM1, SM2 and SM3. SM1 is installed at DS, SM2 is installed at DT and SM3 is installed at customer's house. We also assume that SM1, SM2 and SM3s report respectively with the time delays t_1, t_2 and t_3 after a blackout. Smart meters take these delays into account only in outage data reporting and ignore them for all other data transfers. This change in the smart meter behaviour can be easily introduced by modifying the smart meter MAC software. THS works as follows:

Case i): The major blackouts in U.S. and Europe are due to the failures in power transmission system [32]. Therefore, in the case of a large scale blackout, it is very likely that along with the DS, all the customers that are fed by the DS are also out of power. Hence, instead of each individual SM3 reporting power outage to a BS, SM1 present at the DS reports to the BS that all the customers that are fed by it are out of power. Once BS receives power outage message from SM1, it sends a broadcast message to all the SM2s and SM3s under the coverage of SM1 that, it is aware of the power outage and it is not necessary to report the outage. Thus, with the use of THS, the entire uplink power outage reporting traffic can be suppressed by a single packet transfer on the uplink from SM1 to BS and a broadcast message on the downlink from BS to all SM2s and SM3s. This is assuming that the downlink wireless channel is error free. But in reality the wireless channel is prone to errors and hence the broadcast message may have to be sent more than once for the successful reception of message by all the SMs. The number of times the BS has to send the broadcast message

depends on the wireless channel characteristics, number of SMs, distance between BS and SMs and the transmit power allocated to the broadcast channel. The first three parameters are given and cannot be modified by the designer but the amount of transmit power allocated to the broadcast channel can be varied to find the optimum number of times a broadcast message has to be transmitted. Therefore, the problem we intend to study can be briefly stated as follows:

"*Given the number of SMs (N), the distance between the BS and SMs (d_n), the wireless channel characteristics and the transmit power (P_t) allocated to the broadcast channel, find the average number of times (N_t) a BS has to transmit the broadcast message such that it is successfully received by all the SMs in the network with a probability k*"

In order to study the above problem, we assume that the smart meters are uniformly distributed in a R km radius cell. The wireless channel is assumed to be a multipath ('L' paths) Rayleigh fading channel. COST 231 Walfisch-Ikegami Propagation Model is used for path loss calculations. It is also assumed that each smart meter is equipped with a rake receiver of 'F' fingers. The BER (p_b) of DS-CDMA system with F-finger rake receiver is given by [77].

$$p_b = \left[\frac{1}{2}\left(1-\sqrt{\frac{\bar{\beta}}{1+\bar{\beta}}}\right)\right]^F \sum_{k=0}^{F-1}\binom{F-1+k}{k}\left[\frac{1}{2}\left(1-\sqrt{\frac{\bar{\beta}}{1+\bar{\beta}}}\right)\right]^k \tag{8.1}$$

Here,

$$\bar{\beta} = \begin{cases} \left(\frac{E_b}{N_0 * L}\right) & \text{ignoring inter-path interference} \\ \left(\frac{N_0}{E_b} * L + \frac{L-1}{\rho N}\right)^{-1} & \text{with inter-path interference} \end{cases} \tag{8.2}$$

Let the number of bits in a packet be m and let 't' be the error correction capability of the coding scheme. Assuming that the BER of each bit is i.i.d, the Packet Success Rate (PSR) of m^{th} smart meter is given as follows

$$P_m = \sum_{l=m-t}^{m} \binom{m}{l} p_{bs}^{l} (1 - p_{bs})^{m-l} \tag{8.3}$$

Here, $p_{bs} = 1 - p_b$ is the bit success rate. BER in equation 8.1 is dependent on $^{E_b}/_{N_0}$ and $^{E_b}/_{N_0}$ depends on the transmit power (R_t). Using link budget analysis, the relationship between the transmit power and $^{E_b}/_{N_0}$ is given as follows

$$\frac{E_b}{N_0} = P_t - PL - NF - KTB + PG \tag{8.4}$$

Here, NF is Noise Figure (dB), K is Boltzmann constant, T is Temperature, B is Bandwidth, PG is processing gain. The probability that the broadcast message is successfully received by m_{th} smart meter in N_t slots is

$$\alpha_m = \sum_{n=1}^{N_t} (1 - P_m)^{n-1} P_m \tag{8.5}$$

$$= P_m \sum_{n=1}^{N_t} (1 - P_m)^{n-1} \tag{8.6}$$

Let $q_m = 1 - P_m$ and using the summation of geometric series

$$\sum_{n=1}^{N} q_m^{n-1} = \sum_{r=0}^{N-1} q^r = \frac{1 - q_m^N}{1 - q_m} \tag{8.7}$$

equation 8.6 can be rewritten as

$$\alpha_m = P_m * \frac{1 - q_m^N}{1 - q_m} \tag{8.8}$$

substituting $q_m = 1 - P_m$, α_m is given as follows

$$\alpha_m = 1 - (1 - P_m)^{N_t} \tag{8.9}$$

The probability that the broadcast message is successfully received by all the smart meters in N_t slots is the product of α_m's of all the smart meters and this probability is given in the problem statement as k. Hence, the value of N_t that satisfies equation 8.10 is the number of times a base station has to transmit the broadcast message such that the message is successfully received by all the smart meters with probability k.

$$k = \prod_{m=1}^{N} \alpha_m = \prod_{m=1}^{N} 1 - (1 - P_m)^{N_t} \tag{8.10}$$

Case ii): Consider the scenario with a fault in the primary feeder that is connected between DS and DT. In this case, DS is not experiencing outage but all the DTs and customers are out of power. As per [9], each pad-mount/pole-mount DT can supply power from 7 to 8

houses. Therefore, a single DT can report the outage to the BS on behalf of 7 to 8 houses, which significantly reduces the traffic during an outage. Similar to the above case, once BS receives power outage message from a SM2 at a DT, BS sends a message on the broadcast channel to the SM3s under the coverage of the DT that, it is aware of the power outage and it is not required to report the outage. In this case, the number of outage reportings and the volume of RACH traffic generated on the uplink with THS during an outage can be reduced to approximately 1/7th of that generated without THS. Therefore, in the worst case scenario, i.e., when the number of smart meters handled by a BS is around 30000 [4], the use of THS reduces the number of outage reportings from 30000 to 4285. In this case, we use markov chain analysis to find the average number of outage reportings and the average latency in outage data collection, which is presented in section 8.2.

Case iii): In this case, we assume that a fault occurs in the secondary feeder or DT. As the number of houses fed by a DT is less than 8, the traffic generated in this case is very less and hence the BS can handle the outage traffic from SM3s similar to mobile traffic.

Whenever there is a power outage, SM3s do not know the reason for it, i.e., whether the power outage is due to a transmission system failure or a fault in the primary feeder or secondary feeder (the three cases discussed above). Therefore, SM3s cannot decide whether they have to report the power outage or whether SM1/SM2 will report on their behalf. Hence, we maintain a *time hierarchy* (time delays) in power outage reportings of the three types of smart meters and there exists a relationship between these time delays, i.e., $t_1 < t_2 < t_3$. It is upto the network designer to choose these values.

