

Theses at Department of Telematics Spring 2013 (web v3 11.12.2012)

The thesis proposals are classified due to which main profile they belong to.

These terms are used:

- NT = **N**ett og **T**jenestekvalitet (Networks and Quality of Service)
- TS = **T**jenester og **S**ystemutvikling (Services and System Engineering)
- IS = **I**nformasj**S**ikkerhet (Information Security)
- TØ = **T**ele**Ø**konomi (Tele-economics)
- TSA = **T**elematikk og **S**AMfunn (Telematics and society)

Some of the proposals are related to several main profiles.

The students can choose the topics they want as long as they have the proper scientific basis. Consult a professor if there are any doubts.

Please choose at least 5 topics in preferred order dispersed on several professors by registering name, e-mail address and topic numbers.

The Department will allocate the topics on a fair basis. We seek to distribute the responsibility of supervision equally among the professors. If conflicts occur, we have the opportunity to use a variety of methods to solve it. Drawing lots may be one way to go. Grades are not criteria for allocation. Empirically most students get one of their 3 top-most priorities.

Time schedule:

15 December:

Deadline for registration of wishes for thesis

Week 51:

The Department coordinates the choices and informs the students about the allocation.

By 14 January:

Register basic information about the thesis in DAIM, and submit master's thesis contract to Mona Nordaune, room B-213.

Topics from IDE portalen: <http://www.ideportalen.no/>

If you find an interesting topic here, please contact the Department of Telematics before you approach the company offering the topic.

1. (IS) NFC in vehicles

Problem statement

One of the main problems of effective usage NFC in vehicles is untraceability, anonymity and protection against different types of attacks (the most effective of it is so called “masquerade”).

In many cases (for example stolen the vehicle) it is necessary to have a possibility by owner order to change authentication protocol from anonymity mode to identification mode. It means that in ordinary case nobody could have possibility to watch the vehicle, but in emergency cases and in the consent of the vehicle owner it should be possible to change authentication protocol and to obtain the possibility to watch his/her vehicle.

It is exists some protocols for anonymity authentication for RFID. Main disadvantage of these schemes – they use several rounds of questions-answers and therefore it needs time and energy for authentication protocol. They also have no possibility to change mode from untraceability to “watch the vehicle”.

Purpose and objectives of project

To investigate the authentication protocol for RFID with following properties:

1. To minimize time and energy which is necessary for authentication
2. Anonymity of the RFID
3. Untraceability of the RFID – it means that it should not exist possibility to watch the vehicle with RFID by using authentication protocol
4. Protocol should be protected against “masquerade”
5. It should exist possibility to change protocol mode from untraceability to “watch the vehicle”

Supervisors: Sergey Bezzateev (bsv at aanet.ru)

Professor: Danilo Gligoroski (danilog at item.ntnu.no)

2. (IS) Distributed sensor network for monitoring the status of the pipeline

Problem statement

The task of this project is to design a distributed sensor network, which provides control of the pipeline.

Purpose and objectives of project

The main problems involved in the development of the protocols in the distributed sensor network:

1. Ensuring the chain of transmission from sensor - to sensor till the access point, providing information transmission over long distances. In this case, the topology "ant trail" of sensor network is used. The main problems in the solving of this problem is to ensure the accessibility and diagnosis of such topology. This implies the transfer and processing of information about the state of the pipeline from the sensors to the elements of aggregation (analysis and synthesis of information obtained from the sensors). In addition, by this network the telemetry information about the current state of the sensors (performance, battery level, etc.) is transmitted.

2. Protection of the transmitted information from accidental and intentional distortions. This problem could be solved by the cryptographic primitives based on the methods of the "light-weight" cryptography.

3. Protection against active attacks such as "intrude sensor insertion." The solution of this problem is based by message authentication on "light-weight" cryptography (one-time/multy-time signature on hash-chains, cover free families(CFF), code-based cryptography, etc.) By using the CFF it is possible to develop a system of authentication labels for sensors in the "ant trail" topology.

4. System and protocol for initial key distribution at the stage of the initial sensors installation and the protocol ensures the maintenance of the key distribution system during the installation of additional sensors, and replacing old sensors by new ones. Such protocols should eliminate the possibility of replacing the "right" sensors by "false" ones.

Supervisors: Sergey Bezzateev (bsv at aanet.ru)

Professor: Yuming Jiang (jiang at item.ntnu.no)

3. (IS) Håndtering av alvorlige IT-sikkerhetsbrudd

(Reservert Cathrine Hove og Marte Tårnes)

Alvorlige IT-sikkerhetsbrudd inntreffer med ujevne mellomrom, men i løpet av de siste årene har det vært rapportert et økende antall slike hendelser. Både generelle og målrettede angrep basert på bruk av ondsinnet programvare (malware), samt småfeil med store konsekvenser, er blant de typiske hendelsene. Hvordan hendelsene håndteres, varierer i svært stor grad. Rutiner, rapporteringsmetoder, beredskapsplaner, ansvarsfordeling, evnen til å reagere "riktig" i forhold til alvorlighetsgrad - det er mange faktorer som har innvirkning på hvor vellykket en organisasjon kan håndtere et IKT-sikkerhetsbrudd.

Det eksisterer likevel etter hvert anerkjente standarder og anbefalinger, i tillegg til mye erfaring hos ulike organisasjoner.

Interessante spørsmål er:

- hva slags planer eksisterer for håndtering av IKT-sikkerhetsbrudd?
- i hvor stor grad støtter man seg til eksisterende standarder og anbefalt praksis?
- i hvilken grad ble planene fulgt i et gitt tilfelle?
- i hvor stor grad ble eksisterende standarder og anbefalt praksis brukt?
- hva var vellykket, hva var mindre vellykket?
- hva kan omverdenen lære av enkelthendelsene?

En naturlig første del av oppgaven vil være å samle informasjon om alvorlige IKT-sikkerhetsbrudd som har rammet en eller flere norske virksomheter. Deretter vil det være interessant å systematisere erfaringer fra de ulike hendelsene og gjøre en studie av håndteringsprosessen.

Veileder: Maria B. Line, ITEM (maria.b.line at item.ntnu.no)

Faglærer: Jan Arild Audestad (audestad at item.ntnu.no)

4. (IS) Detection methodology study

As the number of new unique malware-samples seen every day continues to rise, finding new efficient ways to detect these with as little effort as possible is getting increasingly important. The purpose of this study is to find new innovative ways to generically detect large clusters of samples with varying similarities, with as little impact as possible on the system it is running on.

The candidate needs a genuine interest in low level programming and statistical analysis.

References:

<http://www.clamav.net/doc/latest/signatures.pdf>

The Art of Computer Virus Research and Defense, Szor, Addison-Wesley, 2005

This assignment is open for 1 student.

The project work can be conducted both on-site at Norman ASA and off-site. Regular meetings and/or conference calls are planned to support the student.

This research project will be conducted in cooperation with the anti-virus and forensic tools vendor Norman AS in Lysaker, Oslo. Guidance and insights are provided from a professional Research and Development (R&D) point of view.

Supervisor: Snorre Fagerland (snf at norman.com)

Professor: Yuming Jiang (jiang at item.ntnu.no)

5. (IS) Clean file harvesting system

One of the biggest challenges in the AV-business is how to add detection for the massive amount of new malware-samples seen every day without also detecting legitimate or clean files. The purpose of this project is to design and create a system that will automatically crawl the web for commonly used software, install the software on a virtual system and extract files never seen before to create and maintain a huge collection of clean files.

References:

Testing malware detectors, Christodorescu et al., ISSTA 04

This assignment is open for 1 student.

The project work can be conducted both on-site at Norman ASA and off-site. Regular meetings and/or conference calls are planned to support the student.

This research project will be conducted in cooperation with the anti-virus and forensic tools vendor Norman AS in Lysaker, Oslo. Guidance and insights are provided from a professional Research and Development (R&D) point of view.

Supervisor: Trygve Brox (tbr at norman.com)

Professor: Øivind Kure (okure at item.ntnu.no)

6. (IS) Attack vectors and hardening for a cloud-based system

Given is a set of commonly available server applications that can be joined in a 'stack' to provide the back-end for 'cloud based' services. The stack layers are 'database', 'application', web server', and 'user interface'.

Database layer	Application layer	Web Server layer	User Interface layer
MySQL	PHPS	Nginx	Javascript
Postgres	Java	Apache2	Flash
MongoDB	Python	IIS	HTML5
Microsoft SQL	Ruby	Tomcat	
	Node js	Tornado	
	C#		

Create and describe one or more stack constellations using the available components, while exploring the following properties of the stacks:

What possible attack vectors can the stack constellation(s) you choose have?

How can the attack surfaces be reduced?

If a system like this is being attacked, how do you know you are being attacked if the attacker does not want you to know?

Explore and demonstrate new techniques to detect and mitigate attempts to compromise the stacks through their network exposure.

This assignment is open for 1 student.

The project work can be conducted both on-site at Norman ASA and off-site. Regular meetings and/or conference calls are planned to support the student.

