Project description
Optimization techniques in WireLess networks
(OWL)

SUMMARY

This project will apply optimization techniques in order to analyse and design wireless link communication and wireless network communication systems, and to improve capacity bounds for such systems. We apply for funding for hiring one researcher and two PhD students to investigate these problems, for organizing exchange visits of researchers with other high quality groups, and for enabling researchers associated with the project to present their research at international conferences.

During the planned project period (2006-2009), we aim to:

- Produce two PhD candidates and 10 master candidates in the area of wireless communications
- To transfer knowledge about the area to industry and to society at large,
- Contribute to the state of the art of wireless network communications, through the use of optimization techniques to wireless network connections and wireless network links.
- Build and extend contact with other research groups specializing in wireless networks, through exchange visits and active participation in the international community,
- Organize at least one international workshop with leading international researchers as lecturers on the subject of wireless network communication.
- Publish more than 15 papers in leading international refereed journals and a similar number at conferences in the area of coding for ad-hoc networks.

1 Introduction

In modern society, exchange and storage of information in an efficient, reliable and secure manner is of fundamental importance. The nature of such information is virtually unlimited: For example, it can be represented by text, audio, video, medical records, financial transactions, robot commands, or messages between an airplane pilot and a control tower. The communication is almost always in a digital form. Digital mobile communication is becoming increasingly important. Examples of digital communication systems are wire-based and wireless transmission lines, network connections, hard disks for computers, HDTV, CD, and DVD players.

We consider communication networks where computers or other similar devices are partly or exclusively connected with **wireless communication links**. Such networks have specific characteristic properties that, compared with ordinary wire-based networks, are both advantageous and disadvantageous.

A very attractive property is that these networks can be **deployed rapidly**, without tedious cabling. Wireless communication also allows **mobility** and therefore can be used for numerous applications in

for example crisis management, environmental surveillance, medical treatment, industrial control, and security.

On the other hand, wireless transmission can be **overheard** by anyone within range and will interfere with - and will suffer from **interference** from - other transmissions in range. These properties present problems for overall throughput capacity as well as for security. Wireless transmission also suffers in particular from channel impairments like noise and different forms of **fading** of the signal power. For these reasons ***coding techniques*** offer great improvements over non-coded systems.

Any communication is to some extent affected by noise. In order to detect or correct the errors that occur, the information is represented as a sequence of code words in an *error-correcting code*. The reliability of a communication system depends on physical conditions, but also on the error-correcting code and the decoding algorithm being used. **Coding theory** deals with methods to construct and analyze error-correcting codes, and to decode them in an efficient manner. The quality of digital communication, in particular mobile communication, is totally dependent on efficient error correction.

Traditional wireless networks, like Wi-Fi or similar local network technologies or mobile phone systems, are designed on a **cellular** technology with a central base station as a communication server for all mobile or static stations in range. This has proved to be effective in the sense that such networks provide a service that consumers quickly grow dependent on. However, there are many reasons why different technologies need to be and will be developed.

- As the number of users grow it is necessary to split large cells into smaller ones in order to reduce interference and accommodate more users. These smaller cells need to be interconnected; which gives a **network** structure.
- **Ad-hoc** networks are self organizing networks that communicate in a peer-to-peer fashion rather than through a central base station. These networks possess some attractive advantages over ordinary static networks. They are distributed in nature, and may therefore be more robust against some disruptive events (e. g. an explosion) than a network that rely on an efficient but static infrastructure. With a dense population of nodes, such networks can be calibrated to communicate locally at close range, with very low power consumption and with limited interference with other users. On the other hand, implementers of an ad hoc network face several practical problems that current research has failed to solve.
- Similarly, **sensor networks** interconnect very simple devices that communicate wirelessly, often over small distances.

Communication over a network is different than communication with a base station in a single cell. The network requires **routing** between a sender and a receiver. The rewards for this extra work include **reduced transmission power**, **reduced interference**, and possibly **improved robustness** through redundant routes.

