

## ***Challenges in Future Communications Systems - Wireless networks 2020***

Wireless communication has demonstrated its importance in the past decade as a fundamental driver of economic growth, first in the form of cellular networks and more recently for computer networks (WiFi, WiMAX). The next decade is likely to bring equally dramatic developments, driven by:

- increasing demand for bandwidth-hungry services such as HDTV and access to data files of rapidly increasing size;
- increasing rates available from fixed networks (DSL at increased rates, 1000-base-T, FTTH and FTTB), which users will then expect wireless to match;
- the efficiency gains available from coordinated networks of autonomous devices and sensors, for example for security and surveillance.

The full extent of these developments cannot be predicted, but they are sure to include:

- Converged broadband services: “triple-play” services (speech, data, video) at rates up to 1 Gbit/s for users in any environment, delivered by standard/system-agnostic means;
- Ubiquitous computing: distributed intelligence in a multitude of devices operating autonomously;
- Wireless sensor networks for surveillance and environmental sensing.

These applications pose a number of severe challenges for wireless communications:

- Increase in system bandwidth efficiency by around an order of magnitude;
- QoS-aware networks;
- Coping with new and heterogeneous system architectures, such as mesh networks, multi-hop networks; peer-to-peer communication and multi-standard networks;
- Coordination of a multiplicity of autonomous devices using heterogeneous standards;

Efficient, timely transmission of very large volumes of short messages.

We propose that the following four areas of activity now need to be addressed.

### **1.0 Intelligent Spectrum and Resource Management**

The key issues identified in this area are in the context of the accommodation of a very large number of devices in a limited spectrum, where the spectrum may have both constrained and unconstrained usage patterns. Adaptation across several levels of the traditional OSI stack is therefore a major theme of the highlighted research areas and, in addition, there is a significant enabling interest to be serviced from the signal processing community. The following is a brief indication of highlighted areas of research which, it is felt, should form components of a managed programme to address the challenges faced by the development of mobile technology in the next 5 to 10 year period.

- Interference accommodation and mitigation

The unlicensed bands of spectrum available worldwide are constantly being targeted for a whole variety of different usage and are therefore becoming gradually more and more congested and interference prone. This area is concerned with the development of medium access and adaptive spectrum usage techniques to enhance the performance of uncoordinated use of the unlicensed bands.

- **Adaptability of transceivers**

This area of work will investigate how intelligence can be added to the uncoordinated adaptation of transceivers in an also uncoordinated use of spectrum. The feasibility of the development of adaptation policies for transceivers to maximise uncoordinated use of spectrum is the key driver.

- **Stability issues in adaptive systems**

The emphasis over recent years has been to develop adaptive techniques designed to optimise specific parameters such as quality of service power drain etc. It is apparent that when a very large number of devices are accommodated in a limited spectrum that consideration must be given to the interaction of adaptive techniques in order to preserve stable operation in this environment

- **Morphability (multiple adaptability of devices and radio access systems)**

This area of work recognises that adaptivity can occur at various levels (e.g. physical layer, link layer, etc.). This area of work should consider the development of policies to coordinate the multiplicity of adaptivity (morphability) in specific systems and their impact on other systems using the same spectral allocations.

- **Interaction of adaptive techniques**

This area of work is designed to assess the overall impact of using a variety of adaptive techniques across several layers of the OSI stack. The interaction of such techniques can result in a decrease in transmission efficiency and there is a compelling need to prioritise the use of particular techniques to achieve efficient use of available spectrum.

- **Criteria for power control**

Power control is typically a selfish algorithm that seeks to provide the required performance over a single link without regard to the impact on other users, other than trying to minimise the received power for the required QoS. This model is suitable when users use distinct resources. Where resources are shared such algorithms are not optimal and thus new power control algorithms are required that incorporate fairness constraints.

- **RF friendly and efficient signal processing**

Baseband processing is often designed with little regard for the implementation difficulties at RF. The most spectrally efficient waveforms often require high degrees of linearity with high peak to mean power ratios. This leads to low transmitter power efficiency or highly complex RF solutions. New concepts in system design are required where baseband and RF systems are jointly designed to provide a better global system optimisation between complexity, spectrum efficiency and power efficiency.

