Report: NSF Workshop on Future Wireless Communication Research

List of Community Participants

Ian Akyildiz, *Georgia Institute of Technology*
Matthew Andrews, *Bell Laboratories, Alcatel-Lucent*
Victor Bahl, *Microsoft Research*
Hari Balakrishnan, *Massachusetts Institute of Technology*
Suman Banerjee, *University of Wisconsin-Madison*
Elizabeth Belding, *University of California, Santa Barbara*
Randy Berry, *Northwestern University*
Milind Buddhikot, *Bell Laboratories, Alcatel-Lucent*
Mung Chiang, *Princeton University*
Romit Roy Choudhury, *Duke University*
Hesham El-Gamal, *Ohio State University*
Atilla Eryilmaz, *Ohio State University*
Joe Evans, *The University of Kansas*
David Goodman, *Polytechnic Institute of New York University*
Ramesh Govindan, *University of Southern California*
Marco Gruteser, *Rutgers University*
Yih-Chun Hu, *University of Illinois at Urbana-Champaign*
Tara Javidi, *University of California, San Diego*
Dina Katabi, *Massachusetts Institute of Technology*
Sachin Katti, *Stanford University*
Srinivasan Keshav, *University of Waterloo*
Edward Knightly, *Rice University*
Yingbin Liang, *University of Hawaii*
Xiaojun Lin, *Purdue University*
Xin Liu, *University of California, Davis*
Eytan Modiano, *Massachusetts Institute of Technology*
David Molnar, *Microsoft Research*
Jung-Min Park, *Virginia Tech*
Jon Peha, *Carnegie Mellon University*
Radha Poovendran, *University of Washington*
Dipankar Raychaudhuri, *Rutgers University*
Ashutosh Sabharwal, *Rice University*
Anant Sahai, *University of California, Berkeley*
Saswati Sarkar, *University of Pennsylvania*
Srinivasan Seshan, *Carnigie Mellon University*
Sanjay Shakkottai, *University of Texas at Austin*
Ness Shroff, *The Ohio State University*
Doug Sicker, *Colorado State University*
Raghupathy Sivakumar,*Georgia Institute of Technology*
R. Srikant,*University of Illinois at Urbana-Champaign*
Peter Steenkiste, *Carnegie Mellon University*
Lang Tong, *Cornell University*
Don Towsley, *University of Massachusetts*
Patrick Traynor, *Georgia Institute of Technology*
David Tse, *University of California, Berkeley*
Nitin Vaidya, *University of Illinois at Urbana-Champaign*
Gustavo de Veciana, *University of Texas at Austin*
Jean Walrand, *University of California, Berkeley*
David Wetherall, *University of Washington*
Roy Yates, *Rutgers University*
Lei Ying, *Iowa State University*
Junshan Zhang, *Arizona State University*
Heather Zheng, *University of California, Santa Barbara*

Government Agency Personnel

Alhussein Abouzeid, *National Science Foundation*
Robert Bonneau, *The Air Force Office of Scientific Research*
Michael Branicky, *National Science Foundation*
Sajal Das, *National Science Foundation*
Darleen Fisher, *National Science Foundation*
Victor Frost, *National Science Foundation*
Mohamed Gouda, *National Science Foundation*
Krishna Kant, *National Science Foundation*
Jon Peha, *Federal Communications Commission*
Larry Stotts, *Defense Advanced Research Projects Agency*
Ty Znati, *National Science Foundation*
Lenore Zuck, *National Science Foundation*

Table of Contents

1. Introduction

The wireless communication industry is a trillion-dollar, worldwide business that represents a substantial fraction of the global Gross Domestic Product. Over the past two decades, it has had a transformative impact on our society and has revolutionized almost all aspects of human interaction. These networks are inescapably intertwined with the very fabric of both civilian and military environments, and their continued growth and well-being is critical to the success and health of our nation. Nonetheless, with continued improvements in spectrum utilization, resource allocation, hardware, device miniaturization, and development of new renewable energy sources, we find ourselves still very much in the infancy of the development of these systems, with the potential to grow and becoming orders-of-magnitude more sophisticated.

The following are but a few examples of the potential of wireless networks. The ability to sense and control one's environment via a complex array of inexpensive sensor networks capable of distributed computation will result in significant improvements in quality of life, especially for individuals who need assistance due to disabilities, illness, or age. Sensors equipped with renewable batteries and rapidly deployable ad hoc wireless networks will also change the way warfare is conducted, resulting in significantly reduced casualties, especially in urban warfare settings. Multi-hop wireless mesh networks will enable ultra high-speed communications to the home and car, fueling new, high-resolution, multimedia services currently considered science fiction. Finally, sensing, computing, and communication capabilities over static and mobile platforms has the potential for better coordination, early warning, and remote operations that could help save countless lives.

Moving forward, it is important for the community and the National Science Foundation to have a broad vision of the key challenges and application areas of wireless networks and systems. To that end the NSF Workshop on Future Wireless Communication Networks was held on November 2-3, 2009 in Arlington Virginia. Critical challenges in wireless networking were discussed, and a vision for conducting fundamental and inter-disciplinary research in this area was articulated.

2. Workshop Objectives

The overarching goal of the workshop is to help chart a broad vision for the future of wireless research. At the workshop, attendees discussed and debated the critical challenges in wireless networking, and articulated a vision for conducting both fundamental and inter-disciplinary research in the area. The workshop participants were clearly briefed on the goal of the workshop. They were explicitly informed that the goal of the workshop is not to end with intellectual discussions, but rather to work as a team to create a common vision of the area that is presented to the community in the form of a report.

This report has been written with the intention of (i) identifying major issues affecting future wireless research; (ii) exposing the research community to new and exciting inter-disciplinary problems; and (iii) stimulating far reaching future research initiatives, and collaborations that would help along the evolution of the wireless research community.

The focus areas in this report are:

- Network Control and Algorithms
- Wireless Architecture
- Wireless Systems Research in 2020
- Information-theoretic Security
- Cognitive Radio and Dynamic Spectrum Access

3. Workshop Participants, Guidelines, and Program

From the outset the goal was to arrange a workshop where the attendees represented a broad spectrum of the community at large. In the spirit of inclusiveness, which is the hallmark of the National Science Foundation, diversity was emphasized in a variety of different forms. This was felt important not only from the point of view of ensuring fairness, but also to ensure that the best ideas are allowed emerge.

The following general guidelines were used to invite attendees.

1. An organizing committee was formed by the co-chairs (Knightly and Shroff). This organizing committee was made up of two thrust leaders per research thrust area. The members of the organizing committee were:

    a. Wireless Systems Research in 2020: Dina Katabi (Massachusetts Institute of Technology) and Suman Banerjee (University of Wisconsin, Madison)
    b. Cognitive Radio Networks and Dynamic Spectrum Access: Xin Liu (University of California, Davis) and Peter Steenkiste (Carnegie Mellon University)
    c. Architectures and Emerging Technologies: Sanjay Shakkottai (The University of Texas at Austin) and David Wetherall (University of Washington)
    d. Wireless Networking Security: Hesham El Gamal (The Ohio State University) and Yih-Chun Hu (University of Illinois at Urbana-Champaign)
    e. Network Control and Algorithms: R. Srikant (University of Illinois, Urbana Champaign) and Jean Walrand (University of California, Berkeley).

2. The organizers were charted to invite the attendees to the workshop. The participants at the workshop were very diverse and represented a broad spectrum of the community including:

    a. Theorists, experimentalists, and protocol designers.
    b. Core wireless researchers as well as researchers from other application areas and disciplines.
    c. Junior, mid-level, and senior researchers will be invited to the workshop.
    d. Under-represented groups.

3. Participants were specifically instructed at the workshop that our role was to work as a team to create a vision that is presented to the community in the form of a report.

4. Thinking about large, far reaching problems, beyond the individual participants' own research areas was strongly encouraged.

5. A group of researchers (Ian Akyildiz, Victor Bahl, David Goodman, Don Towsley) were requested to provide feedback to the participants in the form of the panel to be held on the second day of the workshop.

6. The structure of the workshop was as follows (The detailed program is provided in the Appendix).

    After opening remarks from the workshop co-chairs (Ness Shroff and Edward Knightly) and NSF personnel (Alhussein Abouzeid and Ty Znati), the session co-chairs of each session were asked to present their vision and a straw-man outline of the important research in their respective areas.

Following these presentations, there was a working lunch during which talks were given by Robert Bonneau, AFOSR; Larry Stotts, DARPA; and Jon Peha, FCC which provided additional research ideas and possibilities that the participants could discuss during the group by group breakout sessions in the afternoon. The afternoon was spent by each group in their breakout sessions, and preliminary results of their discussions and deliberations were presented in the evening to the entire workshop to allow for cross-fertilization. The participants received feedback from the panelists on the second day of the workshop and the rest of the time at the workshop was spent in further deliberations and refining the vision for each focus area.

4. Network Control & Algorithms

A fundamental goal in wireless networking is the provision of ubiquitous, high-speed Internet access. Its realization can enable exciting future applications that will impact a broad range of important areas of our lives such as health-care, employment, and entertainment. Several key techniques have been identified towards the realization of this goal: i) employing architectures of dense and small cells, to increase the area spectral efficiency, ii) multi-hop relaying, to increase the network coverage and availability while reducing costs, and iii) information-theoretic solutions to boost channel capacity.

One key component of the wireless revolution, that is multi-hop wireless architectures, has experienced severe difficulties. Until recently, the conventional wisdom suggested that multi-hop networks generally perform poorly in practice, and that connections longer than three hops yield near-zero throughput. Consequently, after years of funding research on wireless sensor and ad-hoc networks, the focus was redirected. Researchers have now been talking of networked sensors, instead of sensor networks. MAC protocols and ad-hoc networks have been considered by many as areas with no challenges. The industry's path has been parallel. Many startups deploying mesh networks have failed, deployments of mesh networks were discontinued and only a few commercial multi-hop wireless products are available. A major factor for the above pessimistic outlook has been the poor handling of interference by existing distributed algorithms for scheduling and resource allocation. As a result, the achievable network throughput is only a small fraction of the one the network can actually support. Moreover, the theory of distributed resource allocation algorithms hasn't offered much beyond the existing practical state-of-the-art. Thus, there seems to be a wide gap between the vision for revolutionizing the societal impact of wireless networks and the seemingly slow advancement in the state-of-the-art.

There have been some encouraging recent theoretical breakthroughs: i) the acquisition of a deeper understanding of interference in wireless networks, ii) the proposal of lightweight distributed algorithms that are not demanding in terms of control messaging, and iii) the development of an optimization-based theory that incorporates cross-layer and architectural perspectives. These recent results are promising enough to motivate new research that can convert the above pessimistic climate, and enable--after decades of painstaking attempts--ubiquitous broadband access. While these recent breakthroughs are fundamental, they have been developed somewhat independently of each other. Thus, the time is right to explore the interaction between them and develop a novel unifying theoretical framework for wireless network control and algorithmic design. Substantial progress is not only required in further theoretical advances, but also in experimental evaluation of network control algorithms.

