8-2013

Design of Wireless Communication Networks for Cyber-Physical Systems with Application to Smart Grid

Rukun Mao
rmao@utk.edu

To the Graduate Council:

I am submitting herewith a dissertation written by Rukun Mao entitled "Design of Wireless Communication Networks for Cyber-Physical Systems with Application to Smart Grid." I have examined the final electronic copy of this dissertation for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy, with a major in Electrical Engineering.

Husheng Li, Major Professor

We have read this dissertation and recommend its acceptance:

Xueping Li, Seddik M. Djouadi, Qing Cao

Accepted for the Council:

Carolyn R. Hodges

Vice Provost and Dean of the Graduate School

(Original signatures are on file with official student records.)

Design of Wireless Communication Networks for Cyber-Physical Systems with Application to Smart Grid

A Dissertation

Presented for the

Doctor of Philosophy

Degree

The University of Tennessee, Knoxville

Rukun Mao

August 2013

Dedicated to my parents.

Acknowledgements

I would like to thank my advisor, Dr. Husheng Li, for his guidance and patience in advising me. Especially, I want to thank him for his confidence in me. His support gives me courage to pursue my dreams.

I would also like to thank my committee members, Dr. Xueping Li, Dr. Seddik M. Djouadi, and Dr. Qing Cao, for respectively advising from their unique perspectives. Their advice, comments and critics are the reasons that I have kept improving.

I want to express my appreciation to the faculty and staff at EECS department. I want to thank Ms. Dana Bryson in particular for her kindness and hospitality while assisting me to go through procedures in the department.

I am grateful to Dr. Min H. Kao for his generosity. It is my honour to receive the Min H. Kao scholarship, which, in part, provided essential financial support for my PhD study.

I have enjoyed being a member of our wireless communication research group at UTK. Previous and current members, including Dr. Depeng Yang, Dr. Kun Zheng, Dr. Zhenghao Zhang, Dr. Qi Zeng, Ben Early, Shuping Gong, Hannan Ma, Jingchao Bao, and Yifan Wang, are all very supportive. It has been a precious 5-year in my life, spending memorable time with these friends.

"Success is more a function of consistent common sense than it is of genius."

–An Wang

Abstract

Cyber-Physical Systems (CPS) are the next generation of engineered systems in which computing, communication, and control technologies are tightly integrated. On one hand, CPS are generally large with components spatially distributed in physical world that has lots of dynamics; on the other hand, CPS are connected, and must be robust and responsive. Smart electric grid, smart transportation system are examples of emerging CPS that have significant and far-reaching impact on our daily life.

In this dissertation, we design wireless communication networks for CPS. To make CPS robust and responsive, it is critical to have a communication subsystem that is reliable, adaptive, and scalable. Our design uses a layered structure, which includes physical layer, multiple access layer, network layer, and application layer. Emphases are placed on multiple access and network layer. At multiple access layer, we have designed three approaches, namely *compressed multiple access, sample-contention multiple access, and prioritized multiple access,* for reliable and selective multiple access. At network layer, we focus on the problem of creating reliable route, with service interruption anticipated. We propose two methods: the first method is a centralized one that creates backup path around zones posing high interruption risk; the other method is a distributed one that utilizes Ant Colony Optimization (ACO) and positive feedback, and is able to update multipath dynamically. Applications are treated as subscribers to the data service provided by the communication system. Their data quality requirements and Quality of Service (QoS) feedback are incorporated into cross-layer optimization in our design. We have evaluated our design

through both simulation and testbed. Our design demonstrates desired reliability, scalability and timeliness in data transmission. Performance gain is observed over conventional approaches as such random access.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Background and Scope

Cyber-Physical System (CPS) is the next generation of engineered system in which computing, communication, and control technologies are tightly integrated (Kim and Kumar, 2012). The "cyber" part of CPS used to mainly focus on computing, such as embedded computers. However, with CPS covering an increasingly larger spatial area and unprecedented coordination among components within CPS, communication has become indispensable for CPS. The cyber characteristics of CPS are thus now from both its computing and communication subsystems. The "physical" part of CPS refers to physical processes through which CPS interacts with its surroundings. Along with advancements in computing, communication, and control disciplines, CPS has been around in different forms, such as Distributed Embedded Systems, Wireless Sensor and Actuator Networks (WSAN), Networked Control Systems (NCS). While CPS is a unique system that has various dynamics and uncertainties: discrete dynamics from computing, link uncertainty in communication, and continuous dynamics from physical processes, the operating standards for CPS are high. CPS has to work safely, reliably, and timely, with high confidence. Applications of CPS have been playing critical roles in industry sectors such as energy, transportation,

healthcare, tele-communication, which all have profound societal and economic impacts.

In this dissertation, we will focus on the design of communication networks for CPS. On one hand, of the three major technologies integrated into CPS: computing, communication, and control, communication's role in CPS and its impact on CPS are studied the least. This lack of study is in part due to the development of CPS itself, because in the previous generation of CPS, such as embedded system, communication was not a big concern (Lee, 2006). Although communication subsystems in large-scale CPS have been integrated for a long time, such as SCADA in electric power system, they do not prevail and have only limited impact (Wu et al., 2005). On the other hand, in order to reach the full potential of CPS, it is essential to tightly integrate communication into CPS and to allow controllers and actuators in CPS take full advantage of the information provided by communication subsystem.

In sharp contrast to conventional data communication networks, communication networks in CPS have much more dynamics. Different from an audio or video stream on Internet that has fixed priority, a data stream in CPS could constantly change its priority when data with varying importance is transferred through it. This dynamic priority affects both multiple access and routing schemes. The data consumption model is also different in CPS. For example, monitoring sensors may not know the exact destination when they are disseminating their observation data, because the data could be valuable to a set of controllers. Defining the set is difficult as it requires knowledge of the current status of CPS. Finally, Quality of Service (QoS) in CPS communication has its own unique requirements (Wu et al., 2011). Packet delay, packet loss, and real-time guarantee all have to be re-interpreted within CPS framework.

We would further narrow our focus down to wireless communication networks for CPS. Wireless technology saves the hassle of wiring when deploying CPS. It also provides the much-desired plug-and-play feature, which in turn makes CPS scalable and extensible (Dunbar, 2001). In addition, when the scale of a CPS becomes large,

it normally has a hierarchical structure. Upper-level nodes/hubs are much-better equipped in terms of data transmission ability, using high-speed, reliable links such as optical cable, dedicated Ethernet, or microwave link (Tan et al., 2009). CPS has the same "Last Mile" problem as Internet does. The majority of sensors and actuators of CPS fall into the "Last Mile" range, and their performance is critical for CPS. Studying wireless communication networks in the "Last Mile" of CPS thus is the most challenging but also high-rewarding task.

1.2 Design Challenges

Because of its high level of complexity in both structural and functional aspects, CPS presents a wide range of challenges. The interacting dynamics among integrated components pose most of the difficulties in modeling and analyzing the system. The classical models and analysis that are devised within narrowly-defined disciplines would no longer be adequate to capture the semantics of CPS. The dynamics from computing, communication, and physical world have to be addressed in a unified form before any subsystem can actually make contribution to the CPS it belongs to.

As to the design of communication subsystem for CPS, we have identified the following challenges, which are carefully addressed while designing communication subsystem for CPS.

Real-Time while requirement of real-time communication is treated as a luxury in many systems, it is a must in CPS. Data that have missed its deadline is not only deemed useless, but also is harmful for the communication subsystem due to wasted bandwidth and delay caused to other packets. Thus, managing acceptable dynamic traffic load with the ability to deliver data in real-time is an essential task of the communication subsystem in CPS.

Reliability and Robustness A typical data flow in CPS is like this: sensors report monitoring data to interested controllers; controllers make decision and forward

action data to actuators. Reliability and robustness of the communication subsystem are very important in this monitor-control type applications, which are the most common in CPS. Also, interruption in data transmission in CPS could quickly force the system out of stable operation and generate cascade failure, which put the entire system in jeopardy.

Dynamic Traffic and Varying QoS CPS is basically interacting with the physical world, the environment where we live in. Dynamics in the physical world result in dynamic traffic in CPS. Overall traffic within a certain period of time could be much higher than that of other times. For a data stream originated from a specific sensor, data volume and Quality of Service (QoS) could also change dramatically, which is triggered either by large change in the sensors neighborhood, or adjustment of relative priority throughout the entire CPS. In other words, other places have more urgent messages to report.

Scalability and Adaptability The ultimate goal of communication subsystem in CPS is providing a channel for reliable and timely information transmission. It is desirable that sensors, actuators, and controllers in CPS can be flexibly added, removed, or replaced. This flexibility asks for scalability and adaptability of a communication subsystem that can tolerate frequent change from other components in CPS.

1.3 Contributions

An ideal CPS would be able to operate safely, reliably, and efficiently; its system performance is temporally predictable, and system components are able to be verified, validated, and certified (Lee, 2008). In line with the overall CPS design goals, the design of wireless communication networks for CPS presented in this dissertation has made the following contributions:

1. We studied a new topic of significant importance, the design of wireless communication networks for CPS. We analyzed challenges and requirements for the design, presented a layered communication system that is able to provide efficient, reliable, and timely service with scalability and adaptability.

2. We developed a novel multiple access scheme using Compressed Sensing (CS). The scheme is able to provide efficient and reliable service for data traffic in CPS.

3. We proposed a *sample-contention* approach for efficient prioritized multiple access.

4. We introduced a method to systematically select the most important data for transmission when communication resource is limited. The selection process is CPS oriented, taking into consideration system model, environment noise, control requirements and cost.

5. We developed a backup routing approach at network level for communication networks in CPS, which increases communication reliability.

6. We integrated the communication system we designed into smart grid application and tested it, which achieves obvious improvements.

Although CPS introduces a great amount of complexity, its potential is also unprecedented. First, CPS is ubiquitous in our life, though their scale and functionality may be different; The buildings we live in, the vehicles we drive, and the appliance we use are all composed of CPS. Second, the increasing interaction between human beings and physical world via CPS could fundamentally change the way we live. Unlike current exchange of information that is dominantly among people, CPS provides the chance for human beings to interact with physical world. For instance, in the near future, a car could navigate through busy traffic and arrive at the exact specified time at its owner's house. Third, CPS can significantly improve current

engineering systems' reliability and efficiency. A minor disturbance in electric power system would no longer escalate into a wide-area blackout; rush-hour traffic jam in metropolitan area could be greatly alleviated.

1.4 Dissertation Organization

The remainder of this dissertation is organized as the following: next chapter, chapter 2, surveys related work in the literature on designing wireless communication networks for CPS, outlines our layered design briefly. Chapter 3 focuses on the design at multiple access layer. Chapter 4 concentrates on the design at network layer. In chapter 5, application of communication in smart grid, a typical CPS, is presented. We conclude the dissertation with chapter 6.

Chapter 2

Related Work and Design Overview

2.1 Related Work

Through its path of evolution, CPS has presented itself in different forms. Networked Control Systems (NCS) (Yang, 2006), Wireless Sensor and Actuator Networks (WSAN) (Xia, 2008), distributed embedded system (Marwedel, 2010), and certain application specific wireless sensor networks (Wu et al., 2011) all deserve credits for the development of CPS. In order to give a more complete view of the topics in CPS, we not only review the latest research progress in CPS, but also check all the areas closely related to CPS.

Among many challenges identified in developing CPS, the demand for reliable and high quality communication is unanimous (Lee et al., 2012; Yan and Qian, 2012; Baillieul and Antsaklis, 2007). Kim and Kumar (2012) gives a comprehensive overview of the development of CPS, as well as results on relevant research domains such as NCS, real-time networking and WSN. Baillieul and Antsaklis (2007) discusses control and communication challenges in networked real-time system. Progress in designing wireless networks for CPS is meant to address many of those challenges.

Wu et al. (2011) analyzes communication's role in both WSN and CPS, trying to identify its evolving path. Sztipanovits et al. (2012) knowledges the great challenges of system integration in CPS because of heterogeneity of components and interactions. It presents a passivity-based design approach that decouples stability from timing uncertainties caused by networking and computation.

While there are few works in the literature specifically addressing the problem of designing communication networks for CPS, considerable effort is invested in designing general CPS. A system architecture with connected heterogeneous network subsystem for the joint operations of control and communication is proposed in (Wang et al., 2008). Heemels et al. (2010) presents a general framework that incorporates communication constraints, varying transmitting intervals and delays in NCS. Their work provides quantitative information that allows network designers to select appropriate networks and protocols for guaranteed stability, desirable performance, and system robustness against certain level of variations in delays and transmission intervals. Ulusoy et al. (2011) introduces a practical wireless NCS and an implementation of a cooperative medium access control protocol that work jointly to achieve decent control under severe impairments, such as unbounded delay, bursts of packet loss, and ambient wireless traffic. Ilic et al. (2008) discusses the tactics for modeling future cyber-physical energy system. The authors view future energy system as the intertwined cyber-physical network interconnections of many non-uniform components, such as diverse energy sources and different classes of energy users, equipped with their own local cyber. Their modeling approach is qualitatively different from the currently used models that do not explicitly account for the effects of sensing and communications. In Derler et al. (2011), technologies including hybrid system modeling and simulation are discussed using a portion of an aircraft vehicle management systems (VMS), specifically the fuel management subsystem as an example. Lin et al. (2009) presents the CPS domain of intelligent water distribution networks, for which EPANET represents the physical water distribution network, and Matlab provides the decision support algorithms used to control the allocation

of water. A power-network co-simulation framework which integrates power system dynamic simulator and network simulator together using an accurate synchronization mechanism is reported in Lin et al. (2011a). A wide range of tools have been employed in the effort to model and simulate CPS. Modelica (Modelica, 2012) is introduced for CPS modeling and simulation by Henriksson and Elmqvist (2011), in which the authors have presented details on timing simulations, involving both real-time task scheduling and network communication. In Li and Xu (2011), a design of a simulation platform for ad hoc based CPS is proposed based on NS-2. The authors analyze the advantages and disadvantages of CPS simulation platforms that have been developed based on NS-2 and GLOMOSIM.

In communication systems, multiple access is a topic under intensive study. Demirkol et al. (2006) gives a survey on MAC protocols for wireless communication. Kanodia and Li (2002) discusses distributed priority scheduling and medium access in ad-hoc networks. Conventional multiple access protocols, such as 802.15.4 based ZigBee (Xia et al., 2008), WirelessHART (Song et al., 2008), and 802.11 based Cooperative MAC (COMAC) (Gokturk and Gurbuz, 2008) are used in NCS or CPS. However, inherent standard features limit their application in CPS whose diverse data has various QoS requirements at MAC level. Unlike general data transfer networks, certain application specific networks have a much larger range of importance levels defined for data transmission (Ahmadi et al., 2010; Ahmadi and Abdelzaher, 2009; Krishnamachari et al., 2002). When wireless sensor networks (WSN) are used for environmental monitoring and data collection, data transferred over the network is no longer service flow oriented (Akyildiz et al., 2002). Ahmadi et al. (2010) points out that data dissemination protocols must consider the importance of data packets. The authors measure packet importance by data's contribution to the accuracy of estimating the monitored physical phenomenon. In their congestion control scheme for data collection application, both spatial and temporal aggregations are used. A similar idea on how to determine data importance is presented in Ahmadi and Abdelzaher (2009), in which reduction of estimation error is used as a metric to

determine the amount of information that is to be successfully delivered. From NCS perspective, the most important data first have to make sure a system is stable (Zhang et al., 2001). Delay and packet drop are the two primary factors affecting NCS' stability, and these two factors within NCS have been under intensive study (Cloosterman et al., 2009; Schenato, 2008). Therefore, we can infer that in NCS data that could cause critical delay are the most important (impact of packet drop can be converted to impact of delay). For WSAN, it has many characteristics of NCS; under certain scenario, they are NCS. However, compared with NCS, WSAN has a stronger ad hoc feature, thus its stability is not as intensively studied as that of NCS. WSAN places more emphasis on QoS, particularly real-time capability (Xia, 2008). Literature on WSN, WSAN, and NCS has revealed that the criticality of data in a system depends on major factors such as the purpose and application of a system, the status and requirements of a system's operation, and structure of the system. Determining the importance of data in CPS is still a task that needs significantly more research effort, though most of criteria in the three types of systems aforementioned still apply to CPS.

Reliable routing is essentially a multipath routing problem which has been extensively studied in wireless networks (Mohammed Tariquea et al., 2009; Ganesan et al., 2001). For example, node-disjoint and braided multipath schemes are proposed to provide energy efficiency and resilience against node failures (Mohammed Tariquea et al., 2009). Routing the connections in a manner such that link failure does not shut down the entire stream but allows a continuing flow for a significant portion of the traffic along multiple paths is proposed in Zhang et al. (2010). As to routing in NCS or CPS, Liu et al. (2012) studies real-time routing for wireless networked sensing and control. In the paper, time uncertainties is reduced by protocols MTE (Multi-Timescale Estimation) and MTA (Multi-Timescale Adaptation). Routing protocols for CPS with application to smart grid are reported in Li et al. (2012a) and Li et al. (2012b)

2.2 CPS Communication System Design Overview

Our design for wireless communication networks in CPS uses a layered structure, which includes physical layer, multiple access layer, network layer, and application layer. Emphases are placed on multiple access layer and network layer. Layered structure has had a great success in communication system design. The success of Internet is a big testament to the effectiveness of networks with layered structure. By dividing a network into multiple layers, engineers have a smaller problem to concentrate on. Adaptivity and scalability are also improved with each layer only has to comply with pre-defined interfaces between layers. In other words, encapsulation gives each layer more flexibility within its own domain. While we are trying to take full advantage of the benefits of layered structure in communication design, we are also aware of certain aspects for which we can utilize cross-layer design for optimization. We propose a hybrid structure for CPS' communication subsystem whose main framework is layered-based, but we use cross-layer optimization to improve timeliness and reliability.

2.2.1 Multiple Access Layer

At multiple access layer, we have designed three approaches, namely *compressed multiple access, sample-contention multiple access, and prioritized multiple access,* for reliable and selective multiple access in CPS. These three approaches are complementary to one another, and they together provide a strong protocol at multiple access level.

Compressed multiple access is a multiple access approach that utilizes *compressed sensing* algorithm. Compressed Sensing(CS) allows different sensors to report their data without worrying about possible collision while transmitting. Given that the data traffic from sensors is sparse and that data size is small, which both generally are true in CPS, compressed multiple access can provide more efficient access with shorter delay. In addition, its ability to provide normal multiple access even when

traffic volume increases and is no longer sparse makes it a desirable multiple access approach for CPS, which has high standards for adaptability and reliability.

Sample-contention multiple access is suitable for the situation in which the majority of sensors have data to transmit (i.e., no longer sparse); however, only part of these sensors' data is necessary in terms of efficient and robust control. Indiscriminating transmission from sensors with data can overwhelm the multiple access subsystem and thus undermine the stability of CPS. By first sampling sensors' data, then estimating and broadcasting a threshold, sample-contention scheme is able to restrict the number of reporting sensors and select those whose data is essential for control purpose.

In prioritized multiple access, we study the criteria on how to select the most suitable sensor for transmission. Without loss of generality, we consider the scenario in which after a round of data collecting by all the sensors, only one of the sensors, usually the one with the most important data, is given the right to transmit. When selecting the most suitable sensor, a systematic method is applied. The method takes both CPS system model and data processing into consideration.

2.2.2 Network Layer

At network layer, we focus on the problem of how to reliably route sensor data to controllers, with service interruption anticipated. We propose two methods to solve the problem. The first method is a centralized one that creates backup path around zones posing high interruption risk; the other method is a distributed one that is able to update multipath dynamically.

As apposed to other methods for creating backup path in multipath routing, our approach to create backup path first defines a group of nodes named Shared Risk Node Group (SRNG). Backup paths are created exclusively for SRNG to make sure when interruptions happen in a SRNG, data transmission service through backup

path is intact. The backup paths creating problem is formulated and solved as an integer programming problem.

While creating backup path through integer programming is a centralized algorithm, at network layer, we design another distributed algorithm for multipath routing in CPS. The distributed routing algorithm is based on Ant Colony Optimization (ACO), and is adaptive to SRNG change (e.g., position, node member). It also incorporates the latest performance of current route into a feedback mechanism, which reinforces section of good route and explores better routing options at the same time.

2.2.3 Application and Cross-Layer Optimization

CPS includes three key components: sensors, actuators, and controllers. An typical application monitors physical world through sensors, collects information at controllers, reacts using actuators. Controllers subscribe information data from sensors, forming a multi-to-one relationship. Data from sensors first reaches key nodes through multiple access stage; key nodes in core network (at network level) then route data to the destination where specific data has been subscribed by applications. Applications set standard for data quality, such as delay, precision. Generated by cross-layer optimization, feedbacks are given back to both network layer and MAC layer, which adjust accordingly to satisfy requirements from applications.

Chapter 3

Multiple Access in Cyber-Physical System

In this chapter, we study multiple access schemes for wireless communication in CPS. All proposed schemes are at the multiple access layer of our design. We first introduce *compressed multiple access*, a compressed sensing based multiple access scheme that handles dynamic sparse traffic load with high efficiency. The scheme can achieve shorter packet delay with smaller deviation, which improves communication reliability in CPS. Its robustness when traffic is not sparse is also a highly desirable feature in CPS. We then present *sample-contention multiple access*. This scheme is able to selectively allow adequate sensors to transmit data according to pre-set criteria. We design the scheme for WiMAX (Worldwide Interoperability for Microwave Access) with application to voltage control in power system. However, the scheme itself is a general one that can be easily adopted and applied to other CPS' multiple access layer. At the third part of this chapter, we discuss how to select the most suitable data source (e.g., sensor) to transmit data when communication resources is limited at the multiple access level. System model, environment (e.g., noise), control cost and requirements are considered when making the selection.

3.1 Compressed Multiple Access

In the wireless communication system for CPS, multiple transmitters need to transmit their data to a base station, thus requiring the technique of multiple access, such as time division multiple access (TDMA), code division multiple access (CDMA) or orthogonal frequency division multiple access (OFDMA). We suppose that the channels are vectorized, either in frequency or in time, and assume that the dimension of the vector channel is smaller than the number of transmitters. Quite often, the data traffic at a transmitter is bursty, i.e., in one time slot, only a portion of the transmitters have data to transmit. For example, in CPS, there could be hundreds of sensors associated with one base station; however, in many applications, there are only several sensors reporting to the base station simultaneously. Therefore, the base station needs to know the identities of the active transmitters. Moreover, the data packet could be very small, e.g., just a record of local temperature. Thus the identity information may cause significant overhead. The identification problem could be solved using the following three different ways:

1. Adding the identity information into data packets explicitly, i.e., adding an identity field in the packet header. If the receiver can decode a data packet, it can determine the owner of the packet.

2. Setting a preamble before each data transmission. In this preamble, active transmitters send out requests containing their identity information.

3. Similar to CDMA systems, assigning different signature waveforms to different transmitters and projecting the received signal onto all signature waveforms. Only transmitters with sufficiently large projections are considered as being active.

However, all three approaches have drawbacks. Approach 1 includes overhead to the data packet. In approach 2, it may require a long preamble if the requests of different transmitters are kept orthogonal, when the number of transmitters is large. If the

Table 3.1: Typical Multiple Access Approaches

Category	Identifying Method	Cost
1	Decode packet header	Identity field
2	Send request in preamble	Preamble period
3	Assign different signature waveforms	Signature waveforms and their projection

orthogonality constraint in the preamble is removed (e.g., using contention based multiple access), there could be collisions of request signals. In approach 3, when the dimension of the vector channel is smaller than the number of transmitters (like an overloaded CDMA system), the signature waveforms cannot be orthogonal; therefore it is difficult to determine a threshold for the active user selection.

Besides the identification problem, multiple access scheme, i.e., how to separate the signals from different transmitters, is also an important problem. In approach 2, the receiver can allocate different time slots to the transmitters in a TDMA fashion. However, the feedback signaling of time slot allocation induces overhead to the system. In approach 3, CDMA can be used to separate the signals from different transmitters; whereas it suffers from multiuser interference when nonorthogonal spreading codes are used.

In this section, we tackle the multiple access problem by employing the compressed sensing (Candes et al., 2006; Donoho, 2006, 2004), a signal processing technique developed in recent years. Based on the assumption that the signal is sparse, i.e., most elements of the signal in a transformation domain are zero or have small amplitudes, compressed sensing reconstructs original signal from observations. Efficient algorithms like Basis Pursuit (BP) (Tsaig and Donoho, 2006; Chen et al., 1999), Orthogonal Matching Pursuit (OMP) (Pati et al., 1993; Tropp and Gilbert, 2007), and stagewise OMP (StOMP) (Donoho et al., 2006b) have been proposed and applied in fields like data compression (Candes and Tao, 2006), sensor networks

(Wang et al., 2007), statistical signal processing (Davenport et al., 2006) and image processing (Ye, 2007).

It is easy to find the analogy between the multiple access and compressed sensing since the received signal at base station is also given by $\mathbf{\Phi x}$, where $\mathbf{x}$ is the vector of transmitted signal and the columns in $\mathbf{\Phi}$ are the signature waveforms of different transmitters. Therefore, we can allow the transmitters having data to transmit directly without the stage of request in approach 2. When there is no noise, the equation can be perfectly solved, thus avoiding the threshold in approach 3. The identities of the active transmitters are simply a by-product of the solution, i.e., the locations of the non-zero elements in $\mathbf{x}$, thus avoiding the overhead of explicit identity in approach 1. We coin the scheme proposed *Compressed Multiple Access* since the identity information is "compressed" into the data transmission. Moreover, the sparsity required by compressed sensing is assured by the assumption that most transmitters do not have data to transmit. Therefore, *the identification and multiple access problems are solved jointly.* Numerical simulation results will show that, compared with the traditional carrier sense multiple access (CSMA), the proposed multiple access scheme achieves better performance for the expectation and variance of packet delays when the traffic load is not too small.

The following mathematical notations are used in this section.

- $\circ$ denotes Hadamard Product. For two matrices $\mathbf{A}$ and $\mathbf{B}$ having the same size, $(\mathbf{A} \circ \mathbf{B})_{\mathbf{ij}} = \mathbf{A}_{\mathbf{ij}}\mathbf{B}_{\mathbf{ij}}$.
- For matrix $\mathbf{A}$, $\mathbf{A}^T$ means the transpose of $\mathbf{A}$.
- For an n-vector $\mathbf{x}$, its 1-norm equals $\sum_{k=1}^{n} |x_k|$ and its 0-norm means the number of nonzero elements.

3.1.1 Access Model

In a wireless system, suppose that a base station receives signals from m transmitters (e.g., sensors in CPS or mobile phones in cellular systems) via vector channels of dimension n. In general case, the vector channel could be in either time or frequency. We assume that the vector is in frequency, i.e., each dimension corresponds to a subcarrier in the frequency domain. For simplicity, we assume that the received signal is real. It is straightforward to extend the real signal to complex signal case.

At time slot t, the received signal is given by an $n-$vector:

$$\mathbf{r}(t) = \sum_{k=1}^{m} [x_k(t)\mathbf{h}_k \circ \mathbf{s}_k(t)] + \mathbf{n}(t), \tag{3.1}$$

where $\mathbf{h_k}$ is the vector of channel amplitude gains of transmitter k with upper bound $h_{\max}$ and lower bound $h_{\min}$, $x_k(t)$ is the information symbol of transmitter k. $\mathbf{s_k}(t)$ is the vector of signature waveforms of transmitter k at time slot t. $\mathbf{n(t)}$ is the received noise vector at time slot t. We also place the following assumptions on the model.

1. We assume that a transmitter does not always have data to transmit. The data burst is random which means that averagely $\rho m (0 < \rho < 1)$ transmitters generate a new data to transmit at a time slot. When transmitter k has no data, it does not transmit, namely $x_k = 0$. We also assume that the receiver does not have *a priori* information about which transmitters have data.

2. The channel gain vector $\mathbf{h_k}$ does not change in time. The receiver knows the channel gains perfectly by letting the transmitter send out pilot signals periodically. However, the transmitters do not know the channel gains perfectly.

3. Eq. 3.1 implicitly assumes that the transmitters are perfectly synchronized in time. This assumption will be addressed in details and relaxed later.

4. We assume that $\mathbf{s}_k(t)$, the signature waveform of transmitter k, is a vector randomly chosen on the unit sphere in $\mathbb{R}^n$. The signature waveforms are known at both the transmitters and receiver.

5. A buffer is used for each transmitter to store untransmitted data packets.

Applying the assumption on signature waveforms, we can rewrite Eq. 3.1 as

$$\mathbf{r}(t) = \mathbf{\Phi}(t)\mathbf{x}(t) + \mathbf{n}(t) \tag{3.2}$$

where

$$\mathbf{x}(t) \triangleq (x_1(t), \ldots, x_m(t))^T, \tag{3.3}$$

and

$$\mathbf{\Phi} = \mathbf{H} \circ \mathbf{S}(t), \tag{3.4}$$

where $\mathbf{S}(t) \triangleq (\mathbf{s}_1(t), \ldots, \mathbf{s}_m(t))$ and $\mathbf{H} \triangleq (\mathbf{h}_1, \ldots, \mathbf{h}_m)$.

When there are multiple time slots, say from time slot 1 to time slot t, during which the transmitted symbols do not change (will be called a frame later), we can stack the received signals together and obtain the following expression

$$\mathbf{r}(1:t) = \mathbf{\Phi}(1:t)\mathbf{x}(1) + \mathbf{n}(1:t), \tag{3.5}$$

where

$$\mathbf{r}(1:t) = \left(\mathbf{r}(1)^T, ..., \mathbf{r}(t)^T\right)^T, \tag{3.6}$$

$$\mathbf{n}(1:t) = \left(\mathbf{n}(1)^T, \ldots, \mathbf{n}(t)^T\right)^T, \tag{3.7}$$

and

$$\mathbf{\Phi}(1:t) = \left(\mathbf{H}^T, ..., \mathbf{H}^T\right)^T \circ \mathbf{S}(1:t), \tag{3.8}$$

and $\mathbf{S}(1:t) \triangleq (\mathbf{S}(1)^T, ...\mathbf{S}(t)^T)^T$.

