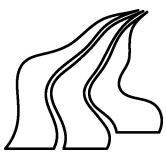
Remote Access for a Wireless System

– User-to-tractor access as a use case

DAT5, Fall 2007.

Anthony Buron
Nicolas Cothereau
Guillaume Delaite
Jacob Eskildsen
Edouard Gourdin
Olivier Monsonego
Faith Oziofu Ogini Nielsen
Elisa Oteo Ovejero



Aalborg University
Department of Computer Science

Aalborg University
Department of Computer Science

TITLE:
Remote Access for a Wireless System
– User-to-tractor access as a use case

THEME:
Distributed Systems and Semantics

PROJECT PERIOD:
01/09/2007-02/01/2008

PROJECT GROUP:
d505a, d506a

GROUP MEMBERS:
Anthony Buron
Nicolas Cothereau
Guillaume Delaite
Jacob Eskildsen
Edouard Gourdin
Olivier Monsonego
Faith Oziofu Ogini Nielsen
Elisa Oteo Ovejero

SUPERVISOR:
Alexandre David

SYNOPSIS:

In this project we implement a system for Lykketronic to provide automatic switching between two complementary networks, namely GPRS and Wi-Fi based upon network availability and cost. Also, we present an implementation of a proxy server, that provides transparent access to agricultural machinery via a login, with access privileges and also provides security, so that only authorized personel can access the data or remote control the machinery.

NUMBER OF COPIES: 6

NUMBER OF PAGES: 56

CONCLUDED: 02/01-2008

This report is a result of the work done in the Dat5 semester of the Cand.Scient study at Department of Computer Science, Aalborg University. This project was done in the research area of Distributed Systems and Semantics and constitutes the complete work towards a master thesis.

We would like to thank our supervisor Alexandre David for supervising this project and the many helpful comments made throughout the project.

This thesis has been revised on 2nd of January, 2008. Some corrections and changes were made to the published edition.

Anthony Buron	Nicolas Cothereau
Guillaume Delaite	Jacob Eskildsen
Edouard Gourdin	Olivier Monsonego
Faith Oziofu Ogini Nielsen	Elisa Oteo Ovejero

Summary

This report presents a solution to access data from a remote mobile device. We provide a solution that is organized around a Proxy. This Proxy will give the user transparent access to a mobile device through the Internet. The remote device will be able to access the Internet through two possible connections, GPRS and Wi-Fi, and will be able to switch between those connections for the user to provide the best bandwidth and cheapest connection. We also provide some test scenarios and experimental results to show that our solution is working and satisfies the requirements.

Contents

Chapter 1

Introduction

This report proposes a solution to remotely access data located on some farming machinery, via a proxy. That is, the user which can be located anywhere in the world, logs into the proxy server via the internet, and thereby transparently gains access to the local data that reside on the web-server of the farming-machinery. First, there will be a brief introduction to the subject, secondly a number of viable wireless technologies that can support the requirements of the users (all-around access, and cheapest possible access) will be introduced. Thirdly, the design decisions and specifications will be described, and finally, a description of the implementation details, and some experimental results gained from using the implementation described.

1.1 Problem Statement

In the ideal world every farmer or service technician should be able to access any farming machinery remotely, not only to read out data, and add other users to access the system, but also to operate and control the machinery remotely, and for the speculative future, even have nano-probes automatically repairing systems in real time, or before flaws even occur.

However, flawless transparent access does not exists at the moment, that allows users to read and write data directly to the agricultural machinery, nor does it allow transparent remote control of the machinery. Currently it only allows users to directly interact with the machinery. No remote control is possible at the moment, nor is any remote access of the data collected.

The project detailed here is proposing to allow remote control and access to read and write data on the computer (the Black-box or just BB) placed locally on the agricultural machinery (e.g. a tractor).

The problem statement of this report is a real-world problem proposed by SKOV [Sko07] – a company that produces electronic systems for Tractors and Machineries for agriculture and forestry following the ISO 11783 [SMFB99] standard. The ISO 11783 standard provides an open, intercon-

nected system for on-board electronic systems. It is intended to enable the Electronic Control Units (ECUs) mounted on a machine to communicate with each other, providing a standardized system.

A serial data network when mounted on a forestry or agricultural machinery(here the machinery is usually a tractor) will allow the transfer of data between the sensors, actuators, control elements, information storage and display units. *Task data* can be collected from the system's CANBUS [RB97] and can be used for *task management* or *task control*. The system consists of a Task Management System and a Task Control System.

Here is a scheme which provides a description of the system given by LYKKETRONIC [Lyk07]:

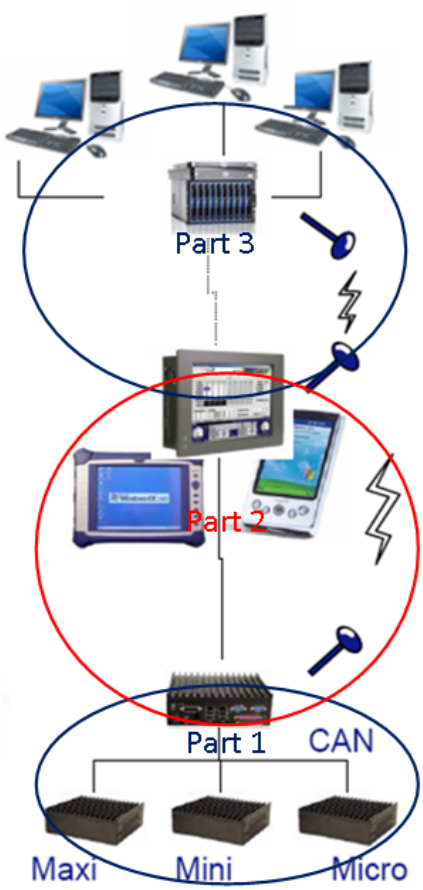


Figure 1.1: Global system from LYKKETRONIC

The system consists of three parts; 1, 2, and 3, as seen in Figure 1.1.

Part 1 consists of the web server – the Black Box – and the three job computers connected through a CANBUS interface, this represents what we can call a mobile device – in this particular example, it is a tractor. As this part is well known by the the company LYKKETRONIC, it is implied that no changes should occur here.

Part 2 of the system consists of mobile devices connected to the Black Box through any kind of connection, and this is the primary focus of the solution.

Part 3 consists of mobile devices connected to fixed devices such as desktop computers or databases, this area is not covered by this project, because mobile devices can easily communicate with fixed devices with known solutions (such as WI-FI-routers, etc).

1.1.1 Task Management System

The purpose of the task management system is for the management of resources like tractors, sensor systems, workers and the products used. It is also for the management of farm activities carried out in the field – these activities are described according to the work that is planned or has been done by the farmer or by a contractor for the customer in one area.

1.1.2 Task Control System

The task control system interacts with a task controller via a *virtual terminal* or an *interface*. This interface can range from very simple to advanced, depending on the designer's intent. For the existing system, a touch screen terminal is connected directly to it.

Through this interface, the operator is able to select and execute a *task*, get *time* and *GPS position data* or *events* that occurred during task processing. Through the terminal, it is also possible to access data log or specific events that should occur in order to ensure proper initialization of the task controller. It can also be used to get current task status or get access to data when the tasks are completed.

1.1.3 Problem Definition - A Statement of current system specific problems

The process of controlling and managing tasks is carried out by reading data directly from the black box (the computer located on the tractor) where the web server is located via this terminal. This system is impractical for use for

a contractor or a service operator, who is located far from where the tractor is operating.

Depending on the category of personnel that need to access data on the web server. Under the assumption that the person in question is a technician, the person will be required to travel to the location where a particular tractor is in operation in order to read or modify the local data or carry out repairs, and in some cases such farm equipment may be located hundreds or even thousands of kilometers away.

Thus, LYKKETRONIC wants to add a functionality to their system, which is the ability to remotely access the data stored on a tractor from anywhere.

1.2 Goal

The goal of the project is to propose an implementation for accessing data on a mobile device. The report will provide a detailed system design prototype for LYKKETRONIC that will work in unison with the already existing system.

We will extract data from this system and send it to a user anywhere in the world. The solution we propose consists of an automatic switching between different wireless networks and an implementation of a proxy server. In fact, this solution will allow us to provide a uniform means of accessing different mobile devices. A concrete example is that we will be allowed to access different farms and in turn, many different tractors on each farm.

Concerning the transmission part, we present an overview of the main wireless technologies to use with those mobile devices. In fact, we chose to use only two of them because of the requirements from LYKKETRONIC. The idea is that these wireless technologies are basically ways to access the mobile devices, you can decide choose the one which fits your requirement best.

In this report, we describe a prototype that will allow us to access the data in the web server. This can be achieved by making remote connections, where we will use some standard wireless technologies – GPRS and WI-FI.

Adding this functionality to the existing system will not only allow us to access the data in the web server but it will also allow us to be able to dynamically switch between the two networks. The switching ability is not only necessary but it is a requirement from LYKKETRONIC. This is because due to the mobility of the tractor, the black box may experience some operational instability or it may loose connection when it moves outside

its Wi-Fi range, but such connection loss must not prevent access to the Black Box. Also, when within range of both connections, that is, if both connections are available, our preferred connection should be the Wi-Fi connection, this is also a requirement from Lykketronic.

1.3 The Structure of the Report

The rest of the report is organized as follows:

Chapter 2: Preliminaries Gives a short overview of the main wireless technologies that can be used in the project.

Chapter 3: Analysis A short listing of requirements, constraints, and possible solutions.

Chapter 4: Design Describes the chosen architecture.

Chapter 5: Implementation Describes how we implemented this architecture with technical details.

Chapter 6: Testing and Experiments Describes some testing scenario and experiments that were carried out.

Chapter 7: Improvements Describes some possible improvements using future technologies.

Chapter 8: Conclusion and future work Concludes this report where we also specify some possible future work.

Chapter 2

Preliminaries

The aim of this chapter is to provide an overview of the wireless technologies which were considered. With this overview, it will be possible select a number of appropriate technologies in accordance with the system requirements. This is to convey that, depending on different requirements, adaption of other wireless technologies are possible.

2.1 Main Wireless Technologies

The following section presents an overview of the wireless technologies that is in common use throughout the world. In addition to these technologies, we have also considered communication between a web server in a mobile device and a user anywhere in the world.

As the requirements have set forth, we need to consider price, connection speed and the distance from the agricultural machinery to the farm, thus, we will now list the different technologies according to range, in two main areas, namely short/medium range, and long range:

2.1.1 Short and Medium Range

Bluetooth: [Wik07a] is an open standard for data and voice transmission between mobile devices such as cell phones, PDAs, laptops, desktop computers, etc. It uses omnidirectional radio waves which can go through walls and non-metallic obstacles. A secure Bluetooth connection requires authorization and authentication before accepting data from an unknown device. As with short range connections, it can only cover relatively short distances of about a few meters (see Fig.2.1). Some of the limitations above prevent us from choosing this technology. Firstly, the metal in the tractor and black box can cause an

obstruction in the transmission from the black box. Secondly, the distance between the black box and the user may be far apart and can thus prevent the possibility of establishing a connection.

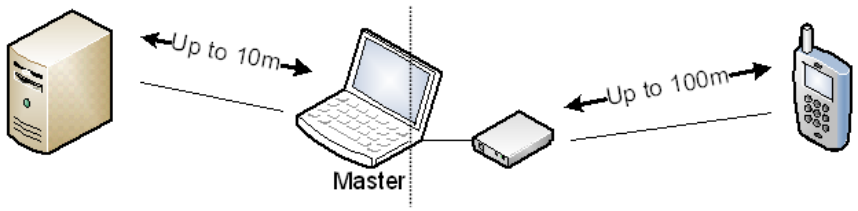


Figure 2.1: Bluetooth Design

ZigBee: Unlike bluetooth, ZigBee [Wik07g] [Zig07] devices have the ability to form a mesh network between nodes. Its transmission range is about 100 meters. ZigBee networks provide smart, low-cost, low-power, low-maintenance monitoring and control systems. These can vary greatly depending on certain constraints like temperature, humidity or extreme environmental conditions which can result in low data transmission or failure. As a result of some of the constraints stated above, we are prevented from choosing this technology firstly because of its low data rate. Secondly, because adding security in a resource constrained network with minimum overhead provides significant challenges and this is still an ongoing area of research.