The OWL project will join the forces of the coding and the optimization groups at the Department of Informatics at the University of Bergen, in order to apply ***optimization techniques*** both to the wireless *links* and to the wireless *networks*. The project will be carried out in the Selmer Center at the University of Bergen (see Section 3). The Selmer Center has, over a period of several decades, developed expertise in cryptography and coding theory at a high international level. Recently, a third research

direction has been investigated: Practical and implementation related aspects of wireless communication.

2 Project description

Wireless communication is essential unreliable and affected by signal degradation of various kinds. Appropriate error correcting or detecting techniques, combined with modulation schemes, may alleviate these problems, but the techniques often need to be adapted to be carried out on devices with low computing power. It is also possible that the redundancy of the network itself may aid the reliability of the communication. Also, it is feasible that a subset of the devices need to multicast substantial amounts of information to another subset of the devices, for example, when a number of tiny video cameras are sending signals simultaneously through the network, thereby putting a strain on the capacity of the network.

In the following we will describe the research themes in the OWL project. We also include an indication of who will be the main researchers involved with each research theme. Because of the broad body of knowledge in the Selmer Center, we also expect contributions from other members of the center, as well as our numerous visiting researchers, with complementing expertise.

Rather than viewing these research themes as separate subprojects, we will attempt to tie them together, and incorporate theoretical ideas in software simulations and physical implementations. By doing this we can obtain a better understanding of the overall processing cost of communication in the network. For this we plan to enroll master students. We expect to produce 10 master students specializing in wireless networks during the duration of the project.

2.1 Coding and modulation

In order to achieve a performance close to capacity in a hostile channel environment like the wireless one, it is essential to use error controlling techniques like error correction, error detection, and space-time coding, and maybe in combination with an appropriate modulation scheme when the channel is bandwidth limited (which we can assume it is).

Several authors (e.g. Feldman and Koetter) have recently considered the use of linear programming (LP) to efficiently decode low-density parity-check (LDPC) and other turbo-like codes. The *obvious* polytope for LP decoding is the convex hull of all codewords, in which case LP decoding is equivalent to maximum-likelihood (ML) decoding. However, the convex hull has a description complexity that is exponential in the codeword length. Thus, different relaxed polytopes containing all valid codewords as vertices, and also additional non-codeword vertices, have been proposed. The vertices of a relaxed polytope are commonly referred to as *pseudo-codewords*. Experimental results with LDPC codes show that the performance of the relaxed LP decoder approximates the performance of iterative decoding.

Reliability in the context of LP and iterative decoding is achieved by

- designing a code with a low iterative decoding threshold, in order to achieve low error rates at signal-to-noise ratios close to the Shannon bound. A low iterative decoding threshold is obtained by designing codes using extrinsic information transfer (EXIT) charts or by other means of density evolution,
- designing a code with good *pseudo-distance* properties, in order to combat additive white Gaussian noise and lower the error floor at moderate to high signal-to-noise ratios, and

- designing a code with large minimum *stopping set size* to combat fading effects. The effects of fading can also be reduced by exploiting any kind of *diversity* in the representation of information.

For a redundant network it may also be feasible to exploit diversity in the form of duplicate packets, but this idea needs to be investigated further. For an ad-hoc network with simple devices, it is further a requirement that encoding and in particular decoding procedures are simple and easy. Thus, the results of a thorough study of the complexity of LP decoding compared to iterative decoding would be very interesting for this type of application. Such a study is still lacking in the literature. We will investigate LDPC and other turbo-like codes in combination with LP decoding for this type of application.

We plan to hire a research scientist for the entire length of the project. We have an excellent candidate for this: Eirik Rosnes. His CV is enclosed as an attachment. We also apply for funding for one PhD student in this area of coding and modulation.

Main people involved: Ytrehus, Rosnes, PhD student, Helleseth, Kløve, Yorgova.

Publication goal: 8 journal papers and 8 conference papers.