3.1.2 Compressed Multiple Access

We are going to propose a novel scheme of multiple access based on compressed sensing, namely *compressed multiple access*. We first explain the procedures of compressed multiple access. Then, we provide an illustrative example, as well as a proposition about the equivalence between 0-norm and 1-norm optimization conditioned on the signal sparsity.

Procedures of Compressed Multiple Access

In contrast to conventional multiple access approaches (e.g., CSMA/CA), the proposed compressed multiple access scheme encourages transmission collisions. Actually, every single measurement is a mixture of received information symbols modulated by their own channel gains and signature waveforms plus noise. As illustrated in Fig. 3.1, we define a *Frame* with varying length (different numbers of time slots). A frame ends only when sufficiently many measurements have been obtained and two adjacent reconstructions generate the same results (Malioutov et al., 2008). Here we assume that a computationally efficient reconstructor, which can reconstruct the original signals exactly when enough samples have been received, is equipped at the base station. Therefore, multiple access is now possible using the smallest number of time slots, and without any *a priori* knowledge about how many transmitters are transmitting data in the current frame.

In each frame, the number of transmitters allowed to transmit data is determined at the beginning of the frame and then fixed throughout the entire frame. Before starting a new frame, the base station broadcasts a very short beacon signal, e.g., a

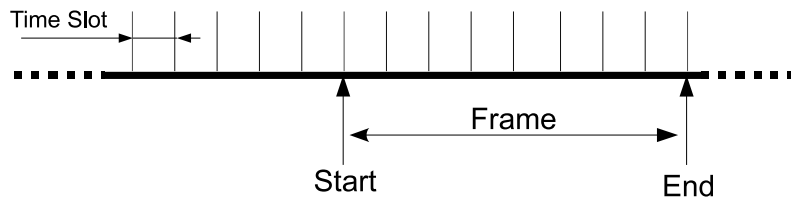


Figure 3.1: Frame

sinusoid, indicating the start of a new frame. Sensors having data in their buffers are legal for transmitting in the new frame. In the entire frame, sensors keep transmitting the same data of their own and only change signature waveforms $\mathbf{s}_k(t)$ in each time slot. If a new data is generated in the middle of a frame, then the transmitter will put the newly generated data into its buffer, and forms a first-in-first-out queue for the data waiting to be transmitted. When the base station finds that it has received sufficiently many observations and is able to distinguish the signals from different transmitters, it sends out a beacon signal to indicate the end of the current frame. Thus, the transmitters stop transmitting the current data. At this time, the received signal at the base station is given by Eq. 3.5 and the base station uses compressed sensing algorithm, e.g., OMP , to reconstruct the signals from different transmitters. In the next time slot, a new frame begins and the procedure is repeated.

The described procedures of the compressed multiple access are summarized in Algorithms 1 and 2 for transmitter and receiver, respectively. In the pseudo codes, *start* and *stop* are control signals broadcast by base station in order to inform transmitters the start and end of a frame.

An Illustrative Example

In Fig. 3.2, we provide an example to illustrate the procedure of compressed sensing based multiple access. For the first frame, transmitters Tx1 and Tx2 have data

Algorithm 1 Procedures at The Transmitter Side

```
if start == TRUE then
    i ← 0
end if
while stop ≠ TRUE do
    Send x_k × s_k[i]
    i ← i + 1
    if New data generated then
        n ← n + 1
        SendBuffer[n]=New Data
    end if
end while
for j = 0 to n − 1 do
    SendBuffer[j]=SendBuffer[j+1]
end for
n ← n − 1
```

Algorithm 2 Procedures at The Receiver Side

```
if Previous Frame Ends then
    Send start = TRUE
end if
repeat
    CS reconstruction
until two consequent recoveries are identical
Send stop = TRUE
```

x_{10}, x_{20} to transmit (here additional subscript n in x_{kn} represents the nth information symbol sent by transmitter k). During the first frame, x_{11} and x_{30} are generated at Tx1 and Tx3 and are saved in their own buffers, respectively. For the second frame, Tx1 and Tx3 start transmitting. The detailed procedure is given below.

1. At time slot 1, a *start* signal is received by all transmitters in base station's coverage; the transmitters initialize signature waveform index i to 0;

2. Within the following several time slots before receiving *Frame 1*'s *stop* signal, transmitters Tx1, Tx2 send $x_{10} \times \mathbf{s}_1(i)$, $x_{20} \times \mathbf{s}_2(i)$ respectively; index i increases by 1; other transmitters keep silent and send nothing;

3. The base station receives the ith measurement $y[i] = x_{10} \times \mathbf{s}_1(i) \circ \mathbf{h}_1 + x_{20} \times \mathbf{s}_2(i) \circ \mathbf{h}_2 + \mathbf{n}(i)$; combined with the previously received measurements, information symbols are reconstructed using the OMP algorithm;

4. Repeat the steps (2) and (3) until two consequent recoveries are the same (Malioutov et al., 2008). Then, at time slot 7, the base station sends out the *stop* signal of *Frame 1*, and this *stop* signal is also treated as the *start* signal of *Frame 2*;

5. Transmitters Tx1 and Tx2 stop current *Frame 1*'s transmission and reset index i to 0;

6. Starting from time slot 8, transmitters Tx1, Tx3 send $x_{11} \times \mathbf{s}_1(i)$, $x_{30} \times \mathbf{s}_3(i)$, respectively; index i is increased by 1; other transmitters keep silent and send nothing;

7. Base station receives the ith measurement $y[i] = x_{11} \times \mathbf{s}_1(i) \circ \mathbf{h}_1 + x_{30} \times \mathbf{s}_3(i) \circ \mathbf{h}_3 + \mathbf{n}(i)$; combined with previously received measurements, information symbols are reconstructed (correct recoveries are x_{11}, x_{30});

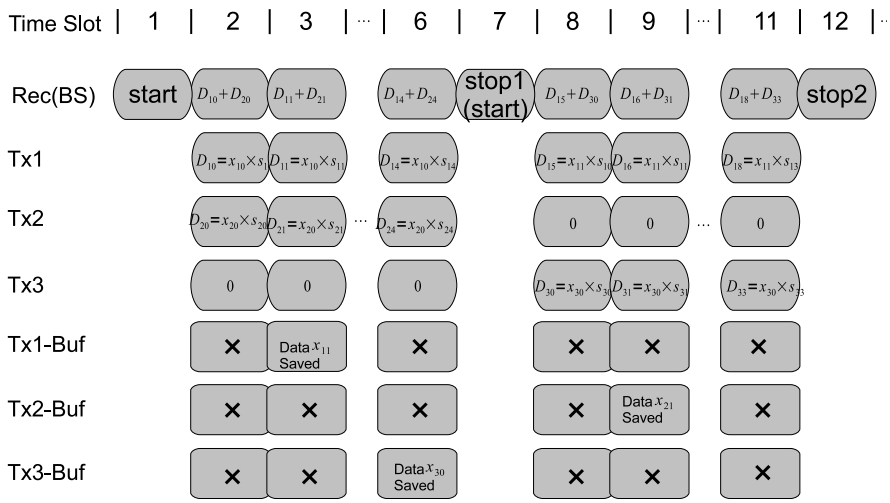


Figure 3.2: The Illustration of Compressed Multiple Access Transmission

8. Repeat steps (6) and (7) until two consequent recoveries are the same. Then, at time slot 12, *Frame 2*'s *stop* signal is broadcast by base station to inform Tx1, Tx3 to stop *Frame 2*'s transmission.

Transmitter Synchronization

As we have mentioned, the transmitters are assumed to be perfectly synchronized in time. In practice, the synchronization can be achieved in the following traditional ways:

- If each transmitter is equipped with a GPS and operates in outdoor environments, their timing can be almost perfectly synchronized.
- The base station can broadcast a time synchronization signal periodically such that all transmitters can keep track the correct timing information.

In some cases, the perfect time synchronization cannot be achieved, e.g., each transmitter keeps in the sleeping mode for most of the time and cannot frequently

listen to the time synchronization signal. In this situation, we can adapt the reconstruction algorithm to a asynchronous manner. In this subsection, we consider adapting the OMP algorithm to an asynchronous one.

First, we assume that each time slot is divided into $T_c + \tau_{\max}$ smaller chips, where $\tau_{\max}$ is the maximal time offset and T_c is the number of chips for transmission within each time slot. The time offsets of active transmitters k_1, ..., k_K are given by τ_{k_1}, ..., τ_{k_K} (measured in chips), respectively ($\tau_{k_i} \leq \tau_{\max}$).

Then, the algorithm of asynchronous OMP is given in Algorithm 3. The performance will be evaluated in the numerical simulations.

Algorithm 3 Asynchronous OMP Algorithm

```
Receive signal r of multiple time slots.
Set the active set as empty and set the candidate set as {1, 2, ..., m}.
for Residual signal is still large do
  for All elements in the candidate set do
    for All possible time offsets do
      Shift the signature waveform according to the time offset.
      Compute the projection of the signature waveform over the received signal.

      if The projection is large then
        Put the element into the active set.
        Delete it from the candidate set.
        Remove the corresponding signal from the received signal r and obtain
        the residual signal.
      end if
    end for
  end for
end for
```

Conditional Equivalence of 0-norm and 1-norm Optimizations

To assure the performance of BP algorithm adopted at the receiver, we need to assure the equivalence of the following two optimization problems (denoted by P0 and P1, respectively) (Donoho, 2006) when there is no noise and the signal is sufficiently

sparse:

$$\min_{\mathbf{x}} \|\mathbf{x}\|_0, \qquad \text{s.t. } \mathbf{r} = \mathbf{\Phi}\mathbf{x}, \tag{3.9}$$

and

$$\min_{\mathbf{x}} \|\mathbf{x}\|_1, \qquad \text{s.t. } \mathbf{r} = \mathbf{\Phi}\mathbf{x}. \tag{3.10}$$

Note that we discuss the received signal in only one time slot, for notational simplicity. The conclusion can be extended to observations in multiple time slots straightforwardly.

When the elements of $\mathbf{\Phi}$ are identically distributed, the equivalence has been proved in Donoho (2006). However, in our case, the elements may not be identically distributed since they are modulated by channel gains, which could be non-uniform, and the conclusions in Donoho (2006) cannot be applied directly. Fortunately, the following proposition assures the equivalence under certain conditions, whose proof is given in the appendix. Note that the quantity $\frac{m}{n}$ measures the sparsity of the signal. Therefore, the condition of the proposition is essentially the limit on the sparsity.

Proposition 1. *Define event $E(\Phi, \rho)$ as that, $\forall \|\mathbf{x}\|_0 \leq \rho m$, (P0) and (P1) yield the same unique solution equaling $\mathbf{x}$. Suppose that $\frac{m}{n} \leq C$, there exists a $\rho(C)$ such that*

$$P\left(E(\Phi, \rho(C))\right) \to 1, \tag{3.11}$$

as $m, n \to \infty$, where the randomness is over the selection of $\mathbf{\Phi}$.

When noise exists, it is almost impossible to recover the original signal precisely. Therefore, we can apply the noise-aware version of (P1) in Donoho et al. (2006a) to recover the original signal. The corresponding optimization problem is given by

$$\min_{\mathbf{x}} \|\mathbf{x}\|_1, \qquad \text{s.t. } \|\mathbf{r} - \mathbf{\Phi}\mathbf{x}\|_2 \leq \delta, \tag{3.12}$$

where δ is a controlling constant. When $\delta = 0$, Eq. 3.12 degenerates to Eq. 3.10. The stability of optimization problem in Eq. 3.12 has been discussed in Donoho et al. (2006a), based on the assumption that the column vectors in $\mathbf{\Phi}$ have unit norm. We extend the conclusions in Donoho et al. (2006a) to the channel gain dependent random matrix in our system. We assume that noise $\mathbf{n}$ has bounded norm, namely

$$\|\mathbf{n}\|_2 \leq \epsilon. \tag{3.13}$$

For unbounded noise, $\|\mathbf{n}\|_2 > \epsilon$, we can claim outage (or erasure) of the communication system. Then, ϵ can be determined by tolerable outage probability and noise distribution. Similar to Donoho et al. (2006a), we define the *coherence* for matrix $\mathbf{\Phi}$ as

$$M(\mathbf{\Phi}) \triangleq \max_{i \neq j} \frac{\left|\phi_i^T \phi_j\right|}{\|\phi_i\|_2 \|\phi_j\|_2}, \tag{3.14}$$

which measures the linear dependency of columns in $\mathbf{\Phi}$. Based on the definition of coherence, we have the following proposition (the proof is given in Appendix .2)

Proposition 2. *When the sparsity of data burst satisfies (f is the ratio of $h_{\min}^2$ and $h_{\max}^2$)*

$$\|\mathbf{x}\|_0 \leq \frac{1}{4}\left(\frac{f}{M} + 1\right), \tag{3.15}$$

we have

$$\|\hat{\mathbf{x}}_{\delta,\epsilon} - \mathbf{x}\|_2 \leq \frac{1}{\gamma_{\max}(f - M(4N-1))}, \tag{3.16}$$

where $\hat{\mathbf{x}}_{\delta,\epsilon}$ is the recovered signal obtained from Eq. 3.12 and

$$\gamma_{\max} \triangleq \frac{h_{\max}^2}{(\epsilon + \delta)^2}.$$

3.1.3 Numerical Results

Numerical simulations have been carried out to evaluate the performance of our proposed compressed multiple access. We assume that the channel amplitude gain satisfies a Rayleigh distribution within the interval $[0.1, 10]$, i.e., $h_{\min} = 0.1$ and $h_{\max} = 10$.

Compressed sensing reconstruction algorithm OMP* is used for compressed multiple access' signal reconstruction process. Because OMP is usually faster than other reconstruction algorithms such as BP (Tropp and Gilbert, 2007); moreover, it can handle noisy compressive measurements efficiently (Boufounos et al., 2007)†. We choose the simple slotted CSMA as a baseline, which employs truncated binary exponential back-off mechanism with the maximum delay of 1023 time slots (Ling and Meng, 2006). We assume that 256 transmitters are associated with a base station. Each transmitter generates data packet independently, and interval between data packets of every transmitter is exponentially distributed. By changing the rate parameter (e.g., 0.43 data/slot means that there are averagely 0.43 active transmitters in each time slot), effects of different data generation rates of traffic are tested. In each realization, 10000 time slots are simulated. We use 100 realizations to obtain the transmission delay statistics, including transmission delay's mean value and standard deviation. The CDF (Cumulative Distribution Function) of the number of active transmitters is provided in Fig. 3.3, which shows that the number of active transmitters, as a random variable, varies significantly.

The length of each data packet sent by transmitters is set to 16 bits (e.g., temperature monitoring sensors report to an intermediate data collector). And for CSMA, we add a header for identifying the reporting transmitters. Since 256 transmitters are deployed, we add extra 8 bits for the transmitter ID. We assume that the PAM-16 modulation is used, thus 4 bits are transmitted in every successful

*Note that OMP tries to directly solve the 0-norm optimization problem instead of solving the 1-norm optimization problem.

†Note that BP is also modified to combat noise (Lu and Vaswani, 2010). However, the computational cost is much higher.

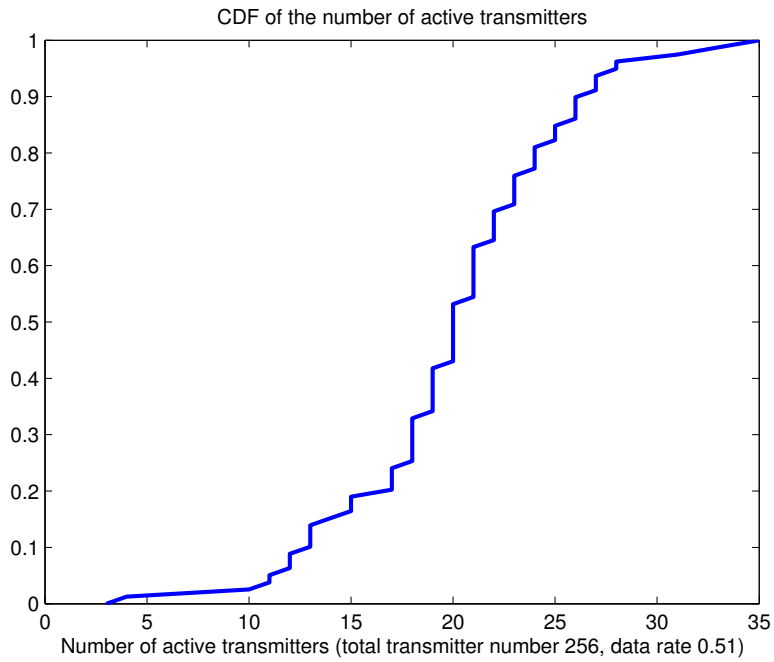


Figure 3.3: CDF of The Number of Active Transmitters

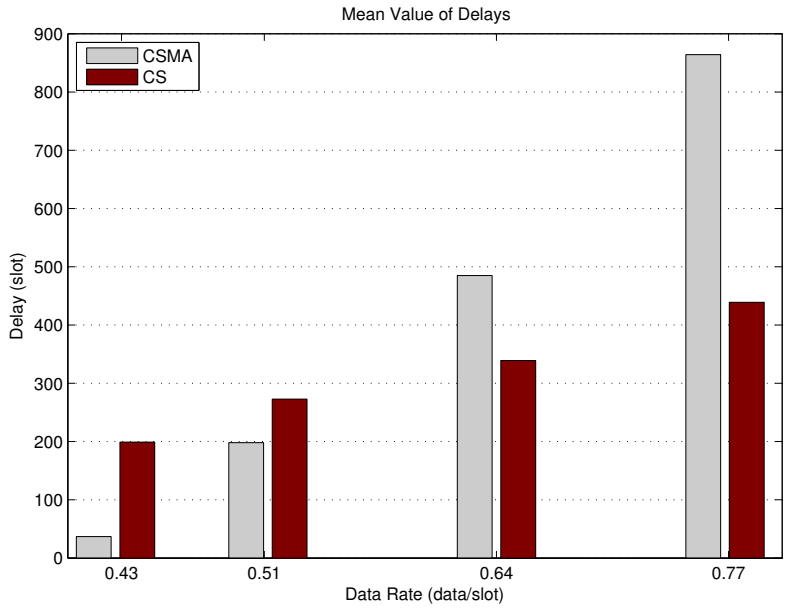


Figure 3.4: Mean Values of Delay under Different Data Rates

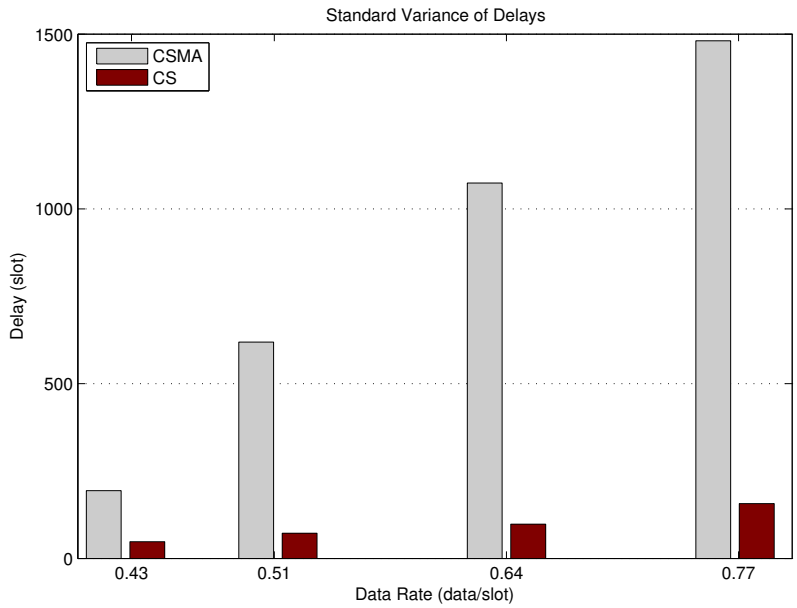


Figure 3.5: Standard Deviations of Delays under Different Data Rates

transmitting time slot. Meanwhile, we assume that the dimension of the vector channel is 2. For a fair comparison, we assume that the CSMA approach can transmit two data symbols over the two dimensions simultaneously. Therefore, in the CSMA approach, all degrees of freedom in the vector channel are used for multiplexing, while they are used for multiple access in the compressed multiple access scheme since the same data symbol is transmitted over all dimensions of the vector channel. As a result, for the compressed multiple access, a data needs 4 frames to transmit, while for CSMA, it takes 3 transmitting time slots, when there are no competing transmitters. For instance, if the average interval between two data packets of every transmitter is 1000 time slots, then for each dimension of the vector channel, its data rate is 0.77, i.e., 0.77 successful transmission is needed for each time slot ($\frac{16+8}{4\times 2} \times 256 \div 1000$, "$16+8$" is the number of bits of a data packet for CSMA, 16 bits data and 8 bits ID; "4×2" is the number of bits transmitted each time slot; PAM-16 transmits 4 bits per time slot and there are 2 dimensions, 256 transmitters; 1000 is average interval). The signature waveform uses random binary variables. We also assume that the

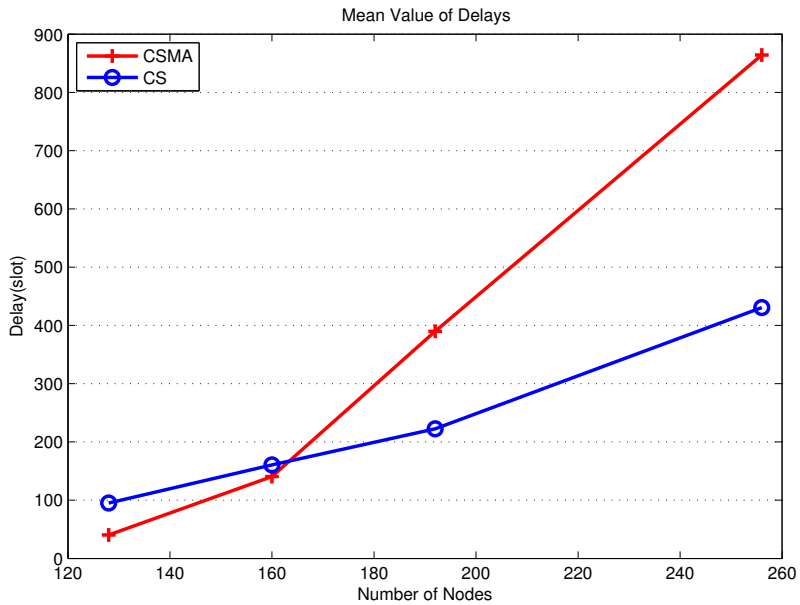


Figure 3.6: Mean Value of Delays with Different Number of Nodes

channel gains **H** are uniformly distributed between -3dB and 3dB. The assumption is reasonable if we consider the power control of transmitters. The transmit power can be incorporated into the channel gains. Then, the randomness of the channel gain is from the granularity of the power control (we assume that the transmit power does not change continuously).

We first compare the performance of proposed compressed multiple access and slotted CSMA under the situation that no noise is presented. Under a very low data rate, CSMA has a shorter average delay than the compressed multiple access. However, when data rate changes from very low (averagely, 0.43 data generated per time slot) to medium or high data rate (0.64 or 0.77 data per time slot), CSMA's average delay increases much faster than compressed multiple access, as observed in Fig. 3.4. Another key observation is that, regardless of the traffic load, the proposed compressed multiple access scheme always achieves much smaller variance of transmission delay (or, equivalently jitter) than CSMA. This implies that the

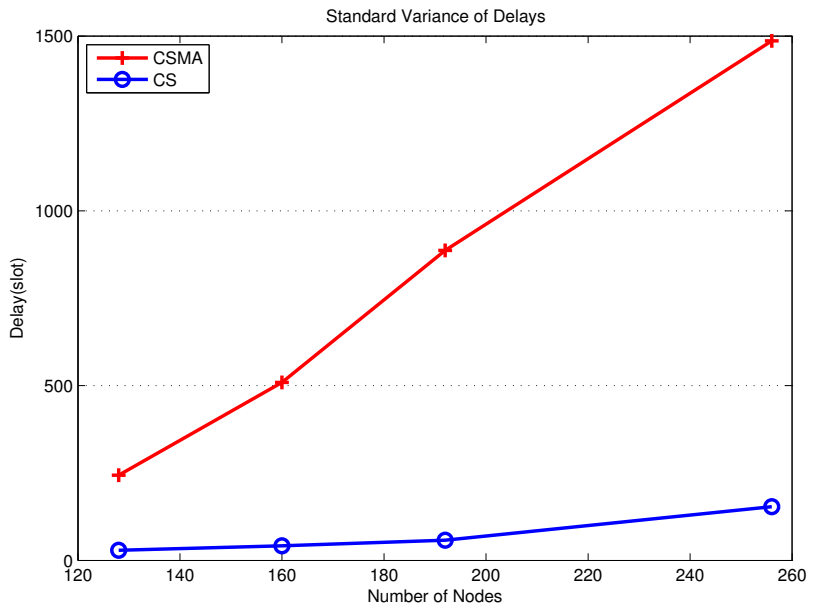


Figure 3.7: Standard Deviation of Delays with Different Number of Nodes

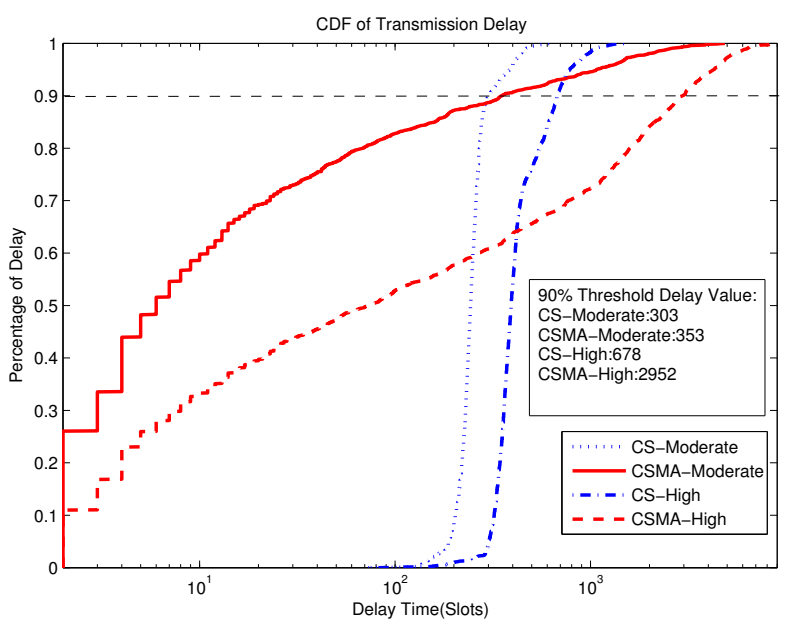


Figure 3.8: CDF of Delays

compressed multiple access scheme is suitable for real-time traffic which has a rigorous requirement for the delay.

We also test the influence of changing the number of transmitters associated with the base station. The results are shown in Figures 3.6 and 3.7. By varying the number of nodes from 128 to 256, the mean value and standard variance of delays for both the compressed multiple access and CSMA increase. Again, the mean value and standard deviation of delays of CSMA increase much faster than that of the compressed multiple access. This implies an advantage of compressed multiple access, i.e., its delays are concentrated in a much smaller range, which is critical for system stability, as observed in Fig. 3.5 and Fig. 3.7. The CDF curves of the delays are shown in Fig. 3.8 for both the compressed multiple access and CSMA, as well as for both moderate and high traffic loads (0.51 and 0.77 data packet per time slot). We can observe that the compressed multiple access has much smaller 90% *percentile* values of the delay (the 90% percentile values are labeled in the figure). Quite often, a system's transmission bottleneck is the tail of long delays which may determine the whole system's performance. Therefore, the compressed multiple access is more suitable to provide Quality of Service (QoS) and is more stable when dealing with heavy traffic.

