UPTEC IT10 012
Examensarbete 30 hp
Mars 2010

Challenges and Considerations for a Delay-Tolerant Wireless Sensor Network Deployment

Anton Ruhnau Pollak

UPPSALA
UNIVERSITET

**Teknisk- naturvetenskaplig fakultet
UTH-enheten**

Besöksadress:
Ångströmlaboratoriet
Lägerhyddsvägen 1
Hus 4, Plan 0

Postadress:
Box 536
751 21 Uppsala

Telefon:
018 – 471 30 03

Telefax:
018 – 471 30 00

Hemsida:
http://www.teknat.uu.se/student

Abstract

Challenges and Considerations for a Delay-Tolerant Wireless Sensor Network Deployment

Anton Ruhnau Pollak

This report identifies the challenges of deploying a Delay-Tolerant Wireless Sensor Network in an environment with a subarctic climate. The network is intended to enable remote access to measuring stations and the environmental data that they record. The report proposes a high-level organization of such a network and reviews several different network and transport layer protocols, as well as services, suitable for the network. It does so by reviewing previous sensor network deployments and identifying the requirements of these networks, as well as the requirements of the applications and conditions found in this particular scenario. In this scenario, the size and spread of the network, along with the complex geographical properties of the deployment area are found to be the greatest challenges. This requires the use of many different network and hardware technologies within the same network. In order to successfully deploy a network of this extent, thorough investigations of the operation environment, the applications' requirements and the conditions for radio communication in the area must be conducted.

Handledare: Olof Rensfelt
Ämnesgranskare: Lars-Åke Larzon
Examinator: Anders Jansson
ISSN: 1401-5749, UPTEC IT10 012
Tryckt av: Reprocentralen ITC

Sammanfattning

All forskning bygger på att experiment och undersökningar utförs i syfte att samla in data som sedan analyseras och tolkas. I takt med att datorer och mätinstrument utvecklas, ökar även mängden data samt dessas noggrannhet och detaljrikedom dramatiskt. Detta gäller speciellt forskning inom naturvetenskapliga discipliner där olika fysiska fenomen undersöks med ibland mycket avancerad mätutrustning.

En viktig del av framgångsrik forskning är utbytet av data, metoder, erfarenheter och resultat med andra forskare runt om i världen. Detta är något som underlättats enormt den senaste tiden i och med internets utbredning; det har blivit enklare, bekvämare och framförallt snabbare. Denna utveckling till trots förekommer det fortfarande forskningsdiscipliner som inte utnyttjar den kapacitet som de tekniska hjälpmedel som finns tillgängliga idag har. Även om majoriteten av de mätdata som samlas in lagras digitalt, förekommer det också fortfarande att data samlas in och lagras med analoga instrument och metoder.

Ett exempel på detta är forskning inom miljö och klimat. Dessa discipliner förlitar sig i mycket stor utsträckning på experiment och observationer som utförs i naturen. Sensorer och mätutrustning som övervakar variabler inom bland annat meteorologi, hydrologi, flora och fauna placeras ut på strategiskt valda platser i naturen för att samla in data. Traditionellt sparar sensorerna de uppmätta värdena till en extern enhet, till exempel en hårddisk, men det förekommer även att de skrivs analogt på en pappersremsa med hjälp av en mekanisk anordning. När experimentet är slutfört besöker forskarna sedan de olika mätstationerna för att samla in hårddiskarna och eventuella pappersrullar. Den här metoden, att besöka varje mätstation efter ett slutfört experiment, är oerhört tidskrävande och opraktisk, framförallt i de fall då mätningar utförs i områden med svåråtkomlig eller farlig terräng.

Följande rapport är en förstudie till ett projekt vars mål är att förenkla den här processen för forskare. Med hjälp av modern, trådlös nätverksteknik ska mätstationer över ett stort område i och omkring Abisko kopplas samman i ett nätverk. Detta nätverk ska var åtkomligt via internet för de forskare som utför experimenten, något som ger dem möjlighet att hämta de mätdata som stationerna registrerar utan att besöka dem och i viss utsträckning helt utan fördröjning. Dessutom ska det vara möjligt att programmera om mätstationerna mellan experiment för att ytterligare undvika tidskrävande besök vid dessa. Utöver detta ska även data från experiment kunna lagras på ett sådant sätt att utomstående forskare kan ges tillgång till dessa, även detta via internet.

Förutsättningar för att bygga ett sådant nätverk i och omkring Abisko är mycket dåliga på grund av flera faktorer. En av dem är klimatet i Abisko, som är av subarktisk karaktär med en medeltemperatur under 0 °C. En annan faktor utgörs av terrängen som är ett svårt hinder på grund av de stora variationerna samt det bergsområde som utgör en del av forskningsområdet. Ytterligare en faktor utgörs av avsaknaden av infrastruktur i området. Strömförsörjning, teknisk utrustning som till exempel antenner för mobiltelefoni samt i viss mån transportvägar förekommer endast i mycket begränsad utsträckning och då främst i områden längs riksvägen som passerar Abisko.

För att kunna bygga ett nätverk under sådana förutsättningar kan man med fördel

använda sig av ett antal speciella tekniker för nätverk, tekniker som har utvecklats enormt det senaste decenniet. Genom att utrusta mätstationerna med små radioenheter för kommunikation kan mätstationerna kopplas samman i flera mindre trådlösa nätverk, beroende på enheternas geografiska position. För att dessa nätverk ska kunna kommunicera med varandra samt även anslutas till internet, kommer ytterligare två nätverkstyper att användas, nämligen fördröjningstoleranta samt opportunistiska nätverk. Ett trådlöst sensornätverk i den här storleken som ska fungera i en svår miljö utgör givetvis en stor utmaning inom många olika områden. Den här rapporten fokuserar på kommunikationen i nätverket och diskuterar kommunikationsprotokoll, nätverkstopologier och tjänster som lämpar sig speciellt för den här sortens nätverk. Rapporten granskar även ett flertal tidigare sensornätverksprojekt i syfte att identifiera vilka krav som ställs och vilka förutsättningarna som existerar för att bygga ett sensornätverk av det slag som planeras i Abisko. I rapporten föreslås även en nätverksstruktur för scenariot i Abisko samt vad som måste undersökas närmare innan utvecklingen påbörjas.

Contents

Chapter 1

Introduction

All researchers within technical disciplines conduct experiments in order to collect data for analysis. The experiments are either simulated or conducted in real-life. The technical advances in computer science have accelerated this process leading to an increase in the amounts of collected data, as well as in its accuracy and resolution, due to more advanced technical measuring equipment. The vast majority of the data is collected automatically and stored digitally, although there still exist analogue equipment that, for instance, records measurements on paper tapes.

Despite the rapid development there is still room for much improvement. A very important aspect of research is the possibility to access material from other researchers, as well as the ability to share data, methods and results from conducted experiments. This is a task that the Internet has made tremendously much easier since its birth. Unfortunately, researchers in some disciplines do not yet take full advantage of modern techniques for data collection and sharing.

One of these disciplines include environmental research. Experiments and data collection conducted within this branch of research is typically performed in wild-life scenarios. This includes setting up measurement equipment, or sensors, such as thermometers, wind gauges, cameras and hydrological instruments. Traditionally, these sensors write data collected to a special purpose logger. After an experiment has finished, the researchers then visit each measuring station and collect the loggers. This is a very inconvenient and time consuming task. It is especially true if the experiments are conducted in remote and inaccessible locations, such as on a mountain or on an uninhabited island.

The Abisko project targets this specific problem. Using state of the art network equipment, it is planned to enable the researchers to access the data collected at the many measuring stations from a remote location. The access is enabled by connecting all stations in a large network which, with some restrictions, is connected to the Internet. Additionally, the network is also intended to enable remote configuration and experiment setup, as well as enabling in-network services such as data aggregation and support future additions as the need arises. The challenges presented by this scenario are complex for many reasons; the area that the measuring stations are spread over is large and the geographical conditions such as vegetation, topology and the weather are varying but generally harsh. Additionally, for most part of the area no power and/or communication infrastructure exists.

In order to meet these challenges, several different recently developed computer networking techniques can be utilized. The measuring stations are equipped with radio transceivers. They will then form several smaller networks (Wireless Sensor Networks, WSN) depending on their location, in order to establish connections between the stations. Further, techniques such as Delay-Tolerant Networks (DTNs) and Opportunistic Networks will be used to connect these WSNs to one another and to the Internet. Such a large sensor network deployment poses a large number of challenges. This pilot study focuses on the computer networking part of these, including considerations on network topologies, services and choice of communication protocols. By reviewing several other WSN deployments, the rudimentary requirements for the Abisko scenario are elicitated. Also, the conditions that apply specifically for Abisko, including the climate and the applications, are discussed and their implications on a network are considered. This report takes a high level network design approach, and proposes a structure for the Abisko scenario. Along with this, recommended future work is outlined and presented in areas divided into suitable subprojects.

Chapter 2

Background

The Abisko Scientific Research Station is a research site situated in and around several nature reserves and a National park in the very north of Sweden, about 200 km north of the Arctic circle. The research station was established in 1903, and acquired by The Royal Swedish Academy of Science in 1935. It comprises several scientific facilities, varying from chemistry labs to greenhouses and computer rooms.

Abisko is a very active research site, visited by approximately 500 researchers every year. This is due to the unique variety of geographical environments and subarctic climate it features. However, because of the climate almost no researchers are present winter-time. During the summer, they conduct studies within biology, geology, ecology and meteorology. A lot of the research is dependent of accurate data collected by measuring stations that are spread over a 60 km^2 large area. The data currently available[1] from the stations include weather data such as air temperature and air pressure, Lake Torneträsk ice thickness, photo active radiation and UV radiation [1]. Other, more complex or compound data may include information of avalanche build-ups, gas release from the ground and the spread of vegetation and animals.

2.1 Experiments

Currently, the experiments conducted include three main phases; experiment setup, sampling sensors and finally data collection. Depending on the experiment, the length of the three phases vary. For some applications, advanced automated measuring equipment is used, resulting in a longer initial setup phase. However, this tends to lead to shorter duration of experiments and faster data collection. Other applications have opposite requirements. Some ecological studies are performed manually, meaning the researchers make observations themselves during certain time periods. Of course, these experiments have a shorter preparation phase because no equipment that needs configuration or calibration is involved. However, the duration of the experiments may become longer because of a lower 'sample rate'. Additionally, these experiments may need post-processing

[1] Although the data is publicly available, a formal request must be filed in order to get access to the records.

such as digitalizing data. A third category of experiments use legacy measuring equipment. This results in fairly short setup and sampling periods, however because legacy equipment is not digitalized, necessary post-processing of the data into a digital format is necessary and time-consuming.

Because the research in Abisko is very active, a lot of measuring stations are deployed in the Abisko environment. Most of the measuring stations are in the near vicinity of the research station, allowing quick and easy access either by car or by hiking. Further, these stations have access to infrastructure such as power supplies and network access which allows them to run for long time periods without maintenance. However, in contrast to these stations, there are measuring stations deployed in many additional locations which are not easy to access. The locations vary from being situated along hiking trails in the National park, to the most remote mountain valleys where hardly any trails exist. In some cases, these locations are not accessible at all; during winter time they may be exposed to avalanches, and in the spring and fall mudslides make them equally dangerous. Also, with few exceptions these locations are isolated and have no access to infrastructure; there is no power, no roads and no radio communication, not even cellular networks.

2.2 Sharing research

The station in Abisko is one of many in a network organization of similar research facilities around the world, called SCANNET [2]. All of the stations are located in the subarctic, ranging from Alaska and Greenland to the Svalbard Islands and Siberia. One of the many reasons this project was initiated is to enable researchers to access up-to-date data from any of these stations, regardless of their location. This would enable comparison and processing of data much faster than previously possible, drastically reducing the time needed for experiments. Also, immediate access to sensor data is of interest in case of certain events, such as an extreme weather situation where the researchers want to track the development of a current storm, or any similar event.

2.3 Computer networks research

This sensor network deployment project also serves as a unique opportunity for computer networks research. Research on WSNs and DTNs has been done since the beginning of the century, resulting in extensive simulations during the development of communication protocols and energy saving measures. However, simulations cannot replace real-life experiments. Although several previous sensor networks have been deployed (see chapter 5), scenarios as wide and multi-disciplinary as the one offered in Abisko are unusual. Also, the sensor network deployment in Abisko is not initiated by computer networking researchers, meaning that the resulting system is primarily intended to serve its purpose as a tool in environmental research, rather than in computer science.

Chapter 3

Thesis purpose

This thesis is a technical pilot study conducted as a part of the preparations for an Opportunistic and Delay-Tolerant Wireless Sensor Network deployment in Abisko, Sweden. The WSN aims at helping the researchers in their work by enabling remote access to the measuring stations. Remote access can potentially save time and create possibilities for services that allow on-demand access to data, remote configuration and minimize the preparation time for an experiment.

The purpose of this thesis is to identify and describe some of the key aspects and challenges that must be considered in order to design and implement such a network. With an understanding of these challenges, several communication protocols for Wireless Sensor Networks and Delay-Tolerant networks are reviewed, identifying services offered and their implications. The theoretical part prepares for a discussion on rudimentary network topologies that are suitable specifically for the Abisko scenario. In order to understand what parameters affect the choice of network architecture, external factors such as user and application requirements as well as implications regarding the operating environment are covered briefly.

3.1 Approach

This thesis takes on a problem-centric approach. It identifies the challenges of the given scenario by reviewing previous research projects within Wireless Sensor Networks where real-life deployments have been conducted. The challenges are used as a starting point for looking into technical aspects and problems introduced by WSNs and DTNs. The network and transport layer protocols are reviewed from a traditional network viewpoint, considering issues such as reliability, congestion and routing choices. However, because of the imminent aspect of energy conservation which is extremely important for WSNs, energy conserving protocols have been favored for the review. As a result, the protocols are all targeting WSNs and DTNs instead of traditional resource hungry networks.

After the technical review, an evaluation of possible network topologies is given with a bottom-up approach. At the bottom, we find the network nodes and their problems which are highlighted and discussed. At the next level, services and implications of organizing these network nodes into Wireless Sensor Networks are discussed. Finally, the evaluation considers the complete network that these individual networks form and what problems must be considered when interfacing with it.

3.2 Delimitations

This pilot study serves as an initial probing of the problems involved in a deployment as comprehensive as this. Therefor, it is not possible nor wanted to dive into deep technical aspects of hardware and software design. The protocols reviewed and the hardware discussed is solely intended as pointers to what services and capabilities that exist and are suitable for the Abisko scenario.

Specifically, design choices such as hardware interface design, as well as user interface design are not covered by this report. Further, it is important to stress that this pilot study does not intend to, and therefore does not, provide solutions for all of the challenges found. Once again, it is intended to give a basic understanding of the problems and point out what problems must be solved in order to design a successful network. The network topologies and architectural designs and services presented in this report are in no way tested, simulated or verified by the author.

This report also does not provide detailed discussions of formal requirements. This is left out, intended as a very important part of future work. There are many stakeholders in a system as large as this, as well as an almost infinitely large range of possible applications and services. At the time of writing, the information available about current and future research in Abisko is limited.