2.2 Network coding for multicasting and unicasting in wireless networks

R. Ahlswede et. al. ("Network Information Flow", IEEE Trans. on Information Theory, 2000) showed that if network routers are allowed to combine several incoming packets and re-encode before forwarding them, it is often possible to increase considerably the information flow through a network. This process, known as **network coding**, has received considerable attention from the research community recently. In particular, this will be useful in network applications where the carrying capacity is limited compared to the needs of users, such as in fixed or mobile wireless networks.

There are a number of issues that have so far not been resolved. Several of these are of a nature that requires solutions based on coding theory and cryptography. Thus the Selmer Center is in an excellent position to attack these problems. We list three such problems below:

- Wireless networks are notoriously unreliable. Network coding increases the sensitivity to packet erasures, in the sense that a single packet erasure in combination with successful network coding will lead to erasure propagation. In order to combat this erasure sensitivity, it is necessary to employ erasure correction coding. Our goal is to design an erasure-resistant and yet effective network encoding scheme.
- Network coding for mobile ad-hoc networks: The topology of a mobile ad-hoc network is continuously changing, something that makes it difficult to apply an efficient routing algorithm to such a network. On the other hand, this is precisely an example of a network where the link capacity is strictly limited, so that the benefits of a proper network coding scheme would be large. As far as we know no solutions have been proposed for this encoding problem. Among other problems, such a scheme must deal with cyclic networks. Some progress in this area was made in "Encodings for cyclopathic networks" (submitted, 2005) by Barbero and Ytrehus.
- Minimization of system-wide transmission power: In wireless packet networks there is a natural coherence between network coding and multicasting with minimum energy. Over the past five years, quite a few models for computing energy-aware routing of broadcast messages have been suggested. However, these assume the existence of a central operator with a global view of the network, which is not realistic. As opposed to such techniques, network coding offers an opportunity to compute energy minimizing routes of information flow on a distributed level

(Lun et al. 2005). In the suggested project we will take advantage of our experience in minimum energy multicast routing (Bauer, Haugland, and Yuan 2005), to develop computationally efficient methods for minimizing transmission power.

We apply for funding for one PhD student in the area of network coding for wireless networks.

Main people involved: Haugland, Ytrehus, PhD student, visiting researchers.
Publication goal: 8 journal papers and 8 conference papers.

3 History and present research

The research group in **coding theory** dates back to the 1960's. The seniors in the group are Helleseth and Kløve that have done research on coding since the 1970's. In 1990 Ytrehus joined the group. The activities of the group were extended in the period after 1995. Two strategic university programs financed by the Norwegian Research Council (1995-98) and (2002-2005) was an important part of this. The group was also strengthened and the scope widened when Danish cryptographer Lars Knudsen joined the group in 1997 (full time professor 1997-2001, adjunct professor since 2001). In 2004 Igor Semaev became a professor in cryptology. At the same time, Kjell Jørgen Hole became a full professor, and started to build the wireless communications activity.

In 2002, the Norwegian Research Council initiated an international evaluation of all ICT groups in Norway. The evaluation was performed by a selected group of international experts. The coding/crypto group received the best grade ***"Excellent"***, and the committee added that the group ***"may be the best ICT group of any kind in Norway and occupies a distinguished position in the international community",*** and that it ***"is one of the gems on the Norwegian Scientific scene, not just in the context of ICT"***.

Based on this evaluation, the University of Bergen decided to organise the coding/crypto group as a new research center, ***Selmersenteret (The Selmer Center)*** named in honour of Ernst S. Selmer, a Norwegian pioneer in coding and cryptology who was previously a professor at the University of Bergen. This research center focuses on research on reliable and secure communication. The Selmer Center was officially opened on February 11, 2003. The group was based on the coding/crypto group at the Department of Informatics, University of Bergen and has recently been extended by including studies in secure wireless communication.