When noise presents, both CSMA and compressed multiple access suffer, however, compressed multiple access preserves its advantages of smaller variance and smaller 90% *percentile* value of transmission delays over CSMA. Fig. 3.9 shows that under both data rates (*high*: 0.77 packet per time slot and *moderate*: 0.51 packet per time slot), compressed multiple access always has smaller variance of delays. As to mean value, under high data rate and low SNR, compressed multiple access provides competitive mean value of delays as CSMA does; under high data rate and high SNR, compressed multiple access has smaller mean value of delays than that of CSMA, therefore outperforms CSMA. When data rate is moderate, CSMA has smaller mean value of delays. But as SNR increases, the difference between mean value of delays associated with CSMA and mean value associated with compressed multiple access

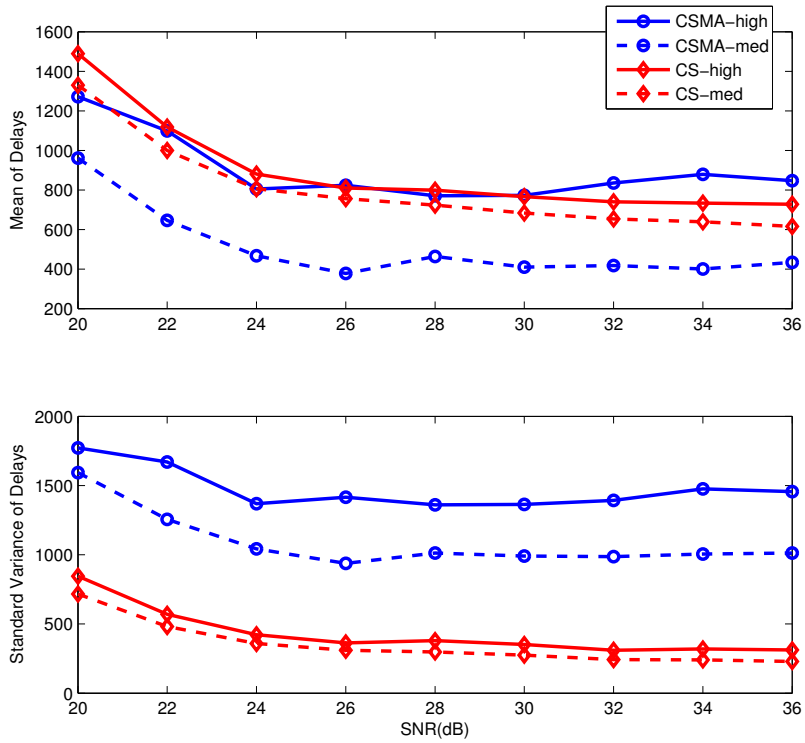


Figure 3.9: Mean Value and Standard Deviation of Delays (With Noise)

becomes smaller. CDF curves of the delays with noise are shown in Fig. 3.10. This figure is obtained when SNR is 35dB and data rate is high (0.77 packet per time slot). As observed from Fig. 3.10, noise presents challenges to compressed multiple access due to increased difficulty in reconstructing signal from measurements polluted by noise (Boufounos et al., 2007). But when SNR is high enough (above 30dB), even performance of compressed multiple access does deteriorate by certain degree, it still has smaller 90% *percentile* value of transmission delays than that of CSMA.

To demonstrate the validity of the asynchronous OMP algorithm in Algorithm 3, we have carried out simulations for a single frame with 50 time slots. We assume that there are 20 users and the number of active users change from 1 to 10. We assume $T_c = 20$ and $\tau_{\max} = 0, 5$. When $\tau_{\max} = 0$, the transmitters are perfectly synchronous. We define an error as the event that the estimated set of active users is wrong. Then,

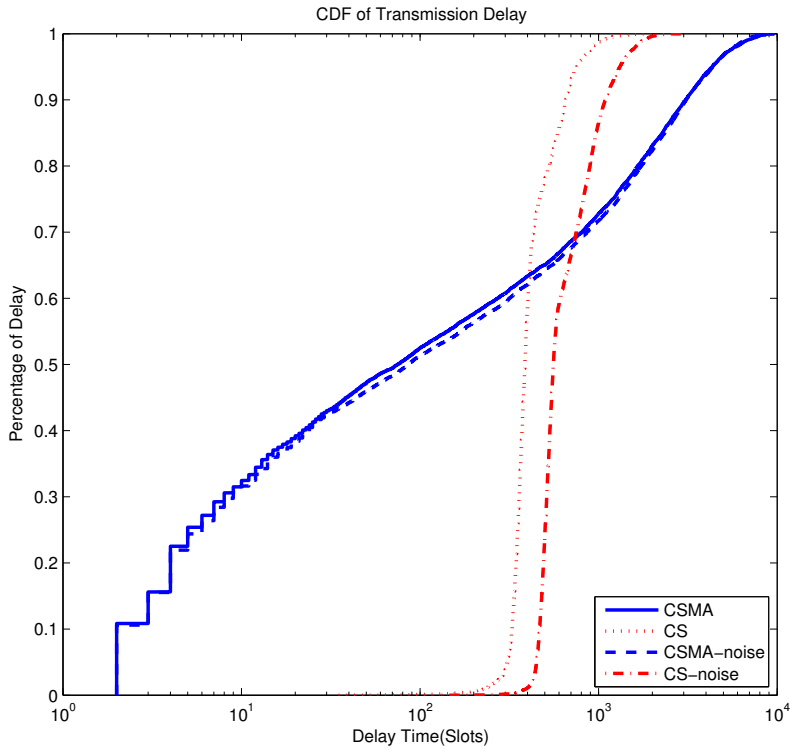


Figure 3.10: CDF of Delays (With Noise)

the error rates are shown in Fig. 3.11 for various numbers of active users. We observe that the asynchronicity incurs some performance degradation; however, the error rate is still low even when the sparsity is around 50% (when there are 10 active users). This significantly demonstrates the validity of the proposed asynchronous OMP algorithm.

3.1.4 Conclusion

We have applied the technique of compressed sensing to compress the data transmission and transmitter identification in a multiple access system with random data traffic. Collision is allowed for the multiple access in a way similar to CDMA. A protocol has been proposed to accomplish the proposed algorithm. Numerical results have demonstrated the small average and variance of delay for the proposed scheme,

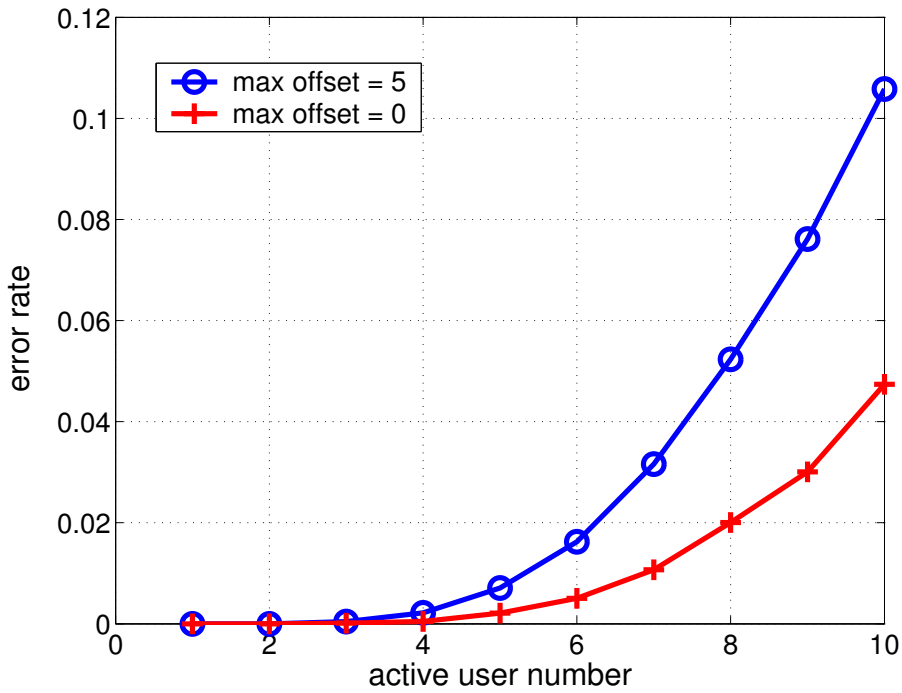


Figure 3.11: Error Rate of Asynchronous OMP

especially under heavy traffic situation, compared with the traditional slotted CSMA. This implies that our proposed multiple access scheme is useful for real-time (soft) data traffic with QoS requirements.

3.2 Sample-Contention Multiple Access

For *compressed multiple access* discussed in the previous section, we made the assumption that traffic from sensors is sparse, and individual sensors are independent, transmitting data when data becomes available. In this section, we consider a scenario in which data generated at sensors is not sparse, but the number of sensors that are allowed to transmit is constrained based on control needs. Thus, sensors have to cooperated with other sensors as well as their base station to satisfy the constraint. We introduce *sample-contention multiple access* scheme that solves the cooperation problem.

To make sample-contention multiple access easy to understand within the context of CPS, we design sample-contention multiple access for WiMAX with a typical application of voltage control in power system. But, the scheme we are going to present is a general multiple access scheme that can be implemented in various communication system. In the following, we give an introduction to WiMAX and voltage control in power system first.

United States and many other countries or regions all over the world are in the middle of a massive process of upgrading their power systems, which at some extreme cases could be almost a century old. With an emphasis on integration and interaction among various components, *smart grid* is playing a leading and representative role of power system automation and upgrade (Smartgrid.gov, 2012). A critical function missing or under-developed in old power systems but repeatedly highlighted in smart grid is communication. The presence of flexible and efficient two-way communication can fundamentally change how power systems work, which in turn can have deep impact on people's daily life.

In this section, we study the problem of cooperative voltage control in smart grid with an efficient sample-contention multiple access scheme using WiMAX. Traditionally, power system voltage control is carried out at substations and certain prefixed infrastructures such as shunt capacitors; thus available control options are comparatively simple and have limited capabilities. Furthermore, little communication or no communication at all is employed when making control decisions, and most control procedures are local, without considering voltage states other than at the point where the local controller stays. The appearance of a large number of Distributed Energy Resources (DER) such as distributed generators, solar panels in smart grid requires coordination among them; otherwise, they can hardly contribute to the power network to their full capabilities. More seriously, their uncoordinated behaviors could actually undermine the stability of the power system by introducing conflicts. To coordinate the collaboration of multiple DERs in voltage control, we propose a *sample-contention* mechanism in WiMAX to prioritize

voltage state reports. An area central controller located at the WiMAX base station (BS) combines newly updated reports with prediction estimations as current complete voltage state and applies optimal control accordingly.

WiMAX is a good platform for communications in power systems. From the perspective of power system operators, what they care most is reliability and Quality of Service (QoS). WiMAX, as one form of the fourth generation (4G) wireless communication, has unprecedented data rate and off-the-shelf products available, which are already deployed in many places around the world (Sekercioglu et al., 2009). Most importantly, its large coverage and specific service classification for QoS support really make it stand out. As opposed to conventional WiFi-based network which has a transmission range of hundreds of meters at most, WiMAX can easily cover tens of kilometers, which makes WiMAX practical to serve hundreds of DERs in its covered area. Inherent five categories of service with QoS priority from high to low, namely unsolicited grant service (UGS), extended real-time polling service (ertPS), real-time polling service (rtPS), non-real-time polling service (nrtPS) and best effort service (BE) (Sekercioglu et al., 2009), guarantee QoS requirements of power system communication to be satisfied. By forming a back-haul WiMAX network with multiple BS's, they are able to cover even larger area and still strictly follow QoS standards.

While WiMAX provides an attractive platform for communications in power systems, cooperative voltage control in smart grid using WiMAX still needs an appropriate design for the traffic scheduling. Existing studies on voltage control in power system either neglect the communication aspect by assuming that the controller has perfect system state knowledge, or mainly focus on control itself and lack an in-depth analysis of the communication subsystem (Li et al., 2010; Fakham et al., 2010; Wen et al., 2004; Jin et al., 2010). On the other hand, researches on WiMAX seldom take into account the unique requirements of its application in power systems (Vu et al., 2010; Belghith et al., 2008). In Li et al. (2010), local adaptive PID feedback is used for voltage control, which greatly reduces voltage overshoot and fluctuation

during voltage regulation process. The authors have also mentioned the performance improvement of voltage control incurred by communication, but do not present the implementation of communication subsystem. Model Predictive Control (MPC) is a popular control method in voltage control; however, studies using MPC for voltage control usually assume that current system state is completely available for state prediction (Jin et al., 2010; Wen et al., 2004). Although ad-hoc network has the problem of weak QoS support, research of performance analysis on them, especially on 802.11e-based networks, provides insight into how to provide QoS service on wireless communication (Lin and Wong, 2006; Hanzo and Rafazolli, 2009). Our *sample-contention* idea is in part inspired by Kanodia and Li (2002), in which transmitters update their local scheduling table using overheard RTS/CTS and ACK information of 802.11 network. However, the proposed sample-contention process in WiMAX and Maximum Likelihood Estimation (MLE) for overall data distribution estimation distinguish our work from Kanodia and Li (2002). Shi et al. (2009) should also receive credits for providing helpful information with its handling of data prioritization from the game theory perspective.

3.2.1 Voltage Control Model in Power System

Suppose that, in the power system we study, N bus voltages are under constant regulation by manipulating M DERs. $\mathbf{v} = [v_1, v_2, ..., v_N]^T$ is the voltage vector of the N buses; and $\mathbf{v}_r = [v_{1r}, v_{2r}, ..., v_{Nr}]^T$ is the predefined corresponding reference voltage vector, which in normal condition $\mathbf{v}$ should stay close to. Denoting the voltage deviation by $\mathbf{x}$, we have $\mathbf{x} = \mathbf{v} - \mathbf{v}_r$. Take the voltage deviation $\mathbf{x}$ as system state, we can model the power system in discrete time by Eq. 3.17.

$$\mathbf{x}_{k+1} = \mathbf{A}\mathbf{x}_k + (\mathbf{B} + \mathbf{m})\mathbf{u}_k + \mathbf{n'}_k, \tag{3.17}$$

in which $\mathbf{u}_k \in \mathcal{R}^M$ is the control action taken by the M DERs; $\mathbf{n'}_k \in \mathcal{R}^N$ is a vector of Gaussian random variables which represent the power system disturbance

at $t = k$; $\mathbf{A} \in \mathcal{R}^{N \times N}$ is a diagonal system transit matrix with elements $a_{ii} > 1,\ i = 1, ..., N$, which means that, without correction from DER, system voltage would change monotonously, resulting in increasing voltage deviations (Wen et al., 2004); $\mathbf{B}, \mathbf{m} \in \mathcal{R}^{N \times M}$, $\mathbf{B}$'s element b_{ji} is a contributing factor reflecting the controlling effect of DER i on the voltage of bus j, and Gaussian random variables in $\mathbf{m}$ are introduced due to calibration error in determining $\mathbf{B}$. Let $\mathbf{n}_k = \mathbf{m}\mathbf{u}_k + \mathbf{n}'_k$. Then $\mathbf{n}_k$ is also a vector of Gaussian random variables because the sum of two independent Gaussian random vector is still a Gaussian random vector. $n_k \in \mathcal{N}(u(k), \sigma(k)^2)$, both $u(k)$ and $\sigma(k)$ are random processes and the expectation of $u(k)$ is 0. Rewriting Eq. 3.17 by substituting $\mathbf{n}_k$ into the equation, we have

$$\mathbf{x}_{k+1} = \mathbf{A}\mathbf{x}_k + \mathbf{B}\mathbf{u}_k + \mathbf{n}_k. \tag{3.18}$$

Consider $\mathcal{S} \subset \mathcal{N}$ as the set of voltage monitors which report to the power system's controller at $t = k$, where $\mathcal{N}$ is the set of all monitors. The estimation of system state $\hat{\mathbf{x}}_k$ is the combination of updated voltage readings by $\mathcal{S}$, $\mathbf{x}_k(\mathcal{S})$, and prediction estimation at $t = k - 1$ of those which have not been updated by $\mathcal{S}$, $\hat{\mathbf{x}}_{k|k-1}(\mathcal{N}/\mathcal{S})$, i.e.,

$$\hat{\mathbf{x}}_k = \mathbf{x}_k(\mathcal{S}) \cup \hat{\mathbf{x}}_{k|k-1}(\mathcal{N}/\mathcal{S}). \tag{3.19}$$

The prediction of system state is carried out according to the following equation:

$$\hat{\mathbf{x}}_{k+1|k} = \mathbf{A}\hat{\mathbf{x}}_k + \mathbf{B}\mathbf{u}_k. \tag{3.20}$$

Meanwhile, we define a cost function $J(\mathbf{u}_k)$ which takes into account both voltage deviation penalty and control input costs, i.e.,

$$J(\mathbf{u}_k) = \sum_{k=1}^{\infty} (\hat{\mathbf{x}}_{k+1|k}^T \mathbf{R} \hat{\mathbf{x}}_{k+1|k} + \mathbf{u}_k^T \mathbf{Q} \mathbf{u}_k), \tag{3.21}$$

where $\mathbf{R} \in \mathcal{R}^{N\times N}$ and $\mathbf{Q} \in \mathcal{R}^{M\times M}$ are both diagonal matrices whose non-zero elements are cost weighting factors. At $t = k$, when voltage readings from set $\mathcal{S}$ are available, by using Eq. 3.19, we are able to obtain system state $\hat{\mathbf{x}}_k$. We further substitute Eq. 3.20 into the cost function $J(\mathbf{u}_k)$ and then $\mathbf{u}_k$ becomes the only variable of $J(\mathbf{u}_k)$. Thus, the voltage controller calculates the optimal control input based on available voltage observations by minimizing the cost function, which can be written as

$$\mathbf{u}_k^*|\mathcal{S} = \underset{\mathbf{u}}{\operatorname{argmin}} J(\mathbf{u}_k) \quad |\mathbf{u}| \leq \mathbf{u}_{max}. \tag{3.22}$$

3.2.2 Sample-Contention Multiple Access for Voltage Control

In this subsection, we present our sample-contention scheme for efficient communication in voltage control. This scheme takes full advantage of WiMAX features we mentioned in the previous introduction section to provide QoS-aware communication service for the set of voltage monitors, $\mathcal{S}$.

Sample-contention Scheme Overview

To help readers better understand the sample-contention scheme, we first give a brief description of the network organization and the frame structure of WiMAX. In centralized point-to-multipoint network organization of WiMAX, subscriber stations (SS) share the uplink to a Base Station (BS) on demand basis (IEEE, 2005). In the downlink, BS acts as a broadcaster. Therefore, if an SS wants to upload data to the BS, it has to send request message first and then waits for the BS to grant uplink transmission opportunities, which are time slots in WiMAX uplink subframe. As illustrated in Fig. 3.12, a WiMAX frame has one downlink subframe and one uplink subframe which is preceded by *ul-map* and *dl-map* broadcast periods from BS. *ul-map* and *dl-map* consist of time slot allocation information for the following uplink subframe and downlink subframe respectively.

As the packet size of voltage state reporting data is really small, the conventional WiMAX request-grant-transmit mechanism is not suitable for voltage state reporting. A better way is to embed voltage data into request slots. In addition, due to the sparseness of voltage disturbance (discussed at the following subsection), the contention-based request fits the requirement of voltage reporting the best. In order to utilize communication resources efficiently, only m ($m < N$) request (reporting) slots are allocated in each reporting interval (*m-contend*). Before the contention-based reporting starts, n randomly selected SS's (voltage monitors) broadcast their current voltage states in the *n-sample* interval (also illustrated in Fig. 3.12). IDs of the n SS's and their transmitting orders are decided by the BS (controller) and broadcast during the *ul-map*. Other unselected SS's prioritize their voltage reporting based on overheard reportings during the *n-sample* interval.

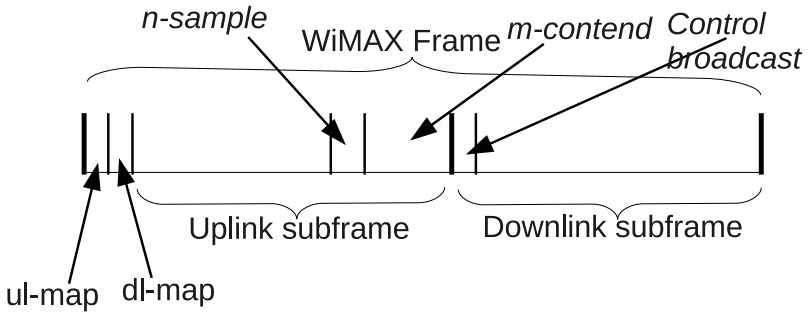


Figure 3.12: Sample-contention Scheme Implemented in A WiMAX Frame

The sample-contention scheme is summarized as follows:

1. At the beginning of a WiMAX frame, in the *ul-map*, BS broadcasts the IDs of randomly selected SS's and their reporting orders in the *n-sample* interval.

2. During the *n-sample* interval, selected SS's send their voltage state data following the predetermined transmitting order. Unselected SS's use these overheard reports as samples and apply MLE to distributively decide the priority of their own reports (will be discussed in details in the next subsection).

3. In the *m-contend* interval, unselected SS's which believe that their priorities are sufficiently high contend for access.

4. In the *control broadcast* interval, which is at the beginning of downlink subframe and right after the *m-contend* is completed, BS broadcasts control instructions to all DERs.

Prioritized Transmission

A key observation of power system is that most of the time the system operates at normal status and the voltage stays close to its desired reference level. Voltage starts drifting away from the reference level dramatically only when significant disturbance happens. These disturbances could be incurred by unexpected severe load change, device malfunction in the system, extreme weather and so on. If the voltage runaway is not curbed in time, power system could collapse, thus leading to catastrophic consequences.

The sparseness of large voltage deviation presents the challenge of efficient utilization of communication resources. This sparseness is both in the time domain and space domain; i.e., at an arbitrary time point large voltage deviation happens only with a small probability, and even when it happens, normally only a small portion of SS's would experience large deviations and have to report urgently. Therefore, it is unwise to allocate a large number of reporting time slots on a regular basis. While SS's that do have large deviation to report should contend for limited reporting slots access, SS's with small deviation should keep silent and leave access opportunity to SS's which really need them. Each SS has to make a critical distributed decision on whether contending for limited access opportunities in the m-contend reporting interval.

When n randomly selected SS's report to BS in the n-sample interval, we assume that their transmitting power is sufficiently large such that all other unselected SS's

are able to overhear all the n reports[‡]. Let $\mathcal{S} = \{x_1, ..., x_n\}$ be the set of the n voltage deviation samples from the n-sample interval. Each of the remaining $N - n$ SS's independently estimates the distribution of current voltage deviation with the set of samples, using MLE. In power systems, voltages stay close to their predicted trajectory most of the time and only a few occasionally deviate far. We assume voltage deviations follow independent and identical normal distribution with expectation u and standard deviation σ, $\mathcal{N}(u, \sigma^2)$. Note that, with the time-varying disturbances in power systems happen at different times, both u and σ^2 could take different values at different reporting intervals. The likelihood function of MLE for the sample set $\mathcal{S} = \{x_1, ..., x_n\}$ with $\mathcal{N}(u, \sigma^2)$ distribution is given by

$$\mathcal{L}(x_1, ..., x_n | u, \sigma^2) = (\frac{1}{2\pi\sigma^2})^{\frac{n}{2}} exp(\frac{-\sum_{i=1}^{n}(x_i - u)^2}{2\sigma^2}). \tag{3.23}$$

Since logarithm is a continuous and strictly increasing function over the range of the likelihood, the values which maximize the log-likelihood will also maximize the likelihood itself. We maximize the log-likelihood over u and σ by differentiating with respect to u and σ and equating to zero. Then, we have

$$\hat{u} = \underset{u}{\operatorname{argmax}} \mathcal{L} = \frac{1}{n} \sum_{i=1}^{n} x_i \tag{3.24}$$

$$\hat{\sigma}^2 = \underset{\sigma}{\operatorname{argmax}} \mathcal{L} = \frac{1}{n} \sum_{i=1}^{n} x_i^2 - \frac{1}{n^2} \sum_{i=1}^{n} \sum_{j=1}^{n} x_i x_j. \tag{3.25}$$

Details on MLE and the process of obtaining its optimal estimation of parameters can be found in Poor (1994).

With estimated $\hat{u}$ and $\hat{\sigma}^2$ available for normal distribution, we can move on to prioritize the $N - n$ SS's transmission. Suppose that, for current m-contend interval, the controller declared in the *ul-map* that K out of $N - n$ SS's were expected to

[‡]Standard WiMAX SS may not have the overhearing function. However, it should not be difficult to add this function to power system devices which are compatible with the standard WiMAX protocol and use them for the purpose of voltage control.

contend for access. The value of K can be adjusted by the controller based on the previous received voltage state reports; the number of time slots in the m-contend interval should be adjusted accordingly when K changes, where the relationship between K and m will be analyzed in the next subsection. With the portion of SS's which should be given the contend access eligibility out of $N-n$ SS's being $\frac{K}{N-n}$, let voltage deviation threshold of contend access eligibility be $D_T > 0$ under which SS is not allowed to transmit in the m-contend interval, we have

$$\int_{-D_T}^{D_T} \frac{1}{\sqrt{2\pi}\hat{\sigma}} exp(-\frac{(x-\hat{u})^2}{2\hat{\sigma}^2})dx = 1 - \frac{K}{N-n}. \tag{3.26}$$

By solving Eq. 3.26, we can obtain threshold value D_T given the estimated normal distribution parameters $\hat{u}$ and $\hat{\sigma}^2$ are available. Fig. 3.13 illustrates the portion of voltage deviations (shaded parts) which are eligible for transmission in the m-contend interval. Each SS of the $N-n$ unselected ones during the n-sample interval can independently go through the above estimation and threshold calculation process with its overheard samples. If its voltage deviation is larger than D_T, then it will contend for reporting to the BS in the m-contend interval.

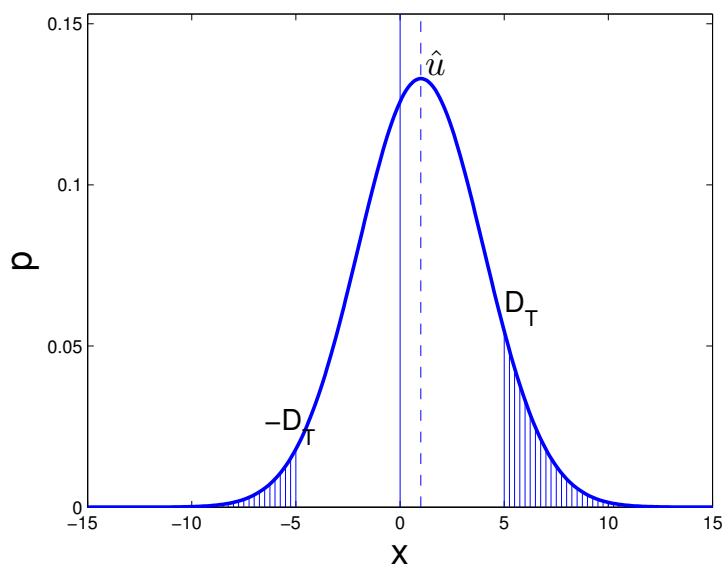


Figure 3.13: Transmission Eligibility Threshold

Analysis of Contending Access

Suppose that there are m time slots in the m-contend interval, and the controller has declared in the *ul-map* that K SS's are expected to contend for access (actual number of contending SS's could be different from K because of estimation error), all with the same contention window size, CW. We also denote by K_s the number of successful access slots, i.e, slots except those either being idle or having a collision. Then, we have

$$K_s = \begin{cases} mK\frac{1}{CW}(1-\frac{1}{CW})^{K-1} & CW \geq m \\ CWK\frac{1}{CW}(1-\frac{1}{CW})^{K-1} & 0 < CW \leq m \end{cases}. \tag{3.27}$$

K_s achieves its maximum value when $K = K^*$, i.e.,

$$K^* = \underset{K}{\operatorname{argmax}} K_s = \frac{-1}{ln(1-\frac{1}{CW})} \approx CW, \quad CW, K \in \mathbb{N}. \tag{3.28}$$

Thus, replacing K in Eq. 3.27 with its optimal value CW, we further have

$$K_s = \begin{cases} m(1-\frac{1}{CW})^{CW-1} & CW \geq m \\ CW(1-\frac{1}{CW})^{CW-1} & 0 < CW \leq m \end{cases}. \tag{3.29}$$

Because $(1-\frac{1}{CW})^{CW-1}$ is a monotonously decreasing function and $CW(1-\frac{1}{CW})^{CW-1}$ is a monotonously increasing function, given $CW \in \mathbb{N}$, we obtain

$$K_{s,max} = m(1-\frac{1}{m})^{m-1} \approx \frac{1}{3}m. \tag{3.30}$$

Eq. 3.30 states that, for the m time slots in the m-contend interval, at most $\frac{1}{3}m$ SS's have successful access if there are m SS's contending for access (i.e., $K = m$) and their contention window size is set to m. However, the voltage state reporting process expects as many as possible SS's of the K contenders having successful access with minimum contending time slots, i.e., maximizing the communication channel efficiency.

Based on Eq. 3.30, we propose multi-contention in the m-contend interval. Given K announced contenders, the controller allocates $m = 3K$ time slots in the m-contend interval. Each self-qualified SS has 3 contending opportunities with different transmitting time slots (local virtual-conflict resolution). Altogether, it imitates the situation that m SS's contend in m time slots. As showed in Fig. 3.14, with the proposed approach, a contender's probability of successful transmission is $1-(1-(\frac{\binom{m-1}{3}}{\binom{m}{3}})^{K-1})^3$, which is larger than $(1-\frac{1}{m})^{K-1}$, the probability of successful transmission when a contender transmits randomly only once in m slots. In the voltage control system where the transmitting power is abundant, it is obvious that the multi-transmitting and multi-contention approach is better.

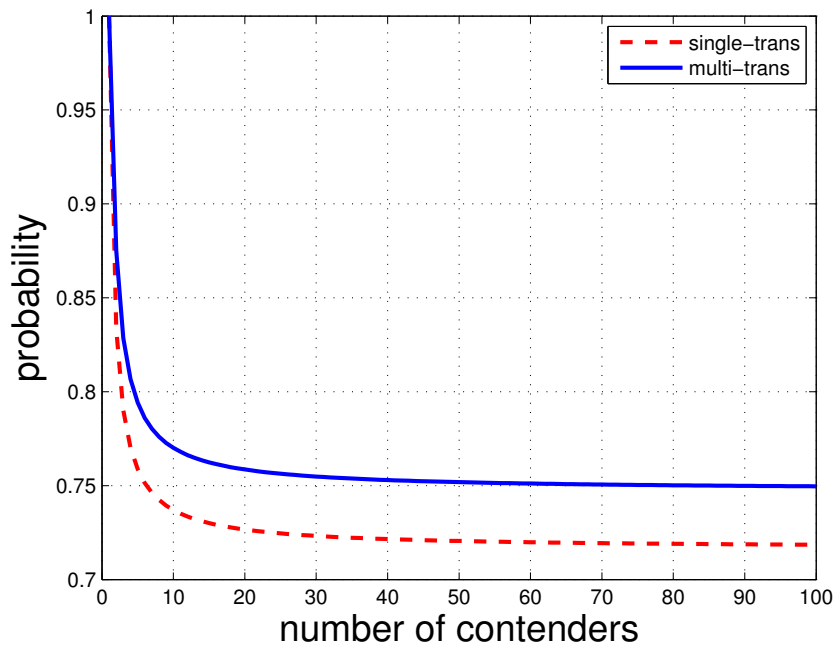


Figure 3.14: Comparison of Successful Transmission Probability

3.2.3 Numerical Simulation and Performance Evaluation

In this subsection, we provide simulation results to demonstrate the effectiveness and efficiency of the proposed sample-contention communication scheme for voltage control in power system.