Wireless USB and Firewire: Firewire is often used for devices that require real-time operations such as audio and video systems, and it is also used frequently in storage area networks. USB can connect more devices (up to 127) than firewire, and the USB 2.0 standard supports speed of up to 480Mbps, and this makes it more competitive with Firewire. Because, both technologies are similar to Wi-Fi and have lower range (around $\frac{1}{10}$) compared to Wi-Fi, neither of them will be used.

Wi-Fi: refers to any system that uses the 802.11 standard. It uses radio waves and can transmit and receive radio waves. PDAs, laptops, or cellphones are designed to be Wi-Fi-compatible. This technology enables devices such as laptops, cellphones or PDAs to connect to the Internet when within the range of a wireless network.

Wi-Fi also allows connectivity in peer-to-peer (wireless ad-hoc network) mode, which enables devices to connect directly with each other.

This connectivity mode is useful in consumer electronics. Devices supporting Wi-Fi can be connected in ad-hoc mode for client-to-client connections without a router.

Nowadays, it is one of the wireless network technology commonly in use mostly when computers are involved. Moreover, the high range (around 100 meters)and the high bandwidth (between 11 and 100 Mb/s) makes this network a good one for outdoor applications. Also, it has the possibility of extending its range by connecting to the Internet through an access point.

As a result of the following reasons, we have chosen to use this technology. Firstly, it will allow point-to-point connection (ad-hoc) between a user within the range of a tractor and secondly, it will allow the farmer to have the possibility of connecting the tractor to the Internet through a Wi-Fi spot in the farm.

This technology is described in more details in the next section of this chapter.

2.1.2 Long Range

GSM: Global System for Mobile [GSM07] communications is the most popular standard for mobile phones in the world. Its ubiquity makes international roaming very common between mobile phone operators, thus enabling subscribers to use their phones in many parts of the world.

The key advantage of GSM systems to consumers has been better voice quality and low-cost text alternatives to making calls. An example is the Short Message Service (SMS, also called 'small text messaging'). The advantage for network operators has been the ease of deploying equipments from any vendor that implements the standard. Like other cellular standards, GSM allows network operators to offer roaming services so that the subscribers can use their phones on GSM networks all over the world.

EDGE: Enhanced Data Rates for GSM Evolution [3G07], is a cell phone communication norm and an evolution of the GSM. The main advantage is that it supports the UMTS[UMT07] network to propose the same high bandwidth services to more people in the country side.

The cost of EDGE is lower than UMTS because EDGE is only an optimization of the radio part of the GSM network, mainly on the data transmission part. This technology has a bandwidth of 473 kbps. The frequency wide band is the same as GSM: from 890 to 915 MHz for the uplink and 935 to 960 MHz for the downlink.

As EDGEis just a small improvement of the GPRS before the implementation of the UMTS, we decided not to use a technology because it is not supported by all the providers.

GPRS: General Packet Radio Service [Wik07d], is a Mobile Data Service available to users of GSM and IS-136 mobile phones. GPRS data transfer is typically charged per megabyte of transferred data. GPRS can be used for services such as Wireless Application Protocol (WAP) access, Short Message Service (SMS), Multimedia Messaging Service (MMS), and for Internet communication services such as email and World Wide Web access. For this reason we have chosen to use this technology.

It provides moderate speed data transfer, by using the unused Time Division Multiple Access (TDMA) channels in the GSM system. A more thorough description of this technology follows later in this chapter.

WiMax: is a wireless digital communications system that is intended for wireless "metropolitan area networks". WiMax [IEE07] [Gou07] can provide up to 50km for fixed stations, and 5-15km for mobile stations in contrast to the Wi-Fi-network. It allows more efficient bandwidth use, and it is intended to allow higher data rates over longer distances. The current bandwidth of this technology is between 10 to 70 Mbps.

This technology was recently added to the 3G norms for mobile communication. It combines the benefit of broadband and wireless. WiMax will provide high-speed wireless Internet over very large distances and will most likely provide access to large areas such as cities. WiMax-technology is expected to be available in the near future.

For this project, we need a network that can provide high bandwidth and long range like WiMax, and this technology should have been the best. The main problem is that devices with WiMax implementation are not yet on the market for the public. Moreover, the implementation of this technology in countries may vary greatly, and even in the precursors, there are no efficient network coverage yet.

2.2 Wi-Fi Details

In this section, we give more details about the Wi-Fi technology [CDK05], also referenced as IEEE 802.11. The web server in the tractor will get Internet connection using both a Wi-Fi modem and a GPRS modem.

2.2.1 802.11 a, b, g and n

The IEEE committee has submitted several standards in the 802.11 (wireless ethernet) realm. Each standard uses different technology to achieve their classified speeds. Here is a short description of the possible 802.11 technologies that we could chose from as at the time of writing.

The 802.11a standard is able to transmit up to 54 megabits of data per second. It uses orthogonal frequency-division multiplexing (OFDM) [Wik07f], this happens to be an efficient coding technique. It works by splitting radio signal into several sub-signals before they reach a receiver and this helps to greatly reduce interference.

The 802.11b standard is the slowest and least expensive standard, it is popular because of its low cost. It is able to handle up to 11 megabits of data per second. It uses complimentary code keying (CCK) [Wik07b] coding.

The 802.11g standard is able to handle up to 54 megabits of data per second. It uses the same OFDM coding as the 802.11a and this makes it to be a lot faster. A lot of people select the 802.11g standard because of its speed and reliability.

The 802.11n standard is the newest standard that is widely available. This standard has improved range and speed. It is able to achieve speeds as high as 140 megabits per second.

The table below gives an overview of the main differences between the four norms:

Table 2.1: IEEE 802.11 Standard

Norms	Range	Bandwidth (in Mbps)	Frequency
802.11a	10m	54	5GHz
802.11b	300m	11	2,4GHz
802.11g	70m	54	2,4GHz
802.11n	90m	140	2,6GHz & 5GHz

As the 802.11n standard would yield the best range and throughput, that would have been the natural choice, but as we could not obtain the correct hardware, and also, because the standard has not been finalized yet (the current estimate is June 2009 [Wik07e]), and therefore, no hardware to truly

support that standard. The next best standard is therefore the 802.11g standard, which is widely available, and we had direct access to hardware, that supported this standard.

2.2.2 Wi-Fi Billing

Wi-Fi has the advantage of being used to build LANs. Therefore, it is free as long as one is communicating with other members connected to the same LAN. If one want to access another network like the Internet, one needs to make sure that the network is connected to it by contacting an Internet provider. Thus, the only cost for Wi-Fi communication is the price of the subscription.

2.2.3 Wi-Fi Connection

A reason for choosing a medium range wireless access point as a solution for Wi-Fi is its ability to allow a user connect a mobile device directly using Ad-Hoc point to point connection. Secondly, it lowers the cost of the Internet connection and provides increased bandwidth.

2.3 GPRS Details

In this section, we give more detail about the GPRS-technology, according to our requirements. Data access/update between a portable device with Wi-Fi or GPRS capability and the web server in the black box can be achieved by using a Wi-Fi or GPRS connection.

GPRS is a non voice service added to the mobile telephone (GSM) network that can allow us to send and receive information across a mobile telephone network. GPRS allows a user to use a packet-based data service on the existing circuit switched GSM-network. Up to 171.2 kbps is achievable with GPRS using all eight time-slots at the same time.

Recent developments allow web browsing, file transfer and even the ability to remotely access and control in-house appliances and machines using a GPRS-service. GPRS also makes the Internet available to mobile users. To use GPRS, users need a mobile phone or terminal that supports GPRS, a subscription to a mobile telephone network that supports GPRS, a destination to send or receive information through GPRS. In the case of (SMS) Short Message Service this was usually to another mobile phone but in the case of GPRS, it is to an Internet address.

The service of GPRS suits the current requirement due to the fact that in some situations, some of the tractors cannot connect to the Internet because they are located in remote areas or country side where Wi-Fi connectivity may be unavailable. When this is the case, the only way a user can be able to access the web server will be when the tractor is connected to the Internet using its GPRS facility.

2.3.1 GPRS Billing

Data communication over GPRS is billed per megabyte of transferred data whereas data communication over traditional circuit switching is billed per minute of connection time, independent of whether the user transferred data or is idle. This is because even when no data are being transferred, the bandwidth is not available to other potential users.

2.3.2 GPRS Range

Wide area coverage is an attribute of GPRS and can provide coverage and in situations where a machine is located in a remote area, which will render other alternatives impossible, and therefore make GPRS the only connection available for use.

In a situation where both connections are available, if the machine drives outside the range of its Wi-Fi-connection, our system should be able to dynamically switch and use the GPRS-connection.

2.3.3 TCP/IP over GPRS

GPRS being a packet switched network allows (TCP/IP) implementation, this means that each device has an IP address behind the service provider's NAT[CDK05]. When using TCP/IP over GPRS, extra care must be taken because this is different from TCP/IP over network links like the Ethernet. The reason is that GPRS uses "leftover" slots from voice calls and this can downgrade the service of GPRS if a new voice call is started resulting in reduced throughput or packet loss.

As a result of delays that may occur at the provider's NAT, the TCP/IP-protocol may decide to retransmit some packages after some specified time-outs. An occurrence of this kind of retransmission can cause us to incur more cost due to the fact that data communication over GPRS is billed per megabyte of transferred data as mentioned earlier on.

Another point to mention here is that a device behind a provider's NAT cannot be accessed from the outside [CDK05], and as a result of this, access

to the black box from the outside will become impossible. We can get around this impossibility by introducing the tunneling protocol. We shall describe how to achieve this goal in more detail in the design and implementation chapters.

Chapter 3

Analysis

In this chapter, the requirements, constraints, and some of the possible solutions will be listed, for further use in the design.

3.1 Requirements

This section will list the requirements that Lykketronic had for the new system:

1. Transparent Access for multiple users, with multiple users per farm, and multiple farms.
2. Automatic Switching
   (a) Cheapest Possible connection
   (b) Fastest Possible connection
3. Security
   (a) For the system not to compromise data to unapproved 3rd parties (outsiders, or other users without privileges to other users data).
   (b) For the users to not reveal data to outsiders, or other users of the system

3.2 Constraints

This section lists the constraints, that was imposed on the system:

1. The server on the Black Box has Encryption, so, extracting all data for direct database storage is not possible, though, another developer is in the process of adding this functionality.

2. Dynamic IP addresses, is needed, as Static IP's are not an option, as the system is required to run for long period of time, and in that meantime some or all IP's might change, and would render the system unusable with Static IP's.

3.3 Solution proposals

To solve the requirements and constraints imposed on the system, the following technologies were considered:

- A Proxy server would yield a satisfying solution to the requirements of transparent access.
- Connection Switching based on database access, that can determine where the connection originates from IP-wise, and then based on this information, make the database provide a low or high bandwidth version of the content that the user requests.
- A Proxy server would also yield a proper way of handling security and login / access privileges.
- Connection Switching, could also provide access to a "video-feed" between the agricultural machinery to the farm, either as a video conversation between the tractor operator and the farm owner, or as a means of observing the exterior / interior of the tractor, while in operation, either by the tractor operator, or the farm owner, or a remote service technician.

Chapter 4

Design

This chapter describes the design solutions that was chosen. As proposed in the tasks, we are going to implement a solution that will allow a user located anywhere to be able to access data in a remote device located anywhere. We will describe the architecture, details, and functionality.