8.2 Optimum Transmission Rate Adaptive MAC

Let N be the number of smart meters reporting the outage. When ever an outage occurs, a smart meter randomly selects one of the available M spreading codes and transmits the packet with a probability λ_n. Here n represents the number of smart meters reporting the outage in the current time slot. In other words, the probability with which smart meters transmit the outage packet varies with the time slot and the optimum transmission probability λ_n is selected such that the PODCL is minimized. If a smart meter transmission is successful, BS sends an ACK on the downlink. On the other hand if the transmission is unsuccessful, a NACK is transmitted and the smart meter retransmits the packet with the probability λ_n.

8.2.1 Markov Chain Analysis

In order to derive the average number of outage reportings and the average data collection latency, markov chain analysis is used. As the number of smart meters reporting the outage reduces as time progresses from the instance of an outage, we use transient analysis. An outage is an impulse to the system that sees a decaying response. A state in a markov chain is defined by the number of smart meters reporting the outage. The one step transition

probability from state j to k is given by equation 8.11.

$$P_{jk} = \begin{cases} \sum_{n=0}^{j} \sum_{cs=0}^{\min(M,n)} \binom{j}{n} \lambda^n (1-\lambda)^{j-n} f(cs|n, M, p_s) \text{ if } (j-k == cs) \\ 1 \qquad \text{if}(j == 0)\&\&(k == 0) \\ 0 \qquad j < k \end{cases} \tag{8.11}$$

In equation 8.11, $\binom{j}{n}\lambda^n (1-\lambda)^{j-n}$ is the probability of n smart meters transmitting power outage packets given that j smart meters are attempting to transmit outage packets with probability λ. $f(k|n, M, p_s)$ is the conditional probability that k packets are successful out of n smart meter transmissions, p_s is the packet success rate and M is the number of spreading codes. $f(k|n, M, p_s)$ is evaluated by the following recursive expression.

$$\begin{aligned} f(k|n, M, p_s) = \sum_{i=0, i\neq 1}^{n} p_n^i f(k|n-i, M-1, p_s) \\ + p_n^1 f(k-1|n-1, M-1, p_s) ps \\ + p_n^1 f(k|n-1, M-1, p_s)(1-ps) \end{aligned} \tag{8.12}$$

In equation 8.12, $p_n^i = \binom{n}{i}\left(1-\frac{1}{M}\right)^{n-i}\left(\frac{1}{M}\right)^i$ is the probability that i out of n smart meters transmit over an arbitrary channel, such as the first channel, with the initial conditions

$$f(k|n, 0, p_s) = \begin{cases} 1 \text{ if } k = 0 \text{ and any } n \\ 0 \text{ if } k > 0 \text{and any } n \end{cases} \tag{8.13}$$

$$f\left(k|0,m,p_s\right) = \begin{cases} 1 \text{ if } k = 0 \text{ and any } m \\ \\ 0 \text{ if } k > 0 \text{and any } m \end{cases} \tag{8.14}$$

$$f\left(k|1,m,p_s\right) = \begin{cases} (1-p_s) \text{ if } k = 0 \text{ and } m \geq 1 \\ \\ p_s \text{ if } k = 1 \text{ and } m \geq 1 \\ \\ 0 \text{ if } k > 1 \text{ and } m \geq 1 \end{cases} \tag{8.15}$$

$$f\left(k|n,1,p_s\right) = \begin{cases} 1 \text{ if } k = 0 \text{ and } n > 1 \\ \\ 0 \text{ if } k > 0 \text{ and } n > 1 \end{cases} \tag{8.16}$$

and

$$f\left(k|n,m,p_s\right) = 0 \text{ if } k < 0 \tag{8.17}$$

It is obvious from the equation 8.11 that the markov chain has an absorbing state. Given a markov state i, transient analysis can be used to calculate the mean time to absorption, t_i and the mean number of transmissions, u_i, until absorption. Let

$$t \Leftrightarrow [t_1, t_2, ..., t_n] \tag{8.18}$$

$$u \Leftrightarrow [u_1, u_2, ..., u_n] \tag{8.19}$$

Let us define Q as the transition matrix of all transient states, we have

$$t = (I - Q)^{-1} C. \tag{8.20}$$

Where I is the identity matrix and C represents a vector with all entries equal to 1. Similarly the expression to calculate u is given as follows:

$$u = (I - Q)^{-1} v \tag{8.21}$$

where $v = [1 * \lambda_1, 2 * \lambda_2, ..., m * \lambda_m)]$ is the vector of the average number of transmissions from a state. m is the number of transient states.

8.2.2 Selection of Optimum Transmission Probabilities

As mentioned earlier, the smart meter optimum transmission probabilities vary with time slot. The main objective of this section is to find the optimal transmission probabilities to minimize the PODCL. The absorbing times in equation 8.20 can be written as

$$t_m = 1 + \sum_{i=1}^{m} p_{mi} t_i \tag{8.22}$$

In [56], Backward Recursive Dynamic Programming (BRDP) approach is used for adaptive cluster based data collection in sensor networks with direct sink access to find the optimum transmission rate. In this research work, we use the same approach for smart meter power

SM ID (16 b)	Time (10 b)	Voltage (12 b)	Power Factor (12 b)	Frequency (16 b)	Real Power (9 b)	Reactive Power (9 b)	CRC - 8 (9 b)

Figure 8.2: Random data frame

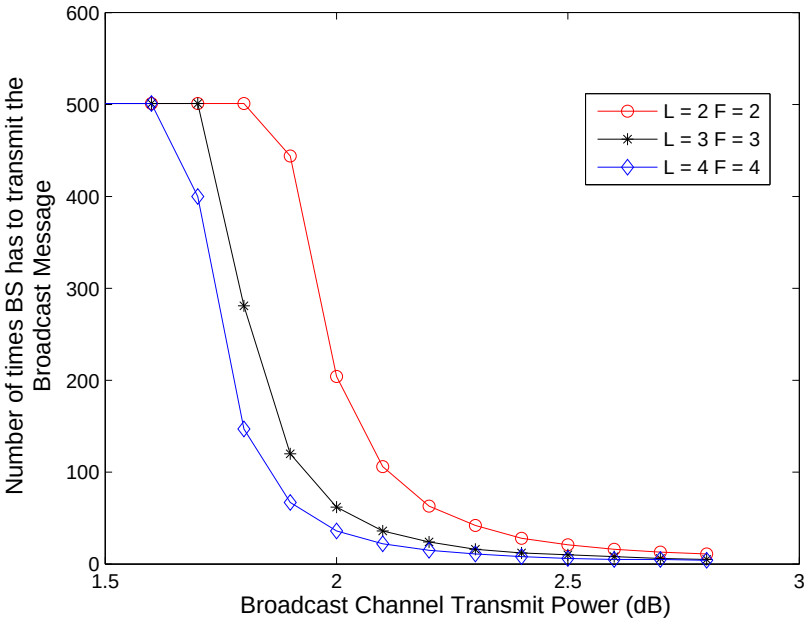

Figure 8.3: Number of times a BS has to transmit the broadcast message with k = 0.99999 vs. Broadcast channel transmit power

outage data collection. The optimal values of λ_m can be determined by using BRDP [78].

$$\lambda_m^* = \underset{0 \le \lambda \le 1}{\operatorname{argmin}} \frac{1}{1 - p_{mm}} \left(1 + \sum_{i=1}^{m-1} p_{mi} t_i \right) \tag{8.23}$$