We consider in our simulation a power system which has $N = 200$ bus voltages under control by manipulating 200 DERs. The diagonal elements in the system state transit matrix $\mathbf{A}$ are all set to be 1.05, and the contributing factors of DERs in $\mathbf{B}$ are set to 1. $n = 20$ randomly selected SS's broadcast their voltage states in the n-sample interval; $m = 60$ time slots are allocated in the m-contend interval for $K = 20$ expected contenders. We compare our sample-contention scheme with three other different state reporting schemes: 1) complete information: at each control iteration, the central controller has complete information of all voltage states, thus consuming 200 time slots; 2) random access: at each iteration, the controller uses the same number of time slots (80) for randomly selected SS's to report voltage states; 3) round-robin access: at each iteration, the controller updates voltage states using round-robin polling (80 SS's each time).

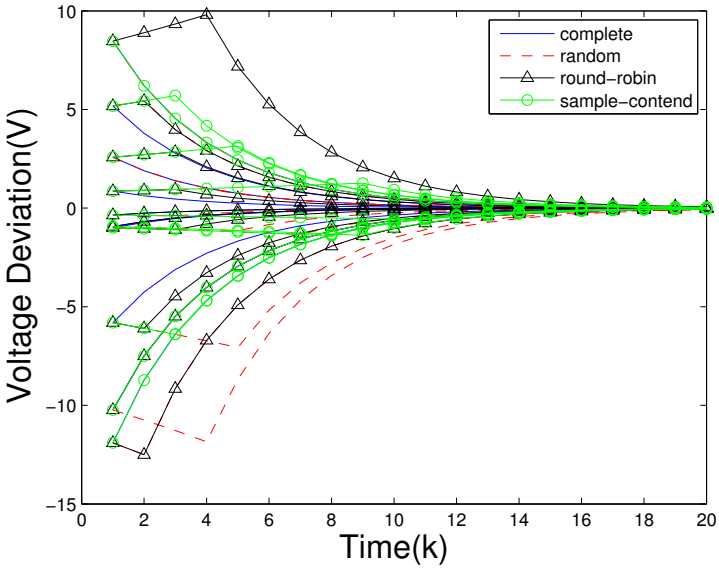


Figure 3.15: Voltage Deviation Trajectories Under Control

Fig. 3.15 shows 10 voltage deviation trajectories under voltage control methods using different voltage state reporting schemes. We observe that the voltage under complete information control method converges the fastest; while both the random access control method and round-robin access control method miss curbing the largest

deviations from the beginning, our proposed sample-contention starts regulating them at the very first control action. This responsive action is attributed to the prioritized reporting transmission in the sample-contention scheme which assigns higher priority to voltage monitors with larger voltage deviation.

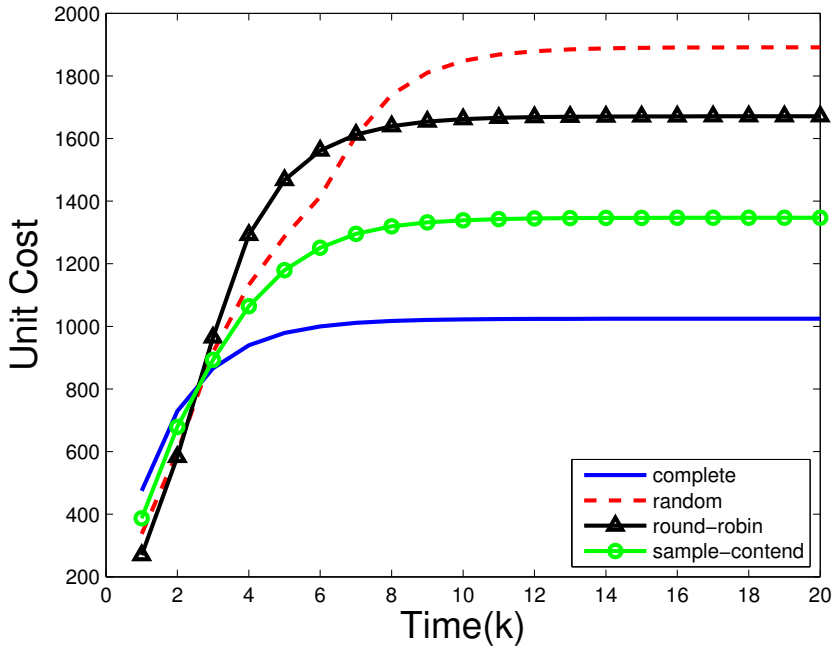


Figure 3.16: Comparison of Total Cost of Different Voltage Control Schemes

Fig. 3.16 shows the accumulated cost of bringing voltage back to the reference level. Again, intuitively, the complete information method has the smallest cost of 1010 unit cost, at the expense of 2.5 (200/80) times communication resource consumption compared with others'. With 1352 unit cost, the sample-contention method is about 20% more cost-effective than the round-robin method. Although the random method has small cost at the early stage of control, it has the largest final cost. The reason is that, at the beginning, it is disguised by randomly selected moderate voltage deviation reports and did not draw much cost from the control input, which actually affected it negatively afterwards. All the above cost statistics are obtained from 100 realizations.

3.2.4 Conclusion

In this section, we have proposed a sample-contention multiple access scheme for the communication system in CPS. It is a complement to the compressed multiple access scheme we introduced in section 3.1. The sample-contention scheme applies to the situation when eligible data from sensors is not sparse, but useful data in terms of control needs is sparse. As a proposed multiple access improvement to WiMAX, the sample-contention multiple access scheme is studied in detail with application to the voltage control in smart grid. By making use of the sparseness of voltage deviation, the sample-contention scheme implemented in the WiMAX framework is able to provide communication resource efficient service for voltage state reporting in smart grid. The effectiveness of the proposed scheme has been demonstrated by numerical simulation results.

3.3 Prioritized Multiple Access

With *compressed* and *sample-contention* schemes, we are able to provide efficient multiple access for wireless communication in CPS. We have not discriminated data from sensors, in other words, we treat all data with equal importance. However, when communication resources are constrained, to preserve CPS' reliability and adaptability, it is critical to identify sensors that have more important data. In this section, we are going to answer this question: in CPS, given a system state, how to decide which sensor(s) is more important and thus deserves prioritized access at the moment.

We again use smart grid for our study as a typical CPS. Smart grid is characterized by a two-way flow of electricity and information and will be capable of monitoring everything in the grid (DOE, 2008). By bringing in a variety of DERs, in particular renewable sources such as solar panels and wind turbines, smart grid addresses both globe warming and emergency resilience issues.

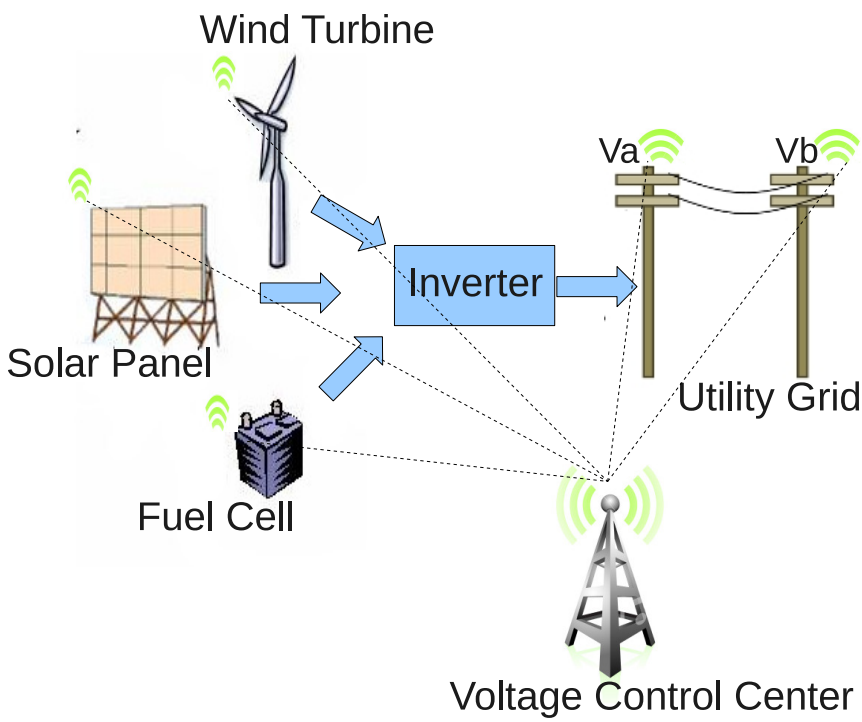


Figure 3.17: Distributed Energy Resources for Voltage Control

We study the wireless communication protocol design for regulating the voltages in smart grid which has a shared communication channel among control center, voltage sensors and DERs. The feasibility of DER for regulating voltage has been well reported in the literature, such as Ko et al. (2007). As shown in Fig. 3.17, multiple sensors monitor the voltage states at $\{V_a, V_b, \dots\}$ and report the states to the voltage control center. Based on all received reports, the control center estimates the voltage states. If the estimated voltage state is deviated from a preset desired value, the control center coordinates all available DERs to regulate voltage. The arrival of new report from sensor triggers the control center to perform another round of voltage state estimation and regulating. The above iterative voltage regulating process continues until the voltages are within a desired range.

The motivation of our work is the increasing availability of DERs, voltage sensors, and the overlaying communication network in power networks (Vaccaro et al., 2010). Although the voltage regulation for power system stability has been a critical problem under intensive study (Jin et al., 2010; Kashem and Ledwich, 2005; Ko et al., 2007; Li et al., 2010), the new properties and potential benefits brought by these new facilities still need more effort to uncover. Take the *microgrid* as an example (Hatziargyriou et al., 2007), in which DERs have demonstrated their abilities of increasing power quality and reliability in practical systems; however, developing alternative control strategies using next-generation information and communication technology is still an open question. Existing solutions for the voltage control problem with DERs either focus on analyzing the power system model or mainly study control method design, e.g., the Model Predictive Control (MPC) (Jin et al., 2010; Kashem and Ledwich, 2005) or PID controller (Ko et al., 2007; Li et al., 2010).

We will focus on the multiple access layer design of the wireless sensor networks for the voltage regulation. When orthogonal communications are required, i.e., only one transmitter can access the channel at the same time and collisions incur packet loss[§], it is of key importance to study the problem of sensor selection. A simple solution is to use round-robin scheduling, i.e., the sensors take regular turns to report their measurements, regardless of the current voltage states. However, as will be seen later, a significant performance gain over the simple scheme will be achieved by manipulating the sensors in a system state aware manner. Particularly, we will model the power grid as a hybrid system (Lunze and Lagarrigue, 2009; Savkin and Evans, 2002), in which the power system is the continuous subsystem while the communication system is the discrete subsystem. The sensor selection will be considered as the switching of the system dynamics mode. Then, we apply a sliding window algorithm to optimize the sensor selection, or equivalently, the system mode selection. To our best knowledge, there have not been any studies applying the hybrid system theory to the communication protocol design in smart grid.

[§]It is straightforward to extend to the case that multiple sensors can be scheduled simultaneously

3.3.1 System Model and Problem Formulation

We first introduce the system model, including the power dynamics, system cost and communication system. Then, we formulate the problem as three sub-problems.

Power System Dynamics

We use the following differential-algebraic equation (DAE) to describe our target power system, which is given by

$$\dot{\mathbf{x}} = f(\mathbf{x}, \mathbf{u}, \mathbf{w}'),\ \mathbf{w}' \sim \mathcal{N}(\mathbf{0}, Q'), \tag{3.31}$$

where $\mathbf{x} \in \mathbb{R}^n$ is the system state representing the voltages; $\mathbf{u} \in \mathbb{R}^m$ is the system control action; $\mathbf{w}'$ is the system process noise which is assumed to be zero-mean, Gaussian and white with covariance matrix Q'. Since the voltage is usually required to stay within a narrow range centered at a desired value, we assume that the function f can be well approximated by its linearization in the neighborhood of desired voltage values.

When voltage fluctuations due to either fault in the system or load change, DERs are able to provide compensation to regulate the voltages. Note that the action taken by a DER, say increasing its voltage, can affect all voltages in the system, more or less. Hence, a single DER as an individual actuator cannot reduce the voltage oscillation efficiently, as it does not have the global information on the voltage state. Therefore, to enable the DERs to collaboratively regulate the power system voltages, we must first obtain as much information as possible about the overall voltage state, and then assign the tasks of voltage adjustment to each DER accordingly.

There exists a group of sensors, $S_1, \ldots, S_i, \ldots, S_N$, monitoring voltage change in the power system. Each is able to obtain a partial observation of the system with its unique measuring function, which is given by

$$\mathbf{y_i} = h_i(\mathbf{x}, \mathbf{v_i'}),\ \mathbf{v_i'} \sim \mathcal{N}(\mathbf{0}, R_i'),\ i = 1, \ldots, N, \tag{3.32}$$

where $\mathbf{y_i}$ denotes the measurement obtained by sensor S_i; h_i is the measuring function associated with S_i; $\mathbf{v'_i}$ is the Gaussian measurement noise with zero mean and covariance matrix R'_i. We assume that $\mathbf{v'_i}$ is independent of the system process noise $\mathbf{w}'$.

With the controlled voltage staying close to preset desired value, we consider a discrete-time linearized model derived from aforementioned DAE. The time continuous functions f and h_i are locally linearized around desired voltage $\mathbf{x}^*$, which are given by

$$\begin{aligned}\mathbf{x}_k =& f(\mathbf{x}^*_{k-1}, \mathbf{u}^*_{k-1}, \mathbf{0}) + A(\mathbf{x}_{k-1} - \mathbf{x}^*_{k-1}) \\ &+ B(\mathbf{u}_{k-1} - \mathbf{u}^*_{k-1}) + F\mathbf{w}'\end{aligned} \tag{3.33}$$

and

$$\mathbf{y}_{ik} = h_i(\mathbf{x}^*_k, \mathbf{0}) + H_{ik}(\mathbf{x}_k - \mathbf{x}^*_k) + G_i\mathbf{v}'_i,\ i = 1, \ldots, N, \tag{3.34}$$

where A, B, F, H_{ik} and G_i are matrices derived from the Jacobian matrices of f and h_i; $\mathbf{x}^*_{k-1} = \mathbf{x}^*_k = \mathbf{x}^*$. Calculation of the Jacobian matrices and discrete-continuous model conversion are standard procedures (Negenborn et al., 2007; Shieh et al., 1980). Since at the steady state, the voltages stay at desired values and the control action is not needed, we have $\mathbf{u}^*_{k-1} = \mathbf{0}$ and $f(\mathbf{x}^*_{k-1}, \mathbf{u}^*_{k-1}, \mathbf{0}) = \mathbf{x}^*$, $h_i(\mathbf{x}^*_k, \mathbf{0}) = \mathbf{y}^*_i$. Substitute them into Eq. 3.33 and Eq. 3.34 respectively, we have

$$\mathbf{x}_k = \mathbf{x}^* + A(\mathbf{x}_{k-1} - \mathbf{x}^*) + B\mathbf{u}_{k-1} + F\mathbf{w}', \tag{3.35}$$

and

$$\mathbf{y}_{ik} = \mathbf{y}^*_i + H_{ik}(\mathbf{x}_k - \mathbf{x}^*) + G_i\mathbf{v}'_i,\ i = 1, \ldots, N. \tag{3.36}$$

Letting $\Delta\mathbf{x}_k = \mathbf{x}_k - \mathbf{x}^*$, $\Delta\mathbf{y}_{ik} = \mathbf{y}_{ik} - \mathbf{y}^*_i$, $\mathbf{w} = F\mathbf{w}'$ and $\mathbf{v}_i = G\mathbf{v}'_i$, we obtain the voltage deviation based system equation 3.37 and the measurement equation 3.38,

which are given by

$$\Delta \mathbf{x}_k = A\Delta \mathbf{x}_{k-1} + B\mathbf{u}_{k-1} + \mathbf{w},\ \mathbf{w} \sim \mathcal{N}(\mathbf{0}, Q), \tag{3.37}$$

$$\Delta \mathbf{y}_{ik} = H_{ik}\Delta \mathbf{x}_k + \mathbf{v}_i,\ \mathbf{v}_i \sim \mathcal{N}(\mathbf{0}, R_i), i = 1, \ldots, N, \tag{3.38}$$

where $Q = FQ'F^T$, $R_i = G_i R_i' G_i^T$. Q represents the power system uncertainties which may be due to variations in the power system parameters, the effects of nonlinearities and the dynamics that have not been included in the power system model. R_i reflects the uncertainties of sensor i's measurement mainly because of noise.

System Cost

We define the time discretized cost function for the system as a quadratic function which penalizes the voltage deviation and minimizes control cost, which is given by

$$J = \mathbb{E}(\sum_{k=1}^{k=K}(\Delta \mathbf{x}_k^T D \Delta \mathbf{x}_k + \mathbf{u}_k^T E \mathbf{u}_k)), \tag{3.39}$$

in which, $k = 1 \sim K$ is the entire voltage adjusting period. D and E are positive definite matrices whose weighting elements depend on power system's penalties for voltage deviations at different buses and different DERs' operating costs.

Communication System

We assume that the sensors can report their measurements to the control center equipped with a base station. The center can then compute the corresponding actions and send them to the DERs. Due to the expensive cost of wired communications, we assume that wireless communication technologies are employed. To avoid the possible collisions, the reports from the sensors are conveyed in a polling manner, i.e., the control center schedules the transmission of the sensors. For simplicity, we assume that only one sensor can be scheduled in a time slot and it is straightforward to extend

to the case of multiple scheduled sensors. Moreover, we ignore the communication details like modulation and coding, as well as the transmission delay and packet drops, thus focusing on the sensor selection at multiple access layer.

Problem Formulation

Our focus is to find an effective algorithm for selecting the voltage sensors. To that end, three subproblems have to be studied towards solving our problem of timely regulating voltage with minimum operating cost: i) how to obtain the optimal system state estimation with partial observation from chosen sensors; ii) what control method should be applied based on the estimated system state; iii) which sensor to choose at each time slot and what is the selection criterion.

3.3.2 Optimal Sensor Selection Sequence

In this subsection, we present our algorithm of sensor selection for the voltage control by employing the framework of hybrid dynamical systems (Savkin and Evans, 2002). We will first introduce the theory of hybrid dynamical systems. Then, we will explain the algorithm of sensor selection.

Hybrid Dynamical System

Hybrid dynamical system (HDS) is a dynamical system which consists of both discrete and continuous dynamics. While continuous dynamics come from continuous subsystems of HDS, discrete dynamics are from the switching among these subsystems. Thus, the interaction between the discrete and continuous dynamics is the focus of HDS study.

One well known method of describing hybrid dynamical systems is using a set of ordinary differential equations with the following format:

$$\dot{\mathbf{x}}(t) = f_i(\mathbf{x}) \tag{3.40}$$

in which, $\mathbf{x}(t) \in \mathbb{R}^n$ is the system state; $i = 1, 2, \ldots, N$ is the switching system mode, and $f_1, f_2, \ldots, f_N$ are continuous functions determined by the corresponding subsystems in the HDS.

Most dynamical systems around us are hybrid dynamical systems. Especially with advancement of modern digital technology, numerous systems have been equipped with computer based controller with digital-sampling blocks, which inevitably changes these systems into HDS. One example of such HDS is robotic system. It uses camera or other sensors to monitor surrounding environment, and chooses the optimal operating mode accordingly. Being a practical analysis model for a variety of modern systems, HDS has received intensive studies in the literature (Labinaz et al., 1997; Van der Schaft and Schumacher, 1998; Seatzu et al., 2006).

Sensor Selection Algorithm

The power voltage control system under our study belongs to an important class of hybrid dynamical system called switching system, in which the continuous variables are the state variables of all continuous time subsystems and the discrete variables are the indices of subsystems. Specifically, in our power system, the continuous variables are the voltage states while the discrete variables are the indices of the chosen sensors.

We use feedback control to regulate the voltage. Since at any given time slot only one sensor can report, the power system is always under partial observations. To perform the feedback control, an estimation of overall voltage state has to be obtained first. The feedback control equation is given by

$$\mathbf{u}_k = -L_k \times \hat{\mathbf{x}}_k = -L_k \times g(\mathbf{y}_{ik}), \tag{3.41}$$

where $\mathbf{u}_k$ is the control input; L_k is the feedback control matrix; $\hat{\mathbf{x}}_k = g(\mathbf{y}_{ik})$ is the state estimation based on sensor i's measurement $\mathbf{y}_{ik}$ and previously received measurements; $g(\cdot)$ is the estimation function. From Eq. 3.37, Eq. 3.38 and Eq.

3.41, we have

$$\Delta \mathbf{x}_{k+1} = A \times \Delta \mathbf{x}_k - B \times L_k \times g(H_{ik} \Delta \mathbf{x}_k + \mathbf{v}_i) + \mathbf{w}. \tag{3.42}$$

With Eq. 3.42, we revisit the three subproblems (section 3.3.1) to be solved for achieving our ultimate goal of sensor selection in voltage control: i) function $g(\cdot)$ gives system state estimation; here we use Kalman filter; ii) feedback matrix L_k represents control method for which we adopt Linear Quadratic Regulator (LQR); iii) H_{ik} indicates the choice among different sensors. The following three subsections address these three individual problems.

The Kalman filter is a set of mathematical equations that provide an efficient recursive computational means to estimate the state of a process by minimizing the mean square error (Welch and Bishop, 1995). The state estimation process has two main interactive procedures: process update and measurement update whose mathematical expressions for our specific voltage control problem are Eq. 3.43 and Eq. 3.44 respectively, namely

$$\Delta \hat{\mathbf{x}}_k^- = A \Delta \hat{\mathbf{x}}_{k-1} + B \mathbf{u}_{k-1}, \tag{3.43}$$

and

$$\Delta \hat{\mathbf{x}}_k = \Delta \hat{\mathbf{x}}_k^- + K_k (\mathbf{y}_{ik} - H_{ik} \Delta \hat{\mathbf{x}}_k^-), \tag{3.44}$$

in which $\Delta \hat{\mathbf{x}}_k^-$ is the preliminary voltage deviation estimation based on the system state dynamics in Eq. 3.37 with control input applied; $\Delta \hat{\mathbf{x}}_k$ is the refined voltage deviation estimation after incorporating the correction provided by current measurement $\mathbf{y}_{ik}$; K_k is the Kalman gain matrix which can be calculated beforehand according to Eq. 3.45, namely

$$K_k = P_k^- H_{ik}^T (H_{ik} P_k^- H_{ik}^T + R_i)^{-1}, \tag{3.45}$$

where $P_k^- = AP_{k-1}A^T + Q$ is the predicted estimation covariance which is iteratively updated by $P_k = (I - K_k H_{ik})P_k^-$.

With the latest state estimation available from Kalman filtering, we use Linear Quadratic Regulator (LQR) (Sontag, 1998) to control the deviated voltage to the desired value. Being an effective control method in solving problem with linear system model and quadratic cost function, LQR is a good fit for voltage control. In fact, LQR, together with the Kalman filter, forms a Linear Quadratic Gaussian (LQG) problem. By LQG separation principle (Zhang and Hristu-Varsakelis, 2005), we are able to decouple the voltage state estimation from LQR control and calculate feedback matrix L_k in advance by Eq. 3.46, which avoids posing a substantial computation burden on voltage control center.

$$L_k = (E + B^T M_k B)^{-1} B^T M_k A, \tag{3.46}$$

in which A and B are system matrices in Eq. 3.37; E is the control input cost matrix in the cost function Eq. 3.39; M_k is found iteratively backwards in time by using the following equation:

$$M_{k-1} = D + A^T(M_k - M_k B(E + B^T M_k B)^{-1} B^T M_k)A, \tag{3.47}$$

with initial condition $M_K = D$, and D is the voltage deviation cost matrix in the cost function Eq. 3.39.

Now we face the key challenge of sensor selection. We denote the sensor querying sequence by $I = \{i_1, \ldots, i_k, \ldots, i_K\}$ for $k = 1 \sim K$, and $i_k \in \{1, \ldots, N\}$. Since the measurement of the current selected sensor, together with all previous sensor reports, determines the voltage control input which in turn determines the voltage states, the system cost function Eq. 3.39 becomes a function of I. Hence, our goal is to minimize

the overall cost by finding an optimal sensor querying sequence I, i.e.,

$$\underset{I}{min}\{J(I) = \mathbb{E}(\sum_{k=1}^{k=K}(\Delta\mathbf{x}_k^T D\Delta\mathbf{x}_k + \mathbf{u}_k^T E\mathbf{u}_k))\}. \tag{3.48}$$

According to the separation principle of LQG problem, its optimal control is totally based on the accurate state estimation. Therefore the optimal sensor querying sequence is the one that can achieve the minimum voltage deviation estimation error. The estimation error covariance is given by

$$P_k = \mathbb{E}[(\Delta\mathbf{x}_k - \Delta\hat{\mathbf{x}}_k)(\Delta\mathbf{x}_k - \Delta\hat{\mathbf{x}}_k)^T]. \tag{3.49}$$

From $k = 1$ to $k = K$, our goal consequently becomes finding the optimal (or near optimal) sensor querying sequence I which minimizes overall estimation error, which can be written as

$$\underset{I}{min}\{\sum_{k=1}^{k=K} trace(P_k)\}. \tag{3.50}$$

By employing Eq. 3.45 and the iterative updating process for Kalman gain K_k, the estimation error covariance evolves as follows:

$$P_k = [I - P_k^- H_{ik}^T(H_{ik}P_k^- H_{ik}^T + R_i)^{-1}H_{ik}]P_k^-, \tag{3.51}$$

$$P_k^- = AP_{k-1}A^T + Q. \tag{3.52}$$

The initial value P_0 can be an approximate one which reflects estimation accuracy of given $\hat{\mathbf{x}}_0$.

Starting from the selection of sensor at $k = 1$ until the voltage is adjusted to the desired value at $k = K$, we have N choices in each step. Thus, we can grow a tree structure for all possible sensor querying sequences. To find the optimal sequence, one straightforward but inefficient method is the *brute force strategy* which traverses all sequences and selects the one with the minimum estimation error as required by

Eq. 3.50. While it guarantees to find the optimal sequence, the *brute force strategy* suffers the exponential increase of computational cost.

We seek a trade-off between the sub-optimality sensor sequence and reasonable computation effort by adopting the *sliding window algorithm* (Chung et al., 2004). Given a window size d (steps), the algorithm proceeds as follows:

1. *Initialization*: start from root node with time $k = 1$.
2. *Traversal*:
   (a) Traverse all the possible paths in the tree for the next d levels from the present node;
   (b) Identify the optimal sensor sequence within the d-window;
   (c) Put the first sensor of the optimal sequence into the output sensor sequence.
3. *Sliding the window*:
   (a) If $k = K$ then quit, otherwise go to the next step;
   (b) Use the sensor which has just been selected as the new root;
   (c) Update time $k = k + 1$;
   (d) Repeat the traversal step.

In the algorithm, the window size d is an adjustable parameter determining the trade-off between the sequence optimality and computational cost (or the speed of decision making). Larger window size d results in a better sensor sequence but more computational intensity, and vice versa. As pointed out in Chung et al. (2004), when we slide the window, the first $d - 1$ steps' error covariances in the new window have already been calculated in the previous window and are available for immediate use. This merit of the algorithm considerably reduces computational demand.