Finally, it should be noted that certain external factors, such as social and economical factors, have not been considered. There are many bureaucratic obstacles, such as regulations if and what equipment may be installed in nature reserves. Further, it is not hard to imagine that the cost of a network of this size is considerable. Where needed, reasonable assumptions about these and other excluded factors are made.

3.3 Terminology

Throughout this report, several different terms are used interchangeably for describing an entity in the Abisko network. These are; a (network) host, a (network) node and a measuring station. Further, the term ”station” may either refer to a measuring station or to the Abisko Scientific Research Station, i.e. the main buildings. However, it should be clear which is referred to depending on the context.

Chapter 4

Problem description

The Abisko scenario is challenging in many ways. One of its most significant features is the size of the network needed. The geographical size of the sites in and around Abisko cover an area of approximately 60 km^2. Within this area there are several larger sites, each containing many smaller measuring stations or simple data loggers. The stations are maintained by different organizations such as the Royal Swedish Academy of Sciences and Sweden's Meteorological and Hydrological Institute (SMHI). The area is very versatile and dynamic regarding vegetation, weather and climate. The main buildings of the research station are located near Lake Torneträsk, while some research sites are located in the surrounding mountains.

Another significant feature is the technological conditions in the area. In and around Abisko a well developed infrastructure with power and mobile phone coverage exists, as well as roads leading to the different research sites. However, outside of Abisko this is not the case. Some of the most remote sites do not have any of the three, presenting a difficult environment for a computer network infrastructure. The equipment currently installed in the stations represents another challenge; it is not uniform in any way, some of which are legacy hardware making modern interfaces unusable. Also, the variety of applications have very different requirements in terms of sample rates, data quantities and data accuracy.

4.1 Applications

As mentioned previously, the research in Abisko is multidisciplinary and very wide. This is reflected by the needs of the applications for the sensor network. The experiments have very different needs in terms of data accuracy, aging, resolution and correlation. However, these requirements are also subject to change between experiments monitoring the same variables, depending on the duration or at what time the measurements are made.

The applications typically monitored in WSNs can be divided into two categories based on how their data is reported; *continuous* or *event-driven*. In order to explain these two types, a representative application from each category is highlighted. The avalanche application is at the time of writing not a real-life example of research in Abisko. However, it is a very realistic example of an application that relies on event-driven reporting. Of course, these two examples only give a glimpse of what research is and may be conducted in Abisko. Table 4.1 summarizes a set of well-known variables that are monitored in Abisko.

4.1.1 Meteorology

The meteorological research discipline is well-known for its extremely complex simulations when analyzing and forecasting weather. The simulations are often run on high-performance computer clusters, running for significant time periods. These simulations are based on collected data from an extensive amount of measuring stations around the world. Forecasts are made on a daily basis, taking into account current conditions at many different locations simultaneously. Because of the fast-changing nature of weather systems, quick access to data is a key requirement. However, the data must also be up-to-date to serve its purpose. Measurements that are one day old are already outdated and do not contribute to a forecast. This is similar to a real-time requirement. Additionally, the data must have a sufficient resolution and accuracy. However, even in cases where the data cannot be reported at a satisfying rate or if a delay occurs which makes the data unusable in real-time calculations, the data is still interesting for statistical and historical reasons. Therefor, it is important with reliable readings without gaps in the data series. Table 4.2 lists common meteorological variables and their properties.

Important to note is that the reporting of the data is continuous. The sensors are sampled with regular intervals, providing a stable and predictable stream of data.

4.1.2 Avalanche hazard detection

Avalanches are a threat both to humans as well as animals. Today, several different techniques are used together in order to discover hazardous areas, as well as preventing avalanches from developing. For prevention it is very common to use snow barriers at strategic positions on the mountains. Such barriers can be seen in the areas surrounding Abisko. Also, if snow patches have already started to build up into dangerously large sizes, explosives may be used either by helicopter deployment or using special built structures on the mountain in order to blow up the snow patch. This way, the avalanche is set of under controlled circumstances, as well as before it grows to big.

While prevention is very important, detection may be even more so. If areas of interest are monitored, actions to prevent avalanches can be taken early enough to minimize or even completely eliminate the risk of an uncontrolled avalanche. Detection is done by visually scanning the area for potential snow patches and slopes well known to develop avalanches. This monitoring could be a possible scenario for a wireless sensor

Research area	Variable	Sampled
Climate	Temperature	Automatic
	Precipitation	Automatic
	Precipitation chemistry	By hand
	Atmospheric pressure	Automatic
	Relative humidity	Automatic
	Wind speed and direction	Automatic
	Hours of sunshine	Automatic
	Cloud coverage	By hand
	Global and longwave radiation	Automatic
	UV-A, UV-B	Automatic
	Photosynthetic active radiation	Automatic
	Soil temperature in peat and till	Automatic
	Active layer of permafrost	By hand
	Ice freeze and break up, Torneträsk	By hand
	Ice thickness	By hand
	Snow cover	By hand
	Snow depth	By hand
	Snow profile	By hand
	Northern lights	Automatic
	Polar stratospheric clouds	Automatic
	$^{14}C/CO_2$	By hand
Hydrology	Ground water chemistry of wells in the area of Abisko	By hand
	Ground water level of wells in the area of Abisko	By hand
	Water chemistry of Abiskojokk	By hand
	Water level of Kärkejokk	By hand
	Water level of Lake Torneträsk	Automatic
Flora	Phenology of birch	By hand
	Phenology of selected species at a mire, Anisko-jokk delta, birch forest	By hand
	Pollen	By hand
Physical environment	Geomagnetism	Automatic

Table 4.1: Monitored variables at the Abisko Scientific Research Station [1].

Variable	Unit	Range	Sample rate
Temperature	°C	-50 - 50	Every 10 minutes
Precipitation	mm	0-50	Every 10 minutes
Wind speed	m/s	0-50	Every two seconds, mean calculated every 10 minutes
Wind direction	°	0-360	Every two seconds, mean calculated every 10 minutes
Humidity	%	0-100	Every five seconds, mean calculated every 10 minutes
Atmospheric pressure	Bar	0-1000	Every five seconds, mean calculated every 10 minutes

Table 4.2: A list of well-known climate variables and their properties [1].

network. Using small, locally deployed sensors, factors such as temperature, wind and humidity could be used to raise an alert if the weather changes rapidly and the risk of avalanches is increasing. To provide enough detail and accurate data to detect trends, such a system would typically have to sample sensor readings in the interval of minutes. However, in event of quickly changing weather, this rate might be increased significantly for higher resolution. If an avalanche is set off, sensors measuring vibrations and sound may be used to determine the size and possibly the location of the avalanche. These situations call for an event-driven reporting with high data rates to collect sufficiently detailed information about an event.

4.2 Geographical environment

The geographical environment at the research site is challenging. Situated in the far north of Sweden, the climate is varying but cold, with an average temperature of $-1\,°C$. However, during winter temperatures may drop well below $-15\,°C$ [3]. The temperatures are not always stable, they may shift very rapidly from above zero, to several degrees minus in only a few hours as an effect of a change in wind direction. The conditions are also very dry in Abisko, in fact it is one of the locations with the least precipitation in Scandinavia, around 400 mm per year [3]. However, the levels of precipitation varies in the region due to the mountains.

The Abisko station is situated in a nature reserve, close to a National park. The measuring stations are located either inside of the National park or the nature reserves as well as outside of them. The distance between the stations range between tens of meters, up to tens of kilometers beeline. The altitudes in the area range from 341 meters (the surface of Lake Torneträsk), up to the highest mountain in the area reaching 1991 meters. Transportation in the area is difficult; there are hardly any roads outside of Abisko, and no roads at all to some of the measuring stations. Fortunately, the area is very popular for hikers, and a lot of routes exist. The locations for a selection of the stations are marked on the map for reference, figure 4.1.

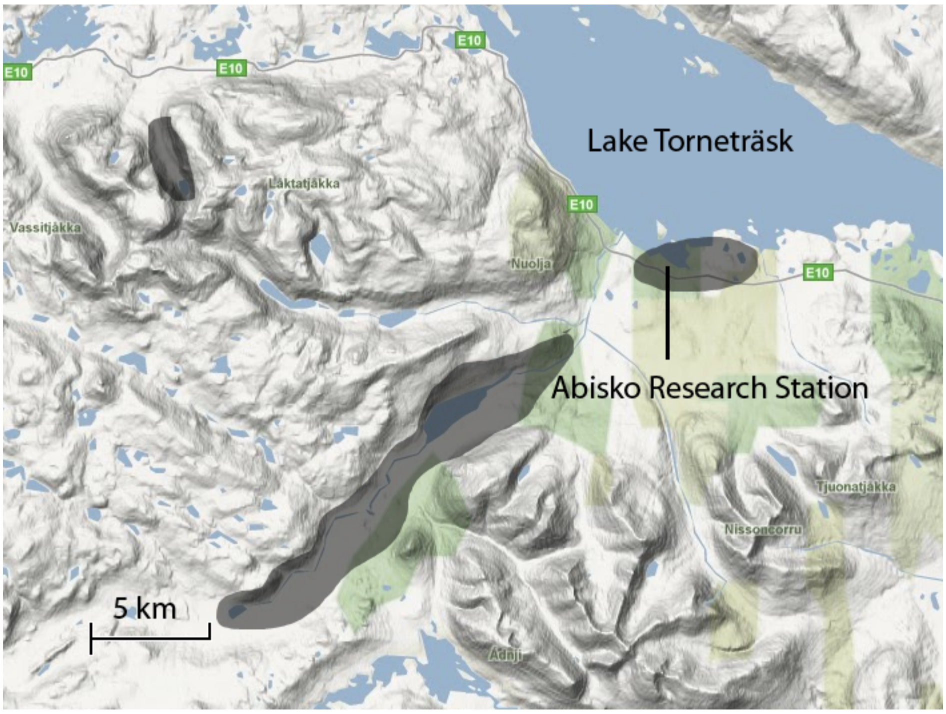

Figure 4.1: The three dark gray areas mark presence of measuring sites (not all areas are marked in the map) [4].

4.3 Additional factors

Apart from the applications' implicit requirements, there are a number of additional requirements that apply in the Abisko scenario. First, no guarantees can be made about existing infrastructure such as electric power lines or mobile phone coverage. In some locations, this means that the equipment installed must either be self-supporting or very efficient in terms of energy consumption, as well as independent of a persistent network connection. Secondly, the location of a station is a factor as well. If it allows for easy access, for example close to a hiking trail or a road, maintenance visits can be made frequently. However, the most remote stations in the mountains might not be accessible at all several months during winter because of snow coverage and the risk of avalanches. Third, it is easy to neglect the number of stations. However, it is an extremely time consuming task to visit each station for maintenance or data collection.

4.3.1 Energy conservation

A station's ability of self-support is in direct relation to the lifetime of the station. Using only batteries, a reasonable requirement is a minimum lifetime of at least a month, a time frame likely to cover most short-term experiments. Preferably though, a station would be able to run for six months. This would allow it to remain active during a winter without the need for a maintenance visit. However, six months is a requirement that is very hard to satisfy. In most situations, especially for stations that use considerable amounts of energy (e.g. for long distance radio transmissions), a wind-power generator would be a very good alternative to achieve this. Even relatively small winder power stations can generate more energy than needed in order to power a station.

Another approach in energy saving is prioritizing a station's tasks. A station may contain several different power consuming units, such as sensors, a GPS (perhaps not only used for location, but for time synchronization as well), one or several radios and possibly a backup data logger. If a station is running low on power, it may choose to turn of the GPS as a first counter-measure. When running critically low, further power saving measures, such as turning of all radios and use the backup-logger instead can be taken. As a last resort, the station may choose to turn off a sensor in favor for another, more important one.

4.3.2 Network connectivity

Network connectivity concerns the availability of a station. This in turn affects its services such as reporting up-to-date sensor data and remote management possibilities. Of course, a persistent connection is always better, however this may not always be possible. In fact, for the Abisko scenario it is unlikely that this will be the case. Without a reliable network connection, issues such as caching, intermediate storage and data aging must be considered. Also, once a station reconnects to the network, it must be able to prioritize between the services that depend on the connection.

If a station is still active within the network, this would imply that remote management is possible allowing researchers to configure the station on-demand. For example, this could be interesting in the case of extreme weather. Without a network connection, such behavior must be predefined or determined autonomously by the station itself.

The issue of availability introduces two of the Abisko network's key components; delay-tolerant networking (DTN) principles and the use of mobile data carriers. Since persistent network connections often are unavailable, the system must be able to cope with extremely long network delays. A common approach used to enable network access in DTNs is the use of data carriers. Data carriers move between locations, connecting and communicating with nodes they encounter. This way, the data carriers can collect and/or distribute data from and to nodes which are not normally connected to the network. DTNs are discussed further in section 6.3.

Chapter 5

Related work

Research on wireless sensor networks has accelerated during the last decade due to the development of smaller, ultra-low power embedded systems. The research on WSNs aims at connecting these into larger networks in an efficient manner. Such networks are becoming an increasingly important tool in a variety of industry applications, mostly for monitoring but also for control systems. However, they also serve a purpose in environmental research with their extended life-time, a small and unobtrusive footprint and relatively straightforward deployment, compared to traditional computers. These are factors that are desirable for monitoring the environment where long-term observations are common, often in locations with a sensitive nature and wild-life situation.

5.1 Sensor network deployments

WSNs have been used in several environmental monitoring projects, mostly dedicated for research purposes. While the long-term goal is to enable more convenient, accurate and faster methods for monitoring the environment, current deployments still focus on technical aspects of the WSNs. This includes communication protocols, network management and hardware design. The actual yield of the sensor networks is still of secondary importance.

- In 2001, a set of sensors was deployed in Yosemite National Park to observe how different sub-basins contribute to the flow of the Merced and Tuolumne rivers [5].
- In [6], the habitat and nesting environment of a seabird is monitored during several months, using small sensors deployed around and inside of a seabirds nest.
- The microclimate of Redwood trees has been studied in [7]. Sensors were deployed evenly on the tree, measuring temperature, humidity and Photosynthetically Active Radiation (PAR).
- Another long-term WSN was deployed inside a greenhouse, monitoring the environment of tobacco plants [8]. The WSN was Internet enabled during the six

month long deployment period, allowing remote querying and surveillance through a publicly available homepage.

- In 2005, a large network was deployed on an active volcano in Ecuador [9]. The multi-hop network consisted of 16 nodes, collecting high-resolution data of volcanic events over three weeks.
- LUSTER [10] is a WSN which measures light under a shrub thicket. The objectives of the sensor network is to offer reliable storage and a delay-tolerant architecture.
- Glacsweb [11] is a WSN project with the application of studying the dynamics of glaciers. The sensor network aims at power management and radio communications with sensor nodes deployed in and under a glacier.

The hydrological study in the Yosemite project featured a sensor network located at hard-to-reach, high altitude locations inside a national park. The researchers found challenges in interfacing with the multitude of different existing and newly deployed sensor equipment. Also, in Yosemite there exists a balance between the need for more environmental monitoring, and the preserving of the wilderness. This posed a problem when deploying equipment in sensitive areas of the national park. This is a situation that is likely to occur in Abisko as well.