The Selmer Center consists presently of the following researchers

- **Professors/senior researchers (6):** Tor Helleseth, Kjell Jørgen Hole, Torleiv Kløve, Lars Knudsen (Adjunct Prof. 20%), Igor Semaev, Øyvind Ytrehus.
- **Post doctoral researchers (7):** Aleksander Kholosha, Matthew G. Parker, Håvard Raddum, Eirik Rosnes, Hans Georg Schaathun, Radinka Yorgova , one new.
- **PhD students (11):** Lars Erik Danielsen, Yngve Espelid, Irina Gancheva, Andre Klingsheim, Patrick Kintu, Vebjørn Moen, Geir Jarle Ness, Lars Helge Neteland, Thomas Tjøstheim , 2 new.
- **Master students (35-40).**
- **3-4 international visitors at any time:** Usually, at least 3-4 additional researchers and PhD students will be visiting the Selmer Center at any time, through our EU project as a Marie Curie Training Site or via our participation in European projects, ECRYPT and NEWCOM or other funding channels, or by their own initiative.

The **optimization** group at Department of Informatics also has a strong research record, and obtained the grade "Excellent" in the evaluation mentioned above. We have been active in the domain of digital communication and wireless applications, including research on algorithms for compact signal representation (Haugland and Storøy 2005; Nygaard and Haugland 1998) and methods for minimum energy multicast routing (Yuan, Bauer and Haugland 2005; Bauer, Haugland and Yuan 2005).

The group consists presently of the following researchers

- **Professors (3):** Professor Trond Steihaug, Associate Professor Dag Haugland, Professor emeritus Sverre Storøy.
- **Post doctoral researchers:** One researcher shortly to be engaged for four years.
- **PhD students (4):** Lennart Frimannslund, Ørjan Bergmann, Geir Gundersen, Joanna Bauer.
- **Master students (5).**

Recently the optimization group has also considered problems in the area of communication and information theory; see the enclosed reference list in the attached CV of Dag Haugland (in particular papers [11,15,17,18].)

3.1 International contacts: Guest researchers

Guest researchers make up a valuable and generally underestimated research resource, which we have previously used on several occasions with great benefits. These guests may be researchers on a senior level who are on sabbaticals or who for other reasons may be able to visit us for an extended period. In this situation the researchers will not receive ordinary salary from us, but instead a compensation for travel and extra living expenses. We plan to invite and support *one* guest researcher each year, for an average stay of *one month*. In addition we plan to invite *two researchers* for an average stay of two *weeks*. This will allow our research group to maintain and extend our international collaboration.

Some examples to illustrate the large number of guest researchers from many countries have visited the group for longer and shorter periods during the last decade is as follows: The numbers of guest researchers and total lengths of visits in weeks to the group during the years 1996 to 2004 were:

Year	1996	1997	1998	1999	2000	2001	2002	2003	2004
Number	6	12	6	7	5	6	8	12	15
Weeks	40	86	37	37	21	30	80	90	120

Several of these visitors are visiting the Selmer Center on a regular basis such as for example world leading coding theorists Kumar, Levenshtein and Zinoviev. An additional nice side effect of this is that we are often invited as guests at the universities of our collaborators, thus providing additional funding.

During the last three years more than 30 researchers have visited the Selmer Center in addition to 11 Marie Curie PhD students. Many such visits have resulted in close collaborations and joint publications. Thus it is important to maintain and develop further such international contacts. The researchers at the Selmer Center have published more than 300 refereed journal papers and conference contributions with more than 100 co-authors from more than 20 countries during the last decade. Since

the year 2000, we have published 185 journal and conference papers including 114 with at least one international co-author.

3.2 National and international networks and related activities

The Selmer Center is part of two Networks of Excellence under the 6th Frame program: ECRYPT and NEWCOM. Our participation here will provide channels for receiving news of the most recent research developments, but also for influencing the future directions of theory and practice.

ECRYPT -The Selmer Center is the only Norwegian partner in ECRYPT, a Network of Excellence that contains the strongest crypto groups in Europe and that will certainly shape the future of cryptology in Europe. ECRYPT consists of participants from about 20 universities and 10 industry partners and will ensure that the Selmer Center will be updated on the status of secure crypto solutions. The Selmer Center has 10 researchers and PhD students participating in the project. ECRYPT is based on the prize winning European project, NESSIE, a three-year project, where The Selmer Center participated, ending with a recommendation of a list of cryptographic primitives for use in Europe.