4.1 Applications

We classify the motivated research into the following complementary areas:

4.1.1 Interference Management

Fundamental research in the area of communication networks and information theory has yielded significant results in the past, both in terms of leading to a better understanding in network design, as well as influencing the industrial development of new products and services. This includes results in LDPC coding, successive interference cancellation and MIMO antenna systems, which have tremendously boosted the capacity of wireless networks. For example, new coding techniques have approached the fundamental limits of compression and information-theoretic capacity and are currently employed in cell phones, flash memory and magnetic storage devices. Another example, multiple antenna systems (MIMO) is a major topic of research in information theory, since the 1990s. This sustained research initiative has resulted in the use of multiple antennas in every conceivable type of radio network, such as cellular, LAN and WAN networks. Finally, a counter-intuitive idea in information theory advocates that in high interference regimes, signal decoding can be as efficient as in low interference regimes. There, successive interference cancellation techniques suggest that receivers can first decode the interferer, subtract his signal from the one received and then decode the desired signal.

However, after 40 years of research in network information theory, novel ideas have emerged for interference management: the capacity of interference channels can be computed within one bit of their capacity, and interference alignment schemes can exploit all of the “degrees of freedom” for high SNR regimes. While information theory widely considers topological building blocks, such as a single transmitter, receiver and interferer, these insights motivate further research on network-wide algorithmic design. Another implication for network control and algorithmic design, both traditional and novel information theoretic concepts can be jointly considered with higher layer information, so that efficiency is increased.

4.1.2 Scheduling and Resource Allocation

A key focus area in the design of algorithms for network control is the development of distributed algorithms that are able to maximize network capacity and minimize delay. Traditional opportunistic scheduling has been proposed in the past, to address fairness provision, throughput maximization, or a combination thereof. Their key ideas advocate that each user's channel rate should be weighted by a quantity such as the queue length, delay or a fairness metric, and the user with the highest such metric should be scheduled. This algorithm has been implemented to deliver data in 3G cellular networks, and has also been discussed for adoption in satellite networks. The idea has also been the staple for many scheduling variations, in switching fabrics of Internet routers.

While “max-weight” scheduling is practical for single-hop networks, as those mentioned above, the problem become extremely complex for multi-hop networks, an application where performance still remains unsatisfactory. Recently, a new understanding has emerged that indicates how to solve--even sub-optimally--certain versions of the generally NP-hard scheduling problem. This has resulted in the development of low-complexity distributed algorithms by making connections to related *spin glass* models traditionally used for statistical mechanics. In addition, the recent advances in interference management suggest that cross-layer scheduling designs driven by information-theory can further enhance network performance. Future research can also tremendously improve the performance of multi-hop networks, by focusing on practical implementations and experimental evaluation of low-complexity scheduling algorithms.

4.1.3 Optimization in Stochastic Networks

While traditional scheduling objectives focus on maximizing the network's capacity region, more broad objectives can be addressed with a suite of network optimization problems. An optimization framework for stochastic networks has emerged for solving a variety of resource allocation problems. This framework answers fundamental architectural questions and provides a functional decomposition to achieve fair resource allocation in wireless and wired networks. We note that optimization-based techniques have led to the design of TCP protocols for future ultra-high-speed Internet and inspired enterprise-networking companies. Also, rate control in EVDO, the data transfer standard in 3G networks, relies on such a principle.

In Sec. 4.1.2, we discuss how future research within the area of control and algorithmic design can increase the network capacity region by designing amenable to implementation, cross-layer scheduling algorithms of low-complexity. We extend the set of applications in this domain, by incorporating optimization techniques to such designs. As a result, a significantly wider set of objectives can be addressed, such as delay, fairness, etc. These enhancements promise to tremendously enhance the end-user experience.

4.1.4 Enabling a Wide Range of Network Services

The above mentioned applications target a system model with either static clients or with limited mobility. It is assumed that the network-to-client connectivity is maintained for a substantial amount of time. However, supporting mobility is a fundamental requirement for providing quality service to network users. Under such a scenario, the prior assumption no longer holds. We readdress the considered problems, for high-mobility scenarios.

In addition, algorithmic design can be the focus for providing a wide range of network services, in general. For example, resource allocation decisions can aid in transparent usage of multiple heterogeneous networks and technologies, aka virtualization. Furthermore, pricing algorithms can enable prioritized Internet access and provision of QoS.

4.2 Challenges & Opportunities

In this section, we outline major challenges in developing a cohesive theory of network control and algorithms, for the future's wireless networks.

4.2.1 Interference Management

Information collection: In Sec. 4.1.1, we explain why interference should not always be treated as an origin of performance degradation. However, significant effort is required to realize the ideas for interference management in practice. For example, accurate channel state information is essential to the implementation of such schemes. In an network with n nodes, this may require up to n^2 pieces of information. It is a challenge to timely collect and disseminate this amount of information, which combined with control messaging overhead can quickly oversaturate the network.

Cross-layer design: The state-of-the-art in distributed MAC algorithms considers simplistic ON-OFF models. Control theoretic approaches widely assume a *slotted* time model and therefore synchronization between nodes, which is hard to attain in multi-hop networks. However, asynchronous MAC schemes yield location-dependent phenomena in practice with severely detrimental effects on performance, such as hidden terminals. Thus, it is imperative to develop new resource allocation algorithms which incorporate more realistic representations of the PHY-layer. In addition, the delay performance of such algorithms requires further study; theoretical predictions suggest very poor delay performance, but simulations are more optimistic for light and moderate traffic regimes. Ideally, experimental evaluation, under actual channel and interference conditions, can yield important insights.

Support for novel architectural designs: While many of the recent developments in wireless network control and algorithms have been motivated by ad-hoc networks, cellular networks are still by far the largest carriers of traffic. Next-generation cellular network designs suggest the adaptation of ideas similar to several in ad-hoc networking. For example, 4G networks employing LTE standards are envisioned to be partitioned in small cells, to constitute a dense deployment, and to enable selfconfiguration, e.g., of channel assignments. Such a design generates substantial interference between clients. It is a challenge to propose distributed algorithms for resource allocation and interference management, that are suitable for such novel architectural environments, that are a mix of dense and cellular architectures.

4.2.2 Scheduling and Resource Allocation

Flow size-dependent design: The majority of all the proposed scheduling algorithms rely on queue length information, as an indicator of local congestion. However, recent developments in cellular networks suggest that queue-length information is not necessarily an indicator of congestion, if traffic flows are of small size. How does one account for such short flows which, in fact, make up the vast majority of Internet sessions, even though they contribute to a small fraction of the traffic volume?

Experimentation: A significant obstacle in research and development of scheduling algorithms is the limited number of testbeds that are employed for validating and evaluating new ideas. The wireless industry adopts many concepts developed in academia, hence it could be argued that commercial wireless networks constitute the ultimate testbeds. However, researchers have no access to them and companies rarely ever dispose any measurement data, mostly for reasons of competition. Therefore, the widespread prevalence of experimental testbeds is of extreme importance in evaluating novel algorithms under realistic channel and interference conditions.

Compressed sensing: Compressed sensing is a methodology used to identify the key features of complex data. This methodology has the potential of compressing the description of the state of the network both during acquisition and transmission. Compressed sensing can reduce the amount of information that must be exchanged over the network. This is of extreme interest, not only for sensor networks, but also for any network that diffuses overhead related to network conditions to enhance distributed resource allocation. It is a challenge to devise distributed compressed sensing schemes that are suitable for specific wireless architectures.

4.2.3 Optimization in Stochastic Networks

From layered to cross-layer architectures: The functions of the Internet are organized in layers of peer protocol entities. For instance, routers and end hosts run distributed routing algorithms to determine the path of packets to a given destination. In this architecture, the layers are isolated; routing decisions are irrelevant to congestion and to the user's application. Recently developed algorithms for ad-hoc wireless networks and also for wired networks do not employ this decomposition. Instead, each node makes a decision of what packet to send to which neighbor based on local information about congestion and link rates. Functions are coupled in each node, instead of being organized in layers. In a sense, the architecture is cross-layer. However, such schemes have not been implemented in practice. Research in layer-free architectures raises important issues of compatibility, extensibility and realizability. It is a challenge to formally standardize protocols and architectures that enable in practice the transition from layered to cross-layer design.

Heterogeneous applications: The modern theory of network optimization considers applications that have different utilities for the throughput of their packet stream. However, models that combine applications with different latency/throughput requirements are still missing.

Heterogeneous networks: The optimization framework focuses in a single architecture at a given time. As we discuss next (Sec. 5), virtualization techniques will support in the future transparent utilization of multiple heterogeneous architectures and technologies. It is a challenge to redesign this cross-layer framework, so that it can enable optimization over multiple stochastic networks, with heterogeneous system models and employed protocols or technologies.

4.2.4 Enabling a Wide Range of Network Services

Virtualization: Network researchers envision a software-defined network where users can request different services such as a secure, a low-latency slice, or a best-effort option. Such virtualization techniques can enhance client access but they also come at an increased cost in terms of efficiency (reduced statistical multiplexing gain) and complexity (programmable routers have limited capabilities). It is a challenge to devise algorithms for such a transparent resource allocation and to identify the conditions under which this direction is of overall benefit for the network. Moreover, pricing the general classes of resources constitutes a further challenge.

Self-organization: Up until the third generation of cellular networks, most of their critical operations such as frequency planning, power management, neighbor-listing, etc.,. were conducted by centralized entities. For 4G systems such as LTE, the numerous dense cells render such centralized operations prohibitively expensive. Research is critically needed in algorithmic design to enable the components of a cellular network to configure themselves, either by sensing the wireless environment directly or by exchanging local information with their immediate neighbors.

Mobility: As of today, high user mobility is a detrimental factor towards supporting applications with stringent delay requirements. Still, elastic applications, which are tolerant to disruptions of communication, can be supported. Hence, optimization for highly mobile systems should be aware of the inherent performance limitation, that are induced by mobility. It should target appropriate objectives by following different problem formulations than traditional approaches.

Pricing: As of today, Internet access is not subject to distinct QoS provisioning between different clients or sessions, assuming that they share the same resources. A fundamental reason for this is the lack of pricing mechanisms. These should also be robust enough to price resources depending on their state of utilization at very short time scales.

5. Research Directions in Wireless Architectures

As the usage and density of wireless networks continues to explode, commensurate advances in the architecture of wireless networks are needed to simultaneously cope with the increasing demand and enhance the quality of service for users. A fundamental goal is that wireless architectures provide universal wireless communications to users at high-speeds, in all places and at low cost. Realizing this goal is instrumental for many vital future applications and services. One example of those is vehicular networking that enables cars to communicate with other cars and infrastructure such as lights or signs. Another example consists of cyber-physical systems in which computers interact with the environment via wireless networks.

The above-mentioned goal of low-cost, universal broadband access is far from being met with today's architectures. High-speed performance can only be achieved at small scale, e.g., 802.11 links employing MIMO technologies. However, as links contend with each other, their concurrent activation does not guarantee network-wide high performance. Emerging technologies, such as 60GHz, also enable high-speed point-to-point links, but not multi-user systems. While cellular approaches, such as LTE, can achieve the latter, this is achieved at a tremendous cost, owing to exclusive spectrum purchases and the infrastructure's operational costs. Thus, none of these technologies enables high-speed *and* low-cost ubiquitous wireless access.