This means that we will first give a description of the existing system and the choices we have made with regards to our solution. We also have a set of requirement from Lykketronic. This entails a discussion of users that have privileges on the system and what each of these users are allowed to see in the system.

It also comprises of design for ensuring data and communication persistency in the presence of switching between the available networks. Furthermore, we will discuss the security issues and how these might be solved. Finally, we will describe the final prototype which has the desired features with regards to system access, access rights, communication and data persistency and security.

4.1 Description of the Existing System

The initial system, that Lykketronic presented is seen in Fig.1.1. A more detailed description of this system can be found in section 1.1.

As explained in the introduction, the focus of the project was mainly on part 2 of Fig.1.1. This part must allow communication between a web server in a mobile device (in our case – a tractor) and a user anywhere.

4.2 Connection Choice

We decided to use two wireless connections (Wi-Fi and GPRS). These choices will allow us to primarily, be able to access the Internet from any place – which is made possible with the GPRS-connection. Secondly, with

a good bandwidth we can access the Internet with the Wi-Fi connection. These choices must be transparent to the user.

4.3 Design of the Proposed System

Fig.4.1 shows an overall architecture of the proposed solution.

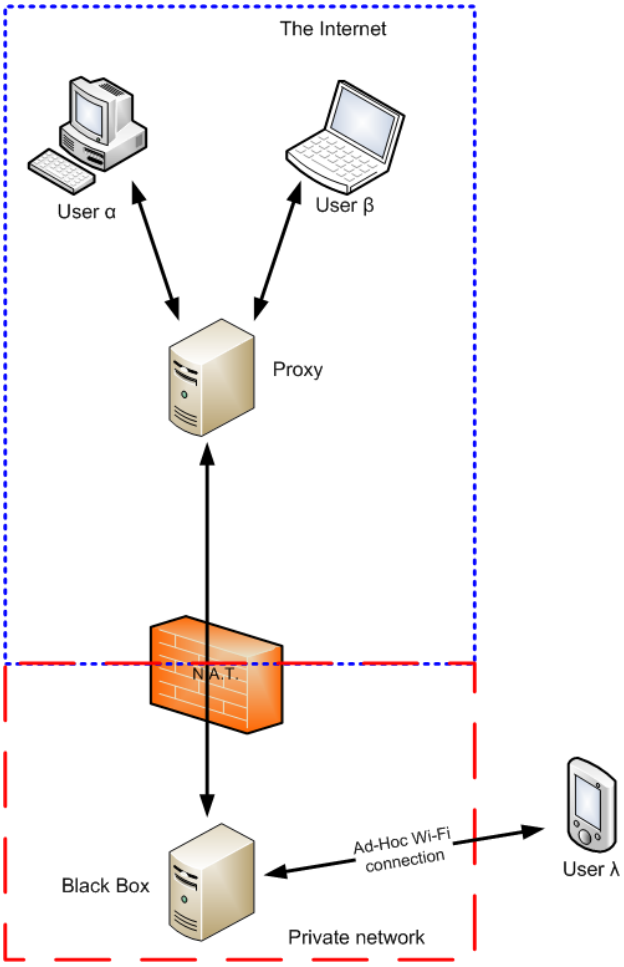


Figure 4.1: Architecture of the system

As seen from Fig.4.1, the proposed solution is made up of two main components. The first one is the Black box (embedded in the tractor) with wireless connections (Wi-Fi or GPRS), while the second one is a Proxy. An

explanation for the inclusion of these components and their functionalities are described in more detail in a later section of this chapter.

There are also some non-functional requirements. The first one is that the user should be able to connect any mobile device that is allowed to access the system without having any physical information about it. Then, there might be a lot of mobile devices and they must all be able to access the system when they are running (or powered on). Finally, the system must be secure. Thus, we have some feasible issues like scaling, security and access problems to solve.

4.3.1 Solution to Access Requirement

Access requirement is an issue mentioned in the previous section, this can be solved by using the Internet as a medium. The point here is that the Black box will be able to connect to the Internet using both a Wi-Fi and a GPRS-connection as explained above, and the user needs to have an Internet access (whichever one is required in this case).

The aim of the Proxy part is to make it possible for the user and the Black box to communicate without the need for any physical information except the url of the Proxy.

4.3.2 Solution to Scaling Requirement

The scaling problem is quite easy to solve with this architecture. This is because a single Proxy can manage a lot of Black boxes. Thus, adding more Black boxes that are accessible implies adding more Proxies to take care of them. This indicates that the cost of adding more black boxes is a constant amount in terms of the Proxy that must be added.

4.3.3 Solution to Security Requirement

To manage the security of the system, we just divided it into different parts, these include the proxy and creating a tunnel. For each part, we designed and implemented the best solutions. The proxy constraints both access to the system and who is allowed to see what in the system. The tunneling also provides secure ssh connection. All of these put together ensure that the global system is very secure.

4.4 Design Overview

In this section, we are going to present an overview of our design and then a section for each of the main parts of the system. The system is summarized in the following schematic:

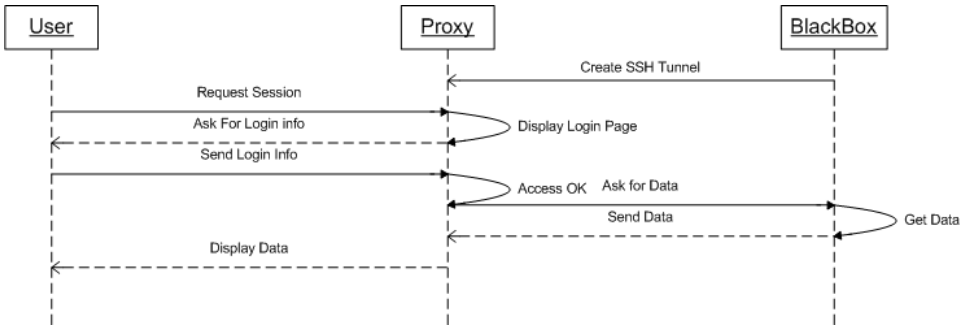


Figure 4.2: Global System Scenario

As we can see in Fig. 4.2, the first step is for the black box to make itself available by initiating a connection to the proxy. The user has to log in before asking for data from the black box. The user's demand for data is relayed by the proxy to black box if the black box is available. After that, the black box responds to the proxy and the data is transmitted to the user.

4.4.1 Black Box to Proxy Overview

The black box takes the initiative of starting a GPRS SSH tunnel to the proxy, as seen in Fig. 4.3. In case of success, if the Wi-Fi-connection is not in ad-hoc mode, the black box will try to connect itself to a Wi-Fi internet network every 15 minutes. If a Wi-Fi internet is available, then the black box will close the GPRS-connection. The black box will also check the connection every 15 min in order to update the port database of the proxy when required. In case of failure the black box will try every 5 min to reach the proxy via GPRS. If the black box is in GPRS mode, then the Wi-Fi is switched into Ad-hoc mode.

4.4.2 User to Proxy Overview

The following schematic (Fig.4.4) focuses on the connection between a user, the proxy and the black box.

The first action is just a summary of the last scheme. The second action is the log of the user via the login page on the proxy. After login, the user will have to choose a tractor to control from the list of available tractors displayed by the proxy. Then the user will perform some actions on the black boxes that he is allowed to access. If the tractor is available, the user will have the answer to the request. If not available, the proxy will display 'tractor not available'.

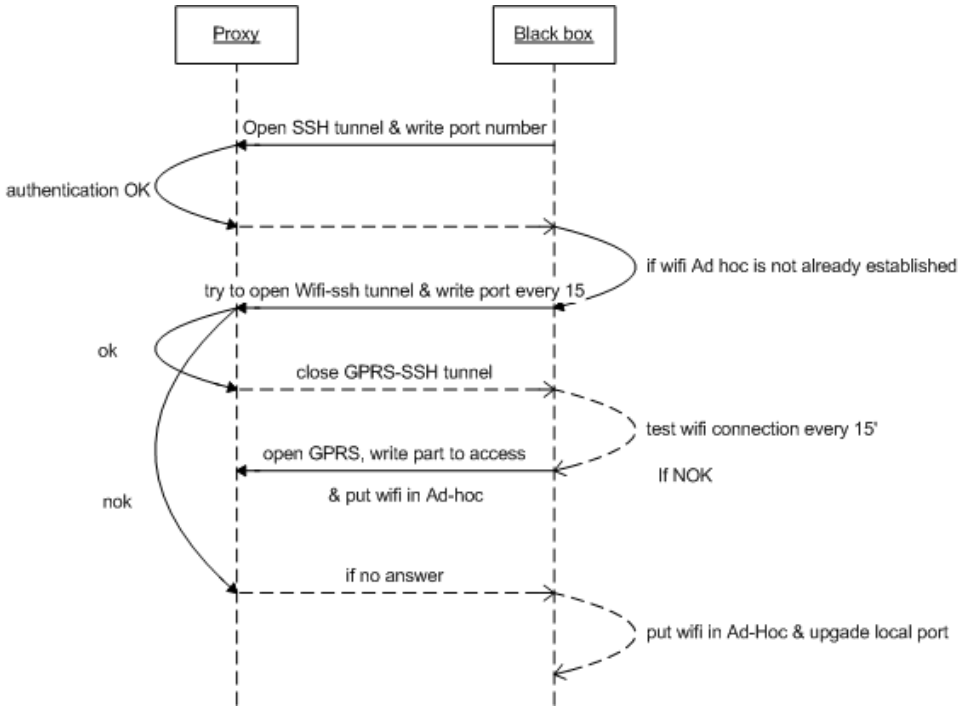


Figure 4.3: Black Box to Proxy Connection

As all actions described in the preceding schematics are small modules, one can adapt them according to the particular need or requirements.

4.5 Design of the Proxy

The aim of this section is to explain the design of a proxy and the use of tunneling protocol. These 2 parts are handled together because they are tightly linked. The proxy is the essential node of our system and tunneling is the way to communicate with this node. The first sub chapter will be about the system's requirements. After that, we will explain our reasons for the choice of a proxy architecture, how it should work and how it has been implemented. Last but not the least are some explanations about our tests which concludes this chapter.

A proxy server can act as an intermediary between a workstation or a network and the Internet in order to ensure security, administrative control or caching services. This will help to protect the workstation or network from the outside world and can also help to reduce the load on some of the individual nodes.

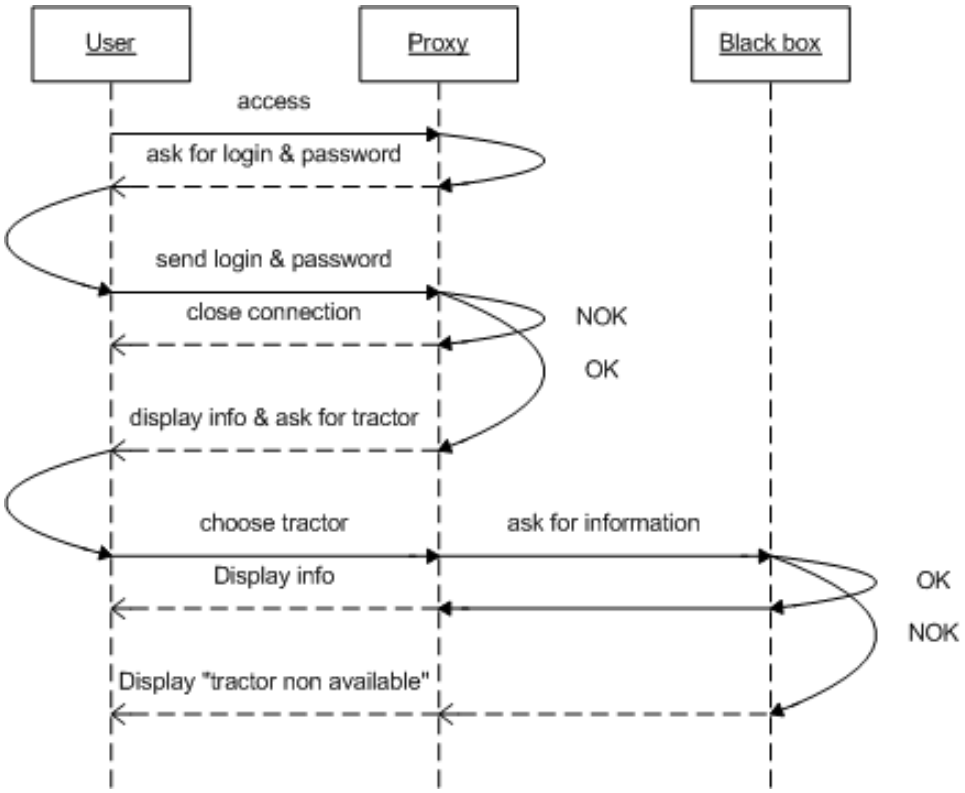


Figure 4.4: User-to-Proxy Experiment

4.5.1 Some Alternative Design Solutions

A possible approach would have been to allow each user have direct connection to a black box, but allowing a user to access the black box directly means that the user knows the black box's IP address and this may not be safe because not all the users are allowed to access the box directly. Also, a box can become over flooded with too many requests from different users which can result in performance bottleneck.