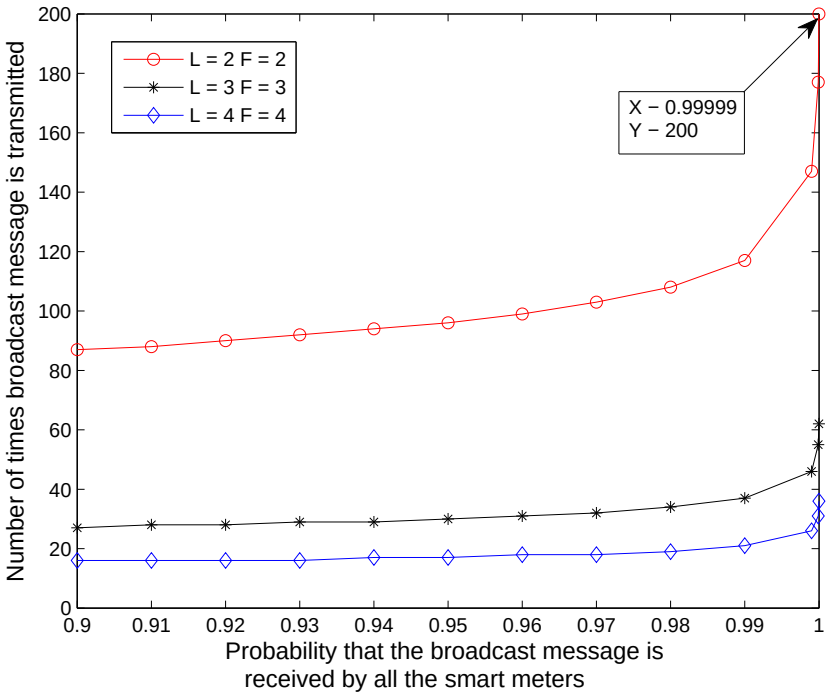

Figure 8.4: Number of times a BS has to transmit the broadcast message vs. Probability that the broadcast message is received by all the smart meters

8.3 Simulations and Results

The simulation parameters are as shown in table 8.1. Random data frame format is as shown in Figure 8.2. We used a 2/3 rate convolutional coding scheme with an error correction capability of 3. Figure 8.3 shows the plot of the number of times a broadcast message has to be transmitted versus the broadcast channel transmit power for different values of F and L. Here L is the number of multipath components and F is the number of rake receiver fingers. As expected, it can be seen from the Figure 8.3 that the number of times a BS has to transmit the broadcast message reduces as the broadcast channel transmit power increases. As the number of multipath components and the number of rake receiver fingers

increases, the number of times the BS has to transmit the broadcast message decreases. In Figure 8.3, when the broadcast channel transmit power is 2 dB, for $L = 2, F = 2$ the BS has to transmit the broadcast message around 205 times, for $L = 3, F = 3$ the broadcast message has to be transmitted 62 times, for $L = 4, F = 4$ it is sufficient for the BS to send the broadcast message 36 times.

Figure 8.4 shows the plot of the number of times (N_t) a BS has to transmit the broadcast message versus the probability (k) that the broadcast message is received by all the smart meters for a fixed broadcast channel transmit power (P_t) of 2 dB. As the probability k increases, the number of times a BS has to transmit the broadcast message increases. When L = 4 and F = 4, for a probability (k) of 0.9, BS has to transmit the broadcast message atleast 20 times and for a probability of (k) of 0.99999, the broadcast message has to be transmitted atleast 36 times by the BS.

The simulation results of *case ii* in section 8.1, i.e., the mean number of outage reportings (u) and the mean PODCL (t) are as shown in Figure 8.5 for M = 7 and N = 10. It can be observed from Figure 8.5 that the values of t and u calculated using analytical expressions and simulations are matched. Figure 8.5 presents simulation results without OTRA (NOTRA) scheme, i.e., the transmission rate λ is kept constant throughout the data collection interval. Figure 8.6 presents the results of OTRA MAC for M = 7 and N = 10. Figure 8.6 also shows the variation of the optimal transmission probabilities with the time slot number after an outage. Initially, during time slot 1, the number of smart meters reporting the outage is 10. Hence, the transmission probability is low, i.e., 0.4. As the time progresses, the number

Table 8.1: Simulation parameters

Parameter	**Value**
Transmit Power (P_t)	24 dBm
Smart meter antenna gain	2 dBi
Effective Isotropic Radiated Power (EIRP)	26 dBm
Base station noise figure	2 dB
Sinc pulse cut off factor	0.22
Transmission scheme	FDD
Uplink bandwidth	2.5 MHz
Downlink bandwidth	2.5 MHz
Chipping rate	2.0491 Mcps
Spreading code length	128
Data rate	16 Kbps
Frame size	10 msec
Cell radius	5 Km
Path loss model	COST 231 WI
Base station antenna gain	18 dBi
Cable loss in base station	2 dB
Max path loss	166.6 dBm
$^{E_b}/_{N_0}$	5.29 dB
Temperature	290 K

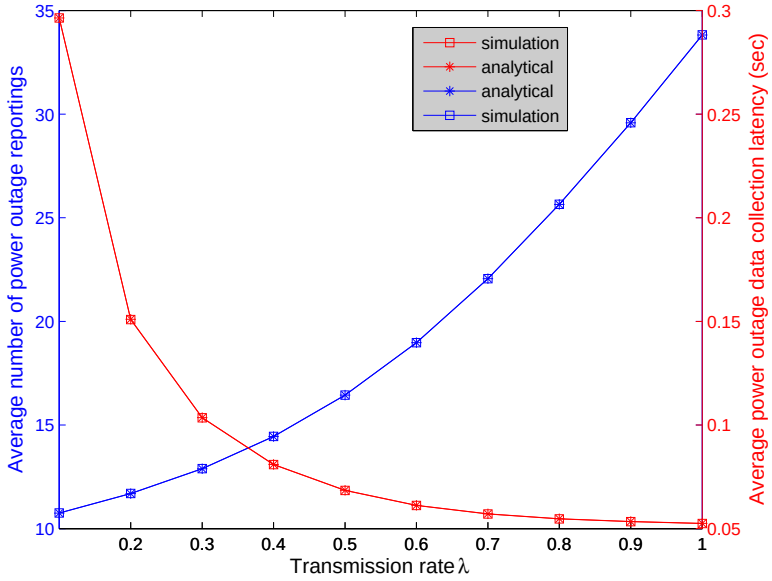

Figure 8.5: Comparison of analytical and simulation results

of smart meters reporting the outage reduces because of some successful transmissions in previous time slots. Hence, optimal transmission rate increases to 0.9 with time. Also, Figure 8.6 shows the optimal PODCL from different stages of markov chain but the optimal PODCL from all smart meters is obtained from time slot 1, i.e., 0.03 sec. On the other hand, the optimal PODCL of NOTRA scheme is 0.06 sec with a constant transmission rate of 0.1 (Figure 8.5). For large values of M and N, evaluating equation 8.12 is computationally very expensive. The number of smart meters in a cell are on the order of tens of thousands. Hence, for $M = 127$ and $N = 10000$, evaluating equation 8.12 was infeasible. As shown in Figure 8.5, simulated and analytical results are matched for different values of λ. Hence, the results presented from now on are obtained using simulations instead of analytical expressions. We considered three different values for the total number of smart meters, i.e., 10000, 20000