Apart from satisfying the long-standing imperatives to “go faster and cheaper,” future wireless architectures must address two further challenges, so that a rich mix of wireless technologies and applications is supported. Neither of these challenges is met by existing architectures:

- *Foster innovation of network technologies.* The success of 802.11 and other technologies notwithstanding, novel wireless technologies are expected to emerge at a rapid pace, in response to tomorrow's applications and capabilities of hardware and PHY-layer. Such new forms of wireless technologies should coexist with their preceding counterparts. They should also support communication at different spatial and mobility scales, as their scope is not simply deteriorated in provision of Internet access, but also includes efficient local, peer-to-peer wireless networking. Such architectures can enable emerging applications (e.g., smart homes), which can also be truly mobile rather than nomadic (e.g., inter-vehicle networking).

- *Efficient operation for a diverse mix of applications.* Spectral efficiency is a traditional requirement of wireless architectures, especially when their access is limited to scarce spectrum. Recent trends in mobile client access recognize energy efficiency as an additional constraint for realizing efficient, sustainable computing. It is a challenge to support these two notions of efficiency while addressing a wide variety of delay and throughput objectives. In addition, it is even more challenging to also consider operation under imperfect estimation of time-varying network conditions.

5.1 Applications

To address the above-mentioned challenges, it is instrumental to conduct research in the following complementary areas:

5.1.1 Coordination and Co-existence

First, it is of key importance for enabling innovation in wireless systems to support coexistence of different networks and technologies that share spectrum in overlapping coverage areas. A compelling example of flourishing innovation via coexistence is the utilization of the ISM bands. The ISM bands can currently be used by multiple heterogenous devices such as WLANs and Bluetooth headsets and are regulated by FCC rules. This model has been tremendously successful, but it only provides a simplistic sharing scheme. Meanwhile, there is demand for other forms of coexistence such as secondary usage of TV white spaces. Emerging radio technologies such as interference cancellation allow us to envision fundamentally different sharing paradigms which can lead to orders-of-magnitude increase in performance. Unfortunately, prior research on coordination and coexistence is limited to preliminary cognitive radio system design and resource allocation in wired networks. We have barely scratched the surface of the necessary research for coexistence of multiple co-located wireless networks, which can be heterogeneous in both hardware and protocols.

In the related literature, design of cognitive radio networks addresses spectrum sharing and coexistence, e.g., as in the DARPA XG program. We recognize two key properties of such designs that are considered to be incorporated in any future research on coexistence. First, cognitive radio networks typically rely on assessment of local spectrum availability. Second, they enforce policies that ensure radios' adherence to local rules for spectrum access. Sharing the bandwidth of a wired backbone is another related area, however it fundamentally differs in nature from network coexistence in a wireless environment. Nevertheless, such wired paradigms provide basic principles for coexistence algorithms, policing, signaling and isolation. Those paradigms primarily consist of congestion control techniques that distribute bandwidth to elastic applications with distinct demands. For QoS-sensitive applications, explicit signaling is employed to coordinate bandwidth allocation, as well as user-isolation techniques.

5.1.2 Virtualization

Research in coordination and coexistence can be complemented by a parallel study on virtualization of wireless resources and network interfaces. In the past couple of years, handsets have become mobile computers running user-contributed applications on potentially open-source operating systems. Hence, we are experiencing a rapid migration towards a more open technological ecosystem than the previously closed and proprietary systems. The greatest winners will be the users, who will have more choices among competing software platforms and devices. Despite being constantly surrounded by abundant wireless capacity originating from multiple, coexisting, heterogeneous wireless networks, it is still a challenge how to best utilize the available resources and access them in a transparent manner.

To enable a more flexible use of wireless infrastructures and resources, we envision the employment of virtualization techniques present in related literature in computer systems and recently in networking. These are related to commercial services (e.g., Multi-Protocol Label Switching Virtual Private Networks, or MPLS VPNs) and network testbeds (e.g., Global Environment for Network Innovations, or GENI). As a result, virtualization yields significant innovation by providing a level of abstraction that enables computer systems to become transparent to the underlying hardware and communication channels. This means that virtual hosting platforms can be decoupled from physical machines. In wireless networking, however, virtualization has not yet included the physical layer. This is due to the legacy of closed and proprietary systems, such as cellular networks, that tend to be vertically defined with a single entity controlling spectrum, equipment and service, and without enabling a flexibility for re-purposing of the individual components.

5.1.3 Efficient Cross-layer Optimization

Traditional network designs are based on a layered network architecture that draws barriers between the individual functionalities of operation, such as power control, coding schemes, medium access, routing, congestion and admission control. Clearly, this modular approach has been very successful in distributed operation of large scale, over-provisioned, and predominantly static networks, including the Internet. Yet it is well-known that this layered design paradigm comes at the cost of significant performance degradation, and is not well-suited for resource-limited and dynamic networks, such as wireless networks. Therefore, a new cross-layer architecture that enables dynamic interaction between the individual network functionalities is necessary. Such interactions are vital to achieve adaptability of the network operation to the varying user demands and physical network conditions, and to therefore maximize performance gains.

The importance of such a cross-layer architecture to the efficient operation of wireless systems has been generally accepted. Nevertheless, only in recent years has a systematic framework been developed which relies on concepts and methods from optimization and stochastic control theory in order to optimize these designs. In particular, dual decomposition techniques and stochastic analysis tools have been extensively employed to develop adaptive, provably optimal, distributed network algorithms for a variety of wireless architectures. It has been shown that the interplay between the network queue lengths and Lagrange multipliers from network optimization problems allows maximization of various network objective metrics while attaining guarantees on queues' stability. Moreover, significant advances have been made towards distributed and low-complexity implementations of such algorithms.

The aforementioned advances in the principled and optimal algorithmic design have significant architectural implications, since they collectively reveal the unifying characteristics of an efficient and distributed wireless architecture. For example, it is observed that global objectives can be optimally achieved by local actions that are supported with limited, but critical information sharing, amongst different network functionalities. Thus, it is essential that the architecture supports such interactions. We acknowledge the need for more research in this direction, to exploit the advantages of a cross-layer network stack, and to maintain a high level of flexibility and robustness.

5.1.4 Sustainability

Calls for sustainable computing in all aspects of information technology are becoming more relevant as computers and data facilities consume a greater and greater fraction of the countries energy budget. Hardware architectures have a major impact on the efficiency with which resources such as materials and electricity are utilized. For example, a system may support a certain architectural upgrade with minor modifications to the given infrastructure as opposed to necessitating an infrastructural re-design and replacement when new technologies become available. Energy efficiency requires that the network architecture and applications can at least monitor, if not manage, the energy consumption in the network. Unfortunately, today's systems fail to achieve this when, for example, existing wireless architectures do not expose their energy-related information to the supported applications.

Substantial advances have taken place in the domain of energy efficiency in mobile devices, such as laptops and smart phones, with battery life being the main focus. Nevertheless, user convenience is often prioritized over sustainability. Moreover, the infrastructure has generally not been considered as part of this equation; for example, power-save modes often aid clients by requiring the infrastructure to be "always-on" and act on their behalf by buffering traffic. The only exception consists of research in sensor network architectures on energy-efficient protocols and mechanisms that extend the network lifetime. A key technique in this work is to transition nodes to "sleep mode" when they are idle. Such architectures differ from those currently providing low-cost, ubiquitous broadband, indicating that energy efficiency is a strong area for future research.

5.2 Challenges and Opportunities

The above applications yield the following challenges and opportunities for future research:

5.2.1 Coordination and Coexistence

Future wireless ecosystems will consist of significantly more diverse wireless technologies than those employed in today's wireless Internet access. These technologies can be operating on dissimilar spatial scales, segregated into licensed spectrum, or dynamically sharing spectrum using cognitive radios. For example, architectures can enable communication between a wide variety of participating nodes, which can range from micro-devices attached to the human body (body networks), to devices integrated with cars, trains, planes, and satellites.

While cognitive radio research has provided some critical first steps towards coexistence, architectures must further address broader issues in spectrum sharing. For example, it is a common practice for cognitive radio networks to model inter-network relationships at the physical layer by accounting for the sensed "interference temperature." However, such interactions cannot capture coexistence relationships under different configurations of the physical layer than those during sensing. Neither can they capture coexistence implications from high layers such as back-offs in the link layer or responses to increased loss rates at the transport layer. These compounded effects can actually result in *significantly* worse performance than interference-driven predictions. To address these issues, we highlight the necessity for future research in the following three areas:

Information collection and coordination protocols. To allow multiple networks to coexist efficiently in a given area, it is instrumental to collect information describing the networks' operational requirements as well as the properties of their RF environment. As of today, this information only consists of channel conditions and the radios' transmission power. It is an open research topic to answer how such information sets should be extended to capture effects from higher layers so that sophisticated and robust sharing policies are enabled. In addition, the practical implementation of information collection schemes also constitutes an open challenge.

Isolation techniques. Coexistence can be supported by improvising methodologies for network isolation. Research towards exploiting or enhancing link directionality, as well as controlling transmission powers across multiple heterogeneous networks can tremendously increase spatial reuse and ameliorate conditions for coexistence. In addition, the effectiveness of isolation techniques is further supported by the agility of future cognitive radios in operating in wide spectral ranges under eventually more flexible FCC policies.

Coexistence behaviors. Today's models for defining coexistence only consider RF link relationships, without accounting for application requirements and interactions above the physical layer. It is a challenge for future work to identify and therefore account for such cross-layer interactions. In addition, future research should transition from link-centric to network-centric coexistence models.

5.2.2 Virtualization

It is an open issue whether architectures can support flexible transitions between heterogeneous wireless subnetworks, so that users can exploit multiple available access options of differing quality and cost. It is a challenge to view the physical infrastructure (hardware and spectrum) as a broad resource, whose parts users can lease commensurately with their needs. Unification of heterogeneous networks in hardware and software implies an interaction between technologies of multiple operators. Hence, an economic study is necessary that advocates virtualization by demonstrating mutual benefits for the individual parties involved.

A key challenge to virtualization lies in enabling multi-network access in a manner transparent to the physical infrastructure. For example, upon purchase of service from a single network provider the provider becomes responsible for allocating physical infrastructure (e.g., hardware and spectrum) for the user. The allocated resources can be a function of the user's requirements and can originate from multiple subnetworks and technologies. Furthermore, spectrum itself could be traded and shipped between physical infrastructure owners, depending on the load they observe in their deployment.

Realizing our vision of virtualization requires solving the following challenges. First, digitizing the entire spectrum is not possible with today's hardware; significant innovation is needed to build adaptive, energy-efficient, wide-band mobile radio hardware. Second, additional innovation is required to exploit non-contiguous pieces of spectrum as a single physical bit-pipe. Finally, innovation is needed to define policies that enable fine-grained spectrum trading. Such policies need to incentivize secondary access of spectrum, facilitate the design of spectrum contracts, and balance competition and cooperation between providers and users.

5.2.3 Efficient Cross-layer Optimization

The development of an efficient and interactive, cross-layer architecture for wireless networks yields multiple challenges:

Heterogeneity. Cross-layer architectures should not only be efficient but also flexible enough to apply to a diverse set of applications and a wide range of wireless systems with different characteristics (e.g. capacity, mobility, etc). So far, promising steps have been taken to incorporate some of these considerations within the optimization-based architecture design methodology described earlier. However, further research in this direction is required to support the framework for heterogeneous environments.