The habitat monitoring at the Great Duck Island, Maine (USA), consisted of a multi-tier network. The sensors were a single hop away from a transit network which connected to a solar powered base station. The base station was connected to the Internet, allowing remote access to the sensor data. The researchers were aware of the difficult operating conditions for the sensors. Thus, they were carefully protected against weather with custom acrylic enclosures. Unfortunately, this was not enough in order to prevent node failure [12]. This is a very important lesson about what measures must be taken in order to protect the equipment.

In the Redwoods, sensors were carefully deployed in strategic positions along the trunk of a single Redwood tree. 27 sensors were placed along the 67 meters tall tree, forming a star topology network. The researchers learned several important lessons. First, the results proved very sensitive to node placement. A slight pitch affected the results for PAR radiation significantly. Secondly, it is not trivial to extract meaningful data from the sensor readings, especially since the data in this project was three-dimensional. Thirdly and most important, they discovered an urgent need for a network monitoring tool. Network failures forced internal logging of the sensor data, but the sensors ran out of storage space which resulted in a loss of data, something that was not discovered until the sensors were recollected after the experiment.

The greenhouse project aimed at energy-efficiency and Internet access. The system, called INSIGHT, was a single-hop network requiring no preconfiguration of the nodes. The lifetime of the nodes was about six months, with a claimed lifetime of one year if Lithium batteries would have been used. The researchers concluded that a single-hop network is much more energy conserving than a multi-hop, since the nodes do not have to wake up to relay an adjacent node's data to the base station. They also believe that in larger networks, multiple base stations should be used instead of switching to a multi-hop network structure. Further, the Internet access was found an important feature of the WSN, since it enabled remote reconfiguration, and even more important, remote on-demand querying for the system's end users.

The 16 node, multi-hop network deployed on an active volcano in Ecuador spanned over a three kilometer long area. The nodes connected to a base station using three 800 MHz long-range radio modems. The communication was assisted by the sparse vegetation in the area, allowing an almost free line of sight between the radio transceivers. The sensors were sampled at a 100 Hz rate and a sophisticated event detection algorithm was used to identify seismic activity. If a sensor detected an event, a message was sent into the network in order to confirm the event by querying other nodes for detected activity. Upon confirmation, a laptop at the base station initiated a data collection cycle. The researchers found a great challenge in the limited bandwidth of the network, since the sampling rate produced more data than the network could swallow. Fortunately, seismic events are fairly short which made logging at the sensor nodes possible, despite their limited storage capacity.

LUSTER is a complex system that enables reliable storage and communication over an unreliable network. It also features remote access through a web interface and tools for deployment validation of the sensor nodes. The system is multi-tiered featuring three distinct layers; the sensor nodes, the DTN layer and finally the back-end system with the database and web server. In addition, a fourth transparent storage layer is used. The nodes in this layer overhear the sensor nodes and store the data they send to the base station. The sensor and storage nodes communicate over IEEE 802.15.4[1], while the base station acts as an interface between the node layers and the back-end, which communicates over 802.11. The storage nodes do not only enable redundant storage, they also enable the DTN allowing retrieval of data at a later time, if the base station was unavailable at the time of collection.

Finally, in the Glacsweb project the sensor nodes and the base station were located in a challenging environment. The researchers found that the behavior of the system was far from the expected once the system was deployed, mainly due to unpredicted communication problems. The system has developed over time and the radio frequency was found a key factor for a reliable data link. As the project developed, they settled for a Very High Frequency (VHF) radio, working at 173 MHz [14]. Lots of efforts were put into base station design and the power management of these. The base station consisted of a master-slave design, were the slave was a low-powered controller which was used to send wake up calls to the master. The station was powered by a wind power station and solar cells. Also, because the glacier is constantly moving, the base station structure could not be bolted into the ground. Instead, the structure was designed with sharp braces that cut into the ice, providing a stable station even during strong winds.

[1]The current standard is IEEE 802.15.4-2006 [13], however it is unclear which revision was used in the LUSTER project.

Chapter 6

Communication

The communication in the Abisko scenario concerns the organization of the network and the services it offers. When planning for a network as large as this, it is inevitable that it will be compromised of several different network types, each selected to suit the needs of different situations. In order to decide on what to use between many different architectures, protocols and services, it is essential to have an understanding of these and their implications on the overall network.

This chapter reviews two branches within computer networking that are considered for the Abisko scenario. Wireless Sensor Networks (WSN) have recently gotten very much attention within the network research community. A WSN consists of very small nodes with on-board sensors, such as a thermometer or an accelerometer. The nodes organize themselves into a network and communicate with each other, exchanging information or relaying other nodes' data. The sensor nodes are very energy efficient with optimal lifetimes measured in months on a single pair of AA batteries. Their sensors are sufficiently accurate for research purposes. Recent advances in protocol design has lead to robust services, improving the reliability of the sensor networks and making them mature for functional real-life deployments.

The other type of networks are Delay-Tolerant Networks (DTN). The development of such networks was initially driven by interplanetary scenarios [15]. DTNs are concerned with networks without persistent end-to-end paths and with intermittent links. The challenges foreseen were the extremely high delays and the long round-trip times due to the planets orbiting. The delay would break currently used protocols such as TCP/IP and called for new development. However, though the interplanetary scenario is still used as motivation for some researchers, another scenario has taken much of the attention; networking in areas without infrastructure, such as remote villages and third-world areas. These are scenarios currently investigated for DTNs.

The network planned for Abisko adds network connectivity to the measuring stations. Primarily, the data from the stations should be accessible remotely through the Internet. Secondary objectives include remote configuration and calibration of the sensing equipment, as well as communication between the measuring stations for in-network services. These objectives have different requirements on reliability and performance and the requirements are used as a starting point for the review of several WSN and DTN protocols.

6.1 Requirements

The sections below introduce some of the most important features and requirements for the Abisko network. These *informal* requirements should be considered in the design decisions. However, a formal and exhaustive requirements elicitation, considering both functional and non-functional requirements, must be conducted prior to the design of the network. This is left out, intended as a part of future work.

6.1.1 Accessibility

A connection to the Internet is the main motivation for building a network in Abisko. The most important advantage of Internet connectivity is remote access. With the measuring stations available online, researchers from around the world can access up-to-date data at any time. In many situations where generic measurement data is needed, the researchers would no longer have to visit the research site in order to prepare and configure the equipment, before collecting the data. With the stations online, they could be remotely configured allowing the researchers to re-task the stations in-between experiments from their desks. Such features could eliminate the need for many time consuming travels. However, the features have very different demands on reliability. For instance, if sensor data is collected for a report, a certain level of data loss may be acceptable as long as the data set is sufficiently large for an accurate report. However, in a reconfiguration or re-tasking scenario, data loss in the transfer may render a corrupt or incomplete system image, ultimately leaving the sensor node unusable if reprogrammed with the faulty system image.

In order to cover the area in and around Abisko, wireless networks are required. However, due to the challenging geographical topology and the large distances between stations, it is not always possible to offer persistent links to all network hosts. This problem is one of the main motivations for using DTNs. However, DTNs alone are not sufficient in order to reach all network endpoints. Therefor, *mobile data carriers* are introduced in order to relay data to these stations.

6.1.2 Reliability

An important use of a network connection is reliability features. Although it may be time consuming for researchers to collect data manually, it would be devastating if collected data, perhaps from several months long experiments, were lost due to a station malfunction. With a connection to another station (not necessarily to the Internet, that is), periodic uploading or sharing of sensor data could minimize the loss if a station is damaged or compromised. Also, by comparing sensor values from different stations it would be possible to perform some diagnostics if a particular sensor is suspected to report unreliable or faulty values. This could be initiated automatically as soon as it is discovered. Simultaneously, a message could be sent in order to alert the researchers about the event. They may then manually analyze the data set from the reported faulty sensor(s) and take appropriate actions.

Another consideration for reliability is redundancy. Data redundancy can include sampling at higher rates than necessary, storing data at several nodes or using traditional data loggers as backup. Redundancy may also be achieved by using more nodes than needed, having several different radio transceivers or having backup batteries for a station normally connected to power infrastructure.

Reliability also concerns whether the data is up to date or not. In traditional networks with low latency and low delays, data does not get outdated before it reaches its destination. However, in sensor networks and especially in DTNs with limited link capacities and intermittent links, that is very likely to happen. In environmental research, data has traditionally been collected after an experiment has finished. In a DTN, a query can return data collected from a nearby station which includes data from current sensor readings, however the very same station may provide forwarded data from another station which may be several hours or even days old. This must be handled by the system in order to avoid confusing the user, for instance by informing the user of the situation.

6.1.3 In-network services

Connecting measuring stations to one another could allow the sharing of data between them. For instance, collected data could be used for sensor calibration. If the data from a sensor at a certain station is examined and decided unreliable, the researchers can initiate a sensor calibration remotely. During calibration, the sensor may collect data from neighboring stations for improved accuracy.

Another possible application for inter-station connections is event triggering. An event-triggered application protocol may be the most efficient solution under some circumstances. For instance, this could be used in avalanche detection, a scenario similar to the seismic activity monitoring in [9] where event triggered data collection is used. In an avalanche scenario, there is little reason to report data to an observatory if there is no snow coverage or if the weather conditions have been stable for a very long time. However, if the weather suddenly changes with heavy snowfall or varying temperatures, stations measuring those parameters can communicate and decide mutually whether a warning event should be sent or not, ultimately triggering the remaining sensors to start or increase their sampling and reporting rate.

6.1.4 Data aggregation

For some experiments, data from a single station may not be interesting or even sufficient. However, if data from a specific subset of stations is aggregated, certain patterns and trends may be identified. Data mining can be helpful to filter larger data sets and extract implicit relations between the data. Not only could this produce interesting results, it could also potentially save energy since only a subset of the collected sensor data must be relayed to a monitoring station for review. How the data collection is initiated is also an interesting topic. Traditionally, the user initiates the collection by a query sent to a database, or in a scenario such as in Abisko, directly to one or many research stations. However, given the opportunity of in-network data aggregation, the queries may also be automatically generated by another station given that some preconditions are fulfilled.

6.2 Wireless Sensor Networks

Wireless Sensor Networks are characterized by their small, energy efficient nodes and their abilities to handle a changing network topology due to node failures or mobile nodes. The nodes are constrained by limited storage and power, similar to embedded systems. They rely on low-power radios using special purpose protocols, such as 802.15.4 (ZigBee), for communication. Of course, the range of these radios is limited, typically only tens of meters in an obstructed environment. WSNs are therefor often associated with, and envisioned to form, dense deployments with up to hundreds or even thousands of nodes. Such large deployments would make manual configuration impossible, therefor a lot of effort has been put into developing protocols that support self-organizing networks. Also, it is very important to handle node failure and interference gracefully and in a energy conservative manner.

As explained, applications for WSNs can be divided into two categories; event-driven or continuous. Event-driven applications are often used for mobile target tracking or observing infrequent actions or behavior. Continuous monitoring applications focus on more predictable, stable phenomenas which generate continuous flows of data[1]. Most of the applications in Abisko are for monitoring purposes. While WSNs introduce a lot of capabilities, they are complex and present many new challenges to networking.

The following sections are based around the problems of traditional networks, with the addition of WSN specific challenges. The problems have been identified from reviewing several different protocols and deployments. Some of these protocols are included to present important characteristics of WSNs. It should also be noted that services associated to the application layer are left out because they are discussed in general throughout the report.

6.2.1 Node structure

The nodes of a sensor network can be deployed in two ways, either structured or unstructured. Typically, an unstructured network consists of a high density network with many nodes spread arbitrarily in a given area, while a structured network consists of fewer nodes distributed evenly or according to a plan (see figure 6.1). The network connectivity and partitioning varies depending on the structure. Some parts of a network may be

[1] An example of this was given in section 4.1

fully connected while other parts rely on a single link not to become partitioned from the rest of the network. A structured network may be minimized with respect to the number of nodes. Such a network could suffer severely from network partitioning in case of node failure. However, if nodes are spread arbitrary it is harder to predict problematic network properties such as bottle-neck links and to recover from failing nodes.

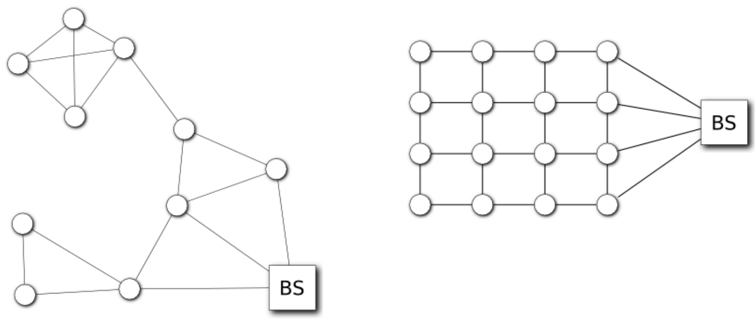

Figure 6.1: An unstructured sensor network with a base station to the left and a structured to the right.

The connectivity in the network is also affected by the geographical spread of the nodes. With a very small deployment area, the network graph will be highly connected while a network over a larger area, which is more likely for the Abisko scenario, will have a low connectivity. In fact, limited node density in combination with a large deployment area might make end-to-end paths impossible. There are several techniques addressing such issues. One is to place helper nodes between stations which relay traffic between stations. However, since standard radio transceivers used with protocols such as 802.11 have a limited range this might not be a viable solution in a situation where distances between nodes extend to several kilometers. It also makes the network vulnerable to partitioning in case a node fails. Another technique is to use an opportunistic approach with mobile data carriers. This is a very interesting approach for Abisko, since many people hike along the trails, some of them which pass measuring stations. See section 6.3.4 for more details on this.

The coverage of a WSN affects its quality and efficiency. For monitoring applications, the quality may be measured by means of the granularity and precision of the data, while the efficiency can be measured in sensor yield [7]. Coverage is also important in terms of energy conservation. To save battery power, nodes can be scheduled to sleep at regular intervals. An example of such a protocol is the Coverage Configuration Protocol [16] which allows the network to configure itself according to the coverage needs of the application.

6.2.2 Transport layer

The transport layer is concerned with the reliability and quality of the network services. Detection and prevention of well-known phenomenons such as packet loss due to signal noise, node memory limitations or congestion must be implemented. An important difference between sensor networks and normal Local Area Networks (LAN) is the type of applications that they support; a sensor network commonly supports only one specific application. This means that the protocols can be adapted to the application in order to optimize performance and energy aspects.

The following sections concern requirements on transport protocols for wireless sensor networks. They are based on the requirements identified by Iyer et al. (2005) [17]. Four different protocols have been reviewed.

- Sensor Transmission Control Protocol (STCP) [17]
- Price-Oriented Reliable Transport Protocol (PORT) [18]
- Event-to-Sink Reliable Transport (ESRT) [19]
- Pump Slowly Fetch Quickly (PSFQ) [20]

The first three protocols consider the case where data flows from sensor to sink (here, a sink is considered to be a base station), the most typical operation for a sensor network. PSFQ targets the opposite which is important when re-configuring sensor nodes. While STCP targets general WSN applications, the other three do not. Therefor, some of the features of these protocols are not suitable for other types of applications, other than the ones used for evaluation.