An alternative approach could have been to introduce a proxy that will act as an intermediary between the black box with a GPRS and Wi-Fi-connection and a user. In this case, the proxy does not only handle some security aspects in our system. The proxy will also function by maintaining a table of the IP address for each black box (in this case, the IP addresses will be fixed/static). It will for example be able to, receive requests such as Web page requests from users connected to it and deliver it on behalf of the box. We chose not to use this approach for our proxy because the black box is a highly mobile equipment and maintaining a fixed address for each box is

expensive. By this, we mean that when a tractor moves to an entirely new location, it may move outside the IP address space of its network provider or it may be the case that its provider is not located in the new location. For this reason, they will not be able to connect to the Internet. Also, this approach will require us to obtain two different fixed IP addresses; one for the Wi-Fi and the other for the GPRS connection.

Due to the reason mentioned above, our proxy server will not be able to initiate a connection with the black box because its address is local and only known to the router of the network the box is connected to. For us to be able to get around this problem, we have chosen to make a tunnel between the proxy and the black box.

4.5.2 The Need for a Proxy Server

Having a proxy server is not only useful for caching services, it is also useful for security purposes. This is because to the user, the proxy server is invisible; all Internet requests and returned responses appear to be directly with the black box but this is actually not the case, the fact is that the proxy is not quite invisible in this case; its IP address has to be static and public.

Dynamic IP address scheme and constraint

For this reason, it has been decided to implement a solution using a different approach. This approach will allow the Black box to connect to the Internet using the dynamic IP address scheme [CDK05]. Here, it obtains a dynamic address from a provider when it connects to the Internet. The only problem with this approach is that each Black box that is connected via this means is actually behind a particular provider's router NAT. For this reason, the proxy cannot be configured to forward and redirect all requests to the box.

This constraint comes as a result of the fact, that each box is assigned a dynamic address which is an unregistered IP address. For this reason, these addresses are completely hidden from the rest of the Internet by the NAT's router, thus making it impossible to reach the box from the outside. For us to be able to get around this problem, we have chosen to make a tunnel between the proxy and the black box.

Authentication and Databases

Another main purpose of our proxy is that it will have the responsibility of maintaining a database of authorized users of the system in its local database. In this case, only authorized users can actually access the system and the view of the system a user gets depends on the group or category the user belongs to. This functionality will help ensure access security.

The first service provided by the proxy is authentication in both ways. The user connects to the proxy via Internet within a secure HTTPS connection. The proxy server is intended to make a coherent interface for the user, no matter where he is located. One of its functions is also not to reveal any detail of how data is fetched from the actual tractor units. It maintains a database over all farms, and for each farm, it has a list of tractors with a black box. The proxy server can fetch web-pages from these units and present them in a uniform way. To resume, its goal is to allow many users connect to the system, and give a transparent access to a wide array of tractors/farms all over Europe depending on the authorization of the users connected.

4.6 Tunneling

As stated in section 4.5.2 our proxy server has a limitation of not being able to initiate a connection to the black box. We chose to get around this limitation by introducing a tunnel.

4.6.1 The Need For Tunneling

Before we state the reason for the need for tunneling, it should be noted that firewalls or NAT's exist for the purpose of security of the nodes behind the firewall. In our case, the black box sometimes have to be connected to the Internet using GPRS-connection and this connection has to go through the firewall of a GPRS or Wi-Fi NAT. NATinsures that connections coming from the Internet cannot be established with devices on the local network. This makes it impossible for us to make direct connection to the black box from the outside over the Internet if we need to. Some possible solutions we can use to get around this problem are:

- Alter the firewall rules or create inbound port mapping entries on the NAT device;
- Use some VPN solution;
- Set up a reverse SSH tunnel traffic back to yourself.

We have chosen alternative 3 in this case. Where a black box at start up will initiate a SSH tunnel to the proxy.

Tunneling can allow one to place a packet that uses a protocol not supported on the Internet such as NetBeui inside an IP packet and send it safely over the Internet. Another advantage is that it is possible to put a packet that uses a private (non-routable) IP address inside a packet that uses a globally unique IP address to extend a private network over the Internet. It can also be used to traverse a firewall. In this case, protocols that are normally blocked by the firewall are encapsulated inside a commonly allowed protocol

such as HTTP. Tunneling happens to fit a requirement in this paper which is the ability of the proxy sever to connect directly to the black box when necessary or needed and send packets via the tunnel in a secure way. As a result of this, every connection of a black box initiates a SSH connection with the proxy server.

4.6.2 How Tunneling Protocol Works

Tunneling is basically a process of placing an entire packet within another packet and sending it over a network. The protocol of the outer packet is understood by the network and the *tunnel interfaces*.

Tunnel interfaces are the two points where the packet enters and exits the network. A tunneling protocol is a network protocol which encapsulates a payload protocol, acting as a payload protocol. A reason for tunneling include carrying a payload over an incompatible delivery network, or to provide a secure path through an untrusted network. SSH is frequently used to tunnel insecure traffic over the Internet in a secure way. Tunneling requires three different protocols namely:

- Carrier protocol: the protocol used by the network that the information is traveling over
- Encapsulating protocol: the protocol that is wrapped around the original data (they include GRE, IPSec, L2F, PPTP, L2TP)
- Passenger protocol: the original data being carried (they include IPX, NetBeui, IP)

A tunnel is either a site-to-site tunnel or a remote access tunnel.

In site-to-site tunneling, GRE (Generic Routing Encapsulation) [Wik07c] is normally the encapsulating protocol that provides the framework for how to package the passenger protocol for transport over the carrier protocol, which is typically IP-based. This includes information on what type of packet you are encapsulating and information about the connection between the client and server. Instead of GRE, IPSec in tunnel mode is sometimes used as the encapsulating protocol. IPSec works well on both remote-access and site-to-site tunneling. IPSec must be supported at both tunnel interfaces to be used.

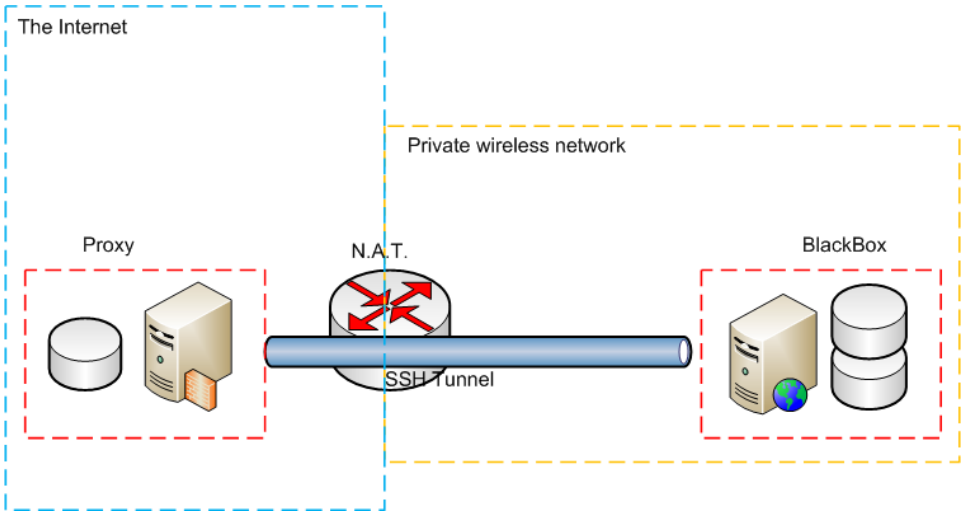


Figure 4.5: Tunneling Scheme

Remote access tunneling normally takes place using PPP (Point to Point Protocol). Part of the TCP/IP stack, PPP is the carrier for other IP protocols when communicating over the network between the host computer and a remote system. Remote-access tunneling relies on PPP.

The incoming tunnel forwards traffic (See Fig.4.5) coming to a remote port to a specified local port. L2TP combines features of both PPTP and L2F, and it also fully supports IPSec. L2TP can be used as a tunneling protocol for site-to-site and as well as remote-access.

4.7 Firewall

This section gives a brief description of the firewall configuration. This configuration is required in both the proxy and in the black box.

A popular firewall package that runs on Linux is iptables. Iptables has some advantages which include the fact that it is the default firewall package installed under RedHat linux - the linux version in the black box is Centos 4.4 which is based on RedHat Linux. Apart from another advantage of its being fast and secure, it also has good integration with the Linux kernel. In addition, it uses the concept of "stateful packet inspection" to keep track of each connection that passes through it.

The firewall serves two purposes; Firstly, it is to block incoming connection to the black box – this is required because incoming connection to the black box is not allowed, it is required that the black box should always

initiate the connection to the proxy. Secondly, it is designed to block all incoming connections to the proxy except the following:

- SSH connections on port 22 - designed only for remote maintenance access.
- HTTPS connections - used for ad-hoc connection.
- Connections involving SSH tunnel ports. The ports are randomly opened during the initialization of the SSH tunnel.

Our iptables configuration defines rules that check incoming packets meant for either the black box or the proxy which are; ACCEPT and DROP. If it says ACCEPT, then the packet continues out to whatever interface it is destined for. Otherwise, this packet is dropped if it says DROP.
These rules are designed to be:

- Executed when a black box creates a SSH tunnel
- Executed when a black box destroys the SSH tunnel
- Executed when a user is logged on and has the right to the access SSH tunnel
- Executed when a user is not logged on anymore or has lost connection- this will destroy the right of this IP address to the SSH tunnel.

4.8 Web Page

This section describes all design concerning the web pages [WT03] available to the user on the Proxy.

4.8.1 User interface

The user interface design will be carried out in parallel with the other design of the system. The user interface design is a diagram which is composed of different parts like other software systems:

The final characteristics of the user interface are:

- The use of alert messages to inform the user about all the actions being carried out.
- The user is allowed to undo an action.
- Another important decision is the user interface navigability, a link is included to allows a user to easily go back to the main page.