Robustness. Architectures should be robust to modeling imperfections and uncertainties in the system behavior. The key to achieving robustness is the cross-layer nature of the architecture as it allows network algorithms to react to the *experienced* (not the expected) state of the system. It therefore allows the network to recover from unforeseen deviations from expected behavior with a closed feedback loop.

Layer security. The cross-layer network architecture, by design, increases the interactions between traditionally separated network functions. While this is the main source of its efficiency, it may also increase the security vulnerabilities of the network. If, for example, a malicious user influences a component of the network stack, it may signal incorrect information to other architectural components and induce a wide deleterious impact on the network operation. Thus, the security implications of the interactive network architecture require more research to prevent or protect against such vulnerabilities. To address this challenge, worst-case analysis and game theoretic approaches may be employed to quantify the vulnerabilities and to design schemes that are resilient to such selfish or malicious behavior.

Framework redesign. Overall, the above challenges also provide great opportunities for further developing the theoretical framework and the systematic methodologies for efficient and distributed wireless network design. These require an interdisciplinary effort from electrical engineering, computer science, mathematics, economics, statistics, and operations research. We expect that, in addition to the development of practical cross-layer architectures, efforts in this area will also lead to new tools within optimization, control and game theories, and stochastic analysis.

5.2.4 Sustainability

Multiple challenges arise from the need to enhance the architectures' sustainability:

Equipment development. First, consider the necessity for equipment development and minimization of operating costs. For example, extending the lifetime of the infrastructure's equipment can tremendously improve the architecture's sustainability properties. Developing the infrastructure's equipment is also related to the challenges in the domains of coexistence and virtualization.

Energy cost. As far as energy expenditure is concerned, a basic challenge lies in accounting for dissimilar cost association across different architectural operations. Empirical observations via measurement acquisition may provide significant insight for applications to adapt their behavior. It is also a challenge for architectures to support energy-performance tradeoffs. For example, transmissions can occur at a lower rate or periodically, in order to meet user-specific energy constraints.

Support of novel energy consumption modes. Another challenge lies in supporting novel modes for energy-consumption of infrastructure and client nodes. As of today, infrastructure is assumed to be always available and does not support operation in duty-cycles or powering-down for a certain period. Therefore, protocols that allow infrastructural “sleep modes” will significantly differentiate from their current counterparts. Moreover, while it is possible for infrastructure and client devices to independently decide under which energy states to operate, it is a challenge to devise more efficient schemes that are based on coordinated, network-wide decisions. As a result, devices can offload functions to their neighbors and allow a smooth expansion or contraction of the infrastructure to serve the operating load.

6. Wireless Systems Research in 2020

Wireless systems research is the subfield of wireless research that studies networks of computing devices that communicate over a wireless medium. The main characteristic of this subfield is its emphasis on practical design, implementation, and empirical evaluation. In the last few decades, wireless systems research has played a key role in advancing wireless communication. Its contributions include:

ALOHANet, which is the world's first computer communication network; *packet radio networks*, which are the predecessor of today's WLANs; Carrier Sense Multiple Access (CSMA), which is the mechanism used by today's computers to access a wireless network; and Software-Defined Radios (SDRs), which are the key enabler of cognitive communication systems. Recent years have witnessed a great momentum leading to innovations along multiple axes: (i) disruptive network designs have emerged including sensor networks, delay tolerant networks (DTN), vehicular networks, and cognitive networks, (ii) system research has shown an unprecedented breadth; its innovations now encompass signal processing at the physical layer as well as novel environment-aware applications, (iii) and a long-awaited convergence between empirical system research and information theory has delivered the first implementations of wireless network coding, physical-layer security, and interference alignment.

6.1 Applications

Wireless systems research has traditionally proved its ability to cut across many disciplines and connect hardware and radio advances with useful applications and social services. Further, because of its emphasis on practical design and empirical evaluation it has proven the vehicle that delivers basic science to industrial success. As a result, it is today positioned to contribute to multiple critical services that can affect all aspects of human lives such as:

HealthIT. Body area networks (BAN) allow a continuous monitoring of a patient condition in her/his own natural environment. Small radios with sensing devices are likely to be implanted under the skin to measure various body functions and report them over a wireless network to wearable radios. The latter collect the measurements and deliver them wirelessly to a central unit, eventually to reach appropriate medical experts in a hospital. This process extends healthcare beyond the hospital, reducing its cost, and significantly increasing its efficiency.

Broadband for all. High bandwidth Internet access is becoming a necessity in today's world. Various studies have shown that people with rich Internet connectivity have access to diverse information and use such information to significantly improve their social and economic conditions. Today, barely 25% of the world's population has any Internet access, leading to a widening standard-of-living gap with the remaining 75%. This inequality has created a new form of socio-economic disparity, referred to as the digital divide. Given the prohibitive costs of deploying a wired Internet infrastructure to every corner of the inhabited world, it is anticipated that a diverse set of wireless technologies will be the only feasible means that can realize the `broadband for all' dream.

Smart grid. Efficient and clean energy usage may be improved with a better understanding and tighter control of energy consumption. A smart grid enables energy sources, carriers, and consumers to better understand and control various processes in the energy grid. Hence, it can help reduce waste, improve efficiency, and divert energy usage during emergencies to where it is most needed. This vision requires entities in the energy grid, including each individual power outlet, to be remotely accessed and manipulated. Because of its tetherless nature, wireless networks have been proposed as the likely medium for such communication.

Smart transportation systems. People regularly move from place to place as never seen before in human history. Wireless communication systems are likely to play an important role in making various modes of transportation safer and more efficient. Communication between pilots and air traffic control, navigation satellite systems, safety mechanisms that detect driver fatigue, and systems that can provide automated safeguard between vehicles, all depend on improving the robustness and quality of wireless communication.

Understanding our environment. An increasing number of mobile devices are equipped with a rich array of sensors, including cameras, microphones, accelerometers, electronic compasses, and GPS receivers. While each such sensor can facilitate new applications in these devices, in aggregate they open up unprecedented opportunities of understanding our environments. If data from billions of such sensors can be effectively collected, they can serve as a rich information telescope for the world. For example, chemical sensors in future mobile phones can track spread of pollutants within a city, feeds from user cameras can provide immediate feedback on outbreak of forest fires and their nature, and GPS receivers in phones can pinpoint locations of trapped individuals after a devastating earthquake.

6.2 Challenges & Opportunities

The applications described above place greater demands on wireless networks that are hard to satisfy with today's technologies. We envision that research in the coming ten years should try to answer the following three big challenges:

- *How do we obtain unbounded wireless bandwidth?* So far, the growth of wireless bandwidth has always lagged behind that of *wired* bandwidth. In the future, unfortunately, wireless will become the dominant medium for connectivity; not only will it be used for Internet access but also it will replace the piles of wires at home and in the office. The scarcity of the wireless spectrum is the main factor that limits the vision for wireless access everywhere anytime, and perhaps the toughest challenge that wireless research has to undertake. Overcoming this challenge requires innovations in various areas including novel ways for spectrum sensing and reuse, mechanisms for using higher frequencies such as 60 GHz and the visible light, novel ideas for dealing with interference, high-density MIMO, and generally more efficient protocols and systems.

- *How do we deal with fast and continuous mobility?* While full mobility is the main premise of wireless communications, current wireless networks fall short of delivering that vision. Today, 802.11 and other computer networks provide a nomadic mode in which users can occasionally move from one place to another. They cannot however support fast continuous mobility. Cellular networks are better at supporting mobile users but they pay for this feature very highly in terms of efficiency with today's 3G systems having a low spectral efficiency about 1 bit/s/Hz. The problem is that fast movements cause unpredictable variations in channel SNR that could be as high as 15-20 dB. These SNR variations make it difficult to select the right modulation and FEC for transmission. The net result is that existing wireless networks either give up on fast mobility (802.11 WLAN) or resort to a very conservative design (cellular networks). Addressing this problem requires innovations at all levels of the network stack.

- *How does a network deal with overwhelming quantities of data?* The future will carry a plethora of sensors that monitor every event anywhere. Some will be carried by human users including cameras and microphones; other will be embedded in the environment including sensors that monitor our energy grid, our factories, and our transportation systems. The result is a flood of sensor readings, some of which have a very rich content including video. Understanding this information, and eliminating the huge correlation and redundancy constitute a major challenge. Furthermore, given the size and speed at which information is generated, the network cannot simply carry the information to a centralized destination where it is processed. The network itself has to actively participate in processing the information to eliminate redundancy locally, transform the information into more manageable formats, and route it to where it is most useful.

In order to address the above challenges, wireless systems research needs to innovate along multiple axes. We briefly discuss the various research areas and challenges here, with more detail in their respective sections in this report.

Communication between the PHY and higher layers. Conventional wireless design has a strict contract between the layers of the network stack. Specifically, the PHY and lower layers deliver fully correct packets and the higher layers route these packets to interested destinations. Recent studies have shown that such strict separation between layers leads to lower throughout and reliability. Future applications are likely to emphasize this trend. For example, implanted and wearable radios proposed for HealthIT cannot afford inefficiencies that stem from a traditional layered network stack. Innovative designs of a `layer-less' network stack that avoids most protocol overheads while maintaining robustness are highly desirable. Significant research is needed to design systems in which applications and other traditional higher layer components are made aware of the physical layer characteristics, i.e., a PHY-aware stack. Similarly, it is also important to seek innovative PHY layer designs that leverage application context and treat the entire network as the communication channel.

Traditional courseware describes wireless systems by partitioning them into discrete areas (e.g., network protocols and applications vs. information and communication theory) and do not cover the inter-disciplinary skills crucial for future cutting-edge wireless research. There is a need for inter-disciplinarily classes as well as hands-on courses and workshops to equip students with a complementary set of skills that allows them to understand and redesign the whole network stack from the PHY layer to the network and application layers.

Theory-inspired PHY design. The battle to push network efficiency to capacity limits needs to continue unabated. Breakthroughs that will impact practical systems are expected to arise from collaboration between information and communication theorists and the experimentalists represented by wireless systems researchers. This is likely to leverage ongoing advances and collaboration at the physical layer, including those in the areas of interference alignment, interference cancellation, and high density MIMO. The net result could be an information-theory driven practical PHY design, where the most advanced theories are realized under practical constraints of feedback overhead, limited synchronization, and unknown and quickly changing environment.

To build a consistent body of research results, which can be reproduced, verified and advanced by independent researchers, it is important to develop common metrics and benchmarks. While there is a common understanding of relevant metrics such as loss rate, throughput, and SNR, it is difficult to translate these metrics into concrete benchmarks because such benchmarks need to involve the whole network setup and the interaction between different nodes. Furthermore, no good characterization exists of the common case behavior, e.g., typical loss patterns or hidden terminal probability in operational WLANs. Characterizing the range of behavior in existing wireless networks is an important area that needs major research efforts. Such characterization however requires monitoring a large number of academic and enterprise networks of various sizes. Thus, it will require the involvement of a large fraction of the community and the support of the funding agencies.

Innovative devices and technologie. The future also depends on innovative uses of advanced wireless technologies and devices in networked systems. In the traditional radio domain, the innovative uses of directional antennas, MIMO, and energy-scavenging radios are important for providing the high-efficiency, high-bandwidth links required in anticipated future systems. Other promising ideas include using 60 GHz links to eliminate wiring in data centers, or the use of ultra-wideband radios for spectrum sensing and access.