NEWCOM - The Selmer Center is one of two Norwegian partners in NEWCOM, a Network of Excellence dedicated to the study of future wireless communication systems. NEWCOM received by far the highest score among all proposals within the wireless communication area during the FP6 call. The network consists of 60 partners from academia, governmental and international organizations, and industry. This provides us with access to ongoing research in these fundamental areas.

National collaborations: The other Norwegian partner in NEWCOM is the Signal Processing Group at NTNU. OWL will cooperate with this group on areas of joint and complementary expertise.

We have also discussed the OWL project with other Norwegian researchers and with companies that share an interest in the area, including

- Nera (Contact persons: Karl Martin Gjertsen/Anders Vahlin),
- Nextgentel (Contact person: Ingvar Henne)
- KDC (Contact person: Anne Marie Hegland)
- FFI (Contact person: Eli Winjum (former student at the Selmer Center)),

and we will of course also exchange expertise and share results and ideas with these groups.

Net-on-Demand

The University of Leeds (led by G. Markarian), the ENST Bretagne, and the Selmer Center together with three companies (including Nera) have been granted a project under the Marie Curie Transfer of Knowledge program. The aim of the Net-on-Demand project is to study dynamic wireless sensor networks. The Net-on-Demand project will fund full duplex researcher exchange visits between academia and industry.

Other International Cooperation

Although formalized research cooperation agreements serve as valuable frameworks for actual research collaboration, we will also maintain and develop informal research outside the boundaries of these frameworks.

3.3 Organization of conferences and workshops

In order to maintain and increase our own visibility in the international community as well as the national awareness of the importance of ad-hoc networks, and also in order to do our share to promote these research areas internationally, we plan to organize at least one **international conference or workshop** (to which we will of course also extend a special invitation to relevant Norwegian researchers) during the project period. One option is to include a special session on optimization techniques in information theory within or in connection with one or more of the following workshops or conferences.

ITW2007
The Selmer Center is negotiating with the Board of Governors of the IEEE: Information Theory Society to organize an International Workshop on Information Theory in 2007. We plan to organize the workshop ITW in Bergen during the summer of 2007.

WCC2009
The conference Workshop on Coding and Cryptology - WCC has been organized by INRIA, France and the Selmer Center. The first three WWC99, WCC01 and WCC03 were organized by INRIA while WCC05 was organized by the Selmer Center. We are scheduled to organize WCC09 in 2009.

Participation in program committees etc
The senior researchers at the Selmer Center are regularly members of program committees of major international conferences. For example during the last year Helleseth, Kløve, Ytrehus, Parker, Semaev have been invited to participate in the program committees for several international conferences such as SASC (Brussel, Oct 2004) SETA04 (Seoul, Oct 2004), Indocrypt 04 (New Dehli, Dec 04), WCC05 (Bergen, March 2004), ITW05 (Rotorua, NZ, Aug 2005), ISIT05 (Adelaide, Sept 2005), NordSec, (Tartu, Estonia, Oct 2005) and IWSDA05 (Yamaguchi, Japan, Oct 2005). This is a very important task since it gives an excellent overview over recent research. At present Helleseth, Kløve and Ytrehus are associate editors of major international journals. This activity requires and produces an extensive international contact.

3.4 Publications
Researchers at the Selmer Center publish the results of their research in international journals of high reputation. Over the last 5 years the number of refereed journal papers and conference papers etc. (also including book chapters) are as follows:

Year	2000	2001	2002	2003	2004
Journal papers	17	29	11	17	27
Conf. papers	13	22	22	16	11

In total the researchers at the Selmer Center published **101** refereed **journal** papers and **84 conference** proceedings and books (chapters) during these 5 years. Among these papers, 35 were published in the IEEE Transactions on Information Theory, the leading journal in this area. The **185** publications above included **60** different **co-authors** from **20** different **countries**. Further, **114** (68 Journal papers and 46 Conference papers) of these had **at least one international co-author** (outside the Selmer Center).