- **Interference limited MIMO operation**

MIMO technologies undoubtedly provide large gains in spectrum efficiency when channel conditions are appropriate and known. The ability to separate multiple data streams sent over the same channel requires knowledge of how the different signals are related. However, an interfering signal is unknown and can severely degrade system performance, therefore methods to mitigate the presence of interfering signals are required. These could include further antenna processing such as combined MIMO detection/beamforming or signal separation techniques.

- Intelligent adaptation of medium access control (e.g. energy adaptive, interference adaptive, etc.) for uncoordinated spectrum demands

This area of work is designed to assess the overall impact of using a variety of multiple access techniques which can adapt to dynamic variation in interference and loading in a combination of coordinated and uncoordinated use of spectrum.

- Integration of handover techniques in uncoordinated spectrum usage scenarios

This area is linked to the concept of dynamic spectrum allocation and the potential for rapid and seamless handing over services to different areas of the spectrum, which will be operating with different resource allocation strategies.

- Specification of the problems which occur in uncoordinated use of spectrum

This is a definitive study on the problems which will occur as a result of increasing the uncoordinated use of particular parts of the spectrum. This is an essential element in the design of adaptive systems referred to elsewhere in this list.

- Enhanced understanding and exploitation of the multidimensional radio channel for new applications.

Developments in MIMO technologies have reminded us that channels cannot be considered as just linear pipes but as complex 3 dimensional processes. The spatial structure of the channel must be exploited to achieve the best performance. This requires integrated design of antennas and signal processing to provide the most flexible exploitation of the channel. The spatial structure can also be exploited in routing messages to improved robustness to channel variability. The end application will determine what classes of channels will be present, e.g. indoor systems will have a significant amount of high elevation components.

- Progress to optimal architecture (hardware/software design)

Much of the progress so far have considered hardware and software in an almost independent manner. This has necessarily prevented any proper optimal design that may be gained from trying to integrate these two aspects from the beginning. This must be one of the priorities of the future.

- Trade-offs between coordinated (managed) and uncoordinated spectrum use

In many systems a fundamental design decision is whether to use centralised or distributed spectrum access. This occurs at the local level in MAC design, through to the regulatory

process of assigning channels to licensed or unlicensed operation. This review will consider the trade offs between coordinated and uncoordinated spectrum utilisation, and the interactions between such choices at the various levels.

- **Limits on uncoordinated spectrum usage (communications theory issues)**

This is a fundamental theoretical evaluation of the limits of uncoordinated use of spectrum.

- **Modelling of high density usage of allocated spectrum**

With the increasing shortage of spectrum compared to the demand, channels will be reused more frequently requiring the implementation of interference avoidance and mitigation measures. The interference environment will change significantly according to the interference management techniques employed. This study will develop interference models with high density spectrum usage and investigate alternative channel access protocols in different interference environments.

- **Routing strategies**

With increased density of spectrum usage some regions of space will become congested and routing a signal through them will not be possible. This study will consider interference aware routing strategies that exploit knowledge of the physical radio channel across the network to route signals to avoid existing congestion, and to avoid creating new congested regions. By understanding the properties of the radio channels, the QoS can be managed more effectively and the channels used more efficiently (e.g. low rate data without tight latency requirements can be sent through poor channels with highly redundant codes).

- **Cross system optimisation (e.g. in the heterogeneous radio access context)**

It is recognised that sharing information between different layer of the protocol stack can improve system performance, though this has only been considered in homogenous networks. This study will consider the benefits and approaches to cross-layer optimisation where a heterogeneous mixture of terminals exists.

- **Energy-efficient wireless communication network design**

Energy-efficient wireless communication network design is an important and challenging problem. It is important because mobile units operate on batteries with limited energy supply. It is challenging because the overall performance depends, in a coupled way, on different subsystems: antenna, power amplifier, modulation, error control coding, and network protocols, etc. Thus, to optimise performance one must account for coupling among various subsystems of a wireless communication system and simultaneously optimise their operation under an energy constraint.