This research project will be conducted in cooperation with the anti-virus and forensic tools vendor Norman AS in Lysaker, Oslo. Guidance and insights are provided from a professional Research and Development (R&D) point of view.

Supervisor: Pål Tønder (pto at norman.com)

Professor: Professor: Øivind Kure (okure at item.ntnu.no)

7. (IS) Protocols for toll road systems

In a free-flow tolling system for cars, such as the AutoPASS system used in Norway, the cars do not have to slow down to pay the toll. The car is either registered by taking a picture of the license plate or by information in the on-board equipment (OBE, the AutoPASS tag installed in the car). The protocols used in the OBE have not been changed much in the last decades and there is room for improvements.

The master thesis will examine current methods for registering cars and current protocols used by the OBE, to analyze what kind of security they provide, and to what degree they are secure. The goal is then to build on current protocols or propose new protocols and systems that use better cryptographic primitives, offer the driver more privacy, uses digital currency, or in other ways are better than current protocols. Then see if such protocols are useful in real world systems.

Supervisor: Tord Ingolf Reistad Brukerfinansiering, Statens Vegvesen (tord.reistad at vegvesen.no)
Professor: Danilo Gligoroski (danilog at item.ntnu.no)

8. (IS) VPN vs LPC/IPLC for Crises Management in an Alert-situation.

SCENARIO:

A continuous and massive Cyber-attack on modern societies' IT-communications technology launched in cooperation between states and data-criminal groups.
(e.g. A variety of DDoS against merchant –, and money-transfer systems)

- May modern nations' computer-based information systems resist long lasting cyber-terrorism against their Virtual Private Networks? (Internet infrastructure!)
- or will fixed Leased Private Circuits (LPC), through "Dark Fiber", or SDH-/PDH- system be more reliable as a National Emergency Network upon a Cyber-attack?
(Permanent established in peace-time and restorable in residual infrastructure!)

Supervisor: Nils M. Aune, Noiseless a/s (nils at noiseless.no)

Professor: Øivind Kure (okure at item.ntnu.no)

9. (NT) Time synchronization in NATO Narrowband Waveform (NBWF)

The Norwegian Defence Research Establishment (FFI) in cooperation with KDA (Kongsberg Defence & Aerospace AS) is developing a TDMA (Time Division Multiple Access) based link layer to be included in the NATO Narrowband Waveform (NBWF), which is strongly capacity limited. In a TDMA system, it is imperative that radio nodes are synchronized w.r.t. time. FFI/KDA has sketched out a network time synchronization protocol for this purpose. It is desired that the student contributes with further development of this solution, as well as an assessment of whether the requirements are met in a set of various situations. Based on the student's background, the thesis can take two alternative approaches; Control-theoretic, or based on network simulation. Either way, the solution's ability to converge quickly in the different situations is to be studied. FFI will be involved with supervising w.r.t the concretization of the proposed algorithm.

Supervisor: Bjørnar Libæk (bjornar.libak at ffi.no)

Professor: Øivind Kure (okure at item.ntnu.no)

10. (TS) Motion detection for games and applications

The project shall develop, extend a library for motion detection of know elements in a picture. This involves both still and video images.

The project should result in a library for use in games and applications.

There are some existing libraries for motion detection like OpenCV, som operating systems also supprt som motion and eyetracking

The product should implement and eventdriven architecture and that lets us define motion patterns and events.

Motion detection is to focus on body parts: arm, hand, finger, face (eyes)
auto mask will also be a good feature.

deliverables:

- research on existing libraries, possibilities, precision, OS support.
- Library for event driven motion detection
- Applikasjon for mac osx that detects motion from camera and maps to scripts or action events like mouse/keyboard. So applications could be controlled by camera.
(typically mouse gestures drag-swipe)
- IOS application that uses the library.

motion events:

- eye tracking, where do the users look at the monitor
- eye blink
- finger recognition: how many fingers, what direction are they moving.
- hand movement (left / right hand)

Important issues:

- how precise can it be.
- what features are already supported in the different OS.
- preview image on screen, mark detected areas
- performance on library.

Supervisor: Jan Erik Wold (janerik at ablemagic.no)

Professor: Leif Arne Rønningen (leifarne at item.ntnu.no)

11. (TS/NT) Telepresence Quality

Give a short reflected overview of existing telepresence systems and research on their perceived quality, e. g., Tandberg/Cisco. Discuss the importance of high perceived quality, low delay, high frame rate and more than two-view video in telepresence. Review proposed, and if necessary extend test paradigms, including necessary equipment for testing perceived quality of video and sound, for testing coming telepresence collaborations. In Item labs, various cameras and projectors that provide 120 fps in 2D and 60 fps in 3D, and sound equipment are available.

Apply the test paradigms to cases when the musicians and the conductor play together over IP networks. <http://www.item.ntnu.no/people/personalpages/fac/leifarne/collaborationspaces>

Supervisor: Leif Arne Rønningen, Item

Professor: Leif Arne Rønningen (leifarne at item.ntnu.no)

12. (TS/NT) Experimentation with sparse aperture cameras and luminance layering

Study and describe the use of separate color (RGB) and luminance (L) sensors, and the sparse aperture technique in video shooting. Carry out experiments where the frame rates of L- and RGB cameras are varied when shooting objects move (controlled, repeatable) at varying speed. Vary the exposure time, the aperture and the position of cameras to simulate sparse apertures and luminance

layering. Premiere/After Effects/Photoshop can be used for off-line editing before the final video is shown on a high-quality display. Apply mixed qualitative and quantitative methods to evaluate the perceived quality of the videos.

<http://www.item.ntnu.no/people/personalpages/fac/leifarne/collaborationspaces>

Supervisor: Leif Arne Rønningen, Item

Professor: Leif Arne Rønningen (leifarne at item.ntnu.no)

13. (NT) The AppTraNetLFC protocol on FIRE

The AppTraNetLFC protocol is a combined protocol supporting the link-, network-, transport- and application layers in IPv6 networks. If network nodes and networks are properly designed, the protocol can guarantee the maximum end-to-end delay. FIRE, Future Internet Research Experimentation, is a big EU FP7 funded project, providing several test beds for experimentation. Design, implement and test by measurement a selected sub-set of the AppTraNetLFC protocol on a selected FIRE experimentation platform.

http://www.item.ntnu.no/people/personalpages/fac/leifarne/the_dmp_architecture

<http://www.ict-fire.eu>

Supervisor: Leif Arne Rønningen, Item

Professor: Leif Arne Rønningen (leifarne at item.ntnu.no)

14. (NT)Implementering av frekvensallokeringsalgoritmer i simulator

Fram til nå har konsesjoner for bruk av frekvenser blitt tildelt av Post og Teletilsynet tidsperioder på flere år. Etter hvert som vi går tom for ledige radiofrekvenser har det blitt foreslått at man åpner for mer fleksibel frekvenstildeling ved hjelp av datamaskiner. Over hele verden har det blitt gjort forsøk med sentrale frekvensdatabaser der brukere som trenger en frekvens kontakter databasen over Internett og kan hente informasjon om hvilke frekvenser de kan bruke. Etter at databasen har blitt kontaktet må radioene selv utføre en frekvensallokering basert på informasjonen de har innhentet.

På FFI har vi utviklet en simulator for å evaluere hvordan dette oppfører seg i store nettverk, typisk på en million noder og oppover. Hvilke algoritmer man velger påvirker både hvor godt man får utnyttet frekvensene og hvor ofte databasen må kontaktes. Denne oppgaven består i å implementere kjente frekvensallokeringsalgoritmer i simulatoren og deretter undersøke hvordan disse oppfører seg i stor skala. For lang oppgave er det aktuelt å se på mulige optimaliseringer som kan gjøres både i databasen og i allokeringsalgoritmene.

Oppgaven krever kunnskap om programmering i Java, samt noe bakgrunn fra signalbehandling.

Simulatoren er utviklet av doktorgrads kandidat **Magnus Skjegstad** som vil være veileder

Veileder: Magnus Skjegstad (magnus at skjegstad.com)

Professor: Øivind Kure (okure at item.ntnu.no)

15. (NT) Simulation and analysis of a routing protocol for heterogeneous mobile ad hoc networks

Mobile ad hoc networks are of particular interest to the military for areas where no infrastructure exists or can be established. FFI has run multiple experiments with MANET in a tactical setting.

Currently we have an ongoing project in close cooperation with the University Graduate Centre (UNIK) where we study routing for very heterogeneous MANETs. With a heterogeneous MANET we mean a network built of radio-links with very different characteristics (data-rate, jitter, delay, etc.). In this project we have proposed an overlay routing protocol for this challenging environment.

We are looking for master students that are interested in working with us on simulation and analysis of a routing protocol for this scenario. We are using state of the art in open source network simulation environment (ns3 <http://www.nsnam.org/>) and will also use ns3's interface to the Click Modular Router (<http://www.read.cs.ucla.edu/click/click>) for implementation of the protocol in a test bed.