In the quest for capacity, visible light frequencies can be exploited for their extremely high bandwidth and directional links. Exploiting this part of the spectrum, however, requires novel network solutions to overcome fast degradation of the signal over distance, and its inability to penetrate obstacles in the line of sight. Innovations could cast traditional network protocols in a completely new light such as having visible-light networks route data using controllable mirrors and lenses.

Open, programmable, and sustainable testbeds. Many past successes were enabled by the accessibility of testbeds and wireless platforms. Without implementation measurements and testbed evaluation, wireless research risks losing its ability to provide practical and realistic designs. However, over time, the complexity and hence the cost of studied wireless technologies has significantly increased. For example, while a traditional wireless node composed of a PC and an 802.11 card costs a few hundred dollars, a MIMO software radio can cost as much as ten thousand dollars. To continue providing cutting-edge experimental wireless research, the funding agencies should incorporate this cost in their model. Furthermore, the choice of platform will impact whether other researchers can reproduce the results or leverage the produced software. It is important that there is some form of standardization in choice of hardware, software codebase, and testbed topologies. Much like NSF NOSS program supported and encouraged the use of Berkeley Motes and FIND program will encourage use of GENI, wireless systems research should encourage use of common platforms. This will build a consistent and coherent body of research results, and ensure high-impact of the supported research activities.

A major problem that hampers efficient and fast research outreach is that every research group has to build its experimental effort from scratch. Ideally, codebase produced by a research project is made publicly accessible to other researchers. For this to happen however research groups need engineering staff that can package software for public release and maintain the package over time to continue to work with new software releases. A similar argument applies to the sustainability of platforms. More generally, projects and platforms that have significant community impact and are crucial for the success of wireless systems research should be supported as community assets beyond project support years. This will ensure that there is an uninterrupted support of the hardware and codebase.

Security. Physical-layer security is a new field that has both systems and theoretical foundations. It advocates new PHY-based security mechanisms that augment the existing repertoire of cryptography-based techniques. For example, the fading patterns on a wireless channel can create a source of randomness to hide private information, the characteristics of the wireless channel can be used to generate device identity, and frequency hopping can be used to combat jamming.

Spatial spectrum. MIMO technology promises a linear gain in capacity with the number of antennas. Unfortunately, for RF communication, this linear gain stops after a few antennas. This is because the linear gain is dependent on the antennas being separated by at least half a wavelength. For 2.4 and 5.5 GHz networks, the wavelengths are on the order of tens of centimeters, which prevents packing many antennas on a small device. In contrast, the wavelengths in the visible light range are much smaller allowing the packing of millions of antennas on a small device. This is apparent from today's cameras and LCD, which carry millions of pixels. These LCD and cameras can be used as high density MIMO transmitters and receivers, capable of delivering much higher throughput than existing RF MIMO channels. Leveraging such channels requires innovative research that combines networking with image processing techniques. Innovations in this direction could extend the existing frequency spectrum with a spatial spectrum that captures spatial frequencies. Further, since transmissions in the visible light range are highly directional and do not suffer major interference, the spatial spectrum expands with the physical space.

Cognitive communication. Today, the available spectrum is fragmented across a number of incumbents governed through strict control mechanisms. Approaches to facilitate dynamic access to the spectrum in an unlicensed manner without interfering with existing incumbents can yield a significantly more efficient spectrum usage. Cognitive communication across all spectrum bands has the potential to enable broadband-for-all. There are many ongoing activities in the domain of spectrum sensing, spectrum access, and cognitive radios that are focused towards this goal. More research is needed however to address questions like: how do we detect and avoid occupied frequencies? How can a user communicate efficiently over a highly fragmented spectrum? How do we leverage frequency selectively for increased throughput?

Context awareness. Wireless networks can leverage context-awareness to decrease overhead and increase information utility. For example, nodes in a MANET may use their accelerometer readings to detect mobility, which gives a coarse indication of the speed at which the channel may change, and hence how fast the routes need to be recomputed. Also, in a participatory sensing application, roaming users and vehicles may participate in monitoring the occurrence of a forest fire. To decide whether this application should report data, the node has to realize the unusually high temperature around a specific region. This might cause the camera to be turned on to take a picture. Further, the node uses its GPS readings to geo-tag each piece of information. Finally, all other users in the area close to the forest fire get an automatic alert based on their geo-locations as well. Innovative ways for leveraging context-awareness can lead to novel and useful applications.

From data-networks to information-networks. Future sensing applications are likely to generate an enormous amount of data to be communicated over the wireless medium. Much of this data however is highly correlated and, in principle, could be compressed. The problem however is that compression needs to occur at the sensors themselves before the data consumes the wireless bandwidth. Said differently, there is a need to move from traditional network design, which focuses on packet delivery to a more encompassing design that addresses information delivery. Recent advances in compressive sensing have the potential of addressing this issue but they need to be integrated with network design. Future research should provide innovations that allow a network to actively participate in compressing the data, manipulating the information, understanding it, and routing it to where it is needed.

7. Wireless Security

We are witnessing a wireless revolution, brought on by the adoption of wireless networks for consumer, military and scientific applications. For example, the consumer potential is clearly evident in the exploding popularity of wireless LANs and Bluetooth-protocol devices. The military potential is also compelling since wireless networks can be rapidly deployed and the failure of individual nodes does not imply the failure of the network. Scientific data-collection applications using wireless sensor networks are also gaining popularity.

The broadcast nature of wireless communication makes it, however, vulnerable a multitude of security threats. Therefore, ensuring the network's robustness against different security attacks is one of the important design objectives. In fact, designing secure wireless networks poses unique research challenges; as compared with the wired counterpart. For example, the geographic location of users is a critical factor in the design of wireless security protocols. In wired networks, the geographical location is of limited importance since users change attachment points only occasionally, and hence, Internet addresses can be mapped to approximately city-level geographic regions. Users of wireless networks, on the other hand, exhibit a much higher degree of mobility and interaction with their surrounding environment, making geographic location a key parameter in many wireless applications and network protocols. Thus many wireless networks and devices contain positioning technologies that allow for determining the device location with high precision. The importance and availability of this location information present both opportunities and challenges from a security perspective; the location information can be leveraged to enhance security, for example to detect Sybil attacks or to provide location-based access control to information and networks, while key challenges lie in verifying location claims and in maintaining location privacy for users of wireless devices. Another source of challenge and opportunity in wireless networks is variable channel conditions. In wired networks, a link typically has a constant channel condition, but in wireless networks, condition can fluctuate from second to second.

Fluctuating link conditions can provide attackers with opportunities, but can also be used to generate secret keys that can be used to secure networks.

7.1 Applications

In many cases deployment of new technologies cannot take place until they are rendered secure enough for widespread use. This is particularly critical when considering the high-impact roles that new wireless technologies will play in the future. There are different requirements and expectations for security that present unique challenges in each of the following applications:

Vehicular networks. Future wireless networking is a key enabling technology for intelligent automotive transportation networks that promises to improve safety, alleviate congestion, and increase energy efficiency. This technology allows cars to communicate with each other and roadside infrastructure such as traffic signals. Example applications include extended electronic brake lights (to warn following cars of stopping vehicles even under poor visibility), intersection collision avoidance, and fully automated driving applications.

In addition to *inter*-vehicular communications, car manufacturers are considering replacing the costly and heavy wiring between sensors and control units inside the vehicle with wireless technologies. While this application area of future wireless networks promises great societal benefits, it also requires a detailed understanding of security mechanisms and their limits in a wireless environment. Vehicular networks are both safety-critical and linked to critical national infrastructure and are therefore attractive targets for attacks. For example, attacks on traffic signals or in-vehicle control could cause accidents with loss of life or injury. Similar attacks could also jam critical links of the road transportation system to cause gridlock and vast economic damage.

Smart grid. Smart power grid technology is expected to revolutionize the way energy is generated, transmitted, distributed, and consumed. Crucial to this revolution is the communication infrastructure that serves as the information backbone connecting millions of sensors on the grid and providing real-time management of the nation's critical infrastructure. The pervasive use of digital technology in the smart grid presents enormous challenges as grid cyber-security (protection of information and commands) interacts with physical system security (protection of facilities and equipment). Attacks on the information backbone of the envisioned smart grid may shut down substations and generation capabilities, potential resulting in blackouts on a large scale. In order to enable the smart grid, communications between a complex family of heterogenous networks and systems must be protected.

Health care. Wireless health monitoring and maintenance devices are on the rise because they offer important benefits. For example, modern pacemakers can be programmed wirelessly after they have been implanted, allowing a doctor to adjust the pacemaker's settings without cutting into the patient. Unfortunately, as demonstrated recently, many of today's wireless pacemakers do not prevent someone other than the doctor from programming it as well. An adversary with a common radio can wirelessly connect to the pacemaker and issue a heart-stopping shock. Such security flaws may discourage patients from using the technology resulting in a decreased quality of life and shorter lifespan. In this case, security is an enabling factor in adoption of critical wireless health care technology.

WiFi networks. Early adoption of IEEE 802.11 "WiFi" wireless networking technology was explosive as inexpensive standardized devices freed computers from dependence on cables for connecting to the global Internet. Today, almost every laptop comes with WiFi capability and the technology is routinely used in the home and workplace. Unfortunately, the security techniques used in the original WiFi standard were vulnerable to several attacks that allowed anyone to eavesdrop on confidential communications sent over the air. In some cases, an attacker could simply sit in a parking lot and connect to sensitive computers inside a building. Network security research discovered these vulnerabilities, then provided the tools to create new security standards that fixed many of these problems. Today, the new security techniques, known as WiFi Protected Access (WPA), are used in millions of laptops, home routers, and corporate networks to enable the freedom of wireless communications with much improved security guarantees. Despite this success story, the opportunity still exists for constructing *provably* secure WiFi protocols with low implementation complexity and friendly user interfaces.

Cellular networks. Cellular networks have long been protected from large-scale attacks by their logical and physical separation from other systems. However, the move towards greater interconnectivity with the Internet and the vastly expanded capabilities of mobile devices fundamentally alters the risks facing such networks. Since these networks represent the only reliable communications infrastructure available to the vast majority of people on the planet, ensuring their robustness under increasingly hostile conditions is critical.

Recent research has demonstrated that adversaries can cause large-scale outages in cellular networks using targeted low-bandwidth attacks. For example, it has been shown that a small volume of text messages targeted at a geographic area could be used to deny legitimate voice and SMS service. Similar results were demonstrated by overloading paging services on shared uplink channels. While it is possible to mitigate the impact of such attacks using a variety of queue and resource management techniques, this line of work has unveiled the fundamental tension caused by the meeting of best-effort IP networks and the circuit-switched air interface of cellular networks.

The previous list of potential applications highlights the fact that wireless security research is critically needed to enable the adoption of wireless networking in a variety of scenarios offering concrete societal benefits.

7.2 Challenges and Opportunities

As mobile wireless services become ubiquitous, new methodologies are needed to detect and defend against intrusions of mobile adversaries. In order to develop a principled approach to security in future wireless, a better understanding of the fundamental tradeoffs among key design parameters is needed. In particular, there is a cogent need to characterize the relationships--both analytical and empirical--among the power of adversary, the strength of network defense (or degree of freedom), and the achievable performance. Such characterization should be based on appropriately defined metrics that quantify these design parameters and performance measures.