- **Intelligent bandwidth allocation**

Intelligent (dynamic) bandwidth allocation is a major challenge in next-generation wireless networks, which has been considered nontrivial and remains mostly unresolved. Solutions for dynamic bandwidth allocation are needed to support integrated multimedia services with a wide range of service rates and different quality-of-service (QoS) requirements while maximising network throughput irrelevant to traffic variation.

## 2.0 Source and Channel Coding

- Realisation of channel capacity approaching codes for NON AWGN channel for short and long codes

Since the early days of information and coding theory researchers and designers of error-control systems have striven to obtain performance close to the fundamental Shannon limit with feasible implementation complexity. The invention of turbo coding in 1993, and the later re-discovery of Gallager low-density parity-check (LDPC) codes, together with recent advances in small, low power and high speed coding devices, has effectively achieved this, enabling these capacity-approaching codes to play an increasingly important role in communications services.

In effect, Turbo, LDPC and related code constructions are concatenations or combinations of very simple component codes, which when iteratively decoded can achieve capacity-approaching performance, with a fraction of a dB of the Shannon limit. Practical implementations of turbo coding are starting to emerge in many applications, but their 'error floor' and long decoding delay (inherent to all capacity-approaching codes) makes them unsuitable in certain scenarios. Well-designed LDPC coding schemes do not suffer from an error floor, and in some cases can out-perform turbo schemes, so they are now being proposed for emerging standards. These codes perform as they do only because of a combination of the following factors: (i) very large block sizes and (ii) many iterative decoding operations (both of which introduce significant delay in decoding time especially crucial for real-time applications), (iii) low code rates which reduce data rates or increase bandwidth, (iv) complex and memory-intensive component codes and decoding algorithms.

Thus the realisation of reliable, short codes with excellent performance, low power requirements and high and flexible data rates is an important research objective.

- Multi-functionality and reconfigurability

So far research has been focused on the theoretical limits that capacity-approaching codes can achieve but the focus is now slowly shifting towards the determination of practical, low complexity coding and (especially) decoding algorithms. Thus, long term research objectives include multifunctionality and reconfigurability, e.g. adaptive low complexity capacity approaching codes for applications such as Digital Video Broadcasting. The integration of essential physical layer functions such as equalization, synchronization, detection, channel estimation and multiple-access techniques with capacity-approaching codes and iterative decoding techniques will pave the way towards multifunctional systems.

- Coding for Networks and associated problems with distributed storage (including multi-user coding)

In multi-hop networks, such as wireless ad hoc and sensor networks, information is conveyed from a source node to destination nodes through multiple intermediate nodes. Each node-to-node transmission introduces interference and consumes power and network resources. The error-prone wireless transmission medium, with limited bandwidth, high interference, low-power transmitters and unpredictability of nodes joining or leaving the network (for ad hoc networks)

imposes new communication challenges. Indeed, severe impairments of the wireless link (noise, interference, fading, shadowing) significantly limit the amount of information that can reliably be transmitted.

Thus, it is important to avoid unnecessary communications while mitigating the effect of interference and fading in wireless links. The key in achieving this goal is to exploit statistical dependence of information present at different network nodes. Information-theoretical results are known only for the simplest setups with few network nodes and ideal sources. However, the increasing demand for multi-user multimedia applications (such as digital video broadcast/multicast over the Internet, ad hoc networks for rescue missions, telemedicine, and those closely related to national security, e.g., video surveillance systems) necessitates in depth research on multi-hop real-time data delivery.

- **Combined channel and source coding (cross-layer design)**

The growing importance of the Internet and the appearance of wireless 3G mobile systems have raised the interest in robust multimedia communication systems over unreliable channels. To develop an efficient communication system, one needs a source coder that reduces the amount of data needed to represent the source symbols and an error-protection scheme that protects the compressed bit-stream against channel impairments. Instead of considering source and channel components separately, significant performance improvements can be achieved by combining source and channel coding via a cross-layer design. Though joint source-channel coding techniques have been intensively studied, the newest developments in source-optimized channel coding and high-efficiency compression based on error-protection codes require revisiting this problem. The research objective is to completely integrate source and channel coding components and use a single advance error-protection code, such as low-density parity-check (LDPC) codes, to perform both source and channel coding. Such a scheme will be self-adaptive in rate, have a residual error rate of zero and can even be included into channel error protection. This way, great flexibility, cost reduction, and performance improvements will be realized.