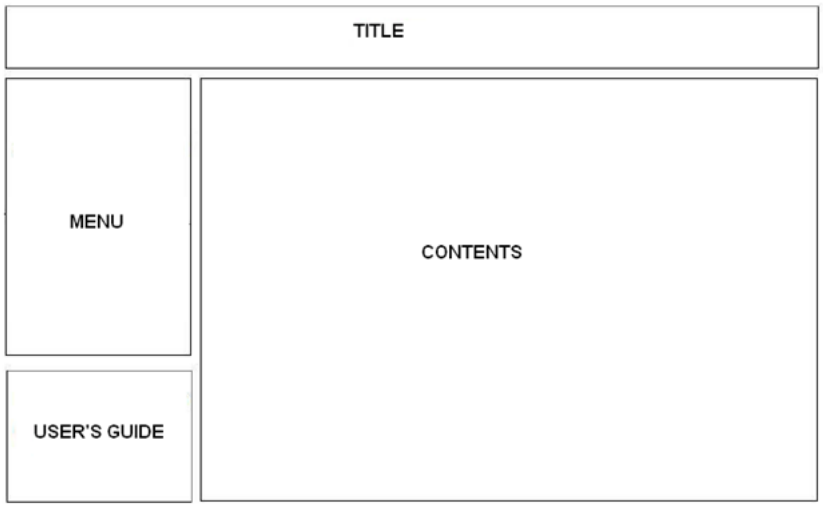


Figure 4.6: User Interface design

The results the experiments gave us are:

- When a user having the right to access the system enters right username and password, then the login part grants him an access. Otherwise, the user is redirected to the first page.
- When a user selects a farm, all tractors which belong to that farm are displayed.
- If a tractor is connected to the Proxy, the web site indicates this to the user by showing colored tractors which is green if connected and red otherwise.
- If a user selects a "red" tractor, the website pops up a warning to inform the user that the tractor is offline.
- If a user selects a "green" tractor, the website pops up a window where the user can find all data he is authorized to view (depending on the privileges defined in the database).
- If either the Wi-Fi or the GPRS is disconnected while the other is running, the information remain displayed on the pop-up.
- If a tractor is disconnected, the database is updated and the website will display the right information highlighting the red tractor otherwise the green tractor is highlighted.

4.8.2 How the Proxy Handles User Login and Authentication

To allow a user access any data on a mobile device through our proxy, we decided to put a login data base, which also provides some useful information about the privileges of a user.

A user wishing to connect to the system makes a HTTPS [WT03] connection to the Proxy over the Internet. The Proxy displays a login web page where the user can enter a username and password to access to the system. The Proxy has a login database where all information about authorized users are stored. This information include their usernames and passwords, this allows the Proxy to know which user can access the system. When a user enters his required username and password, the proxy only has to make queries on its login database and to verify that the data entered by the user is correct or not. If user's data is incorrect, the Proxy will not allow the user to access the system. If the user's data is correct, the Proxy will allow the user to access to the system.

4.9 Connection Switching

The connection switching between GPRS and Wi-Fi is one of the main topics of this report, and it is based on the valuation of connection possibility versus connection price and speed. The requirement is that the system should be able to connect to the machinery at all times and, also, keep any cost derived from that connection to a minimum. So, from this requirement, we will like our system to connect to Wi-Fi whenever it is possible, and only if this is not possible, then it can make its connection via the GPRS-connection.

4.9.1 System Requirements

Currently, there are two types of connections available, namely:

- GPRS
- Wi-Fi

The idea is to automatically switch between the GPRS and Wi-Fi networks as these two network types had the largest availability. There is need to have a system that can switch between the GPRS and Wi-Fi such that the cost is as low as possible and the connection speed the highest (with priority on lowest cost).

4.9.2 Why Connection switching

Connection switching will allow the black box to dynamically switch between the GPRSand Wi-Ficonnection when necessary without any need to restart the box in order to switch connection. It will make it possible to display maximum information to the user using the best connection available. Here are the main points constituting the switching part.

Network Detection

A part of this system will have the task of detecting what kind of connection is available: Ethernet, Wi-Fi internet and Ad hoc. While a Wi-Fi connection is available, the GPRS connection is not launched and when a Wi-Fi connection is launched, the GPRS connection is stopped. When a GPRS connection is enabled, if a Wi-Fi ad hoc connection has not been established before,at every 5 minutes the black box will search if some Wi-Fi internet connection is available. If there is no Wi-Fi internet connection available during the 5 minute cycle, then the black box waits for an ad hoc connection.

Network Throughput

A measurement of how much throughput the current network can handle, would also be used as a determinant of which network you are currently working on. This part will involve measuring the signal strength of the wireless signals to determine which one has more strength.

Connection Testing

For whichever connection launched, some parts of the system will test every 5 min for the availability of that connection to see if it is still enabled or available. If a GPRS connection is not available, this part will try every 2 min to connect the black box to the proxy via a GPRS. If the Wi-Fi internet connection is still not still available, this part will launch the GPRS connection part. If the Wi-Fi ad hoc is not available, the black box will wait for a connection but will check the Wi-Fi internet connection every 5min.

Chapter 5

Implementation

This chapter describes the implementation details of the design discussed in the previous chapter. Here we will describe the simulation of our system. First, we will give a brief overview for the implementation of our network design – here we will give a brief description of the Network Architecture, Network Hardware and Network Software. Next, we will describe the database implementation. Then, we will describe how the proxy can check the connection of the black box – where we will have a look at how a tunnel can be created between a black box and the proxy. Next, we will go on to look at some security aspects as provided by the proxy – here, we will look at firewall configuration in the proxy and black box, and then about Ad-hoc Wi-Fi connection. Finally, we will look at a connection switching implementation.

5.1 Network Design Implementation

The actual implementation is simulated as follows:

5.1.1 Network Architecture

The network is based on ethernet GPRS, Wi-Fi, a laptop computer, the Internet, a black box and a desktop computer.

It uses the following components:

- A GPRS enabled sim card from CBB network which is combined with a Sony Ericsson mobile phone that acts as a modem.
- A USB Wi-Fi dongle whose drivers are installed and configured in the black box
- a laptop computer with Internet access either via wireless or ethernet connection.

- a desktop computer which acts as our proxy server.
- The Internet is simulated by the Aalborg University's LAN.
- of course at least, a black box.

5.1.2 Network Hardware

For this simulation, we have configured the desktop computer to act as a proxy server. Apache web server, MySQL database and server are installed in this computer in order to make it sufficiently robust. The laptop computer simulates a remote user that makes a connection to the proxy server using the IP address of the proxy.

The Sony Ericsson mobile phone is used as a modem in combination with a CBB sim card- Both the phone and the CBB sim card were chosen because they are both good standards for sending and receiving GSM data and also because of their availability.

5.1.3 Network Software

Here, we outline some of the merits for choosing the programming languages used for implementing our application. Apache web server and MySQL database are installed in both the proxy server and black box. The system is also comprised of PHP, java script, python script and bash script. The above specific languages were used in this project for the following reasons.

PHP

PHP [WT03] is used for the design of the dynamic web pages in our system. This are the web pages that allow the users to be able to access our system. PHP is also used in our design for the log in pages and the pages that are used for accessing the database. It is also used for making the necessary database queries.

We chose PHP for the following reasons:

- It is already used in the Black box
- It is open source
- It can be embedded with HTML, Java script and CSS
- Its processing is carried out on the server
- It allows incorporation of interactive elements such as search facilities and message boards, actions such as sending email or buying something

- It allows us to make dynamic web pages
- We knew how to use it before this project.

MySQL

MySQL [WT03] was used for the implementation of the login database and also to create the database queries.

We chose MySQL for the following reasons:

- It is open source
- It is easy to install and deploy
- It is easy to administer as MySQL is a low administration database that eliminates the need for highly skilled and costly database administrators to maintain the database
- It is reliable and highly available
- The embedded MySQL Server Library (lib mysqld) provides in-process data storage engine that delivers all the features of a traditional relational database
- It is platform independent
- It excels in stability, ease of tuning and connectivity
- It offers a high throughput
- Its performance advantage came from a unique feature: the ability to use different database engines on a table-by-table basis
- MySQL supports all the key relational database features

JavaScript

We used JavaScript to validate all the information the users can send. It is also used to show the users alerts about the actions they can perform.

We chose JavaScript for the following reasons:

- It is open source
- It can be embedded with HTML, PHP and CSS
- Its is used to control a page, open and close windows and frames and program access to the history window (which allows the developer to refer to previously viewed documents).

Bash Script

We used Bash Scripts mostly for managing and controlling different softwares without any user input.

For instance we designed a bash script to create the different SSH tunnels between the Black box and the proxy and destroy them when they are not in use anymore. We also developed another bash script that can initiate and terminate the GPRS connection. Some more bash scripts are also designed to regularly check the connection state of the Ethernet Network (Used instead of the Wi-Fi network in our current implementation) and GPRS network and then launch other scripts depending on the state of both network.

We chose Bash Scripts for the following reasons:

- The Bash shell is the default shell on most linux systems, including the version we are using on the Black box.
  It can be run on unix-like operating systems.
- It is a free software
- It has a powerful and flexible way of launching and controlling linux applications.

5.1.4 Database

Here we describe the database design, and the usage of different methodologies.

Design

Database design is used to decide the structure of our database. In the database design, we have to determine the data we can store and the relationship between them.

We use the entity-relationship and relational model [CDK05] to help us to determine which data will form the database and how they are related.

Design and Entity-relationship

Relational Model

When we have done the Entity-Relationship Model the next step is to create the Relational Model using a set of rules. With this we convert the database into “tables”. Relational Model is a model based on tables. We use this

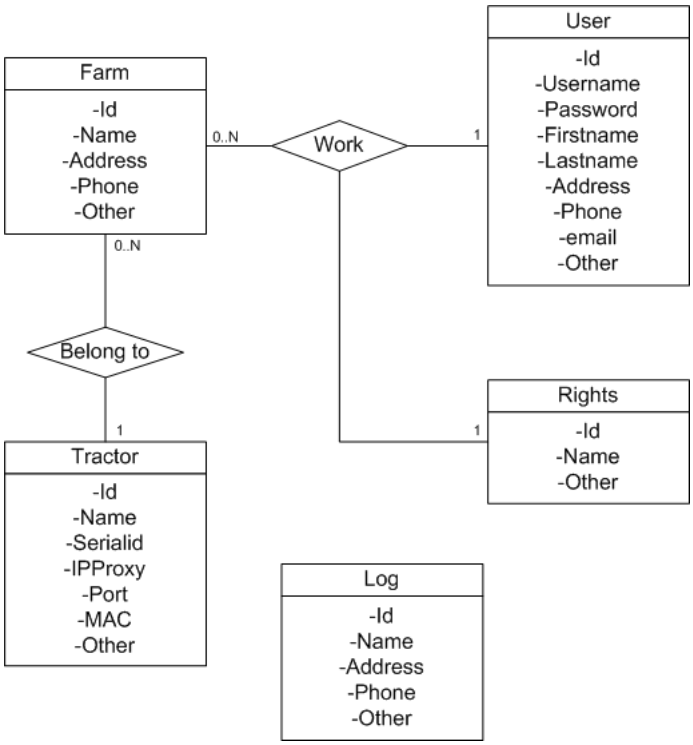


Figure 5.1: Entity-Relationship diagram

relational model of data because it allows us to create a logical representation of information.

Our relational model is the next:

- USER (Id, Username, Password, Firstname, Lastname, Address, Phone, Email, Other);
- FARM (Id, Name, Address, Phone, Other);
- PRIVILEGIES (Id, Name, Other);
- ACCESS (Farmid, Userid, Privilegiesid, Other);
- TRACTOR (Id, Name, Serialid, Other);
- BELONG_TO (Tractorid, farmid, Other);
- LOG (Id, Userid, Date, Time, Log).

Data Dictionary

The definitions and representation of data elements are stored in the data dictionary, which is a set of tables and views. It is a read-only and any user can not alter it.

This Data dictionary [CDK05] has the next information: The consistency between data items across different tables is support by the data dictionary. Here are the data tables used in this project.