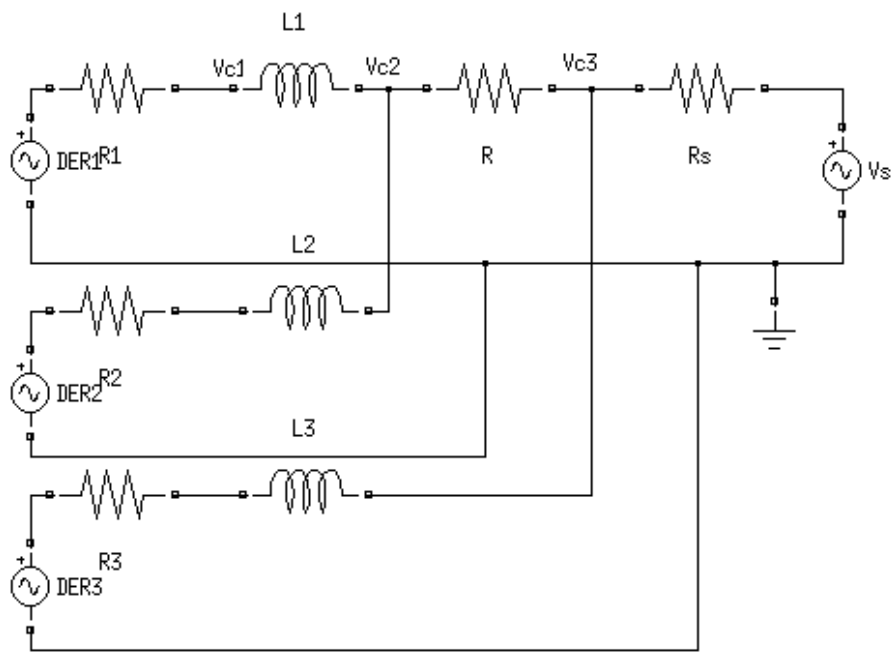


Figure 3.18: Example Power System Model

3.3.3 Example Application and Simulation Results

In this section, we use an example application of power voltage control (Fig. 3.18) to demonstrate the effectiveness of our proposed sensor selection strategy. In this example application, three voltage controlling/regulating DERs and three voltage monitoring sensors are installed in the power system. The system matrices in the power system equation 3.37 are give by

$$A = \begin{pmatrix} 1.03 & 0 & 0 \\ 0 & 1.02 & 0 \\ 0 & 0 & 1.05 \end{pmatrix}, \tag{3.53}$$

and

$$B = \begin{pmatrix} 0.6 & 0.1 & 0.2 \\ 0.1 & 0.7 & 0.15 \\ 0.2 & 0.15 & 0.8 \end{pmatrix}. \tag{3.54}$$

Elements in A being larger than 1 means that, without timely curbing voltage deviated from desired value, the state in the system will keep deteriorating. B shows that action of any single DER affects the state of the entire power system and DERs' control capabilities are coupled with one another, though each DER has its own primary control area. The covariance matrices of the system process noise w and the sensor measurement noise v are given by

$$Q = \begin{pmatrix} 0.05 & 0 & 0 \\ 0 & 0.02 & 0 \\ 0 & 0 & 0.01 \end{pmatrix}, \tag{3.55}$$

and

$$R = \begin{pmatrix} 0.1 & 0 & 0 \\ 0 & 0.2 & 0 \\ 0 & 0 & 2 \end{pmatrix}. \tag{3.56}$$

The noise power at sensor 3 is set to be much larger than those at the other two sensors, because we want to show that our sensor selection strategy is able to compensate the inferior condition by optimally allocating the shared communication channel. We also give voltage deviation penalty matrix D and control input (DER

operation) cost matrix E in Eq. 3.39, which are given by

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}, \text{and } E = \begin{pmatrix} 5 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 5 \end{pmatrix}. \tag{3.57}$$

We set the initial voltage deviation as $\Delta \mathbf{x}_0 = [30, 10, 20]^T$, and use two different methods to perform the sensor selection: one is using our proposed sensor selection strategy which returns the sensor querying sequence below; the other is to use the *round-robin* polling $\{2\ 3\ 1\ 2\ 3\ 1\ \ldots\}$, and this method is used as our baseline. The sliding window size d is set as $d = 5$.

Sensor querying sequence: $\{1\ 2\ 3\ 3\ 1\ 3\ 2\ 3\ 1\ 3\ 1\ 3\ 2\ 1\ 3\ 3\ 1\ 2\ 3\ 1\ 3\ 1\ 2\ 3\ 1\ 3\ 1\ 3\ 2\ 1\ 3\ 3\ 1\ 2\ 3\ 1\ 3\ 1\ 2\ 3\}$

Table 3.2 gives the communication channel allocation statistics for all three sensors. Sensor 3 receives the highest utilization percentage of the channel, i.e., 45% of channel accesses, while sensor 1 and sensor 2 receive 35% and 20% respectively. According to the noise covariance matrices Q and R, sensor 3 suffers the highest level of measurement noise which is overwhelming compared with the other two's; thus it is granted the highest utilization percentage. Sensor 1 has a lower measurement noise but higher process noise than sensor 2; consequently, sensor 1's combined noise effect gives it larger channel utilization percentage (35%) than what sensor 2 receives (20%).

Fig. 3.19 depicts the voltage state of the system during the control process using both methods. The lower figure uses the round-robin polling, and the upper

Table 3.2: Communication Channel Allocation

Sensor	S_1	S_2	S_3
Allocated Slots	14	8	18
Percentage	35%	20%	45%

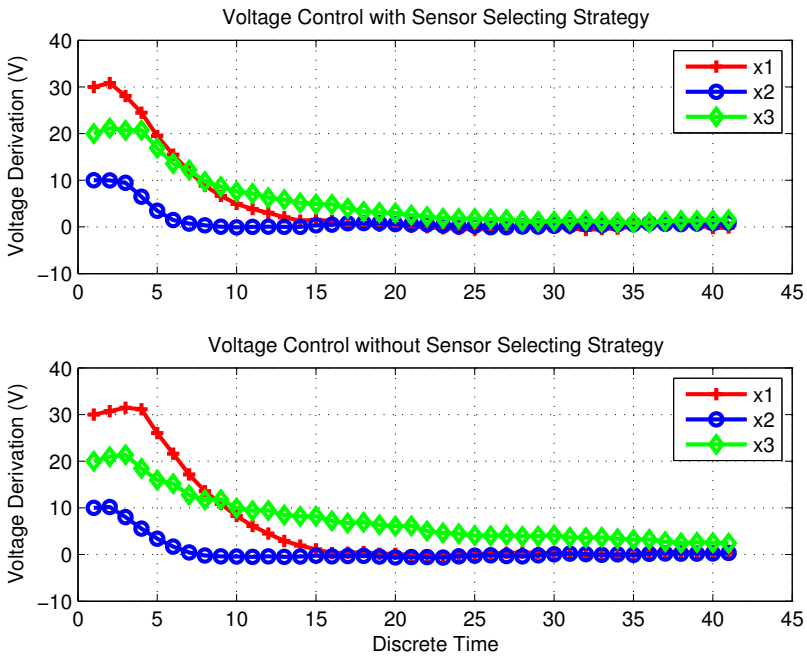


Figure 3.19: Voltage State Evolution. Controlled by sensor selection strategy, deviation of voltage is eliminated by the time $k = 30$; Without the strategy, deviation still exists after $k = 40$.

figure shows results using our proposed strategy. Both methods successfully pull the deviated voltage back to the desired value (deviation becomes zero), while our method forces the voltage to converge faster, in particular for voltage 3 (the green line).

Approaching the desired voltage $\mathbf{x}^*$ faster results in less time staying deviated from $\mathbf{x}^*$ and thus reduces the cost. Fig. 3.20 shows the costs for both voltage control methods. Our proposed strategy outperforms the baseline of round-robin algorithm by reducing the cost by approximately 40%. One of the key reasons that our sensor selection method is able to beat the round-robin method is that our method achieves smaller voltage state estimation error, as demonstrated in Fig. 3.21. The more accurate state estimation of our proposed algorithm helps the control center to timely use DERs to adjust voltage states and reduce the state fluctuation. In Fig. 3.22, the voltage state controlled by the round-robin method, namely the upper curve, has moderate fluctuation from time $k = 5$ to $k = 25$; while the voltage state controlled by

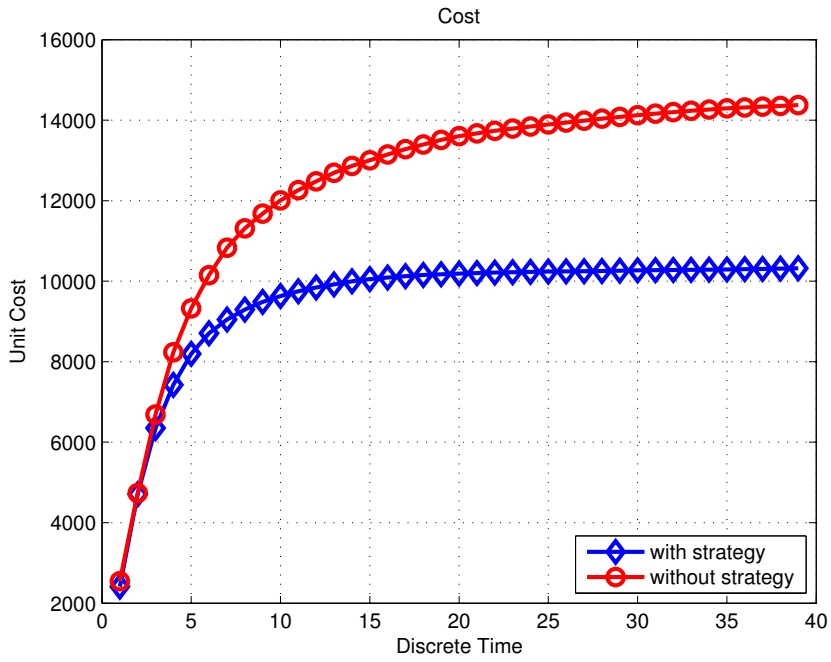


Figure 3.20: Cost Comparison. The method with sensor selection strategy reduces cost by approximately 40% compared with the method using *round-robin* sensor polling

our sensor selection strategy, the lower curve, shows smooth transition. Furthermore, the voltage state with a smoother transition like the one controlled by our sensor selection strategy is much more desired.

3.3.4 Conclusion

In this section, we study prioritized multiple access in CPS. We have treated the power system with sensors and shared communication channel as a hybrid dynamical system, which switches its mode by selecting different sensors. The approach to obtain the optimal sensor querying sequence has been analyzed by minimizing overall system cost. Both LQR control and Kalman filter have been applied for the control. A sub-optimal but computational efficient sliding window algorithm has been applied

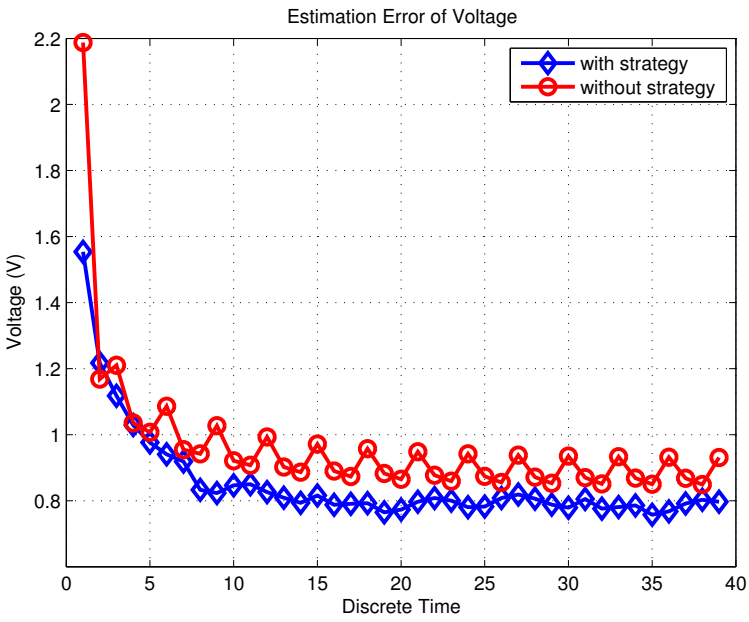


Figure 3.21: State Estimation Error.

and has been demonstrated to achieve a 40% performance gain compared with the simple round-robin sensor polling baseline.

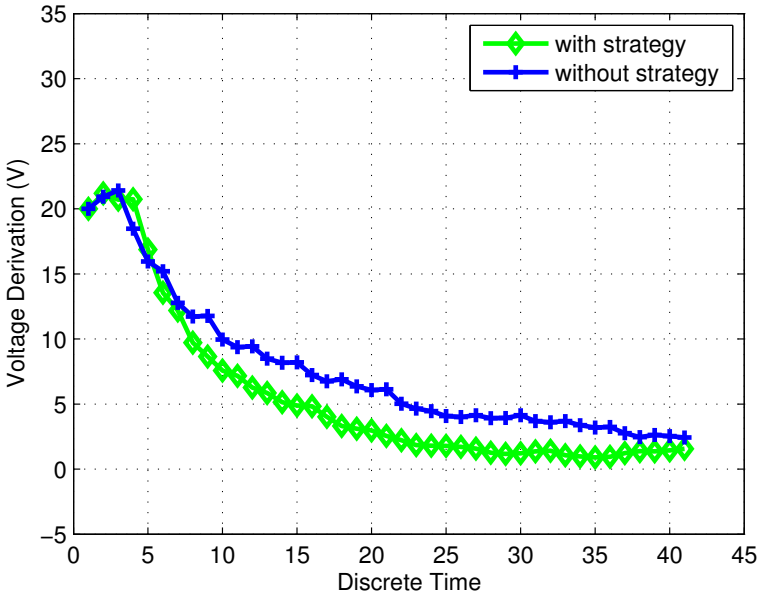


Figure 3.22: Voltage State Transition. *round-robin* sensor polling results in moderate state fluctuation (the upper curve); voltage state controlled by sensor selection strategy has smoother transition (the lower curve).

Chapter 4

Core Network in Cyber-Physical System

In chapter 3, we discussed reliable and selective multiple access in CPS. The *base station* to which multiple sensors are connected is actually one of many *key nodes* in CPS' *core network*. The core network in CPS is illustrated by Fig. 4.1, in which sensors/actuators (represented by stars) are associated with key nodes, which in turn form the core network. Global controller collects and disseminates information through this core network; local controllers reside in key nodes in its neighborhood.

In this chapter, we study how to manage core network in CPS to provide reliable and timely service. In the first section of the chapter, we propose to increase network reliability and predictability by creating backup paths. Service interruption at certain group of key nodes is anticipated, and backup paths are created accordingly through integer programming. In the second section, we address the problem stem from network dynamics by designing an online multipath routing algorithm that is able to adaptively update backup paths.

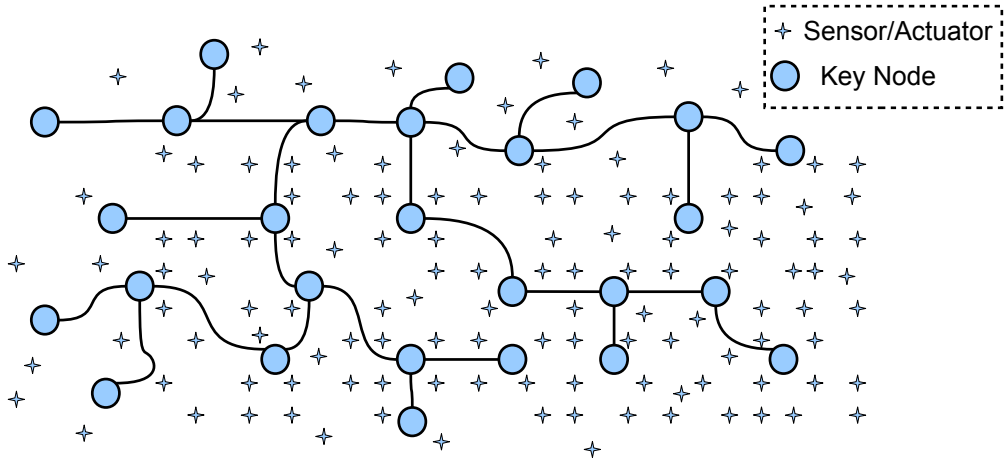


Figure 4.1: Core Network in CPS

4.1 Create Backup Path in Core Network

High reliability is essential for CPS. We define two types of users in CPS: *Primary User* (PU) and *Secondary Users* (SU), with PU having higher priority. When a set of nodes in CPS realize that the data from a user A (sensor or controller) is more important than the data from user B, the set of nodes would grant higher access priority to user A, and deny service for user B by stop serving user B. In a situation like this, user A is PU and user B is SU. SU suffers from interruption on its traffic flow when PU appears, which may cause severe damages to CPS.

It is well known that, in the area of reliability engineering, an effective approach to improve the reliability of a complex system is to prepare backup elements. For example, preparing backup parts for each functional block can significantly improve the overall reliability of a rocket. In this chapter, we study *preparing backup paths for improving the reliability of traffic flows*. To that end, we predetermine one or more backup paths for each traffic flow. When the current path, called *working path*, is interrupted by primary users, the source node can switch to a backup path such that

the traffic flow can be resumed at the minimum performance loss. There also have been many studies on survivable networks, which focus on improving the reliability of networks by preparing multiple paths for each traffic flow. For example, a redundancy tree can be designed for a graph, thus providing multiple redundant paths (Médard et al., 1999). In Li et al. (2008), the self-healing algorithm is studied to improve the survivability. Plenty of algorithms for designing survivable networks are summarized in Stoer (1991).

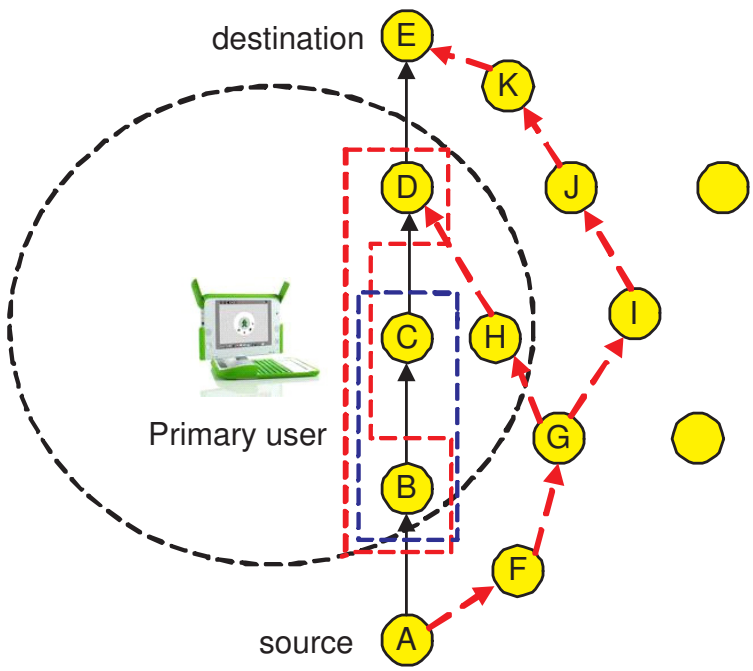


Figure 4.2: An Illustration of Backup Path.

An illustrative example is given in Fig. 4.2 to explain how the backup scheme works. It is possible that nodes B and D or nodes B and C are simultaneously interrupted by the primary user. Suppose that $A \to B \to C \to D \to E$ is the working path. Then, we set path $A \to F \to G \to H \to D$ as the backup path for protecting the working path, when secondary users B and C along the working path are disrupted. If secondary users B and D are interrupted, the backup path $A \to F \to G \to I \to J \to K \to E$ will be activated.

The following two challenges must be addressed for the backup path scheme:

- How to design the backup path?
- When to switch to the backup path?

For the first challenge, we formulate the problem of designing backup paths as an integer programming. We formulate the second problem as a Bayesian decision problem by identifying the cost and *a posteriori* probabilities that the working path is interrupted. The switching rule is implemented and optimized in a USRP GNU Radio node based testbed. The hardware experiment shows that the system cost, defined as a weighted sum of throughput loss and average packet delay, is reduced by around 50% in a typical setup, compared with the scenario of no backup paths.

4.1.1 Backup Path Design

In this section, we present an integer programming formulation for determining the backup path. First, we introduce the concept of *shared risk node group* (SRNG), a key concept facilitating the creation of backup path, followed by the detailed description of the integer programming. Finally, we provide the performance evaluation of the proposed algorithm.

Shared Risk Node Group

A *shared risk node group* (SRNG) is a group of nodes which may be interrupted by primary users (PU) at the same time. An illustrative example is given in Fig. 4.3, where nodes 1, 2 and 3, under the influence of primary user A, and nodes 2, 3, 4, 5 and 6, under the influence of primary user B, are obviously two SRNGs. However, there exists the third SRNG which includes all the nodes since it is possible that both primary users A and B emerge at the same time. Hence, the set of SRNGs in Fig. 4.3 is $\{\{1,2,3\},\{2,3,3,5,6\},\{1,2,3,4,5,6\}\}$. SRNGs can be obtained by

neighboring nodes exchanging and merging the operation history of the network in the neighborhood.

Integer Programming Formulation

Suppose that there are K working paths in a CPS, which have been predetermined by certain routing algorithms. We plan to build a backup path for each SRNG associated with a traffic flow such that the data can be switched to the backup path once the nodes in the SRNG are interrupted by any primary user*. This task is formulated as an integer programming problem, whose essential task is to determine whether a given link is used by any backup path; if yes, which SRNG the link protects. All decisions should be made towards the objective of *minimizing overall delay cost in the entire network with various constraints.*

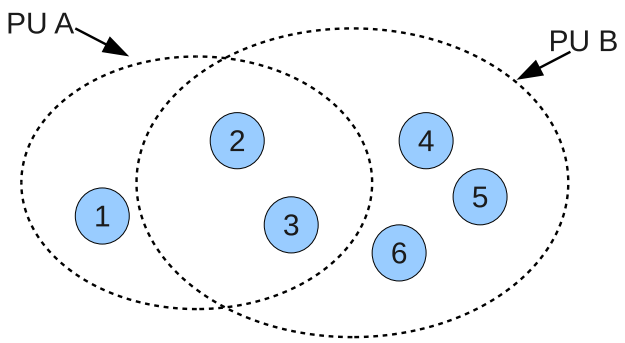


Figure 4.3: An Illustration of SRNG.

Notations

Table 4.1 lists notations used in this section.

*This is an ideal case. In practice, there could exist many SRNG's and it is difficult to find one backup path for every SRNG. Then, we need to study the trade-off between the reliability and the complexity

Table 4.1: Notations.

G	the set of all SRNGs.
N	the set of nodes in the network.
WP_k	the kth working path.
K	total number of working paths.
c_k	unit delay cost of the kth working path.
G_k	the set of SRNGs that WP_k traverses.
BP_g^k	backup path that protects WP_k interrupted by SRNG g.
$BP_{G_k}^k$	set of all backup paths that protect WP_k.
ρ_g	the interrupting probability of SRNG g.
$R_{BP_g^k}^{mn}$	the transmission rate of BP_g^k at link (m,n).
C^{mn}	the link capacity of link (m,n).
$F(n)$	the set of links from node n.
$T(n)$	the set of links to node n.

Variables

The primary variable is $S_{BP_g^k}^{mn}$ which indicates whether existing link between node m and node n, (m,n), is used by backup path BP_g^k or not. All $S_{BP_g^k}^{mn}$ form a variable set $\mathbf{V}$.

$$S_{BP_g^k}^{mn} = \begin{cases} 1, & (m,n) \in BP_g^k \\ 0, & (m,n) \notin BP_g^k \end{cases} . \tag{4.1}$$

Two auxiliary variables are used to compute the numbers of outgoing links and incoming links respectively, which are given by

$$S_{BP_g^k}^{F(n)} = \sum_{(m,n)\in F(n)} S_{BP_g^k}^{mn}, \tag{4.2}$$

and

$$S_{BP_g^k}^{T(n)} = \sum_{(m,n)\in T(n)} S_{BP_g^k}^{mn}. \tag{4.3}$$

Objective

We assume that each node causes one unit delay to the data stream on backup path. Thus, the delay of BP_g^k at node n is given by

$$D^n_{BP_g^k} = \begin{cases} 1, & n \in \ BP_g^k \\ 0, & n \notin \ BP_g^k \end{cases} . \tag{4.4}$$

According to definition of $S^{mn}_{BP_g^k}$, $D^n_{BP_g^k}$ can also be written as

$$D^n_{BP_g^k} = S^{mn}_{BP_g^k}, \quad m \in BP_g^k. \tag{4.5}$$

The delay of $BP^k_{G_k}$ at node n is given by

$$D^n_{BP^k_{G_k}} = \sum_{g \in G_k} (\rho_g \times D^n_{BP_g^k}). \tag{4.6}$$

Altogether, the total cost of all backup path's delay at node n is given by

$$C^n = \sum_{k=1}^{K} \left(c_k \times D^n_{BP^k_{G_k}} \right). \tag{4.7}$$

Finally, the ultimate objective is to minimize the delay cost of all backup paths in the entire network, which is given by

$$\min_{\mathbf{V}} \sum_{n \notin WP} C^n. \tag{4.8}$$

Constraints

We assume that any node at any time can support only one backup path. Therefore, for any node, all backup paths that traverse it should protect different SRNG's. This

constraint can be expressed as

$$\sum_{k=1}^{K} S_{BP_g^k}^{F(n)} \leq 1, \quad \forall n \in N, g \in G, \tag{4.9}$$

and

$$\sum_{k=1}^{K} S_{BP_g^k}^{T(n)} \leq 1, \quad \forall n \in N, g \in G. \tag{4.10}$$

In addition, we apply the following constraints:

- *Continuity*: for $k = 1, ..., K, \forall n \in N, g \in G$,

$$S_{BP_g^k}^{F(n)} - S_{BP_g^k}^{T(n)} = \begin{cases} 1, & \text{if } BP_g^k \text{ begins at node n} \\ 0, & \text{if } BP_g^k \text{ traverses node n} \\ -1, & \text{if } BP_g^k \text{ ends at node n} \end{cases}. \tag{4.11}$$

- *Link Capacity*: The maximum transmission rate should be less than or equal to the capacity.

$$\max_{g \in G} \left(R_{BP_g^k}^{mn} \times S_{BP_g^k}^{mn} \right) \leq C^{mn}, \quad \forall m, n \in N. \tag{4.12}$$

- *Relationship between Working Path and Backup Path*: A backup path should have equal numbers of outgoing and incoming links with the working path it protects to make sure that the backup path can send data back to the working path or the destination:

$$\sum_{n \in WP_k} S_{BP_g^k}^{F(n)} - \sum_{n \in WP_k} S_{BP_g^k}^{T(n)} = 0, \quad g \in G_k, k = 1, ..., K. \tag{4.13}$$

- *Constraint on BP_g^k*: Any backup path should not use node that is in the SRNG it protects, which is expressed as

$$S_{BP_g^k}^{mn} = 0, \text{ if } m \in g \text{ or } n \in g. \tag{4.14}$$

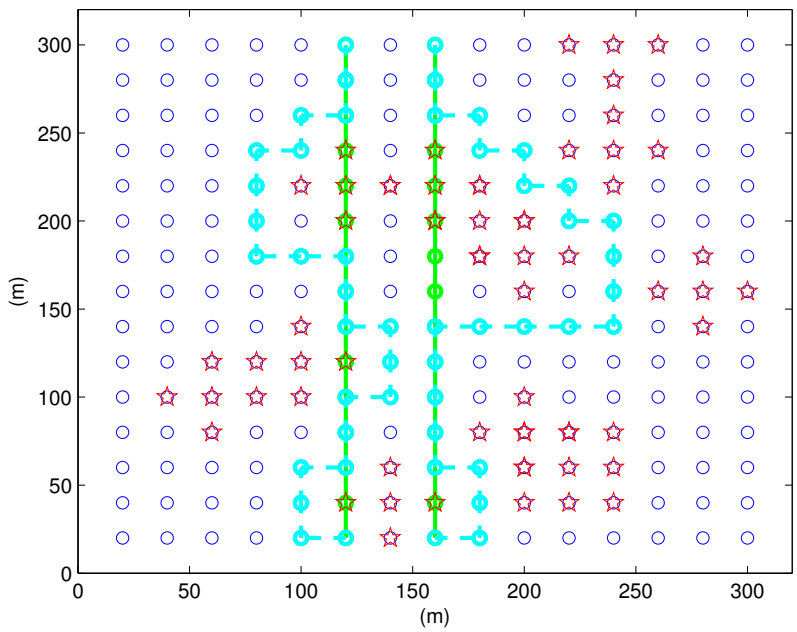


Figure 4.4: Example of Backup Path.

Performance Evaluation

We evaluate the cost of the created backup paths by solving the proposed integer programming problem in a simple 225-node network with a 15×15 grid topology. The integer programming problem is solved by CPLEX 11.2 solver of AMPL (AMPL, 2012). We assume that there are two data flows in the network. The distance between two adjacent nodes (not diagonal) is D and only adjacent nodes can communicate with each other. Primary users are randomly distributed in the network with a covering diameter $3D$ and interrupting probability p. The ratio of capacities of links in working paths and backup paths is $R > 1$, which implies that, when not interrupted, the working path is always the preferred transmission path. We assign a unit cost to each link along the backup path and $\frac{1}{R}$ to each working path links. The total cost of the backup path is a function of its length, while the total cost of working path is a function of both p and the number of corresponding SRNG's. Fig. 4.4 shows

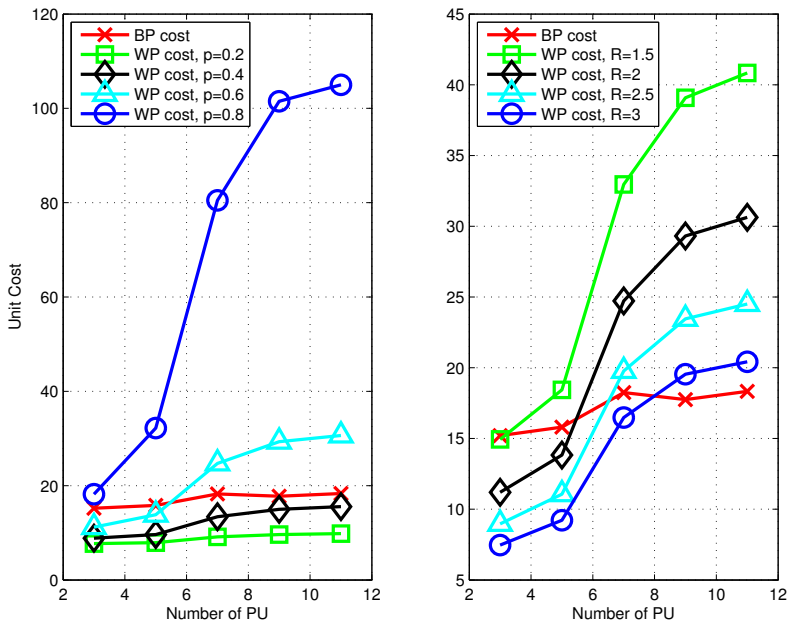


Figure 4.5: Backup Path Versus Working Path.

the result by solving integer programming problem under configuration mentioned above. In the figure, red stars represent SRNG's; blue circles are nodes unaffected by primary users; light blue dash lines denote backup paths; green solid lines denote the working paths, part of which could be covered by backup path. We first vary p from 0.2 to 0.8 and the number of primary users from 3 to 11. The performance of both backup path and working path is given in the left figure of Fig. 4.5. With an increased chance of interruption, the cost of the working paths increases significantly. Compared with the cost at the working path, the cost of backup paths only sees a moderate increase of less than 40% due to its inherent nature of protection. In the right figure of Fig. 4.5, we also assess the impact of the ratio of link capacities R. The conclusion is quite straightforward: the higher the capacity ratio is, the less the cost is, i.e., a better working path has less intention to switch to backup path.