Supervisors: Paal Engelstad, +47 63807958 ,(Paal.Engelstad at ffi.no)

Mariann Hauge, +47 63807269, (Mariann.Hauge at ffi.no)

Professor: Øivind Kure (okure at item.ntnu.no)

16. () Bilens sensor / Vehicle probe data

Cooperative systems enable M2M exchange of information between vehicles and infrastructure. Modern cars are full of sensors containing a lot of information about the condition, temperature, fuel consumption, speed, etc of a vehicle. This information is also of interest to road authorities if this information is made available from a sufficient number of vehicles. This will provide an overview of the road network condition over a large area. For winter maintenance this could be helpful for plowing and sanding of exposed roads if road conditions change.

This is a hands-on activity on using the car as a sensor. In the first place one should connect to the OBD-II connector in a car and upload sensor data to the cloud. One should use sensor data from both the car and a smartphone. Part of the task could be to compare and evaluate data from the vehicle and smartphone sensor platforms.

Lenker/Links:

http://en.m.wikipedia.org/wiki/OBD-II_PIDs#section_2

<http://www.arduino.dev.com/hardware/obd-kit/>

<http://www.redpark.com/c2db9.html>

Supervisor: Erik Olsen (erik_olsen at vegvesen.no), Jo Skjermo (jo.skjermo at vegvesen.no)

Professor: Yuming Jiang (jiang at item.ntnu.no)

17. (TS) Cross-device mobility for HTML5 applications

More and more devices, such as smartphones, smart TVs and tablets, are nowadays able to run applications. Unfortunately, the applications written for one device are not always compatible with

other devices. With HTML5 this scenario is changing. HTML5 allows creating multimedia applications able to work offline, and that can be run on any device with an HTML5-compatible web browser. The importance of HTML5 has been recognized by mobile device manufacturers, telco operators and Internet players that are joining forces to create mobile operating systems, such as FirefoxOS and Tizen, where HTML5 applications will run as native applications (i.e. without the need for a web browser).

While HTML5 allows running the same application on different devices, the user cannot yet move running applications from one device to another (i.e. start a video streaming application in her smart TV, move to her tablet and continue there the streaming at the point she left it on the TV). This project aims at finding a solution for this, by designing a platform providing cross-device mobility mechanisms for HTML5 applications. A prototype of the solution should be implemented and tested with a demo application.

Supervisor: Humberto Castejón, Telenor Research and Future Studies (humberto.castejon at telenor.com)

Professor: Peter Herrmann, Department of Telematics (herrmann at item.ntnu.no)

18. (NT) Flexible Optical Networks

Most of today's deployed Dense Wavelength Division Multiplexing (DWDM) networks carry rigid data-rates (10, 40 and 100 Gbps) channels with a fixed channel spacing (100GHz and 50GHz as defined by the ITU). Where long connections requires frequent optical-electrical-optical regeneration to maintain a low-enough bit error rate while short connections operate with large margins on signal quality that could have been used to transmit at a higher data-rate. Regardless the nature of the incoming client signal and the distance it should be carried the optical system uses the same set of rules to transfer the client signals.

Reconfigurable Optical Add Drop Multiplexers (ROADM) have allowed the remote switching of optical signals at the wavelength level but the establishment of new connections is still a complex issue. Operators are therefore forced to plan their networks according to the peak traffic they expect a few years ahead.

This is a particularly difficult thing to plan given the fast pace at which applications and services evolve. Such estimation of worst-case required capacity is further complicated by the increasingly dynamic nature of the traffic. The traffic churn (peak to average ratio) due to novel rich content services such as High Definition Video indeed increases, even in core networks where numerous demands have been aggregated.

Taking these issues in to consideration optical networking will evolve from being a rigid system with a fixed set of rules regarding symbol rate, modulation, coding, grid and in advance defined hardware fabrications -> to a system controlled by software to define and adjust different parameters with regards to individual wavelength accommodating single or multiple client signals demands.

The evolution in high speed electronics and signal processing makes it possible to use more advance coding and modulations technologies and at the same time coherent technology will allow higher reach pr. channel rate with same OSNR margin as being used in current available systems being

deployed today.

The new functionalities will make it possible to effectively offer more flexibility in the optical systems. This has already been the case for the recent 100G developments which have emerged thanks to new advance technologies brought by high speed electronics and coherent technologies.

Further channel rate expansion will probably use the multi carrier modulation in addition to 100 Gbps technology enablers to reach channel rates beyond 100 Gbps. The utilization of a new set of enabling technologies beside dynamic use of optical spectral frequency and software enabled optic will bring more flexibility into the optical domain. In addition software enabled optic and terabit enabling technologies will work together to optimize optical resources dynamically and more efficient. This task will investigate the novel concept of the ability to optically transmit data with flexible variable spectral efficiency in order to make better use of optical networks.

Supervisor: Kurosh Bozorgebrahimi (kurosh at uninett.no)

Steinar Bjørnstad (ITEM/Transpacket) (Steinar.Bjornstad at item.ntnu.no)

Phone: 90081033

19. (IS) Hvordan avdekke tyveri av identitet eller sesjoner i WLAN?

Til denne oppgaven søkes dyktig nettverksdetektiv!

Kriminalitet skjer i stadig større grad over nett og en viktig forutsetning for å bekjempe denne type kriminalitet er å kunne spore opp brukere. WLAN er den mest utbredte aksessformen til internett og et stort problem er at det per i dag er mulig å stjele og misbruke en brukers tilkobling eller sesjon. Hvordan kan vi avdekke sesjonstyveri?

Trådløse Trondheim har sammen med studenter på NTNU jobbet med ulike måter å detektere sesjonstyveri på. Arbeidet som gjøres her ligger svært langt fremme og nylig det ble det publisert artikkel som oppsummerer arbeidet så langt: http://tradlosetrondheim.no/pdf/Spoof_WiFi.pdf

Vi ønsker nå å se om det er mulig å bruke ett slikt system i praksis.

Veileder: Trådløse Trondheim v/Thomas Jelle (thomas.jelle at item.ntnu.no)

Faglærer: Yuming Jiang (jiang at item.ntnu.no)

20. (TS?) How to combine sensor information and WLAN to obtain more accurate indoor positioning

Since 2009, Wireless Trondheim has been working on indoor navigation with their app found at www.campusguiden.no. The system primarily uses WLAN RSSI values to position the user. Most modern smartphones are equipped with a wide range of sensors that could be used to increase the accuracy and frequency of the positions that our system deliver. E.g. a compass and an accelerometer could be used to determine the users movement and by applying a Kalman filter, these readings can be fused with the initial position estimated by the existing system.

The task is to deliver better positioning by using a smartphone's sensors.

Veileder: Trådløse Trondheim v/Åsmund Tokheim (asmund at tradlosetrondheim.no)

Professor: Yuming Jiang (jiang at item.ntnu.no)

21. (NT) Demanding services and applications in optical packet networks

TransPacket AS (www.transpacket.com) develops the fusion networking technology for efficiently serving both the most demanding services as well as best-effort services.

Latency and synchronisation needs are hot topics when deploying packet switched optical networks.

In the project the student shall analyze the Quality of Service (QoS) performance needs in optical networks for different applications and services like e.g. current and future mobile backhaul services, high-speed robotic trading services, future TV like e.g. 3D-TV, future/current online-gaming etc. Both the needs of current applications and possible future applications shall be analyzed. Special attention shall be given to tolerance to delay and packet delay variation.

Moving from circuit switched to packet switched networks, Quality of Service (QoS) is an important topic. A number of mechanisms exist for packet switched networks for enabling the networks to support demanding applications. Typically, performance parameters like packet loss ratio, packet delay and packet delay variation are measures that should be optimized according to the applications demands. In circuit switched networks, packet loss and packet delay variation may be zero, and packet delay very low. It is however very demanding (if possible) to offer a QoS as good as in a circuit switched network, through a packet switched network. An important question to rise is if such a high QoS is really needed and how high QoS that is needed for current and future applications that shall be serviced by the network.

Co-supervisor: Raimena Veisllari (veisllar at item.ntnu.no)

Professor: Steinar Bjørnstad (ITEM/Transpacket) (Steinar.Bjornstad at item.ntnu.no)

Phone: 90081033,

22. (NT) Fusion network performance experiment

TransPacket is a startup-company that has implemented the novel fusion technology, also called OpMiGua integrated hybrid networks (www.transpacket.com). In the project the student will perform a network experiment involving TransPacket H1 nodes measuring performance parameters like latency, latency variation (packet delay variation) and packet loss. The experiment shall be performed in the laboratory of TransPacket in Oslo. Remote operation of experimental equipment is available.

The fusion concept (<http://www.transpacket.com>) has the main objective of combining the best properties from both circuit and packet switched networks into a hybrid solution. A number of studies show that the performance properties of the OpMiGua (fusion) network are found attractive.