- **Space-time processing to exploit context and location awareness together with interference cancellation**

Space-time and space-frequency coding/diversity techniques are rapidly becoming the new frontier of wireless communications due to the huge performance and capacity advantages that can be achieved through the use of multiple-antenna systems. These include design of space-time codes for single-carrier modulation, optimal maximum-likelihood receiver for channels corrupted by asynchronous impulsive noise, space-frequency coding/diversity designs combined with orthogonal frequency division multiplexing (OFDM) modulation, trellis coding modulation/non-orthogonal space-time block coding (TCM-NOSTBC) combination. Research efforts will be aimed at constructing new variants of the so-called “perfect space-time block codes”, that is, codes that simultaneously achieve full-diversity while transmitting at full rate (also known as the diversity-multiplexing frontier) through the use of augmented rotated constellations.

### 3.0 Heterogeneous Mobile Networks

The next-generation mobile networks will no doubt consist of heterogeneous access networks, ranging from cellular 3G/4G, WiFi (IEEE 802.11), WiMax (IEEE 802.16) to other emerging access technologies such as mesh and ad-hoc networks. These access networks are deployed to

support multimedia services for human-to-human, human-to-device and device-to-device communications in various operating environments where certain service areas may be covered by a multitude of access networks, while others are served by only one of these access technologies. The wide variety of access technologies require drastically different functionalities, capabilities and protocol standards. A key design objective for the future mobile networks is to enhance efficiency and ease of use. In turn, our future mobile networks ought to be capable of enabling users' communication devices to adopt and adapt automatically, dynamically, seamless and efficiently to various access networks for services available at a given time. The key requirement for such adaptation is to ensure end-to-end quality of service (QoS) in terms of data throughput, delay and error rate needed to support users' applications despite the heterogeneous nature of the access technologies.

Several key technical challenges to achieve such QoS in the internetworking of the heterogeneous networks are outlined as follows.

- **Internetworking of heterogeneous networks**

Different air interfaces such as 3G/4G, WiFi, WiMax, etc. have significantly different capabilities in terms of supported data rate and protocol functionalities. For example, the 3G network standards specify the physical (PHY), link, network and to an extent up to the application level, while the WiFi standards are defined primarily for the PHY and medium access control (MAC) levels. However, the end-to-end performance from application perspectives cannot be provided and maintained without an efficient architecture to ensure proper internetworking functions for the access technologies. For certain applications, a reasonable level of convergence for the access technologies is at the network layer so that the details and differences at the PHY and MAC for the access technologies can be "masked" out. On the other hand, while considering the performance impacts of the specific PHY and MAC protocols, other internetworking functions such as transport protocol and security among different access networks as well as between wireless access and wired networks need to be defined and evaluated.

- **Cross-network connection handover**

Due to movement of users or terminal devices, the quality of an established connection can deteriorate as the radio changes, thus requiring connection handover. Seamless handover algorithms for heterogeneous networks remain an open issue. Specifically, in the heterogeneous network environments, a connection may need to be handed off not only from one base station (or access point) to another, but possibly from one access network to another (e.g., from WiFi to 4G). Such makes the handover algorithms far more complicated than those required in the homogeneous networks. Handover in heterogeneous networks needs to consider the capabilities of different air interfaces, costs for using different access networks, possible constraints on simultaneous use of multiple interfaces on the same device, signalling across heterogeneous networks, etc.

- **QoS routing and transport protocols**

Packet routing is interrelated to connection handover. Traditional routing algorithms have not adequately considered possible time gaps for access by terminals during the handover process. It is desirable to devise new routing algorithms to maintain the end-to-end performance with adequate considerations of the handoff process in the heterogeneous networks. Such is particularly important for the networks supporting real-time applications such as voice over IP (VoIP), streaming video, etc. Similarly, performance impacts on transport protocols due to service gaps induced by connection handovers are also not well understood. It is worth investigating and devising new, efficient cross layer interaction

mechanisms to reduce the negative performance impact on transport protocols in the heterogeneous network environments.