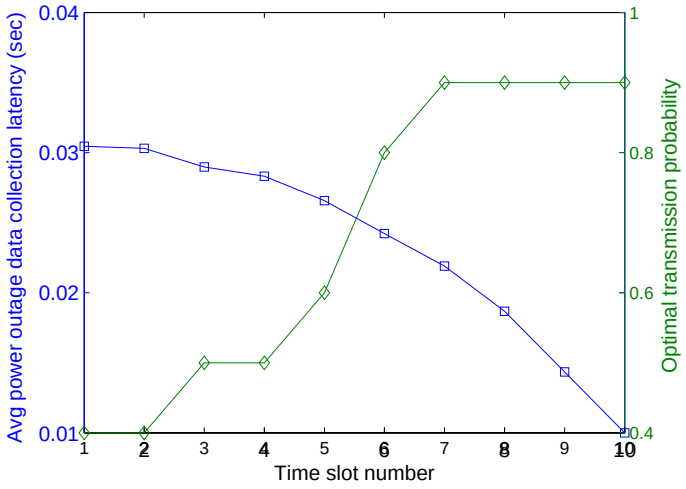

Figure 8.6: Optimal outage data collection latency and optimal transmission rates vs time slot number starting from an outage

and 30000. The mean PODCL of NOTRA MAC, OTRA MAC and OTRA-THS MAC are as shown in table 8.2. When the number of smart meters is 30000, the mean PODCL of OTRA MAC and OTRA-THS MAC are respectively 1/3rd and 1/16th of the data collection latency of NOTRA MAC. As equation 8.12 is computationally intensive, finding optimal transmission probabilities using equation 8.23 is also computationally expensive. Hence, optimal transmission rate of smart meters in time slot n is calculated using equation 8.24.

$$\lambda_n^* = \frac{K}{N_n} \tag{8.24}$$

Here K is the system capacity and N_n is the number of smart meters reporting the outage in time slot n. Figure 8.8 shows the plot of the mean number of outage reportings (u) and the mean PODCL (t) of OTRA-THS scheme for different values of K. As the value of K increases from 10 to 110, t decreases and reaches minimum at K = 90, i.e., at the system

Table 8.2: Mean PODCL in sec

Number of Smart meters	NOTRA	OTRA	OTRA-THS
10000	20.4	8.48	1.252
20000	42.4	17.08	2.46
30000	65.66	25.48	3.68

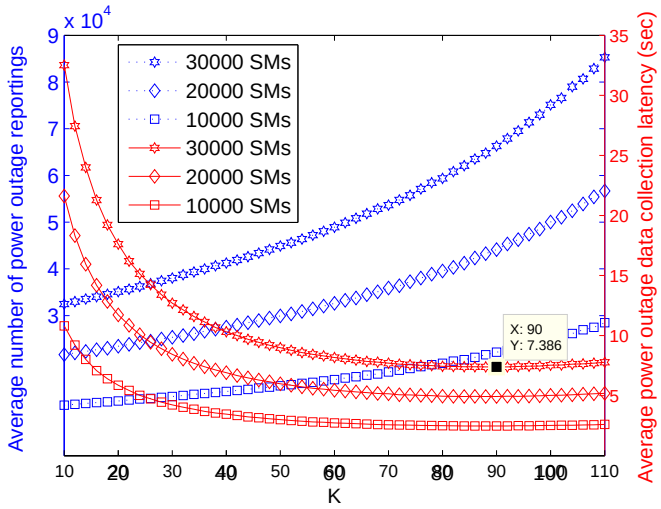

Figure 8.7: Mean number of power outage reportings (dotted line) and mean power outage data collection latency (in sec) vs parameter K with OTRA based MAC (when $K = 90$, minimum latency is 7.386 sec)

capacity and again increases from 90 to 110. On the other hand, u increases as the value of K increases from 10 to 110. As K is a system parameter, BS can send optimal transmission rate (equation 8.24) to be used by smart meters for transmission in the next slot as a part of NACK packet.

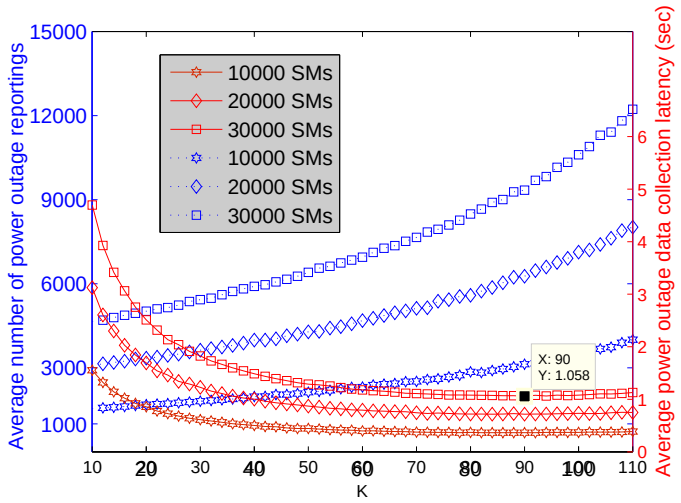

Figure 8.8: Mean number of power outage reportings (dotted line) and mean power outage data collection latency (in sec) vs parameter K with OTRA-THS based MAC (when $K = 90$, minimum latency is 1.058 sec)

8.4 Conclusion

In this chapter, OTRA-THS MAC that aids in reducing the smart meter power outage data collection latency was described. Markov chain transient analysis is used to derive analytical expressions for the mean number of outage reportings and the mean outage data collection latency. It can be concluded from the simulations that the average power outage data collection latency (1.058 sec) of OTRA-THS MAC is 1/16th of the MAC without OTRA-THS scheme (16.676 sec).

Chapter 9

CDMA2000 MAC Layer Simulations

As mentioned earlier in chapter 3, this dissertation assumes the use of a private CDMA2000 network for smart meter data collection as a baseline for comparison. Chapter 7 and 8 discussed the performance of the proposed MAC layer schemes in this dissertation. This chapter presents CDMA2000 MAC layer simulations in terms of average throughput, packet delay and overhead. Also, this chapter compares the performance of CDMA 2000 MAC and the proposed FCR and OTRA-THS MAC layer schemes.

In CDMA2000, depending on its mode of operation, a Mobile Station or Smart Meter selects one of the three reverse access channels, i.e., Random Access CHannel (RACH), Enhanced Access CHannel (EACH) or Reverse Common Control CHannel (RCCCH) to gain access to the network. Smart meters not only use the reverse access channels for gaining access to the network but also to send small sized messages. As mentioned in chapter 7, the size of the

Table 9.1: Simulation parameters

Parameter	**values**
PAM_SZ	1
MAX_CAP_SZ	3
MSG_PSIST	varied
PSIST	varied
PD	$2^{-}((PSIST/4) + (MSG\_PSIST))$
FRAMESIZE	((PAM_SZ * 0.01) + (MAX_CAP_SZ * 0.02)s
PROBE_BACKOFF	15
SEQUENCE_BACKOFF	15
NUM_RANDOM_CHANNELS	50

data generated by smart meters is around 10 Bytes. Hence, it is assumed that the smart meters use reverse access channels to transfer data to the base station.