Co-supervisor: Raimena Veisllari (veisllar at item.ntnu.no)

Professor: Steinar Bjørnstad (ITEM/Transpacket) (Steinar.Bjornstad at item.ntnu.no)

Phone: 90081033,

23. (NT) Green Telecom and lowered cost through power-optimized transport/metro networks

TransPacket AS (www.transpacket.com) develops the fusion networking technology for efficiently serving both the most demanding services as well as best-effort services and save power. Both because of the green telecom trend and the general demands for lowering power consumption in telecom equipment, there is a need for optimizing network designs with respect to lowered power-consumption. There is also an increasing focus on the benefit of the lowered operational cost achieved through lowered power consumption. Availability of electricity depends on the infrastructure of a country. A general rule of thumb may be that heavy processing should be performed where access to renewable electrical power sources is high. The project will explore the effect of optimizing the load-balance and the processing in the network with respect to power-consumption. Generally, processing in the network should be minimized through using e.g. optical bypassing nodes. Furthermore, processing at sites with poor and hence expensive access to electricity should be minimized, moving heavy traffic processing to sites with high and cheaper electricity availability. Electricity availability may experience time-of-day variations. Hence network load-balancing mechanisms may act accordingly. The parameters involved in enabling a green telecom transport/metro network shall be outlined. Reduction in power-consumption and optimization on power-consumption cost shall be analyzed and quantified. Analysis may be performed using e.g. simulation-techniques. Techniques for controlling the network, like e.g. extensions to routing protocols may be explored further in the master-project.

*Professor: Steinar Bjørnstad (ITEM/Transpacket) (Steinar.Bjornstad at item.ntnu.no)
Phone: 90081033,*

24. (NT) Environmentally friendly and cost reduced transport/access network-nodes through power optimization

TransPacket AS (www.transpacket.com) develops the fusion networking technology for efficiently serving both the most demanding services as well as best-effort services. Both because of the green telecom trend and the general demands for lowering power consumption in telecom equipment, there is a need for optimizing network node designs with respect to lowered power-consumption. There is also an increased focus on the benefit of the lowered operational cost achieved through lowered power consumption. The project will explore the effect of different power-reduction techniques on a node-system level (not on a circuit level). Examples of techniques are e.g. reducing the nodes processing needs through avoiding processing of traffic transiting the node and reducing node interface power consumption through turning interfaces off during low-load/idle periods. Parameters impacting the power consumption of a node may be varied for characterizing what are the most important parameters for reducing power in nodes and networks. The reduction in node power-consumption shall be quantified relatively and its implication on total power consumption for a complete network shall be outlined.

*Professor: Steinar Bjørnstad (ITEM/Transpacket) (Steinar.Bjornstad at item.ntnu.no)
Phone: 90081033,*

25. (TØ/NT) Cost analysis comparing the fusion network with pure packet and pure circuit switched networks

TransPacket is a startup-company that has implemented the novel fusion technology, also called OpMiGua integrated hybrid networks.

The fusion concept (<http://www.transpacket.com>) has the main objective of combining the best properties from both circuit and packet switched networks into a hybrid solution. A number of studies show that the performance properties of the OpMiGua (fusion) network are found attractive. However, studies addressing the cost-efficiency of the network are limited. In this project, the student will analyze the cost of a network utilizing a TransPacket OpMiGua node and compare this with the cost of pure circuit and a pure packet switching.

Co-supervisor: Raimena Veisllari (veisllar at item.ntnu.no)

Professor: Steinar Bjørnstad (ITEM/Transpacket) (Steinar.Bjornstad at item.ntnu.no)

Phone: 90081033,

26. (NT) Operation and management (OAM) in Ethernet and MPLS-TP packet based networks

Operation and Management is currently one of the most important issues addressed when carriers are implementing packet switched optical networks. TransPacket is a startup-company (www.transpacket.com) that has implemented the novel fusion technology, also called OpMiGua integrated hybrid networks (www.transpacket.com). TransPacket is now working on implementing monitoring functions in the TransPacket products. In the project, protocols for monitoring will be studied in detail and an overview shall be given. Pros and cons of the different solutions shall then be evaluated. A part of the study may include a simulation analysis.

Migrating from the reliable high performance SDH network to a fully packet based network, puts high demands on the packet network. For fulfilling these demands, existing protocols are extended, trying to bring known functions in circuit switched systems like monitoring and traffic engineering into the packet switched network.

Recently, a number of extensions to existing protocols for transport networks have been proposed. Examples are the Transport Profile extension to MPLS: MPLS-TP, bringing OAM capability to MPLS. Similar features are brought into Ethernet: Link-OAM and Service-OAM. Furthermore, the OTN (Optical Transport Network) standard is proposed as a predecessor for SDH, enabling a physical layer transport protocol for optical networks.

Co-supervisor: Raimena Veisllari (veisllar at item.ntnu.no)

Professor: Steinar Bjørnstad (ITEM/Transpacket) (Steinar.Bjornstad at item.ntnu.no)

Phone: 90081033,

27. (NT) Circuit switching still lives on in optical networks: OTN switching

Market trends shows that circuit switching in optical networks, previously implemented with SDH/SONET but now being replaced by OTN switching, is one of the fastest growing markets in optical networks. TransPacket is a startup-company that has implemented the novel fusion

technology, also called OpMiGua integrated hybrid networks (www.transpacket.com). TransPacket is now looking into the OTN technology for potentially integrating this technology in future products.

In the project, the student will study recent progress in OTN, including the OTN switching capabilities. Performance of a pure packet switched network shall be compared with the performance of an OTN switching based network. The performance comparison will typically be performed on a proposed network scenario. Performance may be found using analytical and/or simulation methods.

The OTN (Optical Transport Network) standard is an ITU-T standard (G.709) describing a method for wrapping in signals of different protocol-formats for transport across an optical network. OTN is seen as a predecessor for SDH, enabling much of the same monitoring and management capabilities known from SDH. While the first versions of the OTN-standard describes transport at 2.5 and 10 Gb/s wavelength-channel bitrates, the standard has recently been extended to include bitrates up to 100 Gb/s and down to 1 Gb/s. Furthermore, while OTN originally where only described as a method for reliable data-transport, switching of sub-wavelength bitrates has recently proposed. This enables e.g. add/drop at the OTN layer of parts of e.g. a 100 Gb/s stream, enabling the use of 10 Gb/s interfaces on IP-routers in a 100 Gb/s transport network.

Co-supervisor: Raimena Veisllari (veisllar at item.ntnu.no)

Professor: Steinar Bjørnstad (ITEM/Transpacket) (Steinar.Bjornstad at item.ntnu.no)

Phone: 90081033,

28. (NT) Mobile-backhaul packet network properties and alternatives

This topic is suitable for 2-3 projects.

TransPacket is a startup-company that has implemented the novel fusion technology, also called OpMiGua integrated hybrid networks (www.transpacket.com). TransPacket addresses the mobile-backhaul network with the unique fusion technology.

There are several student-projects addressing different issues within the same main topic. The projects may typically involve the following topics and is suitable for being continued in a master:

The fusion concept, or also called the “Optical Migration Capable Networks with Service Guarantees” (OpMiGua) concept (<http://www.opmigua.com>) has the main objective of combining the best properties from both circuit and packet switched networks into a hybrid solution. While the OpMiGua previously has been studied for large powerful transport networks with many wavelength channels, the main objective of this project is to find how the OpMiGua hybrid principle may be applied and how it will perform in a network containing only a few, or only a single channel. Mobile-backhaul networks are moving from the use of circuit-switched technology towards using packet switched technology. Ethernet is brought out as the main candidate technology. Combining Ethernet and the OpMiGua principle may be an attractive solution by bringing the circuit switched properties of OpMiGua to Ethernet.

- 1) How to transport synchronisation information across the packet based mobile-backhaul network. The student will study the properties of the alternatives in detail, including synchronous Ethernet and IEEE 1588.
- 2) QoS in mobile backhaul-networks. What level of QoS is required and how is this supported in an OpMiGua Ethernet mobile back-haul.
- 3) Characterizing the node and/or network performance through discrete-event simulation: An OpMiGua network being applied with a single or only a few channels (wavelengths).

Co-supervisor: Raimena Veisllari (veisllar at item.ntnu.no)

Professor: Steinar Bjørnstad (ITEM/Transpacket) (Steinar.Bjornstad at item.ntnu.no)

Phone: 90081033,

29. (NT/TS) Internet Control for Residential Users

Internet based services have become an important part of our lives, and broadband access has reached the commodity phase in most developed countries. A growing portion of the time spent on-line among younger Internet users are related to social media and entertainment services. This evolution is not possible or even desirable to reverse, but for certain user groups it is clear that some level of control and restrictions are required. There are many examples of children which are addicted to "being online" while their parents do not even know about the situation. There are many solutions for parental control in the market today which address this problem, but they are all either very easy to bypass or too difficult to understand and use for e.g. parents. The children are in many cases smarter than their parents when it comes to Internet.

The scope of this project is to make a prototype of an Internet Control solution for Residential Users based on the Raspberry PI model B HW and Linux OS, or an alternative platform if found appropriate. The solution should be controlled from a central server, and the administration interfaces offered to system administrators should come from here. Candidate interfaces are app's for iphone and/or Android, SMS control and regular web interfaces. The development is expected to require programming in Java and HTML, and a selection of whatever scripting tools/languages appropriate on the development platform. Knowledge about Linux, iOS and Android are beneficial.