With the emerging mobile ad-hoc networks (e.g., vehicular networks), the network topology can change rapidly. Often, parts of the network may become disconnected for a short time interval. Although such disconnected networks may not be applicable to supporting all types of services, they however are useful for the so-called delay tolerant applications. Routing and transport protocols for such delay-tolerant networks are still open research issues.

- **Network security and privacy**

To maintain end-to-end security and privacy of homogeneous, wireless networks is already a big challenge, given the open nature of radio communications. As different access networks have their own security protocols and controls, maintaining the overall security and privacy in the heterogeneous settings is challenging but necessary. The new security measures have to be distributed in nature so that they can be applicable to the multitude of access networks, possibly owned by many network operators.

- **Integration with wireless sensor applications**

In the near future, wireless sensors are going to be deployed widely to support a wide variety of applications ranging from environmental and building monitoring, healthcare, agriculture, national security, to military operations and home usage, to name a few. A huge volume of data collected by these sensors is to be forwarded to wired networks for processing via the heterogeneous access networks. Sensing events can take place randomly that cause a large surge of data traffic for the access networks. In addition, when sensors are mounted on mobile platforms (e.g., vehicles), they can access a multitude of different access networks. Furthermore, often due to limited available power, sensor nodes have a small set of protocol functionalities, not directly compatible to the access networks. Future generation networks have to be designed to support and integrate with these sensor applications.

- **Network management and provisioning**

As the future network consists of a large number of access networks, which are owned by many network operators and individual users, managing the “whole” network becomes very challenging, if possible at all. The traditional concept of network management by a single network operator or an enterprise is no longer applicable. However, the new paradigm for network management, provisioning and diagnosis appropriate for the heterogeneous settings are yet to be developed.

## 4.0 Trust, Reputation & Network Security

Engineering reliable and secure networks is now viewed as one of the most important challenges that network designers will be faced with over the next 5 -10 years. While security has always been a major concern for telecommunication networks, in the recent decade, the growth of cyber crime, spamming, denial of service attacks and the like has created a much greater focus on research in this area. Wireless networks have fundamental characteristics that make them significantly different from traditional wired networks, particularly with regard to security and reliability. Therefore the design of secure and reliable wireless networks presents a major challenge to the designers of next generation wireless networks.

It is clear that the areas identified below span the entire network design space; not only are many of these cross layer issues, but they are also cross-disciplinary issues that will require interaction and collaboration between the radio interface research community (e.g. the MAC and Physical layers) and the higher layer research communities (e.g. networking, transport, management and application layers). It is recommended that a managed programme would be the most efficient method of achieving such cross disciplinary collaboration.

The identified key issues that need to be addressed include:

- **Network Health**

The operational condition of a network will play a major role in determining its vulnerability to attack, or whether it can be used to carry secure transactions. The question therefore arises: How can we characterise the “health” of a network? What are the parameters and how can they be measured? One higher-order metric that will be required is a determination of the robustness (and hence vulnerability) of a network. This can also highlight aspects of the network that can be improved, for example increased resilience. Additionally, such analysis would seek to identify and quantify operational issues such as whether or not a given network is fit for purpose, is being used in a proper manner, for example is the level of spam excessive, or is it being overly abused?

One area related to improving resilience in wireless networks is the need to investigate Physical Layer (Front-End) Protection. Through intelligent design of the radio interface and the network topology, it may now be feasible to implement real-time protection mechanisms against network outages or malicious incursions into a network. In a manner similar to optical networks that employ 1+1 protection mechanisms against node or links failures, a radio interface may be able to automatically reconfigure itself (or be configured by some management systems such as an IDS) in order to provide alternate connections or to isolate unwanted incursions.

- **Understanding Vulnerability in Wireless Networks**

In order to characterise the health of a wireless network, a related issue will be to investigate and thoroughly understand the types of incidents that can adversely affect wireless networks (i.e. the “bad things” that can occur). Many of these incidents will have close relationships with the other strands, for example Network link /node outages & resilience issues; some will be linked directly to the function of the network, for example issues in Peer-to-Peer networks such as Free Riders, Malicious Peers, etc.; finally there will be a great many number of incidents that are the result of malicious attacks on the wireless network itself. It is expected that this last category will only increase with the proliferation of next generation wireless networks and their uses.