User: represents all the users who have access to the system:

Id	Nature	Type	Description	Key
Id	Elemental	Int(5)	Unique number to recognize each user	Primary
Name	Elemental	Varcha(32)	User name	–
Password	Elemental	Varcha(32)	User Password	–
Firstname	Elemental	Varcha(32)	User's name	–
Lastname	Elemental	Varcha(32)	User's last name	–
Address	Elemental	Varchar(192)	User's address	–
Phone	Elemental	Varcha(24)	Number user's phone	–
Email	Elemental	Varcha(32)	User's email	–
Other	Elemental	Varcha(512)	Comment about the user	–

Farm: represents all the farms involved in the system:

Id	Nature	Type	Description	Key
Id	Elemental	Int(5)	Unique number to recognize each user	Primary
Name	Elemental	Varcha(32)	Name of the farm	–
Address	Elemental	Varchar(192)	farm's address	–
Phone	Elemental	Varcha(24)	Number farm's phone	–
Other	Elemental	Varcha(512)	Comment about the farm	–

Privilegies: represents the privilegies that each user has got:

Id	Nature	Type	Description	Key
Id	Elemental	Int(5)	Unique number to recognize each user's privilegies	Primary
Name	Elemental	Varcha(32)	Name of the privilegy	–
Other	Elemental	Varcha(512)	Comment about the privilegy	–

Tractor: represents the tractors that belong to each farm:

Id	Nature	Type	Description	Key
Id	Elemental	Int(5)	Unique number to recognize each tractor	Primary
Serialid	Elemental	int	Tractor's serial number	–
Name				
Port			Port on which the tractor is linked with the proxy	
IPProxy			IP address of the Proxy	
MAC			MAC address	
Other	Elemental	Varchar(512)	Comment about the tractor	–

Log: contains a log/history about actions that has happened at the website:

Id	Nature	Type	Description	Key
Id	Elemental	Int(5)	Unique number to recognize each log	Primary
Userid	Elemental	Int(5)		–
Date	Elemental	date	Log's date	–
Time	Elemental	time	Log's time	–
Log	Elemental	Varcha(512)	log	–

5.1.5 Creation of a wired connection

This was our first step because it allows members of the group to work on the tunneling and others to work on the wireless solutions at the same time. This part was not the most difficult but it required a bash script in the black box. This script launches the DHCP client in order to have a local IP address. Our problem was that the DHCP client was not started when the black box is launched. So a script has been added in the run level 3

of the Black box to launch it.(A run level is a function used by linux OS corresponding to applications to start when the system is launched).

5.1.6 Creation of GPRS connection

The establishment of the GPRS-connection needs a GPRS mobile phone with a credited sim card. In our case, the phone model is a Sony Ericsson W880i. There are no parameters to change on the mobile phone which is used as a modem. There are also no special processes to do with the SIM card to establish the GPRS-connection. This is done using a script written in bash with some pre-loaded parameters.

In that case, the DHCP client is launched automatically.

5.1.7 Creation of Wi-Fi connection

The Wi-Fi implementation has not been done yet. The main reason is the impossibility to install the tools and drivers necessary to implement Wi-Fi on the black box. We can only succeed in installing and implementing the Wi-Fi connection on the proxy using Ubuntu 7.10 linux distribution with a Netgear Wi-Fi USB-dongle if a bigger flash card is available for the black box.

We tried to apply the some process to the Black box by updating our version of centos and recompile its kernel. The problem was that there was not enough memory space to effect this operation. However we tried and unfortunately it did not succeed. Another problem is the fact that we are not able to change the internal memory of the Black box because it is protected by a code from Lykketronic. So, at this stage the situation is blocked because we need more memory in the Black box to use the USB-drivers and moreover Wi-Fitools.

5.1.8 SSH tunneling

We mainly use the SSH tunneling possibilities for two reason :

- It is used to secure and encrypt any data communication between the Black box and the Proxy, ensuring a high level of security during the exchange of sensitive information. This part is more detailed later in this chapter.
- It is also used to get around one of our biggest problem while using a GPRSconnection or a Wi-Fi network. Both can be basically represented like a private network with a NAT(Network Address Translation) which primarily prevents us from establishing a direct connection from the Proxy to the Black box. So it is impossible for us to establish

any request initiated by the Proxy to the black box. Each connection have to be explicitly started by the Black box in order to go through the gateway of those private networks.

As previously stated, we use several SSH tunnels to circumvent the drawback of hosts (in our case the Black box) behind NAT-enabled routers which do not have true end-to-end connectivity.

The specificity of the SSH Tunnel we are using is "forwarded-TCP/IP" option used for server-to-client forwarded connections. With this option, you can specify that the given port on the remote server host is to be forwarded to the given host and port on the local side. This works by allocating a socket to listen to port on the remote side, and whenever a connection is made to this port, the connection is forwarded over the secure channel, and a connection is made to the host port specified from the local machine.

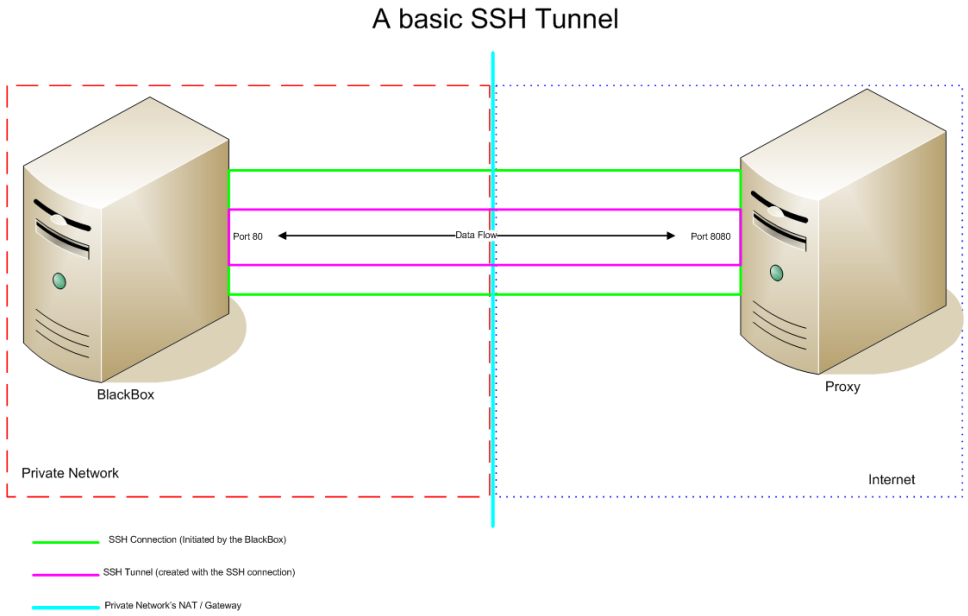


Figure 5.2: A Basic SSH Tunnel

Each Black box has a three ports range allocated for itself in the Proxy's port range of 1500 to 65000. Those three ports are the one used to listen to any connection made to them and forward them to specific ports on the Black box.

For instance, the ports 8080, 8081, 8082 will be allocated to a given Black box. So, in the scripts we created, the Black box's SSH client will initiate a SSH tunnel to the the Proxy's SSH server. The SSH server will allocate a

socket to listen to port 8080 and forward any connections made on this port to the Black box's port 80 (Port listened by the Apache web server).

In this way, when an authenticated user asks to see the Black box web interface, the Proxy sends this request through the port 8080. The SSH tunnel will forward this request to port 80 of the Black box. Then the Black box's web server will respond to this request and send back the web page through the same tunnel. Because the initial request and connection are made by the Black box, then it can cross over the private networks gateways and NAT.

In our current implementation, a third tunnel is needed due to the nature of the AAU network. The Proxy is inside the AAU network as previously mentioned, so the BlackBox can directly reach it from the Internet. In fact, the AAU network is another private network, however a second SSH Server (called homer.cs.aau.dk) has access to both Internet and the private AAU network. We use this server as a "bridge" between the Internet and the Proxy. The BlackBox asks homer.cs.aau.dk to create a tunnel between the Proxy and the BlackBox. Then the BlackBox can use this tunnel to make any SSH request to the SSH Server embedded in the Proxy.

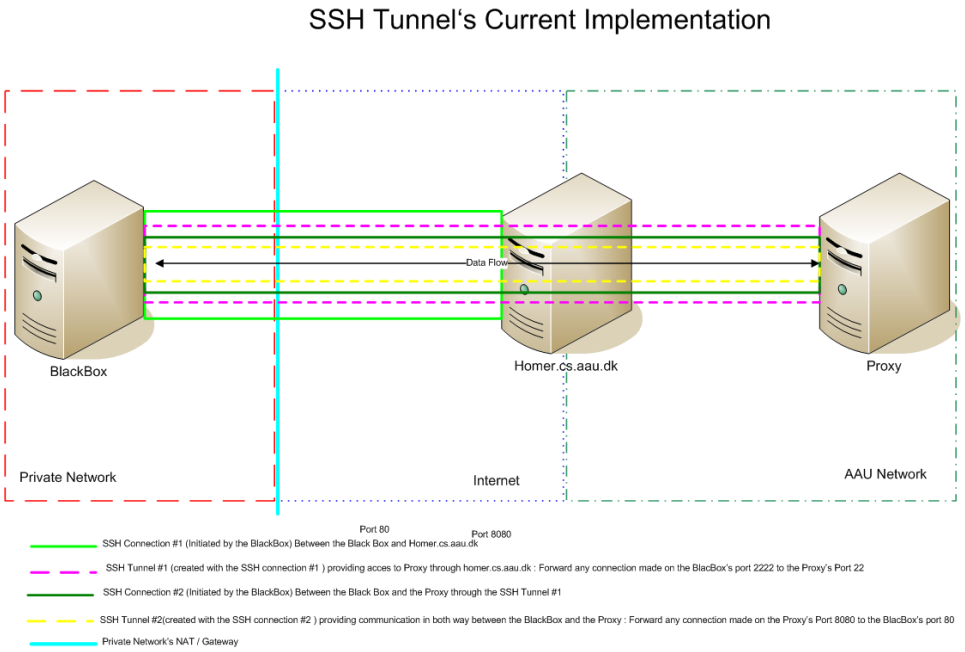


Figure 5.3: Current Implementation of SSH Tunnels

5.1.9 Connection Switch

This part is quite complex and uses scripts. Some of them are included in the preceding parts. For example, the GPRS-connection and the Wi-Fi connection. There will not be a script dedicated to connection switching, but some scripts connected with each other will share this responsibility. We will use the cron table of the centos distribution for the connection timed scripts. These scripts will follow the rules enabled in the design part and will update whenever there is a change in the database on the proxy. The Wi-Fi internet connection script will stop the GPRS-connection if working but the GPRS connection script will not stop the Wi-Fi internet connection. The Wi-Fi internet checker will not stop the Wi-Fi ad hoc connection if this one is in use. If the Wi-Fi internet connection is detected "down" by the connection-checker script, it will launch the Wi-Fi internet connection script.

It has to be noticed that the qualification of those scripts, these goals and structures have been studied but not implemented at the moment because of the impossibility to implement the Wi-Fi on the black box.

5.1.10 How the Proxy checks the connection of the black boxes

In order to be efficient, the proxy must check regularly the available connections with the tractors it is in charge of. This is done using a python script located on the proxy. Python script is used instead of bash script because bash script is not able to send 'get' requests over the Internet.

The script first detects the ports currently in use by checking the connections in the tractor database. If the address in the port column different from '0', it means that a connection with the tractor is possible. So, asking a `GET` request to this address means by the mechanism of SSH tunneling asking a web page of the HTTP server of the black box. Then, the script analyzes the status returned by the `GET` request. If the status is true it means that the connection is still available. Otherwise there is a problem and the connection is not available and then the script updates the database by setting a 0 in the port number corresponding to this tractor.

5.1.11 Firewall Configuration in the Proxy and Black box

To be able to connect to the black box which is behind a NAT, a Black box must create a SSH tunnel to the proxy server. But it is not possible for the proxy to easily determine who is connected to the tunnel in order to allow or deny such access. Below is a proposed solution to this problem.