Supervisor: Bjørn J. Villa (bvilla at item.ntnu.no)

Professor: Poul E. Heegard (poul.heegaard at item.ntnu.no)

30. (NT, IS) Discovering traffic anomalies using flow-based analysis (1 - 2 students)

Internet traffic attacks are increasing in number and can infect / affect a vulnerable machine within a few minutes. Traditional packet level inspection techniques cannot easily be performed at high-speeds. Flow-based intrusion detection techniques are a promising alternative where the flow of data traffic is analyzed, instead of individual packets. This requires that attacks be identified only using header information. There are two main tasks:

T1. Analyze collected traffic data at flow level from UNINETT links.

T2. Identify the classes of attacks that can be detected using NetFlow, determine the frequency of the

different attacks, and see if there has been a general change in the use of Internet.

More specifically, the requirements include

T1.1. Analyze flow level traffic statistics based on NetFlow traffic data, such as flow inter-arrival time distribution, flow size (in packets and in bytes) distribution and flow life-time distribution. This analysis may be applied to different flow aggregate levels, such as source IP address, destination IP address, UDP, TCP, input interface, output interface, etc.

T1.2. Based on flow level traffic analysis, perform traffic anomaly detection using an entropy-based detection method. Particularly, the entropy time series of flow inter-arrival time, flow size, flow lifetime, or their combinations may be considered.

T1.3. Based on flow level traffic analysis, perform structural analysis of flow inter-arrival time, flow size, and flow lifetime, using the principal component analysis (PCA) method, through which, traffic anomalies are detected.

T2.1. Based on detected traffic anomalies, determine the frequency of the anomalies.

T2.2. Based on the properties of various classes of attacks, identify the attack classes from the detected anomalies.

T2.3. Based on detected attacks, determine the frequency of the different attacks and see if there has been a general change in the use of the network.

Supervisor: Arne Øslebø (uninett) (arne.oslebo at uninett.no)

Professor: Yuming Jiang (jiang at item.ntnu.no)

31. (IS) Anti-spyware app for smartphones

The widespread use of smart phones and apps with extensive access rights has left businesses vulnerable to a whole new range of attacks [1]. Seemingly legit apps can activate the microphone or camera and during meetings or situations where sensitive information is discussed. Both users and businesses are left with few tools to ensure that no such recording can take place.

This assignment will develop an anti-spyware app to let users and businesses assess the surveillance potential of running and installed apps and subsequently let users stop, block or remove potential threats to businesses. Different avenues of automation shall also be explored, so as to relieve the user of the effort in monitoring running applications and provide organisations the ability to remotely enforce a security policy.

[1] <http://infosec.sintef.no/2012/03/smartmobiler-er-bedrifter-klare-for-utfordringen/> (In Norwegian)

Supervisor: Åsmund Ahlmann Nyre, SINTEF ICT (Asmund.A.Nyre at sintef.no) or Erlend Andreas Gjerde, SINTEF ICT

Professor: Yuming Jiang (jiang at item.ntnu.no)

32. (TØ,IS,NT). Coded networks

Network coding is a concept utilizing packet redundancy in order to increase performance in communication networks. Network coding has been extensively studied as, among others, an effective approach to provide multicast in communication networks. However, network coding may also be used in a wider context, as a new approach to provide packet transport in the Internet - Coded networks. In this assignment, the student will look into how network coding can be used to provide secure, reliable and cost-efficient packet transport with high performance. The student may choose to focus on one or several aspects of network coded packet transport, depending on the students background.

In particular, the student will study the following:

Background study of network coding

Development and analysis of a network coding scheme, taking into account performance, security and cost aspects

Limit: 1 student

Supervisors: Gergely Biczok (gbiczok at item.ntnu.no), Danilo Gligoroski (danilo.gligoroski at item.ntnu.no)

Professor: Danilo Gligoroski (danilo.gligoroski at item.ntnu.no)

33. (TØ,IS) Cyber insurance: theory and practice

Security breaches are increasingly prevalent in the Internet age causing huge financial losses for companies and their users. Cyber insurance is a powerful economic concept that can help companies in the fight against such malicious behavior. The prospective student will study the basics of cyber insurance, conduct a market survey and explore/model the possible use of cyber insurance in a cloud computing/social network environment.

Limit: 1 student

Supervisor: Gergely Biczok (gbiczok at item.ntnu.no)

Professor: Jan Aril Audestad (audestad at item.ntnu.no)

34. (TØ,IS,NT) Interdependent security: network formation games

Interdependent security demands more attention, as companies, applications, services and software components are increasingly dependent on each other. Such interdependency can be described with a graph, and some graphs yield "higher security" (e.g., insurable topologies) than others. The prospective student will identify favorable networks, study their characteristics and model their emergence using game theory.

This topic enables the student to contribute to cutting-edge research in the intersection of economics, security and network science.

Limit: 1 student

Supervisor: Gergely Biczok (gbiczok at item.ntnu.no)

Professor: Jan Aril Audestad (audestad at item.ntnu.no)

35. (TØ,IS,NT) Interdependent privacy: are your friends for real?

Users of today's online services share massive amounts of personal information and opinion with each other and the respective services every day. In such an interconnected setting, the privacy of individual users is bound to be affected by the decisions of others, giving rise to the phenomenon which we term as interdependent privacy. The prospective student will conduct a case study on a real ecosystem (e.g., Android, cloud service, social network services, blogs, etc.), show the presence of interdependent privacy, and build a game-theoretic model to quantify its impact. This topic enables the student to contribute to cutting-edge research in the intersection of economics, social networks and privacy.

Supervisor: Gergely Biczok (gbiczok at item.ntnu.no)

Professor: Jan Aril Audestad (audestad at item.ntnu.no)

36. (TØ,NT) Know your blogs: a statistical analysis

Blogs are a defining and popular part of the Web 2.0 movement, providing long-tail content to millions of readers. While blogs are everywhere, their statistical properties regarding popularity, number of comments, comment inter-arrival and trackbacks are largely undiscovered. The prospective student will crawl the most popular blog-providers -- Norwegian and international, conventional and micro (Twitter) -- collect data on various blog-related metrics, and use statistical analysis to infer the characteristic distributions of these metrics across the investigated blogs.

Limit: 1 student

Supervisor: Gergely Biczok (gbiczok at item.ntnu.no)

Professor: Poul E. Heegard (poul.heegaard at item.ntnu.no)

37. (TØ,IS) FlipIt: game-theoretical system security

Recently, researchers at leading security company RSA have identified the importance of game theory in understanding and designing secure mechanisms and systems. RSA has proposed FlipIt, a flexible game-theoretical framework capable of capturing stealthy takeover by malicious attackers. The prospective student will study the original FlipIt game, propose useful extensions/modifications and conduct a case study on a practical application scenario (e.g., crypto systems, cloud services, secure file-sharing) using the modified game. This topic enables the student(s) to contribute to cutting-edge research in the intersection of economics and security.

Limit: 2 students

Supervisor: Gergely Biczok (gbiczok at item.ntnu.no) Danilo Gligoroski (danilo.gligoroski at item.ntnu.no)

Professor: Danilo Gligoroski (danilo.gligoroski at item.ntnu.no)

38. (TØ) Can long-tail markets emerge in equilibrium?

The long tail phenomenon have been much discussed both in popular and scientific literature in the last years. However, endogenous models which can explain the emergence of long-tail markets are still mostly qualitative. The prospective student will model both the supply and the demand side of online markets with game theory, and try to reason for a long-tail equilibrium. Also, a repeated game should be formed to see if the change in the tail over time experienced by Brynjolfsson et al. can emerge. This topic enables the student(s) to contribute to cutting-edge research in the intersection of economics and computer science.

Limit: 2 students (1 place reserved for Håvard Halse)

Supervisor: Gergely Biczok (gbiczok at item.ntnu.no)

Professor: Jan Arild Audestad (audestad at item.ntnu.no)

39. (TØ,NT) Network nephology: a content providers's dilemma

Content providers are facing a decision whether to completely migrate their resources to the cloud or to utilize a hybrid of in-house and cloud infrastructure. On the other hand, end-users using the services of these providers have high expectations for their quality of experience. The prospective student(s) will investigate the interplay of end-users, content providers and cloud operators based on a game-theoretical model. The student(s) will analyze the incentives and stable outcomes, and discuss the implication of the results in light of the current cloud operator landscape. This topic enables the student(s) to contribute to cutting-edge research in the intersection of economics and computer networks.