Reliability

Absolute reliability, meaning that every packet that is transmitted is guaranteed to reach its destination, is not always needed nor wanted because it can make a protocol very energy inefficient since retransmissions are needed. Therefor, a transport protocol that can adjust the level of reliability is preferred. This can be achieved with a protocol that implements end-to-end reliability. As an example, assume a multi-hop network with a tree structure where the child nodes rely on their parent nodes to forward their packets (figure 6.2). If a packet is lost between the root node (BS) and its first child node (N2) the retransmitted package must be sent again from the source node (SN). This method enables reliability on a session-basis. The alternative is hop-by-hop reliability. Using this scheme, the packets are cached at intermediate nodes. If a packet is lost, only the previous intermediate node must resend the packet. Unfortunately, this does not work well with variable reliability because there is not one single node that can decide whether a packet should be retransmitted or not, as is the case in the end-to-end scheme. In the case of a re-programming of a sensor node, the new firmware image must be transmitted with absolute reliability, otherwise the image received by the node may be incomplete or corrupt.

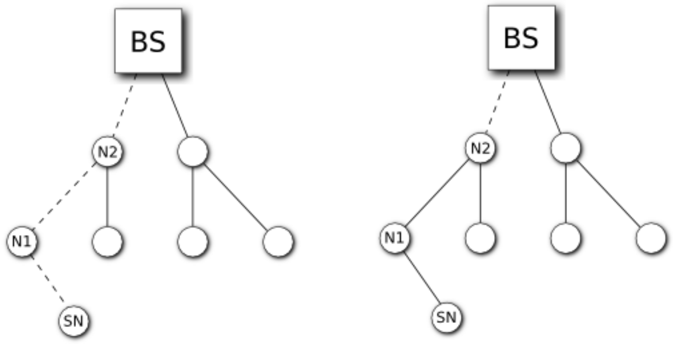

Figure 6.2: Dotted lines mark the path for a retransmissions. End-to-end reliability left, hop-by-hop reliability to the right.

Data flow

Sensor networks typically feature very different data flows depending on their application. A environment monitoring network would produce a stable flow of sensor readings [7], while an event detection network produces an unpredictable, possibly high-rate flow of data [9]. Additionally, the direction of the flow is also a factor. The typical direction of the flow is from a sensing source node to the base station. However, in sensor networks that support re-programming, the opposite must be supported as well. (Such protocols must also implement a multicast functionality.)

Intuitively, a continuous flow is more predictable, allowing more optimizations and fine tuning. This is illustrated by the STCP protocol; when dealing with a continuous flow, a timer is used along with the rate of transmission to calculate the expected time of arrival of a packet. Only if the packet does not arrive in time, a NACK (Negative ACKnowledgement) is sent. The rate at which the packets are expected is estimated by using previous packets' Estimated Trip Time. Using this scheme, the overhead of an ACK for each packet is avoided.

Congestion

Congestion affects the throughput of a regular network. In a sensor network, it will also significantly reduce the lifetime of the network because recurring retransmissions drain the batteries of sensor nodes. Congestion generally appears as packet drop. In STCP, the approach of using a congestion bit in each packet's header is used. This way, each intermediate node has the chance of setting this bit, notifying the sink of congestion which in turn notifies the source node which can then take appropriate actions. In PORT, a price is defined for each node. The price of a node is the cost to deliver a packet successfully from the node. This means that the price depends on packet loss, which includes congestion. Here, PORT becomes an example of a protocol that is specific for its application since it incorporates a routing scheme; nodes in PORT are greedy, they prefer to send packets via nodes that have a low price associated with them. Therefor, nodes avoid congested routes (since they have a high price)[2].

However, deciding upon what actions should be taken when congestion occurs can alternatively be centralized. In ESRT, the sink decides upon a reporting interval for the sensor nodes. Under the assumption that the increase in incoming traffic at each sensor node is constant between reporting periods, the sensors can detect a risk of congestion by monitoring their buffer level for two previous reporting periods. If a sensor detects a pending increase of the buffer level which would overflow its buffer during the next reporting period, it reports this to the sink at the next opportunity which then takes appropriate actions.

6.2.3 Network layer

The network layer considers the problem of finding a path to send a packet along, from a source node to a destination. In wireless sensor networks, most efforts are spent developing protocols that are as energy efficient as possible. Traditional routing as in IP, with explicit node addressing, is not applicable because of the possibly large number of sensors deployed. Also, sensor networks are often location oriented; data queries are often targeted at a set of sensors which are located in the same area. There are a number of general approaches to these problems, namely data-centric, hierarchical and location-based protocols.

An ideal routing protocol is hard to deduce because of the needs of different applications, but general properties, apart from the energy conservation can be summarized. In-network data aggregation, route caching and end-to-end reliability[3] are among the wanted properties. Also, it is desirable to enable localized queries, meaning that sensors that are not in the interesting area, should not have to participate in the routing (unless needed to create a path to the sink). Another feature is a self-configuring network, in case of node failure or if the topology changes (perhaps due to mobile nodes). This especially applies to hierarchical protocols where some high ranked nodes act as 'cluster heads'. This puts a higher load on them, since lower ranked nodes route their data intended for the sink, through the cluster heads.

The following sections have been derived from a review of three protocols. Directed diffusion [22] is a protocol well-known for its pioneering data-centric approach to the challenges stated above. In [23] the sensor network is organized into clusters with a powerful gateway node as cluster head. In GEAR (Geographical and Energy Aware Routing) [24], the nodes are assumed to know their own and their neighbors locations. They also learn about their neighboring nodes' energy levels. This is exploited to make appropriate routing decisions.

[2]The approach is very simple, but it suffers from an oscillation phenomenon further discussed in [18]

[3]In the network layer, this concerns whether a path from source to destination is found. Although it may not seem very intuitive for a routing protocol not to guarantee that if a path exist it is found, such protocols exist [21].

Energy conservation

The main approach to conserve energy when routing, is to minimize the communication overhead. This can be achieved by in-network aggregation and avoiding error-prone paths. Another method is to avoid the overhead of keeping the state of the network topology, something that requires periodic route updating. *Directed diffusion* uses meta-data to describe an interest in data. The interest is propagated through the network in a neighbor-to-neighbor fashion. The data is then routed back to the sink (the source of the interest) along an optimal path according to a chosen metric (e.g. link rate). A path back to the sink is set up simultaneously as the interest message is propagated, however there is no guarantee that the same path is used both ways. Each node keeps a record of what interest came from which neighbor node. If the same interest was received from multiple neighbors, the node makes a local decision which path to follow depending on the metric. This setup happens on demand, thus no topology status must be kept. Another effect of this is that all nodes are capable to aggregate both interest and data messages, reducing redundant transmissions.

In most sensor network applications a gateway node is used to connect the sensor nodes to a larger, long distance network. These gateway nodes are often more powerful, have long distance communication capabilities and are not as constrained in terms of energy as sensor nodes. Therefor, it makes sense to use them in a centralized manner. In [23], the gateway is responsible for keeping an up-to-date routing table. It applies metrics to the paths according to a model based on several parameters, the most interesting being the remaining energy of a node, the rate of energy consumption of a node and the communication cost given as transmission power. This way, the gateway controls which links are used in order to send and relay sensor data, something that may prevent network partitioning. Another feature possible with a centralized approach is a combination with a TDMA (Time Division Multiple Access) MAC protocol. This allows nodes to be scheduled in order to turn off their radio transceiver periodically and thus conserve energy.

A third approach to conserve energy when routing is to use a location based protocol. This assumes that the nodes know their location, which can be achieved by the use of GPS or localization algorithms. In [24], nodes learn about their neighbors, including their location and energy levels. An appropriate path is chosen greedily (a neighbor close to the target region), while minimizing the cost of a path, given by the distance to the target region and the neighboring nodes consumed energy. In three situations, if a packet has traveled for a long distance, if it enters a region with depleted nodes or if it is close to its target region, it is not beneficial to consider energy-consumption. Therefor, only the geographical location is considered in these situations in order to route the packets.

Scaling

The effects of scaling a sensor network are not easy to foresee. In a data-centric protocol such as Directed diffusion, the sink (the node interested in the data from an event) is not different from the rest of the nodes, apart from that it may not feature sensors and therefor does not answer to queries for event data. Thus, there is no intuitive way to support scaling of the network. Instead, such protocols must rely on features such as in-network aggregation and caching to allow scaling without wasting energy. In Directed diffusion, a node can 'reinforce' a path positively or negatively to a neighbor in order to achieve a higher or lower data rate. This mechanism is controlled locally by each node, allowing it to scale well without significant performance degrading. However, in some situations this reinforcement can lead to a sink reinforcing multiple paths which could potentially become a waste of energy if several sources sense the same event. Also, data-centric protocols do not require unique global node identifiers, something that allows an arbitrary number of nodes be deployed without introducing addressing problems.

While Directed Diffusion supports multiple sinks as well as sources, a common approach in sensor networks is to use a single gateway node. When considering scaling, this approach can become very inefficient, for example if a centralized routing scheme is used, and possibly even make the network unusable if the gateway fails. In a cluster-based approach, several gateway nodes exist which balance the load of the sensor nodes in the network. Scaling in a clustered network may be supported by simply adding more gateways (cluster heads) as the network grows. Of course, this requires that it is possible to deploy additional gateway nodes, something that cannot be taken for granted.

Another issue that deserves consideration is scaling in extremely dense sensor networks. If information about neighbor nodes is used for route calculation, an excessive overhead could be introduced when updating this information. Especially if the network is highly connected where each node has tens of neighbors. In such highly connected networks other issues, such as media access, may also become troublesome.

Link failure

Since link failure is imminent in sensor networks, it is important to support a dynamic topology. A protocol, in which the nodes probe for and end-to-end path, might use significant amounts of energy in order to establish a path. While this is a viable approach in normal networks, it is not in energy-constrained, lossy, sensor networks. Instead, an on-demand approach such as that of Directed diffusion may be adopted. Since the next hop is chosen locally by each node, the path is built greedily when needed. Also, this approach does not require periodic probing in order to keep a snapshot of the current topology.

In the GEAR protocol, nodes learn about their neighbors. If the network dynamic is unstable with nodes failing frequently or periodically, or if the radio link is lossy, this can introduce an unwanted overhead or possibly inaccurate information about neighbor nodes.

Application dependency

Finally, some considerations should be made about the application dependency of the routing protocols. In traditional networking, a clear separation between the different network layers is encouraged. However, sensor networks are often application specific, without any significant modifications throughout their existence. Therefor, it is justified to have network layers that are slightly more coupled if needed. This is something that data-centric protocols exploit, choosing network paths by considering the properties of the application data being routed. Location-based protocols must know their position to route successfully, therefor they can benefit from GPS data. Although not every node may be equipped with a GPS unit, neighbor nodes may be used in order to triangulate a position, something that would require application layer interaction.

6.3 Delay-Tolerant Networks

A Delay-Tolerant Network (DTN) is a type of overlay network that aims at enabling communication over links that suffer from extremely long delays or disruption. The motivation of such an architecture is summarized in an RFC[4] [25] and is based on a number of assumptions in the Internet architecture. These assumptions include (but are not limited to):

- An end-to-end path exists during a communication session.
- Retransmissions are based on timely and stable feedback from the receiver.
- The end-to-end loss is relatively small.
- All routers and end nodes support the TCP/IP protocols.
- That packet switching is the most appropriate abstraction for interoperability and performance.

Additionally, factors such as very low and possibly unbalanced data rates of the up and down links also matter. The assumptions make current Internet protocols unsuitable or even unusable in DTNs. Networks that do not rely upon them may become very useful and important in regions without static infrastructure or reliable links.

6.3.1 The Internet approach

The common approach of messaging in Internet enabled networks is to split the message into several packets. Among many reasons, this is to enable link sharing, reduce the bandwidth needed simultaneously, to reduce the size of buffers needed, and to enable routing of the packets over several paths in order to enhance performance and avoid packet loss due to congestion, etc. The TCP protocol and its variants is the most widely used transport protocol on the Internet. It uses a three-way handshake to set up a connection in a controlled manner and features flow-control as well as congestion avoidance algorithms. For reliability, TCP requires that every packet is acknowledged by the receiver, and if it is not acknowledged it is mandatory that the source retransmits

[4] Request For Comments, a memorandum published by the Internet Engineering Task Force (IETF).

the packet. Flow-control is implemented by letting the receiver give feedback to the sender about how much space is available in its receive buffer. The sender uses this information in order to keep the amount of data sent below this threshold at all time[5]. Congestion control is implemented by using a congestion window variable, which is the maximum amount allowed of unacknowledged data in the network. If a packet is lost, the window is decreased (usually divided by two). If no packet loss is detected, the sender assumes that there is available link capacity and increases its window (by a fraction of the window).

These are the fundamental principles for the mechanisms, see [26] for details. However, it becomes clear that these design choices call for persistent, end-to-end paths typically with link delays measured in milliseconds, something that is not available in DTN networks.

6.3.2 The Bundle layer

In order to meet the challenges, DTNs have forced reconsideration of the packet switching approach. Instead of using ordinary packets, a message or *bundle* is introduced [25, 27]. The bundle contains application data, typical meta-data on how to process the data, and information about the bundle itself. These are processed in the Bundle layer between the application and the transport layer in the network stack. The bundle layer is used by all network regions that make up the DTN. Bundles, which can be arbitrarily long, can be fragmented into smaller bundles just as regular datagrams. If a message is fragmented, the bundle layer is responsible for reassembling the separate parts into the original message.

The nodes of a DTN either act as a host (the source or destination of application data), a router (forwards bundles within a single region) or a gateway (forwarding between different regions). The bundle layer supports end-to-end messaging by the use of *Custody transfers* and *Return receipts*. Custody transfers can be seen as node-to-node reliability by retransmissions, while the (optional) use of return receipts adds the last part of reliability by acknowledging that the bundle has been received.

In order to achieve this, the bundle layer overtakes the responsibilities of the transport layer and the layers beneath, in regions where regular protocols (TCP/IP) cannot be used. It should be noted, that end-to-end reliability is only supported in the bundle layer. In the lower layers, the reliability is limited to a node-to-node basis. Gateway nodes implement a double (parallel) network stack in order to interface between regions with different transport, network, link and physical layers. Of course, this may also include interfacing between two non-IP enabled regions.

It should be noted that the bundle approach requires some assumptions itself. Especially, that the nodes have sufficiently large and persistent storage capabilities in order to queue bundles until a communication link is available. However, the storage capa-

[5]Actually, when the threshold is zero, the sender keeps sending one byte data, otherwise it would block the connection.

bilities of modern computers are measured in Gigabytes and even Terabytes, so this is considered a minor issue.