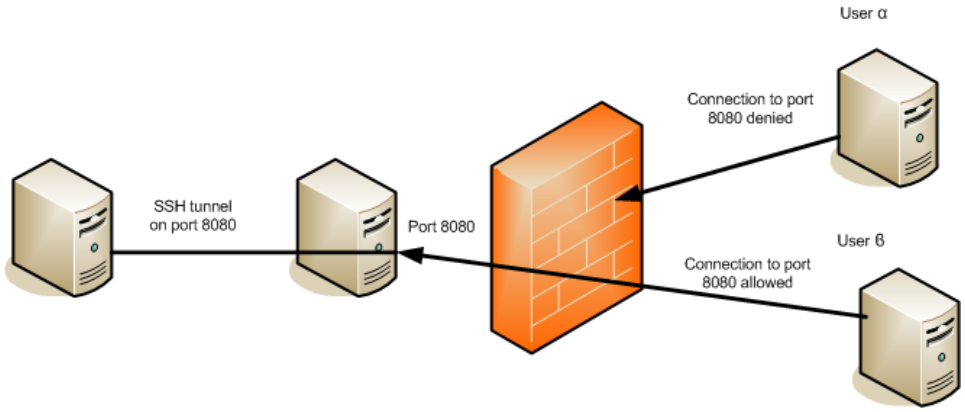


Figure 5.4: Firewall on the proxy server to protect SSH tunnels

By default, the firewall on the proxy will deny all the connection to the SSH tunnel. Once a user is logged on the login page of the proxy, a script is launched, this script adds a rule to the firewall in order to allow the IP address of the user to access the port of the SSH tunnel. When the user logs out or after a long time without any activity from the user, another script is launched to remove the rule on the firewall which allowed the IP address of this user.

A firewall has also been added to the black box in order to protect it. The black box is behind a NATwhen it uses the GPRS connection and when it uses a Wi-Fi access point as gateway to access internet. So, there is a low probability that someone can be able to connect to the black box. But we decided to add a firewall because the black box might be in the future with another connection without NAT.

An other script has also been created, this script resets the firewall rules of the proxy every hour to prevent crashes. It is useful only for the development when a wrong rule is added on the proxy and block the incoming connection. Then, a developer would not be able to access the proxy by networks.

5.2 Security

There are several part to secure in this implementation. Here is a scheme to enlighten us on those parts.

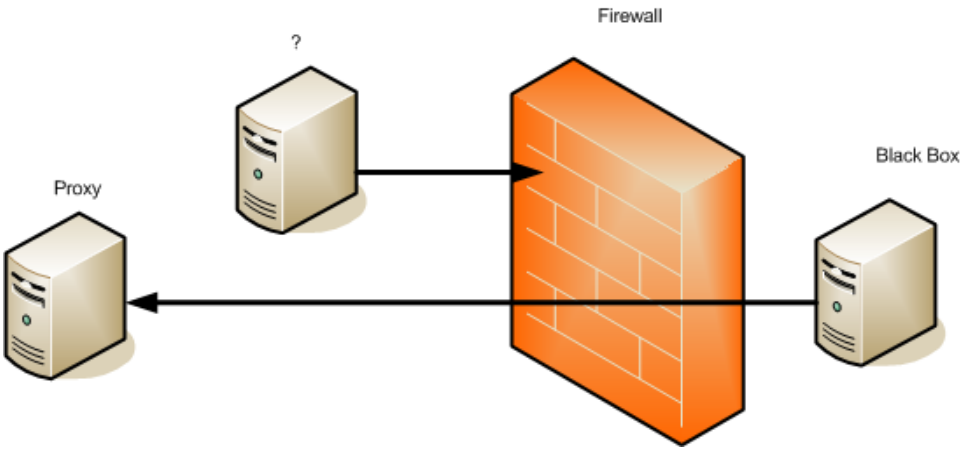


Figure 5.5: Firewall on the black box

5.2.1 User-to-Proxy with HTTPS

The user need to connect to the proxy and send authentication data to be allowed to see any information on the system. Thus, we need to secure this channel of communication.

5.2.2 Proxy-to-Black Box with SSH and RSA-based login

All the information which goes from or to the Black box must be secure. The main reason is that such information can modify how the tractor is working and may inform anyone of what has occurred. Moreover, some personal information may also be transmitted through this channel.

With the use of SSH tunnel, we provide a high security level to this part of the system. Indeed, the SSH protocol provides data encryption and also the assurance that only the receiver will be allowed to see those data. This tunnel is usually a channel between only two entities. In our case, the two entities involved are the tractor on one side and the proxy on the other.

There can be one problem. In fact the SSH tunnel initialization requires sending both a login and a password from one entity to the other. But there is another way to do this: the use of a login associated with a RSA key. Therefore, this solution provides a higher level of security because this protocol requires that both the proxy and the tractor have been initialized and synchronized at least once. There is also the use of public/private key which avoids any "man in the middle" attack, because with only a public key, one can do nothing.

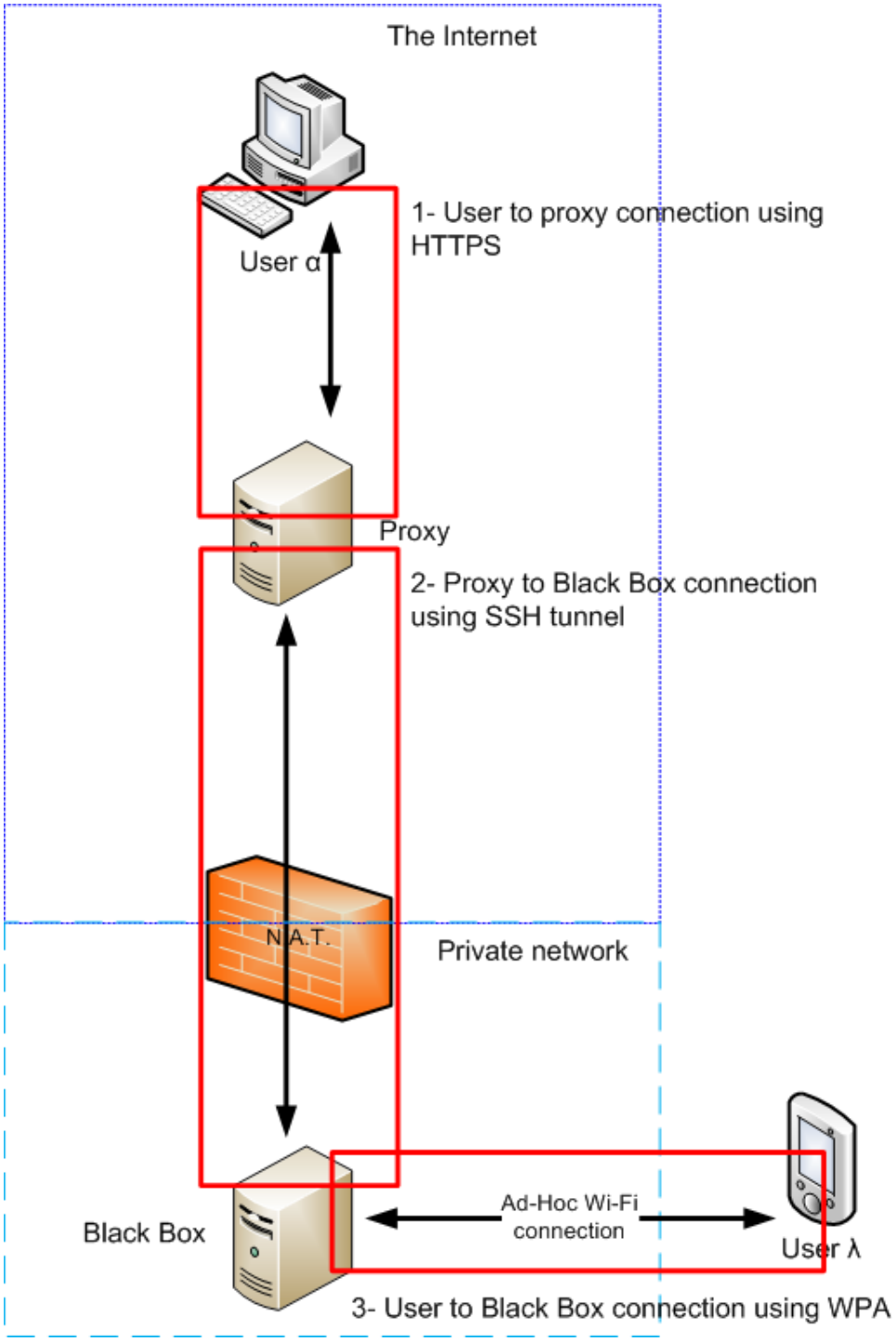


Figure 5.6: Security parts of the architecture

Chapter 6

Testing and Experiments

This chapter describes the test scenarios that were carried out to verify the system. Also included, are the results obtained from the tests which show, that the project requirements were met.

6.1 Test Scenarios

In this section, we describe all tests we made to be sure the entire system is working as we want. Therefore, in order to improve the understanding and to show how we proceeded, we describe in a first time all the tests for each unit of the system.

As those tests were just done to be sure the system works, all were done with wired connection between the Black box and the Proxy.

6.1.1 Login

To test if the login on the website functions properly, we tried to log in with non-existing users, existing users with wrong password and existing users with right password.

The scenario is described in figure 5.1.

The results of this test are:

- with non-existing users: the web page reacts as we want. It returns an error which informs the user that either the entered login or password is incorrect
- with existing users and wrong password: the web page reacts in the same way as the previous test

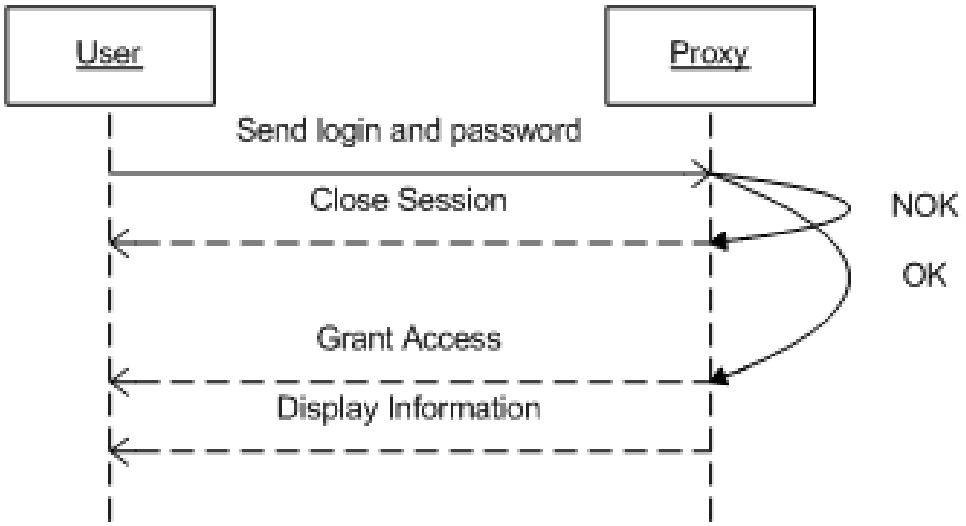


Figure 6.1: Login Test Scenario

- with an existing user and the right password: the web page reacts by granting the user access to the website.

The result is that this part functions correctly as expected, it grants access to registered users but refuses access to unregistered users. It also refuses registered users with wrong password.

6.1.2 Connection Switch

For this part, we a used wired and GPRS-connection to test the switch. The wired connection here simulates the Wi-Ficonnection.

The scenario is described in figure 5.2.

With this test scenario, we can verify that our switch is working.

6.1.3 Tunneling

To be sure that this part is working, we just put a link on the web page with the url of the tunnel, which represents the IP of the proxy and the port of the Black box: 192.168.1.1:2000.

The scenario is described in figure 5.3.

The result of this test shows us that this part function very well. If the tunnel is open, then it is possible to access the web server of the remote device.