Limit: 2 students (1 place reserved for Øystein Wethe Hanssen)

Supervisor: Gergely Biczok (gbiczok at item.ntnu.no)

Professor: Jan Arild Audestad (audestad at item.ntnu.no)

40. (IS/TS) Identity Management in Cloud computing

Reservert Cathrine Hove

Supervisor: Ivar Jørstad, Ubisafe (ivar at ubisafe.no)

Professor: Thanh Van Do (thanh-van.do at telenor.com)

41. (IS/TS) Web login on Smartphones

Reservert Jonas Hoemsnes

Supervisor: Ivar Jørstad, Ubisafe (ivar at ubisafe.no)
Professor: Thanh Van Do (thanh-van.do at telenor.com)

42. (NT) 4G and ITS – How to utilize LTE technology in ITS (intelligent Transport Systems) instrumentation

Reservert Morten André Larsen

Veileder: Roy Ove Nilssen, Tjenestesjef mobildata, Netcom AS
Faglærer: Steinar Andresen (steinara at item.ntnu.no)

43. (NT) Future Rail Communication - A comparison between GPRS, EDGE and LTE

Reservert Steffen Amundsen

Veileder: Ragnhild Wahl R&I Norwegian Railroad
Faglærer: Steinar Andresen (steinara at item.ntnu.no)

44. (IS) “Categorization of the Chrome extensions according to their invasion of users privacy”

There are more than 10,000 extensions in the Google Chrome web browser. The students first will have to describe the programming techniques for producing Chrome extensions, and then will have to make an extensive categorization of the extensions according to their access to the users private browsing data and activity (in the range from non-invasive, via modestly invasive, up to highly-invasive extensions). For example, some of the extensions can be so invasive towards the users privacy, such that they will demand an access to users data on all open tabs and websites and will record the browsing activity (example: TS Magic Player). It would be preferable if the students know some of the programming skills for producing a Chrome extension, and then write an extension that will inform user in which category belongs the extension that they want to install.

This assignment is open for 2 students.

Professor: Danilo Gligoroski (danilo@item.ntnu.no)

45. (IS) “Security and privacy issues and mechanisms in Chrome and Firefox”

Browser security is the application of internet security to web browsers to protect computer systems, networks, and data, from malware or breaches of privacy. Browser security exploits often use JavaScript - sometimes with cross-site scripting (XSS) - sometimes with a secondary payload using Adobe Flash, but can also take advantage of many other vulnerabilities (security holes) that are commonly exploited in all browsers. The students will have to study in details and extensively all the security and privacy issues in two most popular web browsers in the world: Mozilla Firefox and Google Chrome.

This assignment is open for 2 students.

Professor: Danilo Gligoroski (daniloq@item.ntnu.no)

46. (IS) "Security mechanisms in I2P Anonymous Network"

I2P is an anonymizing network, offering a simple layer that identity-sensitive applications can use to securely communicate. All data is wrapped with several layers of encryption, and the network is both distributed and dynamic, with no trusted parties.

Many applications are available that interface with I2P, including mail, peer-peer, IRC chat, and others. The I2P project was formed in 2003 to support the efforts of those trying to build a more free society by offering them an uncensorable, anonymous, and secure communication system. I2P is a development effort producing a low latency, fully distributed, autonomous, scalable, anonymous, resilient, and secure network.

The goal of the thesis is to scrutinize all security mechanisms in I2P, to set up several (at least two) servers, to set up all the applications that are capable to interface with I2P, and to measure the performance of the inbound/outbound traffic of the established environment.

This assignment is open for 2 students.

Professor: Danilo Gligoroski (daniloq@item.ntnu.no)

47. (IS) "Hidden services in Tor"

Tor is free software and an open network that helps you defend against a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security known as traffic analysis. Tor was originally designed, implemented, and deployed as a third-generation onion routing project of the U.S. Naval Research Laboratory. It was originally developed with the U.S. Navy in mind, for the primary purpose of protecting government communications. Today, it is used every day for a wide variety of purposes by normal people, the military, journalists, law enforcement officers, activists, and many others.

Tor makes it possible for users to hide their locations while offering various kinds of services, such as web publishing or an instant messaging server. Using Tor "rendezvous points," other Tor users can connect to these hidden services, each without knowing the other's network identity. This hidden service functionality could allow Tor users to set up a website where people publish material without worrying about censorship. Nobody would be able to determine who was offering the site, and nobody who offered the site would know who was posting to it.

The goal of the thesis is to learn how the hidden service protocol works, to successfully configure hidden services and to measure the performance of the inbound/outbound traffic of the established environment.

This assignment is open for 2 students.

Professor: Danilo Gligoroski (daniloq@item.ntnu.no)

48. (NT) Capacity in vehicular networks

Intelligent Transport Systems (ITS) is the utilization of ICT in the transport sector for e.g. improved safety, efficiency and convenience. Many information services and applications increase the demand for higher network capacity – especially in urban areas with a high vehicle density. Vehicles may connect through both short-range (e.g. WiFi, DSCR) and long-range (e.g. 2G, 3G, 4G) communication technologies, making it hard to estimate the network capacity as seen from the individual vehicles.

The assignment is to look at the different aspects that affect the network capacity, and try to model the network capacity available for a vehicle. Realistic models of the physical channel and mobility models must be used (cooperation is possible with both SINTEF and the Norwegian Road Administration – Statens Vegvesen). The models should be verified through simulations.

Supervisor: TBD

*Professor: Adjunct Associate Professor Tor K. Moseng, NTNU ITEM
(tor.kjetil.moseng at item.ntnu.no)*

49. (NT) Information forwarding in WiFi-based vehicular networks

Intelligent Transport Systems (ITS) is the utilization of ICT in the transport sector for e.g. improved safety, efficiency and convenience. One important enabler for ITS is the communication between vehicles and the infrastructure. The short-range communication to and from vehicles is based on WiFi technologies (i.e. IEEE 802.11p). In urban areas with many vehicles, the network becomes quickly congested – typically for emergency scenarios where safety information is broadcasted. It is therefore important to provide efficient forwarding algorithms between vehicles (i.e. like multi-hop ad-hoc networks).

The assignment is to look at different forwarding algorithms, suggest an improved forwarding algorithm, and find performance metrics (compared to existing algorithms) in highly mobile vehicular environments through simulations.

Supervisor: TBD

*Professor: Adjunct Associate Professor Tor K. Moseng, NTNU ITEM
(tor.kjetil.moseng at item.ntnu.no)*

50. (NT) Performance in WiFi-based vehicular networks

Intelligent Transport Systems (ITS) is the utilization of ICT in the transport sector for e.g. improved safety, efficiency and convenience. One important enabler for ITS is the communication between vehicles and the infrastructure. The short-range communication to and from vehicles is based on WiFi technologies (i.e. IEEE 802.11p). This MAC (Media Access Control) protocol lacks predictability in delay and loss, which is especially important for time critical safety application in ITS (and other areas as well).

The assignment is to look at how different MAC solutions handles performance metrics like delay and packet losses in a highly mobile environment, and whether these are predictable. The solutions are to be tested through simulations for different traffic models and users, and lead to recommendations for an improved MAC.

Supervisor: TBD

*Professor: Adjunct Associate Professor Tor K. Moseng, NTNU ITEM
(tor.kjetil.moseng at item.ntnu.no)*

51. (NT) Modelling mobility and wireless communication for simulations in SIMULA/DEMOS

Simula is a pure object-oriented simulation language developed in Norway, and is together with DEMOS (building blocks for use in discrete event simulators) used at the department of Telematics to simulate packet network behavior. However, there is currently a lack of support for wireless communication (e.g. WiFi infrastructure and ad-hoc networks), which becomes an important necessity in today's society.

The task is to implement support for both mobility and wireless communication in SIMULA/DEMOS. A use case can be transport telematics, where vehicles communicate with each other and with the roadside (e.g. as the travel time system deployed in Trondheim, or safety warnings about collisions, congestions, etc.). If time allows, also the MAC protocol (e.g. IEEE 802.11) could be included in the simulator.

*Professor: Adjunct Associate Professor Tor K. Moseng, NTNU ITEM
(tor.kjetil.moseng at item.ntnu.no)*

52. (IS/NT) Senatus: Attacking and defending the Internet

Intrusion detection is an important technique in computer network security. **Senatus** is a concept we recently propose in order to detect intrusions in a fashion of traffic classification and identification.

There are two main tasks:

1. Understand network attacks and their simulation tools then generate the attacks. Then simulate attacks in real backbone network, collect the data of the form Netflow/Qflow and prepare it to the analysis.
2. **Senatus** performance analysis investigation.

This project involves a direct collaboration with UNINETT.

Note: Multiple students are accepted.

*Supervisor: Atef Abdelkefi (atef at q2s.ntnu.no), Arne Øslebø (arne.oslebo at uninett.no)
Professor Yuming Jiang (jiang at item.ntnu.no)*

53. (IS/NT) Implementation of Senatus : Hacker's fear

Intrusion detection is an important technique in computer network security. **Senatus** is a concept we recently propose in order to detect intrusions in a fashion of traffic classification.

The main task of this project is to extend the implementation of **Senatus** in C++, PhP, python and validate it in real environment and network under real attacks.

A very good programming skills in the three mentioned language is required

This project involves a direct collaboration with UNINETT.

Note: Multiple students are accepted

*Supervisor: Atef Abdelkefi (atef at q2s.ntnu.no), Arne Øslebø (arne.oslebo at uninett.no)
Professor Yuming Jiang (jiang at)item.ntnu.no)*

54. () Analysis of password management architecture

UNINETT is the national research IP network operator in Norway. UNINETT provides universities, university colleges and research institutions with access to the global internet as well as access to a range of online services. UNINETT also offers counselling and act as secretary and coordinator in collaborative activities between the institutions interconnected by UNINETT.