6.3.3 Message routing

While the DTN architecture described enables support for long-delay transmissions, it does not discuss how to route messages. Neither does it describe which medium should be used for relaying messages in and between DTN regions. A common approach in areas without infrastructure is to use mobile nodes, or *data carriers*. This can include almost any moving object, such as humans, cars, autonomous vehicles or animals. In order to relay messages between DTN nodes, data carriers have appropriate equipment for short distance transmissions, such as a mobile phone, a PDA or a laptop. The devices usually have wireless interfaces, for example WiFi or Bluetooth which is used in order to transmit the messages they carry to the stationary DTN node once contact is made. (A contact is made when an opportunity to send a message to another node exists, i.e two nodes are capable of exchanging a message [25].)

The methods used for message routing in DTNs are commonly divided into two categories. The first category relies on message replication. Basically, a message is replicated and sent to any node that it makes contact with. The other category relies on some knowledge about the network, for example at which time a contact is made (scheduled contacts [28]). Whether a message is actually forwarded to a contact or not also depends on the receivers capacity. Capacity can be measured in link quality, buffer space and the duration of the contact. The node capacity can also be seen as network knowledge. In [28], DTN routing protocols are evaluated according to three different metrics; delivery ratio (the fraction of messages correctly delivered to the destination within a given time period), latency (the time between when the message was generated and when it was received) and finally the number of transmissions made to deliver a message. At this point, it should be noted that the energy-conserving theme of this report is somewhat set aside. The protocols reviewed for this part do not take energy-consumption into consideration. However, the number of transmissions needed for successful delivery of a packet is a simple, yet effective way to evaluate energy efficiency.

Message replication

The concept of message replication is quite simple. The more messages sent to forwarding nodes, the greater the probability of successful delivery. However, the obvious method of flooding the network by sending a message to every node that is contacted is very wasteful. In [29], several measures are taken in order to control the flooding. The frequency at which messages are sent is referred to as the *willingness* of a node. Constraints on the willingness results in nodes that do not always forward messages, even if contact is made. Two message life-time mechanisms are implemented to support this; *time-to-live* limits the number of times a message can be forwarded, and the *kill time* is a time interval after which the message should be discarded. These variables are fairly straight-forward. However, a third and more interesting mechanism is also implemented.

This is referred to as a *passive cure*. This is a special type of acknowledgement message which is sent out by the final destination node when a message is received. This is a way to tell other nodes that the message was successfully delivered, and that further copies of the message stored at intermediate nodes can, and should, be discarded.

Network knowledge

In contrast to the simple methods of flooding schemes, those that rely on network knowledge are considerably more sophisticated. By using several abstract knowledge *oracles*, the authors of [30] implement and evaluate a number of protocols and show how network knowledge can be used in order to improve the delay time and delivery ratio. Three kinds of oracles are used; contact oracles can answer questions regarding when a contact will occur and the duration of it. Queuing oracles answer questions about the buffer capacity of nodes (the time a message must wait before it can be transmitted over a path) and the third oracle is aware of the present and future traffic demands. While the oracles may seem slightly unrealistic at first, they are actually not unfeasible. In DTN scenarios contacts may be scheduled, such as a train or bus which follows a timetable. Similarly, it is likely that the hardware of such a contact is known, meaning that the buffer capacity can be assumed to be sufficient or insufficient depending on the size of the message(s) to be sent.

Depending on the knowledge, different routing approaches can be taken. Without using any oracles at all, routes are created on demand in a hop-by-hop fashion. This may lead to routing loops and there is no guarantee of successful delivery. If the contact oracle(s) is introduced, predictions about future contacts can be used in order to establish the complete path from source to destination that a message should follow. This is known as source-routing. If costs are associated with different paths and do not vary with time, routing can be modeled as a cost-minimizing problem and solved using Dijkstra's shortest path algorithm. With knowledge about contacts and the local queue[6], the route can be established in a hop-by-hop manner, making a local optimal path choice. And finally, if the global queue status is known (i.e. the queuing times at all nodes), once again source routing is possible and provides the best performance in terms of delay and message delivery ratio. This is due to the possibility to predict all delays at intermediate nodes and therefor "cherry picking" the best path in advance.

It is not very surprising that increasing network knowledge also increases the performance. However, as is shown in [30], knowledge about some parameters does not improve the performance significantly, making the effort to implement such oracles questionable.

6.3.4 Opportunistic Networks

Opportunistic networks are a subset of Delay-Tolerant Networks. They differentiate from regular DTNs by assuming that contact opportunities are unpredictable. Another distinction is that while DTNs concern contacts between different regions, or networks,

[6]The local queue time is the time a message must wait before it is forwarded.

opportunistic networks do not, i.e. all nodes belong to the same network. Differently put, every node in an opportunistic network is a DTN gateway. Because of the unpredictability and absence of contact schedules, source routing is not an option for these networks. Instead, they must rely on hop-by-hop routing. However, approaches to routing in opportunistic networks are not very different from routing in DTNs. Rather than revisiting the techniques presented in section 6.3.3, this section focuses on a selection of problems that arise in a opportunistic networking scenario. While these networks do not rely on static infrastructure, mobile data carriers can be seen as the equivalent in an opportunistic network. However, the infrastructure is not fixed, but instead mobile. This, once again, affects the predictability of the network topology and the contacts that these data carriers will make. In a real scenario, such as the one in Abisko, these data carriers may be hikers carrying a mobile phone between mountain lodges situated along the paths. While making their way along a path, the phone connects to fixed measuring stations within range, allowing the stations to "dump" their collected data onto the phone which then either carries the data to a base station, or, by using the cellular network, directly uploads the data to a server or a distributed storage layer.

Such a scenario may seem quite trivial, but in order to actually implement a system that offers this functionality, many different design choices must be made. The scenario has a different set of usage patterns and requirements, compared to traditional networking scenarios.

In order to relay data from other nodes, a data carrier must somehow become aware of the existence of the data. Rather than using a node-centric approach, where a node is addressed and polled for the data, a request for the data is issued by the carrier, or the data can be published into the network by the source. (This is known as a publish/subscribe paradigm.) This is a more data-centric approach in which a data carrier does not concern about the source of the data.

Several aspects in this scenario concern the application layer services. For example, the nodes may have different network interfaces, such as Bluetooth, WiFi or 802.15.4. With a traditional network approach, the support for different interfaces must be implemented in the application. Further, a node might be re-configured post-deployment, meaning that it runs several different applications during periods of its lifetime. Hence, every application must implement the interface support. Another important issue is energy conservation. Mobile nodes, as well as data carriers, may be very limited in power resources. This implies that it is not always a wise decision to participate in network activities. A data carrier must be able to choose not to relay data in favor of its own life-time. Such a choice also concern other resources, such as storage space.

Haggle - an architecture for opportunistic networking

Haggle [31, 32] is a networking architecture designed for mobile devices. It deals with many of the challenges presented above. It offers seamless network connectivity and allows applications to be abstracted away from the details of the network logic. At the same time it enables application and user data to be used in the network operations. For instance, it enables applications to find network nodes with high-level identifiers, such as names, instead of IP or MAC identifiers. Another example is that a node may choose to forward a message to another node, depending on the contents of the message. In a traditional network, this decision is made without any context-awareness, it is decided strictly on metrics such as congestion or delay.

Haggle is based on three main principles. First, a mobile device is constantly moving through different network environments which have different properties, such as what interfaces are used, link performance and available neighbors. Therefor, Haggle supports *late-binding*, meaning that the circumstances in the current situation may be regarded when the communication interface, protocols and naming schemes are decided upon. This is the opposite of the approach in the Internet, where these three components are determined before the communication is initiated. Second, Haggle uses a data-centric approach and relies on meta-data for network driven operations. This requires that data and its meta-data, expressed as name-value pairs, is exposed to the architecture, rather than only at an application level. Third, Haggle uses a centralized model for resource management. This is a key feature since mobile devices are limited in terms of power and processing capabilities.

The flexibility that Haggle offers is one of its key features. Not only can multiple interfaces be used by a device - Haggle also allows the use of several different forwarding algorithms. Deciding on which one to use is made according to the late binding principle, choosing the most suitable for a certain situation. The same flexibility is incorporated into the naming scheme system. Instead of relying on one particular name, such as an IP-address, several different high-level names can be used which are then mapped to low-level names.

Since the applications do not interact with the networking logic, they rely on Haggle to decide if a network operation is performed or not. Whenever an application wants to utilize a network connection, it registers a task with the Haggle architecture. Whether this task will be performed (or not) and when, depends on the current context and on user preferences. The tasks can be prioritized according to many different parameters. The authors of Haggle use e-mail as an example; if an application checked for new e-mails only a minute ago, Haggle may prioritize other tasks. However, if the last check was made more than an hour ago, the task may be scheduled immediately.

The features of Haggle, especially the centralized resource management and data-centric networking principles make Haggle a suitable choice for opportunistic networking in a scenario like Abisko. Therefor, it will be considered in the design of the Abisko network.

6.4 Abisko network structure

As should be clear by now, the situation in Abisko is very diverse and depending on many different parameters. On a very high level, the most important factors include the applications and their requirements, the location, what technology is available there and what services the researchers desire. Because of the complexity and in many situations conflicting requirements, it is obvious that a generic solution for all situations does not exist. This section proposes a structure for the Abisko network and what responsibilities each layer should have.

In order to make good decisions, the situation has to be divided into several smaller problems. However, this introduces yet another question; how should this scenario be divided? When reviewing the situation, it appears as if most of the aspects involved somehow relate to a geographic location. It is one, if not the most, significant feature of the Abisko scenario. Further, many of the measuring stations' locations are decided by their application because the phenomena studied appears at specific locations, or are best studied in certain areas. Another example is the accessibility of the measuring stations. While the stations close to the Abisko village are within an hour of transportation, the most remote stations may not be accessed without a day-long hike. Those stations must be highly reliable, something that may be prioritized in a trade-off with other features.

However, even with a scenario divided into smaller geographical regions, certain network related aspects cannot be neglected. It is tempting to further divide the regions into areas depending on network properties, such as node density (which could translate into distances between nodes), services offered and communication hierarchy. The following sections are therefor divided into a layered hierarchy according to locality, but general discussions concerning all layers may be included where appropriate. Also, it is worth noting that discussions about the actual nodes and their operation include node to node communication as well, while at a higher abstraction layer, specifically the measuring sites (research sites) and the global Abisko network, the discussions are more about the services offered.

In order to understand the proposed network topologies, a review of the requirements is in place. The objective of the measuring station is to obtain accurate data within many different research disciplines. The data is collected from hundreds of different stations, either by manually logging values into a spreadsheet or by visiting a station with an interface, such as a USB memory or a laptop. The amounts of data collected varies from low-frequent sampling such as cloud-coverage or water levels, to wind-speed and direction, sampled every five seconds. These variables produce a stable flow, however others such as an avalanche warning system may be event-triggered producing high flows during short periods of time. The accuracy of the data varies, meteorological data might be used in official nation-wide reports, while other may only be used for reference when reviewing the conditions during long time periods.

The researchers desire continuous, remote access to measurement data. The data should be available via the Internet at all times. The data should be up-to-date and reliable. Also, it should be made available continuously if possible, meaning it should preferably not be delivered in aggregated reports in periodic, sparse time intervals.

Another important issue is maintenance. The measuring stations should not require frequent maintenance visits in order to change batteries. An optimal service interval would stretch beyond six months, because of the long winters in Abisko. However, because current maintenance intervals are measured in days, even intervals of weeks or perhaps a month would be a significant improvement. Further, the measuring stations should support remote configuration and re-tasking.

It is important to note that the following sections are not intended as a cookbook recipe for a successful network deployment. However, they discuss some considerations and ideas that may be used in the Abisko scenario.

6.4.1 A network overview

The network scenario in Abisko can be divided into four hierarchical entities; the nodes, the measuring sites, the site regions, and finally the global network as depicted in figure 6.3. The nodes are the network hosts and nodes that are in close proximity to one another, possibly close enough to communicate, form a measuring site. A measuring site is one or many sensing nodes. A site with more than one sensing node typically has a base station which is somewhat more capable in terms of energy reserves, network range and functionality. Several measuring sites together form a region in the network. It is not unlikely that the base stations have different capabilities which are shared within the network region. For instance, this could be true if one base station is connected to power infrastructure, while another is not. The different regions in Abisko form the global Abisko network. At this very high-level abstraction, the services associated with the network can be seen as the backbone in a company network, including servers, databases and external interfaces, such as Internet access and similar services.

6.4.2 Network nodes

The Abisko scenario calls for several different kinds of network nodes. A *sensor node* is what the researchers refer to as a measuring station. A station is located at a predefined, well chosen location in order to sample the environment with its sensors. Every station uses a radio unit for communication with other nearby stations. Of course, the radio unit interfaces with the sensors and is responsible for transmitting the sensor data into the network. The infrastructure available for sensor nodes vary, some may have access to external power supplies and network access points, while some do not. This also affects their capabilities in terms of processing power, life-time and what type of applications they are suitable for. However, a general rule of thumb is that a sensor node is very constrained in terms of energy and storage (i.e. no infrastructure is available). A node should be able to survive for several weeks, preferably with the radio unit turned on and active several times per day, perhaps for one session[7] every hour. This would offer a large enough time frame for making long-term experiments viable.

A second type of nodes are the *relay nodes*. These nodes are not considered measuring stations, since they do not have any sensors attached. Instead, these nodes can be used to relay data from measuring stations that are located in places that make them difficult

[7] Here, a session is enough time for transmitting a predefined amount of sensor data.

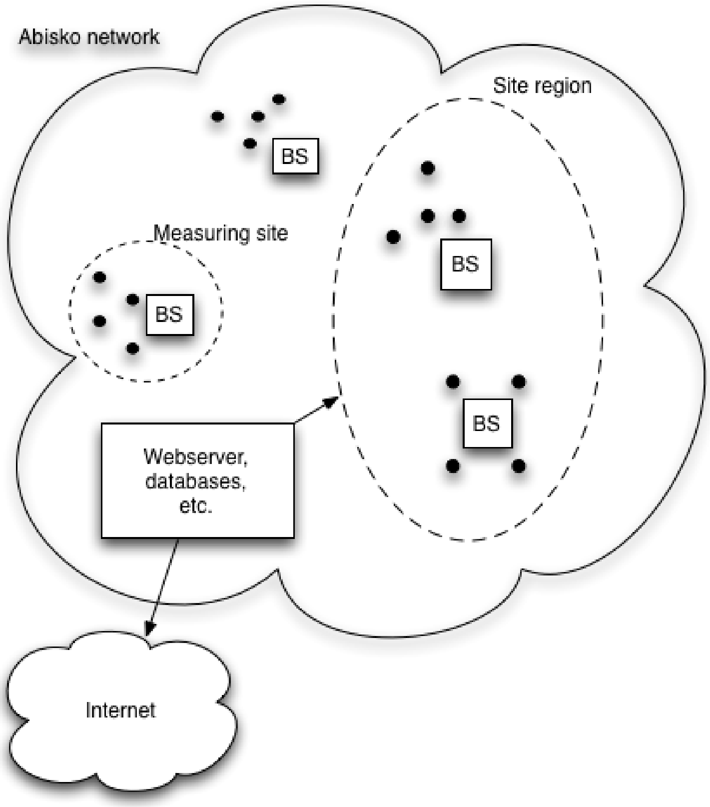

Figure 6.3: An overview of the Abisko network.

to access. These nodes are typically deployed in a on-demand manner. This indicates that they should be small, low-powered devices without any need for infrastructure. A relay node may serve network connectivity for several nodes, meaning they must have sufficient energy supplies for their needs. In certain situations it may also be necessary for them to use special purpose equipment, such as antennas allowing them to relay data traffic over greater distances than a regular sensor node, or extended storage space if it is part of a DTN network.