As mentioned above, in CDMA2000 network, there exists three different reverse access channels, i.e., RACH, EACH and RCCCH. How does a smart meter select one of these three reverse access channels to communicate with the base station? According to [87], RACH is used if the message size is few RACH slots and EACH is used if the message size is around (100 - 150 ms i.e. 120 - 180 Bytes) and RCCCH is used for messages longer than 150 ms (180 Bytes). According to CDMA2000 RACH configuration, the smart meter message size of 10 Bytes is equal to 3 RACH slots. Hence, we assume that the RACH is used as the reverse access channel for smart meter data collection. Readers are advised to refer to [93] for the details of the random access procedure a smart meter goes through in a CDMA2000 network to get access to the network or to send small sized messages via a RACH.

Matlab is used for CDMA2000 MAC layer simulations. In simulation, packet errors are not taken into consideration and the success of a packet transmission depends only on the

Table 9.2: Simulation results

tr (sec)	**MSG_PSIST**	**PSIST**	**Avg Delay (sec)**	**Avg Through-put (per sec)**	**Avg Reportings**	**Total Delay (sec)**
0	7	16	287	23.184	36597	1293.4
20	7	16	288.05	21.84	36149	1361.85
40	7	16	287	21.53	36177	1364.1
60	7	12	149	45.08	57983	661.4
80	7	12	141.68	46.2	42865	647.65
100	7	8	102.33	71.68	1625685	417.75
120	7	0	18.02	127.96	248079	234
130	7	0	2.13	230.72	56226	129.5
140	3	0	1.987	214.72	50184	139.5
160	3	0	1.75	188.44	44626	159
180	3	0	1.61	168	41745	178.5

collisions. If two smart meters transmit packets on the same RACH, it is considered a collision and both the packet transmissions are unsuccessful. On the other hand, if there is no collision the packet transmission is considered to be successful. Table 9.1 lists the values of the parameters used in CDMA2000 MAC layer simulation. The maximum value of MSG_PSIST is 7 and in simulations it is varied from 0 to 7. PSIST is varied from 0 to 20 with an increment of 4. PAM_SZ is the preamble size and it is assumed to be 10 ms. MAX_CAP_SZ is the message size. As explained earlier, MAX_CAP_SZ is 3 RACH slots and one RACH slot is 20 ms. Hence, MAX_CAP_SZ is 60 ms.

The simulation results are as shown in Table 9.2. Avg Delay is measured in seconds, Average Throughput is the number of successful packets per sec, Total Delay is the delay in sec of collecting data from all the smart meters and *tr* is the randomization delay in seconds.

Table 9.3: Comparison of mean data collection latency (secs) of CDMA2000, FCR and OTRA-THS MACs

NSM	**CDMA2000**	**FCR**	**OTRA-THS**
10000	41.51	14.23	5.634
20000	88.622	27.96	11.07
30000	130.34	42.01	16.56

Whenever a smart meter intends to transmit a packet, it randomly selects a delay in the range of [0,$tr * N_{RACH}$] and transmits the packet after the delay. N_{RACH} is the number of frames per sec and the frame size is 70 msec.

From Table 9.2, it can be observed that the average throughput and the total delay in collecting data from all the smart meters are optimum when $tr = 130$ sec. The maximum throughput is 230.72 packets per sec and the minimum total delay is 129.5 seconds. At $tr = 130$, the total number of packet transmissions including retransmissions is 56226. Among all the possible combinations of parameters that are explored, $tr = 130$ with $MSG\_PSIST = 3$ and $PSIST = 0$ was found to be best optimum operating point of CDMA2000 MAC for smart meter data collection. In chapter 7 and 8, analysis and simulations related to the average throughput and the average delay of FCR and OTRA-THS MACs are presented. Table 9.3 compares the performance of FCR and OTRA-THS MACs with CDMA2000 MAC. From Table 9.3 it can be concluded that, when the number of smart meters is 30000, the mean scheduled data collection latency and mean power outage data collection latency of FLEX-MAC are respectively 1/3rd and 1/8th of the mean data collection latency of CDMA2000 MAC. In other words, the proposed FLEX-MAC protocols, i.e., FCR and OTRA-THS schemes

Table 9.4: Power consumption parameters

Parameter	**values (mW)**
CELL_PCH/URA_PCH	30
CELL_RCH	200
CELL_DCH	400
Power Amplifier	93
RF transmit IC	103
RF receive IC	130
Baseband	130

Table 9.5: Mean energy consumption (Joules) of smart meters using CDMA2000 and OTRA-THS MACs

NSM	**CDMA2000**		**OTRA-THS**	
	Total	Avg	Total	Avg
10000	54884.7	1.827	790.66	0.0791
20000	107406	3.58	2690.9	0.1345
30000	502956	16.76	5712.4	0.1904

reduce the smart meter data collection latencies by a considerable amount when compared to CDMA2000 MAC.

Figure 9.1 shows the change in average data collection latency with the number of channels in CDMA2000 MAC. As shown in Table 9.3, FCR MAC can collect scheduled data from 30000 smart meters with 50 spreading codes in 42 seconds. In Figure 9.1, this is shown as a straight line (green color). On the other hand, it can be observed from Figure 9.3 that the CDMA 2000 MAC requires 175 spreading codes to collect data from 30000 smart meters in the same amount of time (42 seconds), i.e., the proposed FCR MAC is 3.5 times more efficient than the CDMA2000 MAC in terms of the number of spreading codes required to collect data from the smart meters.

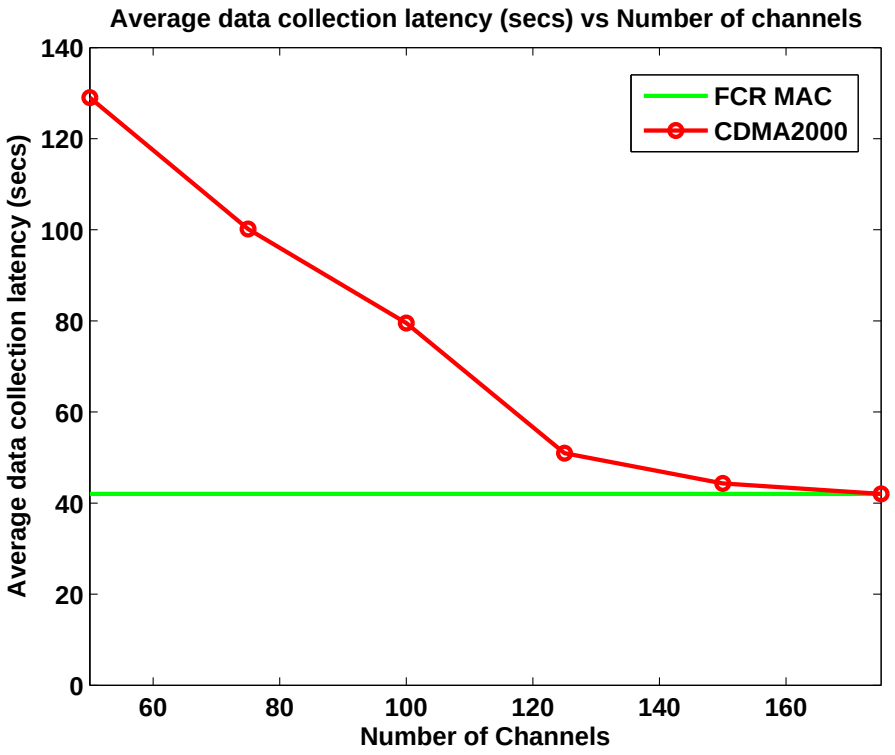

Figure 9.1: Average data collection latency vs Number of channels in 3G CDMA2000 MAC