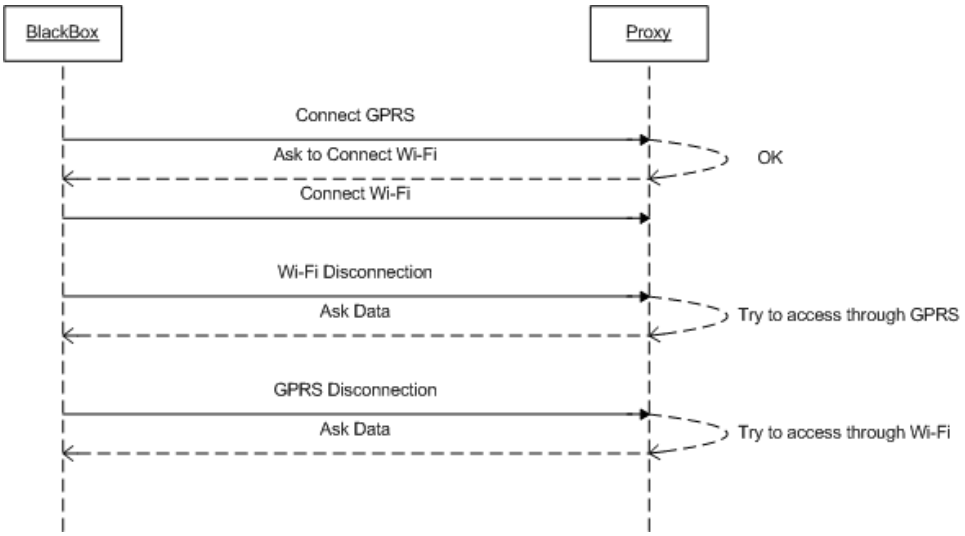


Figure 6.2: Connection Switch Test Scenario

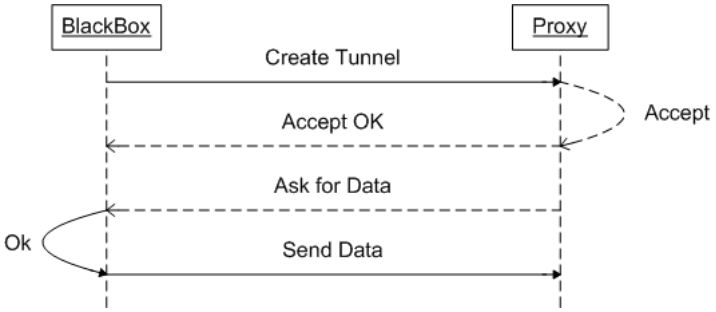


Figure 6.3: Tunneling Test Scenario

6.1.4 Global system

Since the previous parts function well, we have to be sure that they will work together. We therefore implement each of these parts together.

We tried to login with a authorized user's login name and password, display the information of this user, the farm and tractor of this user. Then, we selected one tractor of this user and tried to access it with both the GPRS and Wi-Fi connection. To enlighten more on this, figure 5.4 describes the scenario.

As a result, we logged-in on the system, then selected a connected tractor and got the information displayed in a pop-up window.

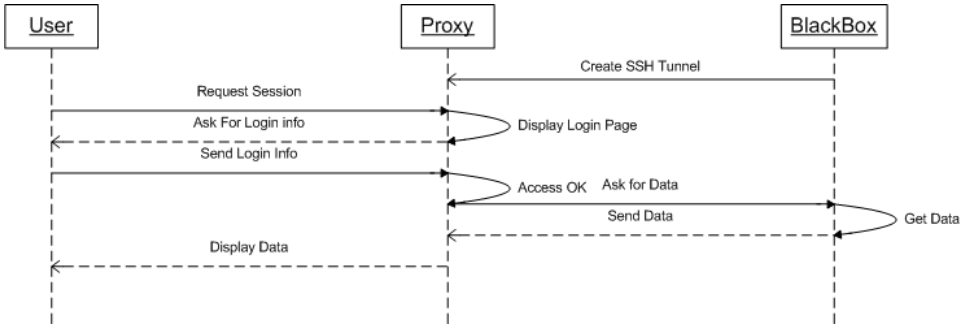


Figure 6.4: Global System Test Scenario

Chapter 7

Improvements

The aim of this chapter is to give an overview of what could be done to improve the actual solution. These improvements are to be considered future work for two main reasons. The first is because some the improvements depend on the requirements of this project, e.g. adding more proxies. The other reason is that some improvements are based on new technologies, e.g. the WiMax, thus, as long as those technologies are not available at the moment, it is not possible to implement them.

7.1 Ad-hoc Wi-Fi Connection

When a user is very near to a tractor he has the possibility to access the tractor and this kind of access can be made to the tractor data using a laptop, a PDA, a cell-phone, etc. This kind of connection is made possible because the user is within the range of the Wi-Fi network of the tractor. The user makes such connection via an ad-hoc connection. In this way they do not need an Internet connection because there is a peer-to-peer connection between them. The ad-hoc connection allows the user to connect directly to a tractor without the obligation to connect to the Proxy. This kind of peer-to-peer connection is made possible as a result of the fact that the login database is installed on both the proxy and on the tractor.

The Ad-Hoc connection allows a user to connect directly to a tractor without the obligation to connect to the Proxy. This is only possible when the user is within the range of the Wi-Fi network of the tractor.

The scenario is quite easy to understand and implement.

Another improvement concerning the Ad-Hoc could be the add of WPA protection (Wi-Fi Protected Access) which is more secure than the WEP (Wired Equivalent Privacy). This could make the channel secure and only users with the adequate key can log on the Black box.

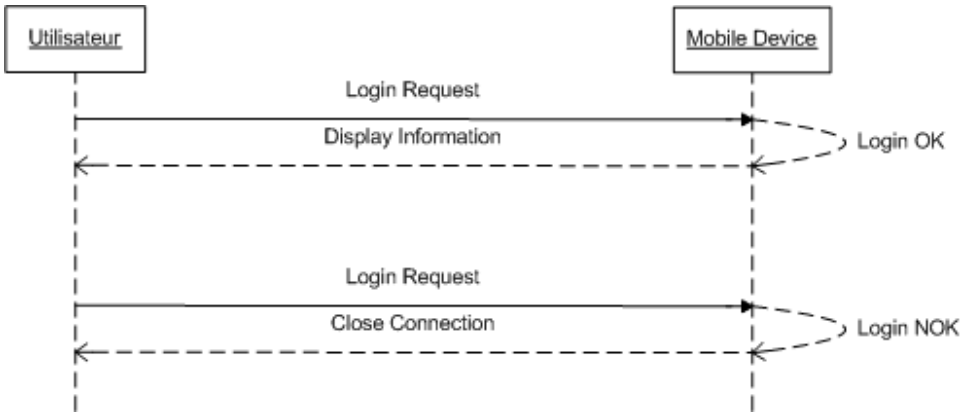


Figure 7.1: Ad-Hoc login Sequence Diagram

7.2 WiMax

New technologies are being developed and third generation of cell phone network is not yet implemented everywhere, so we have decided not to focus on those technologies, but to rely on existing ones.

The first improvement that can be done, and which can provide a lot of new functionalities is the use of WiMax to allow the Black box to communicate. Indeed, as the WiMax is 3G norms for cell phone and also proposes the same functionality as Wi-Fi. In this case, there will be only one network on the Black box, and no need to switch between two networks.

As the theoretical range of IEEE 802.16 family is around 70 km, but in fact around 15 km, we can say that a first idea of improvement with the WiMax technologies is to replace the GPRS network of the Black box, in order to benefit from the higher (around 50 times) bandwidth, from a provider. The second idea is to propose to a farmer to install a WiMax access point in his own farm, connected to the Internet through a common wired network. This second solution will allow a farmer to access all of his tractors in a "local" network of around 15 km range, without paying more than the Internet connection for his farm.

7.3 Adding Proxies

As one Proxy can only handle a lot of different mobile devices, one might want to add more proxies to handle more devices. There are two main ways of doing it. The first one is just to add another proxy, with its own IP/URL

and its own mobile devices. The other way to it is to put several proxies behind a router and create a SSH tunnel for each proxy.

With this possibility, one can build an entire distributed system with some proxies able to handle a lot more different mobile devices and one database for both caching and login services of the system.

7.4 How a Proxy Can Handle the Connection of a New Box

Part of the improvements could be to be able to automatically update the table of the tractors on the proxy via a code transmitted during the first connection. Then, the information could be transmitted and a script can handle these update of the configuration of the new black box. Another solution which is more simple could be that as LYKKETRONIC will own both the proxy and the black box, the black box could be initialized in LYKKETRONIC premises by linking the black box and the proxy via a cable and doing the configuration manually with a technician.

Chapter 8

Conclusion and Future Work

From the initial system, and the envisioned system seen in Fig.1.1 we have implemented all of the requirements into the system. That is, it is now possible for a user to gain transparent access via a proxy server to an agricultural device, from a hand held mobile device. It is possible to via a proxy server to both, read and write data onto the local computer of the machinery. Also, we have the ability to remotely control it, if you have the appropriate privileges. Furthermore, security have been implemented such, that only authorized users are be able to gain access to any unit.

References

[3G07] 3rd Generation 3G. Edge general desription. 2007. http://www.3g-generation.com/gprs_and_edge.htm.

[CDK05] George Colouris, Jean Dollimore, and Tim Kindberg. *Distributed Systems Concept and Design.* Addison Wesley, fourth edition, 2005.

[Gou07] Equipement Gouv. Wimax (french) desription. 2007. http://extranet.ant.cete-ouest.equipement.gouv.fr/article.php3?id_article=9.

[GSM07] World GSM. Gsm general desription. 2007. http://www.gsmworld.com/technology/index.shtml.

[IEE07] IEEE. Ieee wimax general desription. 2007. http://ieee802.org/16/.

[Lyk07] Lykketronic. Lykketronic company web site. 2007. http://www.lykketronic.dk.

[RB97] GMBH Robert Bosch. Bosch 'can' specification. 1997. http://www.semiconductors.bosch.de/pdf/can2spec.pdf.

[Sko07] Skov. Skov a/s company website. 2007. http://www.skov.com.

[SMFB99] Marvin L. Stone, Kevin D. McKee, C. William Formwalt, and Robert K. Benneweis. Iso 11783:an electronic communications protocol for agricultural equipment. *ASAE Distinguished Lecture #23, Agricultural Equipment Technology Conference, 7-10, February 1999, Louisville, Kentuky, USA*, (913C1798), 1999. http://asae.frymulti.com/data/pdf/6/ddp2002/lecture23.pdf.

[UMT07] World UMTS. Umts general desription. 2007. http://www.umtsworld.com/technology/technology.htm.

[Wik07a] Wikipedia. Bluetooth general description. 2007. http://en.wikipedia.org/wiki/Bluetooth.

[Wik07b] Wikipedia. Complimentary code keying. 2007. http://en.wikipedia.org/wiki/Complementary_code_keying.

[Wik07c] Wikipedia. Generic routing encapsulation. 2007. http://en.wikipedia.org/wiki/Generic_Routing_Encapsulation.

[Wik07d] Wikipedia. Gprs general description. 2007. http://en.wikipedia.org/wiki/General_Packet_Radio_Service.

[Wik07e] Wikipedia. Ieee 802.11n general description. 2007. http://en.wikipedia.org/wiki/IEEE_802.11#802.11n.

[Wik07f] Wikipedia. Orthogonal frequency-division multiplexing. 2007. http://en.wikipedia.org/wiki/OFDM.

[Wik07g] Wikipedia. Zigbee general desription. 2007. http://en.wikipedia.org/wiki/ZigBee.

[WT03] Luke Welling and Laura Thomson. *PHP and mySQL Web Development*. Sams, second edition, 2003.

[Zig07] Alliance ZigBee. Zigbee alliance website. 2007. http://www.zigbee.org/en/index.asp.