This overarching goal will require a cross-disciplinary research approach. For example, signal processing, machine learning, and information forensic techniques are needed for the detection of intrusions, whereas game theory can be a unifying theoretical framework in characterizing/achieving tradeoffs among often conflicting design objectives. The information theoretic security paradigm allows for exploiting the unique characteristics of the wireless medium to construct low complexity and provably-secure physical layer algorithms and networking protocols. The following discussions outline a few of the critical research areas in wireless security.

7.2.1 Information Theoretic Security

One can broadly categorize security threats into two groups: *active attacks* in which the adversary can transmit signals over the same wireless channels, (e.g., jammers attempting to disturb the on-going communications, or users injecting malicious signals into the network) and *passive attacks* in which the adversary attempts to eavesdrop on the transmitted messages. Most, if not all, of the state of the art techniques for combating eavesdropping attacks adopt the public key cryptography paradigm in which the destination publishes a public key accessible to the source and eavesdropper, while generating a corresponding secret key known only to it. The source then encodes the message intended to the destination by the public key. Since the key is known to the eavesdropper, it can theoretically decipher the received signal to obtain the message. The trick is that, by properly designing the public and secret keys, the destination attempts to make it computationally infeasible for the eavesdropper to decode the message while still ensuring itself a rather simple decoding task. The enabling idea is to establish the equivalence of deciphering at the eavesdropper with solving a difficult mathematical puzzle (e.g., factoring large primes or decoding a long block code with a random generator matrix). However, the difficulty of these problems does not seem to be mathematically provable at the moment, which leaves the secrecy of the system vulnerable to the discovery of an efficient solution algorithm or the invention of computers with enough processing power to crack the problem in reasonable time (e.g., quantum computers).

The notion of information-theoretic secrecy avoids the aforementioned limitation of computational complexity-based secrecy. This paradigm does not rely on any assumptions about the computational resources available for the eavesdropper, but focuses on the theoretical requirements for ensuring that the *mutual information* of the attacker's received signal and the transmitted signal is zero. In other words, perfect secrecy requires that the signal received by the eavesdropper does not provide any additional information about the transmitted message than was already known. Early work showed that the achievability of perfect secrecy requires the sharing of a private key between the source and destination. Later work introduced the *wiretap channel* and established the achievability of perfectly secure communication without relying on private keys, but requiring that the legitimate channel is less noisy than the eavesdropper channel.

Inspired by these pioneering works, researchers have recently made significant progress applying information theoretic security principles to wireless communications. These efforts have identified guiding principles for the design of wireless security protocols that exploit physical layer radio characteristics. For example, several opportunistic security protocols have been proposed which exploit the *multi-path fading* characteristics of the channel. Similarly, Multiple-Input Multiple-Output (MIMO), feedback, and cooperative security protocols that offer provable security guarantees and enjoy low implementation complexity have been constructed. More recent works have successfully demonstrated the utility of information theoretic principles in securing WiFi and wireless sensor networks. The key idea in these works is the use of information theoretic tools to design security overlays that strengthen the existing protocols while requiring only minimal modifications in the underlying architecture.

These approaches provide new opportunities for building secure wireless networks. Because information-theoretically secure approaches do not rely on computational difficulty, we can be assured that they will still provide effective security for decades, regardless of advances in computational technology; they can also be used to bootstrap keys for use with traditionally secured wireless networks.

Despite this remarkable progress, several key challenges lie ahead. The most pressing ones are, perhaps, the development of a unifying approach that bridges the gap between information theoretic and number theoretic security, and the development of comprehensive and realistic attack models. These generalized attacker models will allow the information theoretic approach to extend beyond the well-studied passive eavesdropping scenario, and thus shrink the existing gap between theory and practice. Some of these models may be informed by trace data of actual attacks in existing deployments. The derivation of attack models, however, cannot only be based on traces of actual attacks but must also anticipate likely attacks to remain one step in front of actual adversaries.

7.2.2 Location Privacy

With the introduction of programmable smart phones, wireless usage is changing significantly from occasional calls and text messages to always-on background applications and data communications and radio-frequency identification devices that can be observed anywhere. This increased frequency of communications allows unprecedented monitoring of users' movements. Movement and location data is privacy sensitive because it allows an attacker to infer who a user meets with and uses their location to infer the users’ health, nightlife, and political activities, for example. Such privacy-sensitive data accumulates at legitimate service providers such as cellular carriers and electronic toll services, but it can also be increasingly recorded by arbitrary third parties. Given the trend towards open wireless platforms like software radios, third parties can construct low-cost monitoring systems in nearly any frequency-band and can therefore also track the movement of users' devices.

Addressing these privacy concerns creates many research challenges. It requires development of criteria and metrics to assess privacy in wireless systems. It calls for design principles and techniques for incorporating fair information practice principles into wireless systems, including more usable ways to notify users about what data is collected from their wireless devices and techniques to increase accountability of data collectors. It also requires technologies that can provide hard privacy guarantees in adversarial environments.

The same wireless features that create privacy risks also represent opportunities for new applications and services. For example, location-aware network applications have already been studied in some level of detail, and proximity devices have been used for physical access control.

7.2.3 Cognitive Wireless Networking

Cognitive radio offers the opportunity for secondary users to share the spectrum with the primary (licensed) users. Some proposals even envision a spot market for spectrum, where wireless devices can compete in an auction for specific uses, thereby enabling greater spectral utilization for all. While this approach offers a remarkable opportunity for enhancing the spectral efficiency, it also poses a number of security and operational threats. For example, some devices may fail to honor their agreements or otherwise create harmful interference. Today, the main method for punishing such interference is to send humans with special equipment to detect, locate, and arrest the perpetrators. If we can design wireless security systems that tolerate or eliminate such interference, we may be able to avoid this expensive method of enforcement partially or totally.

Another potential attack in a cognitive radio network is the primary user emulation attack, in which a malicious user pretends to be the primary user by using the same signal structure in order to cause other secondary users to vacate the spectrum. In such an environment, the malicious user can use the spectrum all by itself.

A third example would be the common control channel jamming attack, in which malicious nodes try to block the control channel in order to cause transmission failure when secondary users negotiate usage of the free spectrum. There may also be attacks on spectrum management, in which malicious users send false information in distributed spectrum sensing process and gain an unfair usage of the free spectrum. Finally, one can easily see that the availability of sophisticated secondary radios will only make the classical passive eavesdropping attack a major concern in all wireless applications.

Overall, it is clear that the specific structure and standards of cognitive radio networks raises several major security issues that must be addressed before wide-scale implementation is possible. In fact, this area of wireless security research is a critical component in enabling the vision of cognitive radio. Furthermore, investigating the different security tradeoffs involved will give policy makers different options when deciding how to best regulate the nation's scarce spectrum resources.

7.2.4 The Interaction Between Security Technology & Policy

Effective security typically requires a multi-pronged approach that involves societal norms and policy, legal recourse, and technical protection. Since many wireless networks are linked to the global Internet, attacks can originate from areas outside the reach of the US legal systems. Thus, technical protection has to remain a key part of the overall solution; an approach only based on policy and legal mechanisms is unlikely to be successful. As with most new technologies, policy and legal standards in this area are likely not yet fully developed, thus technology researchers must also fulfill an important role of providing guidance to lawmakers and the public about key risks and limitations of security mechanisms.

Because wireless technology behaves differently than many people expect, wireless security often involves beliefs about the security properties of the technology that are not justified. For example, the first cordless telephones allowed anyone nearby to listen in with common radio equipment. This came as a surprise to anyone who assumed, guided by previous experience with wired phones, that cordless phone conversations were private. From a legal standpoint, court cases ruled that because of the fundamental broadcast nature of the wireless medium, cordless phone owners had no reasonable expectation of privacy. Until the legal framework was changed, eavesdropping on cordless phones was both practical and legal, despite being quite surprising to most people speaking on these phones. A key challenge in wireless security research is identifying these expectations and designing systems that can provide guarantees meeting these expectations. For example, with cordless phones wireless security research might develop new types of cordless phones that include encryption. More recently, security researchers discovered that the DECT cordless phone standard common in Europe and the United States misapplied encryption in a way that allowed others to eavesdrop, despite its use.

7.2.5 Evaluation & Learning From Deployments

Large scale deployments of wireless systems are expensive, especially in licensed frequency bands. Because wireless security has both a human component and a physical component, however, studying deployments is an invaluable guide to future research. Reasoning about what people expect from a wireless system for security and privacy is difficult to do in small-scale studies, and the physical properties of a deployment can drastically affect the practicality of proposed solutions. Therefore the research community has a critical need to learn from deployments in the form of traces and case studies.

Unfortunately, there are serious challenges facing the research community today that make it difficult to carry out this feedback loop. First, it is difficult for researchers to obtain traces, especially from commercial deployments. Commercial deployment traces, in particular, typically contain proprietary data and private individuals' data that may not be shared widely for legal or contractual reasons. While "anonymization," or the removal of personally identifiable information and addition of noise, is possible, our understanding of how to best perform anonymization is limited. When anonymization fails, the consequences can include complete re-identification of individuals, as America On-Line discovered when a reporter for the New York Times tracked down an individual from an anonymized log of search queries. These events make it difficult for companies, universities, or others to share data in the future. Second, a countervailing problem is that because few traces are shared widely, researchers either cannot perform apples to apples comparisons or the field focuses on a few data points for which information is available. A special issue here for wireless security is that many deployments choose to keep the details of their security systems secret, despite the consensus of the security community. Therefore researchers focus mainly on those deployments for which details are available, either due to an enlightened attitude on the part of the deployment owner, or more often due to painstaking reverse engineering.

In a nutshell, the field needs a framework for overcoming these problems. Recent research in the privacy community has looked at the question of how best to anonymize traces. These directions are promising and offer a potential technical tool for addressing these issues, but they need evaluation in context of wireless networking research. Overall, the field needs to create a process for gathering and appropriate use of traces that contain highly sensitive information, taking into account the needs of companies, customers, academics, and the general public.

8. Cognitive Radio Networks & Dynamic Spectrum Access

In the past ten years, we have witnessed a dramatic growth in wireless communication due to the popularity of smart phones and other mobile devices. As a result, the demand for commercial spectrum has been skyrocketing. For instance, AT&T projects a 5000% increase in data usage in the next three years, Yankee Group predicts 29-fold increase in US mobile data traffic from 2009 to 2015, and CTIA estimates that U.S. cellular companies need at least 800 MHz more spectrum over the next 6 years. In light of exploding demand, limited spectrum is a crucial impediment to continued growth of commercial wireless services. Similarly, we are seeing increasing demand for unlicensed bandwidth, due to the continuing growth of WiFi deployment and the emergence of additional application domains such as sensor networks for safety applications, home automation, smart grid control, medical wearable and embedded wireless devices, and entertainment systems.