In AMI network, a smart meter draws the power required for its operation from the same power system network bus that it is monitoring. On the other hand, during a power outage, a smart meter relies on an external battery to report the power outage to the electric utility. Hence, during the power outage reporting, reducing the energy consumed by a smart meter increases its battery life. The power consumption of different components of a CDMA radio is a confidential information and obtaining such information is extremely difficult. CDMA2000 power consumption parameters were not available in the literature but we were able to find WCDMA parameters. Table 9.4 lists the power consumption of WCDMA Radio Resource Control (RRC) states, power amplifiers, RF and baseband IC's [96] [37]. There exists slight differences in the RRC states of WCDMA and CDMA2000 but the energy consumption is

more or less the same in both. Hence, for the purpose of simulations, we used WCDMA power consumption parameters. Table 9.5 compares the energy consumption of the smart meters using CDMA2000 and OTRA-THS MACs for reporting the power outage. Number of smart meters is varied as 10000, 20000 and 30000. Table 9.5 presents both the total energy consumed by all the smart meters and the average energy consumption per smart meter. When the number of smart meters is 30000, the average energy consumption of a smart meter reporting the power outage using OTRA-THS MAC and CDMA2000 MAC is respectively 0.1904 and 16.76 joules i.e the CDMA2000 MAC approximately consumes 88 times more energy than the proposed OTRA-THS MAC. In other words, the proposed OTRA-THS MAC is significantly energy efficient when compared to CDMA2000 MAC for smart meter power outage data collection.

Chapter 10

Conclusion

In this dissertation, we studied two problems related to the power grid and proposed possible solutions that improve the reliability and reduce the maintenance cost of the grid. First problem involving Zone 3 relay mis-trips in Distance Relaying Protection Scheme (DRPS) is a rare, but a long-standing, problem of transmission grid and it is one of the major causes of blackouts in the USA and Europe. This dissertation proposed an agent based DRPS that reduces the Zone 3 relay mis-trips. The novelty of the proposed scheme is that, unlike the previous research works that use intrusive agent based schemes, our solution employs non-intrusive agents. In other words, agents in the proposed scheme do not take over the relaying functionality. Relay protection engineers are not sure if an agent (software or hardware) can be a surrogate to a relay and hence they do not like the idea of agents taking over the functionality of relays. Hence, the proposed non-intrusive agent based DRPS may be more appealing to protection engineers when compared to the available agent based solutions.

DRPS is a time critical application. In order to verify if the proposed scheme meets the requirements of zonal tripping times or not, different network topologies (star, power system) with different physical media of communication (copper, optical) and different protocols (TCP, UDP) are investigated. The OPNET and NS-2 simulation results indicate that the proposed scheme meets the timing requirements of DRPS with both star and power system topology based communication network, but the star topology comes with an overhead in terms of the number of communication cables needed to set up the network when compared to the power system topology based network. Hence, we suggest the use of power system network topology with optical fiber cables as the physical media of communication and reliable TCP/IP protocol to set up a communication network among agents in DRPS.

In the proposed agent based DRPS, we assume that the communication network that connects different protection relays in transmission grid is populated with master and slave agents. A group of slave agents report their associated relay status to the master agent and any slave relay agent can query the master agent for the status of other slave relay agents. In a larger power system network consisting of thousands of buses, the number of the required master agents is high and the placement of master agents is a challenging task. Hence, the problem of minimizing the number of master agents required to serve the slave agent queries and finding an optimum location for the master agents is modelled as a multiple facility location problem. Optimization models are developed and simulated using *IBM ILOG CPLEX*. As the DRPS is a real time system, using formal verification techniques, we verified the proposed non-intrusive agent based DRPS for timing correctness and deadlocks.

The second problem studied in this dissertation is related to the distribution side of the smart grid, i.e., the Advanced Metering Infrastructure. We classified the data traffic handled by the AMI as scheduled and random data, proposed FLEX-MAC - a novel and flexible MAC layer protocol for data collection. In order to collect the scheduled data, FLEX-MAC employs Frame and Channel Reserved (FCR) or Frame Reserved and Random Channel (FRRC) MAC layer schemes. Using the steady state markov chain analysis, analytical expressions for the average throughput and the average packet delay are derived for FCR and FRRC MAC. The analytical and simulation results indicate that the FCR MAC results in a higher throughput and lower packet delay when compared to the FRRC MAC. In order to collect the power outage data, FLEX-MAC employs the OTRA-THS MAC. The optimum transmission rate adaption and time hierarchical features of the OTRA-THS MAC significantly reduces the number of power outage reportings and also decreases the power outage data collection latency when compared to 3G CDMA2000. Based on the analysis and simulation results presented in this dissertation, it can be concluded that the proposed MAC layer schemes reduce the control overhead by 2144%, mean power consumption data collection latency by 1/3rd and mean power outage data collection latency by 1/8th when compared to the average data collection latency of 3G CDMA2000. During a power outage, a smart meter relies on an external battery to report the outage to the utility. When the number of smart meters reporting an outage is 30000, the average energy consumption of a smart meter reporting an outage using the proposed OTRA-THS MAC is significantly lower (1/88) than the average energy consumption of a smart meter employing 3G CDMA2000 MAC.

Bibliography

[1] SAG (Stake holders advisory group) meeting with southern company.

[2] SEL-421 Protection, Automation, and Control System. http://www.selinc.com/sel-421/.

[3] IEEE standard for relays and relay systems associated with electric power apparatus. *ANSI IEEE Std C37.90-1989*, 1989.

[4] 3GPP. Study on RAN improvements for machine-type communications (Release 11). Technical report, 2011.

[5] 3GPP. Requirements for further advancements for Evolved Universal Terrestrial Radio Access (E-UTRA) (LTE-advanced). Technical report, 2012.

[6] 3GPP. Physical channels and mapping of transport channels onto physical channels (FDD). Technical report, February 2013.

[7] Rajeev Alur and David Dill. Automata-theoretic verification of real time systems, 1995.

[8] Rajeev Alur and David L. Dill. A theory of timed automata. *Journal of theoretical computer science*, 126:183–235, April 1994.

[9] Austin Energy. Pad mounted transformer, Dec 2011.

[10] Johan Bengtsson, Kim Larsen, Fredrik Larsson, Paul Pettersson, and Wang Yi. UPPAAL a tool suite for automatic verification of real-time systems. In Rajeev Alur, ThomasA. Henzinger, and EduardoD. Sontag, editors, *Hybrid Systems III*, volume 1066 of *Lecture Notes in Computer Science*, pages 232–243. Springer Berlin Heidelberg, 1996.

[11] A. R. Bergen and V. Vittal. *Power System Analysis*. Prentice Hall, 2000.

[12] Steve Bible. Spread spectrum: It's not just for breakfast anymore! http://www.tapr.org/ss_intro.html, 2007.

[13] Jacob Brodsky and Anthony McConnell. Jamming and interference induced denial of service attacks on IEEE 802.15.4 based wireless networks. In *SCADA Security Scientific Symposium*, 2009.

[14] B. A. Carreras, V. E. Lynch, I. Dobson, and D. E. Newman. Complex dynamics of blackouts in power transmission systems. *Chaos*, pages 643–652, 2004.

[15] John David Cavanaugh. Protocol overhead in IP/ATM networks, 1994.