Relay nodes may also be mobile. This is something that can be very valuable in Abisko where the distances between nodes are up to several kilometers long. These nodes should typically be hand-held devices, such as a laptop, a phone or perhaps a smaller special-purpose unit design solely for this application. The units can be carried by hikers that hike along marked paths in the terrain, paths that pass by measuring sites or relay nodes. When passing a node, the device offers a contact opportunity for the node, which may choose to forward a message or request for routing information. The precise operation depends on the protocol(s) implemented. Mobile devices are likely to have access to infrastructure in a predictable pattern (for example, the time it takes to hike between two mountain lodges is fairly constant and the hikers are likely to follow a trail). Mobile phones are very good candidates as mobile nodes. They typically have batteries that last several days and some devices may also have a GPS unit, which can be very useful for geo-tagging received data. (For instance, this could be used for positioning a measuring station with reasonable accuracy.)

The third type of network nodes that is likely to be used in Abisko is a more capable node, in sensor networking such nodes are referred to as a *base station.* Base station nodes are typically more powerful with additional storage space, more processor power and a mid or long-range radio link. These stations may also have a GPS unit which can be used for GIS (Geographical Information Systems) purposes, similar to the mobile nodes'. Base stations often have a more organizational role in the network, not necessarily participating with sensors. Powering a base station with an external power source may profit not only the base station itself, but all of the sensor nodes as well since it may then use more power to organize the network. This could include calculations for routing decisions or enabling one-hop transmissions in order to reduce the load on forwarding nodes. Also, a base station may use more power in order to communicate with other base stations, serving as a interface for the low-power sensors and aggregating data, responding to requests from other base stations, etc.

Node locations

The general position of a node is of course determined by the application it is intended for. However, within that area, it is important that the location is chosen primarily according to the needs of the measuring, while considerations related to networking should be set aside. This may result in suboptimal locations in terms of network connectivity, although this can in most cases be compensated with the help of relay nodes. In contrast, optimal placing in terms of networking but a suboptimal placement in terms of sensing possibilities would effectively neutralize the need for the network since the data would potentially become inaccurate or irrelevant.

Once a suitable location for the sensing has been found, secondary needs such as available infrastructure, network topology and radio signal coverage may affect the placing. In a dense sensor deployment with nodes typically within 10 meters of one another and where network connectivity does not pose a problem, it would be wise to prioritize access to power infrastructure if available. Further, the position of a base station could be chosen in order to maximize signal coverage, such as placing it on a nearby hill. A drawback of this would be accessibility, since it is likely that base station is slightly larger and heavier making transport difficult.

A sparse network requires different priorities. For instance, it is more exposed to network partitioning. Placing nodes should, if possible, take this into account and prioritize multiple paths to the base station, or use relay nodes to increase the reliability and performance. Because of the nature of the applications, the nodes locations are generally predefined and therefor form a structured layout. However, since they may not form a symmetric shape, this variant of node deployment may still suffer from drawbacks associated with unstructured layouts.

Radio links

Another factor which may affect the nodes' locations is the type of radio equipment used. In a dense sensor network where communication distances between sensor nodes are short (<10-20 meters), the 802.15.4 standard would suffice in terms of range for communication between nodes. Also, previous research deployments (reviewed in chapter 5) have shown that the transfer rate, tens of kbps, is sufficient for most applications. A more interesting situation occurs in cases when a mobile node enters the area. Given that the mobile node should be able to communicate with the sensor nodes, it is required that the sensor nodes have at least one additional interface, such as Bluetooth. However, with respect to power conservation, sensor nodes' limited storage and processing power and the complexity of implementation, a better approach would be to let the base node support Bluetooth or WiFi and act as an interface on behalf of the other nodes. This presents a trade-off in term of the proximity between the base station and mobile node needed.

The base nodes require significantly more powerful radio equipment. These nodes should be able to forward the data from a possibly large set of sensor nodes over long distances, where the terrain might be obstructed by trees or mountains. Distances of several kilometers implies use of satellite connection, cellular networks, WiMAX or a unlicensed, custom radio unit. Unfortunately, WiMAX is unavailable in Abisko and cellular networks only cover a very small area around the main road passing Abisko. Although a satellite link may seem appropriate, they may require obtrusive hardware and an additional service subscription. Therefor, the preferred choice is to use custom radio units operating in unlicensed frequency bands. These units can be adapted to suit the needs at each station, using different antennas. The main concern for these stations is the lack of power, it is unlikely that they can achieve a viable life-time if only run on battery. Therefor, it should be seen as a necessity to equip base stations with solar panels or a wind-power generator. While a powerful radio is needed for long-range communication, a base station must also feature a low-range radio device for communication with the sensor nodes. As discussed above, this would include a 802.15.4 unit, and possibly a WiFi or Bluetooth device for communication with a mobile phone or laptop.

6.4.3 A measuring site

A measuring site, or research site, is a fairly small geographical area where one or multiple sensor nodes are deployed. Along with the sensing nodes, a base station is also necessary in order to act as a gateway for the low-power nodes, interfacing with the long-distance communication with other research sites. The number of sensor nodes deployed at a site may vary depending on the application and the situation. For some applications, a single node may be sufficient and for these stations, a combined sensor node/base station is the preferred approach, there is no reason to separate the sensing node from the gateway.

Capabilities and services

The capabilities of a measuring site concerns support for site-specific services. These may include data aggregation/collection and self-calibration/configuration. Data aggregation includes tasks associated with data collection including averaging, region based queries or sensor fusion. Sensor fusion is important when several different variables are monitored at a site, and the overall observed situation is affected by them as a whole. Weather monitoring is such an application, for instance wind chill and humidity as well as the sun's radiation and the cloud coverage affects the perceived temperature. Of course, data collection is the main purpose of a measuring site. How and when data is collected may be influenced by time, current or past conditions, researchers demand for data updates, special events such as experiment start or end or by events detected during experiments. Of course, the nodes' hardware, protocol implementations, as well as existing infrastructure also affects the capabilities of a site.

Layout

The layout of a measuring site concerns the physical placement of the nodes within the site. It is depending on several different parameters, but it also has significant implications on the design of other parts of the site. At a site, a set of sensors may be grouped together because they share some properties, perhaps monitoring the same variable or because they are located in the same region. Such a set of sensors is referred to as a *sensor patch*. The size of a sensor patch varies with the application. If considering the number of nodes, a typical sensor patch consists of ten or more nodes, although scaling should be considered thoroughly, allowing large patches with up to hundred sensors or more. The geographical area that a patch covers is of course depending on the number of nodes. Also, larger areas may be covered with a multi-hop network, as opposed to a single-hop. There are no logical limitations as to how many different variables that can be monitored at a site. However, for reasons such as dependency and reliability, as well as complexity, it may be advantageous to separate sensors monitoring the same variables into several different patches.

For an example, consider the case of avalanche detection. For this application, sensors that measure weather variables (temperature, wind, etc.) as well as accelerometers measuring vibrations may be used. In order to predict potentially dangerous situations, as well as sending an alert if an avalanche has been set off, the reliability of the data transfer must be high. In this situation, reliability means that a continuous flow of sensor data is delivered to the observer and that the data is representative for the observed location, something not always obvious. For instance, in windy conditions a sensor measuring snow depth may report very large depths, while in fact it is only due to the wind direction which makes snow accumulate at the position of the sensor. If readings from two sensors in two different locations are used, such abnormalities could be detected and compensated for.

The complexity of a patch increases with the number of nodes. For source-routing approaches, the computations for finding a path will become more demanding. Also, route discovery may affect nodes negatively in terms of energy since more communication is needed in order to establish a route. Further, if a multi-hop network is implemented, more nodes would imply an increase in number of hops.

For the same reasons, sites with many different sensor patches preferably should have several base stations. This could enhance redundancy for critical sensor patches and improve on performance, such as link capacity and coverage. The drawbacks of a site with multiple base stations is increased complexity in network protocols. With two or more base stations that work in a parallel, redundant manner, routing decisions must be agreed upon between the stations, something not needed for the single-base station case.

Topology

The network topology of a measuring site is tightly coupled with its layout. One of the most fundamental design choices is whether to use a single-hop or a multi-hop network. This mainly concerns the nodes within the patches, however for large sites this may also apply to the base stations. Further choices include whether the nodes have a single connection to the base station or if they may connect to other nodes as well and if every patch has only one base station (implicitly choosing between single/multiple patches).

A classic design example of a single-hop network is a star topology. The main advantage of a such a network is that routing is trivial. Only the base station need to know what sensor to forward the data to. Further, all nodes will be only a short distance from the base station, limited by the range of its radio. The nodes also become independent of one another, since they do not need to forward traffic. This may prove important in situations where node failure is common due to extreme weather or exceptionally exposed sensor location. Bottleneck links are not an issue and less energy is spent on routing. Unfortunately, single-hop networks suffer from drawbacks as well. First, the area covered by single-hop networks become limited by the range of the radios. Second, in a very dense single-hop network congestion and collisions may appear frequently. This must be considered when scaling sensor patches. In Abisko, the coverage will pose a significant challenge and single-hop networks may only be used in a limited number of sites. These problems can be overcome by using different techniques. For example, several base stations may be used for increased coverage. This however, in turn introduces other issues discussed below. Another option, although highly impractical, is to increase the transmission power of the radios. This affects node life-time and may result in unreliable links due to interference with other nodes.

Another consideration when dealing with single-hop topologies is connectivity. Although all traffic is routed in one hop to its destination, a node may or may not have multiple connections to several other neighbor sensor nodes. This is useful when a sensor is self-calibrating, or for comparing values within a sensor patch. If this is important, than the advantages may outweigh the disadvantage of increased battery usage.

Multi-hop networks are very useful in situations where measuring stations are not centered around a base station. Such scenarios may occur when monitoring a mountain side, a ridge, a lakeside or any other area that is elongated. Multi-hop allows for more flexible layouts and present a better alternative for large-area deployments in Abisko, especially in areas where base stations may not be deployed because of regulations against installing new equipment.

Transport and network layer protocols

The transport layer concerns reliability, flow control and congestion control. For an ordinary sensor patch in the Abisko scenario, the needs for reliability are likely to be constant during an entire experiment. In wind condition monitoring, the wind speed and its direction is constantly changing, so if the experiment is interested in short term changes, perhaps over an hour with sampling every minute, an unreliable link might cause the loss of several consecutive readings. This would render the data set from the experiment incomplete. In contrast, a long-term experiment may monitor readings over several weeks. The loss of a couple of readings every day might therefor not affect the experiment outcome significantly. Without the need for variable reliability, hop-by-hop retransmissions are possible which can reduce the number of packets in the network which ultimately leads to energy savings.

For Abisko, a general approach would be to implement a protocol with variable reliability. It is the most versatile variant and it allows for sensor patches to monitor different types of variables without any major reconfiguration or reprogramming. Ironically, this also enables the possibility of reprogramming a sensor since it is possible to guarantee that a firmware image is transferred without corruption or loss. However, for patches with more long-term and stable objectives, another approach may of course be more suitable, especially if energy conservation is prioritized. As to decide upon a general approach when looking at data flows, the decisions should be based almost entirely on the intended application of each sensor patch. This way, optimizations are possible to ensure the lowest possible overhead.

6.4.4 Inter-site communication

The individual sensor nodes and the organization of sensor patches are, despite the unique environment in Abisko, problems that have been encountered in several previous projects. For instance, the Glascweb project [14] dealt with very difficult locations for their sensor nodes, submerged under the ice of a glacier while the GDI experiment [6] deployed sensor nodes in the nests of seabirds. However, these two projects had similar connections to their sensor patches. For most deployments reviewed, including the before-mentioned, a single base station was used to interface with the observing researchers. None of the projects focused on the communication between several base stations. For the Abisko scenario, this is a critical moment since the base stations may relay traffic from another station, to provide persistent connections to remote sites.

There are three key problems that these connections will have to deal with.

- Varying distances and terrain

- Several different network protocols
- Non-persistent connections

The varying distances are natural since the measuring stations are deployed in a unstructured, although not unplanned, manner over the Abisko area. Figure 4.1 marks some of the locations for the stations. For those sensor patches which have demanding requirements on availability (a persistent link is required), two options are available; increase the transmission power of the base stations (consumes more power) or deploy relay nodes (introduce another point of failure and possibly a more complex routing situation). One may argue that increasing the transmission power is a simple solution. However, under the circumstances it is very hard to predict the ratio between power and range increase. Also, once again depending on the layout of the measuring sites, a relay node may be used by several base stations for improved network throughput.

In addition to varying distances, the problem of a very non-uniform terrain (again, see figure 4.1) must be considered. This affects the conditions for radio communication. What techniques can, and should, be used is an important topic of further investigation. In order to answer this question, signal propagation and antenna technology must be reviewed for this specific scenario. However, in section 6.5, several commercially available radio communication protocols are reviewed and summarized with respect to the conditions in Abisko. Another possibility for overcoming the distances and harsh terrain is to use mobile data carriers. These can prove very powerful because they allow stations to be located far away from any other station. For example, it could be placed on a floating device in the middle of Lake Torneträsk, a location where only boats pass. However, the downside of using data carriers is a uncertain, possibly very high delay in data propagation. No guarantees of a regular visiting interval can be made, meaning such a station would have to store its data for an indefinite time, which raises the requirements for storage space and node robustness.

The introduction of mobile data carriers also introduces another problem, namely the use of several different types of network protocols. On a region-level, sites which support real-time reporting of observations must be able to co-exist with delay-tolerant sites. Integration (or separation for that matter) between these different types of network protocol paradigms must be handled gracefully. Issues such as distributing resources and prioritizing traffic may be vital for the yield of a sensor patch. For example, a site which supports a delay-tolerant application only has a limited amount of storage space. When this is nearly full, a request to upload some or all of the collected data may be issued at the next contact opportunity. However, a nearby sensor patch which strives to provide real-time observations may also be interested in this contact and, because of its frequent updates, requires considerable network resources. In this situation, a decision must be made on which data or how much of each sensor patch's data should be accepted. The delay-tolerant network layer is critical for many sites in the Abisko scenario. The previously discussed architecture Haggle, is suitable for the data collection process involving mobile data carriers and opportunistic contacts. Its publish/subscribe approach lets a Haggle node register several interests in different types of data. For example, if the age of data is included as meta-data when a sensor patch publishes its messages, another Haggle node (for example a hiker with a mobile phone running Haggle) can choose to register an interest in data that is within a certain age interval, and thereby fetch only the sensor data from the delay-tolerant sensor patch in the example above, or a lot of data from that patch and only the very latest from the patch providing real-time data. This flexibility is very important because of the very different requirements among the sensor applications.