Meeting this huge demand for bandwidth is a challenge since most easily usable spectrum bands have been allocated; however, many studies have shown that more than 90% of the allocated spectrum is unused or underutilized. This suggests that meeting future demands for wireless bandwidth will not only require new, more efficient communication and networking technologies, but also new techniques for increasing spectrum utilization. Today's spectrum policy relies largely on *static* spectrum allocation, which is relatively simple to implement and encourages investment in expensive infrastructure; however, this means that many of the frequency bands are only used in certain areas and/or only part of the time. To address this issue, Dynamic Spectrum Access (DSA) is an alternative strategy that more dynamically allocates spectrum to users and systems in response to system demands for bandwidth. Realizing this strategy through the use of cognitive radios requires not only advances in state-of-the-art radio technology but also new policies and economic models for spectrum use.

8.1 Applications

Cognitive radios are widely viewed as a disruptive technology that can radically improve both spectrum efficiency and utilization. These fully-programmable wireless devices can sense their environment and dynamically adapt their transmission waveform, channel access method, spectrum use, and/or networking protocols as needed to achieve superior network and application performance. One of the applications of cognitive radio is to enable more efficient, flexible, and aggressive DSA. The research community has made significant progress in addressing the many research challenges associated with cognitive networks and DSA.

With the exception of unlicensed spectrum which tends to be used by a multitude of devices, most spectrum bands are used in a fairly homogeneous fashion where the network uses a single (or closely-related) technology designed by a single organization. In contrast, cognitive networks are inherently heterogeneous. This fundamental difference raises many significant challenges, as identified in a recent NSF-sponsored workshop on "Future Directions in Cognitive Radio Network Research." The report covers in detail the topics of spectrum policy, sensing, radio architecture and software abstraction, cooperative communications and networks, DSA technology and algorithms, protocol architectures, resource management, network security, and the relationship between cognitive networks and the Internet.

The March report also observes that significant progress has been made in each of these areas, and that the most critical impediment to further progress is not so much continued research in these individual areas, rather, it is figuring out how the components of a cognitive network fit together and work together under realistic conditions. Only by evaluating the performance of complete cognitive networks at reasonable scale will it be possible to justify the necessary spectrum policy changes or to convince industry to make the necessary investments. To that end, the March report from the NSF workshop on "Future Directions in Cognitive Radio Network Research" emphasizes the need for shared wireless testbeds that can support cognitive networking experiments.

In this section, we do not try to further elaborate on the above topics alone but instead focus on the often complex interactions between the topics. These interactions lead to research challenges that are unique to cognitive networks but need to be addressed before cognitive networks can be deployed. In particular, there are two immediate areas where cognitive radios are of particular interest:

Television white spaces. TV-band white spaces have received significant attention from regulators, industry, and academia alike. After five years of debates, studies, and prototype testing the FCC made the historical decision in November 2008 to grant unlicensed wireless devices access to unused TV bands on a non-interfering basis. TV bands are very attractive for wireless communication due to their superior RF propagation characteristics in the sub-gigahertz frequencies and potentially large available bandwidth. Existing TV transmitters have fixed locations, transmission power, and known modulation schemes with predetermined TV broadcasting schedules. As such, they provide a perfect environment for research in cognitive networks and any results can have an immediate impact on industry by enabling high-performance *unlicensed* wireless networks and reducing the costs of deploying broadband internet access in rural areas.

Long-term Evolution Advanced (LTE-A). LTE-A is receiving a lot of attention from the cellular industry with the objective of allowing users to utilize potentially segmented spectrum bands more efficiently and with flexible upload and download bandwidth allocation. Although this is not a general case of DSA, it offers a great opportunity to demonstrate the concept and benefit of spectrum flexibility without facing the thorny issues of spectrum regulation and primary protection, which we address in the next section. Interesting research topics include fractional spectrum reuse, femtocell spectrum management, admission control, and dynamic spectrum allocation.

8.2 Challenges & Opportunities

Much research has focused on specific cognitive functions and radio design, but what is missing is a holistic approach that develops and evaluates solutions to spectrum sensing, coordinating spectrum access, optimization of communication and networking functions, dealing with mobility and security, and spectrum policy in the context of a complete network. We discuss some challenges and opportunities associated with making the step to full cognitive networks.

8.2.1 Establishing a Network-Level View

Building a network raises questions on how to partition the network functionality into a set of components so that the resulting system has good performance (e.g. high throughput, low overhead, fast adaptation, secure, and robust), can be maintained and deployed given the different stakeholders and their relationships, and can evolve over time. This is challenging because the design decisions for individual functions will often depend on how other functions are supported. In fact, functions often have conflicting requirements that must be addressed at the system level, such as the desire to maximize the data throughput of a cognitive radio user while maximizing the accuracy of its channel measurements through extended quiet sensing periods.

Nowhere is this conflict of system interests more apparent than when balancing the objectives of multiple networks with different tiers of priority across the same spectrum. Many DSA sharing models combine elements from traditional licensed and unlicensed spectrum, however, most academic research has focused on the *unlicensed* spectrum, in part because it is easier to get access to equipment and run experiments. Networking research in the DSA context will need to consider incumbent licensed network operators and their technologies, since they differ substantially from unlicensed counterparts with respect to regulatory, economic, network management, and service quality requirements. Whereas occasional interference-related outages are generally tolerable in a home WLAN, interrupting or delaying emergency communications is not.

Research in cognitive networks has sometimes also ignored some issues that are very important in practice. One example is energy efficiency, which has significant practical importance for mobile users.

While early work has considered energy efficiency in spectrum sensing--such as the tradeoff between sleeping and sensing--energy efficiency needs to be considered in all aspects of cognitive networks, including:

- control channel establishment - the simplicity of a separate control channel vs. higher energy cost,
- control message passing - user coordination vs. channel overhead and idle power drain,
- channel selection - selecting channels with better propagation characteristics,
- transmission configuration - data rate vs. energy consumption per unit data,
- network architecture - number of carriers, additional radios, bandwidth,
- security implications - energy depletion attacks.

These are non-trivial decisions with implications at all levels of the system. In particular, the following general questions must be answered.

Can spectrum policy reflect advancements in technology? There exists close interplay between technology and policy that creates unique challenges. As an example, consider the seemingly straightforward example of protecting TV transmissions in the white spaces with a “Listen Before Talk" (LBT) policy. Based on the traditional estimation and detection framework, the FCC determined a detection sensitivity of -114 dBm in the target white space was required to protect passive TV receivers from Secondary User (SU) interference. Direct measurements suggest that using this threshold will result in limited white space availability, especially in metropolitan areas where spectrum demand is high.

The research community has developed cooperative approaches to spectrum sensing that do not require the same fading margins because they can exploit sensor diversity. However, this approach is impractical because the current regulatory model is based on certification of individual devices and there is no notion of certifying the cooperative performance of devices. This is only an example of a mismatch between a technical result and policy. It also begs the question whether can we design regulatory models and certification techniques that can accommodate a broader range of technical solutions or, alternatively, can we define sensing algorithms that work within specific regulatory models.

The tolerances of primary spectrum users and the sensing/collaboration capabilities of secondary users are constantly in flux. Care must be made to ensure that wireless regulations are consistent with the technological capabilities of next-generation cognitive networks in order to promote innovation and bring ideas from the lab into the field.

How is the primary user protected from secondary interference? Primary user (PU) protection is vital to the success of wide adoption of dynamic spectrum access since no PU would accommodate SU access to its own detriment. This interference is also the major concern for legacy spectrum holders. Most existing research has been focusing on LBT where secondary users sense the spectrum (potentially collectively) before transmitting their own data and good progress has been made in both the theoretical domain and prototype testing. LBT has its limitations, however; because it focuses on the transmitter rather than the receiver, LBT needs to be conservative to protect PUs against SU interference. For instance, the threshold for the LBT devices was set at 30dB below the DTV reception threshold in the FCC TV white space testing.

In order to overcome these limitations, the research community should consider other options. For example, in the context of TV white space, the FCC database of station licenses has been used (sometimes in conjunction with sensing) to predict spectrum availability because TV broadcast locations are fixed and their schedule predetermined. Another option is to focus on receivers, more specifically the observability of receivers. There are both *active* and *passive* approaches. An example of the *active* approach is to introduce a beacon device on the receiver to announce its presence. This may be easier and less expensive then trying to sense for transmitters and it avoids hidden terminal problems. It has been demonstrated that it is possible for a low cost device to detect when a TV set is on and then announce itself. This type of approach has the potential to enable TV white space reuse in metropolitan areas, where the spectrum demand is high and unused TV bands are scarce. Research is needed to study/quantify the tradeoff between the performance gain and the complexity to enable receivers, as well as security implications of such a system.

An example of the *passive* approach is to exploit the inherent feedback information in bidirectional PU communication systems such as power control information, channel quality indicator, or ACK/NACK. Such feedback information from the PU receiver can serve as a good indicator of the actual and aggregated impact of the SU interference on the reception quality of the PU communication link. The principle applies to both directions of the communication. The benefits of using such feedback information are multi-fold: (i) it enables explicit protection of the PU receiver through feedback monitoring; (ii) it facilitates distributed access control of multiple SUs; and (iii) it permits different levels of interaction between PUs and SUs. In this context, there exists a close connection with network algorithm designs.

How are cognitive radios certified? Certification of cognitive radio devices is a challenge. First, it inherits the challenges of software certification (e.g. overwhelming system state permutations) because a cognitive radio is likely to have a large software component. Second, certification authorities must decide whether to certify a device or to certify a component. For example, a cognitive radio may consist of multiple components such as a policy "reasoner," a sensing component, and a RF front end.

A possible example of certifying components is to certify a policy reasoner which is decoupled from the radio platform; such a modular approaches can simplify the process. Third, certification faces the issue of addressing the networking aspect of cognitive networks. The network aspect can have both positive and negative impact on the PU/SU interaction. For instance, it has been well established that cooperative sensing can significantly improve the sensing performance. How can this positive effect be taken into account in certification? On the other hand, a PU may require certain protection, say interference below a given threshold. While a single SU device may not emit above-the-threshold interference, a collective set of SUs may cause outage at the PU. These are problems that will influence both certification and regulatory regimes.

How can spectrum policy be enforced? Enforcement is a challenge related to certification. The current approach, with the FCC being the main enforcer with labor-intensive measurements, is not likely to scale to billions of cognitive devices with much more flexibility and mobility. These have a much bigger potential for malfunction as well as malicious usage and distinguishing between correct and faulty behavior can be a very difficult program. Alternative solutions need to be considered such as enlisting cognitive radios to identify/report potential policy violations, though there is no easy solution to this problem.

National, interactive spectrum usage map. Another long term challenge is the development of a national interactive spectrum use map. While there have been a number of spectrum use studies, they provide a very incomplete picture since spectrum use is dynamic and location dependent. A complete interactive map would provide a "ground truth" on spectrum availability, which directly impacts the potential benefits of cognitive networking technology. It will also offer insight in the dynamics of spectrum use, and would allow evaluation and tuning of key components such as spectrum sensors, wide-band front ends and antennas. It could also provide an alternate means for "sensing" that would depend on database lookup rather than hardware sensing.

8.2.2 Cognitive Networking Beyond DSA

The previous section focused on the most often cited cognitive networking model that involves a legacy spectrum licensee as PU, and (unlicensed) SUs that opportunistically access the "white space" of the PU spectrum. Nevertheless, cognitive networking technology is not limited to this particular form of DSA.