As shown in above performance evaluation, the cost of working path can be worse than that of backup path if a working path is interrupted by a primary user and the data flow is not switched to the backup path. This implies a pressing need to study the rule of switching to backup path, which is the focus of the next section.

4.1.2 Switching Policy

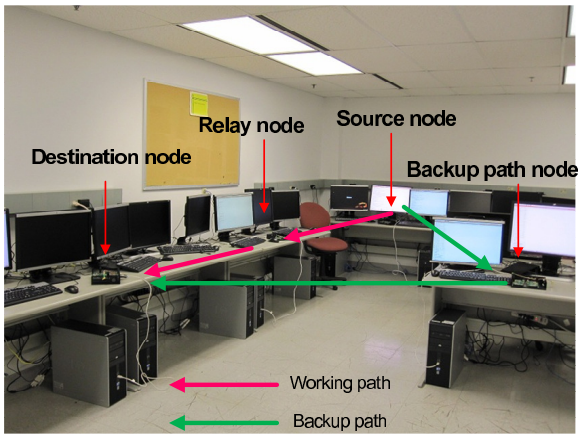
In this section, we study the switching policy given predetermined working path and backup path, i.e., when to switch to the backup path if the working path is malfunctioning, by using a simple USRP node based testbed. We first introduce the configuration of the testbed network. Then, we formulate the switching policy as a Bayesian decision problem, thus obtaining the optimal strategy. Finally, we provide the performance metrics obtained from the experiment in the testbed network. In the following, we briefly introduce the configurations of the testbed, including the network topology, hardware, channel assignment and MAC layer protocol.

Topology

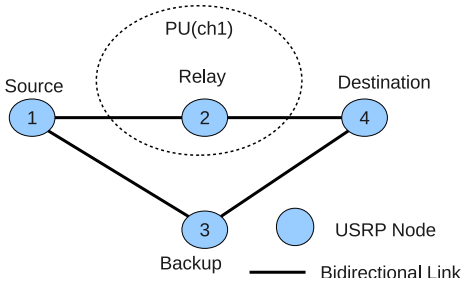
Built in a 10m×4m lab, the testbed consists of four GNU Radio USRP nodes, whose picture and topology are shown in Fig. 4.6a and Fig. 4.6b. The primary user's activity is generated by another dedicated USRP node (not shown in the picture). The testbed has one source node, one relay node (for the working path) and one backup relay node (for the backup path) and one destination node, labeled by nodes 1, 2, 3 and 4, respectively. Therefore, the source has two possible paths for transmitting to the destination. Only the relay node (2) is affected by the primary user node because they use the same channel.

Hardware

Each USRP node is connected to a host computer through a USB cable (Ettus Research LLC, 2012). In each node, the motherboard is mounted by a RFX400



(a) A picture of the testbed network



(b) Topology of the testbed network

Figure 4.6: Testbed

daughterboard which covers frequencies from 400MHz to 500MHz. Each node has independent Tx and Rx paths but shares the same antenna. Therefore, they work in the half-duplex mode and cannot receive any data when transmitting. The transmitting power of each USRP node is controlled by setting parameter *tx-amplitude* to 0.01. Carrier sense threshold is 50dB. Each USRP node uses DBPSK modulation/demodulation with bitrate of 125kb/s. It takes around 20ms for a USRP node to switch channel. Note that these USRP nodes are not time synchronized.

Channel Assignment

We use a fixed channel assignment scheme, i.e., each node has its own dedicated receiving channel. For example, when node 1 wants to send packets to node 2, it tunes its transmitting channel to the receiving channel of node 2. There are totally four channels used by the testbed, ranging from frequency 428M to 431M with 1M interval. We assign the four channels to the four nodes as their receiving channels, i.e., node i uses channel i as its receiving channel. The primary user node uses channels 1 and 4, thus interfering the transmission of the relay node 2. Note that the primary user only affects the transmission, not the receiving, of each node. No common control channel is specified.

Transmission Procedure

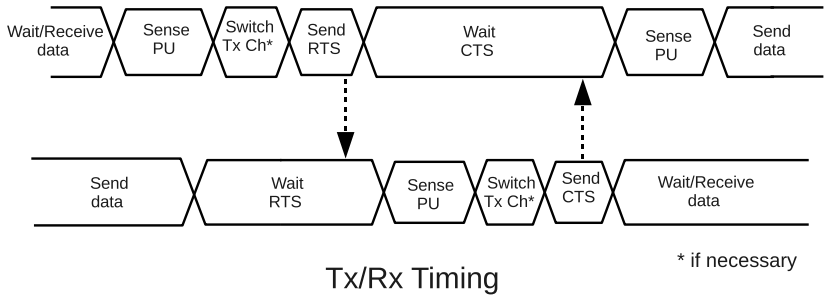


Figure 4.7: An Illustration of The Timing for Transmission.

The mechanism of RTS/CTS (Request To Send/Clear To Send) is used for coordination between nodes. When a node wants to transmit, it first senses primary user over the receiving channel of its receiver, which costs 40ms. If no primary user is detected, it sends an RTS in the receiving channel of the receiver and then waits for the CTS in its own receiving channel. Upon receiving a CTS signal from the receiver, it begins to transmit. The procedure of RTS/CTS costs around 150ms and timing structure is shown in Fig. 4.7.

Decision Making for Path Switching

At the first sight, the decision making for path switching looks to be straightforward: the source node can simply switch to the backup path when the working path is damaged by the primary user. However, the challenge is *how can the source node know that the working path is damaged by the primary user?* Two facts make the source node unable to perfectly determine the working path status. First, an emerging primary user prevents relay node from responding to source node's RTS; second, relay node is unable to hear the RTS from the source while it is transmitting.

Therefore, the source node should distinguish the case of an emerging primary user and the case of a transmitting relay node. For the former case, the source node should

switch to the backup path while it should stay in the working path and continue to contact the relay node in the latter situation. Due to the probabilistic nature of this decision problem, we adopt the Bayesian framework to solve this problem by minimizing the Bayesian risk. To that end, we first define the costs of different scenarios, then compute the *a posteriori* probabilities and finally obtain the decision rule.

Cost

For the Bayesian decision framework, we need to define the costs for different scenarios. There are totally three scenarios in the network, namely transmitting along the working path with an active primary user (S1), transmitting over the backup path (S2) and transmitting over the working path without primary user (S3). We denote by C_1, C_2 and C_3 their costs, respectively, which satisfy the relationship $C1 > C2 > C3$. For defining the costs, we employ two metrics: *end-to-end delay* and *throughput loss*. End-to-end delay is the average delays normalized by that of S1; throughput loss is the normalized gap between the throughput of the corresponding scheme and that of scheme S3. We define the cost of each scenario as a weighted sum of the end-to-end delay and the throughput loss with both weighting factors being 0.5

A Posteriori Probability

The second element in the Bayesian decision is the *a posteriori* probability for the primary user presence given the number of RTS's without responses from the relay node, denoted by n. Applying the Bayesian rule, we have

$$\begin{aligned} P(\text{PU}|n) &= \frac{P(\text{PU}, n)}{P(n)} \\ &= \frac{P(n|\text{PU})P(\text{PU})}{P(n|\text{PU})P(\text{PU}) + P(n|\text{no PU})P(\text{no PU})}. \end{aligned} \tag{4.15}$$

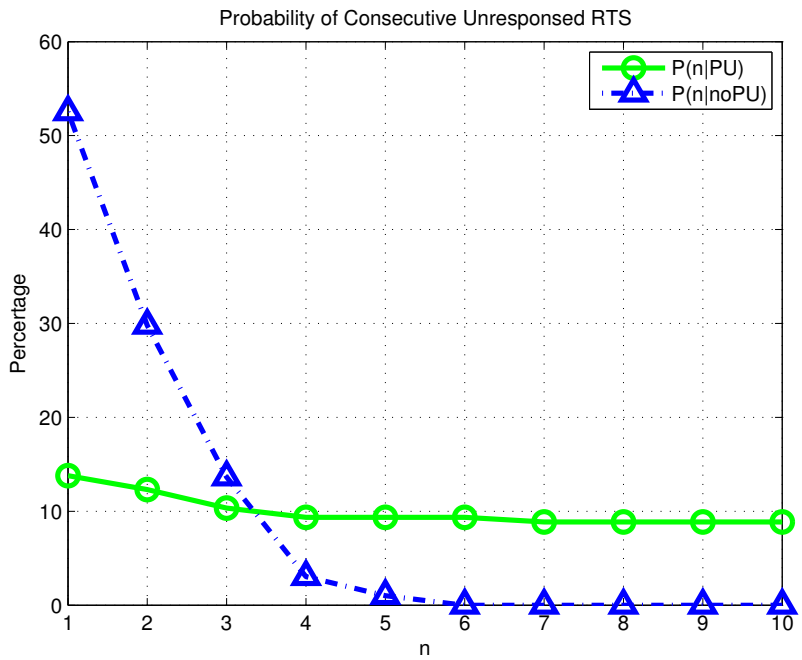


Figure 4.8: Conditional Probabilities of The Number of RTS's Without Responses in Different Scenarios.

We count the number of times when n RTS's are not responded in scenarios S1 and S3, respectively, which were measured in the testbed (the numbers are shown in Table 4.2). Then, we calculate the conditional probabilities $P(n|\text{PU})$ and $P(n|\text{no PU})$ correspondingly. The obtained conditional probabilities are shown in Fig. 4.8. Shown by curve $P(n|\text{no PU})$, when there is no primary user, there are only 1 or 2 consecutive RTS's not responded for most of the time. It is rare to find 5 or more consecutive RTS's not responded by the relay node. When there is primary user, the probability that 3 or more consecutive RTS's not responded increases significantly, as shown by curve $P(n|\text{PU})$.

Table 4.2: The Number of Consecutive Unresponded RTS's.

	The Number of Unresponded RTS's (n)								
	1	2	3	4	5	6	7	8	9
PU	28	25	21	19	19	19	18	18	18
no PU	104	59	27	6	2	0	0	0	0

Table 4.3: Costs of Different Decisions and States.

	Working Path	Backup Path
PU	C_1	C_2
no PU	C_3	C_2

Decision Rule

Table 4.3 shows the costs when different actions, staying in the working path or switching to the backup path, are taken in different primary user states. Note that, once switched to the backup path, the cost is irrelevant to the primary user state.

When the number of RTS's without responses at the source node is n, the expected cost of staying in the working path is given by

$$E[C|n] = P(\text{PU}|n)C_1 + (1 - P(\text{PU}|n))C_3. \tag{4.16}$$

If switching to the backup path, the expected cost is C_2.

To minimize the Bayesian risk, the decision rule is given by

$$\text{decision} = \begin{cases} \text{backup path} & \text{if } E[C|n] > C_2 \\ \text{working path} & \text{if } E[C|n] \leq C_2 \end{cases} \tag{4.17}$$

Note that we choose the working path when there is a tie.

Switch Back to Working Path

After switching to the backup path, the source node will frequently check the status of the working path (once per 10 seconds in the testbed). Once receiving a CTS response from the relay node, the traffic flow will be switched back to the working path.

Performance Evaluation

We let the source node generate a bursty data stream, with the interval of 1s. Each time 10 packets of size 1kb are placed in the source node's sending queue, thus achieving a source rate of 10kb/s. The statistics are obtained from 10 experiments of the testbed, each lasting 500s. We denote by S4 for the scheme of dynamic switching between the two paths.

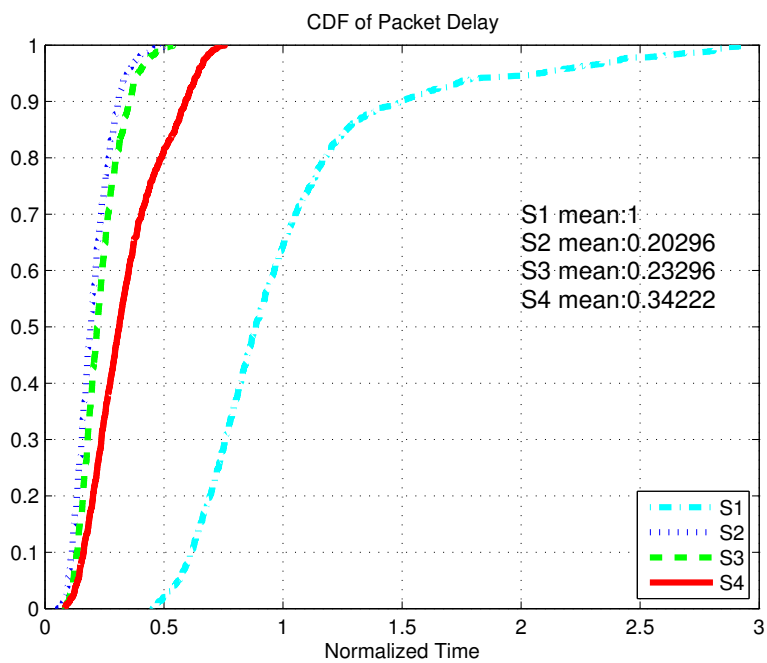


Figure 4.9: CDF Curves of Expected Packet Delay (Normalized).

Fig. 4.9 shows the CDF curves of packet delay, normalized by S1's average delay. The scheme of dynamic switching, S4, achieves an expected delay of 0.34,

i.e., 66% less delay than S1. Therefore, the dynamic switching scheme attains a much smaller packet delay compared with the scheme of always staying on the working path. Meanwhile, the expected delay of S4 is slightly larger than S3, the scheme of using working path without primary user emergence. Note that the expected delay is measured for only the packets successfully arriving at the destination. The expected delay of S2, always using backup path, is even smaller than that of S3. The reason is, in our experiment, inferior backup path carries only half of the working path's data rate load; thus reducing the chance of congestion on the backup path.

The overall performance metrics, the weighted sums of the throughput loss and expected delay, of different schemes are plotted in Fig. 4.10. We observe that the ideal case, S3, achieves the best performance since there is no primary user in this scenario and the working path has a better quality than the backup path. Compared with the practical cases, S1 and S2, the dynamic switching strategy S4 achieves relative performance gains of 51.2% and 23.4% respectively.

4.1.3 Conclusion

In this section, we have studied the backup path mechanism in CPS. Backup paths improve the reliability of the core network, which is subject to the interruptions from primary users. An integer programming problem has been formulated to obtain the optimal backup paths. Once the backup path is fixed, a switching algorithm, which determines when to switch to the backup path, has been proposed based on the Bayesian decision framework. The algorithm has been implemented and optimized over a USRP GNU Radio testbed which consists of four secondary users and one primary user. The experiments using the testbed has shown that the performance of the data transmission in CPS can be significantly improved by this backup path mechanism.

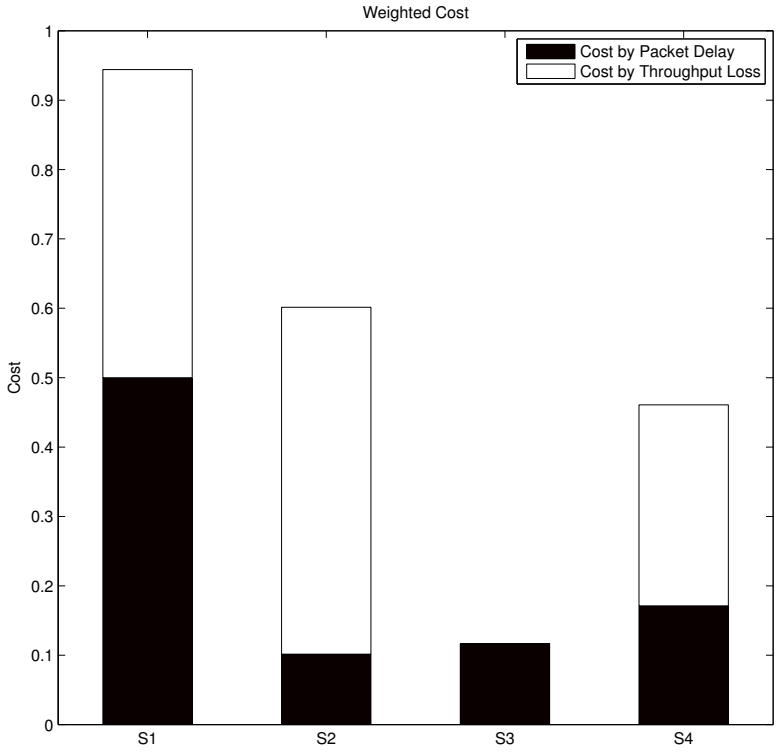


Figure 4.10: Comparison of Performances for The Four Scenarios.

4.2 Online Multipath Routing

In previous section, we discussed creating backup path in CPS core network by solving an integer programming problem, in which global information of the system, such as SRNGs, has to be available. Thus, the integer programming approach is suitable for networks that have low dynamics. In this section we study an online multipath routing approach that is derived from Ant Colony Optimization (ACO), and adapted for networks that contain SRNG.

ACO is a biologically inspired stochastic optimization algorithm that iteratively and incrementally searches for good (but not necessarily globally optimal) solutions (Chen et al., 2006). When an ant colony is trying to trace out the shortest path from

its nest to a food source, each ant as an individual will do two simple things: one, it leaves pheromone along the route it has just past; second, it tends to follow the path that has higher pheromone accumulation. Through this indirect communication mediated by pheromone secretion, ants are able to interact with one another and form a mechanism of *positive feedback*, which implies that the shorter a path is, the more likely ants are going to follow it. Another important feature in ant path exploration is the evaporation of pheromone. The evaporation prevents pheromone accumulating to a dominant level along a few paths, which would handicap path exploration process. Given the simple action of an ant in ACO, it is easy to implement ACO in a distributed manner. The decision of an ant is completely based on local information, and no global information is needed.

4.2.1 Description of the Algorithm

In a wireless communication system for CPS, a controller subscribes information from multiple sensors in the network. As discussed in the previous section, at network layer, we strive to achieve reliable and timely data delivery from sensors to controllers. With service interruption at nodes anticipated, we create multiple path to circumvent potential zone of service interruption. Compared with conventional multipath routing protocols (Mohammed Tariquea et al., 2009), our online multipath routing protocol for wireless communication in CPS has two major features. First, the multipath created by our approach specifically addresses the problem of service interruption caused by SRNG; second, QoS requirements in CPS' wireless communication, such as reliability and real-time, are incorporated into our ACO based design. We will show only one source one destination case in the following. Multiple sources and one destination case can be easily handled by merging routes from different sources then forwarding along the routes that have already explored.

4.2.2 Forward Route Exploration

Routes from data source to destination are maintained by the source periodically sending out route maintaining packet to the destination that has subscribed data service from the source. The maintaining packet performs a function similar to that of an ant trying to trace out the route from its nest to food source.

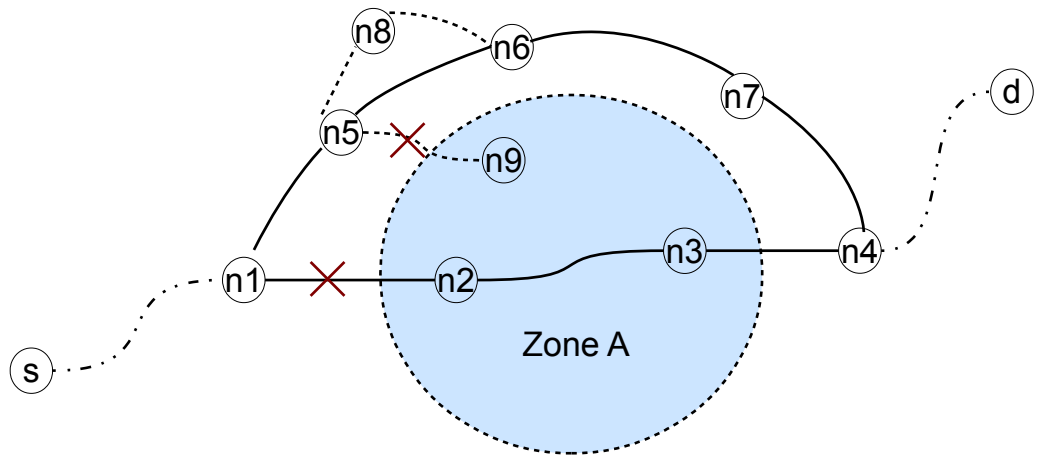


Figure 4.11: Route Exploration

Take Fig. 4.11 as an example, starting from the source, s, the maintaining packet records the nodes that it has traversed into a *tabu_list*. *next* node is chosen opportunistically from nodes that are in the neighborhood of *current* node. The selecting probability that is assigned to each neighboring node is calculated according the amount of pheromone accumulated on the corresponding link between *current* node and the neighboring node. Higher level of pheromone accumulation is granted larger chance of being selected. When service in a zone is interrupted, as illustrated in Fig. 4.11's "Zone A", maintaining packet will notice that links to the interrupted zone, such as $n_1 - n_2$ and $n_5 - n_9$, are down. Those tabbed unresponsive nodes are marked by a *black_list*, which will be utilized at pheromone updating stage. Sudden appearance of interrupted zone could make immediate detour an inferior one before

it is gradually improved. Thus, the detour could take $n_5 - n_8 - n_6$ before it go through $n_5 - n_6$, the better one, directly. Forward route exploration procedures are summarized by algorithm 4.

Algorithm 4 Forward Route Exploration

```
next = null
tabu_list = {source}
black_list = {}
while next ≠ dest do
  current = tabu_list(end)
  if N_current ⊂ tabu_list then
    Reset
  end if
  compute current's neighboring nodes' selecting probability.
  select next based on selecting probability.
  if current − next link broken then
    black_list ← next
    Reselect
  end if
  tabu_list ← next
end while
```

4.2.3 Backward Feedback

When a route maintaining packet arrives at its destination, it submits the tabu_list indicating the route it has travelled. In route maintenance and exploration, proper route reinforcement is critical. Whether or not, or how much to reinforce a route submitted by a maintaining packet is determined by the value of the route. Shorter distance and smaller delay result in higher reward through pheromone updating. On the other hand, there are two sources that decrease pheromone. One is pheromone evaporation, which applies to all links; the other one is penalty to links connected to *black nodes*. When tracing backwards along the tabu list, any link between a node in the tabu list and a node in the black node list will be penalized by reducing its pheromone level. Algorithm 5 describes backward feedback through pheromone updating.

Algorithm 5 Backward Feedback

```
Initialize path length heap to inf (size n)
//Pheromone evaporation
Ph = Ph × p   (0 < p < 1)
if Path_Length < heap_max then
   update heap
   Reward = Q/Path_Lenghth
else
   Reward = 0
end if
for i in tabu_list do
   Ph_{i,i+1} = Ph_{i,i+1} + Reward
   //N_i is the set of neighboring nodes of node i
   for j in N_i do
      if j in black_list then
         //Penalty for black nodes
         Ph_{i,j} = Ph_{i,j} × q   (0 < q < 1)
      end if
   end for
end for
```

Fig. 4.12 shows the performance of ACO based online routing. From source (cross) to destination (star), after iterative update and improvement, the light blue route becomes a stable one. Then comes the interruption whose affected nodes are marked as red circles. A detour has to be immediately established. The detour will be gradually improved and becomes stable, as shown in Fig. 4.13. X-axis of the figure is the number of maintaining packet, and y-axis is the hop number of a route. Before interruption comes, after about 80 packets, the original route has improved itself to around 15 hops and stabilized. When interruption comes at around 100th packet, the initial detour's distance is long before it finally resettles itself (the green route in Fig. 4.12). Figures 4.12 and 4.13 together show the effectiveness of our online routing method's ability to handle interruption and re-establish backup routes with competitive distance.

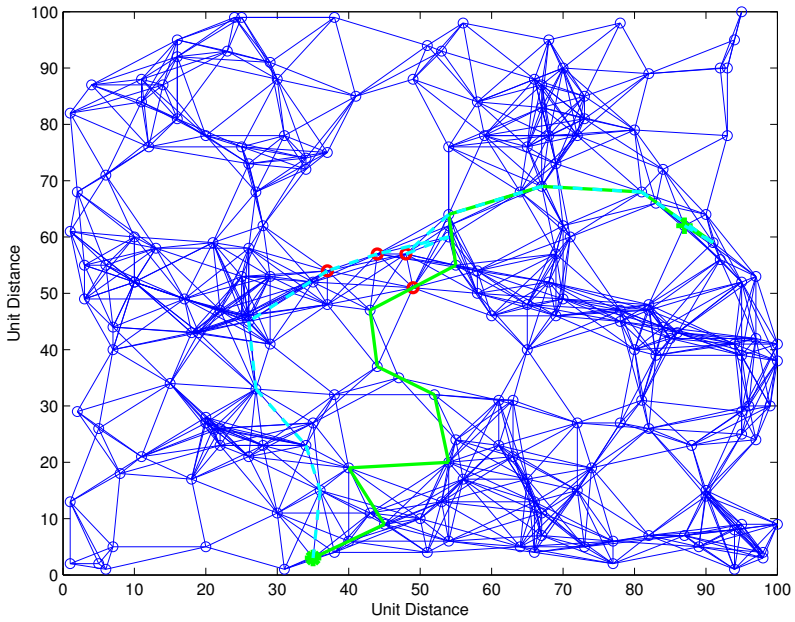


Figure 4.12: Original Route and Detour

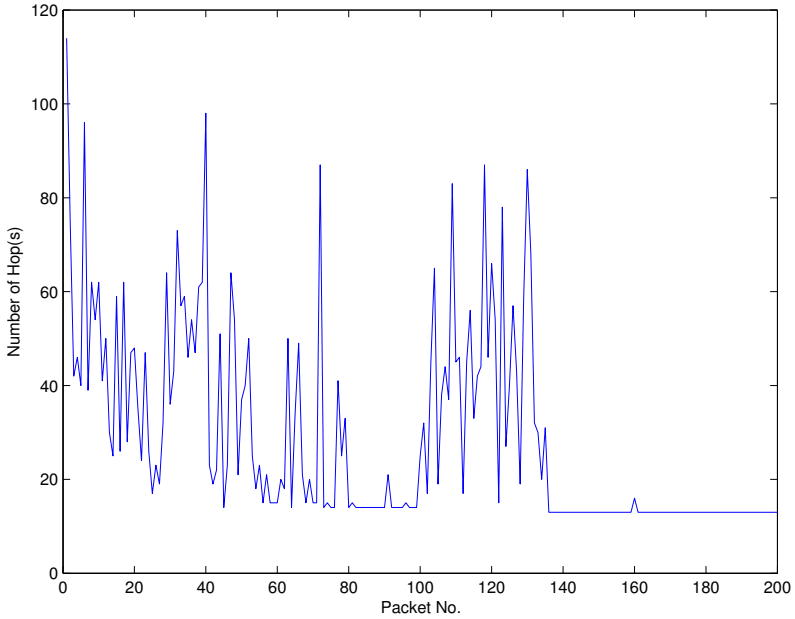


Figure 4.13: Convergence of Routes

Chapter 5

Smart Grid Application

In this chapter, we discuss wireless communication's application for smart grid in detail. Both power and communication subsystems are carefully examined. Challenges and implementation of integrating a wireless communication with a microgrid system are analyzed. We test the integrated system with different configurations, and show communication's impact on the state of the microgrid.

The smart grid is an interdisciplinary research topic, and its development requires effort from researchers with various backgrounds, especially those with expertise in power, communication, and control. Despite their different backgrounds, these researchers have a consensus that communication is essential for the smart grid (Wang et al., 2011; Yan and Qian, 2012). However, the reality is that communication for the smart grid is still at its infant stage, and a simulator able to integrate the power system and communication system as we would like is not even available. Communication experts know network simulators well, such as ns2, OPNET, and Qualnet; similarly, power system experts know PSSE, PSLF, and SimPowerSystem. "Naturally," co-simulators have been devised in an effort to take advantage of original simulators from both sides (Godfrey et al., 2010; Lin et al., 2011b; Hasan et al., 2009). Unfortunately, these co-simulators barely hold two parties together; they cannot be on the same page most of the time (Godfrey et al., 2010; Hasan et al., 2009), which means they

fail to synchronize. In addition, these co-simulators present a tremendous challenge because they demand that researchers from either field dive into another field with an overwhelming body of knowledge unfamiliar to them.

We present a well-integrated smart grid simulation of moderate complexity, consisting of both a power system and a communication system. It covers realistic power and communication characteristics and is not overwhelmingly complex; thus it serves as a thought-provoking example and encourages researchers in need of such a tool to obtain hands-on experience in simulating a smart grid system. The platform we choose is Simulink because of its abundant resources for power system modeling, versatility, and powerful user-defined function block. The power system we simulate is a microgrid that can operate in either on-grid or islanding mode. For communication, we use multiple access approaches we have proposed, and we constrain the communication within one hop. This is a basic setting, but enough for us to study the impact of important communication performance metrics, such as data rate and packet delay, on a power system.

The microgrid has been an evolving concept since it was defined (Microgrid, 2012). Although the definition of a microgrid differs, all definitions have some fundamental functions in common: (1) the capability of stable operation in islanding and/or on-grid modes, (2) minimum load disruption and shedding during transition, and (3) the capability to transition from one mode to the other and stabilize the microgrid after transitions. Many of the issues related to microgrid topology, control, and protection were summarized in Peng et al. (2009). Microgrid control problems, such as islanding detection (Hung et al., 2003; Lopes and Sun, 2006), droop control (Kim et al., 2011; Rokrok and Golshan, 2010), inverter control, and mode transition (Lei et al., 2011; Mohamed and A., 2011) are under intensive study, and results are reported in the literature.