6.4.5 Abisko globally

The global Abisko network is a high-level abstraction of all of the sensor patches within the Abisko region. For end users (a researcher interested in scientific data), this is a interface that is used for making network wide queries, to exploit the capabilities of the sensors deployed and to observe the general state of the network. This layer features one or several main servers that are not necessarily deployed in-situ. Of course, the main servers do not have any constraints on power, nor are there disruptive or unreliable network links. The servers would primarily be responsible for sensor data storage and backup. However, they may also provide services for experiment configurations, keeping track of previous configurations and experiment details. Along with these responsibilities, the servers could also monitor the overall state of the network. The servers have a lot of information about the activities in the network, and may therefor act as a fail-safe mechanism in case of failing sensors, that report infeasible readings. Of course, a set of servers that keep all sensor data may perform fusion or data mining at a minimal network cost, in order to further analyze the state of the network. The servers are also able to keep detailed information about the sensors and their formations in the network. Sensor locations, health, capabilities, utilization and more could be used for load balancing when queries are sent (see below).

In order to communicate with the base stations of the Abisko network (receiving sensor or network status data as well as distributing instructions for configurations etc.), the servers should have a persistent connection to one or preferably several static base stations which in turn serve as an interface between the base stations and the servers.

The global network layer is responsible for providing a user interface to the sensor network. Such an interface must provide secure (authenticated) and reliable access to the sensors. There must exist sophisticated management tools to allow reconfiguration and re-tasking of individual sensors, as well as sets of sensors. Of course, the most important functionality is the ability to construct advanced queries in order to extract sensor data. These queries must support properties such as time, geographical location, specific sensor readings and aggregate queries. Because of the resource constraints on the sensor network, it is important that techniques for load balancing and power preservation are implemented at all layers. For the global layer, this may include data caching and possible limitations on how often a query can be sent or the scope of the query. Queries should also be dividable, such that information that is stored in databases is fetched from the servers rather than from the sensors, while other information such as the current wind conditions, must be fetched directly from the sensor network. An example of this would be a report on the precipitation in different areas the last seven days. While the readings for the last six days may be stored at the server, the current readings for the last 24 hours may not have been reported by the sensors yet and must therefor be fetched directly from each sensor patch.

Two important aspects of the interface to the Internet and its intended users is user interface design and security. First, the sensor network is very large, offering countless of opportunities to extract and combine different data sets. However, the researchers which are the Abisko sensor network's intended users are not computer scientists, but environmental scientists. While some assumptions about general computer knowledge can be made, it is important to distinguish between these two disciplines and recall that this sensor network is primarily for the latter. Second, because the nature of the Internet, anyone may be able to access the global Abisko network interface. In order to keep unauthorized visitors from altering or possibly sabotaging experiments and their configuration, as well as accessing sensor network data, great concerns must be taken when designing the authentication system that handles access privileges. It is also a most likely requirement that researchers should not be able to access the data or alter configurations of experiments not currently owned by themselves.

6.5 Radio technology

The Abisko network spans a large area, partially in a populated area. Thus, cellular networks are a feasible choice for long-range communication. Unfortunately, the entire area is not covered by cellular networks which raises a demand for other wireless technologies. In order to decide upon a technology, several parameters have to be considered. These include,

- Infrastructure - is there existing infrastructure or does the technology need new equipment installed?
- Signal coverage - What is the transmission range and how do external factors such as weather and the geographical environment affect this?
- Data rates - what data rates are achievable with the technology? Is it sufficient for the applications' needs?
- Interference - does the radio equipment introduce interference with existing equipment, such as sensors?
- Energy consumption - how much power is needed to obtain sufficient signal strength?
- Cost - what is the cost of the equipment? (Although important, especially in large deployments with many units, this is not within scope of this report and is therefor left out of the discussion below.)

Existing infrastructure concerns whether existing technologies, such as GSM or UMTS (3G) are available at the location. Although cellular networks are very widespread in

Sweden, there still exists areas without coverage. (A map of the coverage in Abisko is provided in figure 6.4.) In these areas, other techniques such as low-frequency radio[8] may be used. However, the use of such frequencies is restricted by the government and might require additional permits and registrations. Also, transmission over lower frequencies require bigger antennas and presumably more expensive radio equipment.

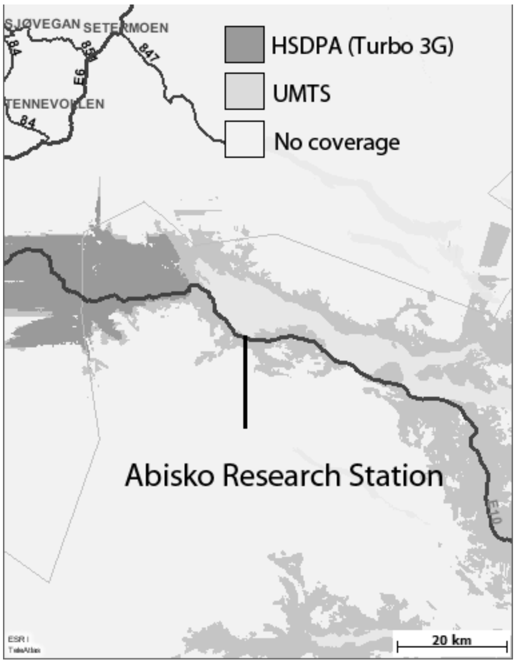

Figure 6.4: Cell phone coverage in and around Abisko [33].

Signal coverage affects the connectivity. However, because of recent development of delay-tolerant networks, a persistent connection is not always a requirement. The signal coverage is also, depending on the technology, affected by the geographical environment. Some high-frequency technologies may be interfered by weather conditions and the topology in the area. These factors are very much present in the Abisko scenario because of the relatively high mountains and periods of harsh weather conditions. Also, when deploying a sensor network in a valley, appropriate measurements must be made in order to make sure that sufficient antennas are used to propagate the signal to its destination. If the signal must traverse mountains, repeaters may be needed.

Data rates within the network will affect the Quality of Service. Data rates may vary extremely between applications; a monitor application may have a low but stable flow of data while a event-driven application has a high but infrequent flow. If measurements are conducted over a long period, large amounts of data may be collected. Transferring this over a low-capacity network might not be possible at all if the link is not available during a long period of time. If mobile data carriers are used, as in a scenario with a

[8]Frequencies between 30 and 300 kHz.

DTN network, the amount of data that can be transmitted simultaneously is limited by the storage capacity of the mobile device and the contact time at each end point.

Interference might occur as with any radio equipment. Precautions must be taken in order to guarantee that the existing equipment and sensors are not interfered, resulting in incorrect or inaccurate data. Interference may be reduced by using low-power transmission devices.

Energy consumption of course affects the lifetime of sensor nodes. However, it may also affect the range of the radio signal depending on how much power is used during transmission. In Abisko, several sites have external power supplies. However, a large set of measuring stations rely on battery power. This has been discussed in section 6.2.

6.5.1 Radio standards

Within the monitored areas, the spread of the measuring stations range from a few meters to hundreds or maybe thousands of meters. Under these conditions, in addition to the planned usage for the network connections, it seems more than reasonable that the type of radio transceivers used for the different parts of the network should be chosen with respect to their location and application.

Low-range

In the direct vicinity of the measuring stations, low-range, license-free technologies such as WiFi (802.11) or 802.15.x are a reasonable choice. 802.11 has become extremely popular in WLAN environments, it is easy to set up and offers low delays and relatively high data rates. Unfortunately, compared to 802.15.x protocols such as ZigBee and Bluetooth, it is not energy efficient making it unsuitable for very low-power devices, such as sensor nodes. However, 802.11 may very well serve a purpose in a powered gateway node were multiple data streams for many sensors are aggregated and relayed to a remote server. Bluetooth's advantages lies in its infrastructure-less operation, fairly high data rate and cheap hardware. Also, it may operate in low-power modes. It uses at most 100 mW but can operate at only 1 mW. ZigBee, based on the IEEE 802.15.4-2006 standard, is another ultra-low power protocol. It has gained attention in the WSN community and it is used in several commercial sensor node products. The radio units, especially their antennas, are very small and compact. This is another advantage which makes these technologies suitable in small sensor nodes and measuring stations.

Mid-range

The mid-range transmissions mainly concern links between measuring stations or sites. Distances typically range from hundred meters (possibly in obstructed terrain) up to some kilometers. At these ranges, battery powered stations become a limitation because of the power versus lifetime trade-off, therefor external power is preferred. However, this does not necessarily require a fixed power infrastructure, solar cells or a wind power

Name	Range(unit)/ Coverage	Infrastructure	Typical hardware used	Application	Limitations
GSM	See figure 6.4	Yes, commercial	Mobile phone	Calls, text messages	Additional costs
UMTS (3G)	See figure 6.4	Yes, commercial	Mobile phone, USB-interface	Calls, text messages, generic data transfers	Additional costs
LTE (4G)	N/A[a]	Yes, commercial	Mobile phone, USB-interface	Calls, text messages, generic data transfers	Additional costs
Satellite	Kilometers	Yes, commercial	Satellite dish, modem	Generic data transfers	Power, additional costs
WiMAX	N/A[b]	Yes, commercial	Nodes, base stations	Generic data transfers	Additional costs
802.11a/b/g/n (WiFi)	Meters	Yes, private	Nodes, gateways	Generic data transfers	
802.15.4-2006 (e.g. ZigBee)	Meters	No	Nodes, gateways	Generic, low-rate data transfers	
802.15.1-2005 (Bluetooth)	Meters	No	USB-interface	Generic data transfers	
Unlicensed frequencies	Kilometers	No	Standard radio transceivers	Generic data transfers	Transmission power limited by regulations

Table 6.1: A list of available radio standards for the Abisko scenario.

[a] LTE is at the time of writing only available in Stockholm, Sweden [34].
[b] WiMax is at the time of writing not available in Abisko.

generator would be sufficient. Techniques such as WiFi fall short in range for these mid-range links. Instead, recent techniques such as WiMAX which may allow communication over several kilometers may serve as an alternative [35]. Although, while WiMAX is a technology in development, widespread unlicensed frequencies such as 868-870 MHz may be used instead[9]. As the next section will show, mid-range technologies may be one of very few viable solutions in order to connect the most remotely located stations to the network.

Long-range

Long-range transmissions are somewhat more complicated. Available technologies use licensed frequencies meaning that regulations apply and special permits are needed. In practice, it is impossible to buy a license for these frequencies. Instead, it is common to rely on cellular networks and/or satellite links in order to communicate over long distances. Satellites offer wide area coverage. A satellite broadband customer typically uses one certain satellite system, although many different exist [36]. Satellite links suffer from relatively high delays, although the connection speeds are fairly good, ranging from tenths of kbps up to several Mbps. A major disadvantage for satellite communication is the need for the very well-known, and obtrusive, satellite dish. As discussed in section 4.2, several of the measuring stations are located in areas where installation of equipment such as satellite dishes is prohibited or not even possible.

UMTS has lately become very wide-spread in Sweden. The coverage offered by TeliaSonera in Sweden can be seen in figure 6.4. Due to huge efforts in expanding the 3G network recent years, the 3G coverage has exceeded that of GSM. In Abisko, GSM/3G coverage is mostly available along the main highway, E10. However, no cellular networks at all are available in the mountains south-west of Abisko.

Summary

This report has given only a brief introduction to the wireless radio techniques available for the Abisko scenario. However, the topic is very complex because many different parameters must be considered for choosing the appropriate technique for each location and application. Besides the practical issues of coverage, performance and availability, other issues such as cost and customization must be considered aswell. Because of the complexity, a thorough analysis and evaluation of wireless transmissions techniques are recommended, preferably in an environment similar to that of Abisko.

[9] National regulations apply as to which frequencies are license free. This specific range is unlicensed in Sweden.

Chapter 7

Measuring stations

This chapter briefly reviews the situation of existing measuring stations, the hardware used and the capabilities it offers. Also, points of improvement of the stations are discussed, introducing state of the art sensor nodes that may replace legacy hardware and extend the capabilities and performance of the measuring stations. Desired features are also discussed along with their requirements on the equipment.

7.1 Existing hardware

Currently, the measuring stations are a composite of several different units. Generally, the units include the actual sensors and their controllers, the data loggers used for storage and the power supplies for the station. The equipment is installed in a casing of varying design. An example is given in figure 7.1a which shows the container for one station measuring meteorological variables, and another monitoring precipitation chemistry (figure 7.1b). However, the design and operation of the stations vary as there, until recently, have existed no guidelines as to how the stations must be designed. Current design guidelines ensure that the stations must have a serial interface to allow a connection to a computer.

Some stations use legacy hardware for sensing. Several instruments, one monitoring the water level of Lake Torneträsk, still record sensor readings on a paper strip (see figure 7.2). It is a slow, impractical and unreliable process to extract data from such a station. Modern stations have different interfaces, including serial connections and memory card readers. The data loggers used are not necessarily fixed to a measuring station and it is therefor not possible to thoroughly describe all interfaces used.

Despite the rather discouraging situation with legacy hardware, some highly modern stations exist as well. They are equipped with continuous power supplies, network connections and modern interfaces. However, these stations may not be accessible to the general public as they are administrated by other organizations, such as the Swedish Meteorological and Hydrological Institute (SMHI).

Apart from the obvious lack of a network connection, existing hardware introduces a number of limitations in the system. Energy consumption is one of the most important.

(a) A weather station (b) Precipitation chemistry

Figure 7.1: Examples of measuring stations in Abisko (Images by Abisko Scientific Research Station).

Current equipment is not very energy efficient, draining batteries in only a few days. This makes maintenance visits necessary in order to recharge or change batteries. As stated in section 4.3, this might not always be possible. Another limitation is the size of a station. Existing hardware takes up a lot of space and is obtrusive in areas where vegetation and wildlife is very sensitive. Additionally, large areas around Abisko belong to nature reserves and a national park where installation of equipment is regulated.

7.2 Measuring stations redesigned

A modern measuring station should take the problems and limitations above in consideration while offering enough capabilities for future needs. The functionality of a measuring station is determined by its hardware. At a minimum, this includes an extremely energy efficient CPU, enough storage for caching sensor readings in case of a disrupted network link, a radio transceiver and batteries for at least several weeks of operation. Of course, one or many sensors are included either onboard or through

Figure 7.2: Sensor readings recorded on a paper strip (Image by Abisko Scientific Research Station).

external connectors. However, additional hardware may be wanted, such as a GPS, a webcam (which could be considered as another sensor), a power generator (wind or solar power), several other wireless or wired interfaces, larger Flash-based storage and custom antennas for optimized radio communication.

Electronic equipment is of course sensitive and must be protected by a robust, weather proof and shock proof casing. Still, the sensors and antennas must be exposed to the outside in order to operate properly and to provide accurate and reliable information. Also, the casing must be as unobtrusive as possible, meaning that size constraints apply, and possibly also aesthetics.