At UNINETT a team of operational managers manage a large collection of servers, routers and switches. Each unit typically has a root account and an associated password. Securely managing the total collection of passwords is a challenge while still ensuring access to them for all relevant personell and in all relevant situations.

The projects main objective will be to evaluate a password management architecture proposed by UNINETT. Comparing it to other potential architectures as well as, if possible, quantifying the level of security the architecture may offer are tasks to be looked into.

Supervisor: Tor Gjerde, UNINETT (tor.gjerde at uninett.no)

Faglærer:

55. (TS) Model-Driven Development for Domain-Specific Data

Most systems need to express concepts of their specific domain (for instance health or logistics) in some form of data model. Depending on the implementation of the system, this data model is actually represented in code and other source files more than once. For instance, the system may contain components that are implemented in different programming languages. In addition, if special frameworks for serialization, transmission or persistence are used (such as for instance Apache Thrift, Google Protocol Buffers or Morphia), the same data model has to be implemented for each of these frameworks. In practice this means that a single change in the domain model needs to be maintained in several places.

To avoid this situation, a model-driven approach can be employed instead, in which the domain model is expressed once in a suitable language, and all other artifacts may be derived from it. While this is conceptually not new, there are many degrees of freedom how to implement such an approach. For instance, which language should be used to express the domain model, and how can this data be sufficient to derive all desired artifacts from it? In which way should code be generated? Which tool support is available for such tasks? In this thesis, possibilities should be compared en evaluated, and an example toolchain should be proposed.

Faglærer / Supervisor: Frank Alexander Kraemer (kraemer at item.ntnu.no)

56. (TS) Building Block Models for Home Automation Standards

Several standards are gaining acceptance in the home automation domain, such as Zigbee or Z-Wave, amongst others. In this work it should be examined in which way such protocols can be made available as building block models, so that they can be used in application development. Interesting questions are how application that use several standards at once can be realized, and which features of the specific standards need to be visible on model-level. As an proof-of-concept, an example application should be proposed, discussed and implemented that connects some simple home automation devices.

Faglærer / Supervisor: Frank Alexander Kraemer (kraemer at item.ntnu.no)

57. (TS) A Study About Rich Descriptions for Interfaces, Contracts and APIs

Interfaces of most standard programming languages are relatively simple; they describe method signatures and types, but leave other aspects, such as the ordering of invocations, response time or threading issues to the documentation. In this thesis, approaches that enrich interfaces in various ways (for instance annotations), or model-based approaches should be studied and compared. Depending on the result of the survey, ways to express interfaces in programming languages for reactive behavior should be proposed, discussed and exemplified.

Faglærer / Supervisor: Frank Alexander Kraemer (kraemer at item.ntnu.no)

58. (IS) Security Analysis of the Terrestrial Trunked Radio (Tetra System)

Tetra is a mobile communication standard that is widely used in radio devices by government, emergency services, police, military etc. throughout Europe, Asia and Africa. The Tetra standard is in many ways similar to the GSM standard.

The student will perform a security analysis of certain aspects of the Tetra system. For instance, he/she may focus on the authentication and key exchange protocol.

Prerequisite: Knowledge of TTM4135 or TTM4137.

Supervisor: Postdoc Joe-Kai Tsay (joe.k.tsay at item.ntnu.no)

Professor: Stig F. Mjøltnes (stig.mjoltnes at item.ntnu.no)

59. (NT) Quantifying UNINETT's high availability infrastructure

UNINETT is the national research IP network operator in Norway. UNINETT provides universities, university colleges and research institutions with access to the global internet as well as access to a range of online services. UNINETT also offers counselling and act as secretary and coordinator in collaborative activities between the institutions interconnected by UNINETT.

UNINETT is in the process of designing, developing and interconnecting infrastructure components with the aim to offer a foundation for application services of high availability. Redundancy and independence of the components have been ensured however so far no formal analysis quantifying the potential availability of component combinations have been performed.

The projects main objective will be to model a set of sample services and quantify their potential availability. If possible, a more general framework for analysis of future services should be purposed. Including factors in the models which quantify the difference between a test installation of a service and an operational installation are desirable. As UNINETT offers “best effort” services in general, a metric showing such a difference would be helpful to motive moving services from test to operational status.

Supervisor: Otto J Wittner (otto.wittner at uninett.no), Roger Skjetlein, Morten Knutsen, UNINETT
Professor: Bjarne Helvik (bjarne.e.helvik at item.ntnu.no)

60. (NT) Multicast capacity estimates for lecture IPTV in UNINETT

UNINETT is the national research IP network operator in Norway. UNINETT provides universities, university colleges and research institutions with access to the global internet as well as access to a range of online services. UNINETT also offers counselling and act as secretary and coordinator in collaborative activities between the institutions interconnected by UNINETT.

UNINETT has been running a pilot IPTV service based on multicast for some years. Many universities and university colleges are already making recordings of lectures, and it is expected that most institutions will record most lectures in the future.

The project's main objective is to investigate the possibility for UNINETT to allocate IPTV-channels (multicast addresses) for live broadcasting of ongoing lectures. How many concurrent lectures can UNINETT's backbone network support without degrading the general IP transport service? Modelling both user and lecture streaming behavior while taking UNINETT's topology and traffic load matrix into account, will be important parts of the project work.

Supervisor: Otto J Wittner, UNINETT (otto.wittner at uninett.no)
Professor: Øivind Kure (okure at item.ntnu.no)

61. (IS) Analysis of password management architecture

UNINETT is the national research IP network operator in Norway. UNINETT provides universities, university colleges and research institutions with access to the global internet as well as access to a range of online services. UNINETT also offers counselling and act as secretary and coordinator in collaborative activities between the institutions interconnected by UNINETT.

At UNINETT a team of operational managers manage a large collection of servers, routers and switches. Each unit typically has a root account and an associated password. Securly managing the total collection of passwords is a challenge while still ensuring access to them for all relevant personell and in all relevant situations.

The projects main objective will be to evaluate a password management architecture proposed by UNINETT. Comparing it to other potential architectures as well as, if possible, quantifying the level of security the architecture may offer are tasks to be looked into.

Supervisor: Tor Gjerde, UNINETT (tor.gjerde at uninett.no)

Professor: Karin Bernsmed (Karin.Bernsmed at sintef.no)

62. (NT) Stochastic routing realized with SDN

UNINETT is the national research IP network operator in Norway. UNINETT provides universities, university colleges and research institutions with access to the global internet as well as access to a range of online services. UNINETT also offers counselling and act as secretary and coordinator in collaborative activities between the institutions interconnected by UNINETT.

UNINETT, together with UNIK, is experimenting with software define networking (SDN) equipment, and has a small laboratory network in operation. SDN enable detailed centralized control over how packet flows are routed.

In this project a control framework to enable stochastic routing in a SDN topology is to be designed and implemented. A variant of the CEAS system developed at ITEM NTNU, may be a candidate for applying the framework. Studying aspects of scalability and dependability of the framework is of interest.

Supervisor: Otto J Wittner, UNINETT (otto.wittner at uninett.no)

Professor: Poul Heegaard (poul.heegaard at item.ntnu.no)

63. (NT) Open network topology services

UNINETT is the national research IP network operator in Norway. UNINETT provides universities, university colleges and research institutions with access to the global internet as well as access to a range of online services. UNINETT also offers counselling and act as secretary and coordinator in collaborative activities between the institutions interconnected by UNINETT.

UNINETT is a multilevel network that is built from cables, fibers, lambdas, VLANs, IP networks and VPNs. There is need to solve the problem of documenting the global research network infrastructure that allows for common tools and for exchange of information between universities and research networks. There has been several initiatives to address part of these problems like : In Norway with NAV a network management system for campuses, in the Nordic area at NORDUnet, in Europe with Geant projects as well as American/Internet2 activities.

The task is to survey state of the art of tools and data models in this area, and recommend an open system architecture containing data models, exchange protocols and available system components . A prototype implementation that demonstrates the capabilities of the architecture should be built.

Supervisor: Olav Kvittem (Olav.Kvittem at uninett.no), Morten Brekkevoll (Nav) and Vidar Faltinsen (Europe)

Professor: Finn Arve Aagesen (finnarve at item.ntnu.no)

64. (IS) Security requirements for the Cloud

As the uptake of Cloud computing services increases, we see a growing number of SaaS, PaaS and IaaS offerings from a broad set of providers. The Cloud broker is foreseen to take an important role in the Cloud ecosystem, providing a one-stop shop for many customers. The Cloud broker will help customers find the best services that fit their particular needs, and that fulfills their requirements on performance, dependability, security and cost

SINTEF ICT is currently working on security requirements related to Cloud brokering. CloudSurfer is a prototype Cloud broker tool that automatically matches a customer's security requirements against different provider offerings. CloudSurfer is based on WS-Agreement, which is a standard for describing requirements in terms of machine-readable Service Level Agreements between service providers and service customers.