Co-simulation involving both control and communication subsystems has long been an interesting topic. Although the fundamental microgrid functions can be easily performed locally and automatically based on local measurements, communication

in the microgrid is essential in order to achieve high performance and high efficiency. Requirements for communication capability vary with the different microgrid functions. For instance, closed-loop voltage and frequency control require more real-time information exchange than does economical dispatch. Co-simulation helps to quantitatively identify the microgrid application's requirements for communication. Also, co-simulation results are closer to the phenomena in real systems and hence give more accurate feedback for better control design.

A networked control system (NCS), the category to which a microgrid with communication belongs, provides a general guideline for these types of co-simulations (Branicky et al., 2003). Andersson et al. (2005) gives an example of NCS implemented in Simulink. There are also Simulink-based smart grid simulations, such as Pipattanasomporn et al. (2009). Despite the progress all these efforts have made, they either lack in-depth treatment of interaction between smart grid and communication or provide little or no flexibility for configuration by which the impact of communication on the smart grid can be studied. Several projects have been working toward more smart grid–oriented simulation; however, they need improvement. In Godfrey et al. (2010), a smart grid application co-simulation using OpenDSS and ns-2 is reported. OpenDSS is not suitable for time series system simulation, and the approach for exchanging information between OpenDSS and ns-2 through feeding scripts to each other has obvious limitations. Lin et al. (2011b) models a smart grid system with PSLF and ns-2; however, creating an interface logic and integrating two sub-simulators remain challenging tasks. Finally, regarding our chosen platform of Matlab/Simulink, we note that Matlab has made noticeable improvements and is completely capable of simulating a complex communication system. Mehlfhrer et al. (2011) has presented a complete LTE simulator, both link level and system level; Truetime (2012) has showcased a Matlab/Simulink-based simulator for real-time control system with communication.

5.1 Power Grid Subsystem

In this section, we describe the power grid subsystem, shown in Fig. 5.1, from two different perspectives: one presenting its layered structure, which consists of grid-level, microgrid-level, and device-level details; the other outlining its operations, highlighting the microgrid's reactions to events happening in the system.

At the grid level, the microgrid as a single entity is connected to the main grid through a microgrid switch, which in turn is connected to the transformer. On the main grid side of the transformer is the feeder, both ends of which have circuit breakers installed. In case of a fault, the circuit breakers trip. If the disconnection resulting from the fault is long enough, the microgrid switch cuts off the microgrid from the main grid, forcing the microgrid into islanding mode from on-grid mode.

At the microgrid level, we have three buses; each bus has one DER (distributed energy resource) and one load. However, the most important component at this level is the microgrid controller, which manages the actions of other components. By exchanging information with devices and the main grid, the microgrid controller conducts system situation awareness, operation mode selection, and power dispatch to achieve optimal power flow, maximum utilization of DER, and system efficiency improvement.

At the device level, we focus on the DER. A simplified circuit diagram of the DER is shown in Fig. 5.3. The DER is connected in parallel with the grid through a coupling inductor L_c. The connection point is referred to as the point of common coupling (PCC), and the PCC voltage is denoted as v_t. The equivalent local load is also connected at the PCC. The rest of the system is simplified as an infinite voltage source with system impedance Zs. The DER energy source is connected on the DC side of the inverter with a capacitor. The inverter current i_c is controlled so that the desired amount of active power and reactive power is provided from the DER. Let $v_t(t)$ and $v_c(t)$ denote the instantaneous PCC voltage and the inverter output voltage (harmonics are neglected), respectively, and α be the phase angle of $v_c(t)$ relative to

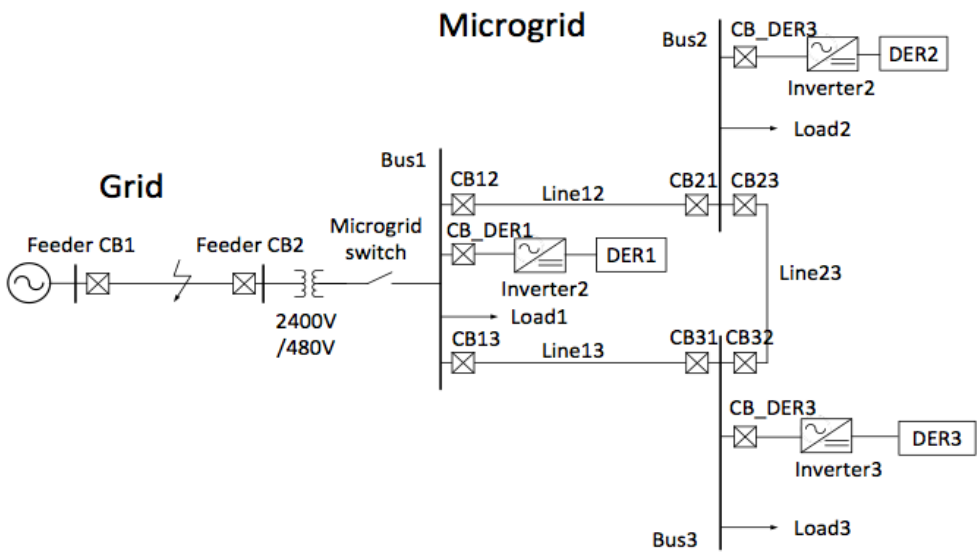


Figure 5.1: A 3-bus 3-DER Microgrid Topology

the PCC voltage. In steady state, the average active power $P(t)$ and average reactive power $Q(t)$ of the inverter can be approximated by the first terms of the Taylor series if the angle α is small, as shown in Eq.5.1 and Eq.5.2, where $Q(t)$ is defined as positive if the inverter injects reactive power to the utility and negative if the inverter absorbs

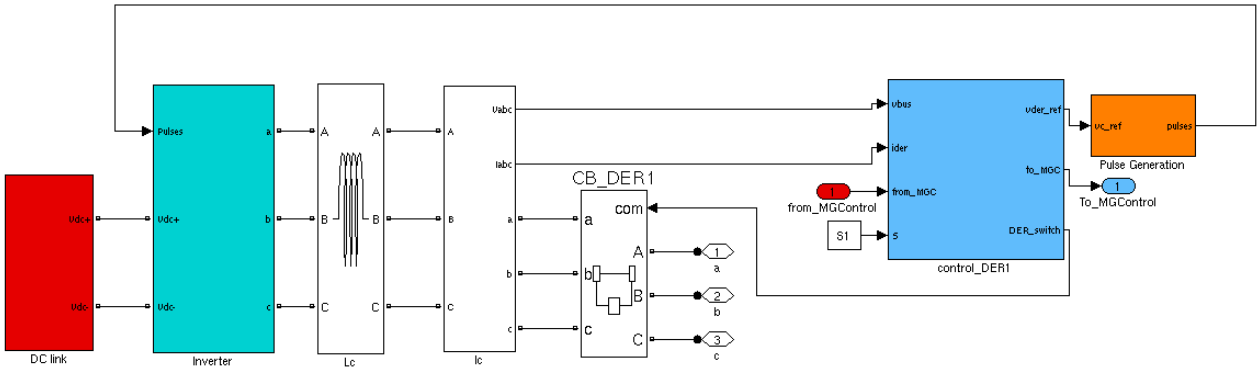


Figure 5.2: DER Implementation in Simulink

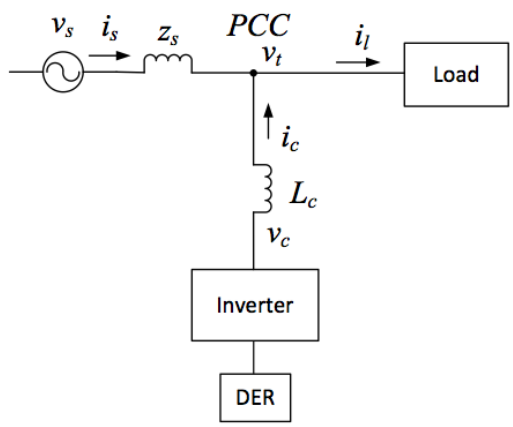


Figure 5.3: Simplified DER Circuit Diagram

reactive power from the utility.

$$P(t) \approx \frac{v_t v_c}{\omega L_c} \alpha. \tag{5.1}$$

$$Q(t) \approx \frac{v_t}{\omega L_c}(v_c - v_t). \tag{5.2}$$

Assuming that α is small ($< \pi/8$ rad) and the system voltage variation is low (true at steady state), the control of active power P and reactive power Q can be decoupled. They can be controlled simultaneously and independently; however, there is some coupling during a transient period. Inverter control methods can be developed based on Eqs. 5.1 and 5.2. The inverter is controlled as a voltage source. The inverter output active power is controlled by controlling the phase angle of the inverter output voltage (v_c), and the reactive power is controlled by adjusting the magnitude of the inverter voltage. Furthermore, different variables can be controlled based on different objectives. The frequency, active power, and active current are in the group of variables related to active power; and the voltage, reactive power, and reactive current are in the group of variables related to reactive power. Any combination of

variables with one from each group can be controlled together. Fig. 5.2 shows our DER model in Simulink.

Microgrid Operation

The microgrid can operate in *on-grid mode* and *islanding mode*. In our simulation, we carefully study the microgrid's behaviors in both modes; more important, we examine the transitions between modes, because smooth transition between different modes is essential to a microgrid.

In the on-grid mode, DER1 and DER2 generate a fixed amount of active power; DER3 generates the active power following the P-f droop control curve. All of the three DERs perform Q-V droop control with the droop curves to control Bus1 voltage.

When a fault occurs on the feeder line, as shown in Fig. 5.1, the circuit breakers on both ends of the feeder trip, and the microgrid is disconnected from the main grid with some other local loads. The islanding detection is based on the magnitude of Bus1 voltage. A microgrid should have some low/high voltage ride-through capability and stay connected before the relay protection trips, as long as the fault current from the DER does not exceed the microgrid protection settings or the DER device protection settings.

The feeder circuit breakers trip first; then, following German low-voltage ride-through standards (BDEW German Association of Energy and Water Industries, 2011), 7.5 cycles after the fault occurs, the microgrid switch is opened. The microgrid starts switching into islanding mode. When the microgrid is operating in the islanding mode, the load and the DER must be rebalanced to maintain the voltage and frequency stability. Because, in on-grid mode, power is usually imported from or exported to the main grid, the total load and the total DER generation within the microgrid are not balanced. Load shedding may be required if the available maximum power from the DER cannot meet the total load demand.

When the main grid is recovered from a fault and back to a normal condition, the microgrid switch will close and the microgrid will transition from islanding to on-grid

mode. A resynchronization signal, either sent by the upper level system operator or generated by the microgrid switch itself based on the local measurement, will trigger the resynchronization process. During the resynchronization, the active power and reactive power will be re-dispatched among the DER so that the magnitude, frequency, and phase angle of the Bus1 voltage are adjusted to synchronize with the system voltage. In the simulation, when the magnitude difference is within 1 V, the frequency difference is within 0.01 Hz, and the phase angle difference is within 5°, the microgrid switch is closed.

5.2 Communication Subsystem

In a microgrid, we assume that all communication nodes are within a one-hop distance of one another and thus are able to communicate with one another directly. Nodes share the same wireless channel and contend for time slots to transmit packets.

Each power system component that needs communication capability is associated with a designated communication module/node. In our specific system, there are eight devices that have a communication module: the microgrid controller (MGC), the microgrid switch (MGS), three DERs (DER1, DER2, DER3), and three Loads (Load1, Load2, Load3). MGC is the communication hub in the system. DERs and Loads report their status to MGC; MGC broadcasts a controlling message to DERs and Loads.

Communication modules are implemented using *matlab function*, which is a type of block in Simulink's *user-defined functions* category. In a matlab function block, users implement a matlab function, whose input and output correspond to the input and output ports generated in the block. When a communication module is connected to its corresponding microgrid component, in data receiving flow, the communication module's data output ports are connected to the microgrid component's data input ports; in data sending flow, the data output ports of the microgrid component are connected to the communication module's data input ports. For example, Fig. 5.4

shows the pairing structure of the MGC component and its communication module. In a Simulink environment, matlab function blocks are similar to different threads in a multi-threaded program; however, each matlab function block completes a complete run whenever the simulation clock moves forward by one step.

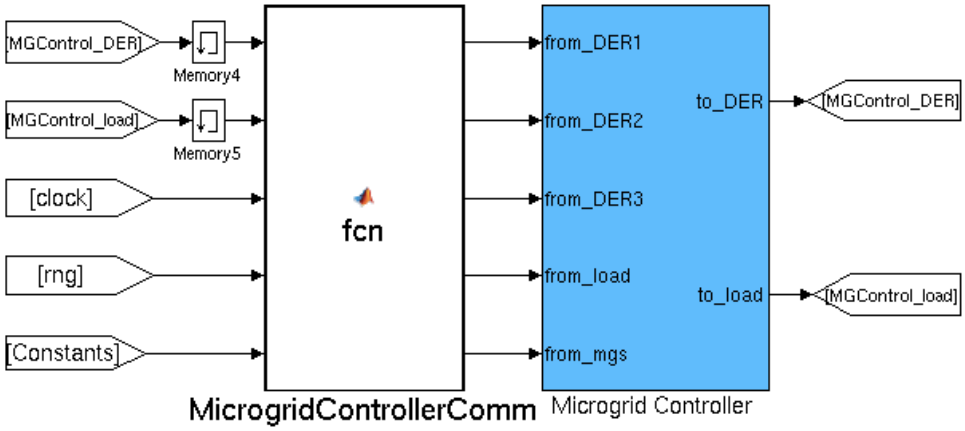


Figure 5.4: Pairing of Communication and Power Components

Synchronization and State Machine

The tactic to achieve synchronization in co-simulation is of prominent importance. In NCS, which usually consists of an event-driven network communication subsystem and a time-driven continuous control subsystem, arranging proper and sufficient common time points at which both systems can share and update their respective statuses is critical for successful and accurate system simulation. Many papers on co-simulation have addressed this problem. They propose and implement various approaches (Lin et al., 2011b; Hasan et al., 2009). Several methods are representative. In Lin et al. (2011b), a global scheduler is created to keep a global event list that contains events sorted by their occurrence times from both systems. This method requires continuous system modeling, which usually has much smaller simulation steps, pauses at every simulation step, and checks possible event(s) from an event-driven communication system outside. This forced pause negatively affects simulation efficiency tremendously; moreover, creating glue code for interfaces to both system is

a delicate task requiring considerable effort. In Hasan et al. (2009), the event-driven network subsystem controls the time-driven control subsystem's progress by setting a pause point in the control subsystem ahead of time. This method is more efficient and easier to implement. However, determining the control subsystem's proper pause point is a challenging job with a noticeable probability of missing an event of interest in the control subsystem.

As opposed to other co-simulation systems, our system is inherently synchronized, taking the Simulink simulation clock (shown at upper left in Fig. 5.5) as a global reference. Recall that each communication module implemented in the *matlab function* block is executed in every simulation step. Not having the freedom to move the simulation clock forward by itself, the communication subsystem runs in parallel with the microgrid subsystem. Without an event queue, we use a *state machine* to manage the behavior of each communication module. We define a *persistent* variable (the matlab counterpart of a static variable in C language) *state* whose possible values are predetermined. We have *state* such as *idle, send, receive, wait* and so on. At each time step, the module combines the current *state*, event in current state, and input to make a decision on state transition. Through this state machine, communication modules proceed following strict procedure.

Access to Common Channel

In Simulink, it is a challenging task to implement a common channel that all communication nodes are able to monitor and access. Unlike in conventional network simulators, which use object-oriented programming techniques and could easily define a globally accessible channel object, defining a global variable itself in Simulink is not easy. To create a global object, we use the *Data Store Memory* component, which provides an interface for defining a user-defined object that is accessible in all matlab function blocks.

Two key variables of our channel modeling are channel status and channel packet, which have the respective functions of carrying channel status information for channel

contention and delivering a packet through the channel to a designated destination. Taking *theChStatus* and *theChPacket* (in Fig. 5.5) as examples, we give a detailed description of how to use the *Data Store Memory* component for the communication subsystem's channel modeling in Simulink. At the top level, through the *data store name* attribute of *Data Store Memory*, a name is given to the global variable; in our case, it is either *theChStatus* or *theChPacket*. The data type of the variable could be user-defined, and the user-defined data type is best saved into a .mat file. Before running the simulation in Simulink each time, the file should be loaded and the user-defined data type made available in the co-simulation project's current workspace. In any matlab function block that wants to use this global variable, the final step is using its *edit data/ports* tool to register the variable and declaring a global variable with the same name. If these steps are followed, every communication module declares *theChStatus* and *theChPacket* global variables for channel access. Note that in the Simulink settings, *Data Store Memory*'s "read before write" warning/error may have to be deactivated.

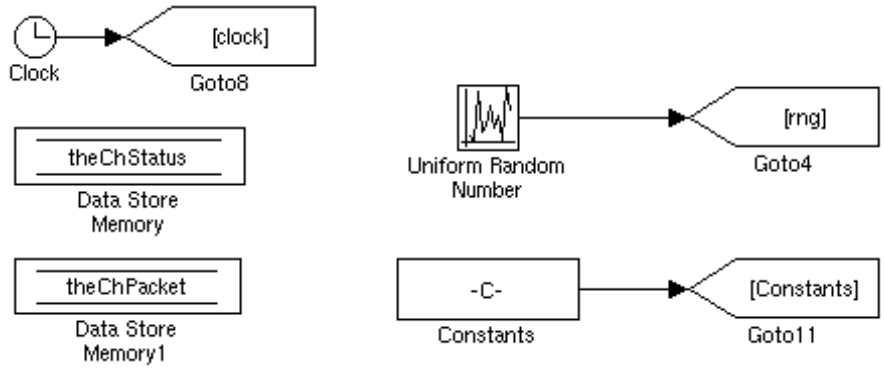


Figure 5.5: Global Clock, Data Store Memory, and Constants for Configuration.

5.3 Results and Analysis

The simulation's time step size is $10us$. In our simulation, at $t = 1s$, a ground fault happens at the feeder from the main grid to the microgrid. After the ride-through

period, the microgrid enters the islanding mode from the on-grid mode, managing to rebalance the power flow in the microgrid. At around $t = 3s$, the fault at the feeder is cleared. Only the transition from the on-grid mode to the islanding mode is simulated because it has higher requirements on the real-time system data. The voltage profile in Fig. 5.6 illustrates this process.

Sampling Period Impact

By changing the signal sampling period, T_0, we study the microgrid system's tolerance to different data updating periods, which is determined by the signal sampling period. The results are shown in Fig. 5.6. As we can see in the figure, the voltage profiles are almost identical with $T_0 = 0.02s$ and $T_0 = 0.05s$. However, increasing the sampling period to $T_0 = 0.08s$ makes a big difference. With this setting, not only does the voltage converge in a slower manner, but also there are a frequency deviation and a phase oscillation. Further increasing the sampling period, we find that the microgrid system becomes unstable over a long period and phase oscillation is observed. With a longer sampling period, the controllers inside the microgrid obtain less frequent feedback on the system situation; when the information-updating delay exceeds some critical time, the controllers may fail to make timely control adjustments, and as a result, the system may lose stability. The sampling period makes a substantial impact, especially when the microgrid transits from on-grid to islanding mode. During the transition, in order to maintain frequency and voltage stability, all the controllable components, including DERs and controllable loads, must receive the islanding signal and make control mode switches accordingly as soon as possible, or at least before some critical point. The risk that the system will lose stability substantially increases with the growth of the control-mode-switch delay, as shown in Fig. 5.6.

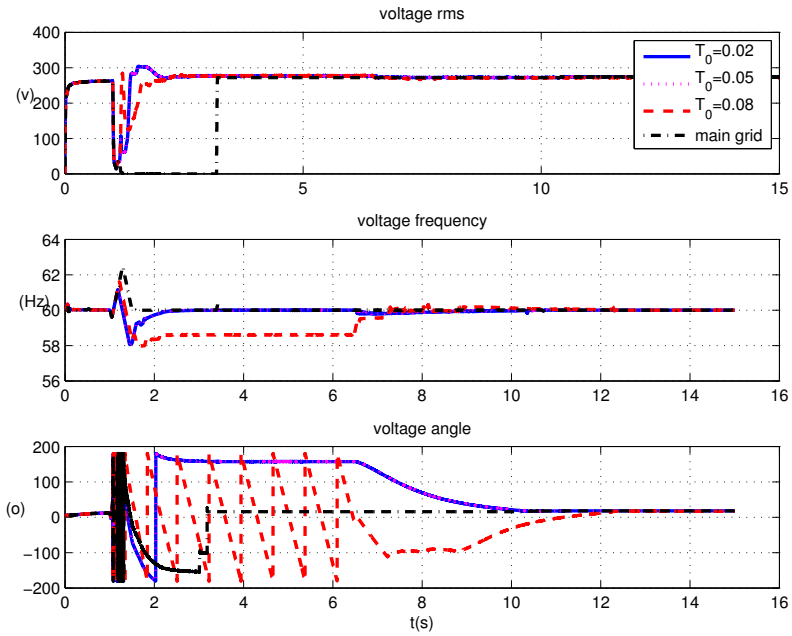


Figure 5.6: Microgrid Voltage Profile with Different Sampling Periods.

Impact of Data Rate and Packet Delay

In a microgrid, messages exchanged among different components usually have predefined formats. For example, in our 3-bus microgrid, at every transmitting opportunity, MGC sends 24 messages to DERs and 6 messages to Loads (broadcasting), Load and DER both send 6 messages to MGC, and MGS sends 10 messages to MGC. A message as payload is enclosed into a packet with auxiliary information, such as source, destination, error detection and correction, in packet header. Setting overhead size as 8 messages and each datum being a 4-byte double, we calculate total data volume as $[(6+8)*7+(10+8)+(24+8)+(1+8)*9]*32 = 7328bits$, with the ACK packets counted. Hence, when the system sampling/updating period is set at T_0, the data rate generated by our microgrid system is $R_1 = 7.328/T_0 kbps$.

With each component transmitting its latest data at fixed intervals, the microgrid uses its communication subsystem similarly to the TDMA (Time Division Multiple Access) format. If no other traffic is involved, such as other control messages or

Internet service, packet transmission uncertainty (e.g. packet delay) is mainly from a noise-corrupted packet that needs retransmission. Delay resulting from packet collision is much less likely, as long as the channel capacity rate is large enough to accommodate packets generated by the microgrid. To better study the impact of the transmission delay on the microgrid when local DERs are allowed to spontaneously talk to neighbors for the purpose of local control, we provide a component in our communication subsystem, modeling the "other traffic." The "other traffic" generates data with size uniformly distributed in the range $[1, D_s]$, and its packet arrival interval follows poisson distribution, with the expected value being λ time steps Thus, the data rate generated by the"other traffic" is

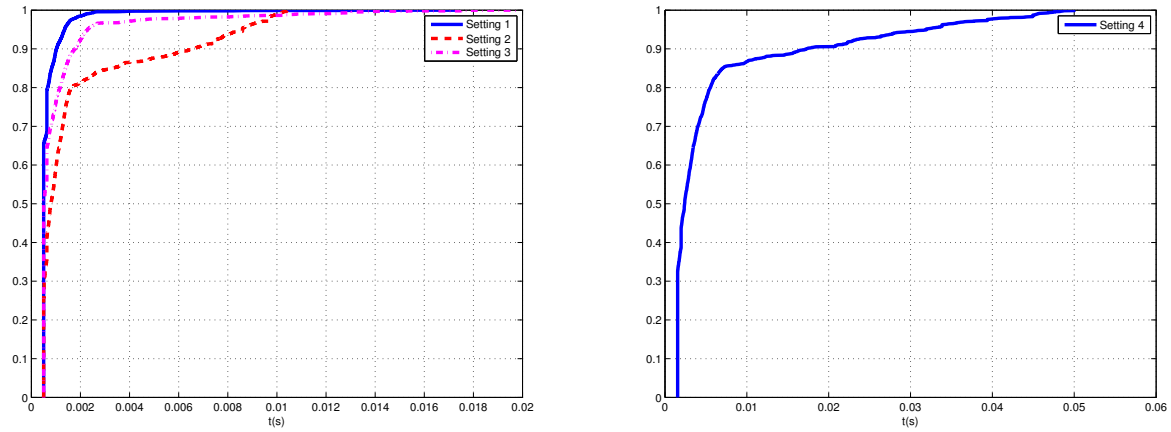
$$R_2 = (D_s/2 + 8) * 32/(\lambda T_s), \tag{5.3}$$

where $T_s = 10us$ is the time step in the simulation.

Table 5.1 lists four settings we used to study the impact of the packet delay on the microgrid. In the table, R is the data transmission rate. Setting 1 represents moderate traffic; setting 3, crowded traffic; and setting 2 congested traffic. The packet delay CDFs (cumulative distribution functions) of the first three settings are given in Fig. 5.7a. As expected, among the three settings, setting 2 has the largest delay and setting 1 the smallest.

Table 5.1: Four Different Settings Used for Studying the Impact of Packet Delay on the Microgrid

	1	2	3	4
T_0	$2000T_s$	$1000T_s$	$2000T_s$	$5000T_s$
D_s	20	20	40	40
λ	250	250	250	500
R_1	366k	732k	366k	147k
R_2	230k	230k	358k	179k
R	1M	1M	1M	300k
$P_{loss}\%$	0%	7.1%	0%	2.8%



(a) Packet delay CDF under the first three settings. **(b)** Packet delay CDF under the 4th setting.

Figure 5.7: Packet Delay CDF.

Microgrid voltage profiles corresponding to these three settings are almost the same, as shown in Fig. 5.8. The reason is that, although packets suffer considerable delay, they are still well within the microgrid's tolerance range. Even with a 7.1% packet loss rate in setting 2, it is almost certain that there is new data for updating within $0.05s$. In setting 4, we create an overcrowded traffic scenario with a larger sampling period at $0.05s$. With a packet delay as large as $0.05s$ (Fig. 5.7b) and possibly a packet lost (at 2.8%), this setting could result in a period longer than $0.1s$ without new updating data being received. The microgrid voltage profile in setting 4 is also shown in Fig. 5.8. Obviously, the result is not good: the magnitude and frequency have more deviations and the angle oscillates. It is straightforward that the microgrid controllable components can only make timely and correct control actions based on fast and accurate updating of the system situation.

5.4 Conclusion

We have presented a communication-enhanced microgrid in Simulink. The modeling of the power subsystem, implementation tactics, and details of the communication

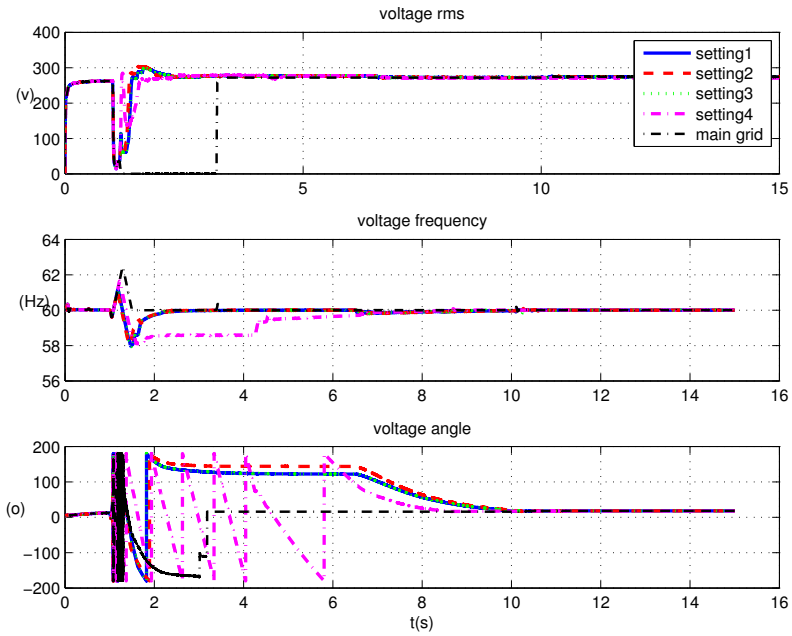


Figure 5.8: Microgrid Voltage Profiles with Different Packet Delays.

subsystem are the primary issues addressed. Simulation performance and results are reported, with emphasis given to the impact of the communication subsystem on the power subsystem. Impacts of communication on microgrid operation have been investigated by varying communication configurations. The results have shown that communication has a substantial impact on microgrid performance, especially in system dynamical transitions. If the delay in updating the controllers with the new system status exceeds a certain critical point, the system will lose stability. The results will help to quantitatively identify the microgrid's requirements on communication and help to improve control designs.

Chapter 6

Conclusion and Future Work

6.1 Conclusion

In this dissertation, we have studied the problem of designing wireless communication networks for CPS. CPS are generally large and complex systems with a large variety of components, including geographically distributed sensors monitoring different events, actuators carrying out various control actions, and controllers collecting information for their own individual needs. To provide a robust channel for information delivery among components in CPS, its communication network has to be efficient, reliable, responsive, and adaptable.