7.2.1 Motes

Recent development has produced a variety of different embedded systems that have been customized for use in WSNs. These units are commonly known as Motes and provide many of the features desired for the measuring stations in Abisko. Wireless sensor network nodes typically feature three very characterizing features; they are physically small, they have limited resources but they are still almost full-featured embedded systems. Motes that are publicly available and used in previous WSN research deployments include the now discontinued Tmote family [37] and Crossbow's MICA2, MICAz, and TelosB nodes [38]. The motes typically feature a 4 or 8 MHz processor with 10-128 kB RAM and 512 kB to 1 MB Flash memory for data logging. I/O connections include USB, UART serial interface or I2C/SPI digital interfaces. A significant feature is the use of a 2.4 GHz radio transceiver, supporting the 802.15.4 protocol. Integrated sensors on the motes sense light, humidity and temperature.

Motes are typically only 5-6 cm long and about 3 cm wide. The majority of the size is made up by a battery compartment for two AA-type batteries. The energy consumption is one of the most challenging limitations of the motes. In real-life deployments, they have proven to be able to operate properly for at least a month without exhausting their batteries [6, 7]. During operation, the motes have sampled their sensors in an interval of minutes, and then transmitted the collected data to a master node for permanent storage in a database.

7.2.2 Limitations and customizations

As discussed in chapter 5, the protection of the motes against external factors has proven to be difficult. The extreme conditions of Abisko will certainly pose a problem and may call for customized, well-thought through and more robust case designs. Also, because of the potentially long time between maintenance visits, external power should be considered as a necessity, at least for base station nodes.

While motes provide a decent set of standard hardware, additional features in Abisko include a GPS and several wireless interfaces. The GPS may be shared between several nodes and may therefor not be needed at every node. However, all nodes must be accessible through another interface to allow mobile data carriers to extract data. Also, the storage space of a mote is limited and additional storage space (at least tens of Megabytes is necessary to support high frequency sampling during experiments if no network link is available.)

Chapter 8

Conclusions

When summarizing the Abisko scenario, three significant features can be identified. These are the size of the network, the geographical properties in Abisko and the wide range of technology needed for this scenario.

8.1 Network size

The size of the network concerns not only the physical spread, but also the the number of sensors needed to cover the area. Abisko is a very active research station and with a network that enables communication with the measuring stations, it will surely not decrease in popularity. The network designed for Abisko must be able to support and handle tens of research sites and far beyond a hundred individual sensors. Scaling is an implicit requirement, not all stations will be active simultaneously and during winter almost no researchers currently visit Abisko, however this might be subject to change if maintenance intervals can be reduced. The network architecture must be very modular to allow seamless deployment of new measuring stations, as well as coping with failing or phased out stations. The deployment will not happen all at once, therefor careful planning for gradually increased coverage is needed, as well as monitoring of the network when it is expanded in order to find bottleneck links as similar unwanted phenomenas.

The number of sensors also hint about the wide range of applications possible at Abisko. While this report has continuously regarded that of meteorology, and in some cases avalanche control, there exists almost countless of possible environmental monitoring applications that have very different needs in terms of availability, reliability and performance. Along with all of these applications comes another important factor namely the end users, the researchers, that make use of the sensors and that will have great use of the network. Their requirements must be included in the requirement elicitation phase.

8.2 Geographical properties

The conditions at Abisko and the implications of its location are very significant for this project. Its subarctic climate in combination the varying landscape creates a unique and challenging environment for a wireless sensor network. This uniqueness also happens to be the main motivation for the research conducted in Abisko. The exceptionally harsh weather conditions during winter affects the hardware and the equipment must be thoroughly protected against it. Custom made casings and structures are likely to be needed in some locations. The weather also affects the locations of measuring stations because of accessibility and exposure to dangerous areas, such as slopes prone to produce avalanches and mud slides. Unfortunately, this is further complicated by the fact that there exists several nature reserves and a national park in the area. These reserves are regulated as to what equipment is allowed to be installed. This may affect the design of the measuring stations, as well as to what radio technology may be used for communication.

The landscape, especially the mountain area which features mountains up to almost 2000 meters is not an ideal environment for radio communication. Signal wave propagation will become a challenge that must be overcome. However, in certain areas where this is impossible, or where the measures that have to be taken for this are infeasible, network techniques such as delay-tolerant networking with mobile data carriers can be utilized.

8.3 Versatile technology

The Abisko network will need to include many different techniques in order to offer the functionality needed by its applications. Regarding the network connections, a foundation based on WSNs is the most appropriate choice since this is the primary use of the network. However, there exists many different protocol implementations depending on what features are prioritized. Therefor, the choice of protocols may be individual for each region or even each sensor patch in order to take full advantage of the sensor networks. The use of WSNs will not suffice in certain situations, for example in areas where network connectivity is sporadic. In these areas, DTNs may be used instead.

Additionally, support for a combination of temporary in-network storage as well as permanent and redundant centralized storage is also recommended. Data loss may render a several month long experiment wasted, and it is not uncommon in WSNs, primarily due to node failures.

A great challenge lies within the fact that the network nodes range from tiny, individual sensor nodes up to the centralized servers that interface to the Internet and offer storage and security. It is therefor intuitive to separate the Abisko network into a multi-tier architecture where each layer has a clear responsibility.

Chapter 9

Future Work

This chapter discusses some of the recommended directions and areas that need attention in order to specify, design and ultimately deploy a successful delay-tolerant wireless sensor network.

9.1 Inventory

The Abisko scientific research station is a fully operational research site with a lot of existing equipment. Rather than replacing all existing components, a scenario which is unfeasible and perhaps even impossible, the new equipment (meaning that that enables network connectivity) must co-exist with previously installations. Therefor, it is necessary to thoroughly examine all the stations that are to be connected to the network. Some of the most interesting parameters include what computer interfaces exist, what is the current status of the station as to utilization, health and required maintenance interval? What is the lifetime of the station (if battery powered)? The properties of the sensor data is also of great interest; what sample rates are used? How often is the data collected from the station? What is the accuracy of the sensors? Without this information, it is very hard to plan and design interfaces and components with appropriate dimensions.

9.2 Requirement elicitation

This is perhaps the most important and the most comprehensive part of the future work needed before designing the network architecture for Abisko. The requirements form the foundation of the design and they include both functional and non-functional requirements. Some requirements may be elicited with the information gained from the inventory above, however most will require detailed analysis of the past, current and future applications of the measuring stations and their users, as well as the operating environment.

9.3 Abisko condition analysis

The weather conditions and the challenging environment in Abisko requires detailed studies within several domains. A detailed study of the radio communication environment is most likely needed. Signal propagation is heavily affected by the geography in the area which varies a lot. Many measuring stations are deployed near the research station's main site where the terrain is relatively flat and unobstructed. On the opposite, measuring stations are also deployed in the mountains and in the valleys, an environment ill-suited for wireless communication. The most challenging locations may require special radio equipment, custom antennas or the use of relay nodes in order to enable link connectivity.

Of course, the same contradictory conditions apply to the rest of the hardware used for the stations. Hardware components such as the main board with its CPU, memory, interfaces, sensors, power supplies and peripherals must be protected against humidity, precipitation, external force, sub-zero temperatures among many other destructive factors.

9.4 Prototyping

When the requirements have been established, it is possible to start evaluating different components and subsystems for use in the network. There are many commercially available hardware components that may suit the scenario, however it is necessary to evaluate if they fulfill the requirements or if they may be modified to do so. Previous research projects have already broken important ground in terms of finding robust solutions that have been tested in real-life scenarios.

The Abisko scenario features unique conditions and therefor, it is important to test components in-situ, as opposed to simulations. Prototyping is a very effective development method and should be considered for all hardware components.

Bibliography

[1] The Royal Swedish Academy Of Sciences, “Abisko Scientific Research Station.” `http://www.linnea.com/~ans/weather/obs1.html`, December 2009.

[2] SCANNET, “SCANNET.” `http://www.scannet.nu/`, March 2010.

[3] Länsstyrelsen i Norrbottens Län, “Abiskoögat - med fokus på klimat.” `http://www.linnea.com/~ans/abiskoogat/Om_Abisko.html`, December 2009.

[4] Google and Tele Atlas, “Map of terrain surrounding Abisko.” `http://maps.google.se/?ie=UTF8&ll=68.297842,18.829193&spn=0.358523,1.392517&t=p&z=10`, March 2010.

[5] J. D. Lundquist, D. R. Cayan, and M. D. Dettinger, “Meteorology and Hydrology in Yosemite National Park: A Sensor Network Application,” in *Sensor Network Application, Information Processing in Sensor Networks*, pp. 518–528, 2003.

[6] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, and J. Anderson, “Wireless Sensor Networks for Habitat Monitoring,” in *Proceedings of the 1st ACM international workshop on Wireless Sensor Networks and applications*, pp. 88–97, 2002.

[7] G. Tolle, J. Polastre, R. Szewczyk, D. Culler, N. Turner, K. Tu, S. Burgess, T. Dawson, P. Buonadonna, D. Gay, and W. Hong, “A Macroscope in the Redwoods,” in *Proceedings of the 3rd international conference on Embedded Networked Sensor Systems*, pp. 51–63, 2005.

[8] M. Demirbas, K. Y. Chow, and C. S. Wan, “INSIGHT: Internet-Sensor Integration for Habitat Monitoring,” in *Proceedings of the 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks*, 2006.

[9] G. Werner-Allen, K. Lorincz, M. Welsh, O. Marcillo, J. Johnson, M. Ruiz, and J. Lees, “Deploying a Wireless Sensor Network on an Active Volcano,” in *IEEE Internet Computing*, pp. 18–25, 2006.

[10] L. Selavo and A. Wood, “LUSTER: Wireless sensor Network for Environmental Research,” in *Proceedings of the 5th international conference on Embedded Networked Sensor Systems*, pp. 103–116, 2007.

[11] K. Martinez, P. Padhy, A. Elsaify, G. Zou, A. Riddoch, J. K. Hart, and H. L. R. Ong, “Deploying a Sensor Network in an Extreme Environment,” in *Proceedings of Sensor Networks, Ubiquitous and Trustworthy Computing*, pp. 186–193, 2006.

[12] R. Szewczyk, J. Polastre, A. Mainwaring, and D. Culler, “Lessons from a Sensor Network Expedition,” in *In Proceedings of the First European Workshop on Sensor Networks (EWSN)*, pp. 307–322, 2004.

[13] IEEE P802.15 Working Group, “IEEE Std 802.15.4-2006,” tech. rep., IEEE Computer Society, 2006.

[14] K. Martinez, J. K. Hart, and R. Ong, “Glacsweb: a Sensor Network for Hostile Environments,” in *Proceedings of The First IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks*, 2004.

[15] S. Burleigh, A. Hooke, L. Torgerson, K. Fall, V. Cerf, B. Durst, K. Scott, and H. Weiss, “Delay-Tolerant Networking: An Approach to Interplanetary Internet,” *IEEE Communications Magazine*, pp. 128–136, 2003.

[16] X. Wang, G. Xing, Y. Zhang, C. Lu, R. Pless, and C. Gill, “Integrated Coverage and Connectivity Configuration in Wireless Sensor Networks,” in *SenSys ’03: Proceedings of the 1st international conference on Embedded networked sensor systems*, pp. 28–39, 2003.

[17] Y. G. Iyer, S. Gandham, and S. Venkatesan, “STCP: a generic transport layer protocol for wireless sensor networks,” in *Computer Communications and Networks, 2005. ICCCN 2005. Proceedings. 14th International Conference on*, pp. 449–454, 2005.

[18] Y. Zhou, M. R. Lyu, J. Liu, and H. Wang, “PORT: A price-oriented reliable transport protocol for wireless sensor networks,” in *In International Symposium on Software Reliability Engineering (ISSRE*, pp. 117–126, 2005.

[19] Y. Sankarasubramaniam, O. B. Akan, and I. F. Akyildiz, “ESRT: Event-to-Sink Reliable Transport in Wireless Sensor Networks,” pp. 177–188, 2003.

[20] C. Wan, A. T. Campbell, and L. Krishnamurthy, “PSFQ: A Reliable Transport Protocol For Wireless Sensor Networks,” in *WSNA ’02: Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*, pp. 1–11, ACM Press, 2002.

[21] J. Kulik, W. Rabiner, and H. Balakrishnan, “Adaptive Protocols for Information Dissemination in Wireless Sensor Networks,” pp. 174–185, 1999.

[22] C. Intanagonwiwat, R. Govindan, and D. Estrin, “Directed Diffusion: A scalable and robust communication paradigm for sensor networks,” pp. 56–67, 2000.

[23] M. Younis, M. Youssef, and K. Arisha, "Energy-aware routing in cluster-based sensor networks," in *In Proc. 10th IEEE/ACM International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems*, pp. 129–136, 2002.

[24] Y. Yu, R. Govindan, and D. Estrin, "Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks," tech. rep., 2001.

[25] V. Cerf, S. Burleigh, A. Hooke, L. Torgeson, R. Durst, K. Scott, K. Fall, and H. Weiss, "Delay-tolerant network architecture," in *Internet draft: draft-irrf-dtnrg-arch.txt*, DTN Research Group, 2006.

[26] J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach (4th Edition)*, ch. 3 Transport Layer. Addison-Wesley, 2008.

[27] F. Warthman, "Delay-Tolerant Networks (DTNs) - A Tutorial," tech. rep., Warthman Associates, 2003.

[28] E. P. Jones and P. A. Ward, "Routing strategies for delay-tolerant networks," *Submitted to ACM Computer Communication Review (CCR)*, 2006.

[29] K. A. Harras, K. C. Almeroth, and E. M. Belding-Royer, "Delay tolerant mobile networks (dtmns): Controlled flooding in sparse mobile networks," *Lecture Notes in Computer Science*, vol. 3462, pp. 1180–1192, 2005.

[30] S. Jain, K. Fall, and R. Patra, "Routing in a delay tolerant network," *SIGCOMM Comput. Commun. Rev.*, vol. 34, pp. 145–158, 2004.

[31] Haggle Project, "The Haggle Project." `http://www.haggleproject.org`, January 2010.

[32] J. Scott, J. Crowcroft, P. Hui, and C. Diot, "Haggle: a Networking Architecture Designed Around Mobile Users," in *Proceedings of the Third Annual Conference on Wireless On-demand Network Systems and Services*, pp. 78–86, 2006.

[33] TeliaSonera and Tele Atlas, "Mobile phone coverage in Sweden." `http://www.telia.se/privat/produkter_tjanster/mobilt/tackningskartor/tackningskartahomerun`, March 2010.

[34] TeliaSonera, "Om 4G." `http://www.telia4g.se/om-4g`, March 2010.

[35] WiMAX.com, "What is the range of wimax?." `http://www.wimax.com/education/faq/faq31`, January 2010.

[36] J. Farserotu and R. Prasad, "A Survey of Future Broadband Multimedia Satellite Systems, Issues and Trends," *IEEE Communications Magazine*, pp. 128–133, 2000.

[37] Sentilla Corporation, "Moteiv Tmote hardware documentation." `http://www.sentilla.com/moteiv-transition.html`, December 2009.

[38] Crossbow Technology, "Crossbow Wireless Module Portfolio." http://www.xbow.com/Products/productdetails.aspx?sid=156, December 2009.