[16] CDG 450 Connectivity Special Interest Group. The 450 MHz band for the smart grid and smart metering, Sep 2013.

[17] CDG 450 Connectivity Special Interest Group. Economics of 450 MHz band for the smart grid and smart metering, Sep 2013.

[18] Jie Chen, James S. Thorp, and Ian Dobson. Cascading dynamics and mitigation assessment in power system disturbances via a hidden failure model, 2003.

[19] A. Chockalingam, Weiping Xu, and L.B. Milstein. Performance of a multi-channel packet cdma protocol in a fading environment. In *Vehicular Technology Conference, 1997, IEEE 47th*, volume 2, pages 1024–1028 vol.2, May 1997.

[20] B.H. Chowdhury and S. Baravc. Creating cascading failure scenarios in interconnected power systems. In *IEEE Power Engineering Society General Meeting*, 2006.

[21] Edmund M. Clarke and E. Allen Emerson. Design and synthesis of synchronization skeletons using branching-time temporal logic. In *Logic of Programs, Workshop*, pages 52–71, London, UK, 1982. Springer-Verlag.

[22] M. M. Begovic D. Novosel and V. Madan. Shedding light on blackouts. In *IEEE power & energy magazine*, Jan & Feb 2004.

[23] Ian Dobson and Benjamin A. Carreras. A loading-dependent model of probabilistic cascading failure. In *Probability in the Engineering and Informational Sciences*, pages 15–32, 2004.

[24] EDX Wireless. Smart planning for smart grid ami mesh networks. `http://www.smartgrid.gov/sites/default/files/doc/files/4503_doc_1.pdf`, 2011.

[25] EFFNET AB. The concept of robust header compression, ROHC, 2004.

[26] Electric Light and Power. Itron to deploy cellular communications, smart meters for Texas Cooperative, August 2013.

[27] E. Allen Emerson and Edmund M. Clarke. Characterizing correctness properties of parallel programs using fixpoints. In *Proceedings of the 7th Colloquium on Automata, Languages and Programming*, pages 169–181, London, UK, 1980. Springer-Verlag.

[28] Ericsson. LTE for utilities, Sep 2013.

[29] Zhong Fan, Georgios Kalogridis, Costas Efthymiou, Mahesh Sooriyabandara, Mutsumu Serizawa, and Joe McGeehan. The new frontier of communications research: Smart grid and smart metering. In *Proceedings of the 1st International Conference on Energy-Efficient Computing and Networking*, e-Energy '10, pages 115–118, New York, NY, USA, 2010. ACM.

[30] Tony Flick. *Securing The Smart Grid*. Elsevier, 2011.

[31] Fitzek Frank, Hendrata Stefan, Seeling Patrick, and Martin Reisslein. Header compression schemes for wireless internet access, July 2003.

[32] S. Garlapati, Hua Lin, S. Sambamoorthy, S.K. Shukla, and J. Thorp. Agent based supervision of zone 3 relays to prevent hidden failure based tripping. In *First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 256 –261, Oct. 2010.

[33] E. Geraniotis. Coherent hybrid DS-SFH spread-spectrum multiple-access communications. *IEEE Journal on Selected Areas in Communications*, 3(5):695 – 705, Sep 1985.

[34] M. Gerasimenko, V. Petrov, O. Galinina, S. Andreev, and Y. Koucheryavy. Energy and delay analysis of LTE-advanced RACH performance under MTC overload. In *IEEE Globecom Workshops (GC Wkshps)*, pages 1632–1637, 2012.

[35] Anu Gokhale. Introduction to telecommunications. In *Thomson Delmar Learning*, 2004.

[36] Harbour Research. Smart devices and services how CDMA technology is driving the connected age, May 2013.

[37] Holma Harri and Toskala Antti. *WCDMA for UMTS*, pages 272,579. John Wiley & Sons Ltd., fifth edition, 2010.

[38] Holma Harri and Toskala Antti. *LTE for UMTS : Evolution to LTE-Advanced*, page 520. John Wiley & Sons Ltd., second edition, 2011.

[39] John Newbury Hendrick C. Ferreria, Lutz Lampe and Theo G. Swart. *Power Line Communications : Theory and Applications for Narrowband and Broadband Communications over Power Lines*. John Wiley & Sons, 2010.

[40] T.A. Henzinger, X. Nicollin, J. Sifakis, and S. Yovine. Symbolic model checking for real-time systems. In *Proceedings of the Seventh Annual IEEE Symposium on Logic in Computer Science, 1992. LICS '92.*, pages 394–406, Jun 1992.

[41] K. Hopkinson, Xiaoru Wang, R. Giovanini, J. Thorp, K. Birman, and D. Coury. EPOCHS: A platform for agent-based electric power and communication simulation built from commercial off-the-shelf components. *IEEE Transactions on Power Systems*, 21(2):548 – 558, May 2006.

[42] S.H. Horowitz and A.G. Phadke. Third zone revisited. *IEEE Transactions on Power Delivery*, 21(1):23 – 29, Jan. 2006.

[43] Stanley H. Horowitz and Arun G. Phadke. Power system relaying. In *Research Studies Press Ltd.*, 2004.

[44] Insup Lee. Real Time Systems. http://www.seas.upenn.edu/ lee/09cis480/lec-RTS-web.pdf.

[45] Jeff St John. ATT launches the cellular smart grid as a service : Smart meters, software and volt-var control, hosted by ATT, May 2013.

[46] PAN Jianping. Research - TCP/IP over air links - CDMA/HDR, March 2001.

[47] Hermann Koptez. Real time systems: Design principle for distributed embedded applications. In *The Springer International Series in Engineering and Computer Science*, 1997.

[48] D K. Kothari and I J. Nagrath. *Power System Engineering.* TataMcGraw Hill, 2008.

[49] M. Krishnam, M. Reisslein, and F. Fitzek. Analytical framework for simultaneous MAC packet transmission (SMPT) in a multicode CDMA wireless system. *IEEE Transactions on Vehicular Technology*, 53(1):223–242, 2004.

[50] Kim Guldstrand Larsen, Paul Pettersson, and Wang Yi. UPPAAL in a nutshell. *International Journal on Software Tools for Technology Transfer*, 1:134–152, 1997.

[51] Depeng Li, Z. Aung, J.R. Williams, and A. Sanchez. Efficient authentication scheme for data aggregation in smart grid with fault tolerance and fault diagnosis. In *IEEE PES Innovative Smart Grid Technologies (ISGT)*, pages 1–8, Jan 2012.

[52] B. Lichtensteiger, B. Bjelajac, C. Muller, and C. Wietfeld. RF mesh systems for smart metering: system architecture and performance. In *First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 379 –384, Oct. 2010.

[53] E. Liu, M.L. Chan, C.W. Huang, N.C. Wang, and C.N. Lu. Electricity grid operation and planning related benefits of Advanced Metering Infrastructure. In *5th International Conference on Critical Infrastructure (CRIS)*, pages 1 –5, Sep 2010.

[54] I-Sheng Liu, F. Takawira, and Hong-Jun Xu. A Hybrid token-CDMA MAC protocol for wireless Ad-Hoc networks. *IEEE Transactions on Mobile Computing*, 7(5):557–569, 2008.

[55] N. Logic. SRP experience with integrating synchronized measurements. In *IEEE Power and Energy Society General Meeting*, pages 1–5, July 2010.