In our design of wireless communication networks for CPS, we divide the network into layers, and have studied multiple access layer and network layer in detail. At multiple access layer, we devise three multiple access approaches: compressed multiple access, sample-contention multiple access, and prioritized multiple access. Compressed multiple access uses compressed sensing at base station to recover data when traffic load is sparse. With no need to worry about possible transmission collision and having transmitter identified automatically in the process of data recovery, compressed multiple access is an efficient and flexible scheme. Sample-contention multiple access allows base station to first survey a field of transmitters

with data, then assess a cut. Eligible transmitters made the cut move to the next round of contention. Prioritized multiple access provides a method to select data that is more desirable for transmission when bandwidth is limited. Both sample-contention and prioritized multiple access incorporate demands from application layer, and use cross-layer optimization. Three approaches at multiple access layer complement one another, allowing them together to provide efficient, reliable service to network layer. At network layer, we focus on creating robust route for data delivery in CPS' core communication network. By creating backup path, transmission interruption is avoided. We use integer programming in creating backup path when global information is available, and Ant Colony Optimization (ACO) and positive feedback in the distributed online method.

For each module in our design, either access scheme or routing method, we evaluate it in a CPS based setting, such as voltage control application in a smart grid. Comparison of performance with conventional counterpart confirms the advantage of our design. We also have specifically discussed the integration of our wireless communication network into a microgrid, a typical smart grid system.

6.2 Future Work

While we have designed building blocks and integrated them at layer-level for wireless communication in CPS, more research work is needed for improvement. The followings are the aspects on which we are working or plan to work.

Addressing Communication Needs of New Components in CPS: CPS themselves are still in the early stage of development. An increasing number of heterogeneous components are expected to connect to CPS. For example, in smart grid, while distributed energy resources bring considerable amount of energy capacity, they also introduce noticeable uncertainties into the power system. As real-time interactions among components are essential in CPS, communication infrastructures, especially wireless, are indispensable in the

processing of integrating more components, and forming large-scale CPS. Our wireless communication design has shown promising results. Obtaining in-depth knowledge of interaction among components in large-scale CPS, identifying and addressing their communication needs through communication network design are one of our research goals next.

Security in CPS Communication Network: We have not specifically studied security problem in our design in this dissertation, but this does not indicate that security is an easy or trivial problem. Actually, communication security is one of the most important problems in CPS , if it is not *the* most important one. Authentication, Deny of Service and others are all critical topics in CPS. In our future work, we plan to tackle these issues from the perspective of communication network architecture. For example, in our compressed multiple access scheme, each transmitter's random code could be strong encryption code.

Bibliography

Ahmadi, H. and Abdelzaher, T. (2009). An adaptive-reliability cyber-physical transport protocol for spatio-temporal data. In *Real-Time Systems Symposium, 2009, RTSS 2009. 30th IEEE*, pages 238–247. IEEE. 9

Ahmadi, H., Abdelzaher, T., and Gupta, I. (2010). Congestion control for spatio-temporal data in cyber-physical systems. In *Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems*, pages 89–98. ACM. 9

Akyildiz, I., Su, W., Sankarasubramaniam, Y., and Cayirci, E. (2002). Wireless sensor networks: a survey. *Computer networks*, 38(4):393–422. 9

AMPL (2012). Cplex solver, http://www.ampl.com. 77

Andersson, M., Henriksson, D., Cervin, A., and Arzen, K. (2005). Simulation of wireless networked control systems. *IEEE Conference on Decision and Control, 2005 and European Control Conference 2005*, pages 476–481. 95

Baillieul, J. and Antsaklis, P. (2007). Control and communication challenges in networked real-time systems. *Proceedings of the IEEE*, 95(1):9–28. 7

BDEW German Association of Energy and Water Industries (2011). Generating plants connected to the medium-voltage network: Guideline for generating plants' connection to and parallel operation with the medium-voltage network. 99

Belghith, A., Nuaymi, L., and Maille, P. (2008). Pricing of differentiated-qos services wimax networks. *Proc. of IEEE Conference of Global Communications (Globecom)*. 38

Boufounos, P., Duarte, M., and Baraniuk, R. (2007). Sparse signal reconstruction from noisy compressive measurements using cross validation. *Proc. of the IEEE Workshop on Statistical Signal Processing*. 28, 34

Branicky, M. S., Liberatore, V., and Phillips, S. M. (2003). Networked control system co-simulation for co-design. *American Control Conference, 2003*, 4:3341–3346. 95

Candes, E., Romberg, J., and Tao, T. (2006). Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information. *IEEE Trans. Inform. Theory*, 52:489–509. 16

Candes, E. J. and Tao, T. (2006). Near optimal signal recovery from random projections: Universal encoding strategies. *IEEE Trans. Inform. Theory*, 52(12):5406–5425. 16

Chen, G., de Guo, T., guo Yang, W., and Zhao, T. (2006). An improved ant-based routing protocol in wireless sensor networks. In *Collaborative Computing: Networking, Applications and Worksharing, 2006. CollaborateCom 2006. International Conference on*, pages 1–7. 87

Chen, S., Donoho, D. L., and Saunders, M. (1999). Atomic decomposition by basis pursuit. *SIAM Journal Science Computing*, 20:33–61. 16

Chung, T. H., Gupta, V., Hassibi, B., Burdick, J., and Murray, R. M. (2004). Scheduling for distributed sensor networks with single sensor measurement per time step. *Proceedings of the 2004 IEEE International Conference on Robotics and Automation*. 61

Cloosterman, M., van de Wouw, N., Heemels, W., and Nijmeijer, H. (2009). Stability of networked control systems with uncertain time-varying delays. *IEEE Transactions on Automatic Control*, 54(7):1575–1580. 10

Davenport, M., Wakin, M., and Baraniuk, R. (2006). Detection and estimation with compressive measurements. Technical Report TREE0610, Rice ECE Department. 17

Demirkol, I., Ersoy, C., and Alagoz, F. (2006). Mac protocols for wireless sensor networks: a survey. *Communications Magazine, IEEE*, 44(4):115–121. 9

Derler, P., Lee, E., and Sangiovanni-Vincentelli, A. (2011). Addressing modeling challenges in cyber-physical systems. Technical report, DTIC Document. 8

DOE (2008). The smart grid: an introduction. Technical report, Department of Energy's Office of Electricity Delivery and Energy Reliability. 50

Donoho, D. L. (2004). For most large underdetermined systems of linear equations, the minimal l_1-norm solution is also the sparsest solution. *Commun. Pure Appl. Math*, 59(6):797–829. 16, 127, 128

Donoho, D. L. (2006). Compressed sensing. *IEEE Trans. Inform. Theory*, 52:1289–1306. 16, 25, 26, 127

Donoho, D. L., Elad, M., and Temlyakov, V. (2006a). Stable recovery of sparse overcomplete representations in the presence of noise. *IEEE Trans. Inform. Theory*, 52(1):6–18. 26, 27, 128, 129

Donoho, D. L., Tsaig, Y., Drori, I., and Starck, J. (2006b). Sparse solution of underdetermined linear equations by stagewise orthogonal matching pursuit. Technical report. 16

Dunbar, M. (2001). Plug-and-play sensors in wireless networks. *Instrumentation & Measurement Magazine, IEEE*, 4(1):19–23. 2

Ettus Research LLC (2012). http://wwww.ettus.com. 79

Fakham, H., Ahmidi, A., F., C., and Guillaud, X. (2010). Multi-agent system for distributed voltage regulation of wind generators connected to distribution network. *Proc. of Innovative Smart Grid Technologies Conference Europe*. 38

Ganesan, D., Govindan, R., Shenker, S., and Estrin, D. (2001). Highly-resilient, energy- efficient multipath routing in wireless sensor networks. *ACM SIGMOBILE Mobile Computing and Communications Review*, 5(4). 10

Godfrey, T., Mullen, S., Dugan, R. C., Rodine, C., Griffith, D. W., and Golmie, N. (2010). Modeling smart grid applications with co-simulation. *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 291–296. 93, 95

Gokturk, M. and Gurbuz, O. (2008). Cooperation in wireless sensor networks: Design and performance analysis of a mac protocol. In *Communications, 2008. ICC '08. IEEE International Conference on*, pages 4284–4289. 9

Hanzo, L. and Rafazolli, R. (2009). Admission control schemes for 802.11-based multi-hop mobile ad hoc networks: a survey. *IEEE Communications Surveys&Tutorials*, 11(4). 39

Hasan, M. S., Yu, H., Carrington, A., and Yang, T. C. (2009). Co-simulation of wireless networked control systems over mobile ad hoc network using simulink and opnet. *IET Communications*, 3(8):1297–1310. 93, 101, 102

Hatziargyriou, N., Asano, H., Iravani, R., and Marnay, C. (2007). Microgrids: an overview of ongoing research, development, and demonstration projects. *IEEE Power Energy Mag.*, 5:78. 52

Heemels, W. P. M. H., Teel, A., Van de Wouw, N., and Nešić, D. (2010). Networked control systems with communication constraints: Tradeoffs between transmission intervals, delays and performance. *Automatic Control, IEEE Transactions on*, 55(8):1781–1796. 8

Henriksson, D. and Elmqvist, H. (2011). Cyber-physical systems modeling and simulation with modelica. In *International Modelica Conference, Modelica Association*. 9

Hung, G., Chang, C., and Chen, C. (2003). Automatic phase-shift method for islanding detection of grid-connected photovoltaic inverters. *IEEE Transactions on Energy Conversion*, 18:169–173. 94

IEEE (2005). Ieee standard for local and metropolitan area networks. *IEEE Std. 802.16e-2005*. 41

Ilic, M., Xie, L., Khan, U., and Moura, J. (2008). Modeling future cyber-physical energy systems. In *Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century*, pages 1–9. IEEE. 8

Jin, L., Kumar, R., and Elia, N. (2010). Model predictive control-based real-time power system protection schemes. *IEEE Trans. on Power Systems*, 25(2). 38, 39, 52

Kanodia, V. and Li, C. (2002). Distributed priority scheduling and medium access in ad-hoc networks. *ACM Wireless Networks*, 8. 9, 39

Kashem, M. and Ledwich, G. (2005). Multiple distributed generators for distributed feeder voltage support. *IEEE Trans. on Energy Conversion*, 20(3). 52

Kim, J., Guerrero, J. M., Rodriguez, P., Teodorescu, R., and Kwanghee, N. (2011). Mode adaptive droop control with virtual output impedances for an inverter-based flexible ac microgrid. *IEEE Transactions on Power Electronics*, 26:689–701. 94

Kim, K. and Kumar, P. (2012). Cyber–physical systems: A perspective at the centennial. *Proceedings of the IEEE*, 100(13):1287–1308. 1, 7

Ko, H., Yoon, G., and Hong, W. (2007). Active use of dfig-based variable-speed wind-turbine for voltage regulation at a remote location. *IEEE Trans. on Power Systems*, 22(4):1916–1925. 51, 52

Krishnamachari, L., Estrin, D., and Wicker, S. (2002). The impact of data aggregation in wireless sensor networks. In *Proceedings of 22nd International Conference on Distributed Computing Systems Workshops*, pages 575–578. IEEE. 9

Labinaz, G., Bayoumi, M. M., and Rudie, K. (1997). A survey of modeling and control of hybrid systems. *Annual Reviews of Control*, 21:79–92. 57

Lee, E. (2006). Cyber-physical systems-are computing foundations adequate. In *Position Paper for NSF Workshop On Cyber-Physical Systems: Research Motivation, Techniques and Roadmap*, volume 1, pages 1–9. Citeseer. 2

Lee, E. (2008). Cyber physical systems: design challenges. In *11th IEEE International Symposium on Object Oriented Real-Time Distributed Computing (ISORC)*, pages 363–369. 4

Lee, I., Sokolsky, O., Chen, S., Hatcliff, J., Jee, E., Kim, B., King, A., Mullen-Fortino, M., Park, S., Roederer, A., and Venkatasubramanian, K. (2012). Challenges and research directions in medical cyber-physical systems. *Proceedings of the IEEE*, 100(1):75 –90. 7

Lei, Q., Peng, F. Z., and Yang, S. (2011). Multiloop control method for high-performance microgrid inverter through load voltage and current decoupling with only output voltage feedback. *IEEE Transaction on Power Electronics*, 26:953–960. 94

Li, H., Lai, L., and Poor, H. (2012a). Multicast routing for decentralized control of cyber physical systems with an application in smart grid. *IEEE Journal on Selected Areas in Communications*, 30(6):1097–1107. 10

Li, H., Li, F., Xu, Y., Rizy, D., and Kueck, J. (2010). Adaptive voltage control with distributed energy resources: Algorithm, theoretical analysis, simulation, and field test verification. *IEEE Trans. on Power Systems*, 25(3). 38, 52

Li, H., Qiu, R., and Wu, Z. (2012b). Routing in cyber physical systems with application for voltage control in microgrids: A hybrid system approach. In *2012 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW)*, pages 254–259. IEEE. 10

Li, Q., Xu, M., Pan, L., and Cui, Y. (2008). A study of path protection in self-healing routing. *Lecture Notes in Computer Science*. 71

Li, X. and Xu, Z. (2011). The design of simulation platform for ad hoc based cyber-physical system. In *2011 Seventh International Conference on Mobile Ad-hoc and Sensor Networks (MSN)*, pages 350–353. IEEE. 9

Lin, H., Sambamoorthy, S., Shukla, S., Thorp, J., and Mili, L. (2011a). Power system and communication network co-simulation for smart grid applications. In *Innovative Smart Grid Technologies (ISGT), 2011 IEEE PES*, pages 1–6. IEEE. 9

Lin, H., Sambamoorthy, S., Shukla, S., Thorp, J., and MiliPower, L. (2011b). System and communication network co-simulation for smart grid applications. *IEEE PES Conference on Innovative Smart Grid Technologies*. 93, 95, 101

Lin, J., Sedigh, S., and Miller, A. (2009). Towards integrated simulation of cyber-physical systems: a case study on intelligent water distribution. In *Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009. DASC'09*, pages 690–695. IEEE. 8

Lin, Y. and Wong, V. (2006). Saturation throughput of ieee 802.11e edca based on mean value analysis. *IEEE Wireless Communications and Networking Conference*, pages 475–480. 39

Ling, Y. and Meng, D. (2006). Study on improved truncated binary exponential back-off collision resolution algorithm. *International Journal of Computer Science and Network Security (IJCSNS)*, 6(11). 28

Liu, X., Zhang, H., Xiang, Q., Che, X., and Ju, X. (2012). Taming uncertainties in real-time routing for wireless networked sensing and control. In *Proceedings of the thirteenth ACM international symposium on Mobile Ad Hoc Networking and Computing*, MobiHoc '12, pages 75–84, New York, NY, USA. 10

Lopes, C. and Sun, H. (2006). Performance assessment of active frequency drifting islanding detection methods. *IEEE Transaction on Energy Conversion*, 21:171–180. 94

Lu, W. and Vaswani, N. (2010). Modified basis pursuit denoising for noisy compressed sensing with partially known support. *Proc. of Acoustics, Speech and Signal Processing (ICASSP)*. 28

Lunze, J. and Lagarrigue, F. L. (2009). *Handbook of Hybrid Systems Control: Theory, Tools, Applications*. Cambridge University Press. 52

Malioutov, D. M., Sanghavi, S., and Willsky, A. S. (2008). Compressed sensing with sequential observations. *Proc. of Acoustics, Speech and Signal Processing (ICASSP)*. 20, 23

Marwedel, P. (2010). *Embedded System Design: Embedded Systems Foundations of Cyber-Physical Systems*. Springer Verlag. 7

Médard, M., Finn, S. G., Barry, R. A., and Gallager, R. G. (1999). Redundant trees for preplanned recovery in arbitrary vertex-redundant or edge-redundant graphs. *IEEE/ACM Trans. on Networking*, 7:641–652. 71

Mehlfhrer, C., Colom Ikuno, J., Simko, M., Schwarz, S., Wrulich, M., and Rupp, M. (2011). The vienna lte simulators—enabling reproducibility in wireless communications research. *EURASIP Journal on Advances in Signal Processing*. 95

Microgrid (2012). http://certs.lbl.gov/certs-der-micro.html. 94

Modelica (2012). http://www.modelica.org. 9

Mohamed, R. I. and A., R. A. (2011). Hierarchical control system for robust microgrid operation and seamless mode transfer in active distribution systems. *IEEE Transactions on Smart Grid*, 2:352–362. 94

Mohammed Tariquea, S. A., Tepeb, K. E., and Erfanib, S. (2009). Survey of multipath routing protocols for mobile ad hoc networks. *Journal of Network and Computer Applications*, 32(6). 10, 88

Negenborn, R., Beccuti, A., Demiray, T., Leirens, S., Damm, G., De Schutter, B., and Morari, M. (2007). Supervisory hybrid model predictive control for voltage stability of power networks. *Proceedings of the 2007 American Control Conference*, pages 5444–5449. 54

Pati, Y. C., Rezaiifar, R., and Krishnaprasad, P. S. (1993). Orthogonal matching pursuit: recursive function approximation with applications to wavelet decomposition. *Signals, Systems and Computers*, 1:40–44. 16

Peng, F. Z., Li, Y. W., and Tolbert, L. M. (2009). Control and protection of power electronics interfaced distributed generation systems in a customer-driven microgrid. *IEEE Power and Energy Society General Meeting, 2009, PES 09*, pages 1–8. 94

Pipattanasomporn, M., Feroze, H., and Rahman, S. (2009). Multi-agentsystemsin a distributed smart grid: Design and implementation. *Proc IEEE Power Systems Conf. and Expo.* 95

Poor, H. (1994). *An Introduction to Signal Detection and Estimation*. New York: Springer-Verlag, second edition. 44

Rokrok, E. and Golshan, M. E. H. (2010). Adaptive voltage droop scheme for voltage source converters in an islanded multi-bus microgrid. *IET,Generation, Transmission & Distribution*, 4:562–578. 94

Savkin, A. V. and Evans, R. J. (2002). *Hybrid Dynamical Systems: Controller and Sensor Switching Problems*. Birkhauser, Boston, MA. 52, 56

Schenato, L. (2008). Optimal estimation in networked control systems subject to random delay and packet drop. *IEEE Transactions on Automatic Control*, 53(5):1311–1317. 10

Seatzu, C., Corona, D., Gina, A., and Bemporad, A. (2006). Optimal control of continuous-time switched affine systems. *IEEE Transactions On Automatic Control*, 51(5). 57

Sekercioglu, Y. A., Ivanovich, M., and Yegin, A. (2009). A survey of mac based qos implementations for wimax networks. *Computer Networks*, 53:2517–2536. 38

Shi, Q., Comaniciu, C., and Agrawal, P. (2009). A prioritized mac game framework for event reporting in sensor networks. *Proc. of International Conference on Game Theory for Networks*, pages 559–564. 39

Shieh, L., Wang, H., and Yates, R. (1980). Discrete-continuous model conversion. *Applied Mathematical Modelling*, 4:449–455. 54

Smartgrid.gov (2012). the gateway to information on federal initiatives that support the development of the technologies, policies and projects transforming the electric power industry. [online]. available: http://www.smartgrid.gov. 37

Song, J., Han, S., Mok, A., Chen, D., Lucas, M., and Nixon, M. (2008). Wirelesshart: Applying wireless technology in real-time industrial process control. In *Real-Time and Embedded Technology and Applications Symposium, 2008. RTAS '08. IEEE*, pages 377–386. 9

Sontag, E. (1998). *Mathematical Control Theory: Deterministic Finite Dimensional Systems*. Springer, Boston, MA, second edition. 59

Stoer, M. (1991). *Design of Survivable Networks*. 71

Sztipanovits, J., Koutsoukos, X., Karsai, G., Kottenstette, N., Antsaklis, P., Gupta, V., Goodwine, B., Baras, J., and Wang, S. (2012). Toward a science of cyber-physical system integration. *Proceedings of the IEEE*, 100(1):29 –44. 8

Tan, Y., Vuran, M., and Goddard, S. (2009). Spatio-temporal event model for cyber-physical systems. In *29th IEEE International Conference on Distributed Computing Systems Workshops (ICDCS Workshops '09)*, pages 44 –50. 3

Tropp, J. and Gilbert, A. (2007). Signal recovery from random measurements via orthogonal matching pursuit. *IEEE Trans. on Information Theory*, 53(12):4655–4666. 16, 28

Truetime (2012). http://www3.control.lth.se/truetime/. 95

Tsaig, Y. and Donoho, D. L. (2006). Extensions of compressed sensing. *Signal Processing*, 86:533–548. 16

Ulusoy, A., Gurbuz, O., and Onat, A. (2011). Wireless model-based predictive networked control system over cooperative wireless network. *IEEE Transactions on Industrial Informatics*, 7(1):41–51. 8

Vaccaro, A., Villacci, D., Osborne, M., Fitch, J., Cai, D., and Terzija, V. (2010). The role of cooperative sensor networks in wide area power systems communication. *Developments in Power System Protection (DPSP 2010)*, pages 1–5. 52

Van der Schaft, A. and Schumacher, H. (1998). Complementarity modeling of hybrid systems. *IEEE Transactions on Automatic Control*, 43(4):483–490. 57

Vu, H. L., Chan, S., and Andrew, L. L. H. (2010). Performance analysis of best-effort service in saturated ieee 802.16 networks. *IEEE Transactions on Vehicular Technology*, 59(1). 38

Wang, W., Garofalakis, M., and Ramchandran, K. (2007). Distributed sparse random matrix projections for refinable approximation. *Proceedings of International Coference on Information Processing in Sensor Networks (IPSN)*. 17

Wang, W., Xu, Y., and Khanna, M. (2011). A survey on the communication architectures in smart grid. *Computer Networks*, 55:3604–3629. 93

Wang, Y., Vuran, M. C., and Goddard, S. (2008). Cyber-physical systems in industrial process control. *SIGBED Rev.*, 5(1):12:1–12:2. 8

Welch, G. and Bishop, G. (1995). An introduction to the kalman filter. Technical Report TR 95-041, University of North Carolina at Chapel Hill. 58

Wen, J. Y., Wu, Q. H., Turner, D. R., Cheng, S. J., and Fitch, J. (2004). Optimal coordinated voltage control for power system voltage stability. *IEEE Transactions on Power Systems*, 19(2). 38, 39, 40

Wu, F., Kao, Y., and Tseng, Y. (2011). From wireless sensor networks towards cyber physical systems. *Pervasive and Mobile Computing*. 2, 7, 8

Wu, F., Moslehi, K., and Bose, A. (2005). Power system control centers: past, present, and future. *Proceedings of the IEEE*, 93(11):1890–1908. 2

Xia, F. (2008). Qos challenges and opportunities in wireless sensor/actuator networks. *Sensors*, 8(2):1099–1110. 7, 10

Xia, F., Ma, L., Dong, J., and Sun, Y. (2008). Network qos management in cyber-physical systems. In *International Conference on Embedded Software and Systems Symposia, 2008. ICESS Symposia'08*, pages 302–307. IEEE. 9

Yan, Y. and Qian, Y. (2012). A survey on smart grid communication infrastructures: motivations, requirements and challenges. *IEEE Communications Surveys Tutorials*, pages 1–16. 7, 93

Yang, T. (2006). Networked control system: a brief survey. In *Control Theory and Applications, IEE Proceedings-*, volume 153, pages 403–412. IET. 7

Ye, J. C. (2007). Compressed sensing shape estimation of star-shaped objects in fourier image. *IEEE Signal Processing Letters*, 14:750–753. 17

Zhang, L. and Hristu-Varsakelis, D. (2005). Lqg control under limited communication. *Decision and Control, 2005 and 2005 European Control Conference. CDC-ECC '05, 44th IEEE Conference on*, pages 185–190. 59

Zhang, W., Branicky, M., and Phillips, S. (2001). Stability of networked control systems. *IEEE Control Systems Magazine*, 21(1):84–99. 10

Zhang, W., Tang, J., Wang, C., and De Soysa, S. (2010). Reliable adaptive multipath provisioning with bandwidth and differential delay constraints. In *INFOCOM, 2010 Proceedings IEEE*, pages 1–9. 10

Appendix

.1 Proof of Proposition 1

Proof. It has been shown in Donoho (2006, 2004) that optimizations P1 and P0 are equivalent if the following conditions about $\mathbf{\Phi}$ are satisfied, where J is an arbitrary subset of $(1, ..., m)$:

- C1: The minimum singular value of $\mathbf{\Phi}_J$ is larger than η_1 uniformly for J satisfying $|J| < \rho_1 n$;
- C2: $\|\mathbf{v}\|_1 \geq \eta_2 \sqrt{n} \|\mathbf{v}\|_2$ uniformly for J satisfying $|J| < \rho_2 n$, where $\mathbf{v} = \mathbf{\Phi}_J \mathbf{x}_J$;
- C3: $\|\mathbf{x}_{J^c}\|_1 \geq \eta_3 \|\mathbf{v}\|_1$ uniformly for J satisfying $|J| < \rho_3 n$, where $\mathbf{v} = -\mathbf{\Phi}_{J^c} \mathbf{x}_{J^c}$.

We check the conditions C1–C3, separately. Throughout the proof, we assume that $J = \{1, 2, ..., k\}$, without loss of generality.

We first check condition C1. The proof follows the argument of Lemma 3.1 in Donoho (2004). We define

$$R_i = \left(\frac{1}{n} \sum_{j=1}^{n} Z_{ij}^2 \right)^{\frac{1}{2}},$$

where $\{Z_{ij}\}$ are independent and identically distributed standard Gaussian random variables, being independent of $\mathbf{\Phi}$. Let $\mathbf{R} = \text{diag}\left(\left\{ \frac{R_i}{\|h_i\|} \right\} \right)$ and $\mathbf{X} = \mathbf{\Phi}\mathbf{R}^{-1}$. Then, we have

$$\lambda_{\min}\left(\mathbf{\Phi}_J^T \mathbf{\Phi}_J\right) \geq h_{\min}^2 \lambda_{\min}\left(\mathbf{X}_J^T \mathbf{X}_J\right) \left(\max_i R_i\right)^{-2},$$

where we applied the assumption that $\|h_i\| \geq h_{\min}$. The subsequent argument is the same as that of Donoho (2004).

Next, we check condition C2. By applying the assumption that $h_{ij} \geq h_{\min}$, for any vector $\alpha \in \mathbb{R}^{|J|}$, we have

$$\begin{aligned}
& \|\mathbf{\Phi}_J \alpha\|_1 \\
= \; & \|\mathbf{H}_J \circ \mathbf{S}_J \alpha\|_1 \\
= \; & \sum_i \left| \sum_j \mathbf{H}_{ij} \left(\mathbf{S}_J\right)_{ij} \alpha_j \right| \\
\geq \; & h_{\min} \sum_i \left| \sum_j \left(\mathbf{S}_J\right)_{ij} \alpha_j \right| \\
= \; & h_{\min} \|\mathbf{S}_J \alpha\|_1 .
\end{aligned}$$

Following the same argument as in Donoho (2004), we can show that C2 also holds.

Finally, we check condition C3. Similar to Eq. (5.4) in Donoho (2004), we set the following linear programming problem:

$$\min_{\delta_{J^c}} \|\mathbf{h}_{J^c} \circ \delta_{J^c}\| , \qquad \text{s.t. } \mathbf{\Phi}_{J^c} \delta_{J^c} = -\mathbf{v}. \tag{1}$$

Applying the assumption that $h_{ij} \leq h_{\max}$, we have

$$\|\delta_{J^c}\| \geq \frac{1}{h_{\max}} \|\mathbf{h}_{J^c} \circ \delta_{J^c}\| . \tag{2}$$

It is easy to check that the dual linear programming of (1) is the same as that in Donoho (2004).

Then, by applying Lemma 5.1 in Donoho (2004), we have shown that condition C3 holds with probability 1 as $n, m \to \infty$. This concludes the proof. □

.2 Proof of Proposition 2

Proof. The proof is the same as that of Theorem 3.1 in Donoho et al. (2006a) before the optimization problem (3.9) in Donoho et al. (2006a). We define $\mathbf{G} = \mathbf{\Phi}^T \mathbf{\Phi}$. The

constraint $\|\mathbf{\Phi w}\|_2^2 \leq \Delta^2$, where $\Delta \triangleq \delta + \epsilon$, implies

$$\begin{aligned}
\frac{1}{\gamma_{\max}} &= \frac{\Delta^2}{h_{\max}^2} \\
&\geq \frac{\mathbf{w}^T \mathbf{G} \mathbf{w}}{h_{\max}^2} \\
&= \|\mathbf{w}\|_2^2 - \mathbf{w}^T \left(\frac{1}{h_{\max}^2} \mathbf{G} - \mathbf{I} \right) \mathbf{w} \\
&\geq \|\mathbf{w}\|_2^2 - |\mathbf{w}|^T \left| \frac{1}{h_{\max}^2} \mathbf{G} - \mathbf{I} \right| |\mathbf{w}| \\
&\geq \|\mathbf{w}\|_2^2 - M \, |\mathbf{w}|^T \, |\mathbf{1} - \mathbf{I}| \, |\mathbf{w}| \\
&- |\mathbf{w}|^T \, (\mathbf{1} - f)\mathbf{I} \, |\mathbf{w}| \\
&= (M + f) \, \|\mathbf{w}\|_2^2 - M \, \|\mathbf{w}\|_1^2 \, . \qquad (3)
\end{aligned}$$

The following argument remains the same as that in Donoho et al. (2006a). Then, the condition (3.17) in Donoho et al. (2006a) becomes

$$(f + M)V - M\mu V \leq \frac{1}{\gamma_{\max}}. \qquad (4)$$

This concludes the proof. □

Vita

Rukun Mao was born in 1984 in Changsha, China. In September 2002, he embarked on a train heading north to Beijing, where he attended Beijing Institute of Technology. He received B.S. and M.S. degrees from the university in 2006 and 2008 respectively, both in Electrical Engineering. In August 2008, he came to US and landed at Knoxville, starting his PhD study at The University of Tennessee at Knoxville. Wireless Communication has been his research topic. He is on track to receive his PhD in Electrical Engineering in August 2013. After graduation, he will join Qualcomm in San Diego, and continues to work in the field of communication system.