The current version of CloudSurfer has two interfaces, one that allows potential Cloud customers to search for available services and another one for administrating the tool. In this task the student will extend CloudSurfer with a new interface, which allows the providers to add service offerings to the broker. The student will then analyze existing service offers from a number of public Cloud providers (Amazon, Google, Microsoft, etc) and investigate to what degree these can be represented in CloudSurfer.

Supervisor: Per Håkon Meland, SINTEF (Per.H.Meland at sintef.no)

Professor: Karin Bernsmed (Karin.Bernsmed at sintef.no)

65. (NT) Dependability Modelling in Smart Grid. A comparison of different modelling techniques.

Modeling a large system leaves the analyst usually with three alternatives: using a structural model such as RBD; using a dynamic model such as Markov model; or abandoning the analytical approach and resorting to simulation. Structural models have a limited usage because of strong independence assumptions between the entities and the missing capability of modeling dynamics. Dynamic models quickly get complex and computationally demanding for large systems. Simulations need a careful implementation and a number of simulation runs to obtain a result with good statistical precision. However, there are a number of techniques that combine structural and dynamic models which allows to profit from their complementary advantages. But what are the strengths and weaknesses of this modelling techniques?

The aim of this Master's thesis is to compare different dependability models by analyzing one and the same system. The system will be chosen from the smart grid area (power grid improved by communication technology). The student will acquire not only a lot of experience with dependability models but also valuable knowledge in smart grid, a quickly developing research area. See also: <http://www.smartgrids.no/>

Required background: TTM4110 or equivalent

Recommended background: TTM4120 and TTM9

Supervisor: Jonas Wäfler (jonaswa at [item.ntnu.no](mailto:jonaswa@item.ntnu.no))

Professor: Poul E. Heegaard (poul.heegaard at [item.ntnu.no](mailto:poul.heegaard@item.ntnu.no))

66. [NT, TØ] Highly dependable green ICT systems; how?

High dependability and low energy consumption are (seemingly) inherently opposing properties of ICT systems. Fault tolerance is achieved by energy consuming redundancy, and the shorter the fault handling times should be, the larger is the requirement for dedicated spares and active replication, with a higher energy consumption as a result. Both high dependability (robust ICT systems) and energy consumption (green ICT) are important properties in high demand in current and future networked systems. However, little research is done on the system/network level how to deal with these two "challenges" at the same time.

In this master assignment, the student should make a initial state of art review with respect to this problem domain. Next a case study should be defined. This may be tailored to the students specialisation and may include proposal of a design suited to meet both kinds of requirements, evaluation of its properties and/or seeking optimal solutions where for instance the cost of equipment, energy, non compliance with SLAs may be cost factors. The type of system addressed may be (core) networks, P2P systems or could computing. At the department, we have done research in this problem domain with respect to the last two types of systems.

Professor: Bjarne E, Helvik (bjarne at item.ntnu.no)

67. (TS/TSA) A Pervasive Communication System for Health Care

Pervasive technology has for some time been singled out as a good fit for the hospital environment, however few actual implementations exists today. This project seeks to improve the current communication possibilities for health care workers by allowing them to use different type of interconnected devices for communication. Using a model driven development approach, the student will be working with the Arcitis SDK [1] to develop a communication system described in [2] using Android based devices. No pre-knowledge of Arcits or Android is required. The student should however be familiar with object-oriented programming.

References

[1] <http://www.bitreactive.org>

[2] Klemets and Kristiansen. *A Pervasive System for Communicating Urgency Cues to Health Care Workers*. [Link](#).

Supervisor: Joakim Klemets, Telematics (joakim at item.ntnu.no)

Professor: Lill Kristiansen, Telematics (lillk at item.ntnu.no)

68. (IS) Making a wireless infrastructure like eduroam for comercial application

Wireless Trondheim has many different groups of users and different access solutions. Not all of these maintains the same security level, and we are considering to gather all users on one secure solution with authentication and encryption.

The assignment is to consider and test doability, security and user friendliness for a WPA Enterprise based solution with a RADIUS proxy for different user groups as guest, subscribers and employees in different organizations.

The goal is that everyone should be able to use a secure SSID with WPA Enterprise, and that bandwidth and other parameters is governed by which rights you have/which organization you come from.

In this assignment a prototype should be made. Is it possible to establish a solution which combines these features:

- Secure
- User friendly
- Authenticate users against different RADIUS solutions and subscriber databases.
- Put wrongly configured users in a "walled garden", where they can be instructed in how to log on or create a new subscription.

Keywords: 802.1x, WPA/WPA2, Security, WiFi, (Free)RADIUS

Veileder: Gunnar Rangøy, Trådløse Trondheim (gunnar at tradlosetrondheim.no)

Faglærer: Yuming Jiang (jiang at item.ntnu.no)

69. (TØ) Forretningspotensial for lokasjonsbasert reklame på SMS

De tradisjonelle reklamekanalene blir mindre verdt etter hver som mer effektive og målrettede reklamekanaler vokser frem. Lokasjon er en joker mhp annonsering. Om du når en bruker i det han ankommer et kjøpesenter så vet du at vedkommende er i kjøpsmodus og at han er i geografisk nærheten av der han kan gjøre kjøpet. Trådløse Trondheim har utviklet en løsning som gjør at vi kan nå en bruker for eksempel når han ankommer et kjøpesenter. Vi ønsker nå å kartlegge markedspotensialet for en slik løsning.

Oppgaven består i å kartlegge forretningspotensialet for lokasjonsbasert reklame på SMS for ulike markedssegmenter for eksempel kjøpesenter. Sentral spørsmål er betalingsvillighet hos kunder for eksempel kjøpesenter, markedsstørrelse og forretningsmodell.

Veileder: Thomas Jelle, Trådløse Trondheim (thomas.jelle at item.ntnu.no)

Faglærer: Yuming Jiang (jiang at item.ntnu.no)

70. () Utvikling av posisjoneringsmotor basert på signaler fra WLAN ?

Lokasjon er en viktig byggestein i fremtidens teletjenester. Trådløse Trondheim har utviklet en løsning og posisjonering innendørs, se campusguiden.no. Løsningen baserer seg på signalstyrke (RSSI) som hentes fra kjernekomponenter i trådløsnettet. Tidligere har vi også utviklet en løsning som baserer seg på Fingerprinting (området som skal ha posisjonering gås opp manuelt og en må samle inn signalstyrke for alle områder). De ulike løsningene gir ulik nøyaktighet i posisjoneringen og ulike forsinkelse på posisjonsdataene. Trådløse Trondheim ønsker nå å utvikle en tredje variant for å lage en ny og bedre posisjoneringsmotor.

Oppgaven består i å kartlegge flaskehalsen med dagens løsning, utvikle en arkitektur for den nye posisjoneringsmotor og teste denne.

Veileder: Thomas Jelle, Trådløse Trondheim (thomas.jelle at item.ntnu.no)

Faglærer: Yuming Jiang (jiang at item.ntnu.no)

71. (TS) Bruk av BIM (Building Information Model) for smarttelefoner

Dagens plantegninger for bygg (for eksempel dwg) er lite egnet for tilpasning og visning på smarttelefoner. Disse er for detaljerte og dataene som er lagt inn er lite strukturerte.

Trådløse Trondheim jobber sammen med Statsbygg med neste generasjons «plantegninger» som er datamodeller BIM (Building Information Model). BIM vil være dataformatet for utveksling av bygningsinformasjon ila 5-10 år. Med BIM er det mulig å plukke ut hvilke data en ønsker å presentere den for brukeren i ulike settinger også på smarttelefon. Dette sammen med innendørs posisjonering åpner for mange anvendelser bla å kunne se rør og ledninger bak vegger (ved hjelp av augmented reality). Oppgaven består i å lage en arkitektur for hvordan en kan hente ut data fra en BIM modell og bruke disse på smarttelefoner.

Veileder: Gunnar Rangøy, Trådløse Trondheim (gunnar at tradlosetrondheim.no)

Faglærer: Yuming Jiang (jiang at item.ntnu.no)

72. (IS) Padding Oracle Attacks on Cryptographic Hardware

In recent work presented at CRYPTO 2012, Bardou, Focardi, Kawamoto, Simionato, Steel and Tsay demonstrated efficient attacks on widely used cryptographic hardware (e.g., usb tokens and smartcards) by exploiting error messages returned by the RSA encryption standard (PKCS#1 v1.5). The student will adapt the attack by Bardou et al. to tokens that were previously not considered as they use slight variations of the encryption standard. The student will test in how far the efficiency of the attacks is impacted by the deployment of these variations.

Prerequisite: Knowledge of a programming language.

Recommended previous knowledge: TTM4135, TMA4155, TMA4160 or MA1301.

Reference: "Efficient Padding Oracle Attacks on Cryptographic Hardware", Bardou, Focardi, Kawamoto, Simionato, Steel and Tsay, In proceedings of the 32nd International Cryptology Conference (CRYPTO 2012), Santa Barbara, CA, USA, Springer LNCS, Vol. 7417, 2012.

Supervisor: Postdoc Joe-Kai Tsay (joe.k.tsay at item.ntnu.no)

Professor: Stig F. Mjølsnes (stig.mjolsnes at item.ntnu.no)