Because of the increasing market penetration and heterogeneity of wireless devices, cognitive networking can enable network integration where both cognitive secondary users and legacy primary users *serve the same entity*. Such examples include the DARPA XG project (both serve military users), femto-cells (both serve cellular users from the same service provider), and public safety (newer and more agile devices sharing spectrum with legacy devices). In this context, PUs can be either legacy devices or similar devices of high priority. SUs are more agile devices or of low priority. Cognitive networking enables efficient and seamless integration of wireless nodes with heterogeneous capabilities and QoS requirements. Such applications offer clear incentive for PUs to allow cognitive SU access, can allow flexible and aggressive resource sharing, and often do not need regulatory changes. Instead, they require cognitive networks to have the flexibility to adapt to a dynamic environment and to effectively cooperate with each other.

Cognitive networking technology also has tremendous potential to improve network performance, even without considering dynamic spectrum use. In fact, in the last few years there has been significant progress in diverse cognitive techniques, including opportunistic forwarding, cooperative communication, transmit power tuning, network coding, interference cancellation, and others. However, many challenges remain. For example, most research has focused on individual techniques, and the tradeoffs between techniques and opportunities for combining techniques have not been explored. This is a challenging problem because of the large optimization space and sensitivity to external factors. Moreover, many cognitive optimizations focus on identifying and reducing interference, e.g. by controlling transmit power, carrier sense, or scheduling. This creates interesting research opportunities in terms of deployment in a DSA context, given the importance of limiting interference in that environment.

Another area requiring research is that of efficient techniques for information gathering, since access to more and more accurate information will often lead to better performance. First, while there is an obvious tradeoff between protocol complexity (degree of sharing) and hardware complexity (how smart is a node by itself), most algorithms require some degree of information sharing and possibly coordination between nodes. Current cognitive optimizations typically use custom solutions, but this will not scale to richer cognitive behavior involving many techniques. Research is needed to reduce overheads, e.g. by sharing information and selecting the optimal mechanisms (e.g. beacons, gossiping, common control channel, etc). Second, most research has focused on cognitive optimizations within a technology, but information sharing and possibly coordination across technologies could substantial improve gains. However, this form of cooperation raises new challenges with respect to sharing mechanisms, incentives, security, bootstrapping, and negotiations. A clean slate cognitive networking approach based on SDRs offers opportunities to explore these advanced techniques.

8.2.3 Evaluation and Integrated Experiments

The evaluation of cognitive networking technologies is challenging because of the high degree of adaptivity of the system. The dependence on many external factors (e.g. user behavior, traffic load, mobility) and the interdisciplinary nature of the technology add further complexity. As a result, a wide variety of tools are needed. Examples include tools that analyze the stability, capacity, and other network properties; simulators that can estimate performance under diverse conditions and for very large topologies; and testbeds that can evaluate complete systems under realistic conditions. Developing these tools is a research problem in its own right, given the known difficulty of modeling and measuring the wireless physical layer of even traditional wireless networks. Another observation that cuts across these different tools is that the wireless networking community does not have a commonly accepted set of metrics and benchmarks. For example, how is the signal propagation environment characterized so that results collected in different locations can be compared in a meaningful manner?

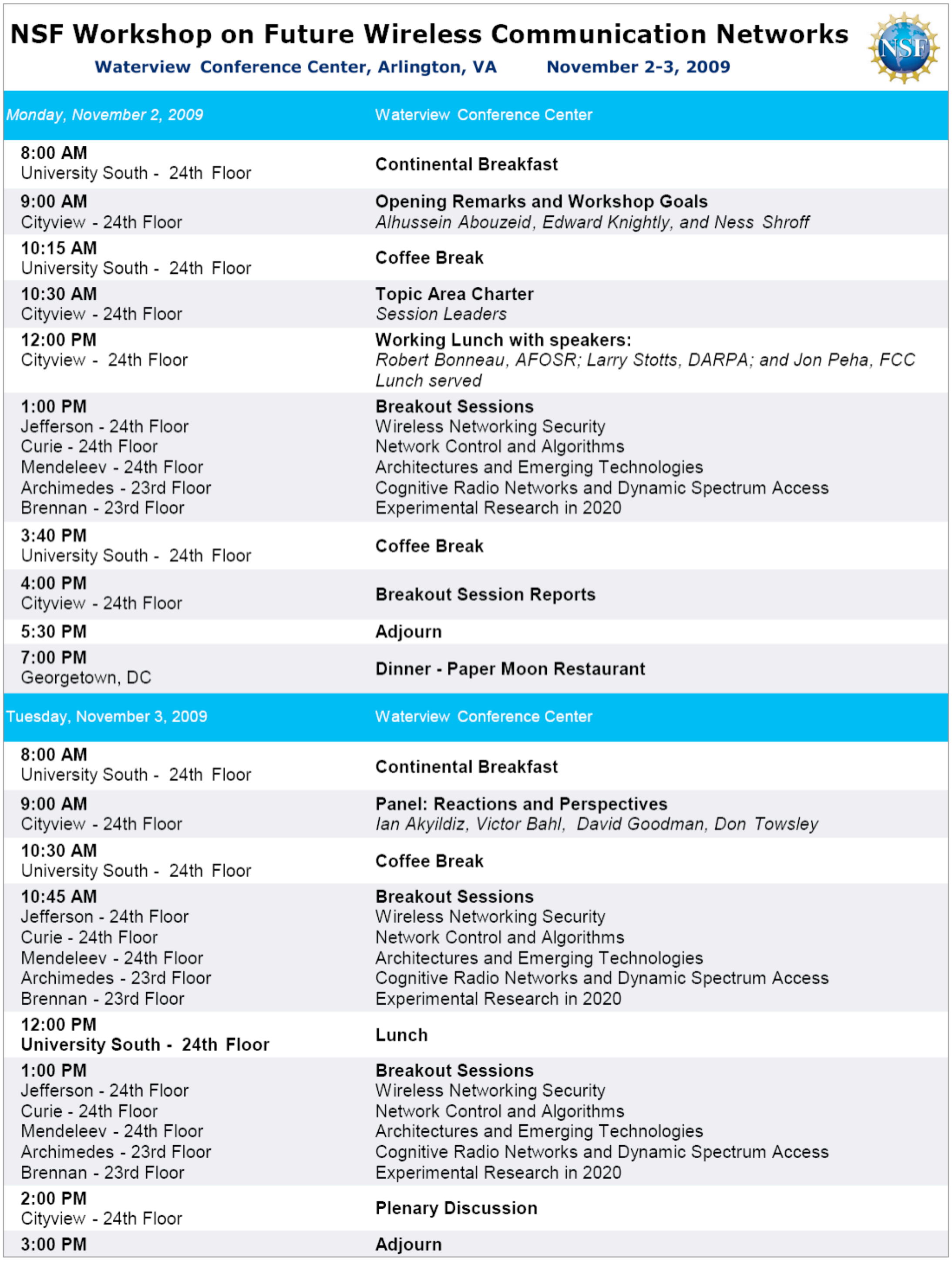
Experience shows that the real world often breaks some of the assumptions made in theoretical research, so testbeds are an important tool for evaluation under very realistic operating conditions. Network level experiments for testbeds also account for overheads resulting in a more accurate measure of the benefits of cognitive networks. This is essential when trying to make a case for deployment.

Because testbeds are location specific, testbeds will be needed for diverse environments such as different types of city, rural, campus, and indoor deployments. These testbeds will often stress different aspects of the technology like spectrum scarcity versus the need for adaptation in the protocol stack.

Because of recent NSF and industry investments in software-defined radios (SDR), a number of attractive cognitive radio platforms exist. For example, interfaces for TV white spaces exist (although they are expensive) and the spectrum is available. This creates a unique opportunity to deploy testbeds that will support hands-on academic research in cognitive networks, and allowing researchers to go well beyond WiFi-based research which is the core of today's research portfolio. SDR-based implementations of LTE are similarly available. Because the importance of both areas, it is an opportunity to make tangible real-world impact. Moreover, there is an opportunity to impact standards since the IEEE 802.22 standardization, for example, is still on-going so solid research results provide valuable input. In parallel, the community also needs testbeds that can support research in more general, longer term, DSA scenarios. These testbeds will need wider front ends, better sensing capabilities, plus access to more diverse parts of the spectrum.

Since many of the problems faced by the cognitive radio community span the entire network stack, and involve the complicated interaction of primary and secondary networks. There is a large gap between individual research results, effectively building blocks, and the large-scale deployment of cognitive networks that dynamically optimize spectrum use. Bridging this gap is one of the major research challenges we identified in the workshop, and the development of a testbed that is able to test radical ideas in a complete, working system is crucial. This includes both efforts to develop the hardware/software, as well as the radio licenses required to allow these testbeds to operate in licensed frequency bands and provide the community with operational results and experience.

Appendix



NSF Workshop on Future Wireless Communication Networks

Waterview Conference Center, Arlington, VA **November 2-3, 2009**

Monday, November 2, 2009	Waterview Conference Center
8:00 AM University South - 24th Floor	**Continental Breakfast**
9:00 AM Cityview - 24th Floor	**Opening Remarks and Workshop Goals** *Alhussein Abouzeid, Edward Knightly, and Ness Shroff*
10:15 AM University South - 24th Floor	**Coffee Break**
10:30 AM Cityview - 24th Floor	**Topic Area Charter** *Session Leaders*
12:00 PM Cityview - 24th Floor	**Working Lunch with speakers:** *Robert Bonneau, AFOSR; Larry Stotts, DARPA; and Jon Peha, FCC* *Lunch served*
1:00 PM Jefferson - 24th Floor Curie - 24th Floor Mendeleev - 24th Floor Archimedes - 23rd Floor Brennan - 23rd Floor	**Breakout Sessions** Wireless Networking Security Network Control and Algorithms Architectures and Emerging Technologies Cognitive Radio Networks and Dynamic Spectrum Access Experimental Research in 2020
3:40 PM University South - 24th Floor	**Coffee Break**
4:00 PM Cityview - 24th Floor	**Breakout Session Reports**
5:30 PM	**Adjourn**
7:00 PM Georgetown, DC	**Dinner - Paper Moon Restaurant**
Tuesday, November 3, 2009	Waterview Conference Center
8:00 AM University South - 24th Floor	**Continental Breakfast**
9:00 AM Cityview - 24th Floor	**Panel: Reactions and Perspectives** *Ian Akyildiz, Victor Bahl, David Goodman, Don Towsley*
10:30 AM University South - 24th Floor	**Coffee Break**
10:45 AM Jefferson - 24th Floor Curie - 24th Floor Mendeleev - 24th Floor Archimedes - 23rd Floor Brennan - 23rd Floor	**Breakout Sessions** Wireless Networking Security Network Control and Algorithms Architectures and Emerging Technologies Cognitive Radio Networks and Dynamic Spectrum Access Experimental Research in 2020
12:00 PM **University South - 24th Floor**	**Lunch**
1:00 PM Jefferson - 24th Floor Curie - 24th Floor Mendeleev - 24th Floor Archimedes - 23rd Floor Brennan - 23rd Floor	**Breakout Sessions** Wireless Networking Security Network Control and Algorithms Architectures and Emerging Technologies Cognitive Radio Networks and Dynamic Spectrum Access Experimental Research in 2020
2:00 PM Cityview - 24th Floor	**Plenary Discussion**
3:00 PM	**Adjourn**