[56] Mahdi Lotfinezhad, Ben Liang, and Elvino S. Sousa. Adaptive cluster-based data collection in sensor networks with direct sink access. *IEEE Transactions on Mobile Computing*, 7(7):884–897, 2008.

[57] Simon K. Marvin, Omura K. Jim, Scholtz A. Robert, and Levitt K. Barry. *Spread Spectrum Communications Handbook*. McGraw Hill, 1984.

[58] Daisuke Mashima and AlvaroA. Crdenas. Evaluating electricity theft detectors in smart grid networks. In Davide Balzarotti, SalvatoreJ. Stolfo, and Marco Cova, editors, *Research in Attacks, Intrusions, and Defenses*, volume 7462 of *Lecture Notes in Computer Science*, pages 210–229. Springer Berlin Heidelberg, 2012.

[59] D. Nedic, I. Dobson, D. Kirschen, B. Carreras, and V. Lynch. Criticality in a cascading failure blackout model. *International Journal of Electrical Power Energy Systems*, 28(9):627–633, 2006.

[60] NERC. System Protection and Control Task Force. Report, Rationale for the Use of Local and Remote (Zone 3) Protective Relaying Backup Systems, February 2005. http://www.nerc.com/docs/pc/spctf/Zone3Final.pdf.

[61] S.C. Ng and E.A. Udren. Business case for protection reliability improvement and summary of industry of protection practices. In *iPCGRID*, 2009.

[62] NYISO. Blackout august 14, 2003 final report. Technical report.

[63] Olivier Pauzet. Cellular communications and the future of smart metering, Sep 2010.

[64] OpenSG users group. SG network system requirements specification v4.0-draft6, Jun 2010.

[65] CPLEX Optimizer. High-performance mathematical programming solver for linear programming, mixed integer programming, and quadratic programming. http://www-01.ibm.com/software/commerce/optimization/cplex-optimizer/.

[66] H. Widmer J.-L. Bermudez A. Vukicevic M. Rubinstein F.Rachidi M.Babic P. Meier, M. Bittner and J. Simon Miravalles. Pathloss as a function of frequency, distance and network topology for various LV and MV european powerline networks. Technical Report EC/IST FP6 Project No 507667 D5v0.9, The OPERA Consortium, April 2005.

[67] Arun G. Phadke. Hidden failures in electric power systems. *International Journal of Critical Infrastructures*, 1(1):64–75, Jan 2004.

[68] Arun G. Phadke and James S. Thorp. Computer relaying for power systems. In *second edition, Research Studies Press Ltd and John Wiley & Sons*, 2009.

[69] R. Pickholtz, D. Schilling, and L. Milstein. Theory of spread-spectrum communications–a tutorial. *IEEE Transactions on Communications*, 30(5):855 – 884, May 1982.

[70] Jussi Poikonen. *Efficient Channel Modeling Methods for Mobile Communication Systems*. PhD thesis, University of Turku, Dept of Information Technology, Turku, Finland, 2008.

[71] Michael B. Pursley. *Introduction to Digital Communications*. Prentice Hall, 2005.

[72] Qualcomm. 3G cellular technology for smart grid communications. http://www.qualcomm.com/media/documents/3g-cellular-technology-smart-grid-communications.

[73] Randy Ressler. Pad-mounted transformer.

[74] Tamronglak S. *Analysis of power system disturbances due to Relay Hidden Failures*. PhD thesis, Virginia Tech, Dept of ECE, Blacksburg, VA, USA, 1994.

[75] Chris Sanders. *Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems*. second edition, Jul 2011.

[76] SEL. The synchrophasor report. http://www.selinc.com/issue3/, May 2009.

[77] Marvin Kenneth Simon, Jim K Omura, and Robert A Scholtz. *Spread Spectrum Communications Handbook*. McGraw-Hill, 2002.

[78] S M Stefanov. *Separable Programming: Theory and Methods (Applied Optimization)*. Springer, 2001.

[79] Cobus Strauss. *Practical Electrical Network Automation and Communication Systems*. Elsevier, 2012.

[80] S. Tamronglak, S.H. Horowitz, A.G. Phadke, and J.S. Thorp. Anatomy of power system blackouts: preventive relaying strategies. *IEEE Transactions on Power Delivery*, 11(2):708 –715, Apr 1996.

[81] Gilles Thonet. Zigbee FAQ, Feb 2006.

[82] J.S. Thorp and A.G. Phadke. Protecting power systems in the post-restructuring era. *IEEE Computer Applications in Power*, 12(1):33 –37, Jan 1999.

[83] JS Thorp, AG Phadke, SH Horowitz, and S Tamronglak. Anatomy of power system disturbances: importance sampling. *International Journal of Electrical Power & Energy Systems*, 20(2):147 – 152, 1998.

[84] Don Torrieri. *Principles of Spread-Spectrum Communication Systems*. Springer, 2011.

[85] V. Tralli and M. Zorzi. Markov models for the physical layer block error process in a WCDMA cellular system. *IEEE Transactions on Vehicular Technology*, 54(6):2102–2113, 2005.

[86] U.S. Census. U.S. household statistics, 2012.

[87] V. Vieri, D. Aleksander, and V. Branimir. *The CDMA2000 System for Mobile Communications : 3G Wireless Evolution*. Prentice Hall, 2004.

[88] A. Viterbi. *CDMA: Principles of Spread Spectrum Communications*. Addison-Wesley, 1995.

[89] I.N. Vukovic. Throughput comparison of random access schemes in 3GPP. In *The 57th IEEE Semiannual Vehicular Technology Conference, VTC 2003-Spring.*, volume 1, pages 616–620 vol.1, 2003.

[90] H. Wang and J.S. Thorp. Optimal locations for protection system enhancement: a simulation of cascading outages. *IEEE Transactions on Power Delivery*, 16(4):528 – 533, Oct 2001.

[91] Xiaoru Wang, k. Hopkinson, J.S. Thorp, R. Giovanini, K.P. Birman, and D.V. Coury. Developing an agent-based backup protection system for transmission networks. In *Power Systems and Communication Systems Infrastructures for the Future*, Oct. 2002.

[92] M.Z. Win and R.A. Scholtz. Impulse radio: How it works. *IEEE Communications Letters,*, 2(2):36 –38, Feb 1998.

[93] Bruno de Souza Abreu Xavier. *Call Processing in CDMA Systems*, pages 239–290. John Wiley & Sons, Ltd, 2005.

[94] Ye Yan, Yi Qian, and H. Sharif. A secure and reliable in-network collaborative communication scheme for Advanced Metering Infrastructure in smart grid. In *IEEE Wireless Communications and Networking Conference (WCNC)*, pages 909 –914, March 2011.

[95] Yang Yang and Tak-Shing Peter Yum. Analysis of random access channel in UTRA-TDD on AWGN channel: Research articles. *International Journal of Communication Systems*, 17(3):179–192, Apr 2004.

[96] Jui-Hung Yeh, Jyh-Cheng Chen, and Chi-Chen Lee. Comparative analysis of energy-saving techniques in 3GPP and 3GPP2 systems. *IEEE Transactions on Vehicular Technology*, 58(1):432 –448, Jan 2009.

[97] Z.W. Zhao and I-Ming Chen. Moving HomePlug to Industrial Applications with Power-Line Communication Network. http://dspace.mit.edu/handle/1721.1/3912.