There is therefore a requirement for a thorough investigation into the types of attacks that can occur on all the major types of wireless networks (mobile, WLAN, WMAN, sensor networks etc). Typically, this will include both active and passive types of attacks, as well as characterising specific types of attacks such as Denial of Service/ Distributed Denial of Service attacks, Man-in-the-middle attacks, Deauthentication attacks, specific snooping for pertinent users’ details, etc

A related task here will be to investigate emergent behaviour that can lead to vulnerability in wireless networks, especially in converged networks, such as will be encountered in NGWNs.

- **Intrusion Detection Systems (IDS) for Wireless Networks**

The design of reliable intrusion detection systems (IDS) will be crucial for the correct operation (and indeed for the expected uptake) of next generation wireless networks. If as expected, NGWNS will be heterogeneous in nature, comprising for example: Sensor networks, WLANs, Mesh, WiMax, & Cellular networks then future IDS will have to operate across all of these. In order to facilitate research into future IDS there will need to be new network testbeds and network simulators/ emulators (for both fixed and wireless networks) coupled with traffic attack pattern analysis and new algorithmic techniques for real-time (and possibly distributed) prediction and identification of attacks. It is recognised that future IDS need to be cross layer in their design and operation, and a key aspect of this will include the ability to measure network events at different network levels including: Physical (PHY) layer events; MAC/Network layer events; other (higher level and application) events. It is anticipated that this area will also be related to: security architecture design, network optimisation, and network reliability.

- **Security Architectures for Wireless Networks**

The increasing diversity and ad-hoc nature of NGWNS presents challenges not only for managing these (distributed) networks, but also for managing their security, and this leads to the design of security architectures for future heterogeneous networks. Key issues that have been identified for the design of such systems include: scalability, complexity and efficiency; robustness; security network overlay architectures for wireless networks; and specific techniques for designing security into ad-hoc (or MANET) and peer-to-peer networks such as algorithms based on new concepts such as trust and reputation.

- **Security Metrics**

The issue of characterising suitable metrics for security is also related to network vulnerability, traffic patterns and IDS and security architecture design. An important distinction can be made between personal metrics that characterise an individual's usage behaviour and /or access privileges, and organisational metrics that characterise how an organisation uses a particular network. These are both important for determining for example, how secure on-demand connectivity can be achieved when roaming through other networks, in automatic VPN selection and establishment (again there will be overlap with other research areas such as constraint based routing and autonomic networking).

- **Intrusion Tolerant Networks**

Current research attempts to secure networks against all types of attack, at all times and generally irrespective of the cost to the performance of the network. It is also expected that many future networks will have to live under the threat of attacks as a matter of course. This may be particularly true for NGWNS, and especially for wide area wireless networks such as WiMax. Instead of attempting to secure all parts of these networks against all types of threat, one alternative is to accept that parts of a network may have different levels of threat at different times, and to design architectures that can dynamically adapt to the changing security states within a network. Current network security systems completely close down a network whenever an attack occurs. An intrusion tolerant network will therefore permit different level of service and security (throughput, access rights etc) in different parts of itself in order to maintain the overall operation of the network while under attack.

- **Encryption**

The design of future encryption systems will be a fundamental part of NGWNS. Key issues that have been identified for NGWNS include new research into key management techniques;

an investigation into the relationships (trade-offs) between power, complexity, and efficiency. This is particularly important for MANETs where the level of encryption / key distributions may scale according to the state of a set of mobile nodes. It is also recognised that there will be significant cross layer issues such as ad-hoc routing, power and key distribution, and well as the need to link encryption to Advanced Modulation & Coding (AMC), which is another cross layer challenge

- **The use of Wireless resources for Security Applications**

In contrast to the issues concerned with securing wireless networks, one additional challenge that was identified was the use of wireless resources for security applications. Here the challenge is to make use of existing resources in wireless networks in order to support a security related application. Examples might include Passive Radar and on-demand monitoring. It is expected that there would be significant overlap between this area of research and that of autonomic networking whereby virtual networks can be instantiated by higher level proxies or applications. As such there should be good synergy between these two research communities.